Finite Fields and Their Applications 78 (2022) 101979

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the density of irreducible polynomials which generate k-free polynomials over function fields

Seoyoung Kim *,[1], M. Ram Murty [2]

Department of Mathematics and Statistics, Queen's University, Kingston, ON, K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 15 January 2020
Received in revised form 20 October 2021
Accepted 20 November 2021
Available online 1 December 2021
Communicated by Sergey Rybakov

MSC:
11T55
11T06
11A51

Keywords:
k-free polynomials
Finite fields
Congruence

ABSTRACT

Let $M \in \mathbb{F}_q[t]$ be a polynomial, and let $k \geq 2$ be an integer. In this note, we will compute the asymptotic density of irreducible monic polynomials $P \in \mathbb{F}_q[t]$ for which $P + M$ is not divisible by the kth power of any irreducible polynomial.

1. Introduction

In 1949, Mirsky [6] proved that every sufficiently large number can be written as a sum of a prime and a k-free number for any given $k \geq 2$. In fact, he derived an asymptotic

* Corresponding author.
E-mail addresses: sk206@queensu.ca (S. Kim), murty@mast.queensu.ca (M.R. Murty).
1 Research of the first author partially supported by a Coleman Postdoctoral Fellowship.
2 Research of the second author partially supported by NSERC Discovery grant.

https://doi.org/10.1016/j.ffa.2021.101979
1071-5797/

formula for the number of such representations. In 2001, Yao [9] attempted to show that an analogous result holds in the case of function fields over finite fields. Apparently, according to Math Reviews (MR1841909), there seem to be errors in the paper. This was highlighted as an open problem in Moree's survey [7]. The purpose of this paper is to correct the error in [9] and establish the analogue in the function field case.

Let $\mathbb{F}_q$ be a finite field of order q, and let $M \in \mathbb{F}_q[t]$ be a fixed polynomial. For $k \geq 2$, a polynomial is *k-free* if it is not divisible by the kth power of any irreducible polynomial. In this note, we want to compute the asymptotic density of irreducible polynomials P for which $P + M$ is k-free. For the most part, we adhere to the notation and arrangement of [9]. More precisely, we will prove the following:

Theorem 1. *Let $M \in \mathbb{F}_q[t]$ be a fixed polynomial, and let $k \geq 2$ be an integer. Denote by $\mathscr{P}_+$ the set of all monic irreducible polynomials. We define the set*

$$U_k(M, d) = \{P \in \mathscr{P}_+ |\deg P = d,\ \ P + M \ \textit{ is } k\textit{-free}\}.$$

Then we have

$$\lim_{d\to\infty} \frac{\#U_k(M, d)}{\#\{P \in \mathscr{P}_+ |\deg P = d\}} = \prod_{\substack{P\nmid M \\ P\in\mathscr{P}_+}} \left(1 - \frac{1}{|P|^k - |P|^{k-1}}\right), \quad \textit{where } |P| = q^{\deg P}. \tag{1.1}$$

Theorem 1 can be directly obtained from the following result and the prime number theorem for $\mathbb{F}_q[t]$:

Theorem 2. *Let $M \in \mathbb{F}_q[t]$ be a fixed polynomial, and let $k \geq 2$ be an integer. If $d >$ $\deg M$, then*

$$\#U_k(M, d) = \frac{q^d}{d} \prod_{\substack{P\nmid M \\ P\in\mathscr{P}_+}} \left(1 - \frac{1}{|P|^k - |P|^{k-1}}\right) + \mathcal{O}\left(q^{\frac{d}{2}+\frac{d+2(1-k)}{2k}}\right). \tag{1.2}$$

It may be possible to improve the error term and we hope to address this question in future work.

2. Preliminaries

We set the following notations throughout this note:

$$\begin{array}{ll} \mathbb{A} = \mathbb{F}_q[t] & \text{The polynomial ring with one variable.} \\ \mathbb{A}_+ & \text{The set of all monic polynomials in } \mathbb{A}. \\ \mathscr{P}_+ & \text{The set of all monic irreducible polynomials in } \mathbb{A}. \end{array} \tag{2.1}$$

For any $Q \in \mathbb{A}_+$, we write its factorization $Q = \prod_{i=1}^r P_i^{n_i}$ with $P_i \in \mathscr{P}_+$. We define the polynomial Möbius function as

$$\mu(Q) = \begin{cases} 1 & \text{if } Q = 1, \\ 0 & \text{if } Q \text{ is not square-free}, \\ (-1)^r & \text{if } Q \text{ is square-free and } Q = P_1 \cdots P_r, \text{ where } P_i \in \mathscr{P}_+. \end{cases}$$

Analogously, for any integer $k \geq 2$, we define

$$\mu_k(Q) = \begin{cases} 1 & \text{if } Q \text{ is } k\text{-free}, \\ 0 & \text{otherwise}. \end{cases}$$

It is easy to verify identity

$$\mu_k(Q) = \sum_{\substack{a \\ a^k b = Q}}{}' \mu(a), \tag{2.2}$$

for powers of irreducible polynomials. The general identity then follows on noting that both sides of (2.2) are multiplicative. Furthermore, we define the polynomial Euler Φ-function $\Phi(Q)$ as the cardinality of $(\mathbb{A}/Q\mathbb{A})^*$. Throughout the paper, we denote by $\sum'$ and $\prod'$ the sum and product taken over only monic polynomials.

We record here a result that will be used below in our error analysis. It is a variation of Lemma 4.17 in [2]. This lemma gives the following bound using a result of Carlitz on the average value of the divisor function on the monic polynomial of fixed degree [1]: for every $n \geq 1$, we have

$$\sum_{\deg a = n}{}' \frac{1}{\Phi(a)} \leq \begin{cases} \frac{3}{4}(n+1) & \text{if } q > 2, \\ n+1 & \text{if } q = 2, \end{cases} \tag{2.3}$$

where the sum (with prime, following our convention) is over monic polynomials in $\mathbb{A}$ of degree n. In fact, the bound (2.3) is sufficient for obtaining the desired result. However, in order to keep this note self-contained, we state and prove the following lemma which gives a slightly different bound from (2.3).

Lemma 3. *For every $n \geq 1$, we have*

$$\sum_{\deg a = n}{}' \frac{1}{\Phi(a)} \leq \left(\frac{q}{q-1}\right)^2, \tag{2.4}$$

where the dashed sum is over monic polynomials $a \in \mathbb{A}$ of degree n.

Proof. Given any polynomial f, we denote by $rad(f)$ the product of the distinct monic irreducible polynomials dividing f, and we call it the radical of f. Now, note that

$$\begin{aligned}
\sideset{}{'}\sum_{\deg a=n} \frac{|a|}{\Phi(a)} &= \sideset{}{'}\sum_{\deg a=n} \sideset{}{'}\prod_{\substack{v\in\mathscr{P}_+\\ v|a}} \left(1-\frac{1}{|v|}\right)^{-1} = \sideset{}{'}\sum_{\deg a=n} \sideset{}{'}\prod_{\substack{v\in\mathscr{P}_+\\ v|a}} \left(1+\frac{1}{|v|}+\frac{1}{|v|^2}+\ \cdots\ \right) \\
&= \sideset{}{'}\sum_{\deg a=n} \sideset{}{'}\sum_{rad(g)|a} \frac{1}{|g|} = \sideset{}{'}\sum_{\substack{g\\ \deg rad(g)\le n}} \frac{1}{|g|} \sideset{}{'}\sum_{\substack{a\\ \deg a=n\\ rad(g)|a}} 1 \ \le \sideset{}{'}\sum_{\substack{g\\ \deg rad(g)\le n}} \frac{1}{|g|} q^{n-\deg(rad(g))} \\
&= \sideset{}{'}\sum_{\substack{g\\ \deg rad(g)\le n}} \frac{1}{|g|}\frac{q^n}{|rad(g)|} = q^n \sideset{}{'}\sum_{\substack{g\\ \deg rad(g)\le n}} \frac{1}{|g||rad(g)|} \\
&\le q^n \sideset{}{'}\prod_{v\in\mathscr{P}_+} \left(1+\frac{1}{|v|^2}+\frac{1}{|v|^3}+\ \cdots\ \right) = q^n \sideset{}{'}\prod_{v\in\mathscr{P}_+} \left(1+\frac{1}{|v|(|v|-1)}\right).
\end{aligned}$$

Hence, since $|a| = q^n$, we have

$$\sideset{}{'}\sum_{\deg a=n} \frac{1}{\Phi(a)} \le \sideset{}{'}\prod_{v\in\mathscr{P}_+} \left(1+\frac{1}{|v|(|v|-1)}\right) = C(q) \quad \text{(say)}. \tag{2.5}$$

Recall that if N_d is the number of monic irreducible polynomials of degree d, then $\sum_{d|m} dN_d = q^m$. Thus, $N_m \le q^m/m$. We use this to estimate $C(q)$ as follows: We observe that

$$C(q) \le \prod_{m=1}^{\infty} \left(1+\frac{1}{q^m(q^m-1)}\right)^{q^m/m}.$$

Using the inequality $1 + x \le e^x$ for $x > 0$, we obtain

$$C(q) \le \exp\left(\sum_{m=1}^{\infty} \frac{1}{m(q^m-1)}\right).$$

Finally, for $q \ge 2$, $q^m - 1 \ge q^m/2$. Inserting this into our estimate and using the familiar Taylor expansion for the logarithm function yields

$$C(q) \le \left(\frac{q}{q-1}\right)^2,$$

as claimed. $\square$

Remark 4. If we consider the following sum over all a of degree less than or equal to n

$$\sideset{}{'}\sum_{\deg a\le n} \frac{1}{\Phi(a)},$$

then the estimation (2.3) gives a bound of order n^2. Whereas Lemma 3 gives a bound $\mathcal{O}(n)$ with implied constant (which is smaller or equal than 4) depending only on q. In fact, as $\Phi(a) \leq |a|$, we also see that

$$\sum_{\deg a \leq n}' \frac{1}{\Phi(a)} \geq \sum_{\deg a \leq n}' \frac{1}{|a|} = n,$$

so that our estimate is (apart from a constant factor) sharp.

3. Proof of Theorem 2

We write

$$\#U_k(M,d) = \sum_{\substack{\deg P = d \\ P \in \mathscr{P}_+}}' \mu_k(P+M). \tag{3.1}$$

Since we assumed $d > \deg M$, using (2.2), we have

$$\#U_k(M,d) = \sum_{\substack{\deg P = d \\ P \in \mathscr{P}_+}}' \sum_{a^k b = P+M}' \mu(a) = \sum_{\substack{\deg a \leq d/k \\ (a,M)=1}}' \mu(a) \sum_{\substack{\deg P = d \\ a^k b = P+M \\ P \in \mathscr{P}_+}}' 1.$$

For any $t \leq d/k$, we can split the sum as

$$\#U_k(M,d) = \sum_{\substack{\deg a \leq t \\ (a,M)=1}}' \mu(a) \sum_{\substack{\deg P = d \\ P \equiv -M \pmod{a^k} \\ P \in \mathscr{P}_+}}' 1 + \sum_{\substack{t < \deg a \leq d/k \\ (a,M)=1}}' \mu(a) \sum_{\substack{\deg P = d \\ P \equiv -M \pmod{a^k} \\ P \in \mathscr{P}_+}}' 1. \tag{3.2}$$

We will choose later a suitable t with $0 < t < d/k$ to minimize the error term (the second term) of (3.2). This is how we fix the mistake in [9], which occurs on lines 10-13, where $\mu(a)$ should be $|\mu(a)|$, but then the result does not follow. The error term cannot be treated by a uniform estimate and one needs to bisect it as we do below. Yao's argument, as it stands, can be fixed for $k > 2$, but not for $k = 2$.

To estimate $\#U_k(M,d)$, we need the well-known result on the number of monic irreducible polynomials which belong to a fixed residue class, which is partially due to Kornblum [3] (we refer the reader to [8, p. 33] for the tragic history surrounding this theorem), along with the Riemann hypothesis for function fields which is proved by Weil. More precisely, we use the following formulation from [8, Theorem 4.8]: Let $M, Q \in \mathbb{A}$ with $(M,Q) = 1$. Then, we have

$$\frac{1}{\Phi(Q)} \frac{q^d}{d} - (\deg Q - 1) \frac{q^{d/2}}{d} \leq \sum_{\substack{\deg P = d \\ P \equiv M \pmod{Q} \\ P \in \mathscr{P}_+}}' 1 \leq \frac{1}{\Phi(Q)} \frac{q^d}{d} + (\deg Q - 1) \frac{q^{d/2}}{d} \tag{3.3}$$

Hence, by letting $Q = a^k$,

$$\frac{1}{\Phi(a^k)}\frac{q^d}{d} - (\deg(a^k)-1)\frac{q^{d/2}}{d} \le \sideset{}{'}\sum_{\substack{\deg P=d \\ P\equiv -M \pmod{a^k} \\ P\in\mathscr{P}_+}} 1 \le \frac{1}{\Phi(a^k)}\frac{q^d}{d} + (\deg(a^k)-1)\frac{q^{d/2}}{d}. \quad (3.4)$$

Thus, when $\deg a \le t$, we have as $tk \le d$,

$$\left| \sideset{}{'}\sum_{\substack{\deg P=d \\ P\equiv -M \pmod{a^k} \\ P\in\mathscr{P}_+}} 1 - \frac{1}{\Phi(a^k)}\frac{q^d}{d} \right| \le q^{d/2},$$

and the first sum of (3.2) satisfies

$$\left| \sideset{}{'}\sum_{\substack{\deg a\le t \\ (a,M)=1}} \mu(a) \sideset{}{'}\sum_{\substack{\deg P=d \\ P\equiv -M \pmod{a^k} \\ P\in\mathscr{P}_+}} 1 - \frac{q^d}{d} \sideset{}{'}\sum_{\substack{\deg a\le t, \\ (a,M)=1}} \frac{\mu(a)}{\Phi(a^k)} \right| \le q^{d/2} \sideset{}{'}\sum_{\substack{\deg a\le t \\ (a,M)=1}} |\mu(a)| = \mathcal{O}(q^{d/2+t}). \quad (3.5)$$

The second double sum in (3.2) satisfies

$$\sideset{}{'}\sum_{\substack{t<\deg a\le d/k \\ (a,M)=1}} \mu(a) \sideset{}{'}\sum_{\substack{\deg P=d \\ P\equiv -M \pmod{a^k} \\ P\in\mathscr{P}_+}} 1 = \sideset{}{'}\sum_{\substack{t<\deg a\le d/k \\ (a,M)=1}} \mathcal{O}(q^{d-k\cdot\deg a}) = \mathcal{O}(q^{d+(1-k)(t+1)}), \quad (3.6)$$

since

$$\sideset{}{'}\sum_{t<\deg a} q^{-k\deg a} \le \sum_{n=t+1}^{\infty} q^{-kn}q^n = \mathcal{O}(q^{(1-k)(t+1)}),$$

where the implied constant depends only on q and k. Therefore, for any $0 < t < d/k$, we have

$$\#U_k(M,d) = \frac{q^d}{d} \sideset{}{'}\sum_{\substack{\deg a\le t \\ (a,M)=1}} \frac{\mu(a)}{\Phi(a^k)} + \mathcal{O}(q^{d/2+t}) + \mathcal{O}(q^{d+(1-k)(t+1)}).$$

By choosing $t = \frac{d}{2k} + \frac{1-k}{k}$, the two error terms become of equal order and we obtain

$$\#U_k(M,d) = \frac{q^d}{d} \sideset{}{'}\sum_{\substack{\deg a\le t \\ (a,M)=1}} \frac{\mu(a)}{\Phi(a^k)} + \mathcal{O}\left(q^{\frac{d}{2}+\frac{d+2(1-k)}{2k}}\right). \quad (3.7)$$

Now, note that

$$\frac{q^d}{d}\sum_{(a,M)=1}{}' \frac{\mu(a)}{\Phi(a^k)} = \frac{q^d}{d}\prod_{\substack{P\nmid M\\ P\in\mathscr{P}_+}}{}' \left(1-\frac{1}{\Phi(P^k)}\right) = \frac{q^d}{d}\prod_{\substack{P\nmid M\\ P\in\mathscr{P}_+}}{}' \left(1-\frac{1}{|P|^k-|P|^{k-1}}\right). \quad (3.8)$$

By using Lemma 3, we have

$$\left|\frac{q^d}{d}\sum_{\substack{\deg a>t\\ (a,M)=1}}{}' \frac{\mu(a)}{\Phi(a^k)}\right| \le \frac{q^d}{d}\sum_{n>t}\sum_{\deg a=n}{}' \frac{1}{\Phi(a^k)} = \frac{q^d}{d}\sum_{n>t}\sum_{\deg a=n}{}' \frac{1}{|a^{k-1}|\Phi(a)} \le \frac{q^d}{d}\sum_{n>t}\frac{C(q)}{q^{n(k-1)}}. \quad (3.9)$$

The error term is of the same magnitude as before, completing the proof. □

Let us make a few remarks about the error term. The main term in Theorem 2 is of order q^d and the error term is

$$\mathcal{O}\left(q^{\frac{d}{2}+\frac{d+2(1-k)}{2k}}\right).$$

We see that for $k \ge 2$, we always have

$$\frac{d}{2}+\frac{d+2(1-k)}{2k} < d,$$

which is as expected. This error term is comparable to what one would get by injecting the Generalized Riemann Hypothesis into the argument of Mirsky.

4. Future directions

As noted earlier, it would be interesting to see if the error term in Theorem 2 can be improved. A generalization of Theorem 1 involving higher dimensional tuples of fixed polynomials can be discussed analogously following the generalization by Mirsky [4] for number fields. Moreover, further generalization is possible following the subsequent result of Mirsky [5].

Acknowledgment

We would like to thank Michael Rosen, Joseph H. Silverman, Wei-Chen Yao, and the anonymous referee for helpful suggestions on an earlier version of this paper.

References

[1] Leonard Carlitz, The arithmetic of polynomials in a Galois field, Am. J. Math. 54 (1) (1932) 39–50, https://doi.org/10.2307/2371075, MR1506871.

[2] Gove W. Effinger, David R. Hayes, Additive Number Theory of Polynomials over a Finite Field, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1991, Oxford Science Publications, MR1143282.
[3] Heinrich Kornblum, E. Landau, Über die Primfunktionen in einer arithmetischen Progression, Math. Z. 5 (1–2) (1919) 100–111, https://doi.org/10.1007/BF01203156 (German). MR1544375.
[4] L. Mirsky, Note on an asymptotic formula connected with r-free integers, Q. J. Math. 18 (1947) 178–182, https://doi.org/10.1093/qmath/os-18.1.178, MR21566.
[5] L. Mirsky, Generalizations of a problem of Pillai, Proc. R. Soc. Edinb., Sect. A 62 (1949) 460–469, MR30560.
[6] L. Mirsky, The number of representations of an integer as the sum of a prime and a k-free integer, Am. Math. Mon. 56 (1949) 17–19, https://doi.org/10.2307/2305811, MR28335.
[7] Pieter Moree, Artin's primitive root conjecture—a survey, Integers 12 (6) (2012) 1305–1416, https://doi.org/10.1515/integers-2012-0043, MR3011564.
[8] Michael Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002, MR1876657.
[9] Wei-Chen Yao, On an elementary density problem for polynomials over finite fields, Finite Fields Appl. 7 (3) (2001) 441–448, https://doi.org/10.1006/ffta.2001.0325, MR1841909.