Math. Proc. Camb. Phil. Soc. (2021), **170**, 247–263 © *Cambridge Philosophical Society* 2019
doi:10.1017/S0305004119000392
First published online 12 December 2019

On square-free values of large polynomials over the rational function field

BY DAN CARMON† with appendix by ALEXEI ENTIN†
Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978*, Israel.*
e-mails: dancarmo@post.tau.ac.il; aentin@tauex.tau.ac.il

(*Received* 07 *December* 2016; *revised* 28 *August* 2019)

Abstract

We investigate the density of square-free values of polynomials with large coefficients over the rational function field $\mathbb{F}_q[t]$. Some interesting questions answered as special cases of our results include the density of square-free polynomials in short intervals, and an asymptotic for the number of representations of a large polynomial N as a sum of a k-th power of a small polynomial and a square-free polynomial.

2010 Mathematics Subject Classification: 11N25(Primary), 11N32, 11N36, 11R58, 14H05 (Secondary)

1. *Overview*

In this paper we establish function field analogues to certain classical open problems in analytic number theory, such as the representation of large integers by a sum of a square-free integer and a k-th power. We replace large integers, by way of analogy, with polynomials of large degree over a fixed finite field $\mathbb{F}_q$. In Section 2, we describe these problems in the context of function fields, previously known results on special cases, and state the new theorems we prove and their applications. In Section 3 we describe the classical problems over the integers which motivated our analogues, and review the partial or conditional results known about these problems. The proofs of our new theorems are detailed in Sections 4 and 5.

2. *Function field theorems*

2·1. *Questions about square-frees in function fields*

Fix a prime power q, let $\mathbb{F}_q$ be the finite field with q elements, and let $A = \mathbb{F}_q[t]$ be the ring of polynomials over $\mathbb{F}_q$. A polynomial $a(t) \in A$ is called square-free if it is not divisible by the square of any non-constant polynomial in $\mathbb{F}_q[t]$. It is well known that the "probability" of a "random" element of $\mathbb{F}_q[t]$ to be square-free is approximately $1/\zeta_q(2) = 1 - 1/q$ (where ζ_q is the Zeta function associated to the rational function field $\mathbb{F}_q(t)$). More precisely, out of the q^n polynomials of degree less than n, exactly $q^n - q^{n-1} + q - 1 = q^n(1 - 1/q + (q-1)/q^n)$ are square-free, for $n \geq 2$. Many more questions can be asked about square-frees. Of particular interest to us are the following:

† 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 n° 320755.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Question 1. Let $f(t, x) \in \mathbb{F}_q[t][x]$ be a polynomial of degree k (in x). For any $a = a(t) \in \mathbb{F}_q[t]$, denote $f(a) = f(t, a(t)) \in \mathbb{F}_q[t]$. Are there infinitely many polynomials $a \in \mathbb{F}_q[t]$ such that $f(a) \in \mathbb{F}_q[t]$ is square-free? If so, how often is $f(a)$ square-free, e.g. when a ranges over all polynomials of degree less than m?

Question 2. Let $N(t) \in \mathbb{F}_q[t]$ be a polynomial of degree n, and let $k \geq 2$ be an integer. Can N always be expressed as a sum $N = x^k + r$, where $x \in \mathbb{F}_q[t]$ is of degree less than $\frac{n}{k}$, and r is square-free, for sufficiently large n? If so, in how many ways?

Question 3. Let m, n be positive integers, $N(t) \in \mathbb{F}_q[t]$ of degree n. Define the interval around N of length $H = q^m$ to be

$$I(N, m) = \{N + a : a \in \mathbb{F}_q[t], \deg a < m\}.$$

The number of square-frees in $I(N, m)$, when averaged over all N of degree n, is $H/\zeta_q(2)$. How small can we take m, as a function of n, so that for *every* choice of N, $I(N, m)$ will contain the expected amount of square-frees, approximately?

One can formulate all of the above as questions about the number of square-free values attained by certain polynomials on restricted inputs. For Question 2, the polynomial is $f_{N,k}(t, x) = N(t) - x^k$, and we are interested in the number of square-free values of $f(a)$ as $a \in \mathbb{F}_q[t]$ ranges over polynomials of degree less than n/k. For Question 3, the polynomial is $f_N(t, x) = N(t) + x$, and the range is over polynomials of degree less than m.

Question 1 has been answered fully by Poonen, as will be described in Section 2·2. Note that this question deals only with polynomials that are kept fixed as the size of the range is increased. In this paper we extend this result to apply to varying families of polynomials, with coefficients of large degrees, which can grow rapidly with the size of the range, allowing us to answer Questions 2 and 3. These new theorems and corollaries are detailed in Section 2·3.

2·2. *Square-free values of polynomials*

Consider Question 1 for $f(t, x) \in \mathbb{F}_q[t][x]$. There are two obvious obstructions to f being square-free infinitely often. If f is divisible by the square of some polynomial $g \in \mathbb{F}_q[t][x]$ which is non-constant (in x), then clearly $f(a)$ can only be square-free when $g(a) \in \mathbb{F}_q^\times$, which occurs for only finitely many a – this is a *global* obstruction. On the other hand, if for some prime $P \in A$ (i.e. an irreducible, monic polynomial), $f(a)$ is divisible by P^2 for every $a \in A$, then clearly $f(a)$ is never square-free. These are the *local* obstructions, as they depend only on the behaviour of f modulo prime powers.

Define for any non-constant $D \in A$,

$$\rho(D) := \#\{a \bmod D : f(a) \equiv 0 \pmod{D}\},$$
$$||D|| := \#\{a \bmod D\} = q^{\deg D}.$$

For primes P of low degree, the probability that $f(a)$ is not divisible by P^2 is exactly $1 - \rho(P^2)/||P||^2$. Heuristically, one expects these events to be nearly independent, hence the probability that $f(a)$ is indivisible by P^2 for all primes P should be approximately

$$c_f := \prod_{P \in \mathcal{P}} \left(1 - \frac{\rho(P^2)}{||P||^2}\right),$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

where $\mathcal{P}$ is the set of all primes in A. Note that not being divisible by any P^2 is equivalent to being square-free. And indeed, this is true:

THEOREM 2·1. *Let $f \in \mathbb{F}_q[t][x]$ be a square-free polynomial, and define c_f as above. Then*

$$\#\{a \in \mathbb{F}_q[t] : \deg_t(a) < m,\ f(a) \text{ is square-free}\} = c_f q^m + o(q^m),$$

as m tends to ∞.

Note that if there is a local obstruction at a prime P, then $\rho(P^2) = ||P||^2$ and thus $c_f = 0$. Otherwise, it is easily seen that $\rho(P^2) \leq k$ for P sufficiently large: Indeed, as will be detailed further in section 4·1, for all but finitely many P, we have $\rho(P) \leq k$ since $\mathbb{F}_q[t]/(P)$ is a field, and $\rho(P^2) = \rho(P)$, by Hensel's lemma. Thus the infinite product converges, and c_f is positive.

Theorem 2·1 was first proved by Ramsay [**9**]; however, his proof was valid only for polynomials $f \in \mathbb{F}_q[x]$, rather than all $f \in \mathbb{F}_q[t][x]$, i.e. only polynomials with constant coefficients. Poonen [**8**] proved the theorem for $f \in \mathbb{F}_q[t][x]$, and generalised it further to multivariate polynomials in $\mathbb{F}_q[t][x_1, \ldots, x_n]$. In 2014 Lando [**7**] gave a quantitative version of Poonen's work, and applied it to the problems of square-free and power-free values at prime polynomials.

2·3. *New results*

Our main goal in this paper is to extend Theorem 2·1 to polynomials f with varying, large coefficients. Our methods include carefully applying Poonen's and Lando's techniques, as well as replacing some naïve sieving arguments with the more sophisticated Brun sieve. Specifically, we show:

THEOREM 2·2. *Let $q = p^e$ be a fixed prime power, let $k > 0$ be a fixed integer, and define $C_{k,q} = 9k \ln q$ – a constant depending only on k and q. Let m, n be varying positive integers with $m \geq C_{k,q} \log_q n \log_q \log_q n$ and $m \to \infty$.*[1] *Let $f \in \mathbb{F}_q[t][x]$ be a square-free polynomial with $\deg_x f \leq k$, $\deg_t f \leq n$. Let c_f be defined as before. Then*

$$\#\{a \in \mathbb{F}_q[t] : \deg a < m,\ f(a) \text{ is square-free}\} = c_f q^m (1 + o(1)).$$

Which we can immediately apply to answer Question 2:

COROLLARY 2·3. *Let $q = p^e$ be a fixed prime power, let $k > 0$ be a fixed integer, and let $N \in \mathbb{F}_q[t]$ be of sufficiently large degree n. Additionally, suppose that either k is co-prime to p, or N is not a p-th power. Then N has $c_{N,k} q^{\lceil n/k \rceil}(1 + o(1))$ representations as $N = x^k + r$, with $x, r \in \mathbb{F}_q[t]$ such that r is square-free and $\deg x < n/k$, where $c_{N,k} = \prod_{P \in \mathcal{P}} (1 - \rho_{N,k}(P^2)/||P||^2)$ and $\rho_{N,k}(D) = \#\{a \bmod D : a^k \equiv N \pmod D\}$.*

Indeed, the number of such representations is exactly the number of square-free values of $f(x) = N - x^k$, which is square-free[2] and has $\deg_x f = k$, $\deg_t f = n$, where x ranges

[1] Note that if n is bounded, Theorem 2·2 is equivalent to Theorem 2·1. We would therefore be interested mostly in the case $n \to \infty$, and $m \to \infty$ would follow from the bound $m \geq C_{k,q} \cdot \log_q n \log_q \log_q n$.

[2] Note that if $N(t)$ is a p-th power and $p \mid k$, then $f(t, x)$ is a p-th power as well, hence not square-free. It is easy to see that in all other cases $f(t, x)$ is square-free, by considering either its derivative by x (if $p \nmid k$) or by t (if N is not a p-th power), both of which are co-prime to f whenever they are non-zero.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

over polynomials of degree less than $m = \lceil n/k \rceil$, which clearly satisfies the assumptions of Theorem 2·2 as $n \to \infty$.

One could also apply Theorem 2·2 to get an answer to Question 3, on the number of square-frees in a short interval $I(N, m)$, by applying it for the polynomial $f(x) = N + x$, with $\deg_x f = 1$ and $\deg_t f = n$. It is immediate to see that f is square-free, and furthermore $c_f = 1/\zeta_q(2) = 1 - 1/q$ holds independently of N, since $\rho(P^2) = 1$ for any N. Thus Theorem 2·2 would imply that the expected asymptotic

$$\#\{a \in I(N, m) : a \text{ is square-free}\} = (1 + o(1))\frac{q^m}{\zeta_q(2)}$$

holds, under the assumption that $m \geq C_{1,q} \log_q n \log_q \log_q n$ as $m, n \to \infty$.

It can be illuminating to consider this relation it terms of the length of the interval, $H = q^m$, and the size of its elements, $X = q^n$, for which we get that our assumption is that $H \geq (\log_q X)^{C_{1,q} \log_q \log_q \log_q X}$. However, it turns out that Theorem 2·2 is very wasteful in this case. We can get the same result for much smaller values of m by using the following variant of the theorem, which takes advantage of special properties of this family of $f(t, x)$:

THEOREM 2·4. *Let $q = p^e$ be a fixed prime power, and $g \in \mathbb{F}_q[t][x]$ a fixed square-free polynomial with $\deg_x g = k$. Let n, m be varying positive integers with $m - p(\log_q n - \log_q \log_q n) \to \infty$, and let $N(t) \in \mathbb{F}_q[t]$ be of degree n. Then*

$$\#\{a \in I(N, m) : g(a) \text{ is square-free}\} = c_g q^m (1 + o(1)).$$

The asymptotic for short intervals is then immediately obtained by applying Theorem 2·4 to $g(t, x) = x$. Note that in terms of H and X, the relation $m - p(\log_q n - \log_q \log_q n) \to \infty$ translates to $H \geq C \left(\log_q X / \log_q \log_q X\right)^p$ for sufficiently large X, for every value of C, i.e. a polylogarithmic relation. We remark further that one can find intervals with $H \gg \log_q X / \log_q \log_q X$ that contain no square-free polynomials at all, by a straight-forward application of the Chinese Remainder Theorem; so this result is nearly sharp.

The appearance of the characteristic p as the exponent in the bound $H \geq C \left(\log_q X / \log_q \log_q X\right)^p$ seems peculiar and surprising, considering that it does not appear in the bound $H \gg \log_q X / \log_q \log_q X$ for longest intervals with no square-frees. This exponent may well be only an artefact of our method of proof, rather than an intrinsic property of $\mathbb{F}_q[t]$. Closing the gap between these two bounds, whether by eliminating the dependence on p from one or introducing it in the other, could be of considerable interest – especially as it might lead to better conjectures for the analogous problem over the integers.

The proofs of the two theorems are very similar – they both involve essentially the same computations, but the different settings lead to different error terms being dominant, hence different lower bounds on m. In fact, these two dominant error terms are almost independent of each other, and thus we may view the two theorems as special cases of a unified theorem:

THEOREM 2·5. *Let $q = p^e$ be a fixed prime power, $k > 0$ a fixed integer, and m, n_1, n_2 be varying positive integers with both $m \geq C_{k,q} \log_q n_1 \log_q \log_q n_1$ and $m - p(\log_q n_2 - \log_q \log_q n_2 + 2k \log_q \log_q n_1) \to \infty$. Let $g \in \mathbb{F}_q[t][x]$ be a square-free polynomial with $\deg_x g \leq k$, $\deg_t g \leq n_1$, and let $N(t) \in \mathbb{F}_q[t]$ be of degree n_2. Then*

$$\#\{a \in I(N, m) : g(a) \text{ is square-free}\} = c_g q^m (1 + o(1)).$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Indeed, note that if n_2 is fixed and $m > n_2$, then the interval degenerates to $I(N, m) = \{a \in \mathbb{F}_q[t] : \deg a < m\}$, and Theorem 2·5 becomes equivalent to Theorem 2·2. Similarly, if instead n_1 is fixed, then g may be one of only finitely many polynomials, and Theorem 2·5 becomes equivalent to Theorem 2·4. The more general statement of Theorem 2·5 allows for both n_1, n_2 to go to infinity together, as long as m grows sufficiently fast as well.

3. *Classical problems over the integers*

The questions discussed above are all motivated by similar, classical questions over the integers, which remain mostly open. For completeness, we review these questions and the progress that has been made on them.

3·1. *Square-free values of polynomials*

For a square-free polynomial $f(x) \in \mathbb{Z}[x]$, define as before

$$\rho(d) = \#\{a \bmod d : f(a) \equiv 0 \pmod d\}, \quad c_f = \prod_{p \in \mathcal{P}} \left(1 - \frac{\rho(p^2)}{p^2}\right),$$

where $\mathcal{P}$ is the set of prime numbers. As before, it is natural to expect that c_f should be the probability of $f(a)$ being square-free for random a, or more rigorously, to conjecture:

CONJECTURE 3·1. *Let $f \in \mathbb{Z}[x]$ be a square-free polynomial of degree k. The set $\{n \in \mathbb{N} : f(n)$ is square-free$\}$ is conjectured to have density c_f.*

For $k = 1$, the conjecture is equivalent to the regular density of the square-frees in $\mathbb{N}$. The conjecture has been proved for $k = 2$ by Ricci in the 1930's [**10**], and for $k = 3$ by Hooley in 1968 [**5**]. Unconditionally, the conjecture remains completely open for all $k \geq 4$. However, in [**4**], Granville proved the conjecture in full generality, assuming the ABC conjecture.

3·2. *Sums of powers and square-frees*

Question 2 is analogous to the question of representing an integer N as $N = x^k + r$, where both x and r are positive integers and r is square-free: Can it be done for all sufficiently large N, and in how many ways? In the case $k = 2$ the expected asymptotic has been proved by Estermann in [**2**]. The case $k = 3$ was stated by Hooley [**6**, section 4·6, theorem 4], in the form that any sufficiently large number is the sum of a cube and a square-free integer, with no claim on the asymptotic number of such representations. All cases with $k \geq 4$ are still open.

3·3. *Square-frees in short intervals*

The short intervals over the integers are sets of the form $I(X, H) = \{n \in \mathbb{Z} : X \leq n < X + H\}$. Question 3 is analogous to the question of how low can H be, as a function of X, such that $I(X, H)$ will necessarily contain approximately $H/\zeta(2)$ square-free integers, for all sufficiently large X. A slightly weaker variant of the question asks only that the interval $I(X, H)$ will contain *some* square-frees.

It is conjectured that we may allow H to be as low as X^ϵ:

CONJECTURE 3·2. *Let $\epsilon > 0$ be fixed, let X be large, and let $H \gg X^\epsilon$. Then*

$$\#\{n \in I(X, H) : n \text{ is square-free}\} = (1 + o(1))\frac{H}{\zeta(2)}.$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Again, this conjecture follows from the ABC conjecture by Granville's method – see the Appendix for more details.

Unconditionally, the best known result is due to Tolev [**11**], who proved the asymptotic for any $H = H(X)$ such that $H/(X^{1/5}\log(X)) \to \infty$, building on results of Filaseta and Trifonov [**3**].

Note that our results on Question 3 in the function field setting, whether using Theorem 2·2 or 2·4, go beyond Conjecture 3·2 and allow for H much smaller than X^{ϵ}.

4. *Proof of main theorem*

We will begin by working in the setting of Theorem 2·2, for simplicity, but most of our computations will be immediately applicable to the other theorems as well. For brevity, let us denote for any set of polynomials A and any degree d, $A^{<d} = \{a \in A : \deg a < d\}$, and similarly define $A^{\geq d}$, $A^{=d}$.

Let us write $N = \{a \in \mathbb{F}_q[t]^{<m} : f(a) \text{ square-free}\}$. The first step towards estimating $\#N$ is to bound it from below and above by terms more closely related to the contributions of certain primes. We define

$$N' = \{a \in \mathbb{F}_q[t]^{<m} : \forall P \in \mathcal{P}^{<m_0},\ P^2 \nmid f(a)\} \tag{4·1}$$

$$N'' = \{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1},\ P^2 \mid f(a)\} \tag{4·2}$$

$$N''' = \{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_1},\ P^2 \mid f(a)\}, \tag{4·3}$$

where m_0 and m_1 are appropriately chosen thresholds. Specifically, we take $m_1 = \lceil m/2 \rceil$, and m_0 will be chosen later.

Clearly $N \subseteq N' \subseteq N \cup N'' \cup N'''$, hence $\#N' - \#N'' - \#N''' \leq \#N \leq \#N'$. We would therefore like to show that $\#N' = c_f q^m(1 + o(1))$ and $\#N'', \#N''' = o(c_f q^m)$. Before we proceed to prove these estimates, we need to establish bounds on certain sums and products related to f.

4·1. *Bounds on the singular sum*

We define the *singular sum* of the polynomial f as $S = \sum_{P \in \mathcal{P}} \rho(P^2)/||P||^2$. We also denote the tail of this series by $S(m_0) = \sum_{P \in \mathcal{P}^{\geq m_0}} \rho(P^2)/||P||^2$. Our goal in this section is to prove the following bounds on S, $S(m_0)$ and c_f:

LEMMA 4·1. *Let q be a fixed prime power, $k > 0$ a fixed integer, and n, m_0 varying integers with $n \to \infty$. Let $f \in \mathbb{F}_q[t][x]$ be a square-free polynomial with $\deg_x f \leq k$ and $\deg_t f \leq n$. Define $\rho(D)$, S, $S(m_0)$, c_f as above. We have the following asymptotic inequalities*:

$$S \leq k \ln\log_q n + O(1) = O(\ln\ln n), \tag{4·4}$$

$$S(m_0) = O\left(\frac{n}{m_0 q^{m_0}}\right), \tag{4·5}$$

$$c_f \gg (\log_q n)^{-2k}. \tag{4·6}$$

Write $f(t,x) = f_i(t,x) f_s(t,x)$ where $f_i(t,x)$ is the product of all irreducible factors of $f(t,x)$ which are inseparable in x, and $f_s(t,x)$ has no x-inseparable factors. Note that irreducible polynomials which are inseparable in x are in fact polynomials in x^p, thus their

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

product f_i is in $\mathbb{F}_q[t][x^p]$ as well. From the fact that $f(t,x)$ is square-free, we immediately see that f_i, f_s are co-prime and square-free, and furthermore f_i is co-prime to $\partial f_i/\partial t$ and f_s is co-prime to $\partial f_s/\partial x$: Indeed, if $P(t,x)$ is an irreducible common divisor of f_s and $\partial f_s/\partial x$, it is easy to see that either $P^2 \mid f_s$, which contradicts f_s being square-free, or else $P \mid \partial P/\partial x$, which then implies that P is inseparable in x – contradicting the fact that f_s has no inseparable factors. Similarly, if $P(t,x)$ is an irreducible common divisor of f_i, $\partial f_i/\partial t$, then again either $P^2 \mid f_i$, which leads to contradiction, or P is inseparable in t. Since both f_i, $\partial f_i/\partial t$ are in $\mathbb{F}_q[t][x^p]$, either P^p must also be a common divisor, contradicting square-freedom, or P is also in $\mathbb{F}_q[t][x^p]$. But since it is also inseparable in t, it follows that $P \in \mathbb{F}_q[t^p, x^p]$, which means that P is a p-th power, contradicting its irreducibility.

Now, define $R(t) = \operatorname{Res}_x(f_i, \partial f/\partial t)\operatorname{Res}_x(f_s, \partial f/\partial x) \in \mathbb{F}_q[t]$, where Res_x is the resultant in the x-variable. Note that $R(t)$ is non-zero: Indeed, by the above claims, $\partial f/\partial t = f_s\partial f_i/\partial t + f_i\partial f_s/\partial t$ is co-prime to f_i, and $\partial f/\partial x = f_i\partial f_s/\partial x + f_s\partial f_i/\partial x$ is co-prime to f_s. Note that the x- and t-degrees of the polynomials f_i, f_s and their derivatives are all at most k and n, respectively. Therefore, both resultants can be given as polynomials of degree at most $2k$ in the $\mathbb{F}_q[t]$-coefficients of their arguments, each of which is of degree at most n. Therefore $\deg R \le 4kn = O(n)$. In particular R has at most $4kn/m_0$ prime factors of degree at least m_0.

For any prime $P \in \mathcal{P}$ such that $P \nmid R$, the residue $f \bmod P \in (\mathbb{F}_q[t]/(P))[x]$ is non-trivial (as every prime dividing the content[3] of f also divides R). The residue also has degree $\le k$, which then implies $\rho(P) \le k$. Let $a \in \mathbb{F}_q[t]$ represent a residue class in $\rho(P)$, i.e. satisfy $f(a) \equiv 0 \pmod P$. If furthermore $\partial f(a)/\partial x \not\equiv 0 \pmod P$, then by Hensel's lemma there is a unique lifting of a to a residue $\tilde{a} \bmod P^2$ satisfying $\tilde{a} \equiv a \pmod P$, $f(\tilde{a}) \equiv 0 \pmod{P^2}$.

If, on the other hand, $\partial f(a)/\partial x \equiv 0 \pmod P$, then P does not divide $f_s(a)$: Otherwise, a is a common root of f_s and $\partial f/\partial x$ modulo P, which then implies $P \mid \operatorname{Res}_x(f_s, \partial f/\partial x)$, contradicting $P \nmid R$. From $P \mid f(a) = f_s(a)f_i(a)$ it then follows that $P \mid f_i(a)$, and by the same argument as above, we must then have $\partial f(a)/\partial t \not\equiv 0 \pmod P$, and thus

$$\frac{\mathrm{d}f(t,a(t))}{\mathrm{d}t} = \frac{\partial f}{\partial t}(a) + \frac{\partial f}{\partial x}(a)\frac{\mathrm{d}a}{\mathrm{d}t} \equiv \frac{\partial f}{\partial t}(a) \not\equiv 0 \pmod P.$$

In particular, it follows that $P(t)^2 \nmid f(t,a(t))$, for any such a. Therefore no residue $\tilde{a} \bmod P^2$ with $\tilde{a} \equiv a \pmod P$ satisfies $f(\tilde{a}) \equiv 0 \pmod{P^2}$.

We have shown that for every residue $a \bmod P \in \rho(P)$, there is at most one lifting modulo P^2 which is in $\rho(P^2)$, assuming $P \nmid R$. Therefore for such primes, $\rho(P^2) \le \rho(P) \le k$.

The contribution of these primes to S is thus at most

$$\sum_{P\in\mathcal{P}:P\nmid R} \frac{\rho(P^2)}{||P||^2} \le \sum_{P\in\mathcal{P}} \frac{k}{||P||^2} = \sum_{d=1}^{\infty}\sum_{P\in\mathcal{P}^{=d}} \frac{k}{q^{2d}}$$
$$\le \sum_{d=1}^{\infty} \frac{k}{q^{2d}}\frac{q^d}{d} = k\sum_{d=1}^{\infty}\frac{1}{dq^d} \le \frac{k}{q-1} = O(1),$$

[3]The *content* of a polynomial is the greatest common divisor of its coefficients. In our case, for $f \in \mathbb{F}_q[t][x]$ considered as a polynomial in x, the content is an element of $\mathbb{F}_q[t]$. In particular, $P \in \mathbb{F}_q[t]$ divides the content of f in $\mathbb{F}_q[t]$ if and only if P divides f in $\mathbb{F}_q[t][x]$.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

and similarly their contribution to the tail $S(m_0)$ is at most

$$\sum_{P\in\mathcal{P}^{\geq m_0}:P\nmid R}\frac{\rho(P^2)}{||P||^2}\leq k\sum_{d=m_0}^{\infty}\frac{1}{dq^d}=O\left(\frac{1}{m_0q^{m_0}}\right).$$

On the other hand, for any prime $P\mid R$, we have $\rho(P^2)\leq k||P||$. Indeed, if P divides the content of f, then $f/P\in(\mathbb{F}_q[t]/(P))[x]$ is non-trivial, as f is square-free and in particular $P^2\nmid f$. Thus

$$\begin{aligned}\rho(P^2)&=\#\{a \bmod P^2 : f(a)\equiv 0 \pmod{P^2}\}\\&=\#\{a \bmod P^2 : \frac{f(a)}{P}\equiv 0 \pmod{P}\}\\&=\#\{a \bmod P : \frac{f(a)}{P}\equiv 0 \pmod{P}\}\cdot||P||\leq k||P||,\end{aligned}$$

while for primes $P\mid R$ that do not divide the content, we simply have $\rho(P)\leq k$ and therefore $\rho(P^2)\leq||P||\rho(P)\leq k||P||$.[4]

Therefore the contribution of the primes $P\mid R$ to the sum $S(m_0)$ is at most

$$\begin{aligned}\sum_{\substack{P\in\mathcal{P}^{\geq m_0}\\P\mid R}}\frac{\rho(P^2)}{||P||^2}&\leq\sum_{\substack{P\in\mathcal{P}^{\geq m_0}\\P\mid R}}\frac{k||P||}{||P||^2}=\sum_{\substack{P\in\mathcal{P}^{\geq m_0}\\P\mid R}}\frac{k}{||P||}\\&\leq\sum_{\substack{P\in\mathcal{P}^{\geq m_0}\\P\mid R}}\frac{k}{q^{m_0}}\leq\frac{4kn}{m_0}\frac{k}{q^{m_0}}=O\left(\frac{n}{m_0q^{m_0}}\right).\end{aligned}$$

In order to obtain a bound on their contribution to S, denote for all $d>0$, $u_d=\#\{P\in\mathcal{P}^{=d}:P\mid R\}$, and let $x_d=du_d$. The contribution to S is

$$\sum_{\substack{P\in\mathcal{P}\\P\mid R}}\frac{\rho(P^2)}{||P||^2}\leq\sum_{\substack{P\in\mathcal{P}\\P\mid R}}\frac{k}{||P||}=k\sum_{d=1}^{\infty}\frac{u_d}{q^d}=k\sum_{d=1}^{\infty}\frac{x_d}{dq^d}.$$

Note that for all $d>0$, $du_d\leq d\pi_q(d)\leq q^d$, and $\sum_{d=1}^{\infty}du_d\leq\deg R\leq 4kn$. We will bound the expression $W=\sum_{d=1}^{\infty}x_d/(dq^d)$, which can be seen as a weighted sum of the x_d, by finding its maximum under the constraints $0\leq x_d\leq q^d$, $\sum_{d=1}^{\infty}x_d\leq 4kn$. Observe that since the weights $1/(dq^d)$ are positive, W always grows when any x_d is increased, so we will have $\sum_{d=1}^{\infty}x_d=4kn$; and, since, the weights $1/dq^d$ are strictly decreasing, W always grows when any x_d is increased at the expense of $x_{d'}$ for $d<d'$. Thus, to maximize W, we should have the first terms of (x_d) be as large as possible, until the bound on the sum $\sum_{d=1}^{\infty}x_d$ is exhausted, with latter terms being 0. In other words, we will have $x_d=q^d$ for all $d<n_0$, $x_{n_0}=4kn-\sum_{d=1}^{n_0-1}q^d$, and $x_d=0$ for all $d>n_0$, where the threshold n_0 is uniquely determined by the constraint $0\leq x_{n_0}\leq q^{n_0}$. These (x_d) would not necessarily correspond to any actual R, but will serve for obtaining an upper bound. It follows that $q^{n_0-1}\leq 4kn$, hence $n_0\leq\log_q(4kqn)=\log_q(n)+O(1)$. Thus

[4]A sharper argument shows that for primes $P\mid R$ that do not divide the content, we in fact have $\rho(P^2)\leq k||P||/2$, as any root of f modulo P that lifts to $||P||$ roots modulo P^2 must be a double root modulo P, and there can be only $k/2$ distinct double roots modulo P. This could allow us to slightly improve the lower bound on c_f for content-free polynomials, but not in general.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

$$\sum_{\substack{P\in\mathcal{P}\\ P|R}} \frac{\rho(P^2)}{||P||^2} \le k\sum_{d=1}^{\infty}\frac{x_d}{dq^d} \le k\sum_{d=1}^{n_0}\frac{1}{d} = k(\ln(n_0)+O(1))$$
$$= O(\ln\ln n).$$

It is quite clear that for both S, $S(m_0)$, the bounds for the contributions of $P \mid R$ dominate those of $P \nmid R$, and yield the bounds (4·4), (4·5).

We now derive the lower bound $c_f \gg (\log_q n)^{-k-o(1)}$ using the upper bound on S. Let $\epsilon > 0$, and split the summands of S into those greater and lesser than ϵ. As each term is at most $k/||P||$, it follows that only boundedly many are greater than ϵ, and the polynomials appearing in these terms are of bounded degree, thus the contribution of these terms to the product $c_f = \prod_{P\in\mathcal{P}}\left(1-\rho(P^2)/||P||^2\right)$ would be bounded from below by some positive constant $C'_\epsilon = C'_{k,q,\epsilon} > 0$ independent of n (assuming no local obstructions exist, so that $1-\rho(P^2)/||P||^2 \ge 1/||P||^2$ for all P). On the other hand, for summands such that $x = \rho(P^2)/||P||^2 < \epsilon$, we have the inequality $\ln(1-x) > -x/(1-\epsilon)$, and hence the contributions of these terms to the product c_f is bounded from below by $\exp\left(-\frac{S}{1-\epsilon}\right) \gg_{k,q} (\log_q n)^{-k/(1-\epsilon)}$. Taking the two terms together then yields $c_f \gg_{k,q} C'_\epsilon(\log_q n)^{-k+O(\epsilon)}$. As C'_ϵ is independent of n, letting $\epsilon \to 0$ sufficiently slowly as $n \to \infty$ would allow us to replace the bound by the aforementioned $c_f \gg (\log_q n)^{-k-o(1)}$. However, the exact exponent will have negligible relevance to our computations, and the bound (4·6) obtained by choosing $\epsilon = 1/2$ suffices for most purposes.

4·2. *Bounding N'': medium primes*

The bound on the medium primes is the easiest of the three, and follows immediately from a simple union bound. Indeed, m_1 is chosen such that for any prime $P \in \mathcal{P}^{<m_1}$ we have $\deg(P^2) < m$ and thus $\#\{a \in \mathbb{F}_q[t]^{<m} : P^2 \mid f(a)\} = \rho(P^2)q^m/||P||^2$. Therefore

$$\begin{aligned}
\#N'' &= \#\{a\in\mathbb{F}_q[t]^{<m} : \exists P\in\mathcal{P}^{\ge m_0}\cap\mathcal{P}^{<m_1},\ P^2 \mid f(a)\}\\
&= \#\bigcup\nolimits_{P\in\mathcal{P}^{\ge m_0}\cap\mathcal{P}^{<m_1}}\{a\in\mathbb{F}_q[t]^{<m} : P^2\mid f(a)\}\\
&\le \sum\nolimits_{P\in\mathcal{P}^{\ge m_0}\cap\mathcal{P}^{<m_1}}\#\{a\in\mathbb{F}_q[t]^{<m} : P^2\mid f(a)\}\\
&= \sum\nolimits_{P\in\mathcal{P}^{\ge m_0}\cap\mathcal{P}^{<m_1}}\frac{\rho(P^2)}{||P||^2}q^m\\
&\le q^m\sum\nolimits_{P\in\mathcal{P}^{\ge m_0}}\frac{\rho(P^2)}{||P||^2} = q^m S(m_0).
\end{aligned}$$

It now suffices to choose m_0 large enough so that $S(m_0) = o(c_f)$. By (4·5), (4·6), we see that we may take any m_0 such that $m_0 q^{m_0}/(n(\log_q n)^{2k}) \to \infty$, which is clearly satisfied when e.g. $m_0 - \log_q n - 2k\log_q\log_q n \to \infty$. For simplicity, we shall either weaken this condition to $m_0 \ge 1.01\log_q n$ as $n\to\infty$, or just assume $m_0 \to \infty$ if n is bounded.

4·3. *Bounding N': small primes*

We write $\mathcal{P}(m_0) = \prod_{P\in\mathcal{P}^{<m_0}} P$. We evaluate the size of N' by inclusion-exclusion:

$$\#N' = \sum_{D\mid\mathcal{P}(m_0)}\mu(D)\#\{a\in\mathbb{F}_q[t]^{<m} : D^2\mid f(a)\}.$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

For any square-free polynomial $D \in \mathbb{F}_q[t]$, let $\nu(D)$ be the number of its prime factors. For a non-negative integer j, define

$$n_j = \sum_{\substack{D|P(m_0) \\ \nu(D)=j}} \#\{a \in \mathbb{F}_q[t]^{<m} : D^2 \mid f(a)\}$$

so that $\#N' = \sum_{k=0}^{\infty}(-1)^j n_j$. Brun's sieve is essentially the observation that the partial sums $N_r = \sum_{j=0}^{r}(-1)^j n_j$ alternate around the limit $\#N'$, i.e. $\#N' \le N_r$ for all even r, and $\#N' \ge N_r$ for all odd r [**1**, chapter 6]. It will therefore suffice to prove that $N_r = c_f q^m(1+o(1))$ for some values of r in a range that includes both even and odd numbers, which will then result in both upper and lower bounds on $\#N'$.

Suppose m_0, r satisfy $2m_0 r \le m$. It follows that for any $D \mid P(m_0)$ with $\nu(D) \le r$ we have $\deg(D^2) < 2m_0 r \le m$. Such D then satisfies

$$\#\{a \in \mathbb{F}_q[t]^{<m} : D^2 \mid f(a)\} = \rho(D^2) q^{m-2\deg D}.$$

Therefore for all $j \le r$, we have $n_j = \sum_{D|P(m_0),\nu(D)=j} \rho(D^2) q^{m-2\deg D}$, hence

$$N_r = q^m \sum_{\substack{D|P(m_0) \\ \nu(D)\le r}} \mu(D)\frac{\rho(D^2)}{||D||^2} =: q^m U(r, m_0).$$

We now wish to estimate $U(r, m_0)$. Note that

$$\begin{aligned} U(\infty, m_0) &= \sum_{D|P(m_0)} \mu(D)\frac{\rho(D^2)}{||D||^2} = \prod_{P\in\mathcal{P}^{<m_0}} \left(1 - \frac{\rho(P^2)}{||P||^2}\right) \\ &= c_f \prod_{P\in\mathcal{P}^{\ge m_0}} \left(1 - \frac{\rho(P^2)}{||P||^2}\right)^{-1} = c_f(1 + O(S(m_0))) = c_f(1+o(1)), \end{aligned}$$

where in the last step we assume m_0 is chosen such that $S(m_0) = o(c_f)$, as was already required for bounding $\#N''$, so in particular $S(m_0) = o(1)$.

It will thus suffice to bound $U(\infty, m_0) - U(r, m_0)$. Let us denote for any non-negative integer j, $v_j = \sum_{D|P(m_0),\nu(D)=j} \rho(D^2)/||D||^2$. Note that v_j is the jth elementary symmetric polynomial of the finite multiset $\left\{\rho(P^2)/||P||^2 : P \in \mathcal{P}^{<m_0}\right\}$, whose elements are positive real numbers. It follows that $v_j \le \frac{v_1^j}{j!}$ (e.g. by expanding the power v_1^j). Furthermore, v_1 is a partial sum of the singular sum S, hence $v_1 \le \lambda$, where $\lambda = k \ln\log_q n + O(1)$ is the right-hand side of (4·4). Suppose $r = \alpha\lambda$ for some $\alpha > 2$. Then

$$\begin{aligned} |U(\infty, m_0) - U(r, m_0)| &= \left|\sum_{j=r+1}^{\infty}(-1)^j v_j\right| \le \sum_{j=r+1}^{\infty} v_j \le \sum_{j=r+1}^{\infty}\frac{\lambda^j}{j!} \\ &< \sum_{j=r+1}^{\infty}\frac{\lambda^r}{r!}\alpha^{r-j} < \frac{\lambda^r}{r!} < \frac{\lambda^r}{(r/e)^r} = \left(\frac{e\lambda}{r}\right)^r = \left(\frac{e}{\alpha}\right)^{\alpha\lambda} \\ &= O\left((\log_q n)^{-\alpha\ln(\alpha/e)k}\right). \end{aligned}$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Now if $\alpha \ln(\alpha/e)$ is sufficiently large[5], then by (4·6),

$$|U(\infty, m_0) - U(r, m_0)| \ll (\log_q n)^{-k\alpha \ln(\alpha/e)} = o(c_f).$$

We have thus shown that if our choice of r satisfies both $r \geq 4.4\lambda$ and $r \to \infty$, then $N_r = q^m c_f(1 + o(1))$, hence also $\#N' = c_f q^m(1 + o(1))$, as claimed.

For the proofs of the bounds on N', N'' to be valid simultaneously, we must be able to choose m_0, r sufficiently large satisfying $2m_0 r \leq m$. This is the source of our conditions $m \geq C_{k,q} \log_q n \log_q \log_q n$ and $m \to \infty$ in Theorem 2·2. Indeed, in the unbounded case $n \to \infty$ we may take $m_0 = \lceil 1.01 \log_q n \rceil$ and $r \in \{r_0, r_0 + 1\}$, where $r_0 = \lceil 4.45k \ln q \cdot \log_q \log_q n \rceil \geq 4.4\lambda$, which would satisfy all assumptions for sufficiently large n; whereas for bounded n, we may take for example $m_0 = r_0 = \lfloor \sqrt{m/2} \rfloor \to \infty$.

4·4. *Bounding N''': large primes*

The large primes require the most sophistication to estimate, though they contribute the smallest error. To do so, we apply Poonen's technique of replacing our target polynomial by an equivalent multivariate polynomial with a simpler t-derivative, and carefully retrace Lando's bounds on the corresponding contributions to N''', noting the size of our coefficients.

Given the polynomial $f(x) \in \mathbb{F}_q[t][x]$, define a new polynomial F by $F(y_0, \ldots, y_{p-1}) = f(y_0^p + t y_1^p + \cdots + t^{p-1} y_{p-1}^p) \in \mathbb{F}_q[t][y_0^p, y_1^p, \ldots, y_{p-1}^p]$. Note that $\deg_x(f) \leq k$, $\deg_t(f) \leq n$ together imply a bound on F's coefficients and degrees: $\deg_t(F) < n + pk = O(n)$, $\deg_{y_i}(F) \leq pk$.

Poonen's lemmas show that f being square-free implies F is, also [**8**, lemma 7·2]; which in turn implies that F and $G = \partial F/\partial t$ are coprime [**8**, lemma 7·3][6]. On the other hand, for any $y \in (\mathbb{F}_q[t])^p$, $P^2 \mid F(y)$ if and only if $P \mid F(y)$ and $P \mid G(y)$. This is due to the fact that, as the y_i-s appear in F only with exponents divisible by p, $G(y) = \mathrm{d}(F(y))/\mathrm{d}t$ for all y. Finally observe that $\deg_t G \leq \deg_t F = O(n)$, $\deg_{y_i}(G) \leq \deg_{y_i}(F) \leq pk$.

Let $m_p = \lceil m/p \rceil \leq \lceil m/2 \rceil = m_1$, and for any positive integer l, let $B_l = (\mathbb{F}_q[t]^{<m_p})^{l+1}$. Note that when we let the p-tuple y range over all B_{p-1}, $a = y_0^p + t y_1^p + \cdots + t^{p-1} y_{p-1}^p$ ranges over all $\mathbb{F}_q[t]^{<pm_p}$, which contains $\mathbb{F}_q[t]^{<m}$. Thus

$$\begin{aligned}
\#N''' &= \#\{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_1},\ P^2 \mid f(a)\} \\
&\leq \#\{y \in B_{p-1} : \exists P \in \mathcal{P}^{\geq m_1},\ P^2 \mid f(y_0^p + t y_1^p + \cdots + t^{p-1} y_{p-1}^p)\} \\
&= \#\{y \in B_{p-1} : \exists P \in \mathcal{P}^{\geq m_1},\ P^2 \mid F(y)\} \\
&= \#\{y \in B_{p-1} : \exists P \in \mathcal{P}^{\geq m_1},\ P \mid F(y) \text{ and } P \mid G(y)\} \\
&= O_{p-1,pk}\left(\frac{n + m_1}{m_1} q^{(p-1)m_p}\right) = O_{p,k}\left(\frac{n+m}{m q^{\frac{m}{p} - p}} q^m\right),
\end{aligned} \tag{4·7}$$

[5] In the case $n \to \infty$ it suffices to choose $\alpha \ln(\alpha/e) > 2$, which holds for $\alpha > 4.32$. If n is bounded, take $\alpha \to \infty$.

[6] Poonen in fact shows only that they are coprime in $\mathbb{F}_q(t)[y_0, \ldots, y_{p-1}]$, whereas we need them to be coprime in $\mathbb{F}_q[t][y_0, \ldots, y_{p-1}]$. This is easy to verify – it is enough to check that they have no common irreducible factor $P \in \mathbb{F}_q[t]$. Such a factor will necessarily divide the contents of both $F(y_0, 0, \ldots, 0) = f(y_0^p)$ and $G(y_0, 0, \ldots, 0) = (\partial f/\partial t)(y_0^p)$. This in turn implies that P^2 divides f, contradicting our assumption that it is square-free.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

where the bound in the final line follows from the following proposition, analogous to [7, proposition 5]:

PROPOSITION 4·2. *Let k, l, n, m_p, m_1 be positive integers with $m_1 \geq m_p$, and let $F, G \in \mathbb{F}_q[t][y_0, \ldots, y_l]$ be coprime polynomials in $l+1$ variables with $\deg_{y_i}(F), \deg_{y_i}(G) \leq k$ and $\deg_t(F), \deg_t(G) \leq n$. Denote $B_l = (\mathbb{F}_q[t]^{<m_p})^{l+1}$ as above, and define*

$$\mathcal{N}_l(F, G) = \#\{y \in B_l : \exists P \in \mathcal{P}^{\geq m_1},\ P \mid F(y) \text{ and } P \mid G(y)\}.$$

Then

$$\mathcal{N}_l(F, G) = O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right).$$

Thus, from (4·7) and (4·6), it follows that $\#N''' = o(c_f q^m)$ when e.g. $m - p(\log_q n + 2k \log_q \log_q n) \to \infty$, which is certainly the case under the assumptions of Theorem 2·2.

Before we prove proposition 4·2, we first need a simpler bound, slightly generalising [7, proposition 6] and giving exact bounds.

PROPOSITION 4·3. *Let k, l, n, m_p, F, B_l be as in Proposition 4·2, and suppose F is not identically 0. Then*

$$\#\{y \in B_l : F(y) = 0\} \leq k(l+1)q^{lm_p}.$$

Proof. If $l = 0$, then $F(y_0)$ is a non-vanishing polynomial of degree at most k in y_0. Hence it has at most k roots in all of $\mathbb{F}_q[t]$, and in particular $\#\{y \in B_0 : F(y) = 0\} \leq k$, as claimed.

We proceed by induction on l. Consider F as a polynomial in y_l, of degree at most k, with coefficients in $\mathbb{F}_q[t][y_0, \ldots, y_{l-1}]$. We write it as $F(y', y_l)$, where $y' = (y_0, \ldots, y_{l-1})$. Let $F_0 \in \mathbb{F}_q[t][y_0, \ldots, y_{l-1}]$ be its leading coefficient. Clearly, F_0 also satisfies the degree requirements of Proposition 4·3, hence by induction,

$$\#\{y' \in B_{l-1} : F_0(y') = 0\} \leq klq^{(l-1)m_p}. \tag{4·8}$$

On the other hand, for any $y' \in B_{l-1}$ with $F_0(y') \neq 0$, there are at most $\deg_{y_l}(F) \leq k$ values of y_l in all $\mathbb{F}_q[t]$ for which $F(y', y_l) = 0$. Thus

$$\#\{(y', y_l) \in B_l : F_0(y') \neq 0,\ F(y', y_l) = 0\} \leq k\#B_{l-1} = kq^{lm_p}. \tag{4·9}$$

Using both (4·8), (4·9), we finally obtain

$$\begin{aligned}
&\#\{(y', y_l) \in B_l : F(y', y_l) = 0\} \\
&\quad \leq \#\{(y', y_l) \in B_l : F_0(y') = 0\} + \#\{(y', y_l) \in B_l : F_0(y') \neq 0,\ F(y', y_l) = 0\} \\
&\quad = q^{m_p}\#\{y' \in B_{l-1} : F_0(y') = 0\} + \#\{(y', y_l) \in B_l : F_0(y') \neq 0,\ F(y', y_l) = 0\} \\
&\quad \leq q^{m_p} klq^{(l-1)m_p} + kq^{lm_p} = k(l+1)q^{lm_p}.
\end{aligned}$$

Using exactly the same arguments, one can also show the following similar proposition:

PROPOSITION 4·4. *Let $k, l, n, m_p, m_1, F, B_l$ be as in Proposition 4·2, let $P \in \mathcal{P}^{\geq m_1}$ be a large prime and suppose F is not identically 0 modulo P. Then*

$$\mathcal{N}_l(F, P) = \#\{y \in B_l : P \mid F(y)\} \leq k(l+1)q^{lm_p}.$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Note that we rely strongly on $m_1 \geq m_p$, which implies that each residue class modulo P has at most a single representative in $\mathbb{F}_q[t]^{<m_p}$. We omit the rest of the proof, which is just a repetition of the proof of Proposition 4·3.

Proof of Proposition 4·2. Again, we induct on l. To avoid repetition, our induction base will be $l = -1$, where $F, G \in \mathbb{F}_q[t]$, and $B_{-1} = \{()\}$ is a singleton containing only the empty tuple. The claim then immediately follows from F, G being coprime in $\mathbb{F}_q[t]$, i.e. $\nexists P \in \mathcal{P}$ such that $P \mid F$ and $P \mid G$, and in particular $\{y \in B_{-1} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid F(y) \text{ and } P \mid G(y)\}$ is empty. Hence $\mathcal{N}_l(F, G) = 0 = O_k((n + m_1)q^{-m_p}/m_1)$.

We denote $A_l = \mathbb{F}_q[t][y_0, \ldots, y_{l-1}]$. Consider $F, G \in A_l[y_l]$ as single variable polynomials in y_l with coefficients in the polynomial ring A_l, and let $F_C, G_C \in A_l$ be their respective contents. We may then write $F = F_C F_I$, $G = G_C G_I$ where $F_I, G_I \in A_l[y_l]$ are indivisible by any non-scalar polynomial in A_l. Clearly F_C, F_I are coprime to G_C, G_I, and all four polynomials have y_i-degrees at most k and t-degrees at most n. We also have

$$\mathcal{N}_l(F, G) \leq \mathcal{N}_l(F_I, G_I) + \mathcal{N}_l(F_I, G_C) + \mathcal{N}_l(G_I, F_C) + \mathcal{N}_l(F_C, G_C).$$

Therefore it is enough to show that each of the four summands on the right hand side is bounded by $O_{l,k}((n + m_1)q^{lm_p}/m_1)$.

Note that, as both F_C and G_C are independent of y_l, and by the induction hypothesis, we have

$$\begin{aligned}\mathcal{N}_l(F_C, G_C) = q^{m_p}\mathcal{N}_{l-1}(F_C, G_C) &= q^{m_p} O_{l-1,k}\left(\frac{n + m_1}{m_1} q^{(l-1)m_p}\right) \\ &= O_{l,k}\left(\frac{n + m_1}{m_1} q^{lm_p}\right).\end{aligned}$$

For both $\mathcal{N}_l(G_I, F_C), \mathcal{N}_l(F_I, G_C)$, we have one polynomial in A_l and the second indivisible by any polynomial in A_l. We wish to bound $\mathcal{N}_l(F_I, G_I)$ by a term of this form as well. To do so, let $H = \mathrm{Res}_{y_l}(F_I, G_I) \in A_l$ be the resultant of F_I, G_I. By basic properties of the resultant, for any choice of $y \in B_l$, $P \in \mathcal{P}$, we have $P \mid F_I(y), P \mid G_I(y) \implies P \mid H(y)$. Thus $\mathcal{N}_l(F_I, G_I) \leq \mathcal{N}_l(F_I, H)$. Further note that from $\deg_{y_l}(F_I), \deg_{y_l}(G_I) \leq k$ it follows that H is given as a polynomial of degree $\leq 2k$ in the A_l coefficients of F_I, G_I, hence in particular $\deg_t(H) \leq 2kn$, $\deg_{y_i}(H) \leq 2k^2$. Also note that H is non-zero, as F_I, G_I are co-prime.

We now claim that for any pair of polynomials $F_I \in A_l[y_l]$, $H \in A_l$ such that F_I is indivisible by non-scalar polynomials in A_l, and with $\deg_t F_I \leq n$, $\deg_{y_i} F_I \leq k$ and $\deg_t H \leq 2kn$, $\deg_{y_i} H \leq 2k^2$, we have $\mathcal{N}_l(F_I, H) = O_{l,k}((n + m_1)q^{lm_p}/m_1)$. These assumptions also hold for the pairs (F_I, G_C) and (G_C, F_I), yielding bounds on $\mathcal{N}_l(F_I, G_C), \mathcal{N}_l(G_I, F_C)$ and $\mathcal{N}_l(F_I, G_I)$, finishing our induction step.

Let $H = \prod_{j \in J} H_j$ be H's decomposition into irreducible polynomials. We have $\mathcal{N}_l(F_I, H) \leq \sum_{j \in J} \mathcal{N}_l(F_I, H_j)$. Note that for each j, $H_j \in A_l$, therefore $H_j \nmid F_I$ and F_I, H_j are coprime. Let us partition $J = J_1 \cup J_2 \cup J_3$, where $J_1 = \{j \in J : H_j \notin \mathbb{F}_q[t]\}$, $J_2 = \{j \in J : H_j \in \mathbb{F}_q[t]^{\geq m_1}\}$, and $J_3 = \{j \in J : H_j \in \mathbb{F}_q[t]^{<m_1}\}$. As $\deg_t H \leq 2kn$ and the total degree of H in all y-variables is at most $2k^2 l$, we have $\#J_2 \leq 2kn/m_1 = O_{l,k}(n/m_1)$ and $\#J_1 \leq 2k^2 l = O_{l,k}(1)$.

For each $j \in J_3$, $y \in B_l$, we have $H_j(y) = H_j$, so clearly $\nexists P \in \mathcal{P}^{\geq m_1}$ with $P \mid H_j$, hence $\mathcal{N}_l(F_I, H_j) = 0$. Similarly, for each $j \in J_2$, the conditions of proposition 4·4 are satisfied for $F = F_I$, $P = H_j$. Hence $\mathcal{N}_l(F_I, H_j) \leq k(l + 1)q^{lm_p} = O_{l,k}(q^{lm_p})$.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

Finally, for each $j \in J_1$, let $F_0 \in A_l$ be some coefficient of F_I (as a polynomial in y_l) such that $H_j \nmid F_0$ as polynomials. Such a coefficient must exist as $H_j \nmid F_I$. We now bound $\mathcal{N}_l(F_I, H_j)$, again by splitting into three trivially covering sets:

$$\begin{aligned}\mathcal{N}_l(F_I, H_j) &= \#\{y \in B_l : \exists P \in \mathcal{P}^{\geq m_1},\ P \mid F_I(y) \text{ and } P \mid H_j(y)\} \\ &\leq \#\{y \in B_l : H_j(y) = 0\} \\ &\quad + \#\{y \in B_l : \exists P \in \mathcal{P}^{\geq m_1},\ P \mid F_0(y) \text{ and } P \mid H_j(y)\} \\ &\quad + \#\{y \in B_l : H_j(y) \neq 0, \exists P \in \mathcal{P}^{\geq m_1},\ P \mid H_j(y),\ P \mid F_I(y) \text{ and } P \nmid F_0(y)\}.\end{aligned}$$

By Proposition 4·3, the first summand is clearly $O_{l,k}(q^{lm_p})$. The second summand, by definition, is $\mathcal{N}_l(F_0, H_j)$. As H_j is irreducible, it follows that F_0, H_j are coprime. We also certainly have $\deg_{y_i}(F_0), \deg_{y_i}(H_j) \leq 2k^2$ and $\deg_t(F_0), \deg_t(H_j) \leq 2kn$. Therefore F_0, H_j satisfy the conditions of Proposition 4·2, but with smaller l (albeit larger degrees). Hence by the induction hypothesis,

$$\begin{aligned}\mathcal{N}_l(F_0, H_j) = q^{m_p}\mathcal{N}_{l-1}(F_0, H_j) &= q^{m_p} O_{l-1,2k^2}\left(\frac{2kn + m_1}{m_1} q^{(l-1)m_p}\right) \\ &= O_{l,k}\left(\frac{n + m_1}{m_1} q^{lm_p}\right). \qquad (4\cdot10)\end{aligned}$$

To bound the third term, note that for each $y = (y', y_l) \in B_{l-1} \times B_0 = B_l$ such that $H_j(y) = H_j(y') \neq 0$, we must have $\deg_t(H_j(y')) \leq 2kn + 2k^2 l m_p$. If we let $\mathcal{P}_{y'} = \{P \in \mathcal{P}^{\geq m_1} : P \mid H_j(y'), P \nmid F_0(y')\}$, it follows that $\#\mathcal{P}_{y'} \leq (2kn + 2k^2 l m_p)/m_1 = O_{l,k}((n + m_1)/m_1)$. On the other hand, for each $y' \in B_{l-1}$, $P \in \mathcal{P}_{y'}$, $F_I(y', y_l)$ is a polynomial of degree $\leq k$ in y_l, which is non-vanishing modulo P. Since $\deg_t(P) \geq m_1 \geq m_p$, it follows that $\#\{y_l \in B_0 : P \mid F_I(y', y_l)\} \leq k$. Therefore

$$\begin{aligned}&\#\{y \in B_l : H_j(y) \neq 0, \exists P \in \mathcal{P}^{\geq m_1},\ P \mid H_j(y),\ P \mid F_I(y) \text{ and } P \nmid F_0(y)\} \\ &\quad = \sum_{\substack{y' \in B_{l-1} \\ H_j(y') \neq 0}} \#\{y_l \in B_0 : \exists P \in \mathcal{P}^{\geq m_1},\ P \mid H_j(y'),\ P \mid F_I(y', y_l) \text{ and } P \nmid F_0(y')\} \\ &\quad \leq \sum_{\substack{y' \in B_{l-1} \\ H_j(y') \neq 0}} \sum_{P \in \mathcal{P}_{y'}} \#\{y_l \in B_0 : P \mid F_I(y', y_l)\} \leq \sum_{\substack{y' \in B_{l-1} \\ H_j(y') \neq 0}} \sum_{P \in \mathcal{P}_{y'}} k \\ &\quad = \sum_{\substack{y' \in B_{l-1} \\ H_j(y') \neq 0}} O_{l,k}\left(\frac{n + m_1}{m_1}\right) = O_{l,k}\left(\frac{n + m_1}{m_1} q^{lm_p}\right).\end{aligned}$$

Taking the three results together, we find $\mathcal{N}_l(F_I, H_j) = O_{l,k}((n + m_1)q^{lm_p}/m_1)$ for all $j \in J_1$. Now combining the different bounds for each J_i, we finally obtain

$$\begin{aligned}\mathcal{N}_l(F_I, H) &\leq \sum_{j \in J_1} \mathcal{N}(F_I, H_j) + \sum_{j \in J_2} \mathcal{N}(F_I, H_j) + \sum_{j \in J_3} \mathcal{N}(F_I, H_j) \\ &= \sum_{j \in J_1} O_{l,k}\left(\frac{n + m_1}{m_1} q^{lm_p}\right) + \sum_{j \in J_2} O_{l,k}\left(q^{lm_p}\right) + \sum_{j \in J_3} 0\end{aligned}$$

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

$$\leq 2k^2 l \cdot O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right) + \frac{2kn}{m_1} \cdot O_{l,k}\left(q^{lm_p}\right)$$
$$= O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right),$$

as we wanted to show.

5. *Proofs of Theorems 2·4, 2·5*

5·1. *Proof of Theorem 2·4*

Define $f(x) = g(t, N(t)+x) \in \mathbb{F}_q[t][x]$. Clearly $\deg_x f = \deg_x g = k$, and $\deg_t f \leq \deg_x g \cdot \deg_t N + \deg_t g = kn + \deg_t g = O(n)$. Furthermore, as f is obtained from g simply by a fixed $\mathbb{F}_q[t]$ translation of the x variable, g being square-free implies that f is square-free, and more importantly, $\rho_f(D) = \rho_g(D) = \rho(D)$ for any polynomial D. Therefore they also have the same singular sum and series, i.e. $S_f(m_0) = S_g(m_0)$, as well as $S_f = S_g$ and $c_f = c_g$ being constants independent of the choice of $N(t)$ or its degree n. Thus taking any $m_0 \to \infty$, $r \to \infty$, we have immediately $S(m_0) = o(1) = o(c_f)$ and $r/S \to \infty$, from which we obtain $\#N' = c_f q^m (1+o(1))$ and $\#N'' = o(c_f q^m)$ following the proofs in Sections 4·3, 4·2. To be able to choose such r, m_0 satisfying $2m_0 r \leq m$, we only need $m \to \infty$.

We are left only with the need to validate the bound on N''', and here finally n does come into play, as it still affects the relevant degrees. As c_f is now a constant, (4·7) implies that $\#N''' = o(1) = o(c_f)$ when $mq^{m/p}/n \to \infty$, which is equivalent to $m - p(\log_q n - \log_q \log_q n) \to \infty$, as we required in the theorem's statement.

5·2. *Proof of Theorem 2·5*

Similarly to the above, we observe that when we move to $f(x) = g(N(t)+x)$, the expressions determined by the singular sum, S, $S(m_0)$ and c_f, will depend only on g and not on N. Thus the bounds (4·4)–(4·6) will all be valid with n replaced by n_1, as will the computations of Sections 4·2, 4·3, as long as we can choose $r, m_0 \to \infty$ with $m_0 \geq 1.01 \log_q n_1$, $r \geq 4.45k \ln \log_q n_1$ and $2m_0 r \leq m$, which is possible due to the assumptions $m \geq C_{k,q} \log_q n_1 \log_q \log_q n_1$ and $m \to \infty$.

For the bound on $\#N'''$, we observe that $\deg_t f \leq kn_2 + n_1$. If $n_2 \leq n_1$, then $\deg_t f \ll n_1$ and we are basically in the case of Theorem 2·2, where the contribution of N''' is negligible. Otherwise, $n_1 \leq n_2$, so $\deg_t f \ll n_2$. Thus (4·7) holds with the degree n replaced by n_2. Taken together with (4·6) with n replaced by n_1, we see that $\#N''' = o(c_f q^m)$ would follow from $mq^{m/p}/(n_2(\log_q n_1)^{2k}) \to \infty$, which is equivalent to

$$m - p(\log_q n_2 - \log_q \log_q n_2 + 2k \log_q \log_q n_1) \longrightarrow \infty$$

as we required.

Remark. We can in fact make a slight improvement here on the required condition: By using $c_f \gg (\log_q n_1)^{-k-o(1)}$ instead of (4·6), the constant coefficient $2k$ can be replaced with any constant greater than k, or with some (specific) function of the type $k + o(1)$.

Acknowledgements. The author wishes to thank Zeév Rudnick for proposing the problems which motivated the majority of this paper, as well as many helpful suggestions and

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

references. The author also thanks Alexei Entin, for contributing the appendix, and for suggesting the use of Brun's sieve, without which the results of this paper would have been far weaker. Finally, the author wishes to thank Andrew Granville and the anonymous referees for their valuable corrections and suggestions.

Appendix A. *On the Number of Squarefree Integers in Short Intervals*
By ALEXEI ENTIN

Abstract

Assuming the ABC conjecture we show that for any fixed $\epsilon > 0$ the number of squarefree integers in the interval $[x, x + H)$ is $\sim 6H/\pi^2$ provided $H > x^\epsilon$.

A·1. *Introduction*

We consider the problem of counting the number of squarefree integers in the interval $[x, x + H)$, where x and H are large positive real numbers. We are interested in the case that $H = x^\epsilon$ for some fixed $\epsilon > 0$ while $x \to \infty$. It is an open problem to show that for any fixed $\epsilon > 0$ there exists even a single squarefree integer in the interval $[x, x + H)$ with $H = x^\epsilon$ for large enough x. The best known result in this direction is due to Filaseta and Trifonov [3] who showed the existence of squarefree integers in $[x, x + H)$ for $H \gg x^{1/5} \log x$. It was shown by Tolev [11] that when $H/(x^{1/5} \log(x)) \to \infty$, the number of squarefrees in the interval $[x, x + H)$ is in fact asymptotic to $(6/\pi^2)H$. It was shown by Granville [4] that assuming the ABC conjecture for any fixed $\epsilon > 0$ there exists a squarefree integer in $[x, x + x^\epsilon)$ for x large enough. Our main result is the following:

THEOREM A·1. *Assume the ABC conjecture. Let $\epsilon > 0$ be fixed. Then the number of squarefree integers in the interval $[x, x + H)$ is $\sim 6H/\pi^2$ provided $H > x^\epsilon$.*

We note that $6/\pi^2 = \zeta(2)^{-1}$, where $\zeta(s)$ is the Riemann zeta-function. By essentially the same argument it can be shown that assuming the ABC conjecture for any fixed k the number of k-power-free integers in $[x, x + H)$ is $\sim \zeta(k)^{-1}H$ provided $H > x^\epsilon$ for fixed $\epsilon > 0$.

A·2. *Proof of Theorem A·1*

PROPOSITION A·2. *The number of integers in the interval $[x, x + H)$ which are not divisible by any square of a prime $p < H$ is $\sim 6H/\pi^2$ as $H \to \infty$.*

Proof. It is elementary to see that the number of integers in $[x, x + H)$ not divisible by p^2 for any $p < \log H/2$ is $\sim \zeta(2)^{-1}H = 6H/\pi^2$ (this is seen by exact sieving over all primes up to $\log H/2$). The number of integers in $[x, x + H)$ divisible by p^2 for some $\log H/2 < p < H$ is bounded by

$$\sum_{\frac{1}{2}\log H < p < H} \left(\frac{H}{p^2} + 1\right) \ll \frac{H}{\log H} = o(H),$$

which is asymptotically negligible.

We will need the following result due to Granville [4, theorem 6]:

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

PROPOSITION A·3. *Assume the ABC conjecture. Let $F(X) \in \mathbb{Z}[x]$ be a fixed squarefree polynomial and $\alpha > 0$ a fixed constant. Let y be a natural number and assume that $s^2 | F(y)$ for some natural number s. Then for y large enough we have $s \leq y^{1+\alpha}$.*

PROPOSITION A·4. *Assume the ABC conjecture. If $H < x$ and $H \to \infty$ then the number of integers in $[x, x+H)$ divisible by the square of any prime $p > x^{\epsilon}$ is $o(H)$.*

Proof. Let $\lambda > 0$ be a constant. Assume that the number of integers in $[x, x+H)$ divisible by p^2 for some prime $p > x^{\epsilon}$ is $> \lambda H$. We want to show that H must be bounded (for any fixed λ). Denote $N = \lceil 2/\epsilon \rceil$, $M = \lceil 2N/\lambda \rceil$ (these are both fixed constants for fixed ϵ, λ). The interval $[x, x+H)$ necessarily contains a subinterval $\left[y, y+M\right)$ with at least $\lambda M/2 \geq N$ (if M divides H the $1/2$ factor is unnecessary) elements divisible by some p^2 for some prime $p > x^{\epsilon} \gg y^{\epsilon}$.

Assuming by way of contradiction that H can be arbitrarily large, we see that there must exist arbitrarily large y s.t. at least N integers in the interval $\left[y, y+M\right)$ are divisible by a square of some prime $p \gg y^{\epsilon}$. By the pigeonhole principle there must exist some fixed distinct $a_1, ..., a_N \geq 0$ s.t. for infinitely many y each $y + a_1, ..., y + a_N$ is divisible by the square of some prime $p \gg y^{\epsilon}$.

Denote $F(X) = (X + a_1)...(X + a_N) \in \mathbb{Z}[x]$. This is a squarefree polynomial. From the above we see that for infinitely many y the value $F(y)$ is divisible by the square of some $d = p_1...p_N \gg y^{N\epsilon} \geq y^2$. But this contradicts Proposition A·3 (taking any $\alpha < 1$ in the proposition).

Combining Proposition A·2 and Proposition A·4 we deduce Theorem A·1.

REFERENCES

[1] A. C. COJOCARU and M. R. MURTY. *An Introduction to Sieve Methods and their Applications* (Cambridge University Press, 2005).
[2] T. ESTERMANN. Einige Sätze über quadratfreie Zahlen. *Math. Ann.* **105** (1931), 653–662.
[3] M. FILASETA and O. TRIFONOV. On gaps between squarefree numbers II. *J. London Math. Soc.* s**2-45** (1992), 215–221.
[4] A. GRANVILLE. ABC allows us to count squarefrees. *Int. Math. Res. Not.* **19** (1998), 991–1009.
[5] C. HOOLEY. On the square-free values of cubic polynomials. *J. Reine Angew. Math.* **229** (1968), 147–154.
[6] C. HOOLEY. *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics vol. 70 (Cambridge University Press, 1976).
[7] G. LANDO. Square-free values of polynomials evaluated at primes over a function field. *Q. J. Math.* **66** (2015), 905–924.
[8] B. POONEN. Squarefree values of multivariable polynomials. *Duke Math. J.* **118** (2003), 353–373.
[9] K. RAMSAY. Square-free values of polynomials in one variable over function fields. *Int. Math. Res. Not.* **4** (1992), 97–102.
[10] G. RICCI. Ricerche aritmetiche sui polinomi. *Rend. Circ. Mat. Palermo* **57** (1933), 433–475.
[11] D. I. TOLEV. On the distribution of r-tuples of squarefree numbers in short intervals. *Int. J. Number Theory* **2** (2006), 225–234.

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press

https://doi.org/10.1017/S0305004119000392 Published online by Cambridge University Press