The Raymond and
Beverly Sackler Faculty
of Exact Sciences
Tel Aviv University

THE LCM PROBLEM FOR FUNCTION FIELDS

Thesis submitted in partial fulfillment of the requirements for the degree
Master of Science (M.Sc.) at Tel Aviv University,
School of Mathematical Sciences

by
Etai Leumi

The Thesis was prepared under the supervision of
Professor Zeév Rudnick

April, 2021

The Raymond and
Beverly Sackler Faculty
of Exact Sciences
Tel Aviv University

THE LCM PROBLEM FOR FUNCTION FIELDS

Thesis submitted in partial fulfillment of the requirements for the degree
Master of Science (M.Sc.) at Tel Aviv University,
School of Mathematical Sciences

by
Etai Leumi

The Thesis was prepared under the supervision of
Professor Zeév Rudnick

April, 2021

Acknowledgments

I thank Lior Bary-Soroker, Ofir Gorodetsky, Uriel Sinichkin and Iddo Yadlin for helpful discussions, and my dear advisor Prof. Zeév Rudnick for everything about this endeavor.

This research was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (Grant agreement No. 786758)

Contents

Abstract. Cilleruelo conjectured that for any irreducible polynomial f with integer coefficients, and $\deg f \geq 2$, the least common multiple of the values of f at the first N integers satisfies $\log \operatorname{lcm}(f(1), \ldots, f(N)) \sim (\deg f - 1) N \log N$, as N tends to infinity. He proved this only for $\deg f = 2$. No example in higher degree is known. We study the analogue of this conjecture for function fields, where we replace the integers by the ring of polynomials over a finite field. In that setting we are able to establish some instances of the conjecture for higher degrees. The examples are all "special" polynomials $f(X)$, which have the property that the bivariate polynomial $f(X) - f(Y)$ factors into linear terms in the base field.

1. Introduction

When studying the distribution of prime numbers, Chebychev had the idea of estimating the least common multiple of the first n integers. This was the first important step towards the prime number theorem, and in fact the asymptotic estimate $\log \operatorname{lcm}(1, \dots, N) \sim N$ is equivalent to the prime number theorem. Later, the l.c.m. problem was generalized to the study of the least common multiple of a polynomial sequence. The linear case was also solved and is a consequence of the prime number theorem for arithmetic progressions [2]. In 2011 Cilleruelo conjectured that for any irreducible polynomial $f \in \mathbb{Z}[X]$ with $\deg f = d \geq 2$, the following estimate holds [3]:

$$\log \operatorname{lcm}(f(1), \dots, f(N)) \sim (d-1)N \log N\,, \quad \text{as } N \to \infty$$

Cilleruelo proved this estimate for quadratic polynomials, but if $\deg f = d > 2$ the conjecture is still open. An examination of Cilleruelo's argument also shows a good upper bound, that is for any irreducible polynomial $f \in \mathbb{Z}[X]$ with $\deg f = d \geq 2$ we have

$$\log \operatorname{lcm}(f(1), \dots, f(N)) \lesssim (d-1)N \log N.$$

Here $f \lesssim g$ means that $|f(x)| \leq (1 + o(1))g(x)$.

In 2018 Maynard and Rudnick provided a lower bound of the correct magnitude, i.e. (see [5, Theorem 1.2])

$$\log \operatorname{lcm}(f(1), \dots, f(N)) \gtrsim \frac{d}{d^2-1} N \log N.$$

In 2019 Ashwin Sah improved the lower bound to (see [10, Theorem 1.4])

$$\log \operatorname{lcm}(f(1), \dots, f(N)) \gtrsim \frac{2}{d} N \log N.$$

Eventhough we have these upper and lower bounds, and due to Rudnick and Zehavi the conjecture holds for almost all f in a suitable sense (see [9]). There is not a single polynomial of degree ≥ 3 for which it is known that Cilleruelo's conjecture holds, e.g. for $x^3 + 2$ we do not know this conjecture. Our goal is to study the analogue of Cilleruelo's conjecture for function fields, and establish examples of arbitrary degree.

The function field analogue.
For a polynomial $f \in (\mathbb{F}_q[T])[X]$, set

$$\text{Ł}_f(n) := \operatorname{lcm}(f(Q) : \; Q \in M_n)$$

where $M_n = M_n^q := \#\{Q \in \mathbb{F}_q[T] \,:\, Q \text{ is monic and } \deg Q = n\}$. So the analogue of Cilleruelo's conjecture for function fields is

Conjecture 1.1. *If $f \in (\mathbb{F}_q[T])[X]$ is absolutely irreducible and separable with $\deg_X(f) = d \geq 2$ (the degree taken w.r.t X), then*

$$\deg L_f(n) \sim (d-1)q^n n \;\;, \;\; n \to \infty$$

Remark. Here $f \in (\mathbb{F}_q[T])[X]$ is **absolutely** irreducible, if for any algebraic extension $\mathbb{F}_q \subset \mathbb{F}$ f is irreducible over $\mathbb{F}[T]$. We need the assumption that f is absolutely irreducible and separable to apply Chebotarev's density theorem over function fields. We establish instances of conjecture 1.1: Let K be a field. We call a polynomial $f(X) \in K[X]$ special, if the bivariate polynomial $f(X) - f(Y)$ factors into a product of linear terms in $K[X, Y]$. For these "special" polynomials in $(\mathbb{F}_q[T])[X]$, when they are also absolutely irreducible and separable, conjecture 1.1 holds. Our main result is the following theorem:

Theorem 1.2. *For the following polynomials in* $(\mathbb{F}_q[T])[X]$ *conjecture* 1.1 *holds:*

(1) $(X+A)^d + C$, *when* $q \equiv 1 \mod d$.

(2) $(X^{p^l} - A^{p^l-1}X)^k + C$, *when* p *is prime,* $q = p^m$ *and* $l, m, k \in \mathbb{N}$ *satisfy* $l \mid m$, $k \mid p^{l-1}$.

where $0 \neq A, C \in \mathbb{F}_q[T]$, *and* $\exists P \in \mathbb{F}_q[T]$ *prime s.t.* $P \mid A, C$, *but* $P^2 \nmid C$.

For instance, take $q = 7^m$ and consider the polynomials $f(X) = X^3 + T$, $g(X) = X^7 - T^6 X + T$ over $\mathbb{F}_q[T]$. Then we know

$$\deg L_f(n) \sim 2q^n n \ , \ \deg L_g(n) \sim 6q^n n \ \ , \text{ as } n \to \infty.$$

Remark on notation. Throughout the next two sections we fix a polynomial $f(X) \in (\mathbb{F}_q[T])[X]$ which is absolutely irreducible and separable, with $2 \leq \deg_X(f) = d$ (the degree taken w.r.t X). we also write

$$f(X) = \sum_{i=0}^{d} f_i X^i$$

finally, note that we follow the same standard notaions in function fields as in [7], e.g. for $Q \in \mathbb{F}_q[T]$ we write $|Q|$ to be the number of elements in $\mathbb{F}_q[T] \mod Q$, i.e.

$$|Q| = q^{\deg Q}.$$

Acknowledgements.

2. The upper bound and the quadratic case

To achieve the upper and lower bounds, similarly to the integer case, we set $P_f(n) := \prod_{Q \in M_n} f(Q)$ and the main idea is to estimate the difference to $L_f(n)$, i.e.

$$\deg L_f(n) = \deg P_f(n) - (\deg P_f(n) - \deg L_f(n))$$

Claim 2.1. $\deg P_f(n) = dq^n n + O(q^n)$

Proof. For n sufficiently large n and $Q \in M_n$, $\deg f(Q) = dn + \deg f_d$. Hence

$$\begin{aligned} \deg P_f(n) = \deg \prod_{Q \in M_n} f(Q) &= \sum_{Q \in M_n} \deg f(Q) \\ &= \sum_{Q \in M_n} (dn + \deg f_d) = dq^n n + O(q^n). \end{aligned}$$

□

To estimate $\deg P_f(n) - \deg L_f(n)$ we write the prime decomposition of $L_f(n)$ and $P_f(n)$ as

$$L_f(n) = \prod_{P:\text{ Prime}} P^{\beta_P(n)} \ \ , \ \ P_f(n) = \prod_{P:\text{ Prime}} P^{\alpha_P(n)}$$

So, for $P \in \mathbb{F}_q[T]$ prime we see that

$$\alpha_P(n) = \sum_{Q \in M_n} v_P(f(Q)) \ \ , \ \ \beta_P(n) = \max\{v_P(f(Q)) : Q \in M_n\}.$$

where $v_P(Q) = \max\{k \in \mathbb{Z} : P^k \mid Q\}$, for $Q \in \mathbb{F}_q[T]$.
Thus,

$$\deg L_f(n) = dq^n n - \sum_P (\alpha_P(n) - \beta_P(n)) \deg P + O(q^n).$$

To evaluate $\alpha_P(n)$, we define for $k, n \in \mathbb{N}$ and $P \in \mathbb{F}_q[T]$ prime:

- $\rho_f(P^k) = \#\{Q \mod P^k \ : \ f(Q) \equiv 0 \mod P^k\}$

- $s_f(P^k, n) = \#\{Q \in M_n \,:\, f(Q) \equiv 0 \mod P^k\}$

Our main tool to estimate α_P, β_P is the following lemma:

Lemma 2.2. *Let $P \in \mathbb{F}_q[T]$ be prime.*

(1) $\beta_P(n) = O\left(\frac{dn}{\deg P}\right)$

(2) if $P \nmid disc(f)$ (a.k.a "good" prime), then

$$\alpha_P(n) = q^n \frac{\rho_f(P)}{|P| - 1} + O\left(\frac{n}{\deg P}\right)$$

and if $P \mid disc(f)$ (a.k.a "bad" prime), then

$$\alpha_P(n) = O(q^n)$$

Proof. 1. Since $P^{\beta_P(n)} \mid f(Q)$ for some $Q \in \mathbb{F}_q[T]$, noting that $f(Q) \neq 0$ we get:

$$\beta_P(n) \deg P \leq \deg f(Q)$$

and for sufficiently large n we have $\deg f(Q) = dn + \deg f_d$, thus

$$\beta_P(n) \ll \frac{n}{\deg P}.$$

2. For any prime P we have

$$\alpha_P(n) = \sum_{Q \in M_n} v_P(f(Q)) = \sum_{Q \in M_n} \sum_{\substack{k \geq 0: \\ P^k \mid f(Q)}} 1$$

$$= \sum_{k \ll \frac{n}{degP}} \sum_{\substack{Q \in M_n: \\ P^k \mid f(Q)}} 1 = \sum_{k \ll \frac{n}{degP}} s_f(P^k, n).$$

Noting that $s_f(P^k, n) = \rho_f(P^k)\left(\left\lfloor \frac{\#M_n}{|P^k|} \right\rfloor + O(1)\right)$ and $\rho_f(P^k) \ll 1$, we get

$$\sum_{k \ll \frac{n}{degP}} s_f(P^k, n) = \sum_{k \ll \frac{n}{degP}} \rho_f(P^k)\left(\frac{q^n}{|P|^k} + O(1)\right)$$

$$= \sum_{k \ll \frac{n}{degP}} \rho_f(P^k)\left(\frac{q^n}{|P|^k}\right) + O\left(\frac{n}{\deg P}\right).$$

Now, if $P \nmid \mathrm{disc}(f)$, then by Hensel's lemma we have $\rho_f(P^k) = \rho_f(P)$, and so

$$\alpha_P(n) = \sum_{k \ll \frac{n}{degP}} \rho_f(P)\left(\frac{q^n}{|P|^k}\right) + O\left(\frac{n}{\deg P}\right)$$

$$= q^n \rho_f(P) \sum_{k \ll \frac{n}{degP}} \left(\frac{1}{|P|}\right)^k + O\left(\frac{n}{\deg P}\right)$$

$$= q^n \frac{\rho_f(P)}{|P| - 1} + O\left(\frac{n}{\deg P}\right)$$

and if $P \mid \mathrm{disc}(f)$, then

$$\alpha_P(n) = \sum_{k \ll \frac{n}{degP}} \rho_f(P^k)\left(\frac{q^n}{|P|^k}\right) + O\left(\frac{n}{\deg P}\right)$$

$$\ll q^n \sum_{k \ll \frac{n}{degP}} \left(\frac{1}{|P|}\right)^k + O\left(\frac{n}{\deg P}\right)$$

$$\ll q^n.$$

□

Corollary 2.3.

$$\deg\left(\prod_{n<\deg P\leq n+\deg f_d} P^{\alpha_P(n)}\right)=O(q^n)$$

Proof. Set $\delta:=\deg f_d$. By lemma 2.2 for n sufficiently large and $P\in\mathbb{F}_q[T]$ prime s.t $\deg P>n$, we have $\alpha_P(n)\ll 1$. Thus, by the Prime Polynomial Theorem (in short PPT, see [7, Theorem 2.2]), we get

$$\begin{aligned}\deg\left(\prod_{n<\deg P\leq n+\delta} P^{\alpha_P(n)}\right) &= \sum_{\deg n<\deg P\leq n+\delta}\alpha_P(n)\deg P\\ &\ll \sum_{\deg n<\deg P\leq n+\delta}\deg P=\sum_{k=n+1}^{n+\delta}\sum_{\deg P=k}k\\ &\ll \sum_{k=n+1}^{n+\delta}k\frac{q^k}{k}=\frac{q^{n+\delta+1}-q^{n+1}}{q-1}\\ &=O(q^n)\end{aligned}$$

□

Claim 2.4. *Denote $R_f(n)=\prod P^{\alpha_P(n)}$, where the product is over primes p s.t. $\deg P\leq n+\deg f_d$. Then*

$$\deg R_f(n)=nq^n+O(q^n)$$

Proof. By lemma 2.2 , noting that in our estimation we can neglect the contributions of "bad" primes with an error term of $O(q^n)$, we have

$$\begin{aligned}\deg R_f(n) &= \sum_{\deg P\leq n}\alpha_P(n)\deg P+O(q^n)\\ &= \sum_{\deg P\leq n}q^n\frac{\rho_f(P)}{|P|-1}\deg P+\sum_{\deg P\leq n}O(n)+O(q^n)\end{aligned}$$

We bound the error term using PPT:

$$\begin{aligned}\sum_{\deg P\leq n}n &= n\sum_{k=1}^{n}\sum_{\deg P=k}1\\ &\ll n\sum_{k=1}^{n}\frac{q^k}{k}=n\sum_{1\leq k<n/2}\frac{q^k}{k}+n\sum_{n/2\leq k\leq n}\frac{q^k}{k}\\ &\ll nq^{n/2}\sum_{1\leq k<n/2}\frac{1}{k}+n\frac{2}{n}\sum_{n/2\leq k\leq n}q^k\\ &\ll nq^{n/2}\log n+2q^{n/2}\sum_{0\leq k\leq n/2}q^k\\ &\ll nq^{n/2}\log n+2q^{n/2}\frac{q^{n/2+1}-1}{q-1}\ll q^n\end{aligned}$$

We evaluate the main term using Chebotarev's density theorem and PPT (for an exposition on Chebotarev's theorem see [1, pages 1-2]). Chebotarev's density theorem yields:

$$\sum_{\deg P=k}\rho_f(P)=\frac{q^k}{k}+O\left(\frac{q^{k/2}}{k}\right)$$

plainly speaking, in our case Chebotarev's density theorem gives a correspondence between the number of roots of $f \mod P$ and the the number of fixed points of a certain Galois automorphism of the spliting field of f. By Burnside's lemma (see [8, Theorem 3.22])), the latter is on average 1 and so the quantity $\rho_f(P)$ is also on average 1.
Thus,

$$\begin{aligned}\sum_{\deg P\leq n} q^n \frac{\rho_f(P)}{|P|-1}\deg P &= q^n \sum_{k=1}^{n}\sum_{\deg P=k}\frac{\rho_f(P)}{q^k-1}k\\ = q^n\sum_{k=1}^{n}\frac{k}{q^k-1}\sum_{\deg P=k}\rho_f(P) &= q^n\sum_{k=1}^{n}\frac{k}{q^k-1}\left[\frac{q^k}{k}+O\left(\frac{q^{k/2}}{k}\right)\right]\\ = q^n\sum_{k=1}^{n}\left[\frac{q^k}{q^k-1}+O\left(\frac{q^{k/2}}{q^k-1}\right)\right] &= q^n\sum_{k=1}^{n}\left[1+O\left(\frac{q^{k/2}}{q^k-1}\right)\right]\\ = nq^n + q^n\sum_{k=1}^{n}O\left(\frac{q^{k/2}}{q^k-1}\right) &= nq^n+O(q^n).\end{aligned}$$

So we conclude

$$\deg R_f(n) = nq^n + O(q^n)$$

□

Proposition 2.5. *(Upper bound)*

$$L_f(n) \lesssim (d-1)nq^n, \quad as \;\; n\to\infty$$

Proof. Using claim 2.1 and observing that $\alpha_P(n)\geq\beta_P(n)$, for all P prime, we get

$$\begin{aligned}\deg L_f(n) &= \deg P_f(n) - (\deg P_f(n) - \deg L_f(n))\\ &= dnq^n - \sum_P(\alpha_P(n)-\beta_P(n))\deg P\\ &\leq dnq^n - \sum_{\deg P\leq n+\deg f_d}(\alpha_P(n)-\beta_P(n))\deg P \quad (1)\\ &= dnq^n - \sum_{\deg P\leq n+\deg f_d}\alpha_P(n)\deg P + \sum_{\deg P\leq n+\deg f_d}\beta_P(n)\deg P\\ &= (d-1)nq^n + \sum_{\deg P\leq n+\deg f_d}\beta_P(n)\deg P + O(q^n) \quad (2)\end{aligned}$$

where (1) follows from neglecting negative terms, and (2) from claim 2.4.

To finish the argument all we need is $\sum_{\deg P\leq n+\deg f_d}\beta_P(n)\deg P = O(q^n)$. By lemma 2.2 and the analysis we already did in claim 2.4, we have

$$\begin{aligned}\sum_{\deg P\leq n+\deg f_d}\beta_P(n)\deg P &\ll \sum_{\deg P\leq n+\deg f_d}\frac{n}{\deg P}\deg P\\ &= \sum_{\deg P\leq n+\deg f_d} n \ll q^n.\end{aligned}$$

□

Definition 2.6. *Let $f\in(\mathbb{F}_q[T])[X]$ s.t $\deg_X f = d\geq 2$, and let f_d be the leading coefficient of f. Define the quantity $S_f(n)$ to be the number of primes $P\in\mathbb{F}_q[T]$ s.t. $\deg P > n+\deg f_d$ and $\alpha_P(n)\neq\beta_P(n)$. Noting that $\alpha_P(n)\neq\beta_P(n) \iff \exists Q_1,Q_2\in M_n$ distinct s.t $P\mid f(Q_1), f(Q_2)$, we see*

$$S_f(n) = \#\left\{P\in\mathbb{F}_q[T] \;:\; {\deg P > n+\deg f_d, \atop \exists Q_1\neq Q_2\in M_n \; s.t\; P|f(Q_1),f(Q_2)}\right\}$$

Corollary 2.7. *Let $f \in (\mathbb{F}_q[T])[X]$ be absolutely irreducible and separable with $\deg_X f = d \geq 2$. Then, conjecture 1.1 is equivalent to*

$$S_f(n) = o(q^n)$$

Moreover, we have

$$S_f(n) \ll q^n$$

Proof. In the proof of the upper bound there is only one inequality (i.e. (1)), namely

$$\sum_{\deg P > n + \deg f_d} (\alpha_P(n) - \beta_P(n)) \deg P > 0$$

so it suffices to prove that

$$S_f(n) = o(q^n) \iff \sum_{\deg P > n + \deg f_d} (\alpha_P(n) - \beta_P(n)) \deg P = o(nq^n)$$

For $P \in \mathbb{F}_q[T]$ prime, let $\mathbb{1}_P(n) = \left\{ \begin{array}{ll} 1 & \text{if } \alpha_P(n) \neq \beta_P(n) \\ 0 & \text{otherwise} \end{array} \right.$.
Note that $\alpha_P(n) \neq \beta_P(n) \iff \exists Q_1, Q_2 \in M_n$ distinct s.t $P \mid f(Q_1), f(Q_2)$, and for n sufficiently large $\deg P > dn \implies \alpha_P(n) = 0$. Hence, for n sufficiently large we have

$$S_f(n) = \sum_{dn \geq \deg P > n + \deg f_d} \mathbb{1}_P(n).$$

From lemma 2.2, for sufficiently large n, if $\deg P > n$ then $\alpha_P(n) \ll 1$, so

$$\begin{aligned} \sum_{\deg P > n + \deg f_d} (\alpha_P(n) - \beta_P(n)) \deg P &\ll \sum_{dn \geq \deg P > n + \deg f_d} \mathbb{1}_P(n) \deg P \\ &\ll \sum_{dn \geq \deg P > n + \deg f_d} \mathbb{1}_P(n) n \\ &= S_f(n) n. \end{aligned}$$

On the other hand

$$\begin{aligned} \sum_{\deg P > n + \deg f_d} (\alpha_P(n) - \beta_P(n)) \deg P &\geq \sum_{\deg P > n + \deg f_d} \mathbb{1}_P(n) \deg P \\ &\geq \sum_{\deg P > n + \deg f_d} \mathbb{1}_P(n) n \\ &= S_f(n) n. \end{aligned}$$

Therefore

$$S_f(n) n \leq \sum_{\deg P > n + \deg f_d} (\alpha_P(n) - \beta_P(n)) \deg P \ll S_f(n) n$$

and so

$$S_f(n) = o(q^n) \iff \deg L_f(n) \sim (d-1) q^n n, \quad \text{as } n \to \infty$$

Finally, note that $S_f(n) \ll q^n$ follows from the upper bound. □

From this corollary we can easily achieve the quadratic case:

Corollary 2.8. *Let $f(X) = f_2 X^2 + f_1(T) X + f_0(T)$ be a quadratic polynomial which is absolutely irreducible and separable over $\mathbb{F}_q[T]$. Then,*

$$\deg L_f(n) = nq^n + O(q^n), \quad \textit{as } n \to \infty$$

Proof. for P prime in $\mathbb{F}_q[T]$, and $A, B \in M_n$ we have

$$\begin{aligned}
P \mid f(A), f(B) &\implies P \mid f(A) - f(B) = (A - B)(f_2 A + f_2 B + f_1) \\
&\implies P \mid (A - B) \vee P \mid (f_2 A + f_2 B + f_1) \\
&\implies \deg P \leq \max\{n + \deg f_2, \deg f_1\}.
\end{aligned}$$

Hence, for sufficiently large n if $\deg P > n + \deg f_2$, then $\alpha_P(n) = \beta_P(n)$. Thus $S_f(n) \ll 1$, and by corollary 2.7 we are done. □

3. A lower bound

Remark. First we prove a lower bound similar to the one Maynard and Rudnick provided (see [5, Theorem 1.2]), then will show an improved lower bound similar to Ashwin Sah (see [10, Theorem 1.4]). Our arguments here are due to Sah, though in the improved lower bound something gets lost in translation to the function field case (e.g. the characteristic is now positive), so we get a lower bound with some restrictions.

Lemma 3.1. *For $n \geq \deg f_d$ and $P \in \mathbb{F}_q[T]$ prime such that $\deg P \geq n$, we have*

$$\alpha_P(n) \leq d^2$$

Proof. Note that $\rho_f(P) \leq d$, since f is irreducible over $\mathbb{F}_q[T]$ of degree d. And since $\deg P \geq n$, at most d polynomials $Q \in M_n$ satisfy $P \mid f(Q)$. For such Q, and $n \geq \deg f_d$, we get

$$\deg P^{d+1} \geq nd + n > nd + \deg f_d = \deg f(Q)$$

Hence,

$$\alpha_P(n) = \sum_{Q \in M_n} v_P(f(Q)) \leq \sum_{\substack{Q \in M_n: \\ P \mid f(Q)}} d \leq d^2$$

□

Proposition 3.2. *(Lower bound) Let $f \in \mathbb{F}_q[T]$ be absolutely irreducible and separable. Then*

$$L_f(n) \gtrsim \frac{d-1}{d^2} n q^n$$

Proof. By lemma 2.4 and claim 2.1, we get

$$\begin{aligned}
(d-1)nq^n \lesssim \deg \frac{P_f(n)}{R_f(n)} &= \sum_{\deg P > n + \deg f_d} \alpha_P(n) \deg P \\
\leq \sum_{\substack{\deg P > n + \deg f_d, \\ \alpha_P(n) \neq 0}} d^2 \deg P &\leq d^2 \deg L_f(n)
\end{aligned}$$

from which the proposition follows. □

Lemma 3.3. *For sufficiently large n, if char$(\mathbb{F}_q) > d$, and $P \in \mathbb{F}_q[T]$ is prime s.t. $\deg P > n + \deg f_d$, then we have*

$$\alpha_P(n) \leq \frac{d(d-1)}{2}.$$

Proof. Fix a prime $P \in \mathbb{F}_q[T]$ s.t. $\deg P > n + \deg f_d$.
Denote $B_i := \#\{Q \in M_n : P^i \mid f(Q)\}$, for $i \in \mathbb{N}$. By lemma 3.1, $B_i = 0 \ \forall i > d$, thus

$$\alpha_P(n) = \sum_{Q \in M_n} \sum_{\substack{i > 0: \\ P^i \mid f(Q)}} 1 = \sum_{i > 0} \sum_{\substack{Q \in M_n: \\ P^i \mid f(Q)}} 1 = \sum_{i=1}^{d} B_i$$

we claim $B_i \leq d-i$ for all $1 \leq i \leq d$, from which the lemma follows immediately.

Suppose for the sake of contradiction that $B_i \geq d-i+1$ for some $1 \leq i \leq d$, and let $Q_1, \ldots, Q_{d-i+1} \in M_n$ be distinct s.t. $P^i \mid f(Q_j)$ for all $1 \leq j \leq d-i+1$. Consider the value

$$A := \sum_{j=1}^{d-i+1} \frac{f(Q_j)}{\prod_{k \neq j}(Q_j - Q_k)}.$$

This value (as we will see) is in $\mathbb{F}_q[T]$. To see this, note that from the theory of Lagrange interpolation polynomial, we have the identity: Let $A_1, \ldots, A_n \in \mathbb{F}_q[T]$ be distinct for some $n > 1$. Then, for $l \geq n-1$

$$\sum_{j=1}^{n} \frac{A_j^l}{\prod_{k \neq j}(A_j - A_k)} = \sum_{a_1+\ldots+a_n = l-(n-1)} \prod_{j=1}^{n} A_j^{a_j}$$

where the sum is over all tuples $(a_1, \ldots, a_n)$ of nonnegative integers that sum to $l-(n-1)$. Note that for $l < n-1$ this value vanishes.

Thus we have

$$\begin{aligned} A &= \sum_{l=0}^{d} f_l \sum_{j=1}^{d-i+1} \frac{Q_j^l}{\prod_{k \neq j}(Q_j - Q_k)} \\ &= \sum_{l=d-i}^{d} f_l \sum_{a_1+\ldots+a_{d-i+1} = l-(d-i)} \prod_{j=1}^{d-i+1} Q_j^{a_j} \end{aligned}$$

where the inner sum is over all tuples $(a_1, \ldots, a_{d-i+1})$ of nonnegative integers that sum to $l-(d-i)$.

Therfore, $A \in \mathbb{F}_q[T]$.

Note that the number of summands in the last inner sum (i.e. $l = d$) is $\binom{d}{d-i}$, and from the condition that $d > \text{char}\mathbb{F}_q$, this value does not vanish in $\mathbb{F}_q$. Thus, for sufficiently large n the degree of A is

$$\begin{aligned} \deg A &= \deg\left(f_d \sum_{a_1+\ldots+a_{d-i+1} = l-(d-i)} \prod_{j=1}^{d-i+1} Q_j^{a_j}\right) \\ &\overset{(1)}{=} \deg f_d + \max_{a_1+\ldots+a_{d-i+1} = l-(d-i)} \deg\left(\prod_{j=1}^{d-i+1} Q_j^{a_j}\right) \\ &= \deg f_d + i \cdot n \end{aligned}$$

where in (1) we used that $Q_1 \ldots, Q_{d-i+1}$ are all monic of degree n.

However, since $P^i \mid f(Q_j)$ for all $1 \leq j \leq d-i+1$, we have from the definition of A that

$$P^i \mid A \prod_{1 \leq j < k \leq d-i+1} (Q_j - Q_k)$$

and since $P^i \nmid (Q_j - Q_k)$ for any $1 \leq j < k \leq d-i+1$, we see that $P^i \mid A$. Whence

$$i \cdot n + \deg f_d < i \cdot \deg P \leq \deg A = i \cdot n + \deg f_d$$

which is a contradiction, so we obtain our result. □

Proposition 3.4. *(Restricted lower bound) Let $f \in \mathbb{F}_q[T]$ be absolutely irreducible and separable s.t. $2 \leq \deg_X f < char(\mathbb{F}_q)$. Then, we have*

$$\deg L_f(n) \gtrsim \frac{2}{d} n q^n$$

Proof. By claim 2.1 and lemma 3.3 we have

$$\begin{aligned}(d-1)nq^n &\lesssim \deg \frac{P_f(n)}{R_f(n)} \\ &= \sum_{\deg P > n + \deg f_d} \alpha_P(n) \deg P + O(q^n) \\ &\leq \sum_{\substack{\deg P > n + \deg f_d, \\ \alpha_P(n) \neq 0}} \frac{d(d-1)}{2} \deg P + O(q^n) \\ &\leq \frac{d(d-1)}{2} \deg L_f(n) + O(q^n)\end{aligned}$$

whence the proposition follows. □

Remark. Note that this lower bound yields the quadratic case, when $\mathrm{char}(\mathbb{F}_q) > 2$.

4. Special polynomials

In this section we will prove Cileruello's conjecture for some special subset of polynomials over function fields with appropriate characteristic. Our method will rely on the following observation:

Definition 4.1. *Let K be a field. We call a polynomial $f \in K[X]$* ***special****, if the bivariate polynomial $f(X) - f(Y) \in K[X,Y]$ factors into a product of linear terms in $K[X,Y]$.*

For *special* polynomials in $(\mathbb{F}_q[T])[X]$ we can prove Cilleruelo's conjecture. This is in fact a generalization of the property that yields the quadratic case. However, over the integers no such polynomial exists with degree greater than 2, as we shall see.

Claim 4.2. *Let K be a field, and $f \in K[X]$ monic of degree $d \geq 2$. Assume that*

$$f(X) - f(Y) = \prod_{i=1}^{d} (X - \alpha_i Y + \beta_i) \in K[X,Y] \text{ (i.e. } f \text{ is a special polynomial).}$$

Then, the coeeficients $\alpha_1, \dots, \alpha_d$ satisfy

$$X^d - 1 = \prod_{i=1}^{d} (X - \alpha_i).$$

Proof. Let $f(X) = X^d + \sum_{i=0}^{d-1} a_i X^i \in K[X]$, assume that $f(X) - f(Y)$ is *special* so that

$$f(X) - f(Y) = \prod_{i=1}^{d} (X - \alpha_i Y + \beta_i) \in K[X,Y]$$

after expanding the product to the right, while grouping together the terms $X - \alpha_i Y$, we get

$$X^d - Y^d + \sum_{i=1}^{d-1} a_i (X^i - Y^i) = \prod_{i=1}^{d} (X - \alpha_i Y) + A(X,Y)$$

where $A(X,Y) \in K[X,Y]$ and $\deg(A) \leq d-1$.
Hence, since $\prod_{i=1}^{d} (X - \alpha_i Y)$ is homogeneous of degree d, we have

$$X^d - Y^d = \prod_{i=1}^{d} (X - \alpha_i Y).$$

Substituting $Y = 1$, we get $X^d - 1 = \prod_{i=1}^{d} (X - \alpha_i)$ and obtain our result. □

Corollary 4.3. *There are no special polynomials of degree greater than* 2 *with rational coefficients.*

Proposition 4.4. *Let* $f(X) \in (\mathbb{F}_q[T])[X]$ *be monic and of degree* d *w.r.t.* X*. If* f *is special, absolutely irreducible and separable. Then*

$$\deg L_f(n) = (d-1)nq^n + O(q^n).$$

Proof. Since f is *special*, by claim 4.2 we assume

$$f(X) - f(Y) = \prod_{i=1}^{d}(X - a_iY + b_i)$$

where $b_i \in \mathbb{F}_q[T]$ and $a_i \in \mathbb{F}_q^\times$.
Let $P \in \mathbb{F}_q[T]$ prime, and $Q_1, Q_2 \in M_n$ distinct, so

$$\begin{aligned} P \mid f(Q_1), f(Q_2) &\implies P \mid f(Q_1) - f(Q_2) = \prod_{i=1}^{d}(Q_1 + a_iQ_2 + b_i) \\ &\implies \exists i \text{ s.t. } P \mid (Q_1 + a_iQ_2 + b_i) \\ &\implies \exists i \text{ s.t.} \deg P \leq \max\{n\,,\, \deg b_i\}. \end{aligned}$$

Hence, for sufficiently large n (i.e. $n > \max_i \deg b_i$), if $\deg P > n$, then $\alpha_P(n) = \beta_P(n)$. Thus, $S_f(n) \ll 1$ and by corollary 2.7 we are done. □

So now our goal is to classify these *special* polynomials, and according to claim 4.2 we will split our study to two cases, whether the degree divides the characteristic or not.

4.1. **First case:** $\gcd(d,p) = 1$**.**

Example: Let $f(X) = X^3 + T \in (\mathbb{F}_q[T])[X]$, for some $q \equiv 1 \mod 3$.
Here we have a primitive third root of unity, namely $\zeta \in \mathbb{F}_q$, $\zeta^3 = 1$, and with that in hand:

$$f(X) - f(Y) = (X-Y)(X^2 + XY + Y^2) = (X-Y)(X - \zeta Y)(X - \zeta^2 Y)$$

so f is *special*, absolutely irreducible and separable. Hence, by proposition 4.4 we get

$$\deg L_f(n) = 2nq^n + O(q^n)$$

To generalize this example, note that for $X^d - H$ to be irreducible is equivalent to requiring that if $4 \nmid d$, that for any prime divisor $\ell \mid d$, we have H is not an ℓ-th power in $\mathbb{F}_q(t)$, and in addition if $4 \mid d$ then $H \notin -4(\mathbb{F}_q(t))^4$, see [6, Theorem 14.1.4].

Claim 4.5. *Let* $f(X) = X^d - H$*, where* $2 \leq d$ *and* $H \in \mathbb{F}_q[T]$*, monic with* $\deg H \geq 1$*. Further assume that:*

(1) $\forall p \mid d$ *prime,* $H \notin (\mathbb{F}_q[T])^p$
(2) $q \equiv 1 \mod d$

Then,

$$\deg L_f(n) = (d-1)nq^n + O(q^n)$$

Proof. By proposition 4.4, we need to verify that f is absolutely irreducible, separable and *special*. Firstly, separablity of f follows easily from $q \equiv 1 \mod d$, and to see that f is absolutely irreducible we'll use the preceding theorem, noting that in this case the second condition of the theorem is contained in the first one, since H

is monic. Let $\prod_{i=1}^{k} P_i^{n_i} = H$ be the prime decomposition of H, and denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$. Take $p \mid d$ prime, then the first assumption yields

$$H \notin (\mathbb{F}_q[T])^p \iff p \nmid \gcd(n_1, \ldots, n_k)$$

and since $\mathbb{F}_q$ is a perfect field, for each i all the roots of P_i are distinct, moreover $\forall i \neq j$ P_i and P_j have no roots in common, therefore

$$H \notin (\overline{\mathbb{F}}_q[T])^p \iff p \nmid \gcd(n_1, \ldots, n_k)$$

whence, f is absolutely irreducible and separable.

Secondly, from the second assumption $d \mid q-1$, and we know $a^{q-1} = 1$, $\forall a \in F_q^\times$ ($\mid \mathbb{F}_q^\times \mid = q-1$). Hence, since $\mathbb{F}_q^\times$ is a cyclic group, $\mathbb{F}_q$ contains all d-th roots of unity, i.e. $\exists a_1, \ldots, a_d \in \mathbb{F}_q$ s.t.

$$x^d - 1 = \prod_{i=1}^{d} (x - a_i), \quad \text{in } \mathbb{F}_q[x] \tag{3}$$

substituting $x = \frac{X}{Y}$ and multiplying by Y^d in (3) we get

$$X^d - Y^d = \prod_{i=1}^{d} (X - a_i Y), \quad \text{now in } (\mathbb{F}_q[T])[X, Y]$$

Whence, f is special and we obtain our result.

□

Corollary 4.6. *Let $f(X) = (X+A)^d - C \in (\mathbb{F}_q[T])[X]$, where $q \equiv 1 \mod d$, $0 \neq A, C \in \mathbb{F}_q[T]$, and $\forall p \mid d$ prime, $C \notin (\mathbb{F}_q[T])^p$ and C is monic. Then we have*

$$\deg L_f(n) = (d-1)q^n n + O(q^n), \qquad \textit{as } n \to \infty$$

Proof. From the assumptions on C note that $f(X - A) = X^d - C$ is absolutely irreducible, hence so is f and separability follows immediately. To see that f is special, note that from $q \equiv 1 \mod d$ their exists $\zeta \in \mathbb{F}_q$ a primitive d-th root of unity, so

$$X^d - Y^d = \prod_{i=1}^{d} (X - \zeta^i Y)$$

and after shifting $(X, Y) \mapsto (X + A, Y + A)$, we get

$$\begin{aligned} f(X) - f(Y) &= (X+A)^d - (Y+A)^d \\ &= \prod_{i=1}^{d} (X + A - \zeta^i (Y + A)) \\ &= \prod_{i=1}^{d} [X - \zeta^i Y + (1 - \zeta^i) A]. \end{aligned}$$

Thus f is special, and by proposition 4.4 we obtain our result. □

Proposition 4.7. *Let $f(X) = X^d + A_{d-1}X^{d-1} + \ldots + A_1 X + A_0 \in (\mathbb{F}_q[T])[X]$ be a special polynomial, of degree $d \geq 3$ where $\gcd(q, d) = 1$. Then $\exists A, C \in \mathbb{F}_q[T]$ s.t.*

$$f(X) = (X + A)^d + C.$$

Proof. Assume WLOG that $A_{d-1} = 0$, otherwise consider $\tilde{f}(X) = f(X - \frac{1}{d} A_{d-1})$ which is also special (we assume that $\gcd(d, p) = 1$ so that d is invertible in $\mathbb{F}_q$)

and its $(d-1)$-coefficient is zero.
So, since f is special, we write

$$f(X) - f(Y) = (X - Y)\prod_{i=1}^{d-1}(X - \zeta_d^i Y + b_i)$$

where $\zeta_d \in \mathbb{F}_q$ is a primitive d-th root of unity (this is a necessary condition by claim 4.2), and $b_i \in \mathbb{F}_q[T]\,\forall i$.
Hence, we have

$$\frac{f(X) - f(Y)}{X - Y} = \prod_{i=1}^{d-1}(X - \zeta_d^i Y + b_i) \tag{4}$$

on the left hand side the degree $(d-2)$-homogeneous part vanishes, i.e.

$$A_{d-1}\frac{X^{d-1} - Y^{d-1}}{X - Y} = 0.$$

Hence comparing the $(d-2)$-homogeneous part of both sides in (4) yields

$$0 = \sum_{i=1}^{d-1} b_i \prod_{\substack{j=1 \\ j\neq i}}^{d-1}(X - \zeta_d^j Y)$$

Take any $1 \leq i_0 \leq d-1$, and substitute $X = \zeta_d^{i_0}, Y = 1$ to get

$$0 = b_{i_0}\prod_{\substack{j=1 \\ j\neq i_0}}(\zeta_d^{i_0} - \zeta_d^j)$$

since all the terms in the sum vanish except the i_0- term.
Thus $b_i = 0$ for any $1 \leq i \leq d-1$, and therefore

$$f(X) - f(Y) = (X - Y)\prod_{i=1}^{d-1}(X - \zeta_d^i Y) = X^d - Y^d$$

so $f(X) = X^d + A_0$, and we obtain our result. □

Thus, we have classified all special polynomials, with degree co-prime to the characteristic of $\mathbb{F}_q$.

4.2. Second case: $\gcd(d, p) = p$.

Example: Take $q = 3^m$ and consider $f(X) = X^3 + 2X + T \in (\mathbb{F}_{3^m}[T])[X]$. Note that for any $Q \in M_n$

$$f(Q) = Q^3 + 2Q + T = 0 \iff Q(Q^2 + 2) = -T$$

but the degree of the left hand side is divisible by three, so this cannot happen. Thus, f is absolutely irreducible and separable. Moreover

$$\begin{aligned} f(X) - f(Y) &= X^3 - Y^3 + 2(X - Y) \\ &= (X - Y)(X^2 + XY + Y^2 + 2) \\ &= (X - Y)(X - Y + 1)(X - Y + 2) \end{aligned}$$

Therefore, f is also special. So, in this case conjecture 1.1 holds .

Proposition 4.8. *Let $f \in (\mathbb{F}_q[T])[X]$ be of degree p^l (w.r.t. X), where $q = p^m$ and $m, l \geq 1$. Then, f is a special polynomial if and only if the following conditions hold:*

(1) f is of the form

$$f(X) = X^{p^l} + \sum_{k=0}^{l-1} A_{p^k} X^{p^k} + A_0$$

meaning all the d-th coefficients of f vanish when $d \neq 0$ and d is not a power of p.

(2) $f(X) - f(0)$ factors into a product of linear terms in $(\mathbb{F}_q[T])[X]$.

Proof. Let $f(X) = X^{p^l} + \sum_{k=0}^{p^l-1} A_k X^k$. Assume that f is special, then by claim 4.2 (noting that by the Frobenius endomorphism $X^{p^l} - 1 = (X-1)^{p^l}$) we have

$$f(X) - f(Y) = \prod_{k=1}^{p^l} (X - Y + B_k) \quad \forall k \; B_k \in \mathbb{F}_q[T]$$

Take $0 < d < p^l$, then by comparing the d-th homogeneous part in both sides of the above we get

$$\begin{aligned} A_d(X^d - Y^d) &= \sum_{1 \leq k_1 < \ldots < k_{p^l-d} \leq p^l} (X-Y)^d \prod_{i=1}^{p^l-d} B_{k_i} \\ &= (X-Y)^d \sum_{1 \leq k_1 < \ldots < k_{p^l-d} \leq p^l} \prod_{i=1}^{p^l-d} B_{k_i}. \end{aligned}$$

Thus, since $X^d - Y^d = (X-Y)^d$ if and only if d is a p-th power, we conclude that for $d > 0$ which is not a power of p we get

$$A_d = \sum_{1 \leq k_1 < \ldots < k_{p^l-d} \leq p^l} \prod_{i=1}^{p^l-d} B_{k_i} = 0$$

which is condition 1. So now

$$f(X) = X^{p^l} + \sum_{k=0}^{l-1} A_{p^k} X^{p^k} + A_0.$$

Hence, by the Frobenius endomorphism and the assumption that f is special, we have

$$\begin{aligned} f(X) - f(Y) &= (X-Y)^{p^l} + \sum_{k=0}^{l-1} A_{p^k} (X-Y)^{p^k} + A_0 \\ &= \prod_{k=1}^{p^l} (X - Y + B_k). \end{aligned}$$

Substitute $X - Y = Z$ to obtain

$$f(Z) - f(0) = Z^{p^l} + \sum_{k=0}^{l-1} A_{p^k} Z^{p^k} = \prod_{k=1}^{p^l} (Z + B_k)$$

which is condition 1.
Now, for the other direction assume that both conditions hold for f. Then we have

$$f(Z) - f(0) = Z^{p^l} + \sum_{k=0}^{l-1} A_{p^k} Z^{p^k} = \prod_{k=1}^{p^l} (Z + B_k)$$

where $\forall k$, $B_K \in \mathbb{F}_q[T]$. hence by substituting $Z = X - Y$ and using the Frobenius endomorphism, we get our result. □

Remark. This proposition reduces the classification of special polynomials of degree p^l in $\mathbb{F}_q$ to the classification of polynomials of degree $p^l - 1$ that factor into a product of linear terms. For small degrees we can get conditions on the coefficients due to Vieta's equations, as the next claim suggests.

Claim 4.9. *Take $q = 3^m$ for some $0 < m \in \mathbb{Z}$. Let $f \in (\mathbb{F}_q[t])[X]$ with $\deg_X f = 9$. Then f is special if and only if*

$$f(X) = X^9 + (C_1^2 + C_2^2)(C_1^4 + C_2^4)X^3 + C_1^2 C_2^2 (C_1^2 - C_2^2)^2 X + C$$

for any $C_1, C_2, C \in \mathbb{F}_q[T]$.

Proof. By proposition 4.8, f is special if and only if f is of the form

$$f(X) = X^9 + AX^3 + BX + C$$

and $\exists B_k \in \mathbb{F}_q[T]$, $k = 1, \ldots 8$ s.t.

$$X^9 + AX^3 + BX = X[(X^2)^4 + AX^2 + B] = X \prod_{k=1}^{8} (X - B_k)$$

Since all monomials (in the brackets) are of even degree this is true if and only if

$$Y^4 + AY + B = \prod_{k=1}^{4} (Y - A_k)$$

where $A_1, A_2, A_3, A_4 \in \mathbb{F}_q[T]$ are squares.
So, by Vieta's equations we need to solve the following:

(1) $\sum\limits_{1 \le i \le 4} A_i = 0$

(2) $\sum\limits_{1 \le i < j \le 4} A_i A_j = 0.$

Squaring the first equation and subtracting twice the second one we get

(1) $A_4 = -(A_1 + A_2 + A_3)$

(2) $\sum\limits_{1 \le i \le 4} A_i^2 = 0.$

Inserting equation (1) into (2) we get a quadratic equation in A_3 with parameters A_1, A_2

$$\begin{aligned} & 0 = A_1^2 + A_2^2 + A_3^2 + (A_1 + A_2 + A_3)^2 \\ \iff & 0 = 2A^3 + 2(A_1 + A_2)A_3 + A_1^2 + A_2^2 + (A_1 + A_2)^2 \\ \iff & 0 = 2A^3 + 2(A_1 + A_2)A_3 + 2A_1^2 + 2A_2^2 + 2A_1 A_2. \end{aligned}$$

Noting that $2 \equiv -1$ since the characteristic is 3, the solution is:

$$\begin{aligned} A_3 &= \frac{A_1 + A_2 \pm \sqrt{(A_1 + A_2)^2 - 2(2A_1^2 + 2A_2^2 + 2A_1 A_2)}}{4} \\ &= A_1 + A_2 \pm \sqrt{A_1^2 + 2A_1 A_2 + A_2^2 - A_1^2 - A_2^2 - A_1 A_2} \\ &= A_1 + A_2 \pm \sqrt{A_1 A_2} = \left(\sqrt{A_1} \pm \sqrt{A_2}\right)^2 . \end{aligned}$$

If $A_3 = \left(\sqrt{A_1} + \sqrt{A_2}\right)^2$, then by the first equation we get:

$$\begin{aligned} A_4 &= -A_1 - A_2 - A_1 - A_2 - \sqrt{A_1 A_2} = A_1 + A_2 - \sqrt{A_1 A_2} \\ &= \left(\sqrt{A_1} - \sqrt{A_2}\right)^2 \end{aligned}$$

and since A_1, A_2 are squares, Let $C_1^2 = A_1, C_2^2 = A_2$, then $A_3 = (C_1 + C_2)^2, A_4 = (C_1 - C_2)^2$.
Now by Vieta's equations we have:

$$\begin{aligned} B &= A_1A_2A_3A_4 = C_1^2C_2^2(C_1+C_2)^2(C_1-C_2)^2 \\ &= C_1^2C_2^2(C_1^2-C_2^2)^2 \end{aligned}$$

and

$$\begin{aligned} A &= A_1A_2A_3 + A_1A_2A_4 + A_1A_3A_4 + A_2A_3A_4 = \\ &= C_1^2C_2^2(C_1+C_2)^2 + C_1^2C_2^2(C_1-C_2)^2 + C_1^2(C_1^2-C_2^2)^2 + C_2^2(C_1^2-C_2^2)^2 \\ &= C_1^2C_2^2[(C_1+C_2)^2 + (C_1-C_2)^2] + (C_1^2-C_2^2)^2(C_1^2+C_2^2) \\ &= C_1^2C_2^2[2C_1^2+2C_2^2] + (C_1^2-C_2^2)^2(C_1^2+C_2^2) \\ &= (C_1^2+C_2^2)[2C_1^2C_2^2 + (C_1^2-C_2^2)^2] \\ &= (C_1^2+C_2^2)[C_1^4+C_2^4]. \end{aligned}$$

So, we have

$$f(X) = X^9 + (C_1^2+C_2^2)(C_1^4+C_2^4)X^3 + C_1^2C_2^2(C_1^2-C_2^2)^2X + C.$$

□

Remark. Note that f is absolutely irreducible with a correct choice of the constant C, and so it is also separable if and only if $C_1, C_2 \neq 0$ and $C_1 = \pm C_2^2$. In which case conjecture 1.1 holds.

Proposition 4.10. *Let p be a prime integer, and take $q = p^m$, $m \geq 1$. Then, for $l \geq 0$ s.t. $l \mid m$, the polynomial*

$$f(X) = X^{p^l} - A^{p^l-1}X + C$$

where $A, C \in \mathbb{F}_q[T]$, is special.

Proof. We need to verify both conditions of proposition 4.8. Condition 1 is trivial and to see condition 2, note that From $l \mid m$ we have $p^l - 1 \mid p^m - 1$, so we can take $\zeta \in \mathbb{F}_q$ a primitive root of unity of order $p^l - 1$. Then by the Frobenius endomorphism we have

$$\begin{aligned} f(X) - f(0) &= X^{p^l} - A^{p^l-1}X \\ &= X(X^{p^l-1} - A^{p^l-1}) \\ &= X\prod_{i=1}^{p^l-1}(X - \zeta^i A) \end{aligned}$$

so f is special. □

Proposition 4.11. *Let $g(X) \in (\mathbb{F}_q[T])[X]$ be a special polynomial s.t.* $\deg_X g = p^l, q = p^m$. *Then, for any $A, C \in \mathbb{F}_q[T]$, and $k \geq 1$ s.t. $p \equiv 1 \mod k$, the polynomial*

$$f(X) = [g(X+A) - g(0)]^k + C$$

is special over $\mathbb{F}_q[T]$.

Proof. Let $A, C \in \mathbb{F}_q[T]$, assume WLOG that $g(0) = A = 0$ (otherwise consider $\tilde{f}(X) = f(X - A)$, and note that if $\tilde{f}$ is special then so is f). By Proposition 4.8 we write

$$g(X) = X^{p^l} + \sum_{i=0}^{l-1} g_i X^{p^i}$$

Let $\zeta_k \in \mathbb{F}_q$ be a primitive k-th root of unity. From $k \mid p - 1$ we have $\zeta_k g(X) = g(\zeta_k X)$, since $\zeta_k^{p^i} = \zeta_k \; \forall i \geq 0$. Therefore

$$\begin{aligned} f(X) - f(Y) &= [g(X)]^k - [g(Y)]^k \\ &= \prod_{i=1}^{k} \left(g(X) - \zeta_k^i g(Y) \right) \\ &= \prod_{i=1}^{k} \left(g(X) - g(\zeta_k^i Y) \right) \end{aligned}$$

and since g is special the result follows. □

To sum up what we found in the last section we have the following thorem:

Theorem 4.12. *For the following polynomials in $(\mathbb{F}_q[T])[X]$ conjecture 1.1 holds:*

(1) $(X + A)^d + C$, when $q \equiv 1 \mod d$.

(2) $(X^{p^l} - A^{p^l - 1} X)^k + C$, when p is prime, $q = p^m$ and $l, m, k \in \mathbb{N}$ satisfy $l \mid m$, $k \mid p^{l-1}$.

where $0 \neq A, C \in \mathbb{F}_q[T]$, and $\exists P \in \mathbb{F}_q[T]$ prime s.t. $P \mid A, C$, but $P^2 \nmid C$.

References

[1] L. Bary-Soroker, O. Gorodetsky, T. Karidi and W. Sawin. Chebotarev density theorem in short intervals for extensions of $\mathbb{F}_q(T)$. Trans. Amer. Math. Soc. 373 (2020), 597-628.

[2] P. Bateman, J. Kalb and A. Stenger. Problem 10797: A limit involving least common multiples. Am. Math. Mon. 109 (2002), no. 4, 393–394.

[3] J. Cilleruelo. The least common multiple of a quadratic sequence. Compos. Math., 147(4):1129–1150, 2011.

[4] S. Hong, G. Qian and Q. Tan, The least common multiple of sequence of product of linear polynomials. Acta Math. Hungar. 135 (2012), no.12, 160–167.

[5] J. Maynard and Z. Rudnick. A lower bound on the least common multiple of polynomial sequences. *Preprint*, arXiv:1910.13218. To appear in the Rivista di Matematica della Università di Parma.

[6] S. Roman. Field theory. Second edition. Graduate Texts in Mathematics, 158. Springer, New York, 2006.

[7] Rosen, Michael I. Number Theory in Function Fields. Graduate texts in mathematics, 210. Springer, New York, 2002.

[8] Rotman, Joseph j. An introduction to the theory of groups. Graduate texts in mathematics, 148. Springer, New York, 1995.

[9] Z. Rudnick and S. Zehavi. On Cilleruelo's conjecture for the least common multiple of polynomial sequences. *Preprint*, arXiv:1902.01102. To appear in Revista Matematica Iberoamericana.

[10] A. Sah. An improved bound on the least common multiple of polynomial sequences. Journal de Théorie des Nombres de Bordeaux, Tome 32 (2020) no. 3, pp. 891-899.

אבסטרקט

סילרואלו שיער שלכל פולינום אי פריק f עם מקדמים שלמים, כך שמעלתו גדולה ממש מאחד, הכפולה המשותפת הקטנה ביותר של הערכים של f ב־N המספרים הראשונים מקיימת $\log lcm(f(1),\dots,f(N)) \sim (\deg f-1)N\log N$, כאשר N שואף לאינסוף. הוא הוכיח זאת רק עבור המקרה $\deg f=2$. לא ידועה אף דוגמה במעלה גבוהה יותר. אנו חוקרים את האנלוגיה של השערה זו מעל שדות פונקציות, כאשר מחליפים את המספרים השלמים בחוג הפולינומים מעל שדה סופי. תחת ההגדרות הללו אנו מסוגלים למצוא מקרים של ההשערה במעלות גבוהות. הדוגמאות הללו כולן פולינומים "מיוחדים" $f(X)$, שלהם התכונה שהפולינום מרובה המשתנים $f(X)-f(Y)$ מתפרק לגורמים לינארים בשדה הבסיס.

הפקולטה למדעים
מדויקים ע"ש ריימונד
ובברלי סאקלר
אוניברסיטת תל אביב

בעיית הכפולה המשותפת הקטנה ביותר מעל שדות פונקציות

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" (M.Sc.) באוניברסיטת תל אביב,
בית הספר למדעי המתמטיקה

על ידי
איתי לאומי

העבודה הוכנה בהדרכתו של
פרופסור זאב רודניק

ניסן, תשפ"א

הפקולטה למדעים
מדויקים ע"ש ריימונד
ובברלי סאקלר
אוניברסיטת תל אביב

בעיית הכפולה המשותפת הקטנה ביותר מעל שדות פונקציות

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" (M.Sc.) באוניברסיטת תל אביב,
בית הספר למדעי המתמטיקה

על ידי
איתי לאומי

העובדה הוכנה בהדרכתו של
פרופסור זאב רודניק

ניסן, תשפ"א