Journal of Number Theory 135 (2014) 60–66

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Square-free values of polynomials over the rational function field ☆

Zeév Rudnick

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

ARTICLE INFO

Article history:
Received 23 August 2013
Accepted 23 August 2013
Available online 15 October 2013
Communicated by K. Soundararajan

Keywords:
Square-free
Finite fields
Function fields

ABSTRACT

We study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well-studied problem of representing square-free integers by integer polynomials, where it is conjectured that a separable polynomial $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. We show that if $f(x) \in \mathbb{F}_q[t][x]$ is separable, with square-free content, of bounded degree and height, and n is fixed, then as $q \to \infty$, for almost all monic polynomials $a(t)$ of degree n, the polynomial $f(a)$ is square-free.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. We wish to study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well-studied problem of representing square-free integers by integer polynomials, where it is conjectured that a separable polynomial (that is, without

☆ We thank Lior Rosenzweig for his comments. This work was conceived during the ERC Research Period on Diophantine Geometry in Pisa during September 2012. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC grant agreement No. 320755.

E-mail address: rudnick@post.tau.ac.il.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2013.08.014

repeated roots) $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. The problem is most difficult when f is irreducible. The quadratic case was solved by Ricci [13]. For cubics, Erdös [2] showed that there are infinitely many square-free values, and Hooley [6] gave the result about positive density. Beyond that nothing seems known unconditionally for irreducible f, for instance it is still not known that $a^4 + 2$ is infinitely often square-free. Granville [3] showed that the ABC conjecture completely settles this problem. An easier problem which has recently been solved is to ask how often an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d attains values which are free of $(d-1)$-th powers, either when evaluated at integers or at primes, see [2,7–9,5,1,4,12].

In this note we study a function field version of this problem. Given a polynomial $f(x) = \sum_j \gamma_j(t)x^j \in \mathbb{F}_q[t][x]$ which is separable, that is with no repeated roots in any extension of $\mathbb{F}_q(t)$, we want to know how often is $f(a)$ square-free in $\mathbb{F}_q[t]$ as a runs over (monic) polynomials in $\mathbb{F}_q[t]$.

We want to rule out polynomials like $f(x,t) = t^2x$ for which $f(a(t),t)$ can never be square-free. To do so, recall that the content $c \in \mathbb{F}_q[t]$ of a polynomial $f \in \mathbb{F}_q[t][x]$ as above is defined as the greatest common divisor of the coefficients of f: $c = \gcd(\gamma_0, \ldots, \gamma_\ell)$. A polynomial is *primitive* if $c = 1$, and any $f \in \mathbb{F}_q[t][x]$ can be written as $f = cf_0$ where f_0 is primitive. If the content c is not square-free then $f(a)$ can never be square-free.

For any field $\mathbb{F}$, let

$$\mathcal{M}_n(\mathbb{F}) = \big\{a \in \mathbb{F}[t]\colon\ \deg a = n,\ a \text{ monic}\big\}, \tag{1.1}$$

so that $\#\mathcal{M}_n(\mathbb{F}_q) = q^n$. Defining

$$\mathcal{S}_f(n)(\mathbb{F}) = \big\{a \in \mathcal{M}_n(\mathbb{F})\colon\ f(a) \text{ is square-free}\big\}, \tag{1.2}$$

we want to study the frequency

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#\mathcal{M}_n(\mathbb{F}_q)} \tag{1.3}$$

in an appropriate limit.

There are two possible limits to take: Large degree ($n \to \infty$) while keeping the constant field $\mathbb{F}_q$ fixed, or large constant field ($q \to \infty$) while keeping n fixed. The large degree limit (q fixed, $n \to \infty$) was investigated by Ramsay [11] and Poonen [10] who showed[1] that for $f \in \mathbb{F}_q[t][x]$ separable,

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#\mathcal{M}_n(\mathbb{F}_q)} = c_f + O_{f,q}\left(\frac{1}{n}\right), \quad \text{as } n \to \infty, \tag{1.4}$$

[1] They actually count all polynomials up to degree n, and do not impose the monic condition.

with

$$c_f = \prod_P \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right), \tag{1.5}$$

the product over prime polynomials P, and for any polynomial $D \in \mathbb{F}_q[t]$, $\rho_f(D) = \#\{C \bmod D\colon\ f(C) = 0 \bmod D\}$. The implied constant depends on f and on the finite field size q. The density c_f is positive if and only if there is some $a \in \mathbb{F}_q[t]$ such that $f(a)$ is square-free.

In this note we deal with the large finite field limit, of $q \to \infty$ while n is fixed. Here it makes little sense to fix the polynomial f, so we also allow variable f, as long as restrict the degree (in x) and height, where for a polynomial $f(x,t) = \sum_j \gamma_j(t)x^j \in \mathbb{F}[t][x]$, the height is $\mathrm{Ht}(f) = \max_j \deg \gamma_j(t)$.

We will show

Theorem 1.1. *For all separable $f \in \mathbb{F}_q[t][x]$ with square-free content, as $q \to \infty$,*

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#\mathcal{M}_n(\mathbb{F}_q)} = 1 + O\left(\frac{(n \deg f + \mathrm{Ht}(f)) \deg f}{q}\right), \tag{1.6}$$

the implied constant absolute.

Thus if we fix n, the degree and the height, as $q \to \infty$ for almost all $a \in \mathcal{M}_n(\mathbb{F}_q)$ the polynomials $f(a)$ are square-free. For instance, the number of $a(t) \in \mathcal{M}_n(\mathbb{F}_q)$ for which $a(t)^4 + 2$ is square-free is, for q odd, $q^n + O(nq^{n-1})$.

Note that since primes (irreducibles) have positive density among all monic polynomials of given degree in $\mathbb{F}_q[t]$, we in particular find that for almost all primes $P \in \mathbb{F}_q[t]$ of given degree, the polynomial $f(P)$ is square-free as $q \to \infty$.

Remark. It is possible to have primitive, separable f with no square-free values, for instance take

$$f(x) = \prod_{\alpha,\beta \in \mathbb{F}_q} (x - \alpha t - \beta) = x^{q^2} + \cdots. \tag{1.7}$$

Then for all $a \in \mathbb{F}_q[t]$, $f(a)$ is divisible by $(\prod_{\gamma \in \mathbb{F}_q}(t-\gamma))^2 = (t^q - t)^2$. Indeed, if we fix $\gamma \in \mathbb{F}_q$, any $a \in \mathbb{F}_q[t]$ is congruent modulo $(t-\gamma)^2$ to some $\alpha t + \beta$ and hence $f(a) \equiv f(\alpha t + \beta) = 0 \bmod (t-\gamma)^2$. Thus we need to impose some restriction on the degree of f in Theorem 1.1.

Theorem 1.1 is a consequence of a purely algebraic result, valid over *any* field $\mathbb{F}$.

Theorem 1.2. *Suppose $f \in \mathbb{F}[t][x]$ is separable over $\mathbb{F}(t)$ and has square-free content. Then $\mathcal{S}_f(n)$ is the complement of a <u>proper</u> Zariski-closed hypersurface of the affine n-dimensional space $\mathcal{M}_n$, of degree $D \leqslant 2(n \deg f + \mathrm{Ht}\, f) \deg f$.*

Theorem 1.2 implies that the number of $a \in \mathcal{M}_n(\mathbb{F}_q)$ for which $f(a)$ is not square-free is at most Dq^{n-1}, where D is the total degree of an equation defining the hypersurface. Indeed, if $h \in \mathbb{F}_q[X_1, \dots, X_m]$ is a non-zero polynomial of total degree at most D, then the number of zeros of $h(X_1, \dots, X_m)$ in $\mathbb{F}_q^m$ is at most Dq^{m-1}. This is an elementary fact, seen by fixing all variables but one (cf. [14, §4, Lemma 3.1]). Hence Theorem 1.1 follows.

2. Proof of Theorem 1.2

2.1. The primitive case

We write

$$f(x,t) = \gamma_0(t) + \gamma_1(t)x + \cdots + \gamma_\ell(t)x^\ell \tag{2.1}$$

with $\gamma_j(t) \in \mathbb{F}[t]$, and $\gamma_\ell(t) \neq 0$. We first assume that $f(x,t)$ is primitive, that is $\gcd(\gamma_j(t)) = 1$. Denote by

$$\Delta_f(t) = \operatorname{disc}_x f(x,t) \tag{2.2}$$

the discriminant of $f(x)$ as a polynomial of degree ℓ with coefficients in $\mathbb{F}[t]$; it is a universal polynomial with integer coefficients in $\gamma_0(t), \dots, \gamma_\ell(t)$:

$$\Delta_f(t) = \operatorname{Poly}_{\mathbb{Z}}\bigl(\gamma_0(t), \dots, \gamma_\ell(t)\bigr) \in \mathbb{F}[t]. \tag{2.3}$$

Separability of f (over $\mathbb{F}(t)$) is equivalent to the discriminant not being the zero polynomial: $\Delta_f(t) \neq 0$.

The key observation is that $f(a) \in \mathbb{F}[t]$ being square-free is equivalent to requiring that the polynomial $t \mapsto f(a(t), t)$ does not have any multiple zeros (in any extension of the field $\mathbb{F}$). This is in fact a polynomial condition, that is a polynomial system of equations for the coefficients $a_0, a_1, \dots, a_{n-1}$ of $a(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n$ which is given by the vanishing of the discriminant:

$$\operatorname{disc} f\bigl(a(t), t\bigr) = 0. \tag{2.4}$$

It suffices to show that this equation defines a *proper* hypersurface.

Before doing so, we bound the degree D of the hypersurface (2.4): For $f(x,t)$ as in (2.1), $f(a(t),t)$ is a polynomial in t of degree

$$\deg f\bigl(a(t), t\bigr) \leqslant n \deg f + \max \deg \gamma_j = n \deg f + \operatorname{Ht}(f). \tag{2.5}$$

The coefficients are polynomials in the a_j of degree at most $\deg f$. Now the discriminant of a polynomial $\sum_{j=0}^m h_j t^j$ is homogeneous in the coefficients h_j of degree $2m-2$. Hence

$a \mapsto \operatorname{disc} f(a(t), t) = \sum_k \delta_k \prod a_i^{k_i}$ has total degree at most

$$D \leqslant 2\bigl(n \deg f + \operatorname{Ht}(f)\bigr) \deg f. \tag{2.6}$$

It remains to show that Eq. (2.4) is nontrivial.

The condition that the polynomial $f(a(t))$ has multiple zeros is that there is some $\rho \in \overline{\mathbb{F}}$ (an algebraic closure of $\mathbb{F}$) with

$$f\bigl(a(\rho), \rho\bigr) = 0, \qquad \frac{\partial f}{\partial x}\bigl(a(\rho), \rho\bigr) \cdot a'(\rho) + \frac{\partial f}{\partial t}\bigl(a(\rho), \rho\bigr) = 0. \tag{2.7}$$

We define

$$W = \bigl\{(\rho, \vec{a}) \in \mathbb{A}^1 \times \mathbb{A}^n \colon \text{(2.7) holds}\bigr\}. \tag{2.8}$$

We have a fibration of W over the ρ line $\mathbb{A}^1$ and a map $\phi : W \to \mathbb{A}^n$, the restriction of the projection $\mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^n$,

$$\begin{tikzcd} & W \subset \mathbb{A}^1 \times \mathbb{A}^n \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ \mathbb{A}^1 & & \mathbb{A}^n \end{tikzcd} \tag{2.9}$$

and the solutions of (2.7) are precisely $\phi(W)$.

We will show that generically the fiber $\pi^{-1}(\rho)$ has dimension $n-2$ and for at most finitely many ρ the dimension is $n-1$. Therefore we obtain that $\dim W = n-1$. Since the solutions of (2.7) are precisely $\phi(W)$, it follows that $\dim \phi(W) \leqslant n-1$. This will conclude the proof of Theorem 1.2 in the primitive case.

We note that for primitive polynomials, $f(x, \rho) = \sum_j \gamma_j(\rho) x^j$ is not the zero polynomial for any $\rho \in \overline{\mathbb{F}}$. Thus for each $\rho \in \overline{\mathbb{F}}$, the condition $f(a(\rho), \rho) = 0$ constrains a to solve an equation $a(\rho) = \beta$, where $\beta \in \overline{\mathbb{F}}$ is one of the at most $\deg f$ roots of $f(x, \rho)$.

We separate into two cases: The singular case when $\frac{\partial f}{\partial x}(a(\rho), \rho) = 0$ and the generic case when we require $\frac{\partial f}{\partial x}(a(\rho), \rho) \neq 0$.

The singular case implies that β is a multiple zero of the polynomial $f(x, \rho)$, that is that ρ is a zero of the discriminant $\Delta_f(t)$, which is not identically zero (since we assume f is separable) and hence there are only finitely many possibilities for such ρ. Given one of those ρ, then we need $a(t)$ to satisfy $a(\rho) = \beta$, i.e.

$$a_0 + a_1\rho + \cdots + a_{n-1}\rho^{n-1} + \rho^n = \beta \tag{2.10}$$

which is a (non-degenerate) linear equation, and therefore carves out an $(n-1)$-dimensional subspace of a's. Thus the singular locus consists of at most finitely many hyperplanes, and hence if non-empty has dimension $n-1$.

In the generic case, we substitute $a(\rho)=\beta$ into (2.7) to get a system

$$a(\rho)=\beta, \qquad a'(\rho)=-\frac{\frac{\partial f}{\partial t}(\beta,\rho)}{\frac{\partial f}{\partial x}(\beta,\rho)} \tag{2.11}$$

that is

$$\begin{aligned} a_0+a_1\rho+a_2\rho^2+\cdots+a_{n-1}\rho^{n-1}&=-\rho^n+\beta,\\ a_1+a_2\cdot 2\rho+\cdots+a_{n-1}\cdot(n-1)\rho^{n-2}&=-n\rho^{n-1}-\frac{\frac{\partial f}{\partial t}(\beta,\rho)}{\frac{\partial f}{\partial x}(\beta,\rho)} \end{aligned} \tag{2.12}$$

which is clearly of rank 2. Hence the fibers $\pi^{-1}(\rho)$ have dimension $n-2$.

2.2. The general case

We now relax the primitivity condition. Write $f(x,t)=c(t)f_0(x,t)$ where $f_0(x,t)=\sum_j \gamma_j^{(0)}(t)x^j$ is primitive, and $c(t)\in\mathbb{F}_q[t]$ is square-free. Since $c(t)$ is square-free, we obtain that $f(a(t),t)$ is square-free if and only if $f_0(a(t),t)$ is square-free and coprime to $c(t)$. Now $f_0(a(t),t)$ being square-free is the condition $\operatorname{disc} f_0(a(t),t)\neq 0$. For $f_0(a)$ to not be coprime to c is the algebraic condition on vanishing of the resultant

$$R=\operatorname{Res}\bigl(c(t),f_0\bigl(a(t),t\bigr)\bigr). \tag{2.13}$$

Thus the set of $a\in\mathcal{M}_n$ so that $f(a)$ is square-free is the complement of the hypersurface

$$\operatorname{disc} f_0\bigl(a(t),t\bigr)\cdot R(t)=0. \tag{2.14}$$

We wish to show that this is a non-zero equation and to bound its total degree.

We have established above that the discriminant equation $\operatorname{disc} f_0(a(t),t)=0$ is non-trivial, of total degree

$$D_0\leqslant 2\bigl(n\deg f_0+\operatorname{Ht}(f_0)\bigr)\deg f_0=2\bigl(n\deg f+\operatorname{Ht}(f_0)\bigr)\deg f \tag{2.15}$$

in $a_0,\dots,a_n$.

We wish to show that the resultant R is not identically zero. Assuming (as we may) that $c(t)$ is monic, we can write the resultant as a product over the zeros of $c(t)$

$$R=\prod_{c(\alpha)=0} f_0\bigl(a(\alpha),\alpha\bigr)=\prod_{c(\alpha)=0}\sum_{j=0}^{\ell}\gamma_j^{(0)}(\alpha)\bigl(a_0+\cdots+\alpha^n\bigr)^j. \tag{2.16}$$

For each zero α of $c(t)$, let $\ell(\alpha)=\deg f_0(x,\alpha)$ be the degree of the polynomial $f_0(x,\alpha)\in\overline{\mathbb{F}}_q[x]$, which is not the zero polynomial by primitivity of f_0. Then the total degree of R is

$$L := \sum_{c(\alpha)=0} \ell(\alpha) \leqslant \deg c \cdot \deg f \tag{2.17}$$

and the coefficient of a_0^L is $\prod_\alpha \gamma_{\ell(\alpha)}^{(0)}(\alpha)$ which is non-zero. Hence R is non-zero and of degree L.

Finally, we compute the total degree of Eq. (2.14) is the sum of D_0 and $\deg R$, which is at most

$$2\bigl(n \deg f + \mathrm{Ht}(f_0)\bigr) \deg f + \deg c \cdot \deg f \leqslant 2\bigl(n \deg f + \mathrm{Ht}(f)\bigr) \deg f \tag{2.18}$$

since $\mathrm{Ht}(f) = \mathrm{Ht}(f_0) + \deg c$. This concludes the proof of Theorem 1.2.

References

[1] T.D. Browning, Power-free values of polynomials, Arch. Math. (2) 96 (2011) 139–150.
[2] P. Erdös, Arithmetical properties of polynomials, J. Lond. Math. Soc. 28 (1953) 416–425.
[3] A. Granville, ABC allows us to count square-frees, Int. Math. Res. Not. IMRN 1998 (19) (1998) 991–1009.
[4] D.R. Heath-Brown, Power-free values of polynomials, Quart. J. Math. 64 (2013) 177–188.
[5] H. Helfgott, Power-free values, large deviations and integer points on irrational curves, J. Théor. Nombres Bordeaux 19 (2007) 433–472.
[6] C. Hooley, On the power free values of polynomials, Mathematika 14 (1967) 21–26.
[7] C. Hooley, On power-free numbers and polynomials II, J. Reine Angew. Math. 295 (1977) 1–21.
[8] M. Nair, Power free values of polynomials, Mathematika 23 (1976) 159–183.
[9] M. Nair, Power free values of polynomials II, Proc. Lond. Math. Soc. 38 (1979) 353–368.
[10] B. Poonen, Squarefree values of multivariable polynomials, Duke Math. J. 118 (2) (2003) 353–373.
[11] K. Ramsay, Square-free values of polynomials in one variable over function fields, Int. Math. Res. Not. IMRN 1992 (4) (1992) 97–102.
[12] T. Reuss, Power-free values of polynomials, arXiv:1307.2802 [math.NT].
[13] G. Ricci, Ricerche aritmetiche sui polinomi, Rend. Circ. Mat. Palermo 57 (1933) 433–475.
[14] Wolfgang M. Schmidt, Equations over Finite Fields: An Elementary Approach, second ed., Kendrick Press, Heber City, UT, 2004.