Prescribing coefficients of invariant irreducible polynomials

Giorgos Kapetanakis[1]

Faculty of Engineering and Natural Sciences, Sabancı Üniversitesi. Ortha Mahalle, Tuzla 34956, İstanbul, Turkey

Abstract

Let $\mathbb{F}_q$ be the finite field of q elements. We define an action of $\mathrm{PGL}(2,q)$ on $\mathbb{F}_q[X]$ and study the distribution of the irreducible polynomials that remain invariant under this action for lower-triangular matrices. As a result, we describe the possible values of the coefficients of such polynomials and prove that, with a small finite number of possible exceptions, there exist polynomials of given degree with prescribed high-degree coefficients.

Keywords: Hansen-Mullen conjecture, Finite fields, Character sums
2010 MSC: 11T06, 11T23

1. Introduction

Let q be a power of the prime number p. By $\mathbb{F}_q$ 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 $F \in \mathbb{F}_q[X]$. Following previous works [10, 22, 24], define

$$A \circ F = (bX+d)^{\deg(F)} F\left(\frac{aX+c}{bX+d}\right). \tag{1}$$

It is clear that the above defines an action of $\mathrm{GL}(2,q)$ on $\mathbb{F}_q[X]$.

Recall the usual equivalence relation in $\mathrm{GL}(2,q)$, namely for $A, B \in \mathrm{GL}(2,q)$,

$$A \sim B :\iff \exists C \in \mathrm{GL}(2,q) \text{ such that } A = C^{-1}BC.$$

Further, define the following equivalence relations for $A, B \in \mathrm{GL}(2,q)$ and $F, G \in \mathbb{F}_q[X]$.

$$\begin{aligned} A \sim_q B &:\iff A = \lambda B, \text{ for some } \lambda \in \mathbb{F}_q^* \text{ and} \\ F \sim_q G &:\iff F = \lambda G, \text{ for some } \lambda \in \mathbb{F}_q^* \end{aligned}$$

Email address: `gnkapet@gmail.com` (Giorgos Kapetanakis)

It follows that, for $F \in \mathbb{F}_q[X]$ the equivalence class $[F] := \{G \in \mathbb{F}_q[X] \mid G \sim_q F\}$ 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. Further, the action defined in (1) also induces an action of $\mathrm{PGL}(2,q) = \mathrm{GL}(2,q)/\sim_q$ on $\mathbb{F}_q[X]/\sim_q$, see [24]. 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 [10, 22, 24]. In a similar manner, we introduce a natural notation abuse for $[A], [B] \in \mathrm{PGL}(2,q)$, i.e.

$$[A] \sim [B] :\Longleftrightarrow \exists\, [C] \in \mathrm{PGL}(2,q) \text{ such that } [A] = [C^{-1}BC].$$

We note that throughout this paper, we will denote polynomials with capital latin letters and their coefficients with their corresponding lowercase ones with appropriate indices. In particular, if $F \in \mathbb{F}_q[X]$ is of degree n, then $F(X) = \sum_{i=0}^{n} f_i X^i$, in other words, f_i will stand for the i-th coefficient of F. Two well-known results in the study of the distribution of polynomials over $\mathbb{F}_q$ are the following.

Theorem 1.1 (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 $a = 0$.*

Theorem 1.2 (Hansen-Mullen Primitivity Conjecture). *Let $a \in \mathbb{F}_q$, $n \geq 2$ and fix $0 \leq j < n$. There exists a primitive polynomial $P(X) = X^n + \sum_{k=0}^{n-1} p_k X^k \in \mathbb{F}_q[X]$ with $p_j = a$, unless one of the following holds.*

1. *$j = 0$ and $(-1)^n a$ is non-primitive.*
2. *$n = 2$, $j = 1$ and $a = 0$.*
3. *$(q, n, j, a) = (4, 3, 2, 0), (4, 3, 1, 0)$ or $(2, 4, 2, 1)$.*

Both results had been conjectured by Hansen and Mullen [16]. Theorem 1.1 was initially proved for $q > 19$ or $n \geq 36$ by Wan [26], while Han and Mullen [15] verified the remaining cases by computer search. Several extensions to these results have been obtained [9, 20], while most authors use a variation of Wan's approach [26]. Recently new methods have emerged [14, 21, 25]. The second result was partially settled by Fan and Han [7, 8] and Cohen [4], while the proof was completed by Cohen and Prešern [5, 6].

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 in [11, 12, 13].

Nonetheless, a description of the coefficient of the polynomials of $\mathbb{I}_n^A$ has not yet been investigated for arbitrary A. In Table 1, we present the results of a quick experiment regarding the distribution of the monic irreducible polynomials of degree 6 of $\mathbb{F}_3$ that remain invariant under 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 $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We see that the last two columns have the same number of entries, that in any case the coefficient of X^5 is always zero as well as some other coefficients, that in the first column, the coefficient of X^4 is always equal to 1 etc., while on the other hand some coefficients seem to take multiple values.

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

Table 1: Monic irreducible polynomials of $\mathbb{F}_3$ of degree 6 such that $F = A \circ F$.

In this work, we explain these observations. We confine ourselves to the case when $A \in \mathrm{GL}(2, q)$ is lower-triangular and wonder whether a monic irreducible polynomial over $\mathbb{F}_q$ of specified degree whose class remains invariant under this action can have a prescribed coefficient. In Section 2, we deal with the case when $A \in \mathrm{GL}(2, q)$ is a lower-triangular matrix that has one eigenvalue and in Section 3 we deal with the case that 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 adopt Wan's method [26] and prove sufficient conditions for the existence of polynomials of $\mathbb{I}_n^A$ that indeed have these coefficients.

These results give rise to Theorems 2.8 and 3.4, where it is roughly shown that the high-degree coefficients of an irreducible monic polynomial invariant under A either take specific values or can be arbitrarily prescribed, with a small finite number of possible exceptions.

We note that from now on, without any special mention, A will always denote a lower-triangular matrix, so the eigenvalues of A are the elements of its diagonal.

2. The case of a single eigenvalue

If A has a single eigenvalue, then

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

The first situation is settled by Theorem 1.1. 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*. The following characterizes those polynomials explicitly.

Lemma 2.1. *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 $F(X) = G(X^p - \alpha^{p-1}X)$.*

Proof. Let $A = \left(\begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix}\right)$. Since $\operatorname{ord}(A) = p$, it follows from [24, Theorem 4.5], that if the degree of an irreducible such polynomial is ≥ 3, then it is pn, for some n. A direct computation reveals that there are no periodic polynomials of degree 1 and the existence of such polynomials of degree 2 requires $p = 2$. It follows that the degree of an irreducible periodic polynomial is a multiple of p, hence the irreducible factors of F are either of degree pn for some n, or they come in p-tuples of irreducible factors of the same degree, thus all polynomials with this property (irreducible or not) have degree pn for some n.

The left direction of the statement is clear. For the right direction, let

$$F(X) = G(X)(X^p - \alpha^{p-1}X) + H(X)$$

where $\deg(H) < p$. Also,

$$F(X) = F(X+\alpha) = G(X+\alpha)(X^p - \alpha^{p-1}X) + H(X+\alpha).$$

The last two equations imply $H(X) \equiv H(X+\alpha) \pmod{(X^p - \alpha^{p-1}X)}$ and since $\deg(H) < p$, this means $H(X) = H(X+\alpha)$ which in turn yields $\deg(H) = 0$. Also, since $H(0) = F(0)$, we conclude that $H = f_0$, that is $(X^p - \alpha^{p-1}X) \mid (F - f_0)$.

Next, let pn be the degree of F. We show the desired result by induction on n. The case $n = 0$ is trivial. Now, assume that $G = H(X^p - \alpha^{p-1}X)$ for all $G \in \mathbb{F}_q[X]$ such that $G(X) = G(X+\alpha)$ and $\deg(G) = (k-1)p$. Let $n = k$. We have that $(X^p - \alpha^{p-1}X) \mid (F - f_0)$, hence $F = (X^p - \alpha^{p-1}X)G + f_0$, for some $G \in \mathbb{F}_q[X]$ with $\deg(G) = (k-1)p$. Also, we have that $G(X) = G(X+\alpha)$, so from the induction hypothesis $G = Z(X^p - \alpha^{p-1}X)$, for some $Z \in \mathbb{F}_q[X]$. The result follows. □

It is now clear that we need the following theorem of [1], also see [19, Theorem 3.3.3].

Theorem 2.2 (Agou). *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 $\operatorname{Tr}(p_{n-1}/\alpha^p) \neq 0$, 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 $Q(X) = P(X^p - \alpha^{p-1}X)$, where $P \in \mathbb{I}_n$ such that $\operatorname{Tr}(P_{n-1}/\alpha^p) \neq 0$. Moreover,

$$Q(X) = \sum_{i=0}^{n} p_i (X^p - \alpha^{p-1}X)^i = \sum_{i=0}^{n}\sum_{k=0}^{i} \binom{i}{k} (-\alpha)^{(p-1)(i-k)} p_i X^{pk+i-k}.$$

It follows that the m-th coefficient of Q, where $0 \leq m \leq pn$, is

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

where

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

In other words, it is a linear expression of some of the $\mu+1$ low-degree coefficients of the *reciprocal* of P, i.e. $P^R := X^{\deg(P)}P(1/X)$, where μ is the largest number such that $\gamma_\mu \neq 0$. First, we observe that it is possible for such μ to not exist (for example when $m = np-1$ and $p > 2$) and, secondly, we observe that if $\mu = 0$ or 1, then the value of q_m has to be a given combination of p_0 and p_1, but since neither of them is chosen arbitrarily, it can only take certain values. So, from now on we assume that μ exists and $\mu \geq 2$. This leads us define to the following map

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

where $\mathbb{G}_\mu := \{f \in \mathbb{F}_q[X] \mid \deg(f) \leq \mu,\ f_0 = 1\}$. Also, it is clear that if $P \in \mathbb{I}_n$, then $P^R \in \mathbb{J}_n$, where $\mathbb{J}_n := \{P \in \mathbb{F}_q[X] \mid P^R \in \mathbb{I}_n\}$. Furthermore, it is now evident that we will need to correlate the inverse image of σ with a set that is easier to handle. The following proposition, see [12, Proposition 2.5], serves that purpose.

Proposition 2.3. *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 2.4. *Let $\kappa \in \mathbb{F}_q$ 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 $P \in \mathbb{J}_n$ such that $\mathrm{Tr}(p_1/\alpha^{p-1}) \neq 0$ and $P \equiv HF^{-1} \pmod{X^{\mu+1}}$ 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 $q_m = \kappa$.*

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 $P \in \mathbb{J}_n$, $\mathrm{Tr}(p_1/\alpha^p) = 0 \iff \psi(P) \neq 1$. Additionally, 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 $\mathbb{F}_q[X]$. 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 in Proposition 2.3. Clearly, if $w \neq 0$ we have our desired result.

In order to proceed, we will have to introduce the concept of Dirichlet characters. Let M be a polynomial of $\mathbb{F}_q$ of degree ≥ 1. The characters of the group $(\mathbb{F}_q[X]/M\mathbb{F}_q[X])^*$, extended to zero with the rule $\chi(F) = 0 \iff \gcd(F, M) \neq 0$, are called *Dirichlet characters modulo M*. If χ is a Dirichlet character modulo M, we define

$$c_n(\chi) = \sum_{d|n} \frac{n}{d} \sum_{P \in \mathbb{I}_{n/d}} \chi(P)^d.$$

Weil's theorem of the Riemann hypothesis for function fields implies the following theorem, see [26] and the references therein.

Theorem 2.5 (Weil). *Let χ be a non-trivial Dirichlet character modulo M, then*

$$|c_n(\chi)| \leq (\deg(M) - 1) q^{\frac{n}{2}}.$$

For a detailed account of the above well-known facts, see [23, Chapter 4], while the following can be deduced, see [26, Corollary 2.8].

Proposition 2.6. *Let χ be a non-trivial Dirichlet character modulo M such that $\chi(\mathbb{F}_{q^*}) = 1$. Then*

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

Further, notice that ψ is a group homomorphism, hence a Dirichlet character modulo $X^{\mu+1}$, while it is clear that $\mathrm{ord}(\psi) = p$. We deduce the following bounds.

Corollary 2.7. *Let χ and ψ be Dirichlet characters modulo M, such that* $\mathrm{ord}(\psi) = p$ *and $\chi(\mathbb{F}_q^*) = 1$.*

1. *If $\chi \notin \langle \psi \rangle$, then*

$$\left| \sum_{P \in \mathbb{I}_n,\ \psi(P) \neq 1} \chi(P) \right| \leq \frac{2(p-1)}{pn} \cdot (\deg(M) q^{n/2} + 1),$$

2. *If $\chi \in \langle \psi \rangle \setminus \{\chi_0\}$, then*

$$\left| \sum_{P \in \mathbb{I}_n,\ \psi(P) \neq 1} \chi(P) \right| \leq \frac{\pi_q(n)}{p} + \frac{2p-3}{pn} \cdot (\deg(M) q^{n/2} + 1).$$

3. *If $\chi = \chi_0$, then*

$$\left| \sum_{P \in \mathbb{I}_n,\ \psi(P) \neq 1} \chi(P) \right| \geq \frac{(p-1)\pi_q(n)}{p} - \frac{p-1}{pn} \cdot (\deg(M) q^{n/2} + 1).$$

Proof. We utilize the orthogonality relations for the group $\langle\psi\rangle$ and conclude

$$\begin{aligned}\sum_{P\in\mathbb{I}_n,\ \psi(P)\neq 1}\chi(P) &= \frac{1}{p}\sum_{P\in\mathbb{I}_n}\chi(P)\left((p-1)-\sum_{j=1}^{p-1}\psi^j(P)\right)\\ &= \frac{p-1}{p}\sum_{P\in\mathbb{I}_n}\chi(P)-\frac{1}{p}\sum_{j=1}^{p-1}\sum_{P\in\mathbb{I}_n}\chi\psi^j(P).\end{aligned}$$

All three results follow directly from the above and Proposition 2.6. □

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

$$\begin{aligned}w &= \frac{1}{|V|}\sum_{H\in\mathbb{G}_{\mu-1}}\Lambda(H)\sum_{P\in\mathbb{J}_n,\ \psi(P)\neq 1}\sum_{\chi\in V}\chi(P)\bar{\chi}(HF^{-1})\\ &= \frac{1}{|V|}\sum_{\chi\in V}\chi(F)\sum_{H\in\mathbb{G}_{\mu-1}}\Lambda(H)\bar{\chi}(H)\sum_{P\in\mathbb{J}_n,\ \psi(P)\neq 1}\chi(P).\end{aligned}$$

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 $w = A_\psi + B_\psi + C_\psi$. For C_ψ, we have

$$|C_\psi| \leq \frac{1}{|V|}\sum_{\chi\in V\setminus\langle\phi\rangle}\left|\sum_{H\in\mathbb{G}_{\mu-1}}\Lambda(H)\bar{\chi}(H)\right|\left|\sum_{P\in\mathbb{J}_n,\ \psi(P)\neq 1}\chi(P)\right|.$$

Afterwards, we observe that any character sum that runs through $\mathbb{J}_n$ that involves a character that is trivial on $\mathbb{F}_q^*$ has the same absolute value as if it would run through $\mathbb{I}_n$. Also, for those characters we have that

$$\sum_{H\in\mathbb{G}_{\mu-1}}\Lambda(H)\chi(H) = \sum_{\deg(H)\leq\mu-1,\ H \text{ monic}}\Lambda(H)\chi(H) = \sum_{j=0}^{\mu-1}c_{\mu-1}(\chi).$$

Now, by taking into account the above, Theorem 2.5 and Corollary 2.7 yield

$$\begin{aligned}|C_\psi| &\leq \frac{|V|-p}{|V|}\left(\sum_{j=0}^{\mu-1}\mu q^{j/2}\right)\cdot\frac{2(p-1)}{p}\cdot\frac{\mu}{n}\cdot q^{n/2}\\ &\leq \frac{q^\mu-p}{q^\mu}\cdot\mu\cdot\frac{q^{\mu/2}-1}{q^{1/2}-1}\cdot\frac{2(p-1)}{p}\cdot\frac{\mu}{n}\cdot q^{n/2}\\ &\leq \frac{4\mu^2}{n}\cdot q^{(n+\mu-1)/2}.\end{aligned}$$

Similarly, for B_ψ we notice that $\psi \in V$, i.e. $\langle\psi\rangle \setminus \{\chi_0\} \subseteq V$, hence we get

$$\begin{aligned}|B_\psi| &\leq \frac{p-1}{q^\mu} \cdot \mu \cdot \frac{q^{\mu/2}-1}{q^{1/2}-1} \cdot \left(\frac{\pi_q(n)}{p} + \frac{2p-3}{p} \cdot \frac{\mu}{n} \cdot q^{n/2} \right) \\ &\leq \frac{2\mu}{q^{(\mu+1)/2}} \cdot \pi_q(n) + \frac{4\mu^2}{n} \cdot q^{(n-\mu-1)/2}.\end{aligned}$$

Finally, for A_ψ, we notice that

$$\sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) = \sum_{m=0}^{\mu-1} \sum_{\substack{\deg(H)=m \\ h_0=1}} \Lambda(H) = \sum_{m=0}^{\mu-1} q^m = \frac{q^\mu - 1}{q-1}, \tag{2}$$

thus

$$\begin{aligned}|A_\psi| &\geq \frac{1}{|V|} \cdot \frac{q^\mu - 1}{q-1} \left(\frac{(p-1)\pi_q(n)}{p} - \frac{p-1}{p} \cdot \frac{\mu}{n} \cdot q^{n/2} \right) \\ &\geq \frac{1}{2q} \left(\pi_q(n) - \frac{\mu}{n} \cdot q^{n/2} \right).\end{aligned}$$

Since $w = A_\psi + B_\psi + C_\psi$, it follows that $w \neq 0$ provided that $|A_\psi| > |B_\psi| + |C_\psi|$. This implies the following condition for $w > 0$:

$$\frac{q^{(\mu-1)/2} - 4\mu}{2q^{(\mu+1)/2}} \cdot \pi_q(n) \geq \frac{\mu}{n} \cdot \left(4\mu + \frac{1}{2q^{\mu/2}} + \frac{4\mu}{q^\mu} \right) \cdot q^{(n+\mu-1)/2}. \tag{3}$$

Further, it is well-known, see [18, Theorem 3.25], that

$$\pi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

where $\mu(\cdot)$ stands for the Möbius function. It follows that

$$\pi_q(n) \geq \frac{1}{n} \left(q^n - q \cdot \frac{q^{n/2}-1}{q-1} \right). \tag{4}$$

The combination of the above and Eq. (3) yields another sufficient condition, namely

$$\begin{aligned}&q^{n/2}(q^{(\mu-1)/2} - 4\mu) + \frac{4\mu}{q-1} \geq \\ &\qquad 2\mu q^\mu \left(4\mu + \frac{1}{2q^{\mu/2}} + \frac{4\mu}{q^\mu} + \frac{1}{2\mu q^{(\mu+1)/2}(q-1)} \right).\end{aligned} \tag{5}$$

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 $2 \leq \mu \leq n/2$. In particular, for $2 \leq q \leq 64$, Table 2 illustrates the values of n such that the Eq. (5) holds for all $2 \leq \mu \leq n/2$. All in all, in this section we have proved the following theorem.

$q=2,\ n\geq 26$	$q=3,\ n\geq 16$
$q=4,\ n\geq 12$	$q=5,\ n\geq 10$
$7\leq q\leq 11,\ n\geq 8$	$13\leq q\leq 27,\ n\geq 6$

Table 2: Pairs (q,n) such that Eq. (5) holds for all $2\leq \mu\leq n/2$.

Theorem 2.8. *Let q be a power of the prime p, $[A]=[\left(\begin{smallmatrix}1&0\\ \alpha&1\end{smallmatrix}\right)]\in \mathrm{PGL}(2,q)$ and $n'\in\mathbb{Z}_{>0}$. If $\alpha=0$, then $\mathbb{I}_{n'}^A=\mathbb{I}_{n'}$. If $\alpha\neq 0$, then $\mathbb{I}_{n'}^A=\emptyset \iff p\nmid n'$. Suppose $p\mid n'$ and write $n'=pn$. Further, fix some $0\leq m\leq pn$ and for all $\max(0,n-m)\leq i\leq n-\lceil m/p\rceil$ 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, $\mu\leq n-\lceil m/p\rceil$.

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 $n\geq 26$.*

3. The case of two distinct 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 $\alpha\in\mathbb{F}_q^*$. It is clear that $F\in\mathbb{F}_q[X]$ satisfies $B\circ F\sim_q F \iff F(X)\sim_q F(\alpha X)$. Our first step is to study the polynomials that remain invariant under B.

Lemma 3.1. *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 $F(X)=X^kG(X^r)$.*

Proof. The result is trivial if F is a monomial. Let $F(X)=X^k\sum_{i=0}^{n'}f_iX^i$ such that $f_0,f_{n'}\neq 0$, $n'\geq 1$ and $F(X)\sim_q F(\alpha X)$. It suffices to show that $f_i=0$ for all $i\nmid r$. We have that

$$F(\alpha X)=\alpha^kX^k\sum_{i=0}^{n'}\alpha^if_iX^i.$$

By comparing the coefficients of X^k and $X^{k+n'}$, we deduce that $r\mid n'$ which yields $F(\alpha X)=\alpha^kF(X)$, i.e. for all i we have $\alpha^kf_i=\alpha^{k+i}f_i$ which implies the desired result. The opposite direction of the statement is straightforward. □

From the above, it is clear that the elements of $\mathbb{I}^B_{n'}$, should be of the form $P(X^r)$ for some monic irreducible $P \in \mathbb{F}_q[X]$. The result below, see [3, Theorem 2], characterizes the irreducibility of such compositions in our special case.

Theorem 3.2 (Cohen). *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 $(-1)^n p_0$.*

Here we note that the above is a special case that suits our case better. For the general case (i.e. for arbitrary r), see [17, Theorem 3.2.5] or [2, Theorem 3.9]. In our case, since r stands for the order of $\alpha \in \mathbb{F}_q^*$, it is clear that $\gcd(r,q) = 1$, $r \mid (q-1)$ and $4 \nmid \gcd(r, q^n+1)$, hence the irreducibility of $P(X^r)$ depends solely on the choice of p_0. In particular, see [3, Lemma 4], there exist exactly $\phi(r)(q-1)/r$ elements of $\mathbb{F}_q$, whose order e satisfies $\gcd(r,(q-1)/e) = 1$, that is we have $\phi(r)(q-1)/r$ choices for p_0. We denote this set by $\mathfrak{C}$, while it is clear that 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 $\mathbb{I}^B_{n'}$. Namely, n' has to be a multiple of r, the order of α, $p_i = 0$ for all $r \nmid i$, while Theorem 1.2 implies that all p_i with $i \neq 0$ and $r \mid i$ can be arbitrarily prescribed, while p_0 can take any value in $\mathfrak{C}$.

Our next step is to move to the case of arbitrary A. The lemma below is derived from [10, Lemma 1] and provides a correlation between $\mathbb{I}^C_{n'}$ and $\mathbb{I}^D_{n'}$, if $[C] \sim [D]$.

Lemma 3.3. *Suppose that $[C], [D] \in \mathrm{PGL}(2,q)$ such that $[C] \sim [D]$, then map*

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

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

Proof. First, it follows from [24, Lemma 2.2] that ϕ maps classes of irreducible polynomials of degree n' to classes irreducible of polynomials of degree n'. Further, if $[F] \in (\mathbb{I}^D_{n'}/\sim_q)$, we have that $\phi([F]) = [U \circ F] = [U \circ (C \circ F)] = [UC \circ F] = [DU \circ F] = [D \circ \phi([F])]$, i.e. $\phi([F]) \in (\mathbb{I}^D_{n'}/\sim_q)$, thus ϕ is well-defined.

It is clear that ϕ is one-to-one, which also implies that $|\mathbb{I}^C_{n'}/\sim_q| \leq |\mathbb{I}^D_{n'}/\sim_q|$. By symmetry, we also get that $|\mathbb{I}^D_{n'}/\sim_q| \leq |\mathbb{I}^C_{n'}/\sim_q|$, hence $|\mathbb{I}^C_{n'}/\sim_q| = |\mathbb{I}^D_{n'}/\sim_q|$ and the result follows. ∎

Before proceeding, we observe that the above combined with what we already know about $\mathbb{I}^B_{n'}$ imply that $\mathbb{I}^A_{n'} \neq \emptyset \iff r \mid n'$, 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 $Q \in \mathbb{I}^A_{n'}$, as a linear expression of the coefficients of some $P' \in \mathbb{I}^B_{n'}$. 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

$$Q(X) \sim_q d^{n'} \left(\sum_{i'=0}^{n'} p'_i \left(\frac{aX+c}{d} \right)^{i'} \right) = \sum_{i'=0}^{n'} \sum_{k=0}^{i'} p'_i \binom{i}{k} a^k c^{i'-k} d^{n'-i'} X^k,$$

Further, note that $p'_{i'} = 0$ for all $r \nmid i'$, so for $r \mid i'$ we write $i = i'/r$ and the m-th coefficient of Q is

$$q_m = \frac{1}{a^{n'}} \sum_{i=\lceil m/r \rceil}^{n} \binom{ir}{m} a^m c^{ir-m} d^{nr-ir} p'_{ir} = \sum_{i=0}^{n-\lceil m/r \rceil} \delta_i p_{n-i}, \tag{6}$$

where

$$\delta_i := \binom{(n-i)r}{m} a^m c^{(n-i)r-m} d^{ir}.$$

In other words, it is a linear expression of the $n - \lceil m/r \rceil$ 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 Eq. (6) 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

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

where $F_{\mathfrak{c}}$ is the polynomial described in Proposition 2.3 for $\kappa/\mathfrak{c}$. 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 in Section 2, we get

$$\begin{aligned} w &= \frac{1}{|V|} \sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) \sum_{P \in \mathbb{I}_n} \sum_{\chi \in V} \chi(P) \bar{\chi}(\mathfrak{c} H F_{\mathfrak{c}}^{-1}) \\ &= \frac{1}{|V|} \sum_{\chi \in V} \chi(\mathfrak{c} F_{\mathfrak{c}}^{-1}) \sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) \bar{\chi}(H) \sum_{P \in \mathbb{I}_n} \chi(P). \end{aligned}$$

By separating the term that corresponds to the trivial character, from Eq. (2), we get

$$\left| w - \frac{(q^\mu - 1)\pi_q(n)}{|V|(q-1)} \right| \leq \frac{1}{|V|} \sum_{\chi \in V \setminus \{\chi_0\}} \left| \sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) \bar{\chi}(H) \right| \left| \sum_{P \in \mathbb{I}_n} \chi(P) \right|.$$

As in Section 2, we observe that $\left| \sum_{H \in \mathbb{G}_{\mu-1}} \Lambda(H) \bar{\chi}(H) \right| \leq \frac{q^{\mu/2}-1}{q^{1/2}-1}$ and take into account Proposition 2.6. It follows that a sufficient condition for $w \neq 0$ is

$$\pi_q(n) \geq 2(\mu+1) q^{(\mu+n+1)/2}. \tag{7}$$

By taking the monic reciprocal of this, i.e. $Q(X) = P^R/\mathfrak{c}$, we that $Q \in \mathbb{I}_n$ and $\sum_{i=0}^{\mu} \gamma_i q_{n-i} = \kappa$, while $Q(X^r)$ is also irreducible. By combining Eqs. (4) and (7), we get another sufficient condition for $w \neq 0$, namely

$$q^{n/2} \geq 2n(\mu+1) q^{(\mu+1)/2} + \frac{q}{q+1}. \tag{8}$$

$q=2,\ n\geq 47$	$q=3,\ n\geq 25$
$q=4,\ n\geq 19$	$q=5,\ n\geq 15$
$q=7,\ n\geq 13$	$q=8,9,\ n\geq 11$
$q=11,13,\ n\geq 9$	$16\leq q\leq 29,\ n\geq 7$

Table 3: Pairs (q,n) such that Eq. (8) holds for all $1\leq\mu\leq n/2$.

The latter 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. Table 3 illustrates the results for the intermediate values of q. All in all, we have proved the following.

Theorem 3.4. *Let q be a prime power, $[A]\in\mathrm{PGL}(2,q)$ be such that $[A]\sim[\left(\begin{smallmatrix}\alpha&0\\0&1\end{smallmatrix}\right)]$ 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 we may assume that $n'=rn$. Further, set $\mathfrak{C}:=\{x\in\mathbb{F}_q\mid\gcd(r,(q-1)/\operatorname{ord}(x))=1\}$.*

If $[A]=[\left(\begin{smallmatrix}\alpha&0\\0&1\end{smallmatrix}\right)]$, 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 $[A]\neq[\left(\begin{smallmatrix}\alpha&0\\0&1\end{smallmatrix}\right)]$, 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 $n\geq 47$.*

Acknowledgements

I would like to thank Profs. Henning Stichtenoth and Alev Topuzoğlu, not only for pointing out this problem to me, but also for the fruitful conversations and their suggestions we had while discussing it. Also, I would like to thank the anonymous referee for her/his comments and corrections. This work was supported by TÜBİTAK Project Number 114F432.

References

[1] S. Agou. Factorisation sur un corps fini F_{p^n} des polynômes composés $f(X^{p^r}-aX)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}(X)$. *J. Number Theory*, 9(2):229–239, 1977.

[2] I. Blake, X. Gao, R. Mullin, S. Vanstone, and T. Vanghoobian. *Applications of Finite Fields*. Springer Science+Business Media, New York, 1993.

[3] S. D. Cohen. On irreducible polynomials of certain types in finite fields. *Proc. Cambridge Philos. Soc.*, 66:335–344, 1969.

[4] S. D. Cohen. Primitive polynomials with a prescribed coefficient. *Finite Fields Appl.*, 12(3):425–491, 2006.

[5] S. D. Cohen and M. Prešern. Primitive polynomials with prescribed second coefficient. *Glasgow Math. J.*, 48:281–307, 2006.

[6] S. D. Cohen and M. Prešern. The Hansen-Mullen primitivity conjecture: completion of proof. In *Number Theory and Polynomials*, volume 352 of *LMS Lecture notes*, pages 89–120. Cambridge University Press, Cambridge, 2008.

[7] S. Fan and W. Han. p-adic formal series and primitive polynomials over finite fields. *Proc. Amer. Math. Soc.*, 132(1):15–31, 2003.

[8] S. Fan and W. Han. Primitive polynomials over finite fields of characteristic two. *Appl. Algebra Engrg. Comm. Comput.*, 14(5):381–395, 2004.

[9] T. Garefalakis. Irreducible polynomials with consecutive zero coefficients. *Finite Fields Appl.*, 14(1):201–208, 2008.

[10] T. Garefalakis. On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible poynomials over $\mathbb{F}_q$. *J. Pure Appl. Algebra*, 215(8):1835–1843, 2010.

[11] T. Garefalakis. Self-reciprocal irreducible polynomials with prescribed coefficients. *Finite Fields Appl.*, 17(2):183–193, 2011.

[12] T. Garefalakis and G. Kapetanakis. On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 18(4):832–841, 2012.

[13] T. Garefalakis and G. Kapetanakis. A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 35(C):61–63, 2015.

[14] J. Ha. Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 40:10–25, 2016.

[15] K. H. Ham and G. L. Mullen. Distribution of irreducible polynomials of small degrees over finite fields. *Math. Comp.*, 67(221):337–341, 1998.

[16] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59(200):639–643, 1992.

[17] M. Kyuregyan. Construction of irreducibles. In G. L. Mullen and D. Panario, editors, *Handbook of Finite Fields*, pages 60–66. CRC Press, Boca Raton, 2013.

[18] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, Cambridge, second edition, 1997.

[19] D. Panario. Conditions for reducible polynomials. In G. L. Mullen and D. Panario, editors, *Handbook of Finite Fields*, pages 66–70. CRC Press, Boca Raton, 2013.

[20] D. Panario and G. Tzanakis. A generalization of the Hansen-Mullen conjecture on irreducible polynomials over finite fields. *Finite Fields Appl.*, 18:303–315, 2012.

[21] P. Pollack. Irreducible polynomials with several prescribed coefficients. *Finite Fields Appl.*, 22:70–78, 2013.

[22] L. Reis. The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$. Submitted for publication.

[23] M. Rosen. *Number Theory in Function Fields*, volume 210 of *Grad. Texts in Math.* Springer-Verlag, New York, 2002.

[24] H. Stichtenoth and A. Topuzoğlu. Factorization of a class of polynomials over finite fields. *Finite Fields Appl.*, 18(1):108–122, 2012.

[25] A. Tuxanidy and Q. Wang. A new proof of the Hansen-Mullen irreducibility conjecture. `arXiv:1604.04023 [math.NT]`.

[26] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.