GUY LANDO

ABSTRACT. Let $f \in \mathbb{F}_q[t]$ be a square-free polynomial. In this paper we evaluate the density of primes $P \in \mathbb{F}_q[t]$, deg $P = n$, such that $f(P)$ is square-free, in the limit $n \to \infty$, $q$ fixed.

Over the integers the analogous result is only known for $f$ of degree at most 3.

CONTENTS

1. Introduction 1
   1.1. Statement of results 1
   1.2. Plan of the proof 3
2. Estimating the main term 5
3. Bounding the remainder 9
4. Proof of Proposition 3 10
5. Proof of Proposition 4 10
   5.1. First Part 10
   5.2. Second Part 11
   5.3. End of proof of Proposition 4 13
6. Remarks 18
   6.1. Sketch of proof of Theorem 2 18
   6.2. Positivity of $c_{f,2}$ 18
   6.3. Final comments 19
References 20

1. INTRODUCTION

1.1. Statement of results. In this paper we study a function field version of a classical problem concerning square-free values of polynomials evaluated at primes. Given a polynomial $f \in \mathbb{Z}[x]$ with integer coefficients, it is conjectured that there are infinitely many primes $p$ for which $f(p)$ is square-free, provided that $f$ satisfies an obvious congruence condition. This conjecture is only known to be true for polynomials of degree at most three. Moreover,
it is believed that the set $\mathcal{P}_{f,2}$ of primes $p$ for which $f(p)$ is square-free has positive density, namely if
\begin{equation}
\mathcal{P}_{f,2}(x) = \{ p \leq x \text{ prime : } f(p) \text{ is square-free} \}
\end{equation}
then

**Conjecture 1.** Assume that for each prime $p$ there is at least one integer $n_p$ for which $f(n_p)$ is not divisible by $p^2$. Then
\begin{equation}
|\mathcal{P}_{f,2}(x)| \sim c_{f,2}\pi(x), \quad x \to \infty,
\end{equation}
where $\pi(x)$ denotes the number of prime integers not larger than $x$, and the positive density $c_{f,2}$ is given by
\begin{equation}
c_{f,2} = \prod_p \left( 1 - \frac{\rho_f(p^2)}{p^2 - p} \right),
\end{equation}
where $\rho_f(d)$ is the number of solutions of $f(x) = 0 \pmod d$ in invertible residues modulo $d$.

More generally, one can ask for the density of the set $\mathcal{P}_{f,k}$ of primes $p$ for which $f(p)$ is $k$-free (meaning $f(p)$ is not divisible by any $k$-th power). The conjectured density is
\begin{equation}
c_{f,k} = \prod_p \left( 1 - \frac{\rho_f(p^k)}{\phi(p^k)} \right).
\end{equation}

Uchiyama [15] proved this conjectured density for $k = \deg f$ by a method that also handles the case $k > \deg f$. The case $k = \deg f - 1$ was singled out by Erdős, who conjectured that the set contains infinitely many primes, and following the works of Hooley [4], Nair [5], [6] Heath-Brown [2], Helfgott [3], Browning [1] and Reuss [10] the quantitative conjecture for $k = \deg f - 1$ is completely solved. The square-free case ($k = 2$) is currently open for $\deg f > 3$. Pasten [7] showed that conjecture [1] follows from the ABC conjecture for number fields.

We turn to the function field version. Let $\mathbb{F}_q$ be a finite field of $q$ elements, where $q = p^k$ is a prime power, and $\mathbb{F}_q[t]$ the polynomial ring. We denote by $M_n(q)$ the set of monic polynomials of degree $n$. We define the absolute value of $a \in \mathbb{F}_q[t]$ to be $|a| = q^\deg a$. We denote by $\pi_q(n)$ the set of monic irreducible polynomials of degree $n$, so that $|\pi_q(n)| = q^n + O \left( \frac{q^{n/2}}{n} \right)$.

Let $f(x) \in \mathbb{F}_q[t][x]$. We denote by $\mathcal{P}(n) = \mathcal{P}_{f,2}(n)$ the set of monic irreducible polynomials $P(t) \in M_n(q)$ (monic irreducible polynomials will be called primes) such that $f(P)$ is square-free [1]. We prove an analogue of Conjecture [1] for square-free values, also establishing asymptotic bounds on the convergence rate.

---

A polynomial $a(t) \in \mathbb{F}_q[t]$ is called square-free if there is no $P \in \mathbb{F}_q[t]$ such that $\deg P > 0$ and $P^2 \mid a$. 

---
Define the content of \( f(x) \in \mathbb{F}_q[t][x] \) to be the greatest common divisor of its coefficients, which is an element of \( \mathbb{F}_q[t] \).

Theorem 1. Assume \( f \in \mathbb{F}_q[t][x] \) is square-free and that its content is 1. Then
\[
\left| \frac{\mathcal{P}(n)}{\pi_q(n)} \right| = c_{f,2} + O_{f,q} \left( \frac{1}{\log_q n} \right) \quad \text{as } n \to \infty,
\]
with
\[
c_{f,2} = \prod_P \left( 1 - \frac{\rho_f(P^2)}{|P|^2 - |P|} \right),
\]
where the product runs over the prime polynomials \( P \), and for any polynomial \( D \in \mathbb{F}_q[t] \), \( \rho_f(D) = |\{ C \mod D, \gcd(D,C) = 1, f(C) = 0 \mod D \}| \). The implied constant in the error term \( O_{f,q} \left( \frac{1}{\log_q n} \right) \) depends only on \( f \) and the finite field size \( q \).

Note that the constant \( c_{f,2} \) is positive if and only if for all primes \( P \), there is some \( C \mod P^2 \), \( C \) coprime to \( P \), such that \( f(C) \neq 0 \mod P^2 \). See Section 6.2 for a discussion.

1.2. Plan of the proof. Fix \( M \in \mathbb{N} \) which will be chosen later, and let
\[
\mathcal{P}'(n, M) = \{ a \in \pi_q(n) : P^2 \nmid f(a), \forall P \text{ prime with } \deg P < M \}
\]
and
\[
\mathcal{P}''(n, M) = \{ a \in \pi_q(n) : \exists P, \deg P \geq M, \text{ s.t. } P^2 \mid f(a) \}
\]
Then clearly
\[
\mathcal{P}(n) \subset \mathcal{P}'(n, M) \subset \mathcal{P}(n) \cup \mathcal{P}''(n, M),
\]
so that
\[
|\mathcal{P}(n)| - |\mathcal{P}''(n, M)| \leq |\mathcal{P}(n)| \leq |\mathcal{P}'(n, M)|.
\]
Thus it suffices to give an asymptotic estimate for \( |\mathcal{P}'(n, M)| \) (the "main term"), which is easy if \( M \) is small, and an upper bound for \( |\mathcal{P}''(n, M)| \) (the "error term"). We will show in Proposition 1 that
\[
|\mathcal{P}'(n, M)| = c_{f,2} \frac{q^n}{n} + O \left( \frac{q^n}{nMq^M} \right) + O \left( \frac{q^{n/2} + q^{M+M}}{n} \right),
\]
and in Proposition 2 that
\[
|\mathcal{P}''(n, M)| \leq \frac{2q^n \deg f}{Mq^M} + O \left( \frac{q^{n+1}}{n^p} \right).
\]
Choosing \( M = \log_q \frac{n}{\log n} \) in (1.11) and (1.12) gives
\[
|\mathcal{P}'(n, M)| = c_{f,2} \frac{q^n}{n} + O \left( \frac{q^n}{n^2 \log_q n} \right).
\]
and
\[ |P''(n, M)| \ll \frac{q^n}{n \log_q n}, \]
which together yield
\begin{equation}
(1.13) \quad |P_{f,2}(n)| = c_{f,2}|\pi_q(n)| + O\left(\frac{q^n}{n \log_q n}\right).
\end{equation}
This proves Theorem 1.

The proof of (1.11) is carried out using a sieve method and an estimate on \(\pi_q(n; Q, A)\), which is the number of primes in arithmetic progressions.

The crucial bound (1.12) for the contribution of large primes uses ideas of Ramsay [9] and Poonen [8], formulated in their work on the related question of square-free values taken at arbitrary (non-prime) polynomials, which we will explain in the proof of (1.12).

A similar argument gives analogous results for \(k\)-free values \((k \geq 2)\). A polynomial \(a(t) \in R[Y]\) in variable \(Y\) over a ring \(R\) is called \(k\)-free if there is no \(P \in R[Y]\) such that \(\deg P > 0\) and \(P^k|a\). We denote by \(P_{f,k}(n)\) the set of primes \(P\) of degree \(n\) for which \(f(P)\) is \(k\)-free, and we define
\begin{equation}
(1.14) \quad c_{f,k} = \prod_P \left(1 - \frac{\rho_f(P^k)}{\phi(P^k)}\right),
\end{equation}
where the product runs over the prime polynomials \(P\) (where \(\phi(h)\) is the Euler totient function for \(\mathbb{F}_q[t]\)). Then

**Theorem 2.** Assume \(f(x) \in \mathbb{F}_q[t][x]\) is \(k\)-free and that its content is 1. Then
\begin{equation}
(1.15) \quad \frac{|P_{f,k}(n)|}{|\pi_q(n)|} = c_{f,k} + O_{f,q}\left(\frac{1}{n^{k-2} \log_q n}\right) \quad \text{as } n \to \infty
\end{equation}

As a final comment, we point out that we have dealt here with the limit of large degree \(n\) and fixed finite field size \(q\). One can also ask an analogous question for the limit of \(q \to \infty\) and \(n\) fixed. In this case, it follows from the recent work of Rudnick [13] that \(f(P)\) is square-free with probability 1, that is
\begin{equation}
(1.16) \quad \lim_{q \to \infty} \frac{|P_{f,2}(n)|}{|\pi_q(n)|} = 1.
\end{equation}
This is because in [13] it is shown that with probability 1 as \(q \to \infty\), for an arbitrary polynomial \(a \in M_n\), \(f(a)\) is square-free. Since the primes have positive density (namely \(1/n\)) in the set of all monic polynomials of degree \(n\), the result follows.
2. Estimating the main term

We now turn back to the proof of Theorem 1. We fixed $M \in \mathbb{N}$ and defined
\[
P'(n, M) = \{ a \in \pi_q(n) : P^2 \nmid f(a), \forall P \text{ prime with } \deg P < M \},
\]
\[
P''(n, M) = \{ a \in \pi_q(n) : \exists P, \deg P \geq M, \text{ s.t. } P^2 \mid f(a) \}.
\]
We wish to prove that for $0 \ll M \leq \frac{2}{Q}$ it holds that
\[
|P'(n, M)| = c f\frac{q^n}{n} + O\left(\frac{q^n}{nMq^M}\right) + O\left(\frac{q^\frac{n}{2}q^2\log q^M}{n}\right)
\]
and
\[
|P''(n, M)| \leq \frac{2q^n\deg f}{Mq^M} + O\left(\frac{q^n}{n}\right).
\]

The rest of the paper will use the following notation:

- $n, N$ natural numbers
- For $a \in \mathbb{F}_q[t]^N$, $a_i$ is the value of the $i$ coordinate of $a$
- $P$ is a prime in $\mathbb{F}_q[t]$
- $f(x) \in \mathbb{F}_q[t][x]$ is a square-free polynomial and its content is 1

We will now prove:

**Proposition 1.** For $0 \ll M \leq n$,
\[
|P'(n, M)| = c f\frac{q^n}{n} + O\left(\frac{q^n}{nMq^M}\right) + O\left(\frac{q^\frac{n}{2}q^2\log q^M}{n}\right).
\]

The proof will use a standard sieve argument. In the calculation, we need an estimate for the size of the set of primes of degree $n$ in an arithmetic progression: $\pi_q(n; Q, A) = \{ P \in \pi_q(n) : p \equiv A \pmod{Q} \}$. We will use the Prime Polynomial Theorem in arithmetic progressions, with a remainder term given by the Riemann Hypothesis for curves over a finite field (Weil’s Theorem):

For $Q, A \in \mathbb{F}_q[t]$ with $\gcd(Q, A) = 1$,
\[
(2.1) \quad |\pi_q(n; Q, A)| = \frac{q^n}{n\phi(Q)} + O\left(\frac{q^n}{n \deg Q}\right).
\]

**Proof of Proposition 1.** Denote $w = |\{ P : \deg P < M \}|$ and enumerate $\{ P : \deg P < M \} = \{ P_j : 1 \leq j \leq w \}$. Define:

- $B = \{(d_1, \ldots, d_w) : \forall j, 1 \leq j \leq w, d_j \in \mathbb{F}_q[t]/P_j^2, f(d_j) \not\equiv 0 \pmod{P_j^2}\}$,
- $C = \{(d_1, \ldots, d_w) \in B : \forall j, 1 \leq j \leq w, \gcd(P_j, d_j) = 1\}$.

Now, for $a \in \pi_q(n)$, if $P_j|d_j$ for some $1 \leq j \leq w$, then from $P_j|(a - d_j)$ it follows that $P_j|a$, but both are prime, thus $P_j = a$. Since $\deg a = n$ and $\deg P < M$, it follows that for $n \geq M$, if $P_j|d_j$, then $\{ a \in \pi_q(n) : \forall 1 \leq j \leq w, a \equiv d_j \pmod{P_j^2} \} = \emptyset$. 


In addition, according to the Chinese Remainder Theorem, for every set $(d_1, \ldots, d_w)$ such that $d_j \in \mathbb{F}_q[t]/P^2$, $\forall 1 \leq j \leq w$, there is a unique class $d_{d_1, \ldots, d_w}$ modulo $\prod_{\deg P < M} P^2$ such that $d_{d_1, \ldots, d_w} \equiv d_j \pmod{P^2}$, $\forall 1 \leq j \leq w$.

Thus for $M \leq n$ it holds that

\[(2.2)\quad |P'(n, M)| = |\{a \in \pi_q(n) : \forall \deg P < M, P^2 \nmid f(a)\}| \]

\[= \sum_{(d_1, \ldots, d_w) \in B} |\{a \in \pi_q(n) : \forall j, 1 \leq j \leq w, a \equiv d_j \pmod{P^2}\}| \]

\[= \sum_{(d_1, \ldots, d_w) \in C} \left|\{a \in \pi_q(n) : \forall j, 1 \leq j \leq w, a \equiv d_j \pmod{P^2}\}\right| \]

\[= \sum_{(d_1, \ldots, d_w) \in C} \left|\{a \in \pi_q(n) : a \equiv d_{d_1, \ldots, d_w} \pmod{\prod_{\deg P < M} P^2}\}\right| \]

Now, the “Explicit Formula” $\sum_{d \mid n} d|\pi_q(d)| = q^n$ (see Proposition 2.1 in [12] for a proof) gives $i|\pi_q(i)| \leq q^i$, which in turn can be used to get

\[(2.3)\quad \deg \prod_{\deg P < M} P^2 = \sum_{\deg P < M} 2 \deg P = 2 \sum_{i=1}^{M} i|\pi_q(i)| \leq 2 \sum_{i=1}^{M} q^i = 2 \left(q^M + \frac{q^M - 1}{q - 1} - 1\right) \leq 4 q^M.\]

Since $\gcd(d_{d_1, \ldots, d_w}, \prod_{\deg P < M} P^2) = 1$, we can use (2.1) with (2.3) to get

\[|\{a \in \pi_q(n) : a \equiv d_{d_1, \ldots, d_w} \pmod{\prod_{\deg P < M} P^2}\}| \]

\[= \frac{q^n}{n\phi(\prod_{\deg P < M} P^2)} + O\left(\frac{q^n}{n} \deg \prod_{\deg P < M} P^2\right) \]

\[= \frac{q^n}{n\phi(\prod_{\deg P < M} P^2)} + O\left(\frac{q^n}{n} q^M\right) \]

\[= \frac{q^n}{n\phi(\prod_{\deg P < M} P^2)} + O\left(\frac{q^{n+M}}{n}\right). \]

Let us now insert this in equation (2.2):
\[
|P'(n, M)| = \sum_{(d_1, \ldots, d_w) \in C} \left( \frac{q^n}{n\phi(\prod_{\deg P < M} P^2)} + O \left( \frac{q_n^{n+M}}{n} \right) \right)
\]

\[
= \left( \prod_{\deg P < M} \phi(P^2) - \rho(P^2) \right) \left( \frac{q^n}{n\phi(\prod_{\deg P < M} P^2)} + O \left( \frac{q_n^{n+M}}{n} \right) \right)
\]

\[
= \frac{q^n}{n} \prod_{\deg P < M} \left( 1 - \frac{\rho(P^2)}{|P|^2 - |P|} \right) + O \left( \frac{q_n^{n+M}}{n} \right)
\]

\[
= \frac{q^n}{n} \prod_{\deg P < M} \left( 1 - \frac{\rho(P^2)}{|P|^2 - |P|} \right) + O \left( \frac{q_n^{n+4q^M+M}}{n} \right).
\]

Now, by Hensel's Lemma, for any \( P \) with \( \deg P > \Delta(f) \), for every \( b \pmod{P} \) for which \( f(b) \equiv 0 \pmod{P} \) there is exactly one \( c \pmod{P^2} \) such that \( c \equiv b \pmod{P} \) and \( f(c) \equiv 0 \pmod{P} \). Thus,

\[
\rho(P^2) = |\{ c \pmod{P^2} : f(c) \equiv 0 \pmod{P}, \gcd(c, P^2) = 1 \}|
\]

\[
\leq |\{ c \pmod{P^2} : f(c) \equiv 0 \pmod{P^2} \}|
\]

which is a uniform bound for all \( P \). It follows that the infinite product

\[
T := \prod_{P} \left( 1 - \frac{\rho(P^2)}{|P|^2 - |P|} \right)
\]

converges because \( \sum_{P} \frac{1}{|P|^2 - |P|} \) converges.

By (2.5),

\[
|P'(n, M)| = \left| \{ a \in \pi_q(n) : \forall \deg P < M, P^2 \nmid f(a) \} \right|
\]

\[
= \frac{q^n}{n} \prod_{\deg P < M} \left( 1 - \frac{\rho(P^2)}{|P|^2 - |P|} \right) + O \left( \frac{q_n^{n+4q^M+M}}{n} \right)
\]

\[
= \frac{q^n}{n} \prod_{\deg P \geq M} \left( 1 - \frac{\rho(P^2)}{|P|^2 - |P|} \right) + O \left( \frac{q_n^{n+4q^M+M}}{n} \right).
\]

Now using the uniform bound \( \rho(P^2) \leq \deg f \), the fact that \( \log \frac{1}{1-x} \ll x \) for \( |x| < 1 \), and that \( |\pi_q(i)| \leq \frac{q^i}{i} \) (which is a consequence of the Explicit Formula), we get
\[
\log \left( \prod_{\deg P \geq M} \frac{1 - \frac{1}{|P|^2}}{|P|^2 - |P|} \right) \leq \sum_{\deg P \geq M} \frac{1}{|P|^2 - |P|} \leq \sum_{\deg P \geq M} \frac{1}{|P|^2} \leq \sum_{i \geq M} \frac{|\pi_q(i)|}{q^{2i}} \leq \sum_{i \geq M} \frac{1}{iq^i} \leq \frac{1}{Mq^M}.
\]

Now insert this back in (2.5) and use the Taylor expansion for \( e \) to get

\[
|P'(n, M)| = |\{ a \in \pi_q(n) : \forall \deg P < M, P^2 \nmid f(a) \}|
\]

\[
= \frac{q^n T}{n} e^{O\left(\frac{1}{Mq^M}\right)} + O\left(\frac{q^{n+4}q^M}{n}\right)
\]

\[
= \frac{q^n T}{n} \left(1 + O\left(\frac{1}{Mq^M}\right)\right) + O\left(\frac{q^{n+4}q^M}{n}\right)
\]

\[
= \frac{q^n T}{n} + O\left(\frac{q^n}{nMq^M}\right) + O\left(\frac{q^{n+4}q^M}{n}\right).
\]

\[\square\]

3. Bounding the remainder

I will prove:

**Proposition 2.** For \( 0 \ll M \leq \frac{n}{2} \):

\[
|P''(n, M)| = |\{ a \in \pi_q(n) : \exists P, \deg P \geq M, P^2 \mid f(a) \}|
\]

\[
\leq \frac{2q^n \deg f}{Mq^M} + O\left(\frac{q^{n+1}}{q^M}\right)
\]

In [9], Ramsay stated a bound for \( |P''(n, M)| \). However, his argument only works for the case where \( f \in \mathbb{F}_q[x] \) has constant coefficients, and even in that case the argument is incomplete. A proof for the general case is given in Poonen [8]. Poonen gave an alternative proof that a multi-variable version of this set has density 0. In his proof he reduces the problem to the calculation of the density of

\[
\{ a \in \mathbb{F}_q[t] : \deg a = n, \exists P, \deg P \geq M, P \mid h(a), g(a) \}
\]

for \( h(x), g(x) \in \mathbb{F}_q[t][x] \) which are coprime as elements of \( \mathbb{F}_q(t)[x] \). He calculates this density in a more general case (Lemma 5.1 in [8]). We will apply some of his ideas to the special case which is needed for the proof in the present paper.

The calculation in this paper is done by dividing the set into two sets, following a suggestion by Rudnick, and then using Poonen’s method in [8]. All the results will have explicit remainder terms.

**Proposition 2** will be proven by the following two propositions:
Proposition 3. For \( \Delta(f) \ll M \leq \frac{n}{2} \),
\[
\left| \left\{ a \in M_n(q) : \exists P, \frac{n}{2} \geq \deg P \geq M, P^2 \mid f(a) \right\} \right| \leq \frac{2q^n \deg f}{M q^M}.
\]

Proposition 4.
\[
\left| \left\{ a \in M_n(q) : \exists P, \deg P > \frac{n}{2}, P^2 \mid f(a) \right\} \right| \ll \frac{q^{n+1}}{p}.
\]

4. PROOF OF Proposition 3

Proof. Notice that if \( \deg P \leq \frac{n}{2} \), then
\[
\left| \left\{ a \in M_n(q) \mid a \equiv C \mod P^2 \right\} \right| = \frac{q^n}{|P|^2}.
\]

Denote \( x(D) = |\{ C \in \mathbb{F}_q[t]/D : f(C) \equiv 0 \mod D \}| \). Since \( f \) is square-free and its content is 1, for any \( P \) with \( \deg P > \Delta(f) \) it holds, by Hensel’s Lemma, that \( x(P^2) = x(P) \leq \deg f \). Since we chose \( M \gg \Delta(f) \), it follows that for any \( P \) with \( \deg P \geq M \) it holds that \( \deg P > \Delta(f) \). Also, by the Explicit Formula, \( |\pi_q(k)| \leq \frac{q^k}{k} \).

Thus,
\[
\left| \left\{ a \in M_n(q) : \exists M \leq \deg P \leq \frac{n}{2}, P^2 \mid f(a) \right\} \right| \leq \sum_{M \leq \deg P \leq \frac{n}{2}} \left| \left\{ a \in M_n(q) \mid P^2 \mid f(a) \right\} \right|
= \sum_{M \leq \deg P \leq \frac{n}{2}} \sum_{C \mod P^2, f(C) \equiv 0 \mod P^2} \left| \left\{ a \in M_n(q) \mid a \equiv C \mod P^2 \right\} \right|
= q^n \sum_{M \leq \deg P \leq \frac{n}{2}} \frac{x(P^2)}{|P|^2} \leq q^n \deg f \sum_{M \leq \deg P \leq \frac{n}{2}} \frac{1}{|P|^2}
= q^n \deg f \sum_{M \leq k \leq \frac{n}{2}} \frac{|\pi_q(k)|}{q^{2k}} = q^n \deg f \sum_{M \leq k \leq \frac{n}{2}} \frac{q^k}{q^{2k}}
= q^n \deg f \sum_{M \leq k \leq \frac{n}{2}} \frac{1}{k q^k} \leq q^n \deg f \sum_{M \leq k \leq \frac{n}{2}} \frac{1}{2^k} \leq \frac{2q^n \deg f}{M q^M}.
\]

\( \square \)

Note: Poonen in [8] estimated this set (in his paper it is \( |\bigcup_{s=0}^{N-1} Q_s| \)) using dimension considerations from algebraic geometry (see the proof of Lemma 5.1 in [8]).
5. Proof of Proposition 4

5.1. First Part.

Lemma 1. There exists $A \subset (\mathbb{F}_q[t])^p$ such that (1)
\[
M_n(q) = \left\{ \sum_{j=0}^{p-1} t^j a_j(t)^p : (a_0(t), \ldots, a_{p-1}(t)) \in A \right\}
\]
and (2)
\[
\forall (a_0(t), \ldots, a_{p-1}(t)) \neq (a'_0(t), \ldots, a'_{p-1}(t)) \in A, \quad \sum_{j=0}^{p-1} t^j a_j(t)^p \neq \sum_{j=0}^{p-1} t^j a'_j(t)^p
\]

Proof. First we show the uniqueness:
\[
\sum_{j=0}^{p-1} t^j a_j(t)^p \neq \sum_{j=0}^{p-1} t^j a'_j(t)^p \iff \sum_{j=0}^{p-1} t^j (a_j(t) - a'_j(t))^p = 0.
\]
Thus it is enough to prove that $\sum_{j=0}^{p-1} t^j a_j(t)^p = 0 \implies (a_0(t), \ldots, a_{p-1}(t)) = (0, \ldots, 0)$.

Suppose that $\sum_{j=0}^{p-1} t^j a_j(t)^p = 0$. Then for each $j$ either $a_j(t) = 0$, or $\deg(t^j a_j(t)^p) \equiv j \pmod{p}$. Thus if for some $j$ it holds that $a_j(t) \neq 0$, then $\sum_{j=0}^{p-1} t^j a_j(t)^p \neq 0$ (since no term can cancel the term of degree $\deg t^j a_j(t)^p$ in $t^j a_j(t)^p$, because for every $0 \leq i \neq j < p$ it holds that $\deg t^i a_j(t)^p \neq \deg t^j a_j(t)^p \pmod{p}$), which is a contradiction. This proves (2).

Now, to prove (1), using (2) it suffices to find a collection $(a_0(t), \ldots, a_{p-1}(t)) \in (\mathbb{F}_q[t])^p$, for every $a(t) \in M_n(q)$, such that
\[
\sum_{j=0}^{p-1} t^j a_j(t)^p = a(t).
\]
The set of all such different collections $(a_0(t), \ldots, a_{p-1}(t))$ will be declared as the desired set $A$.

Recall that the Frobenius automorphism $h(x) = x^p$ is invertible from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Take $\sum_{i=0}^n s_i t^i \in M_n(q)$ with $s_i \in \mathbb{F}_q$. We need to find $(a_0(t), \ldots, a_{p-1}(t)) \in (\mathbb{F}_q[t])^p$ such that $\sum_{j=0}^{p-1} t^j a_j(t)^p = \sum_{i=0}^n s_i t^i$. 

Using the reminder, we get
\[
\sum_{i=0}^{n} s_i t^i = \sum_{j=0}^{p-1} \sum_{0 \leq i_j \leq n} \sum_{i_j \equiv j \pmod{p}} s_{i_j} t^{i_j} = \sum_{j=0}^{p-1} t^j \sum_{0 \leq i_j \leq n} \sum_{i_j \equiv j \pmod{p}} (h^{-1}(s_{i_j}))^p t^{i_j-j}.
\]

Now, since for every \(0 \leq j \leq p-1\) it holds that \(i_j \equiv j \pmod{p}\), we conclude that \(p \mid (i_j - j)\), thus we define
\[
a_j(t) = \sum_{0 \leq i_j \leq n} h^{-1}(s_{i_j}) t^{\frac{i_j-j}{p}}
\]
and the desired equality holds. This proves (1).

### 5.2. Second Part
Denote
\[
F(y_0, \ldots, y_{p-1}) = f \left( \sum_{j=0}^{p-1} t^j y_j(t)^p \right) \in \mathbb{F}_q[t][y_0, \ldots, y_{p-1}],
\]
\[
Q = \left\{ a \in \mathbb{F}_q[t]^p : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid F(a), \frac{\partial F}{\partial t}(a) \right\}.
\]

A will denote the set from Lemma 1.

**Lemma 2.**
\[
\left| \left\{ a \in M_n(q) : \exists P, \deg P > \frac{n}{2}, P^2 \mid f(a) \right\} \right| \leq |Q|
\]

**Proof.** By Lemma 1
\[
(5.1) \left| \left\{ a \in M_n(q) : \exists P, \deg P > \frac{n}{2}, P^2 \mid f(a) \right\} \right|
\]
\[
= \left| \left\{ \sum_{j=0}^{p-1} t^j a_j(t)^p : (a_0(t), \ldots, a_{p-1}(t)) \in A, \exists P, \deg P > \frac{n}{2}, P^2 \mid f(\sum_{j=0}^{p-1} t^j a_j(t)^p) \right\} \right|
\]
\[
= \left| \left\{ (a_0(t), \ldots, a_{p-1}(t)) \in A : \exists P, \deg P > \frac{n}{2}, P^2 \mid F(a_0(t), \ldots, a_{p-1}(t)) \right\} \right|
\]
Therefore, the fact that degrees of polynomials are integers, we get

\[
\left\{ (a_0(t), \ldots, a_{p-1}(t)) \in A : \exists P, \deg P > \frac{n}{2}, P \mid F(a_0(t), \ldots, a_{p-1}(t)), \right. \\
\left. P \mid \frac{dF(a_0(t), \ldots, a_{p-1}(t))}{dt} \right\}.
\]

Notice that by the total derivative formula for \( F \), and since \( F(y_0, \ldots, y_{p-1}) \in \mathbb{F}_q[t][y_1^p, \ldots, y_{p-1}^p] \), it holds that

\[
\frac{dF(a_0(t), \ldots, a_{p-1}(t))}{dt} = \frac{\partial F(y_0, \ldots, y_{p-1})}{\partial y_0}(a_0(t), \ldots, a_{p-1}(t)) \frac{da_0(t)}{dt} + \cdots
\]

Combining (5.1) and (5.2) we get:

\[
\begin{align*}
\left\{ a \in M_n(q) : \exists P, \deg P > \frac{n}{2}, P \mid f(a) \right\} = \\
\left\{ a = (a_0(t), \ldots, a_{p-1}(t)) \in A : \exists P, \deg P > \frac{n}{2}, P \mid F(a), P \mid \frac{\partial F}{\partial t}(a) \right\}.
\end{align*}
\]

Now, by Lemma 1, for every \( (a_0(t), \ldots, a_{p-1}(t)) \in A \),

\[
\sum_{j=0}^{p-1} t^j a_j(t)^p \in M_n(q).
\]

Thus, for an integer \( b \) such that \( b = n \mod p \) and \( 0 \leq b < p \), using the fact that degrees of polynomials are integers, we get

\[
a_b(t) \in M_{\frac{n}{p}}(q), \forall j, 0 \leq j \leq p-1, \deg a_j(t) \leq \frac{n-j}{p} \leq \frac{n}{p} \implies \\
\forall j, 0 \leq j \leq p-1, \deg a_j(t) \leq \left\lfloor \frac{n}{p} \right\rfloor.
\]

Therefore,

\[
\left\{ a = (a_0(t), \ldots, a_{p-1}(t)) \in A : \exists P, \deg P > \frac{n}{2}, P \mid F(a), P \mid \frac{\partial F}{\partial t}(a) \right\} \subseteq Q,
\]
which together with (5.3) proves the lemma. □

5.3. End of proof of Proposition 4. By Lemma 2 the following lemma suffices to conclude Proposition 4.

Lemma 3.\[ |Q| \ll q^{\frac{p-1}{p}}. \]

Proof. By Lemma 7.2 in [S], \( F \in \mathbb{F}_q[t][y_0, \ldots, y_{p-1}] \) is square-free because \( f \) is square-free.

The next argument, showing that the case where \( F, \partial F \in \mathbb{F}_q(t)[y_0, \ldots, y_{p-1}] \) are not coprime is degenerate, replaces Lemma 7.3 in [S] to allow the proof to be easily generalized to the \( k \)-free case.

Set \( G = \gcd (F, \partial F) \in \mathbb{F}_q(t)[y_0, \ldots, y_{p-1}] \). By the total derivative formula one has, just like in the proof of Lemma 2 that for any \( a(t) \in \mathbb{F}_q[t]^p \) it holds that \( \frac{dF(a)}{dt} = \partial F(a) \), because the rest of the partial derivatives vanish since \( F \in \mathbb{F}_q(t)[y_0, \ldots, y_{p-1}] \).

If \( \deg G > 0 \), then for any \( a(t) \in \mathbb{F}_q[t]^p \) let \( P(t) \) be a prime factor of \( G(a) \) (such \( P(t) \) exists because \( \deg G > 0 \)). Then \( P^2 \mid F(a) \) (because \( P \mid G(a), G(a) \mid F(a) \), and \( G(a) \mid \partial F(a) = \frac{dF(a)}{dt} \)).

Thus if \( \deg G > 0 \), then for any \( a(t) \in \mathbb{F}_q[t]^p \), \( f(a) \) is not square-free. By Lemma 1 for any \( a(t) \in \mathbb{F}_q[t] \), \( f(a) \) is not square-free. Now by Theorem 3.4 in [S] we have

\[
\lim_{n \to \infty} \left( 1 - \frac{|\{c \in \mathbb{F}_q[t]/P^2 : f(c) \equiv 0 \pmod{P^2}\}|}{|P|^2} \right)^n = 0.
\]

By Hensel’s Lemma and the fact that the sum \( \sum_P \frac{1}{|P|^2} \) converges, the infinite product converges. So the vanishing of the product happens only when there is some prime \( P \) such that \( P^2|f(c) \) for any \( c \in \mathbb{F}_q[t] \). Thus we get

\[ \rho (P^2) = \left| \{ c \pmod{P^2}, \gcd(c, P) = 1, f(c) = 0 \pmod{P^2} \} \right| = |P|^2 - |P|. \]

This implies that

\[ c_{f,2} = \prod_P \left( 1 - \frac{\rho_P (P^2)}{|P|^2 - |P|} \right) = 0, \]

which is as expected, since \( |P_{f,2}(n)| = 0 \) when for any \( a \in \mathbb{F}_q[t] \), \( f(a) \) is not square-free.
So we showed that the case when \( \deg G > 0 \) is degenerate, as claimed. Now let us assume that \( \deg G = 0 \), which means that \( F \) and \( \frac{\partial F}{\partial t} \) are coprime in \( \mathbb{F}_q(t)[y_0, \ldots, y_{p-1}] \).

Since we are interested in \( P \) with a large value of \( |P| \), we may divide \( F, \frac{\partial F}{\partial t} \) by common factors in \( \mathbb{F}_q[t] \) and assume that \( F, \frac{\partial F}{\partial t} \) are coprime as elements of \( \mathbb{F}_q[t][y_0, \ldots, y_{p-1}] \).

If the decompositions of \( F \) and \( \frac{\partial F}{\partial t} \) into irreducibles are \( F = f_1 \cdots f_i \) and \( \frac{\partial F}{\partial t} = g_1 \cdots g_j \) (\( f_i \neq g_j \) because \( F \) is square-free, thus \( f_i, g_j \) are coprime since they are both irreducible), then

\[
Q = \left\{ a \in \mathbb{F}_q[t]^p : \deg a_i \leq \left\lfloor \frac{n}{P} \right\rfloor, \exists P, \deg P > \frac{n}{2} | F(a), \frac{\partial F}{\partial t}(a) \right\}
\]

\[
= \bigcup_{i,j} \left\{ a \in \mathbb{F}_q[t]^p : \deg a_i \leq \left\lfloor \frac{n}{P} \right\rfloor, \exists P, \deg P > \frac{n}{2} | f_i(a), g_j(a) \right\},
\]

and since this is a finite union, it suffices to prove the following statement:

**Proposition 5.** For coprime irreducible \( f, g \in \mathbb{F}_q[t][x_1, \ldots, x_N] \) and any integer \( N > 0 \), it holds that

\[
\left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{P} \right\rfloor, \exists P, \deg P > \frac{n}{2} | f(a), g(a) \right\} \ll q^\frac{N-1}{p}.
\]

For \( N = 0 \) and \( n \gg 0 \),

\[
\left\{ P : \deg P > \frac{n}{2} | f, g \right\} = \emptyset.
\]

**Proof:** Denote:

\[ Q' = \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{P} \right\rfloor, \exists P, \deg P > \frac{n}{2} | f(a), g(a) \right\}. \]

We proceed by induction on \( N \).

If \( N = 0 \), then \( f, g \in \mathbb{F}_q[t] \). Thus for \( \frac{n}{2} > \max\{\deg f, \deg g\} \) it holds that \( Q' = \emptyset \).

Now assume \( N \geq 1 \). Denote by \( f_1, g_1 \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}] \) the coefficients of the highest power of \( x_N \) in \( f, g \), respectively, when looking at \( f, g \) as polynomials in \( x_N \).

Case 1: Assume the \( x_N \)-degrees of both \( f \) and \( g \) are positive. Since \( f, g \) are coprime in \( \mathbb{F}_q[t][x_1, \ldots, x_N] \), they are also coprime if viewed as single-variable polynomials in \( \mathbb{F}_q(t, x_1, \ldots, x_{N-1})[x_N] \). Thus by the Bézout Identity, there are \( b, c \in \mathbb{F}_q(t, x_1, \ldots, x_{N-1})[x_N] \) such that \( 1 = bf + cg \). Multiplying by the common denominator it follows that there are \( B, C \in \mathbb{F}_q[t][X_1, \ldots, X_{N-1}][X_N] \) and \( 0 \neq D \in \mathbb{F}_q[t][X_1, \ldots, X_{N-1}] \) such that \( D = Bf + Cg \).

Note: The polynomial \( D \) here replaces the resultant used in Poonen’s proof of Lemma 5.1 in [S]. The change is done so that it will be easier to generalize the proof to the \( k \)-free case.
Since $D$ is nonzero and does not involve $x_N$ and since $f, g$ are irreducible, it follows that $D$ is coprime with each of $f, g$. If $P$ divides $f(a)$ and $g(a)$, then from $D = Bf + Cg$ it follows that $P \mid D(a)$. Thus,

$$Q' \subseteq \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \frac{n}{p}, \exists P, \deg P > \frac{n}{2}, P \mid f(a), g(a) \right\}.$$

By looking at the irreducible factors of $D$, just as in the beginning of the proof of Lemma 3, we can assume that $D$ is irreducible. This reduces the problem to dealing with $f, g$ such that one of them is in $\mathbb{F}_q[t][x_1, \ldots, x_{N-1}]$ and thus does not depend on $x_N$.

Case 2: Suppose that one of $f, g$ is in $\mathbb{F}_q[t][x_1, \ldots, x_{N-1}]$. Without loss of generality, we can assume that it is $g$. In this case the proof will be by induction on $\delta$, where $\delta$ is the $x_N$-degree of $f$. If $\delta = 0$, then $f, g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}]$ and according to the outer induction hypothesis,

$$\left\{ a \in \mathbb{F}_q[t]^{N-1} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid f(a), g(a) \right\} \ll q^{\frac{N-2}{p}},$$

whence

$$\left\{ a \in \mathbb{F}_q[t]^{N} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid f(a), g(a) \right\}$$

$$= \left\{ a \in \mathbb{F}_q[t]^{N-1} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid f(a), g(a) \right\} \cdot \left\{ a \in \mathbb{F}_q[t]^{N} : \deg a \leq \left\lfloor \frac{n}{p} \right\rfloor \right\}$$

$$\ll q^{\frac{N-2}{p}} \cdot q^{\left\lfloor \frac{n}{p} \right\rfloor} \leq q^{\frac{N-2}{p} + \frac{n}{p}} = q^{\frac{N-1}{p}}.$$

So let us assume $\delta > 0$ and define

$$S' = \left\{ a \in \mathbb{F}_q[t]^{N} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid f_1(a), g(a) \right\},$$

$$S_0 = \left\{ a \in \mathbb{F}_q[t]^{N} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0 \right\},$$

$$S = \left\{ a \in \mathbb{F}_q[t]^{N} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, \exists P, \deg P > \frac{n}{2}, P \mid f(a), g(a) \right\},$$

$P \nmid f_1(a), g(a) \neq 0 \}.$

It holds that $Q' \subseteq S \cup S' \cup S_0$.

If $g \nmid f_1$, then by subtracting a multiple of $g$ from $f$, $Q'$ is not changed and the new $f$ is still coprime to $g$. In this way the degree of $f$ can be lowered, which then allows us to use the inner inductive hypothesis to get the desired result. So assume now that $g \nmid f_1$ and since we assumed that $g$ is irreducible this means that $g, f_1$ are coprime in $\mathbb{F}_q[t][x_1, \ldots, x_{N-1}]$. Thus by applying
the hypothesis of the outer induction to \( f_1, g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}] \), just like in the case \( \delta = 0 \), we conclude that \( |S'| \ll q^{n^2} \).

So all we have left to prove is the following two propositions:

**Proposition 6.**

\[ |S_0| \ll q^{n^2} \]

**Proposition 7.**

\[ |S| \ll q^{n^2} \]

**Proof of Proposition 6.** We will show that \( |S_0| \ll q^{n^2} \) by using induction on \( N \) to verify that for any \( 0 \neq g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}] \) it holds that

\[
\left| \left\{ a \in \mathbb{F}_q[t]_N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0 \right\} \right| \ll q^{n^2}.
\]

Note that \( g \neq 0 \) because \( f \) and \( g \) are coprime. For \( N = 1 \), since \( g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}] \), it follows that \( g \in \mathbb{F}_q[t] \) and since \( g \neq 0 \),

\[
\left\{ a \in \mathbb{F}_q[t] : \deg a \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0 \right\} = \emptyset.
\]

Let us assume now that the assertion is true for \( N - 1 \), where \( N > 1 \). Denote by \( g_2 \) the coefficient of the highest power of \( x_{N-1} \) in \( g \). If \( g_2 = 0 \), then \( g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-2}] \). By the induction hypothesis, for any \( 0 \neq h \in \mathbb{F}_q[t][x_1, \ldots, x_{N-2}] \),

\[
\left\{ a \in \mathbb{F}_q[t]_N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, h(a) = 0 \right\} =
\left\{ a \in \mathbb{F}_q[t]_{N-1} : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, h(a) = 0 \right\} 
\cdot \left\{ a \in \mathbb{F}_q[t] : \deg a \leq \left\lfloor \frac{n}{p} \right\rfloor \right\}
\ll q^{n^2} \cdot q^{\frac{n^2}{p}} \cdot q^{\frac{n^2}{p}} \leq q^{n^2} \cdot q^{\frac{n^2}{p}} = q^{n^2},
\]

as desired. □

Assume now that \( g_2 \neq 0 \). Since \( g_2 \in \mathbb{F}_q[t][x_1, \ldots, x_{N-2}] \), it follows as we just seen that

\[
\left\{ a \in \mathbb{F}_q[t]_N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g_2(a) = 0 \right\} \ll q^{n^2}.
\]

Now
\[ \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0 \right\} \]
\[ \subset \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g_2(a) = 0 \right\} \]
\[ \cup \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0, g_2(a) \neq 0 \right\}. \]

Thus we only need to show that
\[ \left| \left\{ a \in \mathbb{F}_q[t]^N : \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor, g(a) = 0, g_2(a) \neq 0 \right\} \right| \ll q^{n^{N-1}/p}. \]

Denote by \( \deg_{x_{N-1}} g \) the degree of \( g \) as a polynomial in the variable \( x_{N-1} \). For any \( (a_1, \ldots, a_{N-2}) \in \mathbb{F}_q[t]^{N-2} \) there are at most \( \deg_{x_{N-1}} g \) values of \( a_{N-1} \in \mathbb{F}_q[t] \) such that \( g(a_1, \ldots, a_{N-2}, a_{N-1}) = 0 \); indeed, this holds because \( g(a_1, \ldots, a_{N-2}, x_{N-1}) \) is a polynomial in \( x_{N-1} \) of degree \( \deg_{x_{N-1}} g \). Using this and the induction hypothesis gives
\[ \ll q^{n^{N-1}/p} \cdot \left| \frac{2n}{p} \right| \leq q^{n^{N-1}/p + \frac{2n}{p}} = q^{n^{N-1}/p}, \]
as desired.

\[ \square \]

**Proof of Proposition 7.** Take \( a' = (a_1, \ldots, a_{N-1}) \in \mathbb{F}_q[t]^{N-1} \) with \( \deg a_i \leq \left\lfloor \frac{n}{p} \right\rfloor \). We will count the number of \( a_N \in \mathbb{F}_q[t] \) such that \( a = (a', a_N) \in S \). Let \( \deg g \) be the total degree of \( g \). Since \( a \in S \), the definition of \( S \) implies that \( g(a) \neq 0 \). Since \( g \in \mathbb{F}_q[t][x_1, \ldots, x_{N-1}] \) does not depend on \( x_N \), we get \( g(a) = g(a') \). Therefore,
\[ \deg g(a) = \deg g(a') \leq \deg g \cdot \max\{\deg a_1, \ldots, \deg a_{N-1}\} \leq \deg g \cdot \left\lfloor \frac{n}{p} \right\rfloor. \]

Thus, since \( \left\lfloor \frac{n}{p} \right\rfloor \leq \frac{n}{2} \), there can be at most \( \deg g \) different primes \( P \) such that \( \deg P > \frac{n}{2} \) and \( P \mid g(a) \). Now for \( P \) such that \( P \nmid f_1(a) \), it holds
that \(f(a', x_N) \mod P \in \mathbb{F}_q[t]/P[x_N]\) is a polynomial of degree \(\delta > 0\) over the field \(\mathbb{F}_q[t]/P\) (it is a field since \(P\) is prime). Thus in this case \(f(a', x_N) \mod P\) has at most \(\delta\) roots over the field \(\mathbb{F}_q[t]/P\) (this is the reason why the case \(P \mid f_1(a)\) needs to be dealt with separately, because in that case it might happen that \(f(a', x_N) \mod P\) is 0, which would prevent us from bounding the number of its roots). Now for \(P\) such that \(\deg P > \frac{n}{p}\) it holds that each \(c \in \mathbb{F}_q[t]/P\) has at most one \(a_N \in \mathbb{F}_q[t]\) such that \(\deg a_N \leq \frac{n}{p}\) and \(a_N = c \mod P\).

We see that there are at most \(\deg g\) primes \(P\) such that \(P \mid g(a')\), and for every such \(P\) there are at most \(\delta \cdot O(1)\) values of \(a_N \in \mathbb{F}_q[t]\) with \(\deg a_N \leq \frac{n}{p}\) such that \(P \mid f(a', a_N)\).

We conclude that for any \(a' = (a_1, \ldots, a_{N-1}) \in \mathbb{F}_q[t]^{N-1}\) with \(\deg a_i \leq \frac{n}{p}\) there are \(O(1)\) values of \(a = (a', a_N) \in \mathbb{F}_q[t]^N\) with \(\deg a_N \leq \frac{n}{p}\) such that \(a \in S\). Thus

\[
|S| \ll \left| \left\{ (a_1, \ldots, a_{N-1}) \in \mathbb{F}_q[t]^{N-1} : \deg a_i \leq \frac{n}{p} \right\} \right| \ll q^{\frac{n}{p}(N-1)} \ll q^{n\frac{N-1}{p}}.
\]

\[\square\]

This concludes the proof of Proposition 5.

\[\square\]

6. Remarks

6.1. Sketch of proof of Theorem 2. The proof of Theorem 2 on \(k\)-free values at primes, is similar to that of Theorem 1. Only minor changes are required in the calculation of the main term and Proposition 3; the biggest change is in the proof of Proposition 4, but the bound will stay the same.

The proof can be carried out using:

1. \(M = \log_q \frac{n}{666k}\),
2. \(F, \frac{\partial F}{\partial t}, \frac{\partial^2 F}{\partial t^2}, \ldots, \frac{\partial^k F}{\partial t^k}\) instead of \(F, \frac{\partial F}{\partial t}\) in lemmas 2 and 3,
3. \(\gcd \left(F, \frac{\partial F}{\partial t}, \frac{\partial^2 F}{\partial t^2}, \ldots, \frac{\partial^k F}{\partial t^k}\right)\) in Lemma 3 instead of \(\gcd \left(F, \frac{\partial F}{\partial t}\right)\).

We omit the details.

6.2. Positivity of \(c_{f,2}\). In Theorem 1 we proved that

\[
\frac{|P_{f,2}(n)|}{|\pi_q(n)|} = c_{f,2} + O_f, q \left( \frac{1}{\log_q n} \right) \quad \text{as } n \to \infty,
\]

with

\[
c_{f,2} = \prod_P \left( 1 - \frac{\rho_f \left( \frac{P^2}{|P|^2 - |P|} \right)}{\frac{P^2}{|P|^2 - |P|}} \right),
\]
where the product runs over the prime polynomials $P$, and for any polynomial $D \in \mathbb{F}_q[t]$, $\rho_f(D) = |\{C \pmod{D}, \gcd(D, C) = 1, f(C) = 0 \pmod{D}\}|$.

We now investigate when $c_{f, 2}$ is nonzero:

**Proposition 8.** The following conditions are equivalent:

1. $c_{f, 2} > 0$.
2. There are infinitely many primes $P$ such that $f(P)$ is square-free.
3. There is a prime $P \in \mathbb{F}_q[t]$ with $\deg P > \deg \Delta(f)$ such that $f(P)$ is square-free.
4. For any prime $P \in \mathbb{F}_q[t]$, there is a polynomial $C \in \mathbb{F}_q[t]$ such that $P \nmid C$ and $P^2 \nmid f(C)$.
5. For each prime $P \in \mathbb{F}_q[t]$ such that $\deg P \leq \deg \Delta(f)$, there is a polynomial $C \in \mathbb{F}_q[t]$ such that $P \nmid C$ and $P^2 \nmid f(C)$. Note that this condition can be checked by a finite computation.

**Proof.** By Hensel’s Lemma, for any $P$ with $\deg P > \Delta(P)$ we have $\rho(P^2) = \rho(P) \leq \deg f$. Thus the convergence of the sum $\sum_P \frac{1}{|P^2 - P|}$ implies the convergence of the product in $c_{f, 2}$. Consequently, $c_{f, 2} = 0$ if and only if some term in the product vanishes, which happens if and only if there is some $P$ such that $\rho(P^2) = |P^2 - P|$. However, from Hensel’s Lemma it follows that for $P$ with $\deg P > \Delta(P)$ we have that $\rho(P^2) = \rho(P) \leq |P| - 1 < |P^2 - P|$. This proves that $(1) \iff (4)$ and $(5) \implies (1)$. Also, obviously $(2) \implies (3)$ and $(4) \implies (5)$. Now, if $c_{f, 2} > 0$, then by Theorem 1 there is $N$ sufficiently large such that for any $n > N$ there exists a prime $P$ of degree $n$ such that $f(P)$ is square-free. This proves $(1) \implies (2)$. And finally, if there is some $P \in \mathbb{F}_q[t]$ with $\deg P > \deg \Delta(f)$ such that $f(P)$ is square-free, then for any prime $p \in \mathbb{F}_q[t]$ with $\deg p \leq \deg \Delta(f)$, we have $p \neq P$, and since they are both prime it follows that $p \nmid P$. But $f(P)$ is square-free, thus we also have $P^2 \nmid f(P)$. This proves $(3) \implies (5)$, which completes the proof of the equivalence of the conditions in the proposition. \[ \square \]

6.3. **Final comments.** We make a number of final remarks regarding the proofs in this paper.

1. For general $f(x) \in \mathbb{F}_q[t][x]$ and $a \in \mathbb{F}_q[t]$,
   \[ \frac{df(a)}{dt} = \frac{\partial f(x)}{\partial t}(a) + \frac{\partial f(x)}{\partial x}(a) \frac{da}{dt}. \]
   Since the derivative function $\frac{da}{dt}$ is not a polynomial in $x$, it seems that there is no $g(x) \in \mathbb{F}_q[t][x]$ such that $P^2 \nmid f(a) \implies P \nmid f(a), g(a)$. On the contrary, when working with $h(y_0, \ldots, y_{p-1}) = f(\sum_{j=0}^{p-1} t^j y_j^p)$ there is such $g$, given by $g = \frac{\partial h}{\partial t}$ (lemmas 7.2, 7.3 in \[ S \] and using the total derivative of $h$).
The reason for the change of variables $x \rightarrow \sum_{j=0}^{p-1} t^j y_j^p$ is to simplify the derivative $\frac{df(a)}{dt}$ by making all partial derivatives of $h(y_0, \ldots, y_{p-1}) = f(\sum_{j=0}^{p-1} t^j y_j^p)$ to equal 0, except for the partial derivative with respect to $t$. The reason why $p$ variables are used is evident from the proof of Lemma 1: there are $p$ residues modulo $p$. One could try to change variables as $f(x, t) \rightarrow g(y, h(t^p))$ to make the partial derivative with respect to $t$ to equal 0 and then the proof of Lemma 4 in [9] would work. However, it doesn’t seem that a parallel to Lemma 1 from the present paper exists for this change of variables. This prevents us from using it.

Poonen used a trick that consists of looking only at part of the coordinates of $a \in \mathbb{F}_q[t]^N$ such that $\exists P, \deg P \geq M, P^2 \mid f(a)$, then proving that fixing those coordinates leaves $O(1)$ options for the rest of the coordinates. However, the range of the rest of the coordinates depends on $n$. This proves that the density of the desired set is 0. This trick is not available when working with one variable (last part of the proof of Lemma 5.1 in [8]).

The reason we need to find such a $g$ as in (1) is in order to use a trick to reduce the problem to the case where $g$ depends on one variable less than $f$ does. This allows us, as explained in (3) above, to fix the variables appearing in $g$ and determine the amount of possible values for the variable that does not appear in $g$, but appears in $f$ (last part of the proof of Lemma 5.1 in [8]).

The assumption that the content of $f$ equals 1 is employed in the inequality $\rho(P) \leq \deg f$, which uses the fact that $f$ does not vanish modulo $P$ for no $P$ when the assumption on the content of $f$ holds.

References

[1] T. D. Browning, *Power-free values of polynomials*, Archiv der Math. (2), 96 (2011), 139–150.
[2] D.R. Heath-Brown, *Powerfree values of polynomials*, Q. J. Math. 64 (2013), no. 1, 177–188.
[3] H. Helfgott, *Power-free values, large deviations and integer points on irrational curves*, J. Theorie des Nombres de Bordeaux 19 (2007), 433–472.
[4] C. Hooley, *On power-free numbers and polynomials II*, J. reine angew. Math., 295 (1977), 1–21.
[5] M. Nair, *Power free values of polynomials*, Mathematika, 23 (1976), 159–183.
[6] M. Nair, *Power free values of polynomials II*, Proc. London Math. Soc., 38 (1979), 353–368.
[7] H. Pasten, Int. J. Number Theory (2014) DOI: 10.1142/S1793042115500396.
[8] B. Poonen, *Square-free values of multivariable polynomials*, Duke Math. J. 118 (2003), no. 2, 353–373.
[9] K. Ramsay, Square-free values of polynomials in one variable over function fields, Internat. Math. Res. Notices (1992), no. 4, 97–102.
[10] T. Reuss, Power-free values of polynomials, arXiv:1307.2802 [math.NT]
[11] G. Ricci, Ricerche aritmetiche sui polinomi, Rend. Circ. Mat. Palermo 57 (1933), 433–475.
[12] M. Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210 Springer-Verlag, New York (2002).
[13] Z. Rudnick, square-free values of polynomials over the rational function field, J. Number Theory 135 (2014), 60–66.
[14] A. Titchmarsh, E. C. A divisor problem, Rend. Circ. Math. Palermo 54 (1930), 414–429.
[15] S. Uchiyama, On the power-free values of a polynomial, Tensor (N.S.), 24 (1972), 43–48.

RAYMOND AND BEVERLY SACKLER SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 69978, ISRAEL
E-mail address: guylando@post.tau.ac.il