Discrete Applied Mathematics 217 (2017) 294–303

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On derivatives of polynomials over finite fields through integration

E. Pasalic[a,*], A. Muratović-Ribić[b], S. Hodzić[c], S. Gangopadhyay[d]

[a] *University of Primorska, FAMNIT & IAM, Glagoljaska 6, 6000 Koper, Slovenia*
[b] *University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina*
[c] *University of Primorska, FAMNIT, Glagoljaska 6, 6000 Koper, Slovenia*
[d] *Department of Computer Science and Engineering, Indian Institute of Technology, Roorkee, India*

ARTICLE INFO

Article history:
Received 20 January 2016
Received in revised form 13 June 2016
Accepted 20 July 2016
Available online 22 October 2016

Keywords:
Finite fields
Boolean functions
Derivatives
Linear structures
Planar mappings

ABSTRACT

In this article, using rather elementary technique and the derived formula that relates the coefficients of a polynomial over a finite field and its derivative, we deduce many interesting results related to derivatives of Boolean functions and derivatives of mappings over finite fields. For instance, we easily identify several infinite classes of polynomials which cannot possess linear structures. The same technique can be applied for deducing a nontrivial upper bound on the degree of so-called planar mappings.

1. Introduction

Let $\mathbb{F}_q$ denote the Galois field of order $q = p^n$, and let the corresponding vector space be denoted as $\mathbb{F}_p^n$. For a given polynomial $F(x) \in \mathbb{F}_q[x]$ its derivative at $a \in \mathbb{F}_q^*$ is defined as $D_aF(x) = F(x+a) - F(x)$, where clearly $a = 0$ results in a trivial annihilation. In contrast to the standard notion of derivative, which is for instance useful for determination of multiple roots of F and which coincides to the derivation of polynomials over real numbers, this notion of derivatives is of great importance in cryptography and is directly related to differential properties of the mappings used in the substitution boxes. Indeed, when $p = 2$ the differential properties of F (that reflects the resistance to differential cryptanalysis [1]) are characterized by the number of solutions of $F(x+a) + F(x) = b$ for any $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. On the other hand, for fields of odd prime characteristic $p > 2$, if $F(x+a) - F(x)$ is a permutation for any nonzero a then F is called a planar function [7,5,6].

The concept of linear structures plays an important role in cryptographic applications. Certainly, for functions over finite fields (whose prime field is binary) the substitution boxes (S-boxes) identified as a polynomial $F(x) \in \mathbb{F}_{2^n}[x]$, represented as $F(x) = \sum_{i=0}^{q-1} b_i x^i$, should not contain linear structures a so that $F(x+a) + F(x) = b$ for some fixed $b \in \mathbb{F}_{2^n}$ and for all $x \in \mathbb{F}_{2^n}$. In this case a is called b-linear structure. A few general results are known about the form of polynomials $F(x)$ admitting linear structures [3,4,16,14]. The same applies to the Boolean case when $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ which again may be represented as $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ but the coefficients a_i must satisfy certain conditions, see Section 2. In [16], the properties

[*] Corresponding author. Fax: +386 (5) 611 75 71.
E-mail addresses: enes.pasalic6@gmail.com (E. Pasalic), amela@pmf.unsa.ba (A. Muratović-Ribić), samir_hodzic89@hotmail.com (S. Hodzić), gsugata@gmail.com (S. Gangopadhyay).

http://dx.doi.org/10.1016/j.dam.2016.07.025
0166-218X/© 2016 Elsevier B.V. All rights reserved.

of the set of differential functions defined as $\mathcal{DF}_q = \{D_aF(x) : F(x) \in F_q[x], a \in \mathbb{F}_q^*\}$ was investigated. One should notice that there exist polynomials in $\mathbb{F}_q[x]$ which are not derivatives of any polynomial, thus they do not belong to $\mathcal{DF}_q$. The main result in [16] concerning the existence of linear structures is that $F(x) \in \mathbb{F}_{2^n}[x]$ is a differential function (thus $F(x) \in \mathcal{DF}_q$) if and only if it has a 0-linear structure. This implies that the necessary condition to avoid linear structures is that $F(x) \notin \mathcal{DF}_q$, for $q = 2^n$. In [3], the authors investigated the existence of linear structures for the mappings of the form $F(x) = Tr(\delta x^s)$, where $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$. For polynomials over finite fields a thorough treatment of binomials $F(x) = x^s + \alpha x^d$ was taken in [4]. The case of the discrete integration in finite fields of characteristic two and some result on the 0-linear structures of higher-order derivatives were studied recently in [14].

A detailed study of the cryptanalytic significance of linear structures was initiated by Evertse [9] in which cryptanalysis of DES like ciphers are discussed along with several possible extensions. Linear structures were also considered by Nyberg and Knudsen in the context of provable security against a differential attack [13], and later in many works e.g. [11,8,12,14]. The connection between the existence of linear structures and the differential profile of functions over finite fields is an important area of investigation in the context of the designs of S-boxes. The relevance of this area has increased significantly due to the recent cryptographic need of development of S-boxes (vectorial Boolean functions) suitable for use in lightweight ciphers, see for instance [10,2].

To sum up the critical technological impact of this area of research we refer to the foreword written by Bart Preneel in the recent book by Tokareva [15] which is entirely devoted to bent functions. Preneel writes: "Perhaps the largest impact on modern cryptography to date would be generated by the study of generalizations to vector Boolean functions that offer strong resistance against differential and linear attacks by Nyberg and others. This work resulted in the S-box used in the Advanced Encryption Standard (AES) that is today used in billions of devices". Incidentally bent functions are Boolean functions having no linear structures whose cryptographic applications include employment in the designs of CAST, Grain and HAVAL, as well as "non-cryptographic" uses in the designs of Hadamard matrices, strongly regular graphs, Kerdock codes and CDMA sequences.

In this article we firstly derive the relationship between the coefficients b_i of $F(x) = \sum_{i=0}^{q-1} b_i x^i$ and the coefficients c_i of its derivative $G(x) = F(x+a) - F(x) = \sum_{i=0}^{q-2} c_i x^i$. This connection can be efficiently used for specifying conditions regarding the existence of linear structures for either Boolean functions or for mappings over finite fields. Though the approach is quite elementary it leads to several important results in this direction. For instance, it is sufficient that $F(x)$ contains the highest polynomial degree term x^{q-1} so that F does not admit linear structures, which when translated into the domain of Boolean functions corresponds to a class of functions of highest algebraic degree. Noticing that any n-variable Boolean function can also be represented as a univariate polynomial $f(x) = \sum_{i=0}^{q-1} b_i x^i \in \mathbb{F}_{2^n}[x]$, where the coefficients b_i satisfy certain conditions, we apply the same technique to either mappings over finite fields or to Boolean mappings. While the linear structures of monomials and binomials are quite easy to handle, in general the existence of linear structures for arbitrary polynomials is harder to analyze. Nevertheless, we provide a few interesting results in this direction covering also some particular cases when F contains an arbitrary number of terms. Finally, using the same technique we provide a nontrivial upper bound on the degree of planar mappings.

This article is organized as follows. Some basic definitions and notions are given in Section 2. In Section 3, some general results (based on the derived connection between a given function and its derivative) related to the existence of linear structures for polynomials over finite fields and for Boolean functions are presented. In Section 4, a nontrivial upper bound on the degree of planar mappings is derived. Some concluding remarks are given in Section 5.

2. Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field of characteristic two. Furthermore, let $\mathbb{F}_{2^n}$ denote the Galois field of order 2^n and $\mathbb{F}_2^n$ be its corresponding vector space (once the basis is fixed). Any function from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is called an n variable Boolean function, and the set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. The algebraic normal form (ANF) of a Boolean function, f on $\mathbb{F}_2^n$ is a multivariate polynomial in $x_1, \ldots, x_n$,

$$f(x_1, \ldots, x_n) = \sum_{\mathbf{a} \in \mathbb{F}_2^n} \mu_{\mathbf{a}} \prod_{i=1}^{n} x_i^{a_i}, \quad \text{where } \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The *algebraic degree* of $f \in \mathcal{B}_n$, denoted by $\deg(f)$, is defined as $\max\{wt(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0, \mathbf{a} \in \mathbb{F}_{2^n}\}$, where $wt(\mathbf{a})$ denotes the Hamming weight of a binary vector $\mathbf{a}$.

For the purpose of this paper another equivalent representation of Boolean functions is also of interest. The univariate representation of Boolean functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is given as,

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \quad a_i \in \mathbb{F}_{2^n}, \tag{1}$$

where the coefficients $a_i \in \mathbb{F}_{2^n}$ satisfy the following (Boolean conditions): $a_0, a_{2^n-1} \in \mathbb{F}_2$ and $a_{2i \pmod{2^n-1}} = a_i^2$ for $i = 1, \ldots, 2^n - 2$, due to the condition $f(x)^2 \equiv f(x) \pmod{x^{2^n} - x}$. Consequently, using the univariate representation