Counting distinct roots of a Lacunary polynomial over a finite field

Ethan White
University of British Columbia

Joint work with József Solymosi and Chi Hoi Yip

Carleton Combinatorics Meeting

August 5, 2021

Lacunary polynomials

Definition (Lacunary)

A polynomial is lacunary if there is a gap between the exponent in consecutive terms, e.g. $x^{11} - 3x + 1$.

Notation

Throughout q denotes a prime power, and d will always be a divisor of $q-1$. For $f \in \mathbb{F}_q[x]$ denote by $|Z(f)|$ the number of distinct nonzero roots of f in $\mathbb{F}_q$. Also we use the shorthand $\deg(f) = f^{\circ}$.

Finite fields

Key Observation

$$\#\{x^{\frac{q-1}{d}} : x \in \mathbb{F}_q^*\} = d.$$

Easy consequence: Let $g^\circ < \frac{q-1}{d}$. Solutions to

$$f(x) = x^{\frac{q-1}{d}} + g(x) = 0$$

look like

$$\xi + g(x) = 0$$

for $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. Hence $|Z(f)| \leq dg^\circ$.

Extensions with $f^\circ \leq \frac{q-1}{d}$

Theorem (Solymosi, W., Yip 2021)

Let $\ell \geq 0$ and $d | (q-1)$. Let $g(x) \in \mathbb{F}_q[x]$ be such that $1 \leq g^\circ < \frac{q-1}{d} - \ell$. Then for $f(x) = x^{\frac{q-1}{d} - \ell} + g(x)$ we have

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

Proof of Theorem:

$$|Z(x^\ell f(x))| = |Z(f)|.$$

Therefore $x^\ell f(x) = x^{\frac{q-1}{d}} + x^\ell g(x) = 0$ takes the form $\xi + x^\ell g(x) = 0$ for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. For fixed ξ, $\xi + x^\ell g(x) = 0$ has at most $\ell + g^\circ$ solutions.

Extensions with $f^\circ \geq \frac{q-1}{d}$

Theorem (Solymosi, W., Yip 2021)

Let $m \geq 0$ and $d|(q-1)$. Let $g(x) \in \mathbb{F}_q[x]$ be such that $1 \leq g^\circ < \frac{q-1}{d} + m$. Then for $f(x) = x^{\frac{q-1}{d}+m} + g(x)$ we have

$$|Z(f)| \leq d \max\{m, g^\circ\}.$$

Proof of Theorem: All solutions to $f(x) = 0$ take the form

$$\xi x^m + g(x) = 0,$$

for some $\xi \in (\mathbb{F}_q^*)^{\frac{q-1}{d}}$. For each fixed ξ, the number of solutions to the above is bounded by $\max\{m, g^\circ\}$.

Beating the degree bound

Question: when can we guarantee $|Z(f)| < \deg(f)$? (for lacunary f)

Theorem (Solymosi, W., Yip 2021)

Let $\ell \geq 0$. 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 $d(d^2+1)\ell + d^3 g^\circ < (q-1)(d+1)$.

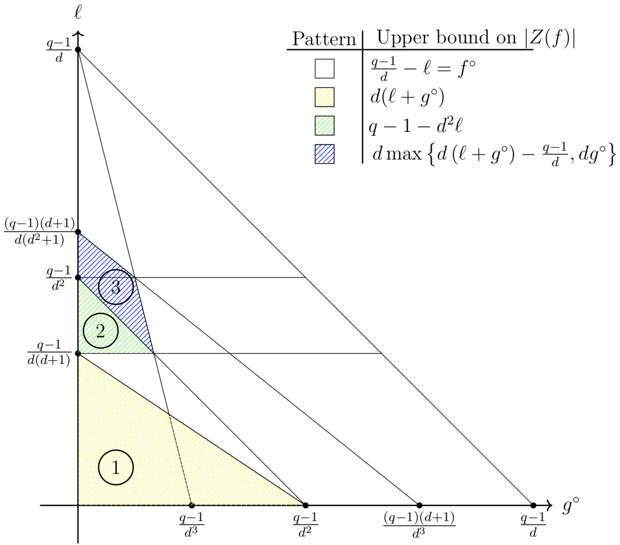

Figure 1: Bounding $|Z(f)|$ for $f(x) = x^{\frac{q-1}{d} - \ell} + g(x)$.

Beating the degree bound: Proof ideas

Main idea: Iterate previous techniques. Partial sketch:

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

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

Substitute $x \mapsto x^{-1}$ and multiply through by the degree, $d\ell + dg^{\circ}$:

$$x^{d(\ell+g^{\circ})} - x^{dg^{\circ}} g^{d}(x^{-1}).$$

The above is lacunary, let $d(\ell + g^{\circ}) = (q-1)/d - \ell'$ and apply the earlier theorem to obtain

$$|Z(f)| \leq q - 1 - d^2\ell.$$

Beating the degree bound: Limiting example

Let n, D be positive integers such that $(n+1)D$ divides $q-1$. Then

$$x^{nD} + x^{(n-1)D} + \cdots + 1 = \frac{x^{(n+1)D} - 1}{x^D - 1}$$

has nD distinct roots. Taking $n = 2$ and $d = 2$ we see that

$$f(x) = x^{2D} + x^D + 1 = x^{\frac{q-1}{2} - \ell} + g(x),$$

has $|Z(f)| = f^\circ$ so long as $3D$ divides $q-1$. Since $g^\circ = D$ we see that for this class of examples

$$f^\circ = 2D = \frac{q-1}{2} - \ell = 2g^\circ,$$

thereby giving a 'limiting line' on the g°, ℓ axes.

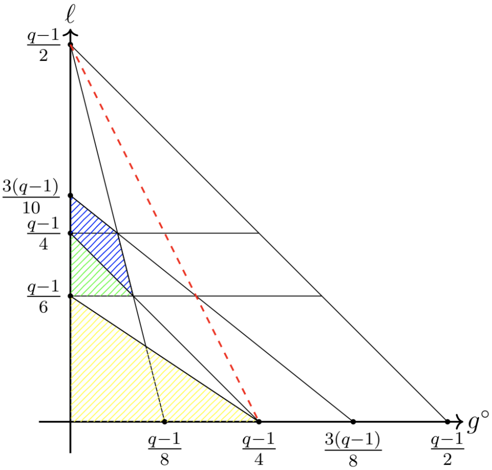

Figure 2: Limitations to improving the degree bound.

Iterating the method

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

$$\to x^{d\ell} g^{d}(x) - 1 \to x^{d(\ell + g^{\circ})} - x^{dg^{\circ}} g^{d}(x^{-1}) = x^{\frac{q-1}{d}-\ell_1} + g_1(x).$$

If we repeat this sequence of steps we obtain a recurrence

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

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

Analyzing the recurrence

Theorem (Solymosi, W., Yip 2021)

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

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

Example

Let $p = 379$, $d = 2$, $\ell = \frac{p-7}{4} = 93, g^\circ = 1$, and $f(x) = x^{96} + x + 317 \in \mathbb{F}_p[x]$. Using iteration we have $|Z(f)| \leq |Z(f_i)|$ for

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