On the number of distinct roots of a lacunary polynomial over finite fields

József Solymosi*   Ethan P. White†   Chi Hoi Yip ‡

Department of Mathematics

The University of British Columbia

Vancouver, BC

Canada V6T 1Z2

August 25, 2020

Abstract

We obtain new upper bounds on the number of distinct roots of lacunary polynomials over finite fields. Our focus will be on polynomials for which there is a large gap between consecutive exponents in the monomial expansion.

1 Introduction

A polynomial is *lacunary* if there is a substantial gap between the degree of two consecutive terms. Most often, the gap between the highest and second highest terms is considered. What entails a substantial and useful gap depends on the context. The theory of lacunary polynomials has been critical in applications to computing theory, character sums, and discrete geometry.

Throughout this work, q is a power of a prime p and $\mathbb{F}_q$ is the field with q elements. All polynomials considered will be in the ring $\mathbb{F}_q[x]$. For a polynomial $f(x) \in \mathbb{F}_q[x]$, we will denote by f° and $f^{\circ\circ}$ the degree of $f(x)$, and the degree of the second highest term of $f(x)$, respectively. For a polynomial $f(x) \in \mathbb{F}_q[x]$ we will denote by $Z(f)$ the set of roots of $f(x)$ in $\mathbb{F}_q^*$. A fundamental question is to improve the trivial degree bound on the number of distinct zeros of a polynomial. László Rédei's monograph [7] is one of the most significant and important works on lacunary polynomials. One of the main theorems proved by Rédei showed that polynomials cannot be too lacunary while also being fully reducible. For other similar results and applications of them, we refer to [1].

---

*solymosi@math.ubc.ca

†epwhite@math.ubc.ca

‡kyleyip@math.ubc.ca

1

A class of polynomials related to lacunary polynomials are sparse polynomials. A t-sparse polynomial is a polynomial with t terms in its monomial expansion. Sparse polynomials are referred to as lacunary by some authors. Analogous to the lacunary results mentioned above, Bibak and Shparlinski showed that few polynomials are simultaneously sparse and fully reducible [2]. An upper bound on the number of roots of sparse polynomials has been investigated by several authors. For a t-sparse polynomial f, Karpinski and Shparlinski showed that $|Z(f)| \leq \frac{t-1}{t}(q-1)$, and gave an efficient approximation algorithm for $|Z(f)|$, see [4]. In Section 3 we give a generalization of this bound. Canetti et al. proved a finite field analogue of Descartes' rule of signs using pigeonholing based on geometry of numbers and affine transformations on the exponents in the monomial expansion of a t-sparse polynomial in [3]. Kelley [5] refined their method and showed that

$$|Z(f)| \leq 2(q-1)^{1-1/(t-1)}C(f)^{1/(t-1)}, \tag{1}$$

where f is a t-sparse polynomial and $C(f)$ denotes the size of the largest coset in $\mathbb{F}_q^*$ on which f vanishes completely. In the case $t = 3$, Kelley and Owen [6] improved the above bound on $|Z(f)|$ for trinomials f to

$$D(f)\left\lfloor \frac{1}{2} + \sqrt{\frac{q-1}{d}} \right\rfloor, \quad \text{for } f(x) = x^n + ax^s + b, \quad \text{where } D(f) = \gcd(n, s, q-1). \tag{2}$$

Moreover, when q is a square, they gave explicit examples for which the above bound is tight. The aforementioned bounds for sparse polynomials do not always improve the trivial degree bound for lacunary polynomials, since lacunary polynomials are not necessarily sparse, and vice versa. In Section 3 our results improve the bounds in (1) and (2) in the case that the polynomial is simultaneously sparse and lacunary. One of Rédei's seminal results on lacunary polynomials is the following.

Theorem 1.1 (Theorem 5 in [7])**.** *Let q be a prime power and $d > 1$ be a divisor of $q - 1$. Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial such that*

$$f(x)|(x^{q-1} - 1), \quad f^\circ = \frac{q-1}{d}, \quad \text{and} \quad f^{\circ\circ} \leq \frac{q-1}{d^2}.$$

Then $f(x)$ is an Euler binomial

$$x^{\frac{q-1}{d}} - \alpha, \quad \text{for some} \quad \alpha \in (\mathbb{F}_q^*)^{\frac{q-1}{d}},$$

or if $p \neq 2$, $4|(q-1)$, and $d = 2$, then possibly takes the form

$$\left(x^{\frac{q-1}{4}} - \beta\right)\left(x^{\frac{q-1}{4}} - \gamma\right), \quad \text{where} \quad \beta^2 = 1, \gamma^2 = -1.$$

The above theorem shows that within a certain class of polynomials, a polynomial $f(x)$ cannot be simultaneously lacunary and possess f° distinct roots. Our main focus will be to extend this property to a larger class of polynomials and show that the number of distinct roots of many lacunary polynomials is often less than its degree. Hereafter $d \geq 1$ will always be a positive divisor of $q - 1$. Our main focus will be on polynomials $f(x) \in \mathbb{F}_q[x]$ of the form

$$f(x) = x^{\frac{q-1}{d} - \ell} + g(x), \tag{3}$$

where $\ell \geq 0$ and $g^\circ < \frac{q-1}{d} - \ell$.

2   Main results

In this section we present our main results. The following theorem serves as the foundation for many of our more involved results.

Theorem 2.1. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. Let $\delta = \frac{q-1}{d} - \ell - g^\circ$, be the gap between the exponents of the two highest terms. Then $|Z(f)| \leq d(\ell + g^\circ) = q - 1 - d\delta$.*

The following is the main theorem of Section 3 and describes when we are able to guarantee that $|Z(f)| < f^\circ$ for $f(x)$ of the form (3).

Theorem 2.2. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. If one of the following holds, then $|Z(f)| < f^\circ$.*

(1) $d(d+1)\ell + d^2 g^\circ < q - 1$;

(2) $d^2(\ell + g^\circ) \leq q - 1$ and $d(d+1)\ell > q - 1$;

(3) $d^2(\ell + g^\circ) > q - 1$, $d\ell + d^3 g^\circ < q - 1$, and $d(d^2 + 1)\ell + d^3 g^\circ < (q-1)(d+1)$.

The inequalities in the cases within Theorem 2.2 create regions on an g°, ℓ-axis system. See Figure 1 for visualization of when $|Z(f)| < f^\circ$.

At the end of Section 3 we present some results on t-sparse polynomials. Theorem 3.9 is a generalization of Theorem 2.1, giving a bound on $|Z(h)|$ for a t-sparse polynomial h. In Section 4 we refine the arguments used in Theorem 2.2 to obtain lower upper bounds on $|Z(f)|$ for some $f(x)$ as in (3). The following theorem is the main result of Section 4.

Theorem 2.3. *Let $f(x) \in \mathbb{F}_q[x]$ be as in (3).*

(1) If $\ell > \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that

$$\ell + g^\circ < (q-1)\left(\frac{1 + d^{-2i-1}}{d(d+1)}\right),$$

  then
$$|Z(f)| \leq \frac{q-1}{d+1} - d^{2i+2}\left(\ell - \frac{q-1}{d(d+1)}\right).$$

(2) If $\ell + g^\circ < \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that

$$\ell > (q-1)\left(\frac{1 - d^{-2i-2}}{d(d+1)}\right),$$

  then
$$|Z(f)| \leq \frac{q-1}{d+1} - d^{2i+3}\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right).$$

(3) If $\ell \le \frac{q-1}{d(d+1)}$, $\ell + g^\circ \ge \frac{q-1}{d(d+1)}$, and $d(d+1)\ell + d^2 g^\circ < q - 1$, then

$$|Z(f)| \le d(\ell + g^\circ).$$

(4) If $\ell \le \frac{q-1}{d(d+1)}$, $\ell + g^\circ \ge \frac{q-1}{d(d+1)}$, and $d(d+1)\ell + d^2 g^\circ \ge q - 1$, then

$$|Z(f)| \le f^\circ = \frac{q-1}{d} - \ell.$$

3 Improving the degree bound

Our main focus in this section is to identify lacunary polynomials $f(x) \in \mathbb{F}_q[x]$ that must have strictly less than f° distinct nonzero roots. As remarked upon in the introduction, we will consider polynomials $f(x) \in \mathbb{F}_q[x]$ of the form

$$f(x) = x^{\frac{q-1}{d} - \ell} + g(x),$$

where $\ell \ge 0$ and $g^\circ < \frac{q-1}{d} - \ell$. Since we are interested in nonzero roots, we will always assume that the constant term of $f(x)$ is nonzero. Our first two theorems are motivated by the following well-known result in the case $d = 1$, we include a proof for completeness.

Lemma 3.1. *Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^m + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \le g^\circ < m$. Let $\delta = m - g^\circ$ be the gap between the exponents of the two highest terms. Then $|Z(f)| \le q - 1 - \delta$.*

Proof. Note that for any $a \in \mathbb{F}_q^*$, $a^{q-1} = 1$. Consequently, for any $a \in \mathbb{F}_q^*$ we have $a^{q-1-m} f(a) = a^{q-1-m} g(a) + 1$. This gives

$$|Z(f)| = |Z(x^{q-1-m} g(x) + 1)| \le q - 1 - m + g^\circ = q - 1 - \delta.$$

$\square$

If the degree of the polynomial f is bounded by $\frac{q-1}{d}$, then we have the following improved upper bound of $|Z(f)|$.

Theorem 2.1. *Let $\ell \ge 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d} - \ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \le g^\circ < \frac{q-1}{d} - \ell$. Let $\delta = \frac{q-1}{d} - \ell - g^\circ$, be the gap between the exponents of the two highest terms. Then $|Z(f)| \le d(\ell + g^\circ) = q - 1 - d\delta$.*

Proof. Since $Z(f) = Z(x^\ell f)$, we consider the roots of $x^{\frac{q-1}{d}} + x^\ell g(x)$. A root of $x^\ell f(x)$ is a root of

$$\xi + x^\ell g(x), \tag{4}$$

for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Since $g^\circ \ge 1$, (4) has at most g° roots. Combining this with $|(\mathbb{F}_q^*)^{\frac{q-1}{d}}| = d$ gives the required bound.

$\square$

4

For a polynomial $f(x)$ satisfying the hypotheses of Theorem 1.1 that is not a binomial, note that Theorem 2.1 implies that $f^{\circ\circ} = \frac{q-1}{d^2}$. Below is an example when Theorem 2.1 is tight.

Example 3.2. Let p be a prime $p \equiv 7 \pmod{20}, p > 7, d = 2, \ell = 1$ and $g^{\circ} = 2$. By the law of quadratic reciprocity, we have

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{2 \cdot \frac{p-1}{2}} = 1.$$

Since $\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$, we have $\left(\frac{5}{p}\right) = -1$, and so 5 is a quadratic non-residue in $\mathbb{F}_p$. Then -5 is a quadratic residue in $\mathbb{F}_p$ since $p \equiv 3 \pmod{4}$. Let $a \in \mathbb{F}_p$ be such that $-5a = 1$, thus a is a quadratic residue in $\mathbb{F}_p$. Let $S = \{1, 4, 4a\}$. Then S is a subset of quadratic residues and $-S$ is a subset of quadratic non-residues. Define the polynomial

$$f(x) = x^{\frac{p-1}{2}-1} - 16ax^2 - (4a + 5) \in \mathbb{F}_p[x].$$

It is easy to check that $S^{-1} \cup (-S^{-1}) \subseteq Z(f)$. By Theorem 2.1, $|Z(f)| \leq 6$, and so $Z(f) = S^{-1} \cup (-S^{-1})$ and Theorem 2.1 is tight in this case. In particular, when $p = 47$, we can take $S = \{1, 4, 18\}$ and $f(x) = x^{22} + 22x^2 + 24$.

We can combine Theorem 2.1 and the trivial degree bound on $|Z(f)|$ to obtain the following bound, which is independent of the divisor d.

Corollary 3.3. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^{\circ} < \frac{q-1}{d} - \ell$. Then $|Z(f)| \leq \sqrt{(q-1)(\ell + g^{\circ})}$.*

Proof. Note that we have the trivial degree bound $|Z(f)| \leq f^{\circ} \leq \frac{q-1}{d}$, and by Theorem 2.1, $|Z(f)| \leq d(\ell + g^{\circ})$. Therefore, $|Z(f)| \leq \sqrt{\frac{q-1}{d}d(\ell + g^{\circ})} = \sqrt{(q-1)(\ell + g^{\circ})}$. ☐

In the above discussion, we restricted ℓ to be a nonnegative integer. When $\ell < 0$, a similar trick leads to the following theorem.

Theorem 3.4. *Let $m \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}+m} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g^{\circ} < \frac{q-1}{d} + m$. Then $|Z(f)| \leq d\max\{m, g^{\circ}\}$.*

Proof. If $x \neq 0$, then

$$f(x) = \xi x^m + g(x), \tag{5}$$

for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Since $g^{\circ} \geq 1$, and the constant term of g is nonzero, then $\xi x^m + g(x)$ is a nonzero polynomial with degree at most $\max\{m, g^{\circ}\}$, so (5) has at most $\max\{m, g^{\circ}\}$ roots. There are d such $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$ and so the required bound follows.

☐

Below is an example when Theorem 3.4 is tight.

Example 3.5. Let p be a prime $p \equiv 3 \pmod 4, p > 3, d = 2, m = 1$ and $g° = 2$. Let $r_1, r_2 \in \mathbb{F}_p^*$ be any two quadratic residues. Note that $r_1 + r_2 \neq 0$ since $p \equiv 3 \pmod 4$. Let $a \in \mathbb{F}_p$ be such that $a(r_1 + r_2) = -1$. Define the polynomial

$$f(x) = x^{\frac{p-1}{2}+1} + ax^2 + ar_1r_2 \in \mathbb{F}_p[x].$$

It is easy to check that $Z(f) = \{r_1, r_2, -r_1, -r_2\}$.

We remark that in general the best known bounds on the number of zeros of a trinomial are due to Kelley and Owen [6] and recorded in Equation (2). Their bounds are on the order of $\sqrt{q}$ in magnitude. For trinomials satisfying the hypotheses of Theorem 2.1 or Theorem 3.4, the respective theorems offer a significantly better bound on $|Z(f)|$. Examples for which Theorem 2.1 or Theorem 3.4 is tight seem harder to construct for larger $g°$. The example below gives a class of examples for primes p for which -29 is a square in $\mathbb{F}_p$.

Example 3.6. Let p be a prime $p \equiv 31 \pmod{116}, d = 2, m = 1$ and $g° = 4$. Let $S = \{4, 9, 16, -29\}$, using a similar argument as in Example 3.2, we can show S is a subset of quadratic residues and $-S$ is a subset of quadratic non-residues. Define the polynomial

$$f(x) = 6500x^{\frac{p-1}{2}+1} + (x-4)(x-9)(x-16)(x+29) - 6500x \in \mathbb{F}_p[x].$$

It is easy to check that $Z(f) = S \cup (-S)$.

In the above example, $f(x)$ is a 4-sparse polynomial with 8 distinct roots. Kelley's bound in Equation (1) gives a bound on $|Z(f)|$ on the order $p^{2/3}$. Once again this demonstrates that a sparsity-only bound on $|Z(f)|$ such as (1) can be significantly improved if f is also lacunary.

We will see that the above two theorems can be combined and iterated to yield a stronger statement on the size of $|Z(f)|$. The coloured regions in Figure 1 indicate when the degree bound on $|Z(f)|$ can be improved in terms of ℓ and $g°$. We will prove the content of Figure 1 in Theorem 2.2. The numbers on the coloured regions of Figure 1 correspond to the cases described in Theorem 2.2. Next we present a proof of Theorem 2.2.

Theorem 2.2. *Let $\ell \geq 0$ be a nonnegative integer. Suppose $f(x) \in \mathbb{F}_q[x]$ has the form $x^{\frac{q-1}{d}-\ell} + g(x)$, for some $g(x) \in \mathbb{F}_q[x]$ such that $1 \leq g° < \frac{q-1}{d} - \ell$. If one of the following holds, then $|Z(f)| < f°$.*

(1) $d(d+1)\ell + d^2 g° < q - 1$;

(2) $d^2(\ell + g°) \leq q - 1$ *and* $d(d+1)\ell > q - 1$;

(3) $d^2(\ell + g°) > q - 1$, $d\ell + d^3 g° < q - 1$, *and* $d(d^2+1)\ell + d^3 g° < (q-1)(d+1)$.

Proof. By Theorem 2.1, we have $|Z(f)| \leq d(\ell + g°)$, which is an improved bound when $d(\ell + g°) < \frac{q-1}{d} - \ell$, i.e. $d(d+1)\ell + d^2 g° < q - 1$.
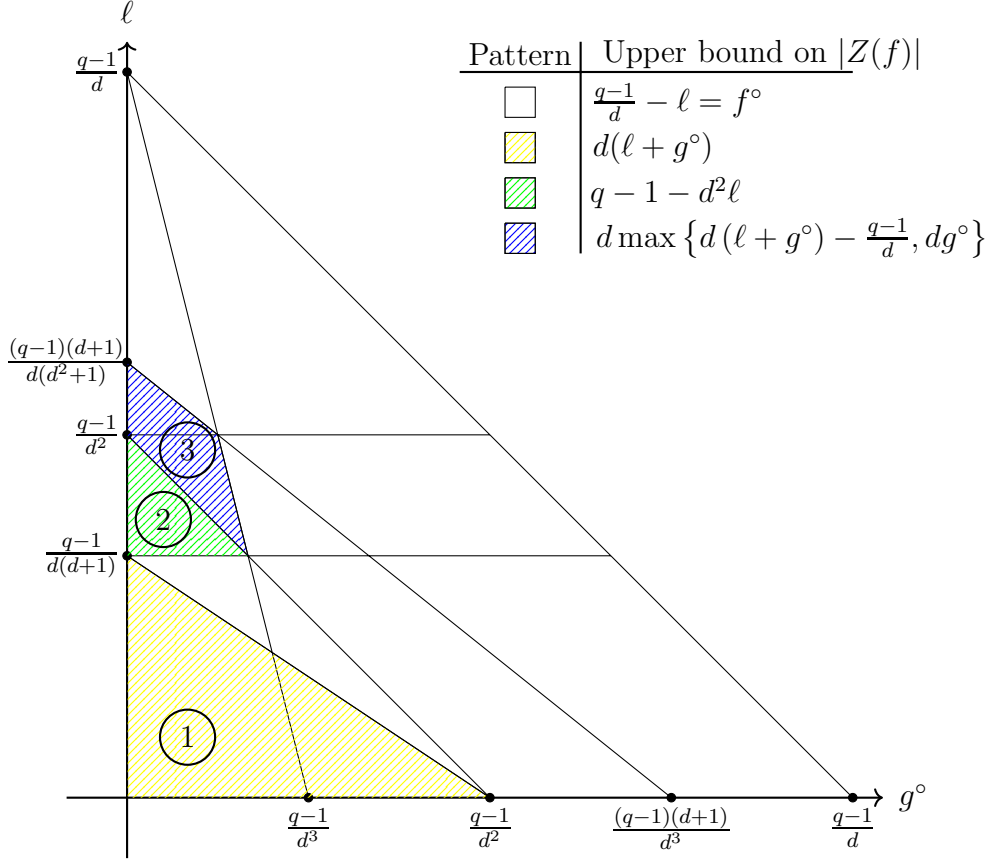
Figure 1: Bounding $|Z(f)|$ for $f(x) = x^{\frac{q-1}{d}-\ell} + g(x)$.

If $\ell = 0$, then obviously (2) and (3) do not hold. In the following discussion, we assume $\ell > 0$. Note the proof of Theorem 2.1 shows that all nonzero roots of $f(x)$ are roots of

$$\prod_{\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}} \left(x^\ell g(x) + \xi\right) = x^{d\ell} g^d(x) - 1, \tag{6}$$

and the constant term of $x^{d\ell} g^d(x) - 1$ is -1 since $\ell > 0$. By using the substitution $x = y^{-1}$ and multiplying by $-y^{d(\ell+g^\circ)}$ in (6), we see the number of roots of (6) is the same as the number of nonzero roots of the following monic polynomial

$$h(y) = y^{d(\ell+g^\circ)} - y^{dg^\circ} g^d(y^{-1}). \tag{7}$$

Note that the degree of h is $d(\ell + g^\circ)$, and the degree of $y^{dg^\circ} g^d(y^{-1})$ is dg°. Let $\ell' = \frac{q-1}{d} - d(\ell + g^\circ)$. We consider two cases.

- If $\ell' \geq 0$, then we can apply Theorem 2.1 to conclude that

$$|Z(f)| \leq |Z(h)| \leq d(\ell' + dg^\circ) = q - 1 - d^2\ell,$$

7

which is an improved bound provided $\frac{q-1}{d} - d(\ell + g^\circ) \geq 0$ and $q - 1 - d^2\ell < \frac{q-1}{d} - \ell$, i.e. $d^2(\ell + g^\circ) \leq q - 1$ and $d(d+1)\ell > q - 1$.

- If $\ell' < 0$, then we can apply Theorem 3.4 to show that

$$|Z(f)| \leq |Z(h)| \leq d \max\left\{-\ell', dg^\circ\right\} = d \max\left\{d(\ell + g^\circ) - \frac{q-1}{d}, dg^\circ\right\},$$

which is an improved bound provided $\frac{q-1}{d} - d(\ell + g^\circ) < 0$ and
$d \max\left\{d(\ell + g^\circ) - \frac{q-1}{d}, dg^\circ\right\} < \frac{q-1}{d} - \ell$, i.e.
$d^2(\ell + g^\circ) > q - 1$, $d^2(\ell + g^\circ) - (q - 1) < \frac{q-1}{d} - \ell$ and $d^2 g^\circ < \frac{q-1}{d} - l$.

$\square$

Below we give examples of polynomials where $|Z(f)| = f^\circ$, showing limitations of extending Theorem 2.2 for a larger range of g°, ℓ.

Example 3.7. Let $D, n \geq 1$ be positive integers such that $D(n + 1)|(q - 1)$. Then $x^{D(n+1)} - 1 = 0$ has $D(n + 1)$ distinct nonzero solutions. Moreover,

$$f(x) = x^{Dn} + x^{D(n-1)} + \cdots + x^D + 1 = \frac{x^{D(n+1)} - 1}{x^D - 1}, \tag{8}$$

has Dn distinct nonzero solutions, i.e. we have a class of lacunary polynomials $f(x)$ with $|Z(f)| = f^\circ$. We will compare these examples to Theorem 2.2 in the case $n = d = 2$. Let
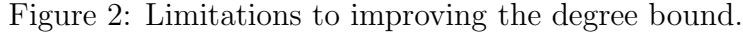$$x^{2D} + x^D + 1 = x^{\frac{q-1}{2} - \ell} + g(x),$$
and so $\ell = (q - 1)/2 - 2D$ and $g^\circ = D$. Therefore such examples lie on a line in the ℓ, g°-axis system used above. In Figure 2 we illustrate the relation between this line of examples and the regions of improvement.

It seems plausible that Theorem 2.2 could be improved to include more regions that appear left of the red dashed line in Figure 2. We leave this as an open problem. We conclude this section with several generalizations of the above results.

Theorem 3.8. *Let $s(x), t(x), g(x) \in \mathbb{F}_q[x]$ be polynomials such that the rational function defined by $r(x) = s(x)/t(x)$ and $g(x)$ are linearly independent. Also let $h(x) \in \mathbb{F}_q[x]$ be a nonconstant polynomial with no zeros in $\mathbb{F}_q^*$. Define the rational function $f(x) = (h(x))^{\frac{q-1}{d}} r(x) + g(x)$. Then the number of distinct nonzero roots of $f(x)$ is at most $d \max\{s^\circ, g^\circ + t^\circ\}$.*

The ideas behind Theorem 2.1 and Theorem 3.4 can be reused to prove Theorem 3.8. Note that the linearly independent assumption is necessary since we need to ensure $\xi s(x) + t(x)g(x)$ is a nonzero polynomial for $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Theorem 3.8 is noteworthy since the polynomials $f(x)$ to which it applies may be neither lacunary nor sparse.

The following is a result for t-sparse polynomials. It extends Theorem 2.1 and Theorem 3.4. The proof employs a similar argument to those seen above. Note that Theorem 3.9 does not require a polynomial with degree close to $\frac{q-1}{d}$.

8

Figure 2: Limitations to improving the degree bound.

Theorem 3.9. *Let*

$$h(x) = \sum_{i=1}^{t} c_i x^{e_i} \in \mathbb{F}_q[x],$$

be a t-sparse polynomial. Suppose that there exist integers $a_i, b_i,\ i = 1, 2, \ldots, t$ *such that*

$$e_i = a_i \frac{q-1}{d} + b_i, \ \text{ where } \ -\frac{q-1}{d} < b_i < \frac{q-1}{d}.$$

Let A, B *be integers such that* $\{b_i : 1 \le i \le t\}$ *are contained in the interval* $[A, B]$. *If* $h(x)$ *does not vanish on any coset of* $(\mathbb{F}_q^*)^d$ *in* $\mathbb{F}_q^*$, *then* $|Z(h)| \le d(B - A)$.

Proof. Let $\{\xi_1, \ldots, \xi_d\} = (\mathbb{F}_q^*)^{\frac{q-1}{d}}$ and define $S_i = \{a \in \mathbb{F}_q^* \colon a^{\frac{q-1}{d}} = \xi_i\}$. Note that $S_1, \ldots, S_d$ are the cosets of $\mathbb{F}_q^*$ of size $\frac{q-1}{d}$. Fix an i in $[1, t]$. For $y \in S_i$ we have

$$y^{-A} h(y) = y^{-A} \sum_{i=1}^{t} c_i y^{e_i} = \sum_{i=1}^{t} c_i \xi_i^{a_i} y^{b_i - A}. \tag{9}$$

Observe that above expression is a polynomial in y. Moreover, since h does not vanish on any coset of $\mathbb{F}_q^*$ of size $\frac{q-1}{d}$, (9) is a nonzero polynomial with degree at most $B - A$. Therefore, for each i, h has at most $B - A$ zeros in S_i. It follows that $|Z(h)| \le d(B - A)$. $\qquad\square$

We remark that the assumption that $h(x)$ does not vanish on any coset of $(\mathbb{F}_q^*)^d$ in $\mathbb{F}_q^*$ is often guaranteed. This is the case for the polynomials we will discuss in the remaining of the section. Below we see an example of Theorem 3.9 in practice.

Example 3.10. Let $h(x) = \sum_{j=1}^{m} c_j x^{\frac{q-1}{d_j}} + ax + b$, where $d_j \mid (q-1)$ and $d_j < q-1$. Take $d = \text{lcm}\{d_1, d_2, \ldots, d_m\}$, then it follows that the interval we obtained is $[A, B] = [0, 1]$ since $\frac{q-1}{d}$ divides all the exponents expect the linear term and the constant term. So $|Z(h)| \leq d = \text{lcm}\{d_1, d_2, \ldots, d_m\}$.

Theorem 2.1 and Theorem 3.4 can be obtained from Theorem 3.9 in the following way. For Theorem 2.1, we can take the interval $[A, B]$ to be $[-\ell, g^\circ]$. For Theorem 3.4, we can take the interval $[A, B]$ to be $[0, \max\{m, g^\circ\}]$. Theorem 3.9 is strongest when the remainders of the exponents dividing $\frac{q-1}{d}$ are concentrated in a short interval.

The following is a corollary of Theorem 3.9. It generalizes Theorem 2.1. The point is that if a large gap appears between any consecutive exponents, then an improved bound on the number of distinct roots may be possible.

Corollary 3.11. *Let* $h(x) = \sum_{i=1}^{t} c_i x^{e_i} \in \mathbb{F}_q[x]$ *be a* t*-sparse polynomial, where* $\frac{q-1}{d} \geq e_1 > e_2 > \cdots > e_t$. *Define the gap* δ *of* $h(x)$ *to be the largest difference between consecutive exponents, i.e.* $\delta = \max\{e_{i-1} - e_i : 2 \leq i \leq t\}$, *then* $|Z(h)| \leq q - 1 - d\delta$.

Proof. Suppose $\delta = e_{j-1} - e_j$, then the exponents modulo $\frac{q-1}{d}$ are all contained in the interval $[-(\frac{q-1}{d} - e_{j-1}), e_j]$. By Theorem 3.9, $|Z(h)| \leq d(e_j + \frac{q-1}{d} - e_{j-1}) = q - 1 - d\delta$. $\quad\square$

We remark that Karpinski and Shparlinski's bound $|Z(h)| \leq \frac{t-1}{t}(q-1)$ given in [4] can be recovered from the above corollary by taking $d = 1$.

4   Iterating to obtain stronger bounds on $|Z(f)|$

In this section we build on the ideas presented in the proof of Theorem 2.2. In particular we iterate the argument of Theorem 2.2 as many times as possible, to yield a stronger bound on $|Z(f)|$. Throughout this section, $d, \ell \geq 1$ will be positive integers such that $d \mid (q-1)$ and $\frac{q-1}{d} - \ell > 1$, $g(x) \in \mathbb{F}_q[x]$ will be such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$, $x \nmid g(x)$, and $f(x) \in \mathbb{F}_q[x]$ will be given by

$$f(x) = x^{\frac{q-1}{d} - \ell} + g(x).$$

Put $\ell_0 = \ell$, and $g_0(x) = g(x)$. For $i \geq 0$, define

$$g_{i+1}(x) = -x^{dg_i^\circ} g_i^d(x^{-1}), \quad \text{and} \quad \ell_{i+1} = \frac{q-1}{d} - d(\ell_i + g_i^\circ). \tag{10}$$

Lemma 4.1. *Let the sequences* $\{g_i\}_{i \geq 0}$, $\{\ell_i\}_{i \geq 0}$ *be as in* (10). *Suppose that for an integer* $k \geq -1$ *we have*

$$d(\ell_i + g_i^\circ) < \frac{q-1}{d}, \quad for \quad 0 \leq i \leq k.$$

Then

$$|Z(f)| \leq \min_{0 \leq i \leq k+1} d(\ell_i + g_i^\circ).$$

Proof. The case $k = -1$ is Theorem 2.1. Suppose the hypothesis of the theorem holds for $k \geq 0$. Put

$$f_i(x) = x^{\frac{q-1}{d} - \ell_i} + g_i(x).$$

Note that $f_0 = f$. Fix any i, $0 \leq i \leq k+1$. If $i = 0$, then $\ell_i > 0$ by definition. For $i \geq 1$, since $d(\ell_{i-1} + g_{i-1}^\circ) < \frac{q-1}{d}$, we again have $\ell_i > 0$. A nonzero root of $f_i(x)$ is a root of $x^{\ell_i} f_i(x)$, and therefore is also a root of

$$\prod_{\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}} \left(x^{\ell_i} g_i(x) + \xi \right) = x^{d\ell_i} g_i^d(x) - 1.$$

Substituting $x = y^{-1}$ and multiplying by $-y^{d(\ell_i + g_i^\circ)}$ in the above gives the polynomial

$$y^{d(\ell_i + g_i^\circ)} - y^{dg_i^\circ} g_i^d(y^{-1}) = f_{i+1}(y).$$

Therefore $|Z(f_{i+1})| \geq |Z(f_i)|$. Since $|Z(f_{i+1})| \leq f_{i+1}^\circ$, we have the desired result. $\square$

Lemma 4.1 potentially provides many upper bounds on $|Z(f)|$. To aid with determining the best bound, we use explicit formulae for the sequences $\{g_i^\circ\}, \{\ell_i + g_i^\circ\}$.

Lemma 4.2. *The sequences $\{g_i^\circ\}$ and $\{\ell_i + g_i^\circ\}$ are given by*

$$g_i^\circ = d^i g^\circ,$$

and

$$\ell_i + g_i^\circ = \begin{cases} d^i(\ell + g^\circ) - \frac{q-1}{d(d+1)}(d^i - 1) & \text{if } i \text{ is even;} \\ -d^i \ell + \frac{q-1}{d(d+1)}(d^i + 1) & \text{if } i \text{ is odd.} \end{cases}$$

Proof. From the assumption that $g(x)$ has a nonzero constant term and the recurrence relation $g_{i+1}(x) = -x^{dg^\circ} g_i^d(x^{-1})$, the first statement immediately follows. For the second statement, note that $\ell_{i+1} = \frac{q-1}{d} - d(\ell_i + g_i^\circ)$ implies that

$$\ell_{i+1} + g_{i+1}^\circ = \frac{q-1}{d} - d\ell_i = \frac{q-1}{d} - d(\ell_i + g_i^\circ) + d^{i+1}g^\circ.$$

Dividing d^{i+1} on both sides yields

$$\frac{\ell_{i+1} + g_{i+1}^\circ}{d^{i+1}} = \frac{q-1}{d^{i+2}} - \frac{\ell_i + g_i^\circ}{d^i} + g^\circ.$$

Now if we set $a_i = \frac{\ell_i + g_i^\circ}{d^i}$ for $i \geq 0$, then we get $a_0 = \ell + g^\circ$, and $a_{i+1} + a_i = \frac{q-1}{d^{i+2}} + g^\circ$ for $i \geq 0$. If i is odd, then

$$a_i = (a_i + a_{i-1}) - (a_{i-1} + a_{i-2}) + \cdots + (a_1 + a_0) - a_0$$
$$= -\ell + \frac{(q-1)(1-d)(1+d^{-i})}{d(1-d^2)} = -\ell + \frac{(q-1)(1+d^{-i})}{d(d+1)}.$$

11

If i is even, then

$$a_i = (a_i + a_{i-1}) - (a_{i-1} + a_{i-2}) + \cdots + (a_2 + a_1) - (a_1 + a_0) + a_0$$

$$= \ell + g^\circ + \frac{(q-1)(1-d)(1-d^{-i})}{d(1-d^2)} = \ell + g^\circ + \frac{(q-1)(1-d^{-i})}{d(d+1)}.$$

Now applying the relation $\ell_i + g_i^\circ = d^i a_i$ gives the required result. $\qquad\square$

From now on, we will use Lemma 4.2 without explicitly saying so. If $d = 1$, then the sequence $\{\ell_i + g_i^\circ\}$ oscillates between the values $\ell + g^\circ$ and $q - 1 - \ell$, and so nothing is gained by considering later terms in $\{d(\ell_i + g_i^\circ)\}$. We will only consider $d \geq 2$. Now better estimates of $|Z(f)|$ may appear later in the sequence $\{d(\ell_i + g_i^\circ)\}$. For example, the first five terms of $\{d(\ell_i + g_i^\circ)\}$ are

$$d(\ell + g^\circ), \ q - 1 - d^2\ell, \ d^3(\ell + g^\circ) - (q-1)(d-1),$$

$$(q-1)(d^2 - d + 1) - d^4\ell, \ d^5(\ell + g^\circ) - (q-1)(d^3 - d^2 + d - 1). \qquad (11)$$

In Figure 3 we illustrate which bound in Equation (11) is best when it is applicable. The formulae in Lemma 4.2 can be used to determine the minimum $d(\ell_i + g_i^\circ)$.

Lemma 4.3. *(1)* If $\ell > \frac{q-1}{d(d+1)}$, then for all $i > j \geq 0$ and $t \geq 0$,

$$\ell_{2i+1} + g_{2i+1}^\circ < \ell_{2j+1} + g_{2j+1}^\circ < \frac{q-1}{d} - \ell, \quad and \quad \ell_{2i+1} + g_{2i+1}^\circ < \ell_{2t} + g_{2t}^\circ.$$

(2) If $\ell + g^\circ < \frac{q-1}{d(d+1)}$, then for all $i > j \geq 0$ and $t \geq 0$,

$$\ell_{2i} + g_{2i}^\circ < \ell_{2j} + g_{2j}^\circ < \frac{q-1}{d} - \ell, \quad and \quad \ell_{2i} + g_{2i}^\circ < \ell_{2t+1} + g_{2t+1}^\circ.$$

(3) If $\ell \leq \frac{q-1}{d(d+1)}$, and $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, then for all $i > j \geq 0$,

$$\ell_{2i} + g_{2i}^\circ \geq \ell_{2j} + g_{2j}^\circ, \quad and \quad \ell_{2i+1} + g_{2i+1}^\circ \geq \ell_{2j+1} + g_{2j+1}^\circ.$$

Proof. By Lemma 4.2, for each $i \geq 0$, we have

$$\ell_{2i} + g_{2i}^\circ = \frac{q-1}{d(d+1)} + d^{2i}\left(\ell + g^\circ - \frac{q-1}{d(d+1)}\right), \quad \ell_{2i+1} + g_{2i+1}^\circ = \frac{q-1}{d(d+1)} + d^{2i+1}\left(\frac{q-1}{d(d+1)} - \ell\right).$$

To determine the monotonicity of the two sequences, it suffices to compare the size of $\ell + g^\circ, \ell$ and $\frac{q-1}{d(d+1)}$. Therefore, there are the following three cases:

(1) If $\ell > \frac{q-1}{d(d+1)}$, then the sequence $\{\ell_{2i} + g_{2i}^\circ\}$ is strictly increasing, the sequence $\{\ell_{2i+1} + g_{2i+1}^\circ\}$ is strictly decreasing, and $\ell_1 + g_1^\circ < \ell_0 + g_0^\circ$.

(2) If $\ell + g^\circ < \frac{q-1}{d(d+1)}$, then the sequence $\{\ell_{2i} + g_{2i}^\circ\}$ is strictly decreasing, the sequence $\{\ell_{2i+1} + g_{2i+1}^\circ\}$ is strictly increasing, and $\ell_1 + g_1^\circ > \ell_0 + g_0^\circ$.

(3) If $\ell \leq \frac{q-1}{d(d+1)}$, and $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, then both sequences $\{\ell_{2i} + g_{2i}^\circ\}$ and $\{\ell_{2i+1} + g_{2i+1}^\circ\}$ are increasing.
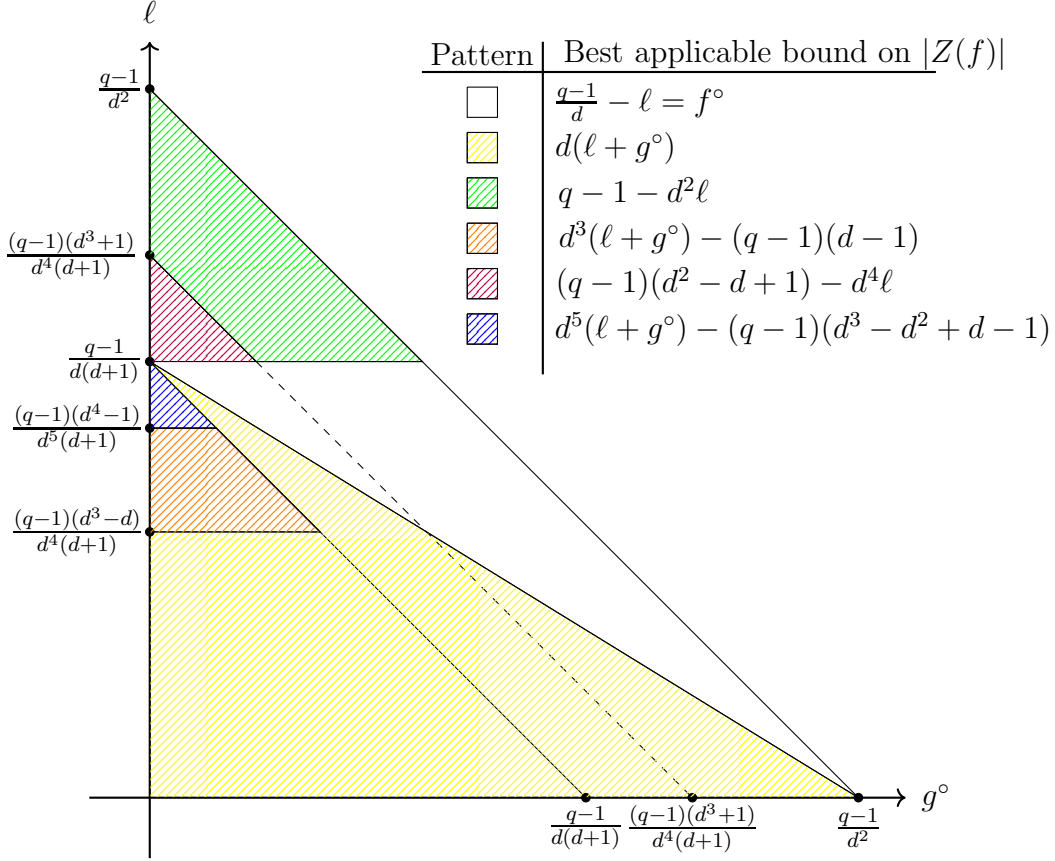
12

Figure 3: Comparing the six bounds in (11) for $|Z(f)|$

$\square$

It remains to understand the inequalities $d(\ell_i + g_i^\circ) \leq \frac{q-1}{d}$. Using the formulae in Lemma 4.2, we see that for $i \geq 0$, $d(\ell_{2i} + g_{2i}^\circ) \leq \frac{q-1}{d}$ is equivalent to

$$\ell + g^\circ \leq (q-1)\left(\frac{1 + d^{-2i-1}}{d(d+1)}\right).$$

And for $i \geq 0$, $d(\ell_{2i+1} + g_{2i+1}^\circ) \leq \frac{q-1}{d}$ is equivalent to

$$\ell \geq (q-1)\left(\frac{1 - d^{-2i-2}}{d(d+1)}\right).$$

The following theorem puts the above discussion together. We use Lemma 4.3 to determine what bound from Lemma 4.1 is best. Now we are ready to prove our main result, Theorem 2.3. We restate the theorem for convenience.

Theorem 2.3. *Let $f(x) \in \mathbb{F}_q[x]$ be as in (3) and assume that the constant term of f is nonzero. Then exactly one of the following holds.*

13

(1) *If $\ell > \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell + g^\circ < (q-1)\left(\frac{1 + d^{-2i-1}}{d(d+1)}\right), \tag{12}$$

then

$$|Z(f)| \leq \frac{q-1}{d+1} - d^{2i+2}\left(\ell - \frac{q-1}{d(d+1)}\right).$$

(2) *If $\ell + g^\circ < \frac{q-1}{d(d+1)}$ and $i \geq -1$ is the largest integer such that*

$$\ell > (q-1)\left(\frac{1 - d^{-2i-2}}{d(d+1)}\right), \tag{13}$$

then

$$|Z(f)| \leq \frac{q-1}{d+1} - d^{2i+3}\left(\frac{q-1}{d(d+1)} - (\ell + g^\circ)\right).$$

(3) *If $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, and $d(d+1)\ell + d^2 g^\circ < q-1$, then*

$$|Z(f)| \leq d(\ell + g^\circ).$$

(4) *If $\ell \leq \frac{q-1}{d(d+1)}$, $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, and $d(d+1)\ell + d^2 g^\circ \geq q-1$, then*

$$|Z|(f)| \leq f^\circ = \frac{q-1}{d} - \ell.$$

Proof. **(1)** The condition $\ell > \frac{q-1}{d(d+1)}$ gives that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all odd $j \geq 1$. Equation (12) implies that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all even $0 \leq j \leq 2i$. By Lemma 4.1, $|Z(f)| \leq d(\ell_j + g_j^\circ)$ for $0 \leq j \leq 2i+1$. By Lemma 4.3, the lowest upper bound of this set is

$$d(\ell_{2i+1} + g_{2i+1}^\circ) = \frac{q-1}{d+1}\left(d^{2i+1} + 1\right) - d^{2i+2}\ell.$$

(2) The condition $\ell + g^\circ < \frac{q-1}{d(d+1)}$ gives that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all even $j \geq 0$. Equation (13) implies that $d(\ell_j + g_j^\circ) < \frac{q-1}{d}$ for all odd $1 \leq j \leq 2i+1$. By Lemma 4.1, $|Z(f)| \leq d(\ell_j + g_j^\circ)$ for $0 \leq j \leq 2i+2$. By Lemma 4.3, the lowest upper bound of this set is

$$d(\ell_{2i+2} + g_{2i+2}^\circ) = d^{2i+3}(\ell + g^\circ) - \frac{q-1}{d+1}\left(d^{2i+2} - 1\right).$$

(3&4) If $\ell \leq \frac{q-1}{d(d+1)}$ and $\ell + g^\circ \geq \frac{q-1}{d(d+1)}$, then by Lemma 4.3, $\{d(\ell_{2i} + g_{2i}^\circ)\}_{i \geq 0}$ is increasing. Similarly, $\{d(\ell_{2i+1} + g_{2i+1}^\circ)\}_{i \geq 0}$ is increasing and $f^\circ < d(\ell_1 + g_1^\circ)$. Therefore either f° or $d(\ell + g^\circ)$ is the lowest upper bound on $|Z(f)|$, and the remaining two cases follow immediately.

$\square$

To illustrate how the bound improves over the iteration employed in Theorem 2.3, consider the difference between the bound on $|Z(f)|$ given in part (2) of Theorem 2.3 and the degree bound.

$$\frac{q-1}{d} - \ell - \left(\frac{q-1}{d+1} - d^{2i+3} \left(\frac{q-1}{d(d+1)} - (\ell + g^\circ) \right) \right)$$

$$= \left(1 + d^{2i+3} \right) \left(\frac{q-1}{d(d+1)} - (\ell + g^\circ) \right) + g^\circ.$$

In other words, the difference in the degree bound and the iterative bound grows exponentially in the number of iterations.

In Example 3.2 and in Example 3.7, we saw that the bound in cases (3) and (4) of Theorem 2.3 can be tight. The following is an example where the bound in case (1) of Theorem 2.3 is tight.

Example 4.4. Let $p = 379$, $d = 2$, $\ell = \frac{p-7}{4} = 93$, $g^\circ = 1$, and $f(x) = x^{96} + x + 317 \in \mathbb{F}_p[x]$. Below we give $f_i(x) = x^{\frac{q-1}{d} - \ell_i} + g_i(x)$ for $i = 1, 2$. These are the polynomials formed in the iteration technique and have the property $|Z(f)| \le |Z(f_i)|$.

$$f_1(x) = x^{188} - 54x^2 - 255x - 1, \quad f_2(x) = x^6 + 378x^4 + 248x^3 + 55x^2 + 127x + 116.$$

Therefore $|Z(f)| \le |Z(f_1)| \le |Z(f_2)| \le 6$. Note that we can also bound $|Z(f)|$ by applying Theorem 2.3 which gives $|Z(f)| \le p - 1 - d^2\ell = 6$. Indeed, we can verify that $Z(f) = \{21, 37, 89, 303, 322, 365\}$, so the iterative technique gives a tight bound in this case.

Below is an example where the bound in case (2) of Theorem 2.3 is close to tight.

Example 4.5. Let $p = 367$, $d = 2$, $\ell = \frac{p+1}{8} = 46$, $g^\circ = 1$, and $f(x) = x^{137} + x + 111 \in \mathbb{F}_p[x]$. By Theorem 2.3, we can take $i = 1$ and get $|Z(f)| \le d^3(\ell + g^\circ) - (p-1)(d-1) = 8(\ell + g^\circ) - (p-1) = 10$. We can verify that $Z(f) = \{82, 105, 109, 195, 216, 246, 333\}$.

Note that in the two above examples, the degree bound on $|Z(f)|$ and the bound obtained by earlier stages of the iteration are very far from the true size of $|Z(f)|$. This demonstrates the effectiveness of the iterative technique.

5   Concluding remarks

The main theorem of Section 4, Theorem 2.3 was proved by iterating Theorem 2.1 as many times as possible. A more complicated procedure involving both Theorem 2.1 and Theorem 3.4 can be used in some cases to obtain bounds on $|Z(f)|$ for more pairs of g°, ℓ. Indeed, this idea was partly used in the proof of Theorem 2.2.

We expect there are ways to extend some of our results. We propose the following problem, which would extend Theorem 2.2.

Problem 5.1. *For what pairs of g°, ℓ can the degree bound on $|Z(f)|$ in (3) be improved?*

6   Acknowledgements

References

[1] S. Ball, A. Blokhuis, Lacunary polynomials over finite fields, in G. Mullen, D. Panario (Eds.), *Handbook of Finite Fields*, (2013), pp. 556-562. CRC Press.

[2] K. Bibak, I. Shparlinski, On Fully Split Lacunary Polynomials in Finite Fields, *Bulletin Polish Acad. Sci. Math.* 59 (2011), 197-202.

[3] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, I. Shparlinski, On the statistical properties of Diffie-Hellman distributions, *Israel J. Math.* 120 (2000), 23-46.

[4] M. Karpinski, I. Shparlinski, On some approximation problems concerning sparse polynomials over finite fields, *Theoretical Computer Science*, 157 (1996), 259-266.

[5] Z. Kelley, Roots of Sparse Polynomials over a Finite Field, *LMS J. Comput. Math.* 19 (2016), 196-204.

[6] Z. Kelley, S. Owen, Estimating the Number Of Roots of Trinomials over Finite Fields, *Journal of Symbolic Computation*, 79 (2017), 108-118.

[7] L. Rédei, "Lückenhafte Polynome über endlichen Körperrn," Birkhäuser, Basel, 1970 (Engl. trans. Lacunary Polynomials over Finite Fields, North Holland, Amsterdam, 1973).