VALUE SETS OF POLYNOMIAL MAPS OVER FINITE FIELDS

GARY L. MULLEN, DAQING WAN, AND QIANG WANG

ABSTRACT. We provide upper bounds for the cardinality of the value set of a polynomial map in several variables over a finite field. These bounds generalize earlier bounds for univariate polynomials.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field of q elements with characteristic p. The *value set* of a polynomial f over $\mathbb{F}_q$ is the set V_f of images when we view f as a mapping from $\mathbb{F}_q$ to itself. Clearly f is a *permutation polynomial (PP)* of $\mathbb{F}_q$ if and only if the cardinality $|V_f|$ of the value set of f is q. As a consequence of the Chebotarev density theorem, Cohen [3] proved that for fixed integer $d \geq 1$, there is a finite set T_d of positive rational numbers such that: for any q and any $f \in \mathbb{F}_q[x]$ of degree d, there is an element $c_f \in T_d$ with $|V_f| = c_f q + O_d(\sqrt{q})$. In particular, when q is sufficiently large compared to d, the set of ratios $\frac{|V_f|}{q}$ is contained in a subset of the interval $[0, 1]$ having arbitrarily small measure. It is therefore natural to ask how the sizes of value sets are explicitly distributed, and also how polynomials are distributed in terms of value sets. For example, there are several results on bounds of the cardinality of value sets if f is not a PP over $\mathbb{F}_q$; Wan [13] proved that $|V_f| \leq q - \lceil (q-1)/d \rceil$ and Guralnick and Wan [6] also proved that if $(d, q) = 1$ then $|V_f| \leq (47/63)q + O_d(\sqrt{q})$. Some progress on lower bounds of $|V_f|$ can be found in [4, 14], as well as *minimal value set polynomials* that are polynomials satisfying $|V_f| = \lceil q/d \rceil$ [1, 5, 10]. All of these results relate $|V_f|$ to the degree d of the polynomial. Algorithms and complexity in computing $|V_f|$ have been studied recently, see [2].

Let $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a polynomial map in n variables defined over $\mathbb{F}_q$, where n is a positive integer. In Section 2 we extend Wan's result on upper bounds of value sets for univariate polynomials in [13] to

2000 *Mathematics Subject Classification.* 11T06.

Key words and phrases. polynomials, value sets, permutation polynomials, finite fields.

Research of the authors was partially supported by NSF and NSERC of Canada.

polynomial maps in n variables. Denote by $|V_f|$ the number of distinct values taken by $f(x_1, \ldots, x_n)$ as $(x_1, \ldots, x_n)$ runs over $\mathbb{F}_q^n$. Following the approach of studying value set problems in terms of the degree of a polynomial, we give an upper bound of $|V_f|$ in terms of the total degree of the multivariate polynomial f over $\mathbb{F}_q$ in Theorem 2.1. In particular, this answers an open problem raised by Lipton [9] in his computer science blog.

2. Value sets of polynomial maps in several variables

In this section, we let $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a polynomial map in n variables defined over $\mathbb{F}_q$, where n is a positive integer. We give a simple upper bound for the number $|V_f|$ of distinct values taken by $f(x_1, \ldots, x_n)$ as $(x_1, \ldots, x_n)$ runs over $\mathbb{F}_q^n$ when f does not induce a permutation map.

We write f as a polynomial vector:

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)), \tag{1}$$

where each f_i $(1 \le i \le n)$ is a polynomial in n variables over $\mathbb{F}_q$. The polynomial vector f induces a map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$. By reducing the polynomial vector f modulo the ideal $(x_1^q - x_1, \ldots, x_n^q - x_n)$, we may assume that the degree of f_i in each variable is at most $q-1$ and we may further assume that f is a non-constant map to avoid the trivial case. Let d_i denote the total degree of f_i in the n variables $x_1, \ldots, x_n$ and let $d = \max_i d_i$. Then d satisfies $1 \le d \le n(q-1)$. Let $|V_f|$ be the cardinality of the *value set* $V_f = \{f(x_1, \ldots, x_n) | (x_1, \ldots, x_n) \in \mathbb{F}_q^n\}$. It is clear that $|V_f| \le q^n$. If $|V_f| = q^n$, then f is a *permutation polynomial vector*, see [8, Chapter 7]. If $|V_f| < q^n$, we prove the following:

Theorem 2.1. *Assume that $|V_f| < q^n$. Then*

$$|V_f| \le q^n - \min\{\frac{n(q-1)}{d}, q\}. \tag{2}$$

In the special case when $n = 1$, the bound in (2) reduces to the bound (3) proved in [13] for the case of a univariate polynomial:

$$|V_f| \le q - \frac{q-1}{d}. \tag{3}$$

Based on computer calculations, the bound in (3) was first conjectured by Mullen [11]. The original proof of (3) in [13] is elementary, and uses power symmetric functions and involves a p-adic lifting lemma. A significantly simpler proof of (3) is given by Turnwald [12], who uses elementary symmetric functions instead of power symmetric functions

and works directly over the finite field $\mathbb{F}_q$ without p-adic liftings. Independently and later, Lenstra [7] showed one of us another simple proof which uses power symmetric functions in characteristic zero and avoids the use of the p-adic lifting lemma.

The proof of (3) gives a stronger result as shown in [14]. This information will be used later to prove the higher dimensional Theorem 2.1. We first recall the relevant one dimensional result in [14]. Let $\mathbb{Z}_q$ denote the ring of p-adic integers with uniformizer p and residue field $\mathbb{F}_q$. Let f be a polynomial in $\mathbb{F}_q[x]$ of degree $d > 0$. For a fixed lifting $\tilde{f}(x) \in \mathbb{Z}_q[x]$ of f and a fixed lifting $L_q \subset \mathbb{Z}_q$ of $\mathbb{F}_q$, we define $U(f)$ to be the smallest positive integer k such that

$$S_k(f) = \sum_{x \in L_q} \tilde{f}(x)^k \not\equiv 0 \pmod{pk}. \tag{4}$$

The number $U(f)$ exists (see the proof of Lemma 2.2 below) and is easily seen to be independent of the choice of the liftings $\tilde{f}(x)$ and L_q. One checks from the definition that $U(f) \geq (q-1)/d$. Thus, we have the inequality,

$$\frac{q-1}{d} \leq U(f) \leq q-1.$$

The following improvement of (3) is given in [14]:

Lemma 2.2. *If $|V_f| < q$, then*

$$|V_f| \leq q - U(f).$$

Proof. To be self-contained, we give a simpler proof of this lemma using ideas of Lenstra and Turnwald, closely following the version given by Lenstra [7]. Note that in this lemma we are dealing with a polynomial f in one variable.

Let $w = q - |V_f|$. Assume $|V_f| > q - U(f)$, that is, $w < U(f)$, where we define $U(f) = \infty$ if it does not exist. We need to prove that f is bijective on $\mathbb{F}_q$. By the definition of $U(f)$ and the assumption $w < U(f)$, we can write

$$\sum_{k=1}^{\infty} \frac{S_k(f)}{k} T^k \equiv pg(T) \pmod{T^{w+1}}$$

for some polynomial $g \in \mathbb{Z}_q[T]$. This together with the logarithmic derivative identity

$$\prod_{x \in L_q} (1 - \tilde{f}(x)T) = \exp(-\sum_{k=1}^{\infty} \frac{S_k(f)}{k} T^k)$$

shows that

$$\prod_{x\in L_q}(1-\tilde{f}(x)T)\equiv \exp(-pg(T)) \pmod{T^{w+1}} \equiv 1 \pmod{(p,T^{w+1})},$$

where in the last congruence we used the fact that $p^k/k!$ is divisible by p for every positive integer k. Reducing this congruence modulo p, one obtains

$$\prod_{x\in \mathbb{F}_q}(1-f(x)T)\equiv 1 \pmod{T^{w+1}}.$$

On the other hand, since f is not a constant, we have $w < q-1$ and

$$\prod_{y\in \mathbb{F}_q}(1-yT) = 1-T^{q-1} \equiv 1 \pmod{T^{w+1}}.$$

Thus,

$$\prod_{x\in \mathbb{F}_q}(1-f(x)T) \equiv \prod_{y\in \mathbb{F}_q}(1-yT) \pmod{T^{w+1}}.$$

By hypothesis, the two products have exactly $|V_f|$ factors in common. Removing the $|V_f|$ common factors which are invertible modulo T^{w+1}, we obtain two polynomials of degree at most w which are congruent modulo T^{w+1}, and therefore identical. Multiplying the removed factors back in, we conclude that

$$\prod_{x\in \mathbb{F}_q}(1-f(x)T) = \prod_{y\in \mathbb{F}_q}(1-yT).$$

This proves that f is bijective on $\mathbb{F}_q$ as required. □

We use Lemma 2.2 to prove Theorem 2.1. Recall that f is now the polynomial vector in (1). Let $e_1,\ldots,e_n$ be a basis of the extension field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Write $x = x_1e_1+\cdots+x_ne_n$ and

$$g(x) = f_1(x_1,\ldots,x_n)\ e_1+\cdots+f_n(x_1,\ldots,x_n)\ e_n.$$

The function g induces a non-constant univariate polynomial map from the finite field $\mathbb{F}_{q^n}$ into itself. Furthermore, one has the equality $|V_f| = |g(\mathbb{F}_{q^n})|$. We do not have a good control on the degree of g as a univariate polynomial and thus we cannot use the univariate bound (3) directly. The following lemma gives a lower bound for $U(g)$, which is enough to prove Theorem 2.1.

Lemma 2.3. *If $d \geq n$, we have the inequality*

$$\frac{n(q-1)}{d} \leq U(g) < q^n.$$

If $d < n$, we have the inequality

$$q \leq U(g) < q^n.$$

Proof. The upper bound is trivial. We need to prove the lower bound. We may assume that $g(x_1e_1 + \cdots + x_ne_n)$ is already lifted to characteristic zero and has total degree d when viewed as a polynomial in the n variables $x_1, \ldots, x_n$. Furthermore, we can assume that the coefficients of g as a polynomial in n variables are either zero or roots of unity, that is, we use the Teichmüller lifting for the coefficients. Let L_q denote the Teichmüller lifting of $\mathbb{F}_q$.

Let k be a positive integer such that $k < n(q-1)/d$ if $d \geq n$ and $k < q$ if $d < n$. We need to prove the claim that

$$S_k(g) = \sum_{(x_1,\cdots,x_n)\in L_q^n} g(x_1e_1 + \cdots + x_ne_n)^k \equiv 0 \pmod{pk}.$$

Expand $g(x_1e_1+\cdots+x_ne_n)^k$ as a polynomial in the n variables $x_1, \ldots, x_n$. Let

$$M(x_1, \ldots, x_n) = ax_1^{u_1} \cdots x_n^{u_n}$$

be a typical non-zero monomial in g^k. It suffices to prove that

$$\sum_{(x_1,\ldots,x_n)\in L_q^n} x_1^{u_1} \cdots x_n^{u_n} \equiv 0 \pmod{pk}.$$

The sum on the left side is zero if one of the u_i is not divisible by $q-1$. Thus, we shall assume that all u_i's are divisible by $q-1$. The total degree

$$u_1 + \cdots + u_n \leq dk.$$

Thus, there are at least $n - \lfloor dk/(q-1) \rfloor$ of the u_i's which are zero. This implies that

$$S_k(g) \equiv 0 \pmod{q^{n-\lfloor dk/(q-1)\rfloor}}.$$

Let v_p denote the p-adic valuation satisfying $v_p(p) = 1$. If the inequality

$$v_p(q)(n - \lfloor kd/(q-1)\rfloor) \geq 1 + v_p(k)$$

is satisfied, then the claim is true and we are done.

In the case that $d < n$ and $k < q$, we have $dk/(q-1) < n$ and $v_p(k) < v_p(q)$. Thus,

$$v_p(q)(n - \lfloor kd/(q-1)\rfloor) \geq v_p(q) \geq 1 + v_p(k).$$

In the case $d \geq n$ and $k < n(q-1)/d$, we have

$$k < \frac{n(q-1)}{d} < q.$$

It follows that $v_p(k) < v_p(q)$. Since $kd/(q-1) < n$, we deduce

$$v_p(q)(n - \lfloor kd/(q-1)\rfloor) \geq v_p(q) \geq 1 + v_p(k).$$

The proof is complete. □

Remark. For a sharp example, we may take $n = d = 2$ and $f(x_1, x_2) = (x_1, x_1x_2)$. This is a birational morphism from $\mathbb{A}^2$ to $\mathbb{A}^2$, but not a finite morphism. Asymptotic upper bounds for value sets of non-exceptional finite morphisms are given in [6].

References

[1] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961), 121-130.

[2] Q. Cheng, J. Hill and D. Wan, Counting value sets: algorithms and complexity, Tenth Algorithmic Number Theory Symposium ANTS-X, 2012.

[3] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970), 255-271.

[4] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, in *Finite Fields with Applications in Coding Theory, Cryptography and Related Areas*, G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, Eds., Springer, 2002, 80-85.

[5] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988), no. 2, 167-188.

[6] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101(1997), 255-287.

[7] H. W. Lenstra, Jr., private communication to Daqing Wan.

[8] R. Lidl and H. Niederreiter, Finite Fields, Sec. Ed., Cambridge University Press, Cambridge, 1997.

[9] R. Lipton, Claiming Picard's math may have gaps, http://rjlipton.wordpress.com/2011/09/26/claiming-picards-math-may-have-gaps/.

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

[11] G. L. Mullen, Permutation polynomials over finite fields, Lecture Notes in Pure and Appl. Math., Vol. 141, Marcel Dekker, New York, 1992, 131-151.

[12] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1(1995), 64-82.

[13] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, Lecture Notes in Pure and Appl. Math., Vol. 141, Marcel Dekker, New York, 1992, 209-216.

[14] 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.

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802

E-mail address: mullen@math.psu.edu

Department of Mathematics, University of California, Irvine, CA 92697-3875

E-mail address: dwan@math.uci.edu

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive,, Ottawa, ON K1S 5B6, Canada
E-mail address: wang@math.carleton.ca