Canad. Math. Bull. Vol. 65 (4), 2022, pp. 1071–1073
http://dx.doi.org/10.4153/S0008439521000928

Corrections to "Value sets of sparse polynomials"

Igor E. Shparlinski and José Felipe Voloch

Abstract. We give a corrected version of our previous lower bound on the value set of binomials (Canad. Math. Bull., v.63, 2020, 187–196). The other results are not affected.

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 $\mathcal{V}(f) = \{f(a) : a \in \mathbb{F}_q\}$ and we define $V(f) = \#\mathcal{V}(f)$.

In the case of binomials $f(X) = X + aX^n \in \mathbb{F}_p[X]$ the bound of [ShVo18, Theorem 3.5] asserts that

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

where

$$d = \gcd(n, p-1) \qquad \text{and} \qquad e = \gcd(n-1, p-1). \tag{1.1}$$

Unfortunately, the proof contains some wrong calculations, and in particular, the bound $V(f) \geq p/d$ is not correctly justified. In fact, it is easy to see that this bound is wrong. For example, for $f(X) = X - X^n$ for $d = 1$, this bound implies $V(f) = p$, while we have $f(0) = f(1) = 0$ and thus $V(f) \leq p - 1$.

Here, we formulate and prove a corrected version.

Theorem 1.1 *Let $f(X) = X + aX^n \in \mathbb{F}_p[X]$, $1 < n < p$, and let d and e be as in (1.1). Then*

$$V(f) \geq \max\{d, (p-1)/(e+1), e+1\}.$$

Proof Note, that for distinct dth roots of unity, that is, for u with $u^d = 1$, the values $f(u) = u + a$ are pairwise distinct. Thus $V(f) \geq d$.

We now consider only the values $x \in \mathbb{F}_p^*$. The equation

$$f(x) = f(y), \qquad x, y \in \mathbb{F}_p^*, \tag{1.2}$$

Received by the editors July 27, 2021; revised October 6, 2021; accepted October 7, 2021.
Published online on Cambridge Core November 2, 2021.
AMS subject classification: **11T06**, 14G15.
Keywords: Sparse polynomials, value set, rational points on curves.

becomes, with $y = tx$, $t \in \mathbb{F}_p^*$, the same as

$$x + ax^n = tx + at^n x^n, \qquad t, x \in \mathbb{F}_p^*,$$

or

$$1 + ax^{n-1} = t + at^n x^{n-1}, \qquad t, x \in \mathbb{F}_p^*, \tag{1.3}$$

If $t = 1$, then there are $p - 1$ possible values of x satisfying (1.3).

For other $p - 2$ values of t, if $t^n = 1$, the equation (1.3) has no solution whereas if $t^n \neq 1$, it defines a unique value of x^{n-1}, which leads to e possible value of x. Hence, the number of solutions to the equation (1.3), and thus equation (1.2) as well, is $p - 1 + e(p - 2)$, which is bounded by $(e + 1)(p - 1)$.

By the Cauchy inequality,

$$\begin{aligned}(p-1)^2 &= \left(\sum_{\lambda \in \mathbb{F}_p} \#\{x \in \mathbb{F}_p^* : f(x) = \lambda\}\right)^2 \\ &\leq V^*(f) \sum_{\lambda \in \mathbb{F}_p} \left(\#\{x \in \mathbb{F}_p^* : f(x) = \lambda\}\right)^2,\end{aligned}$$

since the sum over λ is supported on $V^*(f)$ terms, where $V^*(f)$ is the number of distinct values of $f(x)$ with $x \in \mathbb{F}_p^*$. Hence,

$$\begin{aligned}(p-1)^2 &\leq V^*(f)\#\{(x, y) \in \mathbb{F}_p^* \times \mathbb{F}_p^* : f(x) = f(y)\} \\ &\leq V^*(f)(e+1)(p-1).\end{aligned}$$

Therefore,

$$V(f) \geq V^*(f) \geq (p-1)/(e+1).$$

Furthermore, we now fix a nonzero eth power c with $1 + ac \neq 0$. Clearly for e distinct eth 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 $V(f) \geq e + 1$.

The result now follows. ∎

We now immediately obtain:

Corollary 1.2 *If $f(X) = X + aX^n \in \mathbb{F}_p[X]$, $1 < n < p$, then $V(f) \geq \sqrt{p-1}$.*

Acknowledgment The authors would like to thank Michael Zieve for pointing out some gaps in the original version of [ShVo18, Theorem 3.5].

References

[ShVo18] I. Shparlinski and J. F. Voloch, *Value sets of sparse polynomials*. Canad. Math. Bull. **63**(2020), 187–196.

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

https://doi.org/10.4153/S0008439521000928 Published online by Cambridge University Press