VALUE SETS OF SPARSE POLYNOMIALS

IGOR E. SHPARLINSKI AND JOSÉ FELIPE VOLOCH

Abstract. We obtain a new lower bound on the size of 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 of 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 which canted 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 $V(f) = \#\mathscr{V}(f)$. A much studied problem is to estimate $V(f)$ in terms of f. An easy lower bound is $V(f) \geqslant q/\deg f$ as $f(x) = c$ has at most $\deg f$ solutions for any c. This is essentially best possible in general but, given conditions on f it can sometimes be improved. In this paper, we study the question of bounding from below $V(f)$ as a function of the number of terms in f, rather than its degree. Specifically, if $f(X) = a_0 + \sum_{i=1}^{t} a_i X^{n_i}$, 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 (see [CFKLLS00, Lemma 7]) 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 [CFKLLS00, Lemma 7] on the number of roots, when it applies, for $t \geqslant 9$.

We obtain our results in three steps. First, using a monomial change of variables we reduce the degree of the polynomial, as in [CFKLLS00]. Second, we bound the number of irreducible components of $f(X) -$

2010 *Mathematics Subject Classification.* 11T06, 14G15.

Key words and phrases. sparse polynomials, value set, rational points on curves.

$f(Y)$ by adapting a result of Zannier [Z07]. Finally, we use the results of [V89] 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.

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$, are all equivalent to the statement that $|U| \leqslant cV$ for some constant c which throughout this work may depend on the positive integer parameter t (the number of terms of the polynomials involved), and is absolute otherwise.

2. Factors of differences of sparse Laurent polynomials

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

The following result and its proof are motivated by a result in [Z07].

Theorem 2.1. *Let K be a field of positive characteristic p and let*

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

be a nonconstant Laurent polynomial over K with $a_i \neq 0$ and nonzero integer exponents $n_1 < \ldots < n_t$ with $n_t \geqslant |n_i|$, $i = 1, \ldots, t$. 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 $XY - \alpha$, $\alpha \in K$. Then $d \gg \min\{p/n_t, \sqrt{n_t/t^2}\}$.

Proof. Let $\mathscr{X}$ be a smooth model of the curve $h = 0$. 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 $\#S \leqslant 3d$. Consider the functions x^{n_i}, y^{n_i}, $i = 1, \ldots, t$ which are also S-units. Let $u_1 = x^{n_t}, u_2 \ldots, u_m$ be a subset of these functions such that

$$u_1 = \sum_{i=2}^{m} c_i u_i, \qquad c_i \in K,$$

and m minimal. Note that $m \leqslant 2t$ as the equation $f(x) - f(y) = 0$ yields a relation of this form with $m = 2t$ but 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, on the curve $h = 0$, we have $x^{n_t} = c_2 y^{n_j}$ we must have $n_j \neq 0$ and $y = cx^{n_t/n_j}$ for some c (as algebraic functions) and 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 hypothesis, so $m \geqslant 3$.

The u_i are functions on $\mathscr{X}$ so

$$(u_1{:}\ldots{:}u_{m-1})$$

defines a morphism $\mathscr{X} \to \mathbb{P}^{m-1}$ of degree at most $3dn_t$, since each coordinate is a monomial in x or y or their inverses to a power at most n_t. If $3dn_t \geqslant p$, the desired result follows immediately. If $3dn_t < p$, then [V85, Theorem 4] holds with the same proof in characteristic $p > 0$ (as the morphism has classical orders by [SV86, Corollary 1.8]). Also $\deg u_1 \geqslant n_t$ so we get

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

proving the desired result. □

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 of the Dirichlet pigeonhole principle (see also the proof of [CFKLLS00, Lemma 6]).

Lemma 3.1. *For an integer $S \geqslant 1$ and arbitrary integers $n_1, \ldots, n_t$, there exists a positive integer $s \leqslant S$, such that*

$$sn_i \equiv m_i \pmod{p-1} \qquad \text{and} \qquad |m_i| \ll pS^{-1/t}, \qquad i = 1, \ldots, t.$$

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 $(sn_1, \ldots, sn_t)$, $s = 0, \ldots, S$ fall in the same cube. Assume they correspond to $S \geqslant s_1 > s_2 \geqslant 0$. It is easy to see that $s = s_1 - s_2$ yields the desired result. □

Furthermore, by [CFKLLS00, Lemma 7] we have:

Lemma 3.2. *For $r \geqslant 2$ given elements $b_1, \ldots, b_r \in \mathbb{F}_p^*$ and integers $k_1, \ldots, k_r$ in $\mathbb{Z}$ let us denote by T the number of solutions of the equation*

$$\sum_{i=1}^{r} c_i x^{k_i} = 0, \qquad x \in \mathbb{F}_p^*.$$

Then

$$T \leqslant 2p^{1-1/(r-1)} D^{1/(r-1)} + O\left(p^{1-2/(r-1)} D^{2/(r-1)}\right), \tag{3.1}$$

where

$$D = \min_{1 \leqslant i \leqslant r} \max_{j \neq i} \gcd(k_j - k_i, p-1).$$

We also use that by the Cauchy inequality

$$\begin{aligned} p^2 &= \left(\sum_{a\in\mathbb{F}_p} \#\{x \in \mathbb{F}_p :\ f(x) = a\}\right)^2 \\ &\leqslant V(f) \sum_{a\in\mathscr{V}(f)} \left(\#\{x \in \mathbb{F}_p :\ f(x) = a\}\right)^2 \\ &= V(f)\#\{(x,y) \in \mathbb{F}_p^2 :\ f(x) = f(y)\}, \end{aligned} \tag{3.2}$$

see also [V89, Lemma 1].

We are now ready to estimate $V(f)$.

Theorem 3.3. *For any $t \geqslant 2$ there is a constant $c(t) > 0$ such that for any primes p and integers $1 \leqslant n_1, \ldots, n_t < p-1$ integers with*

(i) $\max_{1\leqslant j<i\leqslant t} \gcd(n_j - n_i, p-1) \leqslant c(t)p$,
(ii) $\gcd(n_1, \ldots, , n_t, p-1) = 1$,

for any polynomial

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

we have $V(f) \gg \min\{p^{2/3}, p^{4/(3t+4)}\}$.

Proof. We chose the integer parameter

$$S = \left\lceil p^{3t/(3t+4)} \right\rceil, \tag{3.3}$$

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

We see from Lemma 3.2 that for a sufficiently small $c(t)$ the condition (i) guarantees that there is $c \in \mathbb{F}_p^*$ such that

$$\sum_{i\in\mathscr{I}} a_i c^{n_i} \neq 0, \tag{3.4}$$

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

We now fix some $c \in \mathbb{F}_p^*$ satisfying (3.4) 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

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

and, after collecting like powers of X, we consider two situations: when $g(X)$ is a constant functions and when $g(X)$ is of positive degree.

We observe that due to the condition (3.4) the number of terms of $g(X)$ is exactly the same as the number of distinct values among $m_1, \ldots, m_t$.

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

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

This implies that

$$S \geqslant s \geqslant \frac{p-1}{\gcd(n_1, \ldots, , n_t, p-1)} = p-1$$

which is impossible for the above choice of S, due to the condition (ii).

So we can now assume that $g(X)$ 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

$$m_t = \max\{|m_1|, \ldots, |m_t|\} > 0.$$

We now derive a bound on

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

which is based on Theorem 2.1.

If $\sqrt{m_t} \leqslant p/m_t$ then $m_t \leqslant p^{2/3}$ and the result is trivial. We immediately obtain

$$N \ll m_t p \ll p^{5/3}. \tag{3.5}$$

Hence we now assume that

$$\sqrt{m_t} > p/m_t. \tag{3.6}$$

First, in order to apply Theorem 2.1, 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 $\mathscr{G}_s \subseteq \mathbb{F}_p^*$ be the multiplicative subgroup of elements $\alpha \in \mathbb{F}_p$ with $\alpha^s = 1$. Note that $\mathscr{G}_s$ is a subgroup of elements of multiplicative order $\gcd(s, p-1)$, and thus

$$\#\mathscr{G}_s = \gcd(s, p-1).$$

We show that for some $\gamma \in \mathbb{F}_p$ factors of $g(X) - g(Y)$ of the form $X - \alpha Y$ and $XY - \alpha$ we have $\alpha \in \mathscr{G}_s$ and $\alpha \in \gamma\mathscr{G}_s$, 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 the condition (ii) we have

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

Hence $\alpha \in \mathscr{G}_s$.

The factors of $g(X) - g(Y)$ of the form $XY - \alpha$, $\alpha \in K$ imply that $g(X) - g(\alpha/X)$ is identical to zero. This may occur only if for every $i = 1, \ldots, t$ there exists $j = 1, \ldots, t$ 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 $m_1, \ldots, m_t$) such that

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

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

$$N_0 \ll pS \tag{3.7}$$

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 $XY - \alpha$.

As $m_t \ll pS^{-1/t}$, all such factors $h_1, \ldots, h_k$ of $g(X) - g(Y)$ have degree $d_j = \deg h_j$ for which, then, by Theorem 2.1 and also using (3.6) we derive

$$d_j \gg \min\{p/m_t, \sqrt{m_t/t^2}\} = p/m_t \geqslant S^{1/t}, \quad j = 1, \ldots, k.$$

and there are

$$k \leqslant \frac{2m_t}{\min\{d_1, \ldots, d_k\}} \ll pS^{-2/t}$$

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 $d_j \geqslant p^{1/4}$, respectively.

If a factor h has degree $d < p^{1/4}$ the number of rational points on $h = 0$ is $O(p)$ by the Weil bound (see [L96]), so those factors all together contribute

$$N_1 \ll \sum_{\substack{j=1 \\ d_j < p^{1/4}}}^{k} p \leqslant kp \ll p^2 S^{-2/t}. \tag{3.8}$$

The factors with degree $d \geqslant p^{1/4}$ contribute $O(d^{4/3}p^{2/3})$ by [V89, Theorem (i)] and, in total they contribute

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

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

$$N_2 \leqslant p^{2/3} \left(\sum_{j=1}^{k} d_j \right)^{4/3} \leqslant m_t^{4/3} p^{2/3} \ll p^2 S^{-4/(3t)}. \tag{3.9}$$

Combining (3.7), (3.8) and (3.9) we obtain

$$N \ll pS + p^2 S^{-4/(3t)}$$

which with the choice S as in (3.3), becomes

$$N \ll p^{(6t+4)/(3t+4)}. \tag{3.10}$$

Combining (3.5) and (3.10) with (3.2) we derive the result. □

We now consider the case of binomials in more detail.

Theorem 3.4. *If $f(X) = X + aX^n \in \mathbb{F}_p[X]$ and*

$$d = \gcd(n, p-1) \qquad \textit{and} \qquad e = \gcd(n-1, p-1),$$

then

$$V(f) \gg \max\{d, p/d, e, p/e\}.$$

Proof. Assume that $d \leqslant p^{1/2}$. There exists a positive $r \leqslant (p-1)/d$ 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 at most

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

solutions, as $d \leqslant p^{1/2}$. By (3.2), we have $V(f) \gg p^2/pd = p/d$. If $d > p^{1/2}$, note that $d > p/d$.

Now, regardless of the size of d, notice that for every u with $u^d = 1$ the values $f(u) = u + a$ are pairwise distinct. Thus $V(f) \geqslant d$.

Similarly, there exists 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 (3.2), we have $V(f) \gg p^2/pe = p/e$.

Furthermore, notice that for every u with $u^e = c$, where c is a fixed non-zero e-th power with $1 + ac \neq 0$, the values $f(u) = u(1 + ac)$ are pairwise distinct, and we can also add $f(0) = 0$. Thus $V(f) \geqslant e$.

The result now follows. □

We now immediately obtain:

Corollary 3.5. *If $f(X) = X + aX^n \in \mathbb{F}_p[X]$ then $V(f) \geqslant p^{1/2}$.*

4. Comments

Theorem 3.4 extends, with the same proof, for arbitrary finite fields. On the other hand, Theorem 3.3 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 $q = p^t$. The trace polynomial can be combined with a monomial $X^{(q-1)/d}$ for some divisor d to break the linearity of $T(X)$. Clearly, for $f(X) = X^{(q-1)/d} + T(X)$ we have $V(f) \leqslant (d+1)p$.

We note that one can use Lemma 3.2 directly in a combination with (3.2). 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 3.3 for $t \geqslant 9$.

If p is a prime such that $(p-1)/2$ is also prime, then it follows from Theorem 3.4 that, for $f(X) = X + aX^n$, $a \neq 0$, $2 \leqslant n \leqslant p-1$, we have $V(f) \geqslant (p-1)/2$. 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 $\mathbb{F}_p$ have 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 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 $\zeta^d = 1$. Then, 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 $\zeta \neq 1$ with $\zeta^d = 1$. A rational point with $u = a \neq 0$ 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 (see [L96]), there is such a point if $p > d^{2d}$. This construction succeeds if $d \ll \log p/(\log\log p)$.

We also conclude with posing an 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 like to thank Domingo Gómez-Pérez for several useful comments.

During the preparation of this work the first author was supported by the ARC Grants DP170100786 and DP180100201

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. (p. 1)

[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. (p. 1)

[CFKLLS00] 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. (pp. 1 and 3)

[L96] D. Lorenzini, *An invitation to arithmetic geometry*, Amer. Math. Soc., 1996. (pp. 6 and 8)

[SV86] K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields. *Proc. London Math. Soc.*, **52** (1986), 1–19. (p. 3)

[V85] J. F. Voloch, Diagonal equations over function fields, *Boletim da Sociedade Brasileira de Matematica*, **16** (1985), 29–39. (p. 3)

[V89] J. F. Voloch, On the number of values taken by a polynomial over a finite field. *Acta Arith.*, **52** (1989), 197–201. (pp. 1, 4, and 6)

[Z07] U. Zannier, On the number of terms of a composite polynomial *Acta Arith.*, **127** (2007), 157–168. (pp. 1 and 2)

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au

School of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand

E-mail address: felipe.voloch@canterbury.ac.nz