Finite Fields and Their Applications 54 (2018) 253–272

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Value sets of bivariate folding polynomials over finite fields

Ömer Küçüksakallı

Middle East Technical University, Mathematics Department, 06800 Ankara, Turkey

ARTICLE INFO

Article history:
Received 15 November 2017
Received in revised form 14 February 2018
Accepted 2 May 2018
Available online xxxx
Communicated by Wang Qiang

MSC:
11T06

Keywords:
Lie algebra
Weyl group
Fixed point
Permutation

ABSTRACT

We find the cardinality of the value sets of polynomial maps associated with simple complex Lie algebras B_2 and G_2 over finite fields. We achieve this by using a characterization of their fixed points in terms of sums of roots of unity.

Introduction

Let q be a power of a prime p. Given a polynomial $f \in \mathbf{Z}[\mathbf{x}]$ with n variables, we write $\bar{f}$ for the induced map over $\mathbf{F}_q$. If $\bar{f} : \mathbf{F}_q^n \to \mathbf{F}_q^n$ is not a bijection, then one may ask how far it is away from being a bijection. An approach to investigate this problem is to find the cardinality of the value set $\bar{f}(\mathbf{F}_q^n)$. For an arbitrary polynomial map $f \in \mathbf{Z}[\mathbf{x}]$, there is no easy formula for this quantity. However, there are certain families with nice underlying

E-mail address: komer@metu.edu.tr.

https://doi.org/10.1016/j.ffa.2018.05.008
1071-5797/

algebraic structures which allow us to find the cardinality explicitly. An interesting single variable example is the family of Dickson polynomials for which a formula was found by Chou, Gomez-Calderon and Mullen [1].

There is a generalization of Dickson polynomials, or Chebyshev polynomials, to several variables introduced by Lidl and Wells. They provide easy to check conditions for these functions to induce permutations over finite fields [5]. Lidl and Wells achieve this by using the theory of symmetric polynomials together with some basic methods in the theory of finite fields. On the other hand, their construction can be related to the simple complex Lie algebras A_n [2]. In general, for an arbitrary Lie algebra $\mathfrak{g}$, there is an associated infinite sequence of integrable polynomial mappings $P_{\mathfrak{g}}^k$ determined from the conditions

$$\Phi_{\mathfrak{g}}(k\mathbf{x}) = P_{\mathfrak{g}}^k(\Phi_{\mathfrak{g}}(\mathbf{x})).$$

Here, the components of the vector function $\Phi_{\mathfrak{g}}$ are given by exponential sums which are obtained by the orbits of the Weyl group of $\mathfrak{g}$. All coefficients of the polynomials defining $P_{\mathfrak{g}}^k$ are integers. This result was first given by Veselov [6], and somewhat later by Hofmann and Withers [2], independently. These maps $P_{\mathfrak{g}}^k$ are also referred as folding polynomials [7]. This is because the parameter k acts by folding over the underlying triangular fundamental region in the case of a rank two simple complex Lie algebra.

In our previous work [4], we have provided easy to check conditions for the bivariate folding polynomials associated with B_2 and G_2 to induce permutations over finite fields. In this paper, we extend our results, by finding the cardinality of the value set for each member in those families, not only for the members that give permutations.

The organization of the paper is as follows: In the first section we give three examples which illustrate the idea that will be used for the further cases; the first example is the power maps which is the most elementary, the other two examples are the folding polynomials associated with the Lie algebras A_1 and A_2. In the second and the third sections, we consider the folding polynomials associated with B_2 and G_2, respectively. For each one of these two families, we prove a formula for the cardinality of its value set over finite fields.

1. Motivation

In this section, we consider the cardinality of the value sets of three basic families, namely the power maps and folding polynomials associated with A_1 and A_2. We give alternative proofs of formulas for the cardinality of their value sets which will be a motivation for the further cases B_2 and G_2.

1.1. The power maps

The nonzero elements of $\mathbf{F}_q$ can be parametrized by roots of unity. This parametrization is useful while studying the action of power maps $P_k(x) = x^k$ on such fields. Let