# SHORT INTERVAL RESULTS FOR POWERFREE POLYNOMIALS OVER FINITE FIELDS

ANGEL KUMCHEV, NATHAN MCNEW, AND ARIANA PARK

Abstract. Let $k \geq 2$ be an integer and $\mathrm{F}^q$ be a finite field with $q$ elements. We prove several results on the distribution in short intervals of polynomials in $\mathrm{F}_q[x]$ that are not divisible by the $k$th power of any non-constant polynomial. Our main result generalizes a recent theorem by Carmon and Entin [1] on the distribution of squarefree polynomials to all $k \geq 2$. We also develop polynomial versions of the classical techniques used to study gaps$k$-free integers in Z. We apply these techniques to obtain analogues in $\mathrm{F}_q[x]$ of some

between classical theorems on the distribution of $k$-free integers. The latter results complement the main theorem in the case when the degrees of the polynomials are of moderate size.

## 1. Introduction

Recall that if $k \geq 2$ is a fixed integer, an integer $n$ is called $k$-free if $n$ is not divisible by the $k$th power of any prime. This is a generalization of the classical concept of a squarefree integer, which occurs in the special case when $k = 2$. Much work has been done studying the distribution of $k$-free integers in short intervals, especially in the squarefree case: see [2–10,12–15,18,21,22,24,26–28]. In particular, Filaseta and Trifonov [8] proved that there exists a constant $c > 0$ such that the interval $(x, x + cx^{1/5} \ln x]$ contains a squarefree integer for all sufficiently large $x$. Trifonov [28] further generalized this result to $k$-free integers for all $k \geq 2$. He showed that for some constant $c = c(k) > 0$, the interval $(x, x+cx^{1/(2k+1)} \ln x]$ contains a $k$-free integer when $x$ is sufficiently large. To the best of our knowledge, these are the sharpest unconditional upper bounds on the maximum gap between consecutive $k$-free numbers. Conditionally on the $abc$-conjecture, Granville [13] has shown that for any fixed $\varepsilon > 0$, the interval $(x, x + x^{\varepsilon}]$ contains squarefree integers for sufficiently large $x$.

There are many parallels between the arithmetic of Z and that of $\mathrm{F}_q[x]$, the ring of polynomials in $x$ over a finite field $\mathrm{F}_q$ with $q$ elements (see [19,23] for background on such research). In particular, a polynomial in $\mathrm{F}_q[x]$ is called *$k$-free* if it has no irreducible factors of multiplicity $k$ or higher; when $k = 2$, we call such a polynomial *squarefree*. One may expect to find ample existing research on analogues for polynomials from $\mathrm{F}_q[x]$ of the aforementioned research on the gap problem for $k$-free integers, but that does not appear to be the case. Indeed, a search of the literature on the distribution in short intervals of $k$-free polynomials over a finite field yields very limited results, almost entirely focused on the squarefree case.

Let $q = p^f$, with $p$ prime and $f \in \mathrm{N}$, be the cardinality of a finite field $\mathrm{F}_q$. Henceforth, we restrict $q$ to integers of this form. We let $\mathrm{M}_q$ denote the set of monic polynomials in $\mathrm{F}_q[x]$ and write $\mathrm{M}_q(d)$

for the subset of monic polynomials of degree $d$. When $F \in \mathrm{M}_q$ and $h < \deg F$, an interval in $\mathrm{F}_q[x]$ of length $h$ centered at $F$ is the set

$$\mathcal{I}_q(F,h) = \{Q \in \mathbb{F}_q[x] : \deg(F-Q) \le h\}. \tag{1}$$

In this paper, we study $k$-free polynomials in short intervals of this kind. To draw an analogy with short intervals $(x, x+h]$ in Z, we observe that when $F \in \mathrm{M}_q(n)$, the "size" of the polynomials in $\mathrm{I}_q(F,h)$ is $q^n$, whereas the number of polynomials in the interval is $q^{h+1}$. In particular, the interval is "short" whenever $0 < h \le n-2$. Thus, a proper analogue of a short interval $(x, x+h]$, where $x \to \infty$ and $h = O(x^\theta)$, $0 < \theta < 1$, is an interval $\mathrm{I}_q(F,h)$, where $q^n \to \infty$ and $h \le \theta n$.

Note that the condition $q^n \to \infty$ above can occur in different ways. For example, one may fix $n = \deg(F)$ and let $q \to \infty$. In this regime, the question was studied by Keating and Rudnick [17]. Drawing on earlier work by Rudnick [25] on the density of squarefree polynomials over $\mathrm{F}_q$, they showed that for any integers $h,n$ with $0 < h \le n-2$, one can take $q$ sufficiently large so that there exists a squarefree polynomial in every interval $\mathrm{I}_q(F,h)$, with $F \in \mathrm{M}_q(n)$. The theorem of Keating and Rudnick does not quantify how fast $q$ must grow in terms of $n$, but an examination of their proof suggests that it can be made effective to show that such a conclusion holds as long as $q > c(n+h)$ for some constant $c$.

In this paper, we focus on the case when $q$ is fixed and $n \to \infty$. The behavior of powerfree polynomials in this regime turns out to be quite different, and the analogy with Z is more direct. For example, in the case of gaps between squarefree integers, Erdős [2] proved long ago that the maximum gap is unbounded: there are arbitrarily large $x$ such that the interval $(x, x+h]$ contains no squarefree integers when

$$h \le \frac{c \ln x}{\ln \ln x}$$

for any constant $c$ such that $2c < \zeta(2)$. In §3, we establish a version of Erdős' result for polynomials over $\mathrm{F}_q$. If $\zeta_q(s) = (1-q^{1-s})^{-1}$ denotes the zeta-function of the ring $\mathrm{F}_q[x]$ (see [23, Ch. 2]), our result can be stated as follows.

**Theorem 1.** *Let $k \ge 2$ and $q \ge 2$ be fixed integers, and suppose that $c$ is any constant with $kc < \zeta_q(k)$. If $n$ is sufficiently large, there exist monic polynomials $F$ of degree at most $n$ such that the interval $\mathrm{I}_q(F,h)$ contains no $k$-free polynomials for any length $h$ such that*

$$q^{h+1} \le \frac{cn}{\log_q n}. \tag{1}$$

In the squarefree case $k = 2$, this is a direct analogue of Erdős' result, as stated by Erdős in [3]. To the best of our knowledge, for $k > 2$, the corresponding result for integers has never been formally stated, though it has been known to researchers in the field and can be extracted from the remarks in [3].

We include Theorem 1 and its proof here, since it transpires that in the study of $k$-free polynomials over $\mathrm{F}_q$, the upper bounds on the least $h$ (as $n \to \infty$) for which $\mathrm{I}_q(F,h)$ must contain a $k$-free polynomial come much closer to the lower barrier imposed by Theorem 1. Recently, Carmon and Entin [1] have shown that when

$$q^{h+1} > \left(\frac{g(n)n}{\log_q n}\right)^p, \tag{2}$$

where $g(n) \to \infty$ as $n \to \infty$, one can obtain an asymptotic formula for the number of squarefree polynomials in the interval $\mathrm{I}_q(F,h)$. They derive this result as a special case of a theorem on the density of squarefree values of bivariate polynomials over $\mathrm{F}_q$. In particular, their proof is considerably more elaborate than is necessary for the application to the gap problem considered here. In the special case of interest, we developed a much simplified variant of their method, which we present in §2.2; it yields a rather quick proof that when $n \to \infty$ and (2) holds with $g(n) = 1$, the interval $\mathrm{I}_q(F,h)$ contains (many) squarefree polynomials. Then, in §4, we extend the method to $k$-free polynomials, for any $k \geq 2$, and establish the following result.

**Theorem 2.** *Let $k \geq 2$ and $q \geq 2$ be fixed integers, and suppose that* $\mathrm{char}(\mathrm{F}_q) = p$. *Let $k = dp^a + \cdots + d_1 p + d_0$, $0 \leq d = d_a, \ldots, d_1, d_0 < p$, $d = 0$, be the base-$p$ representation of $k$. If $n$ is sufficiently large and*

$$q^{h+1} > \left(\frac{n}{\log_q n}\right)^{1/\theta}$$

*$F \in \mathrm{M}_q(n)$, the interval $\mathrm{I}_q(F,h)$ contains a $k$-free polynomial whenever*

$$\theta = 1 - (p - d + 1)p^{-a-1}.$$

, (3)

*where*

Note that when $k = 2$, we have $\theta = p^{-1}$, and inequality (3) becomes (2) with $g(n) = 1$. In general, $\theta$ is a non-decreasing function of $k$ such that $\theta = (k-1)p^{-1}$ when $2 \leq k \leq p$, and

$$1 - \frac{(d+1)(p-d+1)}{pk} < \theta \leq 1 - \frac{1}{k}$$

when $k > p$. In particular, as $k$ increases, the gap between the barrier imposed by (1) and the hypothesis (3) of Theorem 2 shrinks, and our result gets closer to being best possible.

The method of proof of Theorem 2 can be adjusted to yield variants that are superior in different ways. As stated, the theorem is close to the best result one can obtain from the basic version of our method. This lets us avoid some technical details. However, as we note at the end of §4, if one is

interested in an asymptotic for the number of $k$-free polynomials in $\mathrm{I}_q(F,h)$, similar to that in the original work of Carmon and Entin [1], one may obtain such an asymptotic for $n \to \infty$ at the cost of strengthening condition (3) to

$$q^{h+1} > \left(\frac{g(n)n}{\log_q n}\right)^{1/\theta} \tag{4}$$

with $g(n) \to \infty$. One can also relax hypothesis (3) to (4) with $g(n) = c$, where $c$ is any constant satisfying $c > \theta\zeta_q(k)p^{-a}$. As $\theta\zeta_q(k)p^{-a} < 1$, this is a slight improvement on Theorem 2.

A notable feature of the modern results on gaps between $k$-free integers is that they can be made fully explicit. For example, in recent joint work with McCormick, Scherr, and Ziehr [18], the authors proved an explicit version of the theorem of Filaseta and Trifonov [8]: the main result of [18] establishes that the interval $(x, x + 11x^{1/5}\ln x]$ contains a squarefree integer for any $x \geq 2$. The next theorem provides a model for such results for polynomials over $\mathrm{F}_q$. Note that—in contrast to Theorems 1, 2, and 5 and similar to the main result of [18]—this theorem makes the restriction on the size of the degree $n$ explicit.

**Theorem 3.** *Let $k \geq 2$ and $q \geq 3$ be fixed integers. If $n \geq k + 1$ and $F \in \mathrm{M}_q(n)$, the interval $\mathrm{I}_q(F,h)$ contains a $k$-free polynomial for all $h \geq n/(k + 1)$.*

When $k = 2$, this theorem corresponds to the classical result that the interval $(x, x+x^{1/3}]$ contains a squarefree integer for all sufficiently large $x$. A slightly stronger version of this was first proved by Davenport in 1951, but not published at the time; its elementary and rather elegant proof can be found in Halberstam's survey [14]. While all the estimates in the proof of Theorem 2 can be made fully explicit, thus allowing us to quantify the hypothesis that "$n$ is sufficiently large," the method is not suited to yield non-trivial results when $n$ and $h$ are as small as they can be in Theorem 3. See Table 1 for a comparison of the values of $h$, $n$ and $q$ for which the results developed in this paper are applicable. We prove this result using a variant for polynomials over finite fields of a differencing technique introduced by Halberstam and Roth [15,24] and later developed by Filaseta and Trifonov [6–8,28]. The proof of Theorem 3 requires only the most basic form of the differencing method. A slightly more sophisticated version of those ideas yields the following result.

**Theorem 4.** *Let $k \geq 2$ and $q \geq 7$ be fixed integers such that $\mathrm{char}(\mathrm{F}_q) \nmid (k+1)$. If $n \geq k+1$ and $F \in \mathrm{M}_q(n)$, the interval $\mathrm{I}_q(F,h)$ contains a $k$-free polynomial for all $h \geq n/(k + 2)$. Moreover, the same conclusion holds when $k \geq 3$ and $q \geq 5$.*

In the case $k = 2$, this result matches a theorem due to Roth [24] (after some modification by Nair [20]) that the interval $(x, x + cx^{1/4}]$ contains a squarefree integer for some absolute constant $c > 0$. When $k \geq 3$, however, Theorem 4 falls short of matching the theorem of Halberstam and Roth [15] that, for any fixed $\varepsilon > 0$, the interval $(x, x + x^{1/(2k)+\varepsilon}]$ contains $k$-free integers when $x$ is sufficiently large. The next theorem accomplishes this.

**Theorem 5.** *Let $k \geq 3$ and $q \geq 3$ be fixed integers such that* $\mathrm{char}(\mathbb{F}_q) \nmid k\binom{2k-1}{k-1}$. *If $n$ is sufficiently large and $F \in \mathrm{M}_q(n)$, then the interval $\mathrm{I}_q(F, h)$ contains a $k$-free polynomial for all $h \geq n/(2k)$.*

While this theorem matches the Halberstam–Roth result in terms of the sizes of the intervals, it is much weaker than Theorem 2 (and, unlike Theorem 4, it says nothing about polynomials of small degrees). On the other hand, its proof adapts the method used by Halberstam and Roth in their seminal paper [15] (as presented in [6]). It also demonstrates how one may develop further the ideas behind Theorems 3 and 4. In the integer setting, it is more advanced versions of those ideas that yield the best results by Filaseta and Trifonov on gaps between $k$-free integers. Indeed, Filaseta and Trifonov (see [6,9]) have used those ideas to make progress in other problems, and it is conceivable that further applications may exist in the function field setting too. For these reasons, it seems that the proof of Theorem 5 is of independent interest (even though the result itself is superseded by Theorem 2), and so it appears as an appendix to this paper.[1]

The remainder of the paper is organized as follows. In §2, we present the basic setup for the proofs and gather some preliminary facts about polynomials over finite fields. We also present present the proofs of Theorem 2 for $k = 2$ and of Theorem 3 in the case when $k$ is not divisible by the characteristic. In §3, we establish Theorem 1. The proof of Theorem 2 in the general case appears in §4. In §5, we develop polynomial analogues of the basic form of the methods used by Filaseta and Trifonov in their work on the gap problem for $k$-free integers: see Propositions 1 and 2 below. We then apply those results to prove Theorems 3

and 4. Finally, as noted earlier, the appendix contains the proof of Theorem 5, including our version of the Halberstam–Roth method (see Proposition 3).

**Notation.** Throughout the paper, the finite field $\mathrm{F}_q$ is considered fixed, and we use $p$ to denote its characteristic (so that, $q = p^f$ for some $f \in \mathrm{N}$). Beside the sets of monic polynomials $\mathrm{M}_q$ and $\mathrm{M}_q(d)$, we use $\mathrm{P}_q$ to denote the set of monic irreducible polynomials and $\mathrm{P}_q(d)$ the set of monic irreducible

[1] It is possible to generalize the improvements of Filaseta and Trifonov to the polynomial setting as well. These methods can be used to show that the interval$_q$ $\mathrm{I}_q(F, h)$ contains a squarefree polynomial for all2 and $h \geq n/5 + \log n$ when $n$ is sufficiently large and $p > 3$. This result is strictly weaker than Theorem the proof substantially more involved, so we will not pursue it further here.

polynomials of degree $d$. We write $\pi_q(d) = |\mathrm{P}_q(d)|$ for the number of monic irreducible polynomials of degree $d$ in $\mathrm{F}_q[x]$; in general, $|\mathrm{A}|$ denotes the cardinality of a finite set A.

## 2. Preliminaries

Fix an integer $k \geq 2$. Our strategy to prove the existence of $k$-free polynomials in an interval $\mathrm{I}_q(F,h)$ will be to bound from above the number $\mathrm{N}_q(F,h)$ of polynomials in $\mathrm{I}_q(F,h)$ that are not $k$-free and to show that

$$\mathrm{N}_q(F,h) < |\mathrm{I}_q(F,h)| = q^{h+1}. \tag{5}$$

Since every polynomial that is not $k$-free is divisible by the $k$th power of some monic irreducible polynomial (and the $k$th power of a polynomial of degree greater than $n/k$ cannot divide any polynomial in $\mathrm{I}_q(F,h)$), we find that

$$\begin{aligned} \mathrm{N}_q(F,h) &\leq \mathrm{X}_q |\{Q \in \mathrm{I}_q(F,h) : P^k \mid Q\}| \\ &P\in\mathrm{P} \\ &= \mathrm{X}_{n/k\,P}\mathrm{X}\,|\{Q \in \mathrm{I}_q(F,h) : P^k \mid Q\}|. \\ &d\leq\in\mathrm{P}_q(d) \end{aligned} \tag{6}$$

It will be useful to recall how many polynomials in $\mathrm{I}_q(F,h)$ are divisible by a fixed polynomial $G$.

**Lemma 1.** *Suppose $G \in \mathrm{M}_q(d)$. Then either $\mathrm{I}_q(F,h)$ contains no multiple of $G$, or*

$$|\{Q \in \mathcal{I}_q(F,h) : G \mid Q\}| = \begin{cases} q^{h-d+1} & \text{if } d \leq h, \\ 1 & \text{if } d > h. \end{cases} \tag{7}$$

*Proof.* Suppose that $GA \in \mathrm{I}_q(F,h)$ for some polynomial $A \in \mathrm{M}_q$. When $d > h$, the interval can contain no other multiples of $G$; and when $d \leq h$, we need to count the polynomials

$GB$, with $B \in \mathrm{I}_q(A,h-d)$. □

The above lemma suffices to estimate the contribution to the right side of (6) from irreducible polynomials $P$ of degrees $d \leq \ell$, when $\ell$ is not much larger than $h$. We have

$$\sum_{d\leq\ell}\sum_{P\in\mathcal{P}_q(d)} |\{Q \in \mathcal{I}_q(F,h) : P^k \mid Q\}| \leq \sum_{d\leq h/k} \pi_q(d) q^{h-kd+1} + \sum_{h/k<d\leq\ell} \pi_q(d) =: \Sigma_1 + \Sigma_2. \tag{8}$$

To bound $\Sigma_1$, $\Sigma_2$, and other similar sums below, we will use some well-known bounds for $\pi_q(d)$, which we state in the next lemma. The first claim of this lemma can be found in [19, Corollary 3.21], and the second claim is an immediate consequence of the first.

**Lemma 2.** *For any natural number n, one has*

$$\sum_{d|n} d\pi_q(d) = q^n \qquad \text{and} \qquad \pi_q(n) \leq \frac{q^n}{n}.$$

Suppose that $k \le h$. Using this lemma, we find that

$$\Sigma_1 \le \sum_{d \le h/k} \frac{q^{h+1}}{dq^{(k-1)d}} < q^{h+1} \ln\left(\frac{1}{1-q^{1-k}}\right) = q^{h+1} \ln \zeta_q(k), \tag{9}$$

and (assuming that $\ell \ge h$)

$$\Sigma_2 \le \sum_{h/k < d \le \ell} \frac{q^d}{d} < \frac{q^\ell}{\ell} + \frac{k}{h} \sum_{j=0}^{\infty} q^{\ell-1-j} \le \frac{q^\ell}{h} + \frac{kq^\ell}{(q-1)h} = \frac{(q+k_h-1)q^\ell}{(q-1)h}, \tag{10}$$

where $k_h := \min(k,h)$. When $k > h$, the sum $\Sigma_1$ is empty, while $\Sigma_2$ satisfies the same bound, after a small adjustment to its proof:

$$\Sigma_2 \le \sum_{d \le \ell} \frac{q^d}{d} < \frac{q^\ell}{h} + \frac{q^\ell}{(q-1)} = \frac{(q+k_h-1)q^\ell}{(q-1)h}.$$

2.1. **The classical approach.** Returning to the contribution to the right side of (6) from degrees $d > h$, we may apply Lemma 1 to show that when $h < d \le n/k$, we have

$$\sum_{P \in \mathrm{P}_q(d)} |\{Q \in \mathrm{I}_q(F,h) : P^k \mid Q\}| \le |S_q(d)|, \tag{11}$$

where

$$\mathcal{S}_q(d) = \left\{G \in \mathcal{M}_q(d) : G^k A \in \mathcal{I}_q(F,h) \text{ for some } A \in \mathcal{M}_q\right\}. \tag{12}$$

The shift of focus from the polynomials in $\mathrm{I}_q(F,h)$ to their $k$th-power divisors that occurs in inequality (11) is an $\mathrm{F}_q[x]$-variant of the basic idea at the core of the proofs of most bounds on gaps between $k$-free integers mentioned in the introduction. In later sections, we prove several results about the "spacing" between polynomials divisible by $k$th powers as measured by the degrees of the differences between their $k$th-power factors. Such spacing results lead to upper bounds on $|S_q(d)|$ through the following lemma.

**Lemma 3.** *Let* $\mathrm{S} \subseteq \mathrm{M}_q(d)$*, and suppose that* $\kappa, \delta \in \mathrm{R}^+$*,* $\delta \le d$*, have the following property: for any fixed polynomial* $G \in \mathrm{S}$*, there exist at most* $\kappa$ *polynomials* $H \in \mathrm{S}$ *such that* $\deg(G-H) < \delta$*. Then*

$$|\mathrm{S}| \le \kappa q^{d-\delta}.$$

*Proof.* Choose $k \in \mathrm{N}$ so that $k-1 < \delta \le k$. The intervals $\mathrm{I}_q(x^k Y(x), k-1)$, with $Y \in \mathrm{M}_q(d-k)$, form a partition of $\mathrm{M}_q(d)$. Let I be one such interval, and fix a polynomial $G \in \mathrm{S} \cap \mathrm{I}$. Since any two elements $G,H$ of $\mathrm{S} \cap \mathrm{I}$ must satisfy $\deg(G-H) < \delta$, by hypothesis, there are at most $\kappa$ possible polynomials $H \in \mathrm{S} \cap \mathrm{I}$, including $G$ itself. Thus, $|\mathrm{S} \cap \mathrm{I}| \le \kappa$. Summing this estimate over all $q^{d-k} \le q^{d-\delta}$ intervals I of the above form, we get the desired bound. □

For example, in Section 5, we will show that when $p \nmid k$—and so Proposition 1 holds with $r = 1$, any two distinct polynomials $G,H \in S_q(d)$ satisfy $\deg(G - H) \geq (k + 1)d - n$. Thus, when $d > n/(k + 1)$, we may apply the above lemma with $\kappa = 1$ and $\delta = (k + 1)d - n$ to obtain

$$|\mathcal{S}_q(d)| \leq q^{n-kd}. \tag{13}$$

This bound suffices to give a quick proof of Theorem 3 in the case when $k$ is not divisible by the characteristic. The proof in the case $p \mid k$ will appear in Section 5.

*Proof of Theorem 3: The case $p \nmid k$.* When $h \geq n/(k + 1)$, the condition $d > h$ implies $d \geq (n + 1)/(k + 1)$. So, we may apply (13) to all $d$ in the range $h < d \leq n/k$ to get

$$\sum_{h<d\leq n/k} |\mathcal{S}_q(d)| \leq \sum_{h<d\leq n/k} q^{n-kd} < q^{n-k(n+1)/(k+1)} \sum_{j\geq 0} q^{-kj} = \frac{q^{(n+k^2)/(k+1)}}{q^k - 1} \leq \frac{q^{h+1+1/(k+1)}}{q^2 - q^{2-k}}.$$

Combining this bound with (6) and (8)–(11) with $\ell = h$, we find that

$$\mathcal{N}_q(F, h) \leq q^{h+1} \left( \ln \zeta_q(k) + \frac{q + k_h - 1}{q(q - 1)h} + \frac{q^{1/(k+1)}}{q^2 - q^{2-k}} \right). \tag{14}$$

When $k = 2$, this establishes (5) when $q \geq 5$ and $h \geq 1$ or when $q = 3$ and $h \geq 2$. Similarly, when $k \geq 3$, this inequality proves the theorem when $q \geq 3$. When $k = 2$, $q = 3$, and $h = 1$, we are in the case $k > h$, so by our earlier observation, $\Sigma_1$ is empty and the logarithmic term on the right side of (14) is superfluous. The stronger version of (14) that results from its omission establishes the theorem in this last remaining case. □

2.2. **The Carmon–Entin approach.** We now present a simplified version of the method of Carmon and Entin [1], which gives a quick proof of Theorem 2 in the squarefree case $k = 2$ for $q > 2$. (With small adjustments, the method can be applied to the case $q = 2$ as well, but we defer that discussion to the general proof in §4.)

The method relies on two main observations. First, we note that when $G = P^2A$ for some polynomials $P$ and $A$, we have also $P \mid G'$, since $G' = 2PP'A + P^2A'$. This simple observation is central also to the proofs in [1] of the more general theorems there.

Our second observation, which replaces a more elaborate construction in [1], is that in characteristic $p$, the coefficients of the monomials $x^{p-1}, x^{2p-1}, \ldots$ in $G'$ vanish, and so $G' \in D_{q^{p-1}}$, where

$$\mathcal{D}_q^j := \{a_m x^m + \cdots + a_0 \in \mathbb{F}_q[x] \mid a_i = 0 \text{ if } i \equiv j \pmod p\}.$$

Let

$$\Sigma_3 = |\{G \in I_q(F,h) : P^2 \mid G \text{ for some } P \in P_q, \deg(P) > h\}|.$$

By the above observations, any polynomial $G$ counted by $\Sigma_3$ has derivative $G'$ lying in $I_q(F',h-1) \cap D_{q^p-1}$, and $G'$ shares an irreducible factor $P$ with $G$, where $\deg P > h$. Note that

$$|I_q(F',h-1) \cap D_{qp-1}| = q^{h-\lfloor h/p \rfloor},$$

which is significantly smaller than the total number of polynomials in $I_q(F,h)$. Next, we show that the number of polynomials counted by $\Sigma_3$ is not much larger than the number of their derivatives.

Fix $H \in I_q(F',h-1) \cap D_{q^p-1}$, and let $P$ be an irreducible divisor of $H$ of degree at least $h+1$. Note that $P$ can divide at most one such polynomial $H$, so $P^2$ divides a polynomial in $I_q(F,h)$ if and only if $H$ has an antiderivative in this interval which is divisible by $P$. Since, $H \in D_{q^p-1}$, each monomial $a_i x^i$ of $H$ has an "obvious" antiderivative $a_i(i+1)^{-1}x^{i+1}$; let $H_0$ be the resulting antiderivative of $H$. The general antiderivative of $H$ is $H_0 + C$ for any polynomial $C \in F_q[x^p]$. So, $H$ has an antiderivative divisible by $P$ in the interval $I_q(F,h)$ if and only if there is a polynomial $C \in \mathbb{F}_q[x^p]$ [7] that lies in the congruence class $C \equiv -H_0 \pmod P$ (in $F_q[x]$) and is such that $H_0 + C \in I_q(F,h)$. Since $\deg P > h$, if such polynomials exist, at most one can lie in the interval $I_q(F,h)$.

Thus, whenever $H \neq 0$, each irreducible factor of $H$ of degree at least $h+1$ corresponds to at most one polynomial $G$ counted by $\Sigma_3$. Since $H$ has degree at most $n-1$, it has $\leq (n-1)/(h+1) < n/(h+1)$ such irreducible factors. On the other hand, if $H$ is identically zero (which can happen only when $I_q(F,h)$ contains a $p$th power), then $H$ has exactly $q^{\lfloor h/p \rfloor + 1}$ antiderivatives in $I_q(F,h)$. We conclude that

$$\Sigma_3 \leq \frac{n}{h+1} q^{h-\lfloor h/p \rfloor} + q^{\lfloor h/p \rfloor + 1}.$$

Combining the last bound with the estimates for $\Sigma_1$ and $\Sigma_2$ in (9) and (10) with $k=2$ and $\ell = h$, we find that

$$\mathcal{N}_q(F,h) \leq q^{h+1}\left(\ln\left(\frac{q}{q-1}\right) + \frac{q+1}{(q-1)qh} + \frac{nq^{-(h+1)/p}}{h+1} + q^{h(1/p-1)}\right). \tag{15}$$

When $h+1 \geq p(\log_q n - \log_q \log_q n)$ (this is equivalent to (3) with $\theta = p^{-1}$), we have

$$(h+1)q^{(h+1)/p} \geq pn\left(1 - \frac{\log_q \log_q n}{\log_q n}\right),$$

and our bound on $N_q(F,h)$ simplifies to

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln\left(\frac{q}{q-1}\right)+\frac{1}{p}+O\left(\frac{\log_q\log_q n}{\log_q n}\right)\right).$$

When $n$ is large and $q > 2$, this proves (5) and establishes Theorem 2.

## 3. Intervals without $k$-free polynomials

In this section, we establish the polynomial analog of Erdős' result on large gaps between squarefree integers stated in Theorem 1. In its proof, we make use of the following lemma, which can be found in [11, Theorem 4.1].

**Lemma 4.** *Let $P_1, P_2, \ldots, P_j, \ldots$ be any ordering of the irreducible monic polynomials in $\mathbb{F}_q[x]$ such that $\deg P_j \le \deg P_{j+1}$. Then, as $j \to \infty$,*

$$\deg P_j \le \log_q j + \log_q \log_q j + \log_q(q-1) + o(1).$$

We also count precisely the number of polynomials in an interval covered by congruences modulo powers of irreducible polynomials of small degrees.

**Lemma 5.** *Let $k \ge 2$, $\ell \le \log_q(h/k) - 1$, and fix a congruence class $Q_j \pmod{P_j^k}$ for every irreducible polynomial $P_j$ with $\deg P_j \le \ell$. Then the number of polynomials in any interval $\mathbb{I}_q(F,h)$ satisfying at least one of these congruences is exactly*

$$q^{h+1}\left(1-\prod_{d=1}^{\ell}\prod_{d\in\mathcal{P}_q(d)}\left(1-\frac{1}{q^{kd}}\right)\right) = q^{h+1}\left(1-\frac{1}{\zeta_q(k)}+O\left(\frac{1}{\ell q^{\ell}}\right)\right).$$

*Proof.* Define $M = \prod_{d=1}^{\ell}\prod_{P\in\mathcal{P}_q(d)} P^k$. We find that

$$\deg M = \sum_{d=1}^{\ell} kd\pi_q(d) \le \sum_{d=1}^{\ell} kq^d < \frac{kq^{\ell+1}}{q-1} \le \frac{h}{q-1} \le h.$$

Thus, we can apply the inclusion-exclusion principle and Lemma 1 to get an exact count of the polynomials in $\mathbb{I}_q(F,h)$ covered by the congruence classes $Q_j \bmod P_j^k$. In particular, since $\deg M < h$ such an interval will always contain exactly

$$q^{h+1}\left(1-\prod_{d=1}^{\ell}\prod_{d\in\mathcal{P}_q(d)}\left(1-\frac{1}{q^{kd}}\right)\right) = q^{h+1}\left(1-\prod_{d=1}^{\ell}\left(1-\frac{1}{q^{kd}}\right)^{\pi_q(d)}\right)$$

polynomials satisfying at least one of the congruences.

Using that $\prod_{P\in\mathcal{P}_q}\left(1-q^{-k\deg P}\right) = \zeta_q(k)^{-1} = 1-q^{-k+1}$, and the estimate

$$\sum_{d>\ell} \ln\left(1-\frac{1}{q^{kd}}\right)^{-\pi_q(d)} \le \sum_{d>\ell} \frac{q^d}{d} \ln\left(1-\frac{1}{q^{kd}}\right)^{-1} \ll \frac{1}{\ell q^\ell}\ .$$

we find that

$$\begin{aligned}\prod_{d=1}^{\ell}\left(1-\frac{1}{q^{kd}}\right)^{\pi_q(d)} &= (1-q^{1-k})\prod_{d>\ell}\left(1-\frac{1}{q^{kd}}\right)^{-\pi_q(d)}\\ &= \zeta_q(k)^{-1}+O\left(\frac{1}{\ell q^\ell}\right)\end{aligned}$$

and the result follows. □

*Proof of Theorem 1.* Let $h$ be large. We will use the Chinese Remainder Theorem to construct a polynomial $F$ of degree at most $n$ such that no polynomial in $I_q(F,h)$ is squarefree when $h$ satisfies (1).

The construction is based on a simple idea. Let $P_1,P_2,\ldots$ be an ordering of $P_q$ such that $\deg P_j \le \deg P_{j+1}$. If $Q_1,Q_2,\ldots,Q_m$ are any polynomials such that the congruence classes $Q_j \bmod P_j^k$, $j \le m$, cover the interval $I_q(0,h)$, then the interval $I_q(F,h)$ contains no $k$-free polynomial whenever $F$ satisfies the congruences

$$F \equiv -Q_j \pmod{P_j^k} \qquad (1 \le j \le m).$$

Since the Chinese Remainder Theorem determines such a polynomial $F$ modulo $P_1^k \cdots P_m^k$, we can find a nontrivial solution of these congruences of degree $\le \deg(P_1^k \cdots P_m^k)$. We can use Lemma 4 to bound the degree of such a polynomial $F$. We have

$$\begin{aligned}F &\le k\sum_{j=1}^{m}\deg P_j \le k\sum_{j=1}^{m}(\log_q j+\log_q\log_q j+\log_q(q-1)+o(1))\\ &= \frac{k}{\ln q}\ln(m!)+km\log_q\log_q m+km\log_q(q-1)+o(m)\\ &= km\left(\log_q m+\log_q\log_q m+\log_q\left(\frac{q-1}{e}\right)+o(1)\right) =: \delta(m),\end{aligned}$$

deg

where the last step uses Stirling's formula. Thus, the proposition will follow, if we show that condition (1) allows us to find an integer $m$ with $\delta(m) \le n$ and $m$ congruence classes $Q_j \bmod P_j^k$ that cover $I_q(0,h)$.

The simplest way to find such a congruence cover is to use a separate congruence class for every polynomial in $I_q(0,h)$. Then $m = q^{h+1}$. This already suffices to establish the theorem when the constant $c$ in (1) satisfies $c < (kq)^{-1}$. It is clear, however, that this simple argument is somewhat wasteful. Next, we use Lemma 5 to cover multiple polynomials by congruences modulo small irreducible polynomials.

Define $\ell := \lfloor \log_q(h/k) \rfloor - 1$ and let $m_0 = \sum_{d=1}^{\ell} \pi_q(d)$ be the number of irreducible polynomials in $M_q$ of degree at most $\ell$. By Lemma 5, we find that the number of polynomials in $I_q(0,h)$ covered by any choice of congruence classes $Q_i \bmod P_i$, for each $i \le m_0$ is exactly

$$q^{h+1}\left(1 - \prod_{d=1}^{\ell} \prod_{d \in \mathcal{P}_q(d)} \left(1 - \frac{1}{q^{kd}}\right)\right).$$

This leaves us, as $h \to \infty$, with

$$\begin{aligned} m_1 := q^{h+1} \prod_{d=1}^{\ell} \prod_{d \in \mathcal{P}_q(d)} \left(1 - \frac{1}{q^{kd}}\right) &= q^{h+1}\left(\frac{1}{\zeta_q(k)} + O\left(\frac{1}{\ell q^{\ell}}\right)\right) \\ &= q^{h+1}\left(\zeta_q(k)^{-1} + o\left(h^{-1}\right)\right) \end{aligned}$$

uncovered polynomials, which we cover trivially, using one congruence class for each. Thus, the total number of congruences we require is

$$\begin{aligned} m = m_0 + m_1 &= m_0 + q^{h+1}\left(\zeta_q(k)^{-1} + o\left(h^{-1}\right)\right) \\ &= q^{h+1}\left(\zeta_q(k)^{-1} + o\left(h^{-1}\right)\right), \end{aligned} \tag{16}$$

after noting that $m_0 \le \sum_{q \le \ell} \frac{q^d}{d} \ll q^{\ell} \ll h$. Using this value of $m$ in our expression for $\delta(m)$ we find that

$$\delta(m) = k\zeta_q(k)^{-1} q^{h+1}\left(h + \log_q h + c_0 + o(1)\right),$$

where $c_0 = \log_q((q-1)/e) + 1 - \log_q \zeta_q(k)$. Hypothesis (1) ensures that, for sufficiently large $h$ and $n$,

$$\delta(m) \le \frac{kcn}{\zeta_q(k)\log_q n}(\log_q n + O(1)) < n, \tag{17}$$

by the assumption that $kc < \zeta_q(k)$. Thus, the polynomial that we have constructed has degree at most $n$ and the result follows. □

*Remark* 1. One sees readily that if hypothesis (1) is replaced by

$$q^{h+1} \le \frac{\zeta_q(k)}{k} \cdot \frac{nq^{\varepsilon(n)}}{\log_q n},$$

inequality (17) can be refined to

$$\delta(m) \le \frac{nq^{\varepsilon(n)}}{\log_q n}\left(\log_q n + \log_q\left(\frac{q-1}{ke}\right) + o(1)\right).$$

In particular, when $\varepsilon(n) \le \log_q\left(1-\frac{c'}{\log_q n}\right)$ with $c' > \log_q((q-1)/ke)$, we find that $\delta(m) < n$.

## 4. Proof of the main theorem

In this section, we extend the ideas from §2.2 to prove Theorem 2. We finish the section with brief remarks on the proof that justify our comments in the introduction about possible enhancements to the theorem. We also remark on the conclusions one can draw when $h$ and $n$ are of moderate size and how such conclusions compare to Theorems 3 and 4.

*Proof of Theorem 2.* Consider an integer $k \ge 2$. Similarly to §2.2, we start from (6) and use (8)–(10) to bound the contribution to the right side of (6) from irreducible polynomials $P$ with $\deg P \le \ell = h$. Thus, we focus on the quantity

$$\Sigma_3 = |\{G \in \mathrm{I}_q(F,h) : P^k \mid G \text{ for some } P \in \mathrm{P}_q,\ \deg(P) > \ell\}|.$$

As in the case $k = 2$ before, we find that if $P^k$ divides $G$, then $P$ divides the first $k-1$ derivatives of $G$, and that the $j$-th derivative, $G^{(j)}$, lies in the set

$$\mathcal{I}_q^{(j)}(F,h) := \mathcal{I}_q(F^{(j)}, h-j) \cap \bigcap_{i+j \ge p} \mathcal{D}_q^i.$$

When $k < p$, we may use these observations in a similar fashion to §2.2 to complete the proof. To begin, let $h = ps + r$, with $0 \le r < p$. We observe that $\mathcal{I}_q^{(k-1)}(F,h)$ is contained in a shift of a finite-dimensional linear space over $\mathrm{F}_q$ of dimension

$$h+1-\sum_{i=1}^{k-1}\left\lceil\frac{h+1-i}{p}\right\rceil = h+1-(k-1)s-\min(r+1,k-1) \le (h+1)\left(1-\frac{k-1}{p}\right).$$

Hence,

$$\left|\mathcal{I}_q^{(k-1)}(F,h)\right| \le q^{(h+1)(1-(k-1)/p)}.$$

By a similar counting argument, we find

$$\le q^{(k-1)(h/p+1)}$$

that there are polynomials $G \in \mathrm{I}_q(F,h)$ with $G^{(k-1)} = 0$. Next, we will show that for each of the $< n/(\ell+1)$ irreducible factors $P$, with $\deg P > \ell$, of a nonzero polynomial $H \in \mathcal{I}_q^{(k-1)}(F,h)$, there is at most one $G \in \mathrm{I}_q(F,h)$ divisible by $P^k$. From this, we can conclude that

$$\Sigma_3 \le \frac{n}{\ell+1} q^{(h+1)(1-(k-1)/p)} + q^{(k-1)(h/p+1)}. \tag{18}$$

Consider a nonzero $H \in \mathrm{I}_q^{(k-1)}(F,h)$ and an irreducible factor $P$ of $H$ of degree at least $h+1$. A polynomial $G \in \mathrm{I}_q(F,h)$ divisible by $P^k$ exists if and only if we can find a finite sequence of polynomials $H_{k-1} = H, H_{k-2}, \ldots, H_1, H_0 = G$, each divisible by $P$, such that

$$H_j \in \mathcal{I}_q^{(j)}(F,h), \quad H_j' = H_{j+1} \qquad (0 \le j < k-1).$$

Since $\deg P > h$, $I_q^{(j)}(F,h)$ can contain at most one multiple of $P$, so for each $j$, there is at most one possibility for the polynomial $H_j$. In particular, at most one possible polynomial $G \in I_q(F,h)$ is divisible by $P^k$. This establishes our earlier claim and completes the proof of (18).

Suppose now that $k \ge p$ and $G \in I_q(F,h)$ is divisible by $P^k$ for some $P \in P_q$. We intend to take $p-1$ derivatives of $G$, but we need to proceed with care. Recall the base-$p$ representation of $k$:

$$k = dp^a + \cdots + d_1 p + d_0 =: k_1 p + d_0$$
$$11 \qquad .$$

After taking $d_0$ derivatives of $G$, we have $G^{(d_0)} = P^{k_1 p} Q$ for some polynomial $Q$, and afterwards we find that

$$G^{(j)} = P^{k_1 p} Q^{(j-d_0)} \qquad (j \ge d_0).$$

In particular, $P^{k_1 p} \mid G^{(p-1)}$. On the other hand, $G^{(p-1)} \in F_q[x^p]$, so $G^{(p-1)} = H^p$ for some polynomial $H \in F_q[x]$.

When $i > (h+1)/p - 1$, the coefficient of $x^i$ in $H$ depends only on a single coefficient of $F$. So $H \in I_q(F_1,h_1)$, where $h_1 = \lfloor (h+1)p^{-1} \rfloor - 1$ and $F_1 = (F^{(p-1)})^{1/p}$ is a polynomial of degree $< np^{-1}$ determined uniquely by $F$. Moreover, by the uniqueness of polynomial factorization in $F_q[x]$, we have $P^{k_1} \mid H$. On the other hand, if $H \in I_q(F_1,h_1)$ is nonzero and divisible by $P^{k_1}$ for some irreducible polynomial $P$, with $\deg P > \ell$, the argument we gave to justify (18) shows that there is at most one polynomial $G \in I_q(F,h)$ such that $G^{(p-1)} = H^p$

(and $G, G', \ldots, G^{(p-1)}$ are all divisible by $P$).

Let $S_1 \subset I_q(F_1,h_1)$ be a set (with $0 \in S_1$ if $0 \in I_q(F_1,h_1)$) to be specified shortly. For any $H \in S_1$, there are $q^{h-h_1}$ polynomials $G \in I_q(F,h)$ with $G^{(p-1)} = H^p$, so we find that

$$\Sigma_3 \le \Sigma_{3,1} + q^{h-h_1}|S_1|, \tag{19}$$

where $\Sigma_{3,1}$ counts pairs $(H,P)$, with $P \in P_q$, $H \in I_q(F_1,h_1) \setminus S_1$, $P^{k_1} \mid H$, and $\deg P > \ell$.

When $k_1 \ge p$ (equivalently $a \ge 2$), we can iterate the above argument, with a slight twist. If $(H_1,P)$ is one of the pairs counted by $\Sigma_{3,1}$, the above construction with $H_1$ in place of $G$ yields a polynomial $H_2 \in I_q(F_2,h_2)$, where $h_2 = \lfloor (h_1+1)p^{-1} \rfloor - 1$ and $F_2$ a polynomial of degree $< np^{-2}$ determined uniquely by $F_1$ (and therefore, by $F$). Moreover, we have

$P^{k_2} \mid H_2$, where $k_2 = (k_1 S_2 - d_1)/p$. Suppose now that $0 \in \mathcal{S}$ if $0 \in \mathcal{I}(F, h)$ $\subset \mathrm{I}_q(F_2, h_2)$ is a set of polynomials, to be specified shortly (with $q$ 2 2 .

We now specify $S_1$ as the set of polynomials $H \in \mathrm{I}_q(F_1, h_1)$ such that $H^{(p-1)} = A^p$ for some $A \in S_2$ (note that this condition ensures that 1 2 $0 \in S_1$ if $0 \in \mathrm{I}_q(F_1, h_1)$). For each $A \in S_2$, there are $\le q^{h-h}$ polynomials $H \in S_1$, so

$$|S_1| \le q^{h_1 - h_2} |S_2|. \tag{20}$$

For any such choice of $S_2$, we find that $\Sigma_{3,1} \le \Sigma_{3,2}$, where $\Sigma_{3,2}$ counts pairs $(H,P)$, with $P$ irreducible, $H \in \mathrm{I}_q(F_2, h_2) \setminus S_2$, $P^{k_2} \mid H$, and $\deg P > \ell$. Therefore, we deduce that

$$\Sigma_3 \le \Sigma_{3,2} + q^{h - h_2} |S_2|. \tag{21}$$

In general, we can iterate this argument a total of $a$ times to find a polynomial $F_a$ of degree $< np^{-a}$, determined uniquely by $F$, such that

$$\Sigma_3 \le \Sigma_{3,a} + q^{h - h_a} |S_a|,$$

where $h_a = \lfloor (h_{a-1} + 1)p^{-1} \rfloor - 1$, the set $S_a \subset \mathrm{I}_q(F_a, h_a)$ is at our disposal to choose (so long as $0 \in S_a$ if $0 \in \mathrm{I}_q(F_a, h_a)$), and $\Sigma_{3,a}$ is the number of pairs $(H,P)$, with $P$ irreducible, subject to

$$H \in \mathrm{I}_q(F_a, h_a) \setminus S_a, \qquad P^d \mid H, \qquad \deg P > \ell.$$

A short computation shows that

$$(h+1)p^{-a} - 3 \le h_a \le (h+1)p^{-a} - 1. \tag{22}$$

At this point, we choose $S_a$ to be the set of polynomials $H \in \mathrm{I}_q(F_a, h_a)$ with $H^{(d-1)} = 0$, so $|S_a| \le q^{(d-1)(h_a p^{-1} + 1)}$. Hence,

$$\Sigma_3 \le \Sigma_{3,a} + q^{h - h_a + (d-1)(h_a/p + 1)}. \tag{23}$$

When $d = 1$, we apply the trivial bound for $\Sigma_{3,a}$:

$$\Sigma_{3,a} \le (\deg F_a)(\ell+1)^{-1}|\mathcal{I}_q(F_a, h_a)| < \frac{n}{p^a(\ell+1)} q^{(h+1)p^{-a}}. \tag{24}$$

When $d > 1$, we may bound $\Sigma_{3,a}$ using a variant of (18) with $h = h_a$, $k = d$, and $n = \deg F_a$. Recall that the second term on the right side of (18) accounts for polynomials in $G \in \mathrm{I}_q(F,h)$ with $G^{(d-1)} = 0$. Thus, by our choice of $\mathrm{S}_a$, the respective bound for $\Sigma_{3,a}$ becomes

$$\Sigma_{3,a} \le (\deg F_a)(\ell+1)^{-1} q^{(h_a+1)(1-(d-1)/p)} < \frac{n}{p^a(\ell+1)} q^{(h+1)p^{-a}(1-(d-1)/p)}.$$

Note that setting $d = 1$ in the bound above yields the exact same expression as (24). So, in either case, using this in (23) along with (22) yields

$$\Sigma_3 \le \frac{n}{p^a(h+1)} q^{(h+1)p^{-a}(1-(d-1)/p)} + q^{(h+1)(1-(p-d+1)p^{-a-1})+d+1}. \tag{25}$$

Note that when $a = 0$ and $d = d_0 = k < p$, (18) is a slightly stronger version of (25) (whose second term contains an extra factor of $q^{2+(k-1)/p} < q^3$). Therefore, we combine (25) with (6) and (8)–(10) to conclude, for sufficiently large $h$ and any $k \ge 2$, that

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln \zeta_q(k) + \frac{n}{p^a(h+1)} q^{-\theta(h+1)} + O\left(h^{-1}\right)\right), \tag{26}$$

where $\theta = 1 - (p-d+1)p^{-a-1}$.

If $h$ is chosen so that

$$q^{h+1} \ge \left(\frac{cn}{\log_q n}\right)^{1/\theta} \tag{27}$$

for some absolute constant $c > 0$, it follows that

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln \zeta_q(k) + \frac{\theta}{p^a c} + O\left(\frac{\log_q h}{h}\right)\right). \tag{28}$$

Since $\theta \le 1 - k^{-1}$, this establishes the theorem for $c \ge 1$. □

*Remark* 2. Suppose that $n$ and $h$ are large, and let $\Sigma_1'$, be the subsum of $\Sigma_1$ (in (8)) with $h_0 < d \le h$, where $h_0 = o(h)$. Also, let

$$\Sigma_0 = \left|\left\{Q \in \mathcal{I}_q(F,h) : P^k \mid Q \text{ for some } P \in \mathrm{P}_q, \deg P \le h_0\right\}\right|.$$

Choosing $h_0$ sufficiently small in terms of , one may apply a sieve argument (similar to the proof of Lemma 5) to $\Sigma_0$ to obtain an asymptotic formula for $\Sigma_1$. One can then replace the term $\ln\zeta_q(k)$

in (28) by $1 - \zeta_q(k)^{-1} + o(1)$. From this we see that $c$ can be taken to be any constant $c > \theta\zeta_q(k)p^{-a}$ so long as $n$ is taken sufficiently large.

On the other hand, if the constant $c$ in (27) is replaced by a function $g(n) \to \infty$ as $n \to \infty$, one may turn the above bounds into an asymptotic formula for the number $Q_q(F,h)$ of $k$-free polynomials in $I_q(F,h)$, since

$$\Sigma_0 \quad \Sigma_1' \quad \Sigma_2 \quad \Sigma_3 \le \mathcal{Q}_q(F,h) \le \Sigma_0 \_ \quad \_ \quad \_ \quad .$$

*Remark* 3. Theorems 3 and 4 give fully explicit ranges of $q$ and $n$ for which the short interval $I_q(F,h)$ contains $k$-free polynomials under the respective constraints on $h$, because bounds like (14) above (see also (34), (45), and (49) in §5) are explicit. Theorem 2, on the other hand, is stated for sufficiently large $n$ to simplify the analysis of (26), which focuses on the

| $h \setminus q$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 | 11 | 19 | 25 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $h = 1$ | — | 3* | 3* | 3* | 4† | 11 | 4 | 4† | 4† | 6 | 14 |
| $h = 2$ | — | 6* | 12 | 6* | 8† | 89 | 20 | 8† | 8† | 19 | 75 |
| $h = 3$ | — | 9* | 57 | 9 | 12† | 393 | 61 | 12† | 12† | 49 | 307 |
| $h = 4$ | — | 12* | 174 | 17 | 16† | 1467 | 164 | 16† | 16† | 118 | 1156 |
| $h = 5$ | — | 23 | 459 | 29 | 25 | 5092 | 414 | 20† | 20† | 271 | 4173 |
| $h = 6$ | — | 42 | 1124 | 48 | 39 | 16984 | 1013 | 28 | 24† | 603 | 14629 |
| $h = 7$ | — | 73 | 2641 | 77 | 60 | 55234 | 2417 | 40 | 28† | 1314 | 50207 |
| $h = 8$ | 23 | 123 | 6048 | 120 | 90 | 176448 | 5674 | 57 | 34 | 2818 | 169578 |

Table 1. Values of $n_0(q,h)$ for which $I_q(F,h)$ contains a squarefree polynomial whenever $\deg F \le n_0$. Numbers marked with an * or a † were obtained using Theorems 3 or 4, respectively.

case when $h$ and $n$ are large. However, if the contributions to the right side of (26) from $\Sigma_2$ and $\Sigma_3$ are kept explicit, one can determine, for every fixed triple $(k,q,h)$, with $h \ge h_0(k,q)$, a range of degrees $n$ for which $I_q(F,h)$ contains $k$-free polynomials. It appears difficult to channel such

observations into a general statement similar to Theorems 3 and 4, but it is possible to draw on them to gain some broad insights.

For example, Table 1 lists several pairs $(q,h)$ and the values of respective integers $n_0(q,h)$ such that the interval $I_q(F,h)$ contains a squarefree polynomial whenever $\deg F \le n_0$. For values of $q$ with $p > 2$, these bounds are computed using (15), taking the largest value of $n$ such that the coefficient of $q^{h+1}$ is less than 1. For those values with $p = 2$, an explicit version of (26) is used, after noting that in this specific case, $k = p = 2$, the lower bound in (22) can be improved to $(h+1)/2-3/2$. This results in an expression identical to (15), but in which the second to last term is half as large. Note that even these values are likely much smaller than the "truth." For example, in the case $q = 2$ these methods do not prove that all short intervals with $h = 1$ or 2 and any value of $n$ are guaranteed to contain squarefree polynomials, however direct computation shows that every such short interval contains a squarefree polynomial in these cases when $n \le 9$ and 16 respectively.

In some cases, the bounds obtained using Theorems 3 and 4 are stronger than those obtained here. Such improved bounds are included in the table above marked with the symbols * or †.

## 5. The differencing method for polynomials

Recall the set $S_q(d)$ defined in (12). In this section, we prove several results about the spacing between elements of $S_q(d)$. Through applications of Lemma 3, these results will then yield upper bounds on $|S_q(d)|$, which apply to prove Theorems 3 and 4.

Our first result is a bound on the minimum degree of the difference of distinct elements of $S_q(d)$. Recall that we use $p$ to denote the characteristic of the finite field $F_q$. We note that when $p \nmid k$, we have $r = 1$ in the proposition below, while when $p \mid k$, we have $1 < r \le k$.

**Proposition 1.** *Suppose that $h < d \le n/k$ and $G,H \in S_q(d)$, with $G \ne H$. Let $r = r(k,p)$ be the least positive integer such that $p \nmid \binom{k}{r}$. When $r < k$, we have*

$$\deg(G - H) \ge \frac{(k+r)d - n}{r}. \tag{29}$$

*When $r = k$, we have either (29) with $r = k$, or*

$$\deg(G - H) \le \frac{h + kd - n}{k}. \tag{30}$$

*Proof.* Let $A,B \in M_q(n-kd)$ be such that $G^kA, H^kB \in I_q(F,h)$. Then $\deg(G^kA - H^kB) \le h$, and we deduce that

$$\deg\big((G^k - H^k)A + H^k(A - B)\big) \le h. \tag{31}$$

Note that

$$G^k - H^k = \big((G-H)+H\big)^k - H^k = \sum_{j=1}^{k} \binom{k}{j} (G-H)^j H^{k-j}.$$

Since $\deg(G-H) < d = \deg H$, it follows that

$$\deg(G^k - H^k) = r\deg(G-H) + (k-r)d. \tag{32}$$

Suppose first that $A \neq B$. Then the degree of the second term on the left side of (31) is

$$\deg(H^k(A-B)) = kd + \deg(A-B) \geq kd > h.$$

This is only possible if the two terms on the left side of (31) have the same degree, meaning that

$$\deg((G^k - H^k)A) = \deg(H^k(A-B)) \geq kd.$$

Combining this with (32) gives

$$kd \leq r\deg(G-H) + (k-r)d + \deg A = r\deg(G-H) + (n-rd),$$

which establishes (29) in this case.

Next, we consider the case $A = B$. Then (31) and (32) give

$$r\deg(G-H) + (n-rd) = \deg((G^k - H^k)A) \leq h,$$

and hence,

$$\deg(G-H) \leq \frac{h+rd-n}{r}.$$

When $r = k$, this establishes (30), and when $r < k$, we get

$$\deg(G-H) < \frac{(r+1)d-n}{r} \leq 0,$$

which contradicts our assumption that $G \neq H$. Therefore, this case occurs only when $r = k$. □ We remark that when $r = k$ and $h)/k$, $d < (n-$ inequality (30) contradicts the assumption $G \neq H$ of the proposition, so for in this range, we always have (29). On the other hand, when $r = k$ and $(n - h)/k \leq d \leq n/k$, we can combine (29) and (30) to obtain a rather sharp bound on $|S_q(d)|$, which we state in the following lemma.

**Lemma 6.** *Assume the notation of Propositon 1. If $r = k$ and $(n-h)/k \leq d \leq n/k$, we have*

$$|S_q(d)| \leq q^{h/k+1}.$$

*Proof.* Let $\delta = (2kd - n)/k$. According to the proposition, any two elements $G,H$ of $S_q(d)$ with $\deg(G - H) < \delta$ must satisfy (30). In particular, for a fixed $G$, there are at most

$$|I_q(G,(kd + h - n)/k)| \le q^{(kd+h-n)/k+1} =: \kappa$$

polynomials $H \in S_q(d)$ with $\deg(G - H) < \delta$. Thus, Lemma 3 gives

$$|S_q(d)| \le \kappa q^{d-\delta} = q^{h/k+1}. \qquad \square$$

Recall that in §2 we derived Theorem 3 in the case when $p \nmid k$ from (29) with $r = 1$. We can use Lemma 6 to complete the proof of Theorem 3 in the case when $p \mid k$.

*Proof of Theorem 3: $p \mid k$.* To begin, we observe that when $d \le n/k$ and $r > 1$ in Proposition 1, the bound (29) is stronger than its version with $r = 1$. Therefore, when $1 < r < k$, we still have inequality (13) (and more), and so we may follow the proof from the case $p \nmid k$ (given in §2.1) without any changes. Thus, we may focus on the case $r = k$.

Note that when $h \ge n/(k + 1)$, Lemma 6 is applicable in the full range $h < d \le n/k$. Hence,

$$\sum_{h<d\le n/k} |\mathcal{S}_q(d)| \le \left(\frac{n}{k} - h\right) q^{h/k+1} \le (h/k)q^{h/k+1}. \tag{33}$$

Combining this with (6) and (8)–(11) with $\ell = h$, we find that

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln \zeta_q(k) + \frac{q + k_h - 1}{q(q-1)h} + (h/k)q^{(1-k)h/k}\right). \tag{34}$$

When $k \ge 3$, the last expression is $< q^{h+1}$, provided for all $q \ge 3$ and $h \ge 1$. When $k = 2$ (note that in this case, we have $p = 2$ and $q = 2^f$), the same holds for $q \ge 4$ and $h \ge 1$. □

Next, we consider $s$-tuples of distinct polynomials $\mathbf{G} = \{G_1,\dots,G_s\}$ in $S_q(d)$, with $s \ge 3$. If $\mathbf{G}$ is such an $s$-tuple, we write

$$\delta(\mathbf{G}) = \min_{1\le i<j\le s} \deg(G_i - G_j),$$

$$\Delta(\mathbf{G}) = \max_{1\le i<j\le s} \deg(G_i - G_j).$$

By Proposition 1, we have

$$\delta(\mathbf{G}) \ge (k + 1)d - n, \tag{35}$$

whenever $h < d \leq n/k$ and $r = r(k,p) < k$ (or $r = k$ and $d < (n - h)/k$). Our next result is a lower bound on $\Delta(\mathbf{G})$ for triples.

**Proposition 2.** *Suppose that* $p \nmid k(k+1)$ *and* $h < d \le n/k$. *If* $\mathbf{G} = \{G_1, G_2, G_3\}$ *is a set of distinct polynomials in* $\mathrm{S}_q(d)$, *then*

$$\Delta(\mathbf{G}) \ge \frac{(k+2)d - n}{3}. \tag{36}$$

*Proof.* For each $1 \le i \le 3$, let $A_i \in \mathrm{M}_q(n - kd)$ and $R_i$ be polynomials such that

$$F = G_i^k A_i - R_i, \qquad \deg R_i \le h. \tag{37}$$

We now consider the rational function

$$\Phi[G_1, G_2, G_3] = (G_3 - G_2)\frac{F}{G_1^k} + (G_1 - G_3)\frac{F}{G_2^k} + (G_2 - G_1)\frac{F}{G_3^k},$$

essentially a second divided difference of the function $\Phi(t) = Ft^{-k}$ on $\mathrm{F}_q(x)$ (see [16] for background on divided differences). By (37), we have

$$\Phi[G_1, G_2, G_3] = N - \Theta, \tag{38}$$

where

$$N = (G_3 - G_2)A_1 + (G_1 - G_3)A_2 + (G_2 - G_1)A_3,$$
$$\Theta = (G_3 - G_2)\frac{R_1}{G_1^k} + (G_1 - G_3)\frac{R_2}{G_2^k} + (G_2 - G_1)\frac{R_3}{G_3^k}.$$

Our immediate goal is to show that $N$ is a nonzero polynomial by showing that $\deg N \ge 0$. In the rest of the proof, we suppress the dependence on $\mathbf{G}$ and write simply $\Delta, \delta$, and $\Phi$ instead of $\Delta(\mathbf{G}), \delta(\mathbf{G})$, and $\Phi[G_1, G_2, G_3]$.

We can rewrite the definition of $\Phi$ as the polynomial identity

$$\Phi G_1^k G_2^k G_3^k = F\left(\prod_{i<j}(G_j - G_i)\right)\left(\sum_{a+b+c=2k-2} G_1^a G_2^b G_3^c\right), \tag{39}$$

where the product on the right is over all pairs of indices $i,j$ with $1 \le i < j \le 3$, and the sum is over all triples $a,b,c$ with $0 \le a,b,c \le k-1$ and $a+b+c = 2k-2$. Observe that if both $\deg(G_j - G_i) < \Delta$ and $\deg(G_k - G_i) < \Delta$, then also

$$\deg(G_j - G_k) \le \max\{\deg(G_j - G_i), \deg(G_k - G_i)\} < \Delta,$$

which contradicts the choice of $\Delta$. Thus, at least two of the differences in the above product must have degree $\Delta$, and we get

$$2\Delta + \delta \le \deg\left(\prod_{i<j}(G_j - G_i)\right) \le 3\Delta. \tag{40}$$

Also, the sum on the right side of (39) has $\binom{k+1}{2}$ terms, each of them in $\mathrm{M}_q((2k-2)d)$. Since $p \nmid \binom{k+1}{2}$, it follows that the sum is a polynomial of degree $(2k-2)d$, and we deduce

$$n + (2k-2)d + 2\Delta + \delta \le \deg(\Phi^{G_1^k G_2^k G_3^k}) \le n + (2k-2)d + 3\Delta. \tag{41}$$

On the other hand, we have

$$\Theta G_1^k G_2^k G_3^k = R_1(G_3 - G_2)G_2^k G_3^k + R_2(G_1 - G_3)G_1^k G_3^k + R_3(G_2 - G_1)G_1^k G_2^k. \tag{42}$$



Since each of the three terms on the right side of (42) has degree $\le h + \Delta + 2kd$, we obtain

$$\deg\left(\Theta G_1^k G_2^k G_3^k\right) \le 2kd + \Delta + h. \tag{43}$$

Moreover, since $p \nmid k$, we have (35) by Proposition 1. Combining (35), (41), and (43), we conclude that

$$\begin{aligned}\deg(\Phi^{G_1^k G_2^k G_3^k}) &\ge n + (2k-2)d + 2\Delta + \delta \\ &\ge (3k-1)d + 2\Delta \\ &> 2kd + h + 2\Delta \ge \deg\left(\Theta G_1^k G_2^k G_3^k\right).\end{aligned}$$

Thus, by (38),

$$\deg(N G_1^k G_2^k G_3^k) = \deg(\Phi G_1^k G_2^k G_3^k) \ge 0,$$

which establishes our prior claim that $N \not\equiv 0$. Using the upper bound in (41), we get

$$3kd \le \deg(N G_1^k G_2^k G_3^k) = \deg(\Phi G_1^k G_2^k G_3^k) \le n + (2k-2)d + 3\Delta,$$

and the desired conclusion follows. □

We now use Proposition 2 and Lemma 6 to prove Theorem 4.

*Proof of Theorem 4.* Suppose first that $p \nmid k(k+1)$. When $d > h$, we have $d \ge (n+1)/(k+2)$, and Proposition 2 allows us to apply Lemma 3 with $\kappa = 2$ and $\delta = ((k+2)d - n)/3$ to deduce the bound

$$|S_q(d)| \le 2q^{(n-(k-1)d)/3}. \tag{44}$$

Therefore,

$$\sum_{h<d\le n/k} |\mathcal{S}_q(d)| \le 2 \sum_{h<d\le n/k} q^{(n-(k-1)d)/3} < 2q^{(n-(k-1)d_0)/3} \sum_{j\ge 0} q^{-(k-1)j/3} = \frac{2q^{(n+1)/(k+2)}}{q^{1/3} - q^{-(k-2)/3}},$$

where $d_0 = (n+1)/(k+2)$. This inequality, (6), and (8)–(11) with $\ell = h$ now give

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln \zeta_q(k) + \frac{q + k_h - 1}{q(q-1)h} + \frac{2q^{-(k+1)/(k+2)}}{q^{1/3} - q^{-(k-2)/3}}\right), \tag{45}$$

which implies (5) when $k = 2$ and $q \ge 7$ or when $k \ge 3$ and $q \ge 5$.

Next, let $p \mid k$ and suppose that $r < k$ in Proposition 1. Then Proposition 1 yields (29) with $r \ge 2$, and hence, with $r = 2$. Thus, Lemma 3 with $\kappa = 1$ and $\delta = ((k+2)d - n)/2$ yields the bound

$$|S_q(d)| \le q^{(n-kd)/2}, \tag{46}$$

which supersedes (44). Hence, (45) holds also in this case.

Finally, let $p \mid k$ and $r = k$, and assume that $n/(k+2) \le h < n/(k+1)$. When $h < d < (n-h)/k$, we can again use Proposition 1 to obtain (46). Hence,

$$\sum_{h<d<(n-h)/k} |\mathcal{S}_q(d)| \le q^{(n-kd_0)/2} \sum_{j\ge 0} q^{-kj/2} = \frac{q^{(n+1)/(k+2)}}{q^{1/2} - q^{-(k-1)/2}}. \tag{47}$$

Moreover, when $(n-h)/k \le d \le n/k$, we may use Lemma 6 in a similar fashion to (33) to show that

$$\sum_{(n-h)/k\le d\le n/k} |\mathcal{S}_q(d)| \le \left(\frac{h}{k}+1\right) q^{h/k+1}. \tag{48}$$



Combining (47) and (48) with (6) and (8)–(11) with $\ell = h$, we conclude that

$$\mathcal{N}_q(F,h) \le q^{h+1}\left(\ln \zeta_q(k) + \frac{q+k_h-1}{q(q-1)h} + \frac{q^{-(k+1)/(k+2)}}{q^{1/2}-q^{-(k-1)/2}} + \left(\frac{h}{k}+1\right) q^{(1-k)h/k}\right), \tag{49}$$

which again implies (5). □

Appendix A. An analogue of the methods of Halberstam and Roth As in the proofs of Theorems 3 and 4, we need to estimate

$$\Sigma_3 = \sum_{\ell<d\le n/k} |\mathcal{S}_q(d)|,$$

where $\ell \ge h$. When $k \ge 3$, the estimation of $\Sigma_3$ relies on the following proposition.

**Proposition 3.** *Let $k \ge 3$ and $p \nmid k\binom{2k-1}{k-1}$. If $n/(2k) \le h < d \le n/k$, we have*

$$|S_q(d)| \le 2kq^{(n-d)/(2k-1)}.$$

We postpone the proof of this result until the end of the section and focus first on the proof of Theorem 5. By the proposition,

$$\Sigma_3 \le \sum_{\ell<d\le n/k} 2kq^{(n-d)/(2k-1)} < 2kq^{(n-\ell)/(2k-1)} \sum_{j\ge 0} q^{-j/(2k-1)}$$

$$= \frac{2kq^{(n-\ell)/(2k-1)}}{1-q^{-1/(2k-1)}} \le \frac{2kq^{h+(h-\ell)/(2k-1)}}{1-q^{-1/(2k-1)}},$$

on recalling that $h \ge n/(2k)$. Writing $\delta_q = q^{-1/(2k-1)}$, we have

so

$$1-\delta_q > \frac{1-\delta_q^{2k-1}}{2k-1} = \frac{q-1}{(2k-1)q}, \tag{50}$$

Together, (6), (8)–(11), $\Sigma \le \frac{2k(2k-1)q^{h+1}h^{(h-\ell)/(2k-1)}}{q-1}$ and (50) give

$$\mathcal{N}_q(F,h) < q^{h+1}\left(\ln\zeta_q(k) + \frac{(q+k)q^{\ell-h}}{q(q-1)h} + \frac{k(4k-2)q^{(h-\ell)/(2k-1)}}{q-1}\right).$$

We now select

$$\ell = h + \log_q(qh)_{(2k-1)/2k}.$$

This choice essentially balances the second and third terms on the right side of the last inequality and gives

$$\mathcal{N}_q(F,h) < q^{h+1}\left(\ln\zeta_q(k) + \frac{(q+4k^2-k)(qh)^{-1/2k}}{q-1}\right) \tag{51}$$

When $h$ is sufficiently large in terms of $k$, this completes the proof of the theorem.

All that remains is to prove Proposition 3.

*Proof of Proposition 3.* Consider the polynomials $P_0, Q_0 \in \mathbb{Z}[x]$ given by

$$P_0(x) = 1 - \binom{2k-1}{1}x + \cdots + (-1)^{k-1}\binom{2k-1}{k-1}x^{k-1},$$
$$(1-x)^{2k-1} = P_0(x) - x^k Q_0(x).$$

We use these to define the degree-$(k-1)$ forms

$$P(x,y) = x^{k-1}P_0(y/x), \qquad Q(x,y) = x^{k-1}Q_0(y/x),$$

which satisfy the algebraic identity

$$(x-y)^{2k-1} = x^kP(x,y) - y^kQ(x,y).$$

In particular, for any polynomials $G_1, G_2 \in \mathbb{F}_q[x]$, we obtain

$$(G_1-G_2)^{2k-1} = G_1^kP(G_1,G_2) - G_2^kQ(G_1,G_2). \tag{52}$$

Next, we consider (52) when $G_1, G_2 \in S_{q,k}(d)$. We find polynomials $A_i \in M_q(n-kd)$ and $R_i$ with

$$F = G_i^kA_i - R_i, \qquad \deg R_i \le h. \tag{53}$$

We may then rearrange (52) as

$$(G_1-G_2)^{2k-1}F = F\left(G_1^kP(G_1,G_2) - G_2^kQ(G_1,G_2)\right) = N + \Theta, \tag{54}$$

where

Note that

$$\deg\Theta \le (2k-1)d + h < 2kd.$$

When

$$N = G_1^k G_2^k \big(P(G_1, G_2)A_2 - (G_1, G_2)A_1\big)$$
$$\Theta = G_2^k Q(G_1, G_2)R_1 - G_1^k P(G_1, G_2)R_2,$$

$$G_1 - G_2) < \frac{2kd - n}{2k - 1} =: \Delta_k \qquad \deg($$

(55)

we find also that

$$\deg\big((G_1 - G_2)^{2k-1}F\big) = (2k-1)\deg(G_1 - G_2) + n < 2kd. \deg$$
$$\big(G_1^k G_2^k (P(G_1, G_2)A_2 - Q(G_1, G_2)A_1)\big) < 2kd.$$

Thus, under condition (55), we can deduce from (54) that

Since $\deg($$G_1^k G_2^k) = 2kd$, this is possible only if

$$P(G_1,G_2)A_2 - Q(G_1,G_2)A_1 = 0. \tag{56}$$

That is, if $G_1,G_2 \in S_q(d)$ satisfy (55), then $G_1,G_2$, and the respective polynomials $A_1,A_2$ must satisfy the polynomial identity (56).

Consider a third polynomial $G_3 \in S_q(d)$ such that

$$\deg(G_3 - G_i) < \Delta_k \tag{57}$$

holds for $i = 1$. Then, as an immediate consequence of (55), (57) holds also for $i = 2$. Further, by the argument in the last paragraph, we have also

$$P(G_1, G_3)A_3 - Q(G_1, G_3)A_1 = 0$$
$$20 \qquad , \tag{58}$$

and

$$P(G_3,G_2)A_2 - Q(G_3,G_2)A_3 = 0. \tag{59}$$

Finally, from (58) and (59), we readily obtain that

$$P(G_1,G_3)P(G_3,G_2)A_2 - Q(G_1,G_3)Q(G_3,G_2)A_1 = 0. \tag{60}$$

We now consider an interval I of length $\le \Delta_k$ and fix distinct polynomials $G_1,G_2 \in S_q(d) \cap I$. Then $G_1,G_2$ satisfy (55), and any other polynomial $G_3 \in S_q(d) \cap I$ must satisfy (60). We view

$$P(G_1,t)P(t,G_2)A_2 - Q(G_1,t)Q(t,G_2)A_1 = 0 \tag{61}$$

as a polynomial equation in $t$ over $\mathrm{F}_q[x]$. By the construction of $P$ and $Q$, the left side of (61) is a polynomial of degree $2k-2$ with leading coefficient

$$(-1)^{k-1}\binom{2k-1}{k-1}(A_2-A_1).$$

We will show that this coefficient is nonzero. The hypothesis on the characteristic $p$ reduces this task to showing that $A_1 \neq A_2$.

When $A_1 = A_2 = A$, say, conditions (53) yield

$$\deg(G_1^k - G_2^k) + \deg A \leq \deg(R_1 - R_2) \leq h.$$

We have

$$G_1^k - G_2^k = (G_1 - G_2)\sum_{j=0}^{k-1} G_1^j G_2^{k-j-1}.$$

The sum over $j$ is a polynomial of degree $(k-1)d$ with leading coefficient $k$, which does not vanish since $p \nmid k$. As $G_1 \neq G_2$, this implies that

$$(k-1)d \leq \deg(G_1^k - G_2^k) \leq h - \deg A < (k+1)d - n,$$

a contradiction. Therefore, $A_1 \neq A_2$.

Thus, (61) is a (univariate) polynomial equation of degree $2k-2$ over $\mathrm{F}_q[x]$. The number of solutions of such an equation is bounded above by its degree, so once $G_1$, $G_2$ (and hence, $A_1$ and $A_2$) are fixed, there are at most $2k-2$ possibilities for $G_3 \in \mathrm{S}_q(d) \cap \mathrm{I}$. We conclude that

$$|\mathrm{S}_q(d) \cap \mathrm{I}| \leq 2k.$$

Therefore, the conclusion of the proposition follows from Lemma 3 with $\kappa = 2k$ and $\delta = \Delta_k$. □

**Acknowledgments.** This work is the result of an REU project that took place on the campus of Towson University during the summer of 2022, with the financial support of the National Science Foundation under grants DMS-2136890 and DMS-2149865. The authors also acknowledge financial support from the Fisher College of Science and Mathematics and TU's Mathematics Department. Finally, the authors want to thank the anonymous referee for their thorough reading of the manuscript and for several improvements to the exposition.

## References


[1] D. Carmon and A. Entin, *On square-free values of large polynomials over the rational function field*, Math. Proc. Cambridge Philos. Soc. **170** (2021), no. 2, 247–263. MR4222433

[2] P. Erdős, *Some problems and results in elementary number theory*, Publ. Math. Debrecen **2** (1951), 103–109. MR45759

[3] _____, *On the difference of consecutive terms of sequences defined by divisibility properties*, Acta Arith (1966/1967), 175–182. MR207673

[4] M. Filaseta, *An elementary approach to short interval results for k-free numbers*, J. Number Theory **30** (1988), no. 2, 208–225. MR961917

[5] _____, *Short interval results for squarefree numbers*, J. Number Theory **35** (1990), no. 2, 128–149. MR1057318

[6] M. Filaseta, S. W. Graham, and O. Trifonov, *Starting with gaps between k-free numbers*, Int. J. Number Theory **11** (2015), no. 5, 1411–1435. MR3376218

[7] M. Filaseta and O. Trifonov, *On gaps between squarefree numbers*, Analytic Number Theory (Allerton Park, IL, 1989), 1990, pp. 235–253. MR1084183

[8], ~~*On gaps*~~ *between squarefree numbers. II*, J. London Math. Soc. (2) **45** (1992), no. 2, 215–221. MR1171549

[9], *The distribution of fractional parts with applications to gap results in number theory*, Proc. London Math. Soc. ~~(3) **73** (~~1996), no. 2, 241–278. MR1397690

[10] E. Fogels, *On average values of arithmetic functions*, Proc. Cambridge Philos. Soc. **37** (1941), 358–372. MR4843

[11] A. Gómez-Colunga, C. Kavaler, N. McNew, and M. Zhu, *On the size of primitive sets in function fields*, Finite Fields Appl. **64** (2020), 101658, 23. MR4078938

[12] S. W. Graham and G. Kolesnik, *On the difference between consecutive squarefree integers*, Acta Arith. **49** (1988), no. 5, 435–447. MR967330

[13] A. Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009. MR1654759

[14] H. Halberstam, *Gaps in integer sequences*, Math. Mag. **56** (1983), no. 3, 131–140. MR701971

[15] H. Halberstam and K. F. Roth, *On the gaps between consecutive k-free integers*, J. London Math. Soc. **26** (1951), 268–273. MR43120

[16] E. Isaacson and H. B. Keller, *Analysis of Numerical Methods*, Dover Publications, Inc., New York, 1994. Corrected reprint of the 1966 original. MR1280462

[17] J. Keating and Z. Rudnick, *Squarefree polynomials and Möbius values in short intervals and arithmetic progressions*, Algebra Number Theory **10** (2016), no. 2, 375–420. MR3477745

[18] A. Kumchev, W. McCormick, N. McNew, A. Park, R. Scherr, and W. Ziehr, *Explicit bounds for large gaps between squarefree numbers*, J. Number Theory. To appear.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, Second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. MR1429394

[20] M. Nair, *Power free values of polynomials. II*, Proc. London Math. Soc. (3) **38** (1979), no. 2, 353–368. MR531167

[21] R. A. Rankin, *Van der Corput's method and the theory of exponent pairs*, Quart. J. Math. Oxford Ser. (2) **6** (1955), 147–153. MR72170

[22] H.-E. Richert, *On the difference between consecutive squarefree numbers*, J. London Math. Soc. **29** (1954), 16–20. MR57898

[23] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657

[24] K. F. Roth, *On the gaps between squarefree numbers*, J. London Math. Soc. **26** (1951), 263–268. MR43119

[25] Z. Rudnick, *Square-free values of polynomials over the rational function field*, J. Number Theory **135** (2014), 60–66. MR3128452

[26] P. G. Schmidt, *Abschätzungen bei unsymmetrischen Gitterpunktproblemen*, Dissertation, Göttingen, 1964. Dissertation zur Erlangung des Doktorgrades der Mathematisch-Naturwissenschaftlichen Fakultät der Georg-August-Universität zu Göttingen. MR0181609

[27] O. Trifonov, *On the squarefree problem. II*, Math. Balkanica (N.S.) **3** (1989), no. 3-4, 284–295. MR1048051
[28] ———, *On gaps between k-free numbers*, J. Number Theory **55** (1995), no. 1, 46–59. MR1361558

Department of Mathematics, Towson University, Towson, MD 21252, U.S.A. *Email address*: akumchev@towson.edu

Department of Mathematics, Towson University, Towson, MD 21252, U.S.A. *Email address*: nmcnew@towson.edu

School of Mathematics, University of Minnesota Twin Cities, Minneapolis, MN 55455, U.S.A. *Email address*: park2968@umn.edu