Canad. Math. Bull. Vol. 63 (1), 2020 pp. 187–196
http://dx.doi.org/10.4153/S0008439519000316

Value Sets of Sparse Polynomials

Igor E. Shparlinski and José Felipe Voloch

Abstract. We obtain a new lower bound on the size of the value set $\mathscr{V}(f) = f(\mathbb{F}_p)$ of a sparse polynomial $f \in \mathbb{F}_p[X]$ over a finite field of p elements when p is prime. This bound is uniform with respect to the degree and depends on some natural arithmetic properties of the degrees of the monomial terms of f and the number of these terms. Our result is stronger than those that can be extracted from the bounds on multiplicities of individual values in $\mathscr{V}(f)$.

1 Introduction

The value set of a polynomial $f(X) \in \mathbb{F}_q[X]$ over a finite field $\mathbb{F}_q$ of q elements, is the set $\mathscr{V}(f) = \{f(a) : a \in \mathbb{F}_q\}$ and we define $V(f) = \#\mathscr{V}(f)$. The problem of estimating $V(f)$ in terms of f has been actively studied for over a half a century; see [BS-D59, CLMS61, Mil64, WSC93] for some classical results, and [MZ13] for a brief survey. We also refer to [Kur09] for a more recent result about the distribution of elements in $\mathscr{V}(f)$.

For example, it is known that

$$V(f) \ge \left\lfloor \frac{q-1}{\deg f} \right\rfloor + 1$$

(which is slightly more precise than the trivial bound $V(f) \ge q/\deg f$ based on the fact that $f(x) = c$ has at most $\deg f$ solutions for any c), and, in fact, polynomials which attain equality in that bound are fully classified [CLMS61, Mil64]. Given additional conditions on f, this lower bound can sometimes be improved, for example, for a prime $q = p$; by [WSC93, Corollary 2.5] we have

$$V(f) \ge \left\lfloor \frac{p-1}{\deg f} \right\rfloor + \left\lfloor \frac{2(p-1)}{(\deg f)^2} \right\rfloor,$$

provided that $\deg f \nmid p-1$. One can also find in [WSC93] some nontrivial upper bounds on $V(f)$, provided that $V(f) < q$, *i.e.*, that f is not a permutation polynomial.

In this paper, we study the question of bounding $V(f)$ from below as a function of the number of terms in f, rather than its degree. Specifically, if

$$f(X) = a_0 + \sum_{i=1}^{t} a_i X^{n_i},$$

Received by the editors September 17, 2018; revised May 29, 2019.
Published online on Cambridge Core September 24, 2019.
Author I. E. S. was supported by ARC Grants DP170100786 and DP180100201.
AMS subject classification: **11T06**, 14G15.
Keywords: sparse polynomial, value set, rational point on curve.

we want to estimate $V(f)$ in terms of t and q. When the degree of f is much higher than t, the polynomial f is said to be sparse. One can bound the number of roots of sparse polynomials [CFKLLS, Lemma 7], [Kel16, Theorems 2.2 and 2.3] and convert this to a lower bound on $V(f)$, as above. Oftentimes, as described in [BCR16, CGRW17], a sparse polynomial may have many roots. We prove, however, that for $q = p$ prime, one can give a nontrivial lower bound on $V(f)$, for f sparse, even when equations of the form $f(x) = a$ have many roots in $\mathbb{F}_p$. In addition, this bound is always better than the one obtained from the upper bound of [CFKLLS, Lemma 7] or [Kel16, Theorems 2.2 and 2.3] on the number of roots, when it applies, for $t \geq 9$.

We obtain our results in three steps. First, using a monomial change of variables, we reduce the degree of the polynomial [CFKLLS]. Second, we bound the number of irreducible components of $f(X) - f(Y)$ by adapting a result of Zannier [Zan07]. Finally, we use the results of [Vol89] to get our bounds.

We also give a special treatment in the case of binomials, via different arguments, and we obtain stronger results in that case.

2 Factors of Differences of Sparse Laurent Polynomials

We start with the following version of [Vol85, Theorem 4], and refer to [St09] for background on function fields. For example, we recall that the degree of an element u of a function field K over a field of constants F is defined as $\deg u = [K{:}F(u)]$ if u is not in F and zero otherwise. We also define the degree of the point $(u_1 : \cdots : u_t)$ in a projective space over K as

$$\deg(u_1 : \cdots : u_m) = \max \deg\Big(\sum_i \alpha_i u_i\Big),$$

where the α_i vary in an algebraic closure of F. Such a point defines a morphism from the curve whose function field is K to projective space and the degree of the point is the degree of the morphism. A morphism as above is classical in the sense of [SV86] if there is a valuation v of K and linear combinations $w_1, \ldots, w_t$ of $u_1, \ldots, u_t$ with coefficients in F such that $v(w_i) = i - 1$ for $i = 1, \ldots, t$.

Lemma 2.1 *Let K be a function field of genus g with a field of constants F of characteristic p and let S be a finite set of places of K. If $u_1, \ldots, u_t$ are S-units of K, linearly independent over F, satisfying*

$$\deg(u_1 : \cdots : u_t) < p \quad \textit{and} \quad u_1 + \cdots + u_t = 1,$$

then

$$\max_{i=1,\ldots,t} \deg u_i \leq \frac{t(t-1)}{2}(2g - 2 + \#S).$$

Proof The condition $\deg(u_1 : \cdots : u_t) < p$ means that the degree of the corresponding morphism is less than p and [SV86, Corollary 1.8] states that a morphism whose degree is less than p is classical in the above sense. It also ensures that [Vol85, Equation (3)] holds and, with that, the proof of [Vol85, Theorem 4] goes through verbatim in the present situation, and its conclusion is the desired inequality. ■

We say a polynomial $g(X,Y)$ is a factor of a rational function $f(X,Y)$ if it is a factor of its numerator (in lowest terms).

The following result and its proof are motivated by a result of Zannier [Zan07]. We recall that Zannier proved a conjecture of Schinzel to the effect that a sparse polynomial in characteristic zero is not the composition of two other polynomials except in a few exceptional cases. This is achieved by investigating the factors of $f(X) - f(Y)$ for a sparse univariate polynomial $f(X)$, which is directly related to our situation.

Theorem 2.2 *Let F be a field of positive characteristic p and let*

$$f(X) = \sum_{i=1}^{t} a_i X^{n_i} \in F(X)$$

be a nonconstant Laurent polynomial over F with $a_i \neq 0$ *and nonzero integer exponents* $n_1 < \cdots < n_t$ *with* $n_t \geq |n_i|$ *for all* $i = 1, \ldots, t$*. If* $h(X,Y)$ *is an irreducible polynomial factor of* $f(X) - f(Y)$ *of degree d not of the form* $X - \alpha Y$ *or* $XY - \alpha$, $\alpha \in F$*, then*

$$d \geq \min\left\{\frac{p}{3n_t}, \frac{\sqrt{n_t}}{t}\right\}.$$

Proof Let $\mathscr{X}$ be a smooth model of the curve $h = 0$ and K/F its function field. The genus of $\mathscr{X}$ is at most $(d-1)(d-2)/2$. On $\mathscr{X}$, the functions x and y have at most d zeros and d poles (on the line at infinity), so they are S-units for some set S of places of $\mathscr{X}$ with $\#S \leq 3d$, since x and y both have poles at the at most d points at infinity, where S is formed by these poles and by the two sets of at most d zeros of x and y. Consider the functions x^{n_i}, y^{n_i}, for $i \in \{1, \ldots, t\}$, which are also S-units. Let $u_1 = x^{n_t}$, $u_2, \ldots, u_m$ be a subset of these functions such that

$$u_1 = \sum_{i=2}^{m} c_i u_i, \quad c_i \in F,$$

and m is minimal. Note that $m \leq 2t$, as the equation $f(x) - f(y) = 0$ yields a relation of this form with $m = 2t$, but $2t$ may not be minimal. Note also that $m > 1$.

If $m = 2$, then u_2 is a power of y as, otherwise, h would be a polynomial in X, which is clearly not possible. Let $u_2 = y^{n_j}$. As we have $x^{n_t} = c_2 y^{n_j}$ on the curve $h = 0$, we must have $n_j \neq 0$ and $y = cx^{n_t/n_j}$ for some c (as algebraic functions). Plugging this into $f(x) - f(y) = 0$ and comparing powers of x, yields $n_j = n_t$ or n_1 (the latter only if $n_1 = -n_t$). Consequently, $h = X - \alpha Y$ or $h = XY - \alpha$, $\alpha \in K$, contrary to the hypothesis, so $m \geq 3$.

The u_i are functions on $\mathscr{X}$ and are thus elements of K, and we have that $\deg(u_1 : \cdots : u_{m-1}) \leq 3dn_t$, since each coordinate is a monomial in x or y or their inverses to a power at most n_t. If $3dn_t \geq p$, the desired result follows immediately. If $3dn_t < p$, then by Lemma 2.1, using that $\deg u_1 \geq n_t$, we get

$$n_t \leq \deg u_1 \leq (m(m+1)/2)(d(d-3) + 3d) \leq d^2 m^2 \leq d^2 t^2,$$

proving the desired result. ∎

https://doi.org/10.4153/S0008439519000316 Published online by Cambridge University Press

3 Value Sets of Sparse Polynomials

Here we only concentrate on the case of a prime field $\mathbb{F}_p$, where p is a prime. We start with the following simple application of the Dirichlet pigeonhole principle (see also the proof of [CFKLLS, Lemma 7]).

Lemma 3.1 *For an integer $S \ge 1$ and arbitrary integers $n_1, \dots, n_t$, there exists a positive integer $s \le S$, such that*

$$sn_i \equiv m_i \pmod{p-1} \quad \text{and} \quad |m_i| \le pS^{-1/t}, \quad i = 1, \dots, t.$$

Proof We cover the cube $[0, p-1]^t$ by at most S cubes with the side length $pS^{-1/t}$. Therefore, at least two of the vectors formed by the residues of modulo $p-1$ of the $S+1$ vectors $(sn_1, \dots, sn_t)$, $s = 0, \dots, S$, fall in the same cube. Assume they correspond to $S \ge s_1 > s_2 \ge 0$. It is easy to see that $s = s_1 - s_2$ yields the desired result. ∎

For a sparse polynomial

$$g(x) = \sum_{i=1}^{r} b_i X^{k_i} \in \mathbb{F}_p[X] \tag{3.1}$$

with $r \ge 2$ elements $b_1, \dots, b_r \in \mathbb{F}_p^*$ and integer exponents $k_1, \dots, k_r \in \mathbb{Z}$ let us denote by $T(g)$ the number of distinct zeros of g in $\mathbb{F}_p^*$, that is, the number of solutions to the equation $g(x) = 0$, $x \in \mathbb{F}_p^*$. By [CFKLLS, Lemma 7] we have

$$T(g) \le 2p^{1-1/(r-1)}D^{1/(r-1)} + O_r(p^{1-2/(r-1)}D^{2/(r-1)}), \tag{3.2}$$

where

$$D = \min_{1\le i\le r} \max_{j\ne i} \gcd(k_j - k_i, p-1). \tag{3.3}$$

and $O_r(\cdot)$ indicates that the implied constant may depend on r.

Kelley recently gave a version of (3.2) without an error term, which is slightly more convenient for our applications [Kel16, Theorem 2.3] (see also the follow-up discussion).

Lemma 3.2 *For $g(x) \in \mathbb{F}_p[X]$ is of the form (3.1), we have*

$$T(g) \le 2(p-1)^{1-1/(r-1)}D^{1/(r-1)},$$

where D is given by (3.3).

Our main tool is the following bound of [Vol89, Theorem (i)] on the number of points on curves over $\mathbb{F}_p$.

Lemma 3.3 *Let $F(X,Y) \in \mathbb{F}_p[X,Y]$ be an absolutely irreducible polynomial of degree d with $p^{1/4} < d < p$. Then*

$$\#\{(x,y) \in \mathbb{F}_p^2 : F(x,y) = 0\} \le 4d^{4/3}p^{2/3}.$$

We also use that, by the Cauchy inequality,

$$p^2 = \Big(\sum_{a\in\mathbb{F}_p} \#\big\{x \in \mathbb{F}_p : f(x) = a\big\}\Big)^2 \le V(f) \sum_{a\in\mathscr{V}(f)} \Big(\#\big\{ x \in \mathbb{F}_p : f(x) = a\big\}\Big)^2 = V(f)\#\big\{(x, y) \in \mathbb{F}_p^2 : f(x) = f(y)\big\}. \tag{3.4}$$

See also [Vol89, Lemma 1] for a similar argument.

We are now ready to estimate $V(f)$. We present our bound and necessary conditions in fully explicit forms. However, we trade some possible improvements of numerical constants and dependencies on t (which we treat as a secondary parameter) in favour of the brevity and simplicity of the argument.

Theorem 3.4 *For any prime $p \ge 5$ and integers $1 \le n_1, \dots, n_t < p-1$ that satisfy the following conditions,*

(i) $\max_{1\le j<i\le t} \gcd(n_j - n_i, p-1) \le 2^{-t^2}(p-1)$,
(ii) $\gcd(n_1, \dots, n_t, p-1) = 1$,

and for any polynomial

$$f(X) = \sum_{i=1}^{t} a_i X^{n_i} \in \mathbb{F}_p[X] \quad \textit{with } a_i \ne 0, i = 1, \dots, t,$$

we have

$$V(f) \ge \min\Big\{\Big(\frac{3p}{t}\Big)^{2/3}, \frac{1}{12}p^{4/(3t+4)}\Big\}.$$

Proof We chose the integer parameter

$$S = \lceil p^{3t/(3t+4)}\rceil, \tag{3.5}$$

and define s and $m_1, \dots, m_t$ as in Lemma 3.1.

Clearly we can assume that $p^{4/(3t+4)} \ge 2$, as otherwise the bound is trivial. Hence we observe that

$$S \le \lceil p/2\rceil = (p+1)/2 < p-1 \tag{3.6}$$

for $p \ge 5$, which we have assumed.

We see that the condition (i) guarantees that

$$2^{t+1}(p-1)^{1-1/(r-1)}\Big(\max_{1\le j<i\le t} \gcd(n_j - n_i, p-1)\Big)^{1/(t-1)} < p-1.$$

Hence, by Lemma 3.2 there is $c \in \mathbb{F}_p^*$ such that

$$\sum_{i\in\mathscr{I}} a_i c^{n_i} \ne 0, \tag{3.7}$$

for all non-empty sets $\mathscr{I} \subseteq \{1, \dots, t\}$.

https://doi.org/10.4153/S0008439519000316 Published online by Cambridge University Press

We now fix some $c \in \mathbb{F}_p^*$ satisfying (3.7) and for the above s, we consider the polynomial $f(cX^s)$. Then the values of $f(cX^s)$ in $\mathbb{F}_p^*$ coincide with those of

$$g(X) = \sum_{i=1}^{t} b_i X^{m_i} \quad \text{with } b_i = a_i c^{n_i}, i = 1, \dots, t,$$

and, after collecting like powers of X, we consider two situations.

Case 1: The polynomial $g(X)$ is a constant function.

Case 2: The polynomial $g(X)$ is of positive degree.

We observe that due to condition (3.7), the number of terms of $g(X)$ is exactly the same as the number of distinct values among $m_1, \dots, m_t$.

In Case 1, if $g(X)$ is a constant, then $m_1 = \dots = m_t = 0$ and thus using that $sn_i \equiv m_i \equiv 0 \pmod{p-1}$, $i = 1, \dots, t$, we also see that

$$s \gcd(n_1, \dots, n_t, p-1) \equiv 0 \pmod{p-1}.$$

This, together with condition (ii), imply that $S \geq s \geq p-1$, which is impossible by (3.6).

We now consider Case 2, that is, when $g(X)$ is a nontrivial Laurent polynomial. Furthermore, making, if necessary, the change of variable $X \to X^{-1}$, without loss of generality, we can assume that

$$m_t = \max\left\{|m_1|, \dots, |m_t|\right\} > 0.$$

We now derive an upper bound on

$$N = \#\left\{(x,y) \in \mathbb{F}_p^2 : g(x) = g(y)\right\},$$

which is based on Theorem 2.2.

If

$$\sqrt{m_t} \leq \frac{tp}{3m_t},$$

then $m_t \leq (tp/3)^{2/3}$, and the result is trivial as we immediately obtain

$$N \leq m_t p \leq (t/3)^{2/3} p^{5/3}. \tag{3.8}$$

Hence, we now assume that

$$\sqrt{m_t} > \frac{tp}{3m_t}. \tag{3.9}$$

First, in order to apply Theorem 2.2, we need to investigate the factors of $g(X) - g(Y)$ of the form $X - \alpha Y$ or of the form $XY - \alpha$ with α in the algebraic closure of $\mathbb{F}_p$.

In fact, for an application to N, only factors of these forms with $\alpha \in \mathbb{F}_p$ are relevant.

Let $\mathcal{G}_s \subseteq \mathbb{F}_p^*$ be the multiplicative subgroup of elements $\alpha \in \mathbb{F}_p$ with $\alpha^s = 1$. Note that $\mathcal{G}_s$ is a subgroup of elements of multiplicative order $\gcd(s, p-1)$, and thus $\#\mathcal{G}_s = \gcd(s, p-1)$. We show that, for some $\gamma \in \mathbb{F}_p$, the factors of $g(X) - g(Y)$ of the form $X - \alpha Y$ and $XY - \alpha$ satisfy $\alpha \in \mathcal{G}_s$ and $\alpha \in \gamma\mathcal{G}_s$, respectively.

Clearly, if $g(X) - g(Y)$ has a factor of the form $X - \alpha Y$, then $g(X) - g(\alpha X)$ is identical to zero. Since $g(X)$ is not constant, we see that $\alpha \neq 0$. Hence, denoting by m the multiplicative order of α in $\mathbb{F}_p^*$, we see that by condition (ii) we have

$$m \mid \gcd(m_1, \dots, m_t, p-1) = \gcd(sn_1, \dots, sn_t, p-1) = \gcd(s, p-1).$$

Hence, $\alpha \in \mathcal{G}_s$.

The factors of $g(X) - g(Y)$ of the form $XY - \alpha$, $\alpha \in K$ imply that $g(X) - g(\alpha/X)$ is identically zero. This may occur only if, for each $i = 1, \dots, t$, there exists $j = 1, \dots, t$ with $m_i = -m_j$ and $\alpha^{m_i} = b_i/b_j$. In particular, there is some $\beta \in \mathbb{F}_p^*$ (which may depend on $m_1, \dots, m_t$) such that

$$\alpha^{\gcd(m_1,\dots,m_t,p-1)} = \beta,$$

which puts α in some fixed coset $\mathcal{G}_s$. Hence, there are at most $s \le S$ such values of α that contribute at most

$$N_0 \le pS \tag{3.10}$$

to N.

We proceed to get an upper estimate on N and notice that any further contribution to N may only come from factors of $g(X) - g(Y)$, not of the form $X - \alpha Y$ or $XY - \alpha$.

Since $m_1, \dots, m_t$ are as in Lemma 3.1, we have

$$m_t \le pS^{-1/t}. \tag{3.11}$$

Hence, for the degrees $d_j = \deg h_j$ of all such factors $h_1, \dots, h_k$ of $g(X) - g(Y)$ via Theorem 2.2 and the inequality (3.9), we derive that

$$d_j \ge \left\{\frac{p}{3m_t}, \frac{\sqrt{m_t}}{t}\right\} = \frac{p}{3m_t} \ge \frac{1}{3}S^{1/t}, \quad j = 1, \dots, k.$$

In particular, there are

$$k \le \frac{2m_t}{\min\{d_1, \dots, d_k\}} \le 3pS^{-2/t}$$

such factors.

Let N_1 and N_2 be contributions to N from the factors h_j of degree $d_j < p^{1/4}$ and $d_j \ge p^{1/4}$, respectively.

If a factor h has degree $d < p^{1/4}$, then the number of rational points on $h = 0$ is at most $2p$ by the Weil bound [Lor96, Section X.5, Equation (5.2)], so those factors all together contribute

$$N_1 \le 2 \sum_{\substack{j=1 \\ d_j < p^{1/4}}}^{k} p \le 2kp \le 6p^2 S^{-2/t}. \tag{3.12}$$

The factors with degree $d \ge p^{1/4}$ contribute $4d^{4/3}p^{2/3}$ by Lemma 3.3 and, in total they contribute

$$N_2 \le 4 \sum_{\substack{j=1 \\ d_j \ge p^{1/4}}}^{k} d_j^{4/3} p^{2/3}.$$

Using the convexity of the function $z \mapsto z^{4/3}$ and then extending the range of summation to polynomials of all degrees and recalling (3.11), we obtain

$$N_2 \le 4p^{2/3}\left(\sum_{j=1}^{k} d_j\right)^{4/3} \le 4m_t^{4/3} p^{2/3} \le 4p^2 S^{-4/(3t)}. \tag{3.13}$$

https://doi.org/10.4153/S0008439519000316 Published online by Cambridge University Press

Combining (3.10), (3.12), and (3.13), we obtain $N \le pS + 10p^2 S^{-4/(3t)}$, which, with the choice of S as in (3.5), implies that

$$p^{3t/(3t+4)} \le S < 2p^{3t/(3t+4)}$$

becomes

$$N < 12p^{(6t+4)/(3t+4)}. \tag{3.14}$$

Combining (3.8) and (3.14) with (3.4), we obtain the result. ∎

We now consider the case of binomials in more detail.

Theorem 3.5 *If $f(X) = X + aX^n \in \mathbb{F}_p[X]$, $d = \gcd(n, p-1)$, and $e = \gcd(n-1, p-1)$, then $V(f) \ge \max\{d, p/d, e, p/e\}$.*

Proof Assume that $d \le p^{1/2}$. There exists a positive $r \le (p-1)/d$ with $rn/d \equiv 1 \pmod{(p-1)/d}$ so that $rn \equiv d \pmod{p-1}$. Hence, if $x = u^r$, then $f(x) = g(u)$, where $g(u) = u^r + au^d$.

The equation $g(u) = g(v)$ has degree $\max\{r, d\}$ in v so $g(u) = g(v)$ thus has at most

$$p \max\{r, d\} \le p \max\{(p-1)/d, d\} \le p^2/d$$

solutions, as $d \le p^{1/2}$. By (3.4), we have $V(f) \ge p^2/pd = p/d$. If $d > p^{1/2}$, note that $d > p/d$.

Now regardless of the size of d, notice that for distinct d-th roots of unity, that is, for u with $u^d = 1$, the values $f(u) = u + a$ are pairwise distinct. Thus $V(f) \ge d$.

Similarly, there exists an integer s with $s(n-1)/e \equiv 1 \pmod{(p-1)/e}$ so that $sn \equiv e + s \pmod{p-1}$. Hence, if $x = u^s$, then $f(x) = h(u)$, where $h(u) = u^s + au^{e+s}$. The equation $h(u) = h(v)$ becomes, with $v = tu$, the same as $u^s + au^{e+s} = t^s u^s + au^{e+s} t^{e+s}$, and we get that either $u = 0$ or $1 + au^e = t^s + au^e t^{e+s}$, which has at most pe solutions. By (3.4), we have $V(f) \ge p^2/pe = p/e$.

Furthermore, we now fix a non-zero e-th power c with $1 + ac \ne 0$. Clearly, for distinct e-th roots of c, that is, for u with $u^e = c$, the values $f(u) = u(1 + ac)$ are pairwise distinct, and we can also add $f(0) = 0$. Thus $V(f) \ge e$.

The result now follows. ∎

We now immediately obtain the following.

Corollary 3.6 *If $f(X) = X + aX^n \in \mathbb{F}_p[X]$, then $V(f) \ge p^{1/2}$.*

4 Comments

Theorem 3.5 extends, with the same proof, to arbitrary finite fields. On the other hand, Theorem 3.4 is false as stated for arbitrary finite fields. Indeed, the trace polynomial $T(X) = X + X^p + \cdots + X^{p^{t-1}}$ has $T(\mathbb{F}_{p^t}) = \mathbb{F}_p$, so $V(T) = q^{1/t}$ if $q = p^t$. If the linearity is to be avoided for some reason, then the trace polynomial can be combined with a monomial $X^{(q-1)/d}$ for some divisor d.

Clearly, for $f(X) = X^{(q-1)/d} + T(X)$, any element in $\mathscr{V}(f)$ is of the form $u + v$, where $u \in \mathscr{V}(X^{(q-1)/d})$ and $v \in \mathscr{V}(T)$. Hence, we have

$$V(f) \le V(X^{(q-1)/d})V(T) = (d+1)p.$$

We note that one can use Lemma 3.2 directly in combination with (3.4). However, in the best possible scenario this approach can only give a lower bound of order $p^{1/(t-1)}$, which is always weaker than that of Theorem 3.4 for $t \ge 9$.

If p is a prime such that $(p-1)/2$ is also prime, then it follows from Theorem 3.5 that, for $f(X) = X + aX^n$, $a \ne 0$, $2 \le n \le p-1$, we have $V(f) \ge (p-1)/2$. It can be proved that equality is attained if $n = p-2$ and a is a non-square. In this case the pre-image of non-zero elements of $\mathbb{F}_p$ has zero or two elements and the pre-image of zero has three elements. A different example is $f(X) = X - X^{(p+1)/2}$, which has $V(f) = (p+1)/2$ and the pre-image of 0 has $(p+1)/2$ elements and other pre-images have zero or one elements.

For arbitrary primes, we have the following. Assume that $d \mid (p-1)$ and consider $f(X) = X + aX^{1+(p-1)/d}$. Choose a, if possible, such that $((1+a)/(1+\zeta a))^{(p-1)/d} = \zeta$ for all ζ with $\zeta^d = 1$. If $x_1^{(p-1)/d} = 1$ and $x_\zeta = (1+a)x_1/(1+\zeta a)$, then $x_\zeta^{(p-1)/d} = \zeta$ and $f(x_\zeta) = f(x_1)$ and it follows that $V(f) = 1 + (p-1)/d$.

To see when we can find such a, let c_ζ be such that $c_\zeta^{(p-1)/d} = \zeta$ with $\zeta^d = 1$. Consider the curve given by the system of equations $(1+u)/(1+\zeta u) = c_\zeta v_\zeta^d$ in variables u and v_ζ, indexed by $\zeta \ne 1$ with $\zeta^d = 1$. A rational point with $u = a \ne 0$ provides the necessary a. The genus of this curve is at most $d^d/2$ so by the Weil bound on the number of $\mathbb{F}_p$-rational points on curves [Lor96, Section X.5, Equation (5.2)], there is such a point if $p > d^{2d}$. This construction succeeds if $d \le c \log p/(\log\log p)$ with some absolute constant $c > 0$.

We conclude by posing a question about estimating the image size of polynomials of the form $F(X) = \prod_{i=1}^{t}(X^{n_i} + a_i)$. Although most of our technique applies in this case as well, investigating linear factors of $F(cX^s) - F(cY^s)$ seems to be more complicated.

Acknowledgements The authors would like to thank Domingo Gómez-Pérez and the referee for the very careful reading of manuscript and many useful comments.

References

[BCR16] J. Bi, Q. Cheng, and J. M. Rojas, *Sub-linear root detection, and new hardness results, for sparse polynomials over finite fields*. SIAM J. Comput. 45(2016), 1433–1447. https://doi.org/10.1137/140990401

[BS-D59] B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*. Acta Arith. 5(1959), 417–423. https://doi.org/10.4064/aa-5-4-417-423

[CFKLLS] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski, *On the statistical properties of Diffie-Hellman distributions*. Israel J. Math. 120(2000), 23–46. https://doi.org/10.1007/s11856-000-1270-1

[CLMS61] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Strauss, *Polynomials over finite fields with minimal value sets*. Mathematika 8(1961), 121–130. https://doi.org/10.1112/S0025579300002230

[CGRW17] Q. Cheng, S. Gao, J. M. Rojas, and D. Wan, *Sparse univariate polynomials with many roots over finite fields*. Finite Fields Appl. 46(2017), 235–246. https://doi.org/10.1016/j.ffa.2017.03.006

[Kel16] A. Kelley, *Roots of sparse polynomials over a finite field*. LMS J. Comput. Math. 19(2016), suppl. A, 196–204. https://doi.org/10.1112/S1461157016000334

[Kur09] P. Kurlberg, *Poisson spacing statistics for value sets of polynomials*. Int. J. Number Theory 5(2009), 489–513. https://doi.org/10.1142/S1793042109002237

[Lor96] D. Lorenzini, *An invitation to arithmetic geometry*. Graduate Studies in Mathematics, 9, American Mathematical Society, Providence, RI, 1996. https://doi.org/10.1090/gsm/009

[Mil64] W. H. Mills, *Polynomials with minimal value sets*. Pacific J. Math. 14(1964), 225–241.

[MZ13] G. Mullen and M. Zieve, *Value sets of polynomials*. In: *Handbook of finite fields*, CRC Press, Boca Raton, FL, 2013, pp. 232–235. https://doi.org/10.1201/b15006

[St09] H. Stichtenoth, *Algebraic function fields and codes*. Graduate Texts in Mathematics, 254, Springer-Verlag, Berlin, 2009.

[SV86] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*. Proc. London Math. Soc. 52(1986), 1–19. https://doi.org/10.1112/plms/s3-52.1.1

[Vol85] J. F. Voloch, *Diagonal equations over function fields*. Bol. Soc. Brasil. Mat. 16(1985), 29–39. https://doi.org/10.1007/BF02584799

[Vol89] J. F. Voloch, *On the number of values taken by a polynomial over a finite field*. Acta Arith. 52(1989), 197–201. https://doi.org/10.4064/aa-52-2-197-201

[WSC93] D. Wan, P. J.-S. Shiue, and C. S. Chen, *Value sets of polynomials over finite fields*. Proc. Amer. Math. Soc. 119(1993), 711–717. https://doi.org/10.2307/2160504

[Zan07] U. Zannier, *On the number of terms of a composite polynomial*. Acta Arith. 127(2007), 157–168. https://doi.org/10.4064/aa127-2-5

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand
e-mail: felipe.voloch@canterbury.ac.nz