ARTICLE IN PRESS
JPAA:5694

Journal of Pure and Applied Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Differential uniformity and second order derivatives for generic polynomials

Yves Aubry [a,b], Fabien Herbaut [a,c]

[a] Institut de Mathématiques de Toulon, Université de Toulon, France
[b] Aix-Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
[c] ESPE Nice-Toulon, Université Nice Sophia Antipolis, France

ARTICLE INFO

Article history:
Received 18 January 2016
Received in revised form 18 May 2017
Available online xxxx
Communicated by I.M. Duursma

MSC:
14G50; 11T71; 94A60

ABSTRACT

For any polynomial f of $\mathbb{F}_{2^n}[x]$ we introduce the following characteristic of the distribution of its second order derivative, which extends the differential uniformity notion:

$$\delta^2(f) := \max_{\substack{\alpha \in \mathbb{F}_{2^n}^*, \alpha' \in \mathbb{F}_{2^n}^*, \beta \in \mathbb{F}_{2^n} \\ \alpha \neq \alpha'}} \sharp\{x \in \mathbb{F}_{2^n} \mid D^2_{\alpha,\alpha'} f(x) = \beta\}$$

where $D^2_{\alpha,\alpha'} f(x) := D_{\alpha'}(D_\alpha f(x)) = f(x) + f(x+\alpha) + f(x+\alpha') + f(x+\alpha+\alpha')$ is the second order derivative. Our purpose is to prove a density theorem relative to this quantity, which is an analogue of a density theorem proved by Voloch for the differential uniformity.

1. Introduction

For any polynomial $f \in \mathbb{F}_q[x]$ where $q = 2^n$, and for $\alpha \in \mathbb{F}_q^*$, the derivative of f with respect to α is the polynomial $D_\alpha f(x) = f(x+\alpha) + f(x)$. The differential uniformity $\delta(f)$ of f introduced by Nyberg in [6] is then defined by

$$\delta(f) := \max_{(\alpha,\beta) \in \mathbb{F}_q^* \times \mathbb{F}_q} \sharp\{x \in \mathbb{F}_q \mid D_\alpha f(x) = \beta\}.$$

To stand against differential cryptanalysis, one wants to have a small differential uniformity (ideally equal to 2). Voloch proved that most polynomials f of $\mathbb{F}_q[x]$ of degree $m \equiv 0, 3 \pmod 4$ have a differential uniformity equal to $m-1$ or $m-2$ (Theorem 1 in [11]).

E-mail addresses: yves.aubry@univ-tln.fr (Y. Aubry), fabien.herbaut@unice.fr (F. Herbaut).

http://dx.doi.org/10.1016/j.jpaa.2017.06.009

When studying differential cryptanalysis, Lai introduced in [5] the notion of higher order derivatives. The higher order derivatives are defined recursively by $D_{\alpha_1,\dots,\alpha_{i+1}} f = D_{\alpha_1,\dots,\alpha_i}(D_{\alpha_{i+1}} f)$, and a new design principle is given in [5]: "*For each small i, the nontrivial i-th derivatives of function should take on each possible value roughly uniform*". After considering the differential uniformity, it seems natural to investigate the number of solutions of the equation $D_{\alpha_1,\alpha_2} f(x) = \beta$, that is of the equation

$$f(x) + f(x + \alpha_1) + f(x + \alpha_2) + f(x + \alpha_1 + \alpha_2) = \beta$$

and thus to consider the second order differential uniformity of f over $\mathbb{F}_q$:

$$\delta^2(f) := \max_{\substack{\alpha\in\mathbb{F}_q^*,\alpha'\in\mathbb{F}_q^*,\beta\in\mathbb{F}_q \\ \alpha\neq\alpha'}} \sharp\{x \in \mathbb{F}_q \mid D^2_{\alpha,\alpha'} f(x) = \beta\}.$$

For example, the inversion mapping from $\mathbb{F}_q$ to itself which sends x to x^{-1} if $x \neq 0$ and 0 to 0 (and which corresponds to the polynomial $f(x) = x^{q-2}$) has a differential uniformity $\delta(f) = 2$ for n odd and $\delta(f) = 4$ for n even (see [6]). We will prove in Section 8 that it has a second order differential uniformity $\delta^2(f) = 8$ for any $n \geqslant 6$.

The purpose of the paper is to prove that, as Voloch proved it for the differential uniformity, most polynomials f have a maximal $\delta^2(f)$. More precisely, we prove (Theorem 7.1) that: for a given integer $m \geqslant 7$ such that $m \equiv 0 \pmod 8$ (respectively $m \equiv 1, 2, 7 \pmod 8$), and with $\delta_0 = m - 4$ (respectively $\delta_0 = m - 5, m - 6, m - 3$) we have

$$\lim_{n\to\infty} \frac{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m,\ \delta^2(f) = \delta_0\}}{\sharp\{f \in \mathbb{F}_{2^n}[x] \mid \deg(f) = m\}} = 1.$$

We follow and generalize the ideas of Voloch in [11]. Let us present the strategy.

- In Section 2, we associate to any integer m an integer d depending on the congruence of m modulo 4 (Definition 2.1). Then, if α and α' are two distinct elements of $\mathbb{F}_q^*$, we associate (Proposition 2.2) to any polynomial $f \in \mathbb{F}_q[x]$ of degree m a polynomial $L_{\alpha,\alpha'}(f)$ (which will be sometimes denoted by g for simplicity) of degree less than or equal to d such that:

$$D^2_{\alpha,\alpha'} f(x) = g\big(x(x + \alpha)(x + \alpha')(x + \alpha + \alpha')\big).$$

- In Section 3, we determine the geometric and the arithmetic monodromy groups of $L_{\alpha,\alpha'}(f)$ when this polynomial is Morse (Proposition 3.1). For α and α' fixed, we give an upper bound depending only on m and q for the number of polynomials f of $\mathbb{F}_q[x]$ of degree at most m such that $L_{\alpha,\alpha'}(f)$ is non-Morse (Proposition 3.2).
- Section 4 is devoted to the study of the monodromy groups of $D^2_{\alpha,\alpha'} f$. In order to apply the Chebotarev's density theorem (Theorem 5.1) we look for a condition of regularity, that is a condition for $\mathbb{F}_q$ to be algebraically closed in the Galois closure of the polynomial $D^2_{\alpha,\alpha'} f(x)$ (Proposition 4.6).
- In Section 5, we use the Chebotarev theorem to prove that (Proposition 5.2) for q sufficiently large and under the regularity hypothesis the polynomial $D^2_{\alpha,\alpha'} f(x) + \beta$ totally splits in $\mathbb{F}_q[x]$.
- In Section 6, we show that we can choose a finite set of couples (α_i, α'_i) such that most polynomials $f \in \mathbb{F}_q[x]$ of degree m satisfy the above regularity condition (Proposition 6.1).
- Finally, Section 7 is devoted to the statement and the proof of the main theorem (Theorem 7.1).

To fix notation, throughout the whole paper we consider n a non-negative integer and $q = 2^n$. We denote by $\mathbb{F}_q$ the finite field with q elements, by $\mathbb{F}_q[x]$ the ring of polynomials in one variable over $\mathbb{F}_q$ and by

Please cite this article in press as: Y. Aubry, F. Herbaut, Differential uniformity and second order derivatives for generic polynomials, J. Pure Appl. Algebra (2017), http://dx.doi.org/10.1016/j.jpaa.2017.06.009