Irreducible polynomials with consecutive zero coefficients

Theodoulos Garefalakis

Department of Mathematics, University of Crete, 71409 Heraklion, Greece

Abstract

Let q be a prime power. We consider the problem of the existence of monic irreducible polynomials over $\mathbb{F}_q$ with consecutive coefficients fixed to zero. We show that asymptotically, there exist monic irreducible polynomials of degree n over $\mathbb{F}_q$ with roughly $n/3$ consecutive coefficients fixed to zero.

Key words: Irreducible polynomials, finite fields

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, of characteristic p. We denote by $A = \mathbb{F}_q[T]$ the ring of polynomials over $\mathbb{F}_q$. It is well-known that asymptotically, the number of irreducible polynomials in A of degree n is approximately q^n/n. However, much less is known about the number, or even the existence of irreducibles of certain form, for instance with some coefficients fixed to given values.

Given an integer $n > 1$, it has been proved independently by S.D. Cohen [2] and R. Ree [13], that for all large enough q, there always is an irreducible polynomial over $\mathbb{F}_q$ of the form $T^n + T + a$. However, much less is known when q is fixed and n large. In [10], T. Hansen and G.L. Mullen conjecture that given integers $n > m \geq 0$ there exists a monic irreducible polynomial over $\mathbb{F}_q$ of degree n with the coefficient of T^m fixed to any given element $a \in \mathbb{F}_q$. Of course, $a \neq 0$ if $m = 0$. By considering primitive polynomials with given trace, S.D. Cohen [4] proves that the conjecture is true for $m = n - 1$. In [15], D. Wan settles

Email address: theo@math.uoc.gr (Theodoulos Garefalakis).

the conjecture subject to the condition that either $q > 19$ or $n \geq 36$, leaving a finite number of cases to be checked. By machine assisted computations, K.H. Ham and G.L. Mullen have verified the conjecture for these remaining cases in [9]. Prior to this work, E.N. Kuz'min [12] determined the number of monic irreducibles of degree 4 with the coefficients of T^3, T^2, T fixed to given values. Special attention is given to the case where the coefficients of T^3 and T^2 are zero. Similar results on the number of polynomials of given degree n of given factorization pattern which satisfy an additional property, such as that certain coefficients are prescribed, have been obtained by S.D. Cohen in [3]. The analogous problem for primitive polynomials has also attracted considerable attention. The analogue of Wan's result has been proved to be true by S.D. Cohen [5]. A survey on the subject by S. Gao, J. Howell and D. Panario, including experimental results as well as some applications can be found in [8].

It is natural to ask, and in fact to expect, that much more than the above is true. Namely, one would expect that irreducible polynomials exist with many coefficients fixed to given values. The objective of this work is to show that monic irreducible polynomials of degree n over $\mathbb{F}_q$ exist with up to $\lfloor cn \rfloor$ consecutive coefficients fixed to zero, where $0 < c < 1$ and the condition $(1 - 3c)n \geq 2 + 8 \log_q n$ is satisfied. Such irreducibles are called sparse and have many practical applications, see [6,7]. The proof of the main theorem is based on an estimate of a weighted sum, which is very similar to the one that D. Wan considers. The main tool is Weil's bound for character sums.

We record the following elementary lemma, which will be useful later. Let $f(T) = \sum_{i=0}^{n} a_i T^i \in \mathbb{F}_q[T]$ and denote by $f^*(T) = \sum_{i=0}^{n} a_{n-i} T^i$ its reciprocal.

Lemma 1 *Let $f(T) = \sum_{i=0}^{n} a_i T^i \in \mathbb{F}_q[T]$ with $a_n a_0 \neq 0$. The polynomial f is irreducible over $\mathbb{F}_q$ if and only if f^* is irreducible over $\mathbb{F}_q$.*

2 Character sums

It is well known that Dirichlet's theorem for primes in arithmetic progression has an analogue in A. Let $f, h \in A$ relatively prime. We reserve the letter P to denote a monic irreducible polynomial in A. Let

$$S_n(h, f) = \{P \in A \mid P \equiv h \pmod{f},\ \deg(P) = n\}.$$

We denote by $\pi_n(h, f)$ the cardinality of $S_n(h, f)$. The following asymptotic version of Dirichlet's theorem is well-known, see for instance [14].

Theorem 1 $$\pi_n(h,f) = \frac{1}{\Phi(f)}\frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Here $\Phi(f)$ is the order of the group $(A/fA)^*$, and the degree of f is assumed to be constant (not depending on n).

Let $f = T^m \in A$ and $h \in A$ with $\deg(h) \leq m-1$. Then $S_n(h,f)$ contains all irreducibles with the lower m coefficients fixed to those of h. For m fixed, Theorem 1 gives an estimate of the number of irreducibles with the lower m coefficients fixed to any values. Lemma 1 then implies that the same estimate holds if the upper m coefficients are fixed.

It is well-known that the truth of the Riemann hypothesis for function fields leads to effective versions of Theorem 1, see for instance [15]. The basic tools are bounds for character sums, sometimes referred to as Weil character sums. We recall here the main notions and results for future reference.

Let χ be a character of the group $(A/fA)^*$, that is, a homomorphism from $(A/fA)^*$ to $\mathbb{C}^*$. The character χ extended to A by zero is called a Dirichlet character mod f. The trivial character, that maps all polynomials prime to f to 1 is denoted by χ_o. Define the sum

$$c_n(\chi) = \sum_{d|n} \sum_{\deg(P)=d} d\chi(P^{n/d}),$$

where the inner sum is over all monic irreducible polynomials of degree d. It will be convenient to express, as in [15], $c_n(\chi)$ in terms of the von Mangolt function Λ, which is defined on A as follows: $\Lambda(h) = \deg(P)$ if $h = P^e$ for some irreducible P and an integer e, and is zero otherwise. It's rather easy to see that

$$c_n(\chi) = \sum_{\deg(h)=n} \Lambda(h)\chi(h),$$

where the sum is over all monic polynomials of degree n. Further, we define

$$c_n'(\chi) = \sum_{\deg(P)=n} \chi(P),$$

where the sum is over monic irreducibles of degree n. We denote by π_n the number of irreducible polynomials of degree n in A. It is well-know that $\sum_{d|n} d\pi_d = q^n$. The Moebius inversion formula then implies that

$$n\pi_n = \sum_{d|n} \mu(d) q^{n/d} = q^n + \sum_{d|n, d>1} \mu(d) q^{n/d}.$$

Since

$$|\sum_{d|n,d>1} \mu(d)q^{n/d}| \leq \sum_{0\leq d\leq n/2} q^d \leq 2q^{n/2},$$

it follows that

$$\left|\pi_n - \frac{q^n}{n}\right| \leq \frac{2}{n}q^{n/2}.$$

The following theorem follows from the Riemann hypothesis for function fields, see [15].

Proposition 1 *If $\chi \neq \chi_o$ then*

(1) $|c_n(\chi)| \leq (\deg(f) - 1)q^{n/2}$,
(2) $|c_n'(\chi)| \leq \frac{1}{n}(\deg(f) + 1)q^{n/2}$.

Also, $c_n(\chi_o) = q^n$ and $c_n'(\chi_o) = \pi_n$.

Using Proposition 1 it is not hard to show the following effective version of Dirichlet's theorem for A.

Theorem 2 (Theorem 5.1 of [15]) *Let $f, h \in A$, with $(f, h) = 1$. Then*

$$\left|\pi_n(h, f) - \frac{q^n}{n\Phi(f)}\right| \leq \frac{m+1}{n}q^{n/2}.$$

Theorem 2, applied with $f = T^m$, immediately implies that there always exists a monic irreducible polynomial of degree n with the coefficients of roughly $n/2 - \log_q n$ lower coefficients fixed (provided that the constant term is not zero). Lemma 1 then ensures the existence of a monic irreducible of degree n with roughly $n/2 - \log_q n$ higher coefficients fixed. More precisely we have the following corollary.

Corollary 1 *Let $n > m \geq 1$ be integers satisfying $q^{n/2} \geq (m+1)q^m$. For any $\beta_0, \beta_1, \ldots, \beta_{m-1} \in \mathbb{F}_q$ with $\beta_0 \neq 0$, there exists a monic irreducible polynomial $P = T^n + \sum_{i=0}^{n-1} a_i T^i$ in A of degree n, with $a_i = \beta_i$, $0 \leq i \leq m-1$. Also, there exists a monic irreducible polynomial with $a_{n-i} = \beta_i$, $1 \leq i \leq m-1$.*

Irreducibles of degree n with roughly $n/2$ leading or trailing coefficients prescribed can by found effectively: heuristic arguments and experimental results suggest that one may prescribe up to $n - 2\log_q n$ leading or trailing coefficients, and an irreducible still exists. This set polynomials is of reasonable size – polynomial in $n, \log q$ – and can therefore be searched exhaustively. This method of course depends on unproven assumptions. To the author's knowledge, there is no method that provably constructs the irreducibles of Corollary 1.

We note that Theorem 2 and Corollary 1 are classical. Generalizations have been obtained by M. Car [1] and C-N. Hsu [11]. It follows from these generalizations that irreducible polynomials of degree n exist with the leading n_1 and trailing n_2 coefficients are fixed to given values, subject to the condition $n_1 + n_2$ is less than roughly $n/2$. Unfortunately, the above results do not give us any information about irreducibles with some of the middle coefficients fixed.

3 Irreducible polynomials with consecutive zero coefficients

Let $n \geq m > l > 1$ be integers, and denote by H_{l-1} the set of monic primary polynomials of A of degree $l-1$. We recall that a polynomial in A is called primary if it is a power of an irreducible polynomial of A. We define

$$w(n,m,l) = \sum_{h \in H_{l-1}} \Lambda(h) \sum_{P \equiv h \pmod{T^m}} 1, \tag{1}$$

where the inner sum is over monic irreducibles of degree n with stated property. Proving that $w(n,m,l) > 0$ implies that there is a monic irreducible polynomial $P = T^n + \sum_{i=0}^{n-1} a_i T^i$ of degree n with the coefficients $a_i = 0$ for $l \leq i \leq m-1$.

Theorem 3 *With the above notation,*

$$\left| w(n,m,l) - \frac{q^{l-m}\pi_n}{q-1} \right| < \frac{m^2-1}{n} q^{(n+l-1)/2}.$$

PROOF. First we rewrite the sum defining $w(n,m,l)$ as

$$w(n,m,l) = \frac{1}{\Phi(T^m)} \sum_{\chi} \sum_{h \in H_{l-1}} \Lambda(h) \sum_{\deg(P)=n} \chi(P)\bar{\chi}(h),$$

where the first sum is over the Dirichlet characters mod T^m and the third sum is over monic irreducibles of degree n. Separating the term corresponding to χ_o and rearranging we have

$$w(n,m,l) - \frac{q^{l-1}\pi_n}{\Phi(T^m)} = \frac{1}{\Phi(T^m)} \sum_{\chi \neq \chi_o} \sum_{\deg(P)=n} \chi(P) \sum_{h \in H_{l-1}} \Lambda(h)\bar{\chi}(h).$$

Therefore,

$$\begin{aligned}
\left|w(n,m,l)-\frac{q^{l-1}\pi_n}{\Phi(T^m)}\right| &\leq \frac{1}{\Phi(T^m)}\sum_{\chi\neq\chi_o}\left|\sum_{\deg(P)=n}\chi(P)\right|\left|\sum_{h\in H_{l-1}}\Lambda(h)\bar{\chi}(h)\right| \\
&= \frac{1}{\Phi(T^m)}\sum_{\chi\neq\chi_o}|c'_n(\chi)||c_{l-1}(\bar{\chi})| \\
&< \frac{m+1}{n}q^{n/2}(m-1)q^{(l-1)/2} \\
&= \frac{m^2-1}{n}q^{(n+l-1)/2},
\end{aligned}$$

where we used the estimates of Proposition 1, and the fact that there are $\Phi(T^m)$ distinct characters of $(A/T^mA)^*$. □

Corollary 2 *Let $n > m > l > 1$ such that $q^{n+l-2m} \geq qm^4$. Then there exists a monic irreducible polynomial $P = T^n + \sum_{i=0}^{n-1} a_iT^i \in A$ of degree n such that $a_{m-1} = \cdots = a_l = 0$.*

PROOF. From Theorem 3 it follows that

$$w(n,m,l) > \frac{q^{l-m}\pi_n}{(q-1)} - \frac{m^2-1}{n}q^{(n+l-1)/2}.$$

Since $\pi_n \geq \frac{q^n}{n} - \frac{2q^{n/2}}{n}$, we have

$$w(n,m,l) > \frac{q^{n+l-m}}{n(q-1)} - \frac{2q^{n/2+l-m}}{n(q-1)} - \frac{(m^2-1)q^{(n+l-1)/2}}{n}. \tag{2}$$

It suffices to prove that under the condition of the corollary, the right-hand-side is non-negative. Indeed, the right-hand-side is at least

$$\begin{aligned}
&\frac{1}{n}\left(q^{n+l-m-1} - m^2q^{(n+l-1)/2} + \left(q^{(n+l-1)/2} - \frac{2q^{n/2+l-m}}{q-1}\right)\right) \\
\geq &\frac{q^{(n+l-2)/2}}{n}\left(q^{(n+l)/2-m} - \sqrt{q}m^2\right) \\
\geq &0
\end{aligned}$$

where the first inequality holds since $q^{(n+l-1)/2} \geq \frac{2q^{n/2+l-m}}{q-1}$ for $1 < l < m$. □

Corollary 2 can be used to show that there exist irreducible polynomials with a large number of consecutive coefficients fixed to zero.

Corollary 3 *Let $0 < c < 1$ and n a natural number such that $(1-3c)n \geq 2 + 8\log_q n$. Then, there exists a monic irreducible polynomial of degree n over $\mathbb{F}_q$ with any $\lfloor cn \rfloor$ consecutive coefficients, other than the first and the last, fixed to zero.*

PROOF. We apply Corollary 2 to fix

$$m - l = \lfloor cn \rfloor \tag{3}$$

coefficients. First, we observe that it suffices to consider the case

$$m + l \leq n. \tag{4}$$

The case $m + l > n$ follows from this by an application of Lemma 1. We also record that the conditions in Eq. (3) and Eq. (4) imply that

$$2m \leq n + \lfloor cn \rfloor. \tag{5}$$

The corollary will follow if

$$\begin{aligned} q^{n-\lfloor cn \rfloor - m} &\geq qm^4 \quad \iff \\ n - \lfloor cn \rfloor - 1 - 4\log_q m &\geq m. \end{aligned}$$

Given Eq. (5), the last condition is satisfied if

$$\begin{aligned} 2n - 2\lfloor cn \rfloor - 2 - 8\log_q n &\geq n + \lfloor cn \rfloor \quad \iff \\ n - 3\lfloor cn \rfloor &\geq 2 + 8\log_q n. \end{aligned}$$

The last inequality is clearly satisfied, under the assumption of the corollary. □

The corollary shows that for any $\epsilon > 0$ there exist monic irreducible polynomials of degree n with up to $\lfloor (1/3 - \epsilon)n \rfloor$ coefficients fixed to zero, provided that n is large enough. As an example, we show the following corollary.

Corollary 4 *Let q be a prime power, and n a positive integer. Then there exists a monic irreducible polynomial of degree n over $\mathbb{F}_q$ with any $\lfloor n/4 \rfloor$ coefficients fixed to zero for prime powers $2 \leq q \leq 59$ and the ranges for n shown in the table below, and for $q \geq 60$ and $n \geq 37$.*

q	n	q	n	q	n
2	≥ 266	13	≥ 59	32	≥ 43
3	≥ 155	16	≥ 55	37	≥ 41
4	≥ 119	17	≥ 53	41	≥ 40
5	≥ 100	19	≥ 51	43	≥ 40
7	≥ 81	23	≥ 48	47	≥ 39
8	≥ 75	25	≥ 47	49	≥ 38
9	≥ 70	27	≥ 45	53	≥ 38
11	≥ 64	31	≥ 44	59	≥ 37

PROOF. This is a consequence of Corollary 3 for $c = 1/4$. We have to show that

$$n/4 \geq 2 + 8 \log_q n \tag{6}$$

for the parameters in the table. The function $y_q(t) = t - 8 - 32 \log_q t$ is increasing for $t \geq 32/\log q$. For various values of q, we compute the single zero of $y_q(t)$ numerically, and conclude that for t greater of equal to the zero $y_q(t) \geq 0$. The ranges of t for each value of q are shown in the table above. Since $y_{q'}(t) \geq y_q(t)$ for $q' \geq q$, we conclude that Eq. (6) holds for any $q \geq 60$ and $n \geq 38$. □

4 Concluding Remarks

We have proved that there exist monic irreducible polynomials of degree n over $\mathbb{F}_q$ with roughly $n/3$ coefficients fixed to zero. This is only a partial extension of the result of D. Wan [15], which shows that (under the mild technical condition that either $q > 19$ or $n \geq 36$) there exist monic irreducible of degree n with any one coefficient can be fixed to *any* value. It would be interesting to extend the present result, and show that for n large enough, there exist monic irreducibles of degree n with roughly $n/3$ coefficients fixed to *any* values.

Acknowledgements

I would like to thank the anonymous reviewers for providing helpful comments and for pointing out related work.

References

[1] M. Car. Distribution des polynomes irreductibles dans $\mathbb{F}[t]$. *Acta Arith.*, 88:141–153, 1999.

[2] S.D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255 – 271, 1970.

[3] S.D. Cohen. Uniform distribution of polynomials over finite fields. *J. London Math. Soc.*, 2(6):93–102, 1972.

[4] S.D. Cohen. Primitive elements and polynomials with arbitrary trace. *J. American Math. Soc.*, 83:1 – 7, 1990.

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

[6] D. Coppersmith. Fast evaluation of logarithms in fields of characteristic two. *IEEE Trans. Inform. Theory*, IT-30:587–594, 1984.

[7] S. Gao. Elements of provable high orders in finite fields. *Proc. American Math. Soc.*, 127:1615 – 1623, 1999.

[8] S. Gao, J. Howell, and D. Panario. Irreducible polynomials of given forms. *Contemporary Mathematics*, 225:43–53, 1999.

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

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

[11] C-N. Hsu. The distribution of irreducible polynomials in $\mathbb{F}_q[t]$. *J. Number Theory*, 61(1):85–96, 1996.

[12] E.N. Kuz'min. Irreducible polynomials over finite fields i. *Algebra and Logic*, 33(4):216–232, 1994.

[13] R. Ree. Proof of a conjecture of S. Chowla. *J. Number Theory*, 3(2):210–212, 1971.

[14] M. Rosen. *Number theory in function fields.* Springer Verlag, 2002.

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