SQUARE-FREE VALUES OF POLYNOMIALS OVER $\mathbb{F}_q[t]$ COURSE NOTES, 2015

ZEÉV RUDNICK

Our goal in this lecture is to explore some of the ideas concerning the sieve of Eratosthenes and Legendre in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$, specifically treating the question of squarefree values of polynomials.

Contents

1. The polynomial ring over a finite field

1.1. **Basics.** Let $\mathbb{F}_q$ be a finite field of q elements, and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. The units (invertible elements) are the scalars $\mathbb{F}_q^\times$, and any nonzero polynomial may be uniquely written as $cf(t)$ with $c \in \mathbb{F}_q^\times$ and $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ a *monic* polynomial. We denote by M_n the set of monic polynomials, whose cardinality is

$$\#M_n = q^n \ .$$

The ring $\mathbb{F}_q[t]$ is a Euclidean ring: Given $A, B \neq 0$ in $\mathbb{F}_q[t]$, there are $Q, R \in \mathbb{F}_q[t]$ so that

$$A = QB + R$$

and $R = 0$ (in which case $B \mid A$) or $\deg R < \deg B$. A standard consequence of this property is that irreducible polynomials are *prime*, that is if $P \mid AB$ then either $P \mid A$ or $P \mid B$. Moreover the Fundamental Theorem of Arithmetic holds: Any polynomial of positive degree is "uniquely" a

Date: April 15, 2015.

product of irreducible polynomials, that is up to ordering and multiplication by scalars.

The norm of a nonzero polynomial is defined as

$$|f| := \#\mathbb{F}_q[t]/(f),$$

the number of residue classes modulo f. The norm depends only on the degree of f:

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

The next fact deals with counting monic polynomials in an arithmetic progression. Over the integers, we would be looking to count the number of positive integers $a \leq X$ so that $a = c \mod d$, the answer being $X/|d| + O(1)$. The analogous statement for $\mathbb{F}_q[t]$ is

Lemma 1.1. *Let $0 \neq D \in \mathbb{F}_q[t]$ be a monic polynomial, and $C \in \mathbb{F}_q[t]$. Then*

$$\#\{A \in M_n : A = C \bmod D\} = \begin{cases} q^n/|D|, & \deg D \leq n \\ \\ O(1), & \text{otherwise.} \end{cases}$$

Proof. Assume first that $n \geq \deg D$. We may, after subtracting a multiple of D, assume that $C = 0$ or $\deg C < \deg D$. Then we claim that there is a bijection

$$\begin{aligned} M_{n-\deg D} &\leftrightarrow \{A \in M_n : A = C \bmod D\} \\ B &\mapsto C + BD \end{aligned}$$

Indeed, if $A \in M_n$, $A = C \bmod D$ then by definition, $A = C + BD$ for some $C \in \mathbb{F}_q[t]$ and we need to check that B is monic, of degree $n - \deg D$. But because $\deg C < \deg D$, necessarily

$$n = \deg A = \deg(C + BD) = \deg BD = \deg B + \deg D$$

so that $\deg B = n - \deg D$, and because both A and D are monic and $\deg C < \deg D$, we must have B monic. Thus we have

$$\#\{A \in M_n : A = C \bmod D\} = \#M_{n-\deg D} = q^{n-\deg D} = \frac{q^n}{|D|}$$

establishing our claim if $\deg D \leq n$.

If $\deg D > n$ then there is at most *one* $A \in M_n$ in the progression $A = C \bmod D$, because any two elements of the arithmetic progression have to differ by a multiple of D: $A - A' = BD$ and if the degrees of both are $n < \deg D$ then $\deg(A - A') \leq n < \deg D$ and hence $B = 0$ forcing $A = A'$. □

1.2. **The Prime Polynomial Theorem.** We denote by $\pi_q(n)$ the number of monic irreducibles (primes) of degree n. The Prime Polynomial Theorem states that

$$\pi_q(n) = \frac{q^n}{n} + O\Big(\frac{q^{n/2}}{n}\Big) .$$

In fact we will only need the upper bound, corresponding to Chebyshev's theorem:

$$\pi_q(n) \leq \frac{q^n}{n}$$

(that we can achieve a constant of 1 here requires an additional argument).

1.3. **Separability.** The formal derivative of a polynomial $a = \sum_{j\geq 0} a_j t^j \in \mathbb{F}_q[t]$ is

$$a'(t) := \sum_{j\geq 1} j a_j t^{j-1}$$

Note that if $p = \mathrm{char}(\mathbb{F}_q)$ is the characteristic of the finite field $\mathbb{F}_q$, then $(t^p)' = 0$, and more generally it is easy to check that:

Lemma 1.2. *If $q = p^e$ with p prime, then $a' = 0$ is equivalent to $a(t) = b(t^p)$.*

A polynomial $f \in \mathbb{F}_q[t]$ is separable if it has no repeated factors of positive degree, i.e. if it is squarefree in $\mathbb{F}_q[t]$. Equivalently, if it has no double roots in an algebraic closure of $\mathbb{F}_q$.

Lemma 1.3. *$f \in \mathbb{F}_q[t]$ is separable if and only if $\gcd(f, f') = 1$.*

2. Squarefree values of polynomials

Our goal is to prove a function field version of the conjecture that a separable polynomial $f \in \mathbb{Z}[x]$ for which the sequence $\{f(n) : n \in \mathbb{Z}\}$ has no fixed square divisors, takes on infinitely squarefree values at integers.

Let $f \in \mathbb{F}_q[x]$ be a separable of positive degree. We denote by $\mathcal{N}_f(n)$ the set of monic polynomials $a(t) \in M_n$ so that $f(a(t)) \in \mathbb{F}_q[t]$ is squarefree.

For any polynomial $D \in \mathbb{F}_q[t]$, let

$$\rho_f(D) = \#\{C \bmod D : f(C) = 0 \bmod D\} \ .$$

Theorem 2.1. *Assume $f \in \mathbb{F}_q[x]$ is separable . Then*

$$\#\mathcal{N}_f(n) = c_f q^n + O_{f,q}(\frac{q^n}{n}), \quad \text{as } n \to \infty \tag{2.1}$$

with

$$c_f = \prod_P (1 - \frac{\rho_f(P^2)}{|P|^2}) \ ,$$

the product over prime polynomials P.

The density c_f is positive if and only if there is some $a \in \mathbb{F}_q[t]$ such that $f(a)$ is squarefree.

Remark. Ramsay [3] stated a variable coefficient version (e.g. $f(x,t) = x^2 + t$) of Theorem 2.1, where $f \in \mathbb{F}_q[t][x]$ is separable and irreducible[1]. However, Ramsay's argument only seems to work when $f \in \mathbb{F}_q[x]$ has *constant* coefficients! In fact even then, there is a (fixable) gap in his argument. The general variable coefficient case was proved by Poonen [2].

[1] Its not clear to me why he needs irreducibility

Theorem 2.1 (the constant coefficient case) is proved by an elementary sieve argument, with one crucial novel ingredient due to Elkies (cf Lemma 6.1) to deal with the contribution of large primes to the sieve, which is completely unavailable in the number field case (in Granville's work [1], the ABC conjecture plays an analogous rôle).

Remark. Theorem 2.1 deals with the large degree limit $n \to \infty$, which is similar in nature to the number field problem. The large finite field limit $q \to \infty$, n fixed, is also of interest, but does not fall into the domain of sieve theory. The problem in that case has recently been solved using algebro-geometric methods [4].

3. Analysis of the density c_f

We will need a version of Hensel's Lemma for separable polynomials $f \in \mathbb{F}_q[x]$:

Lemma 3.1. *Assume $f \in \mathbb{F}_q[x]$ is separable. Let $P \in \mathbb{F}_q[t]$ be a prime. Then each solution $a_1 \in \mathbb{F}_q[t]/P$ of the congruence $f(a_1) = 0 \bmod P$ has a unique lift $a_2 \in \mathbb{F}_q[t]/P^2$ so that $a_2 = a_1 \bmod P$ and such that $f(a_2) = 0 \bmod P^2$.*

Proof. Write $a_2 = a_1 + Py$. Then by the (formal) Taylor expansion of f around a_1, we obtain

$$f(a_2) = f(a_1) + f'(a_1)Py + \sum_{j\geq 2} \frac{f^{(j)}(a_1)}{j!}(Py)^j$$

-we have to check that $f^{(j)}/j!$ makes sense in $\mathbb{F}_q[x]$: Indeed, if $f(x) = \sum_k c_k x^k$ then

$$\frac{f^{(j)}(x)}{j!} = \sum_{k\geq j} c_k \frac{k(k-1)\cdot \dots \cdot (k-j+1)}{j!} x^{k-j} = \sum_{k \geq j} c_k \binom{k}{j} x^{k-j} \in \mathbb{F}_q[x] \ .$$

Therefore

$$f(a_2) = f(a_1) + f'(a_1)Py \bmod P^2$$

Therefore $f(a_2) = 0 \bmod P^2$ is equivalent to

$$f(a_1) + f'(a_1)Py = 0 \bmod P^2$$

or, since $P \mid f(a_1)$ by assumption, this is equivalent to

$$f'(a_1) \cdot y = -f(a_1)/P \bmod P$$

So if we show that $f'(a_1) \neq 0 \bmod P$ then we will have determined $y \bmod P$ uniquely and conclude the Lemma.

Now note that since $f \in \mathbb{F}_q[x]$ is separable, it cannot have double roots in any extension of $\mathbb{F}_q$, in particular in $\mathbb{F}_q[t]/P$ which is an extension of degree equal to $\deg P$; since a_1 is a root of $f(x) \bmod P$, it cannot be a root of $f'(x) \bmod P$ so that $f'(a_1) \neq 0 \bmod P$. Alternatively, use that $\gcd(f, f') = 1$ so that there are $u, v \in \mathbb{F}_q[x]$ with $uf + vf' = 1$; hence

$u(a_1)f(a_1)+v(a_1)f'(a_1)=1 \bmod P$ and since $f(a_1)=0 \bmod P$ we obtain $v(a_1)f'(a_1)=1 \bmod P$, and in particular $f'(a_1)\neq 0 \bmod P$. □

For any polynomial $D\in\mathbb{F}_q[t]$, let

$$\rho_f(D)=\#\{C \bmod D : f(C)=0 \bmod D\}\ .$$

As a consequence of Lemma 3.1, we see that

Corollary 3.2. *If $f\in\mathbb{F}_q[x]$ is separable then for any prime $P\in\mathbb{F}_q[t]$*

$$\rho_f(P^2)=\rho_f(P)\ .$$

We defined the density c_f as the product over all primes $P\in\mathbb{F}_q[t]$

$$c_f:=\prod_P(1-\frac{\rho_f(P^2)}{|P|^2})$$

In view of Corollary 3.2, and the fact that $\rho_f(P)\leq\deg f$, being the number of solutions of a polynomial equation over a field $\mathbb{F}_q[t]/P$, the product defining c_f is absolutely convergent. We claim that it is in fact nonzero:

Proposition 3.3. *If $f\in\mathbb{F}_q[x]$ is separable then the following are equivalent:*

1. *The density c_f is positive*
2. *There is some $a\in\mathbb{F}_q[t]$ such that $f(a)$ is squarefree.*
3. *For all primes P with $\deg P\leq\frac{1}{2}\log_q(\deg f)$, there is some $a_P \bmod P^2$ for which $f(a_P)\neq 0 \bmod P^2$.*

Proof. Since $\rho_f(P^2)=\rho_f(P)\leq\deg f$, if $|P|^2>\deg f$ then the local factor $1-\frac{\rho_f(P^2)}{|P|^2}>0$ is nonzero. So we only need to check the primes with $q^{2\deg P}\leq\deg f$. But for such P, the local factor vanishes iff for all $a\in\mathbb{F}_q[t]$, $f(a)=0 \bmod P^2$, which means the sequence $f(a)$ has a fixed square factor. □

4. The strategy

Let $f\in\mathbb{F}_q[x]$ be a separable. We denote by $\mathcal{N}(n)=\mathcal{N}_f(n)$ the set of monic polynomials $a(t)\in M_n$ so that $f(a(t))\in\mathbb{F}_q[t]$ is squarefree.

Fix $\zeta>0$, eventually taken as

$$\zeta=\log_q\frac{n}{4} \tag{4.1}$$

and let

$$\mathcal{N}'(n)=\{a\in M_n : P^2\nmid f(a),\forall P \text{ prime with} \deg P\leq\zeta\}$$

and

$$\mathcal{N}''(n)=\{a\in M_n : \exists P \text{ prime},\ \deg P>\zeta,\ \text{s.t. } P^2\mid f(a),\}$$

Then clearly

$$\mathcal{N}(n)\subseteq\mathcal{N}'(n)\subseteq\mathcal{N}(n)\cup\mathcal{N}''(n)$$

so that

$$\#\mathcal{N}'(n)-\#\mathcal{N}''(n)\leq\#\mathcal{N}(n)\leq\#\mathcal{N}'(n)$$

Thus it suffices to give an asymptotic for $\#\mathcal{N}'(n)$ (the "main term"), which is easy if ζ is small, and an upper bound for $\#\mathcal{N}''(n)$. We will show that for $\zeta \leq \log_q n/4$,

$$\#\mathcal{N}'(n) = C_f q^n + O(\frac{q^n}{q^\zeta}) \tag{4.2}$$

and

$$\mathcal{N}''(n) \ll q^{n/p} + \frac{q^n}{\zeta q^\zeta} + \frac{q^n}{n} \tag{4.3}$$

Taking $\zeta = \log_q \frac{n}{4}$ in (4.2) and (4.3) we obtain (2.1).

5. The main term

To estimate $\mathcal{N}'(n)$ (the main term), one uses inclusion-exclusion, observing that if we put $\mathcal{P}_\zeta := \prod_{\deg P \leq \zeta} P$ then for $a \in M_n$,

$$\sum_{\substack{d \mid \mathcal{P}_\zeta \\ d^2 \mid f(a)}} \mu(d) = \begin{cases} 1, & a \in \mathcal{N}'(n) \\ 0, & \text{otherwise} \end{cases}$$

and thus

$$\#\mathcal{N}'(n) = \sum_{d \mid \mathcal{P}_\zeta} \mu(d) \#\{a \in M_n : d^2 \mid f(a)\}$$

Lemma 5.1. *For $0 \neq D \in \mathbb{F}_q[t]$,*

$$\#\{a \in M_n : D \mid f(a)\} = \begin{cases} \frac{q^n \rho(D)}{|D|}, & \deg D \leq n \\ \\ O\Big(\rho(D)\Big), & \text{otherwise.} \end{cases}$$

Proof. We decompose

$$\#\{a \in M_n : D \mid f(a)\} = \sum_{\substack{C \bmod D \\ f(C)=0 \bmod D}} \#\{a \in M_n : a = C \mod D\}$$

By Lemma 1.1,

$$\#\{a \in M_n : a = C \mod D\} = \begin{cases} q^n/|D|, & \deg D \leq n \\ O(1), & \text{otherwise.} \end{cases}$$

Summing over all $\rho_f(D)$ solutions $C \bmod D$ of $f(C) = 0 \bmod D$ gives the result. □

Now

$$\deg \mathcal{P}_\zeta = \sum_{\deg P \leq \zeta} \deg P = \sum_{j \leq \zeta} j\pi(j) \leq \frac{q^\zeta - 1}{1 - \frac{1}{q}} \leq 2q^\zeta \leq n/2$$

by our choice (4.1) and so we find that for <u>all</u> $d \mid \mathcal{P}_\zeta$,

$$\#\{a \in M_n : d^2 \mid f(a)\} = \frac{q^n \rho_f(d^2)}{|d|^2}$$

and hence using multiplicativity of ρ_f we obtain

$$\#\mathcal{N}'(n) = q^n \sum_{d \mid \mathcal{P}_\zeta} \frac{\mu(d)\rho_f(d^2)}{|d|^2} = q^n \prod_{\deg P \leq \zeta} (1 - \frac{\rho_f(P^2)}{|P|^2}) \,.$$

By Corollary 3.2, for all primes P, $\rho_f(P^2) = \rho_f(P) \leq \deg f = O(1)$ and thus setting $c_f = \prod_P (1 - \frac{\rho_f(P^2)}{|P|^2})$ we get

$$\prod_{\deg P \leq \zeta} (1 - \frac{\rho_f(P^2)}{|P|^2}) = c_f \prod_{\deg P > \zeta} (1 - \frac{\rho_f(P^2)}{|P|^2})^{-1} = c_f \exp(O \sum_{\deg P > \zeta} \frac{1}{|P|^2})$$

and since

$$\sum_{\deg P > \zeta} \frac{1}{|P|^2} \leq \sum_{\substack{F \text{ monic} \\ |F| > q^\zeta}} \frac{1}{|F|^2} \ll \frac{1}{q^\zeta}$$

we obtain

$$\prod_{\deg P \leq \zeta} (1 - \frac{\rho_f(P^2)}{|P|^2}) = c_f(1 + O(\frac{1}{q^\zeta}))$$

and therefore

$$\#\mathcal{N}'(n) = c_f q^n + O(\frac{q^n}{q^\zeta})$$

proving (4.2).

6. The remainder term

The fundamental difference between the number field case and $\mathbb{F}_q[t]$, is the following observation:

Lemma 6.1. *Let $f \in \mathbb{F}_q[x]$ be a separable polynomial. If $a \in M_n$ is such that the formal derivative $a' \neq 0$ and $d^2 \mid f(a)$ for monic $d \in \mathbb{F}_q[t]$, then $d \mid a'$ (the formal derivative of a) and hence* $\deg d \leq n - 1$.

Proof. Since f is separable, $\gcd(f, f') = 1$ in $\mathbb{F}_q[x]$, that is there are $u, v \in \mathbb{F}_q[x]$ with $uf + vf' = 1$. Hence for any substitution $a \in M_n$, $u(a)f(a) + v(a)f'(a) = 1$ so that $f(a)$ and $f'(a)$ are coprime in $\mathbb{F}_q[t]$.

Assume that $d^2 \mid f(a)$. Now d is coprime to $f'(a)$, since we certainly have $d \mid f(a)$ but $\gcd(f(a), f'(a)) = 1$, Differentiating using the chain rule gives $d \mid \frac{\mathrm{d}}{\mathrm{dt}}\Big(f(a)\Big) = f'(a)a'$. Hence $d \mid f'(a)a'$, and since d is coprime to $f'(a)$ we must have $d \mid a'$. Since we assume that $a' \neq 0$, we obtain $\deg d \leq \deg a' \leq n - 1$. □

Bounding $\mathcal{N}''(n)$ is done by noting that according to Lemma 6.1,

$$\mathcal{N}''(n) \subseteq \{a \in M_n : a' = 0\} \bigcup \bigcup_{\zeta < \deg P \leq n-1} \mathcal{N}_{P^2}(n)$$

where for any polynomial D,

$$\mathcal{N}_D(n) = \{a \in M_n : D \mid f(a)\}$$

If $q = p^e$ with p prime, then $a' = 0$ is equivalent to $a(t) = b(t^p)$ (which forces $p \mid n$), and so $b \in M_{n/p}$ and hence

$$\#\{a \in M_n : a' = 0\} = \# M_{n/p} = q^{n/p}$$

Thus

$$\mathcal{N}''(n) \leq q^{n/p} + \sum_{\zeta < \deg P \leq n-1} \#\mathcal{N}_{P^2}(n)$$

By Lemma 5.1,

$$\#\mathcal{N}_D(n) = \begin{cases} q^n \frac{\rho_D(n)}{|D|}. & \deg D \leq n \\ O(\rho_D(n)), & \text{otherwise} \end{cases}$$

Thus

$$\begin{aligned} \mathcal{N}''(n) &\leq q^{n/p} + \sum_{\zeta < \deg P \leq n-1} \#\mathcal{N}_{P^2}(n) \\ &= q^{n/p} + \sum_{\zeta < \deg P \leq n/2} \frac{q^n}{|P|^2} \rho_f(P^2) + \sum_{n/2 < \deg P \leq n-1} O(\rho_f(P^2)) \ . \end{aligned}$$

By Lemma 3.1, $\rho(P^2) = \rho(P) \leq \deg f$ and hence

$$\begin{aligned} \mathcal{N}''(n) &\ll_{\deg f} q^{n/p} + q^n \sum_{\zeta < \deg P \leq n-1} \frac{1}{|P|^2} + \sum_{n/2 < \deg P \leq n-1} 1 \\ &\ll q^{n/p} + q^n \sum_{\zeta < m \leq n-1} \frac{1}{m q^m} + \sum_{n/2 < m \leq n-1} \frac{q^m}{m} \\ &\ll q^{n/p} + q^n \frac{1}{\zeta q^\zeta} + \frac{q^n}{n} \ . \end{aligned}$$

This proves (4.3). □

In the number field setting, Lemma 6.1 is not available which renders the above argument useless once $\deg f > 2$.

References

[1] A. Granville, *ABC allows us to count squarefrees.* Internat. Math. Res. Notices 1998, no. 19, 991–1009.

[2] B. Poonen, *Squarefree values of multivariable polynomials.* Duke Math. J. 118 (2003), no. 2, 353–373.

[3] K. Ramsay, *Square-free values of polynomials in one variable over function fields.* Internat. Math. Res. Notices, no. 4 (1992) 97–102.

[4] Z. Rudnick Square-free values of polynomials over the rational function field , Journal of Number Theory 135 (2014), 60–66.