Finite Fields and Their Applications 38 (2016) 13–26

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A refinement of multivariate value set bounds

Luke Smith *, Daqing Wan

340 Rowland Hall (Bldg. # 400), University of California, Irvine, Irvine, CA 92697-3875, United States

ARTICLE INFO

Article history:
Received 24 September 2015
Received in revised form 27 November 2015
Accepted 29 November 2015
Available online 21 December 2015
Communicated by Rudolf Lidl

MSC:
11T06
11T55
11H06

Keywords:
Value set
Polynomial image set
Multivariate polynomials
Newton polytopes
p-adic liftings

ABSTRACT

Over finite fields, if the image of a polynomial map is not the entire field, then its cardinality can be bounded above by a significantly smaller value. Earlier results bound the cardinality of the value set using the degree of the polynomial, but more recent results make use of the powers of all monomials.

In this paper, we explore the geometric properties of the Newton polytope and show how they allow for tighter upper bounds on the cardinality of the multivariate value set. We then explore a method which allows for even stronger upper bounds, regardless of whether one uses the multivariate degree or the Newton polytope to bound the value set. Effectively, this provides improvement of a degree matrix-based result given by Zan and Cao, making our new bound the strongest upper bound thus far.

1. Recent multivariate value set theorems

For a given polynomial $f(x)$ over a finite field $\mathbb{F}_q$, let $V_f := \mathrm{Im}(f)$ denote the value set of f. Determining the cardinality and structure of the value set is a problem with a

* Corresponding author.
E-mail addresses: smithla@uci.edu (L. Smith), dwan@math.uci.edu (D. Wan).

http://dx.doi.org/10.1016/j.ffa.2015.11.002
1071-5797/

rich history and wide variety of uses in number theory, algebraic geometry, coding theory and cryptography.

Relevant to this paper are theorems which provide upper bounds on the cardinality of our value set when $f(x)$ is not a permutation polynomial.[1] These upper bounds have been extensively studied in the case of univariate polynomials (see [10] for more information), but results on multivariate polynomial maps have gained more recent attention.

A result published by Mullen, Wan, and Wang in 2012 [8] gives a bound on the value set of polynomial maps, one with no error terms:

Theorem 1.1. *Let* $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ *be a polynomial map over the vector space* $\mathbb{F}_q^n$*, and let* $\deg f = \max_i \deg f_i$*.*

$$\text{If } |V_f| < q^n, \text{ then } |V_f| \leq q^n - \min\left\{q, \frac{n(q-1)}{\deg f}\right\}.$$

Since the time their paper was published, multiple refinements have been made to this theorem.

One approach towards improving Theorem 1.1 is to replace the term $\frac{n(q-1)}{\deg f}$ by using different properties of the polynomial map f. Note that the degree only takes one monomial of f into account, so it is reasonable to expect tighter bounds on $|V_f|$ if we account for every monomial. Smith [10] improved upon Theorem 1.1 by generalizing Mullen, Wan, and Wang's p-adic lifting approach and utilizing the Newton polytope $\Delta(f)$ of the polynomial map f. The Newton polytope is constructed using all monomials of f using discrete geometry, meaning it encodes more information than $\deg f$ and allows for a stronger statement to be made:

Theorem 1.2. *(See Smith [10], 2014.) Let* $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ *be a polynomial map over the vector space* $\mathbb{F}_q^n$*, let* $\Delta(f)$ *be the Newton polytope of* f*, and let* μ_f *be a certain constant (defined explicitly later) dependent on* $\Delta(f)$*.*

$$\text{If } |V_f| < q^n, \text{ then } |V_f| \leq q^n - \min\{q, \mu_f \cdot (q-1)\}.$$

Zan and Cao also refine Theorem 1.1 by using the degree matrix D_f of the polynomial map f in order to account for all of the monomials of f. Their approach generalizes the p-adic lifting technique as well and improves upon Smith's statement in [10]:

Theorem 1.3. *(See Zan, Cao [15], 2014.) Let* $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ *be a polynomial map over the vector space* $\mathbb{F}_q^n$ *and let* D_f *be the degree matrix of* f*.*

[1] Permutation polynomials have also been studied extensively in literature, in view of their application to cryptography and combinatorics. For more information about other ways value sets have been studied historically, please refer to [6].