ON THE HIGHER TERM OF THE DIFFERENTIAL SPECTRUM OF A FUNCTION

YVES AUBRY

Abstract. We deal with the number of times that the differential uniformity of a function is reached with a connection to a conjecture of Voloch.

1. Introduction

For a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, and for $\alpha \in \mathbb{F}_{2^n}$, we define the derivative of f with respect to α as the function $D_\alpha f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ defined by

$$D_\alpha f(x) = f(x+\alpha) + f(x), \ \forall x \in \mathbb{F}_{2^n}.$$

We define the differential uniformity $\delta(f)$ of the function f by:

$$\delta(f) = \max_{\alpha \neq 0, \beta} \sharp\{x \in \mathbb{F}_{2^n} \mid D_\alpha f(x) = \beta\}.$$

2. Voloch conjecture

Voloch has conjectured in [3] the following:

Conjecture 1. *For a given integer $m > 4$, there exists $\varepsilon_m > 0$ such that for all sufficiently large n, if f is a polynomial of degree m over $\mathbb{F}_{2^n}$ for at least $\varepsilon_m 2^{2n}$ values of $\alpha \neq 0$, $\beta \in \mathbb{F}_{2^n}$,*

$$\sharp\{x \in \mathbb{F}_{2^n} \mid f(x+\alpha) + f(x) = \beta\} = \delta(f).$$

A corollary of this conjecture would be that picking $\alpha \neq 0$, $\beta \in \mathbb{F}_{2^n}$ at random gives a probabilistic polynomial time algorithm for computing $\delta(f)$.

3. The quantity $\Delta(f)$

For a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ and for $\alpha, \beta \in \mathbb{F}_{2^n}$, let us define $\delta_f(\alpha, \beta)$ or for convenience $\delta(\alpha, \beta)$ by:

$$\delta(\alpha, \beta) = \sharp\{x \in \mathbb{F}_{2^n} \mid f(x+\alpha) + f(x) = \beta\}.$$

Hence, the differential uniformity of f is just: $\delta(f) = \max_{\alpha \neq 0, \beta \in \mathbb{F}_{2^n}} \delta(\alpha, \beta)$.

Now we denote

$$\Delta(f) = \sharp\{(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid \delta(\alpha, \beta) = \delta(f)\}.$$

Date: May 12, 2010.

2000 *Mathematics Subject Classification.* 11R29,11R58,11R11,14H05.

Key words and phrases. Differential uniformity, power functions, APN functions.

The quantity $\Delta(f)$ corresponds to the number of 2-uplets which maximise the function $\delta(.,.)$.

The conjecture of Voloch can be rephrase as: For any $m \geq 5$, there exists $\varepsilon_m > 0$ such that for all sufficiently large n, if f is a polynomial of degree m over $\mathbb{F}_{2^n}$,

$$\Delta(f) \geq \varepsilon_m 2^{2n}.$$

We propose here to study $\Delta(f)$.

4. Differential spectrum

In analogy with the differential spectrum defined in [1] for power functions, we define the complete differential spectrum of $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ by:

$$\mathrm{Spec}(f) = \{\Omega_0, \Omega_2, \ldots, \Omega_{\delta(f)}\}$$

where

$$\Omega_i = \sharp\{(\alpha, \beta) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid \delta(\alpha, \beta) = i\}.$$

The quantity $\Delta(f)$ is nothing but $\Omega_{\delta(f)}$.

If f is a power function, namely $f(x) = x^d$, then for any nonzero $\alpha \in \mathbb{F}_{2^n}$ the equation $(x+\alpha)^d + x^d = \beta$ can be written

$$\alpha^d\Big((\frac{x}{\alpha} + 1)^d + (\frac{x}{\alpha})^d\Big) = \beta.$$

Thus $\delta(\alpha, \beta) = \delta(1, \beta/\alpha^d)$ for all $\alpha \neq 0$.

Hence, for all $\alpha \neq 0$, we have:

$$\sharp\{\beta \in \mathbb{F}_{2^n} \mid \delta(\alpha, \beta) = i\} = \sharp\{\beta \in \mathbb{F}_{2^n} \mid \delta(1, \beta) = i\},$$

i.e. it suffices to consider the derivative $D_1 f$ to get the complete differential spectrum of a power function f. In this sipirit, Blondeau, Canteaut and Charpin in [1] have defined the differential spectrum of a power function f as the set of ω_i, $i = 0, 2, \ldots, \delta(f)$ where

$$\omega_i = \sharp\{\beta \in \mathbb{F}_{2^n} \mid \delta(1, \beta) = i\}.$$

We have of course: $\Omega_i = 2^{n-1}\omega_i$.

5. First bounds

We have:

Proposition 1. *If $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ then:*

$$\Delta(f) \leq (2^n - 1) \times \frac{2^n}{\delta(f)} \leq (2^n - 1) \times 2^{n-1}.$$

Moreover, if f is is a power function then:

$$\Delta(f) \geq 2^n - 1.$$

Remark 2. *Recall that a function f is called APN if $\delta(f) = 2$, i.e. the function $(\alpha, \beta) \longmapsto \delta(\alpha, \beta)$ has for image $\{0, 2\}$. Another way to say that is to say that all the derivatives $D_\alpha f$ of f are 2-to-1 (for any $a \in \mathbb{F}_{2^n}$), hence half of the elements of $\mathbb{F}_{2^n}$ have two preimages by $D_\alpha f$. Thus if f is APN, then $\Delta(f) = (2^n - 1)2^{n-1}$ and the upper bound of the previous proposition is reached.*

Remark 3. *Nyberg has shown in* [2] *that $f(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ has $\delta(f) = 4$ when n is even. Moreover, we can show that $\Delta(f) = 2^n - 1$. Indeed, the derivative $D_1 f$ is given by: $D_1 f(x) = \frac{1}{x(x+1)}$ if $x \neq 0$ and $x \neq 1$, and $D_1 f(0) = D_1 f(1) = 1$. If $\beta = 1$, then β has four preimages: 0, 1 and the two roots of $x^2 + x + 1 = 0$. If $\beta \neq 0$ and $\neq 1$, then a preimage x of β, if it exits, would satisfies the equation $x^2 + x + b = 0$ where $b = \beta^{-1}$. But, by Hilbert's Theorem 90, this equation has two solutions if $Tr(b) = 0$ and zero solution else. Here, Tr denotes the trace function of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ which is a linear form, thus its kernel is an hyperplane and hence has 2^{n-1} elements. Thus $\Omega_0 = (2^n - 1)(2^{n-1} + 1)$, $\Omega_2 = (2^n - 1)(2^{n-1} - 2)$ and $\Delta(f) = \Omega_4 = 2^n - 1$. Thus, the lower bound of the previous proposition is reached.*

Example 1 : If $f(x) = x^m$ is a power permutation of $\mathbb{F}_{2^n}$ (i.e. $(2^n - 1, m) = 1$) and if $\delta(f) = 4$ then it is proved in [1] (corollary 4.2) that

$$\Delta(f)/(2^n - 1) = \kappa - 2^{n-2}$$

where $2^{n-2} < \kappa \leq 2^{n-1}$. Hence, we deduce that $\Delta(f) \leq (2^n - 1)2^{n-2}$. Note that for a Kasami exponent (i.e. $m = 2^{2k} - 2^k + 1$ with $(n, k) = 1$), we have $\Delta(f) = (2^n - 1)2^{n-2}$.

Example 2 : Let us consider functions f with a two-valued differential spectra i.e. such that $\delta(\alpha, \beta)$ takes two values, namely 0 and κ. As shown in [1], κ must be a power of 2 since in this case the function $x \longmapsto D_\alpha f(x)$ is $\delta(f)$-to-1 for any fixed α. Hence, we find:

$$\Delta(f) = (2^n - 1) \times \frac{2^n}{\delta(f)}.$$

We will study here the quantity $\Delta(f)$ and the related Voloch conjecture in different cases.

References

[1] C. Blondeau, A. Canteaut and P. Charpin, *Differential properties of power functions*, Int. J. Information and Coding Theory, Vol. 1, No. 2, 149-170, (2010).

[2] K. Nyberg, *Differentially uniform mappings for cryptography*, In Advances in Cryptology, Eurocrypt'93, LNCS vol. 765, p. 55-64, Springer-Verlag, 1993.

[3] J. F. Voloch, *Symmetric cryptography and algebraic curves, Algebraic Geometry and its Applications*, Series on Number Theory and Its Aplications, Vol. 5, World scientific, 135-141, (2008).

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France
E-mail address: yves.aubry@univ-tln.fr