Sabancı Üniversitesi

Faculty of Engineering and Natural Sciences

Prescribing coefficients of invariant irreducible polynomials

Giorgos Kapetanakis

Supported by TÜBİTAK Project 114F432

May 20, 2017

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

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

  It is clear that the above defines an action of $\mathrm{GL}(2, q)$ on $\mathbb{F}_q[X]$.
- We define the following equivalence relations for $A, B \in \mathrm{GL}(2, q)$ and $F, G \in \mathbb{F}_q[X]$.

$$\begin{aligned} A \sim B &\iff \exists\, C \in \mathrm{GL}(2, q) \text{ such that } A = C^{-1}BC, \\ A \sim_q B :&\iff A = \lambda B, \text{ for some } \lambda \in \mathbb{F}_q^* \text{ and} \\ F \sim_q G :&\iff F = \lambda G, \text{ for some } \lambda \in \mathbb{F}_q^* \end{aligned}$$

- For $A \in \mathrm{GL}(2, q)$ and $n \in \mathbb{N}$, we define

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

where $\mathbb{I}_n$ stands for the set of monic irreducible polynomials of degree n over $\mathbb{F}_q$.
- Recently, the estimation of the cardinality of $\mathbb{I}_n^A$ has gained attention (Garefalakis 2010, Stichtenoth-Topuzoğlu 2011, Reis 2017).

A famous result in the study of the distribution of polynomials over $\mathbb{F}_q$ is the following.

Theorem (Hansen-Mullen irreducibility conjecture)

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

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

- The latter had been conjectured by Hansen and Mullen 1992.
- It was initially proved for $q > 19$ or $n \geq 36$ by Wan 1997,
- while Han and Mullen 1998 verified the remaining cases by computer search.
- Several extensions to these results have been obtained (e.g. Cohen 2005, Cohen-Prešern 2006, Garefalakis 2008, Fan 2009, Panario-Tzanakis 2011).
- While most authors use a variation of Wan's approach, recently new methods have emerged (Ha 2016, Pollack 2013, Tuxanidy-Wang 2017).

- One special class of polynomials are self-reciprocal polynomials, that is polynomials such that $F^R := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \circ F = F$, where F^R is called the reciprocal of F.
- The problem of prescribing coefficients of such irreducible polynomials has been investigated (Garefalakis 2010, Garefalakis-Kapetanakis 2012, Garefalakis-Kapetanakis 2014).
- Nonetheless, a description of the coefficient of the polynomials of $\mathbb{I}_n^A$ has not yet been investigated for arbitrary A.

Here are the results of a quick experiment for $q = 3$.

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

Table: The set $\mathbb{I}_6^A$ for different A.

- Here, 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 $F \in \mathbb{I}_n^A$ can or cannot take any value in $\mathbb{F}_q$ are provided.
- For the former case we prove sufficient conditions for the existence of polynomials of $\mathbb{I}_n^A$ that indeed have these coefficients.

If A has one eigenvalue, then

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

The first situation is already settled. For the second case, we have that that $A \circ F \sim_q F \iff F(X) \sim_q F(X+\alpha) \iff F(X) = F(X+\alpha)$. The polynomials with this property are called periodic. We prove that the following characterizes those polynomials explicitly.

Lemma

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

It is now clear that we need the following theorem.

Theorem (Agou, 1977)

Let q be a power of the prime p, $\alpha \in \mathbb{F}_q$ and $P \in \mathbb{I}_n$. 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 $\mathbb{F}_q \to \mathbb{F}_p$.

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

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 $\mu \geq 2$.

We define to the following map

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

where $\mathbb{G}_\mu := \{f \in \mathbb{F}_q[X] \mid \deg(f) \le \mu,\ f_0 = 1\}$. We will need to correlate the inverse image of σ with a set that is easier to handle. The following, serves that purpose.

Proposition (Garefalakis-Kapetanakis, 2012)

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

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

is a bijection.

The following summarizes our observations.

Proposition

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

We define the following weighted sum

$$w := \sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) \sum_{\substack{P \in \mathbb{J}_n,\ \psi(P) \neq 1 \\ P \equiv HF^{-1} \pmod{X^{\mu+1}}}} 1,$$

where F is the polynomial defined earlier and Λ is the von Mangoldt function. Clearly, if $w \neq 0$ we have our desired result.

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

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

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

Proposition

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

1. *If* $\chi \notin \langle\psi\rangle$*, then* $\left|\sum_{\substack{P\in\mathbb{I}_n \\ \psi(P)\neq 1}} \chi(P)\right| \leq \frac{2(p-1)}{pn} \cdot (\deg(M) q^{n/2} + 1)$,
2. *If* $\chi \in \langle\psi\rangle^*$*, then* $\left|\sum_{\substack{P\in\mathbb{I}_n \\ \psi(P)\neq 1}} \chi(P)\right| \leq \frac{\pi_q(n)}{p} + \frac{2p-3}{pn} \cdot (\deg(M) q^{n/2} + 1)$.
3. *If* $\chi = \chi_0$*, then* $\left|\sum_{\substack{P\in\mathbb{I}_n \\ \psi(P)\neq 1}} \chi(P)\right| \geq \frac{(p-1)\pi_q(n)}{p} - \frac{p-1}{pn} \cdot (\deg(M) q^{n/2} + 1)$,

   Where $\pi_q(n)$ *stands for the number of monic irreducible polynomials of degree* n *over* $\mathbb{F}_q$.

By adjusting Wan's approach to our case, we prove that a sufficient condition for our desire result is

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

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 $2 \leq \mu \leq n/2$.

Theorem

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

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

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

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

If A has two distinct eigenvalues, then $[A] \sim [B]$, where $B = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for some $\alpha \in \mathbb{F}_q^*$. It is clear that $F \in \mathbb{F}_q[X]$ 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 $\mathbb{F}_q^*$ of multiplicative order r. A polynomial $F \in \mathbb{F}_q[X]$ satisfies $F(X) \sim_q F(\alpha X)$ if and only if there exists some $G \in \mathbb{F}_q[X]$ and $k \in \mathbb{Z}_{\geq 0}$ such that $F(X) = X^k G(X^r)$.

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

Theorem (Cohen, 1969)

Let $P \in \mathbb{I}_n$ 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 irreducibility of $P(X^r)$ depends solely on the choice of p_0.
- It is known that we have exactly $\phi(r)(q-1)/r$ choices for p_0. We denote this set by $\mathfrak{C}$, while the primitive elements of $\mathbb{F}_q$ are in $\mathfrak{C}$.
- Notice that we already have enough to prescribe the coefficients of the polynomials in $\mathbb{I}_{n'}^{B}$.

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

The lemma below provides a correlation between $\mathbb{I}_{n'}^{C}$ and $\mathbb{I}_{n'}^{D}$, if $[C] \sim [D]$.

Lemma

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

$$\phi \ : \ (\mathbb{I}_{n'}^{C} / \sim_q) \to (\mathbb{I}_{n'}^{D} / \sim_q), \ [F] \mapsto [U \circ F],$$

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 $\mathbb{I}_{n'}^{B}$ imply that $\mathbb{I}_{n'}^{A} \neq \emptyset \iff r \mid n'$, 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 $Q \in \mathbb{I}_{n'}^{A}$, as a linear expression of the coefficients of some $P' \in \mathbb{I}_{n'}^{B}$. In particular, since both A and B are lower-triangular, there exists some $U = \left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, q)$ such that $Q = U \circ P'$.

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 $\kappa \in \mathbb{F}_q$. Next, we fix $\sigma : \mathbb{G}_\mu \to \mathbb{F}_q$, $H \mapsto \sum_{i=0}^{\mu} \delta_i h_i$ and set

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

It is now clear that if $w \neq 0$, then there exists some $P \in \mathbb{I}_n$ 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 $Q \in \mathbb{I}_{n'}^{A}$ with $q_m = \kappa$.

- 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 $1 \leq \mu \leq n/2$ for $n \geq 5$ and $q \geq 31$ and for $n \geq 47$ and arbitrary q.

Theorem

Let $[A] \in \mathrm{PGL}(2,q)$ *be such that* $[A] \sim [(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix})]$ *for some* $\alpha \in \mathbb{F}_q$ *of order* $r > 1$ *and* $0 \leq m \leq n'$. *First,* $\mathbb{I}_{n'}^A \neq \emptyset \iff r \mid n'$, *so assume* $n' = rn$. *Further, set* $\mathfrak{C} := \{x \in \mathbb{F}_q \mid \gcd(r, (q-1)/\mathrm{ord}(x)) = 1\}$. *If* $[A] = [(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix})]$, *then for any* $P \in \mathbb{I}_{n'}^A$, $p_i = 0$ *for all* $r \nmid m$ *and* $p_0 \in \mathfrak{C}$, *while for any* $\kappa \in \mathbb{F}_q$ *there exists some* $P \in \mathbb{I}_{n'}^A$ *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* $[A] \neq [(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix})]$, *compute* $a, c, d \in \mathbb{F}_q$ *such that* $[A] = [UBU^{-1}]$, *where* $B = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $U = \left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right)$ *and for* $0 \leq i \leq n - \lceil m/r \rceil$, *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* $\mu \leq n - \lceil m/r \rceil$.

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

Thank You!