Contemporary Mathematics
Volume **521**, 2010

Differentially 4-uniform functions

Yves Aubry and François Rodier

Abstract. We give a geometric characterization of vectorial Boolean functions with differential uniformity ≤ 4. This enables us to give a necessary condition on the degree of the base field for a function of degree $2^r - 1$ to be differentially 4-uniform.

1. Introduction

We are interested in vectorial Boolean functions from the $\mathbb{F}_2$-vectorial space $\mathbb{F}_2^m$ to itself in m variables, viewed as polynomial functions $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ over the field $\mathbb{F}_{2^m}$ in one variable of degree at most $2^m - 1$. For a function $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$, we consider, after K. Nyberg (see [**16**]), its differential uniformity

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

This is clearly a strictly positive even integer.

Functions f with small $\delta(f)$ have applications in cryptography (see [**16**]). Such functions with $\delta(f) = 2$ are called almost perfect nonlinear (APN) and have been extensively studied: see [**16**] and [**9**] for the genesis of the topic and more recently [**3**] and [**6**] for a synthesis of open problems; see also [**7**] for new constructions and [**20**] for a geometric point of view of differential uniformity.

Functions with $\delta(f) = 4$ are also useful; for example the function $x \longmapsto x^{-1}$, which is used in the AES algorithm over the field $\mathbb{F}_{2^8}$, has differential uniformity 4 on $\mathbb{F}_{2^m}$ for any even m. Some results on these functions have been collected by C. Bracken and G. Leander [**4, 5**].

We consider here the class of functions f such that $\delta(f) \leq 4$, called differentially 4-uniform functions. We will show that for polynomial functions f of degree $d = 2^r - 1$ such that $\delta(f) \leq 4$ on the field $\mathbb{F}_{2^m}$, the number m is bounded by an expression depending on d. The second author demonstrated the same bound in the case of APN functions [**17, 18**]. The principle of the method we apply here was already used by H. Janwa et al. [**13**] to study cyclic codes and by A. Canteaut [**8**] to show that certain power functions could not be APN when the exponent is too large.

2000 *Mathematics Subject Classification.* 11R29,11R58,11R11,14H05.
Key words and phrases. Boolean functions, almost perfect nonlinear functions, varieties over finite fields.

Henceforth we fix $q = 2^m$.

In order to simplify our study of such functions, let us recall the following elementary results on differential uniformity; the proofs are straightforward:

PROPOSITION 1. *(i) Adding a polynomial whose monomials are of degree 0 or a power of 2 to a function f does not change $\delta(f)$.*

(ii) For all a, b and c in $\mathbb{F}_q$, such that $a \neq 0$ and $c \neq 0$ we have

$$\delta(cf(ax+b)) = \delta(f).$$

(iii) One has $\delta(f^2) = \delta(f)$.

Hence, without loss of generality, from now on we can assume that f is a polynomial mapping from $\mathbb{F}_q$ to itself which has neither terms of degree a power of 2 nor a constant term, and which has at least one term of odd degree.

To any function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, we associate the polynomial

$$f(x) + f(y) + f(z) + f(x+y+z).$$

Since this polynomial is clearly divisible by

$$(x+y)(x+z)(y+z),$$

we can consider the polynomial

$$P_f(x,y,z) := \frac{f(x) + f(y) + f(z) + f(x+y+z)}{(x+y)(x+z)(y+z)}$$

which has degree $\deg(f) - 3$ if $\deg(f)$ is not a power of 2.

2. A characterization of functions with $\delta \leq 4$

We will give, as in [**17**], a geometric criterion for a function to have $\delta \leq 4$. We consider in this section the algebraic set X defined by the elements (x, y, z, t) in the affine space $\mathbb{A}^4(\overline{\mathbb{F}}_q)$ such that

$$P_f(x,y,z) = P_f(x,y,t) = 0.$$

We set also V the hypersurface of the affine space $\mathbb{A}^4(\overline{\mathbb{F}}_q)$ defined by

$$(x+y)(x+z)(x+t)(y+z)(y+t)(z+t)(x+y+z+t) = 0. \tag{1}$$

The hypersurface V is the union of the seven hyperplanes $H_1, \ldots, H_7$ defined respectively by the equations $x + y = 0, \ldots, x + y + z + t = 0$.

We begin with a simple lemma:

LEMMA 2. *The following two properties are equivalent:*

(i) there exist 6 distinct elements $x_0, x_1, x_2, x_3, x_4, x_5$ in $\mathbb{F}_q$ such that

$$\begin{cases} x_0 + x_1 = \alpha, & f(x_0) + f(x_1) = \beta \\ x_2 + x_3 = \alpha, & f(x_2) + f(x_3) = \beta \\ x_4 + x_5 = \alpha, & f(x_4) + f(x_5) = \beta \end{cases}$$

(ii) there exist 4 distinct elements x_0, x_1, x_2, x_4 in $\mathbb{F}_q$ such that $x_0 + x_1 + x_2 + x_4 \neq 0$ and such that

$$\begin{cases} f(x_0) + f(x_1) + f(x_2) + f(x_0 + x_1 + x_2) = 0 \\ f(x_0) + f(x_1) + f(x_4) + f(x_0 + x_1 + x_4) = 0. \end{cases}$$

Proof. Suppose that (i) is true. Then we have $x_0+x_1+x_2=\alpha+x_2=x_3$ and so $f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)=f(x_0)+f(x_1)+f(x_2)+f(x_3)=0$. The second equation holds true in the same way. Finally, we have $x_0+x_1+x_2+x_4=x_3+x_4\neq 0$.

Conversely, let us set $\alpha=x_0+x_1$, $\beta=f(x_0)+f(x_1)$ and $x_3=\alpha+x_2=x_0+x_1+x_2$. Then $f(x_2)+f(x_3)=f(x_2)+f(x_0+x_1+x_2)=f(x_0)+f(x_1)=\beta$. Furthermore, we have $x_3\neq x_0$ because $x_1\neq x_2$ and we have $x_3\neq x_1$ since otherwise we would have $x_2=\alpha+x_3=\alpha+x_1=x_0$.

Setting $x_5=\alpha+x_4=x_0+x_1+x_4$ we have $f(x_4)+f(x_5)=f(x_4)+f(x_0+x_1+x_4)=f(x_0)+f(x_1)=\beta$. We have $x_3\neq x_4$ since otherwise we would have $0=x_3+x_4=x_0+x_1+x_2+x_4$ which is not the case by hypothesis.

Finally $x_3\neq x_5$ since otherwise we would have $x_2=x_4$, and so all the six elements x_0,x_1,x_2,x_3,x_4,x_5 are different. □

We can now state a geometric characterization of differentially 4-uniform functions:

Theorem 3. *The differential uniformity of a function $f:\mathbb{F}_q\longrightarrow\mathbb{F}_q$ is not larger than 4 if and only if:*

$$X(\mathbb{F}_q)\subset V$$

where $X(\mathbb{F}_q)$ denotes the set of rational points over $\mathbb{F}_q$ of X.

Proof. The differential uniformity is not larger than 4 if and only if for any $\alpha\in\mathbb{F}_q^*$ and any $\beta\in\mathbb{F}_q$, the equation

$$f(x+\alpha)+f(x)=\beta$$

has at most 4 solutions, that is to say

$$\sharp\{x\in\mathbb{F}_q|f(x)+f(y)=\beta,\quad x+y=\alpha\}\leq 4.$$

But this is equivalent to saying that we cannot find 6 distinct elements x_0,x_1,x_2,x_3,x_4,x_5 in $\mathbb{F}_q$ such that

$$\begin{cases} x_0+x_1=\alpha, & f(x_0)+f(x_1)=\beta\\ x_2+x_3=\alpha, & f(x_2)+f(x_3)=\beta\\ x_4+x_5=\alpha, & f(x_4)+f(x_5)=\beta.\end{cases}$$

By the previous lemma, this is equivalent to saying that we cannot find 4 distinct elements x_0,x_1,x_2,x_4 in $\mathbb{F}_q$ such that $x_0+x_1+x_2+x_4\neq 0$ and such that

$$\begin{cases} f(x_0)+f(x_1)+f(x_2)+f(x_0+x_1+x_2)=0\\ f(x_0)+f(x_1)+f(x_4)+f(x_0+x_1+x_4)=0.\end{cases}$$

But this can be reformulated by saying that the rational points over $\mathbb{F}_q$ of the variety X are contained in the variety V, that is to say $X(\mathbb{F}_q)\subset V$.

□

3. Monomial functions with $\delta\leq 4$

If the function f is a monomial of degree $d>3$:

$$f(x)=x^d$$

then the polynomials $P_f(x,y,z)$ and $P_f(x,y,t)$ are homogeneous polynomials and we can consider the intersection X of the projective cones S_1 and S_2 of dimension 2 defined respectively by $P_f(x,y,z)=0$ and $P_f(x,y,t)=0$ with projective coordinates $(x:y:z:t)$ in the projective space $\mathbb{P}^3(\overline{\mathbb{F}}_q)$.

Even if X is now a projective algebraic subset of the projective space $\mathbb{P}^3(\overline{\mathbb{F}}_q)$, Theorem 3 tells us also that:

$$\delta(f)\leq 4 \ \text{ if and only if } \ X(\mathbb{F}_q)\subset V,$$

where V is the hypersurface of $\mathbb{P}^3(\overline{\mathbb{F}}_q)$ defined by Equation (1).

Indeed, the algebraic sets X and V in this section are closely related to but not equal to the sets X and V of the previous section. The set X of this section (resp. V) is the set of lines through the origin of the set X (resp. V) of the previous section which is invariant under homotheties with center the origin. For convenience, we keep the same notations.

LEMMA 4. *The projective algebraic set X has dimension 1, i.e. it is a projective curve.*

PROOF. We have to show that the projective surfaces S_1 and S_2 do not have common irreducible components. Since S_1 and S_2 are two cones, it is enough to prove that the vertex of one of the cones doesn't lie in the other cone. The coordinates of the vertex of the cone S_2 is $(0:0:1:0)$. To show that it doesn't lie in S_1, we will prove that $P_f(0:0:1:0)\neq 0$. Indeed, S_1 is defined by the polynomial

$$P_f(x,y,z)=\frac{x^d+y^d+z^d+(x+y+z)^d}{(x+y)(x+z)(y+z)}.$$

Setting $x+y=u$, we obtain:

$$P_f(x,y,z)=\frac{x^d+(x+u)^d+z^d+(u+z)^d}{u(x+z)(x+u+z)},$$

which gives

$$P_f(x,y,z)=\frac{x^{d-1}+z^{d-1}+uQ(x,z)}{(x+z)(x+u+z)},$$

where Q is some polynomial in x and z. This expression takes the value 1 at the point $(0:0:1:0)$. □

Now we know that X is a projective curve in $\mathbb{P}^3(\overline{\mathbb{F}}_q)$, and in order to estimate its number of rational points over $\mathbb{F}_q$, we must determine its irreducibility. We will prove that the curve C_7, defined as the intersection of S_2 with the projective plane H_7 of equation $x+y+z+t=0$, is an absolutely irreducible component of X, and hence that X is reducible.

PROPOSITION 5. *The intersection of the curve X with the plane H_7 with the equation $x+y+z+t=0$ is equal to the curve $C_7:=S_2\cap H_7$.*

PROOF. Since $X=S_1\cap S_2$, it is enough to prove that $C_7\subset S_1$. Since $t=x+y+z$ the points of intersection of the cone S_2 with the plane $x+y+z+t=0$

satisfy:

$$\begin{aligned} 0 = P_f(x,y,t) &= \frac{x^d + y^d + t^d + (x+y+t)^d}{(x+y)(x+t)(y+t)} \\ &= \frac{x^d + y^d + (x+y+z)^d + z^d}{(x+y)(y+z)(x+z)} \\ &= P_f(x,y,z), \end{aligned}$$

so they belong to S_1. □

PROPOSITION 6. *The projective plane curve C_7 is isomorphic to the projective plane curve C with equation*

$$P_f(x,y,z) = \frac{x^d + y^d + z^d + (x+y+z)^d}{(x+y)(x+z)(y+z)} = 0.$$

PROOF. The projection from the vertex of the cone S_1 defines an isomorphism of the projective plane H_7 with equation $x+y+z+t=0$ onto the plane with equation $t=0$, and it maps C_7 onto the curve C with equation $P_f(x,y,z)=0$. □

PROPOSITION 7. *Let $\mathcal{C}$ be a plane curve of degree $\deg(\mathcal{C})$ and which is not contained in V. Then:*

$$\sharp(\mathcal{C} \cap V)(\mathbb{F}_q) \leq 7\deg(\mathcal{C}).$$

PROOF. The variety V is the union of seven projective planes. Each plane cannot contain more than $\deg(\mathcal{C})$ points, therefore V contains at most $7\deg(\mathcal{C})$ rational points in $\mathcal{C}$. □

In order to get a lower bound for the number of rational points over $\mathbb{F}_q$ on the curve C, hence on the curve X, we need to know if C is absolutely irreducible or not. This question has been discussed by H. Janwa, G. McGuire and R. M. Wilson in [**14**] and very recently by F. Hernando and G. McGuire in [**10**].

PROPOSITION 8. *If $d = 2^r - 1$ with $r \geq 3$, then the projective curve X has an absolutely irreducible component C' defined over $\mathbb{F}_2$ in the plane $x+z+t=0$ and this component C' is isomorphic to the curve C.*

PROOF. One checks that the intersection of the cone S_1 with the plane $x+z+t=0$ is the same as the intersection of the cone S_2 with that plane. Hence one can show, as in Proposition 6, that the intersection of the curve X with the plane $x+z+t=0$ is isomorphic to the curve C. Furthermore, it is proved in [**14**] that the curve C is absolutely irreducible since, $\deg(C) = 2^r - 1 \equiv 3 \pmod 4$. □

Hence we can state

THEOREM 9. *Consider the function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ defined by $f(x) = x^d$ with $d = 2^r - 1$ and $r \geq 3$. If $5 \leq d < q^{1/4} + 4.6$, then f has differential uniformity strictly greater than 4.*

PROOF. The curve C' is an absolutely irreducible plane curve of arithmetic genus $\pi_{C'} = (d-4)(d-5)/2$. According to [**1**] (see also [**2**] for a more general statement), the number of rational points of the (possibly singular) absolutely irreducible curve C' satisfies

$$|\#C'(\mathbb{F}_q) - (q+1)| \leq 2\pi_{C'} q^{1/2}.$$

Hence

$$\#C'(\mathbb{F}_q) \geq q + 1 - 2\pi_{C'} q^{1/2}.$$

The maximum number of rational points on the curve C' on the surface V is $7(d-3)$ by Proposition 7. If $q+1-2\pi_C q^{1/2} > 7(d-3)$, then $C'(\mathbb{F}_q) \not\subset V$, therefore $X(\mathbb{F}_q) \not\subset V$, and $\delta(f) > 4$ by Theorem 3. But this condition is equivalent to

$$q - 2\pi_{C'} q^{1/2} - 7(d-3) + 1 > 0.$$

The condition is satisfied when

$$q^{1/2} > \pi_{C'} + \sqrt{7(d-3) - 1 + \pi_{C'}^2}$$

hence when

$$q \geq d^4 - 18d^3 + 121d^2 - 348d + 362$$

or

$$5 \leq d < q^{1/4} + 4.6.$$

□

4. Polynomials functions with $\delta \leq 4$

If the function f is a polynomial of one variable with coefficients in $\mathbb{F}_q$ of degree $d > 3$, we consider again as in section 3 the intersection X of S_1 and S_2, which are now cylinders in the affine space $\mathbb{A}^4(\overline{\mathbb{F}}_q)$ with equations respectively $P_f(x,y,z) = 0$ and $P_f(x,y,t) = 0$ and which are of dimension 3 as affine varieties.

Lemma 10. *The algebraic set X has dimension 2, i.e. it is an affine surface. Moreover, it has degree $(d-3)^2$.*

Proof. We have to show that the hypersurfaces S_1 and S_2 do not have a common irreducible component. Since these hypersurfaces are two cylinders, it is enough to prove that the polynomial defining S_1 does not vanish on the whole of a straight line (x_0, y_0, z, t_0) where x_0, y_0, t_0 are fixed and satisfy $P_f(x_0, y_0, t_0) = 0$. Indeed, S_1 is defined by the polynomial $P_f(x,y,z)$, which takes the value

$$P_f(x_0, y_0, z) = \frac{f(x_0) + f(y_0) + f(z) + f(x_0 + y_0 + z)}{(x_0 + y_0)(x_0 + z)(y_0 + z)}$$

at the point (x_0, y_0, z, t_0). If we set $x_0 + y_0 = s_0$, the homogeneous term of degree d_i in $P_f(x,y,z)$ becomes

$$\frac{d_i(x_0^{d_i - 1} + z^{d_i - 1}) + s_0 Q_i(x_0, z)}{(z + s_0 + x_0)(z + x_0)}$$

where Q_i is a polynomial in x_0 and z of degree $d_i - 2$. If d_i is odd, the numerator of this term is of degree $d_i - 2$, and hence does not vanish, so it is the same for the polynomial $P_f(x_0, y_0, z)$. Hence, X has dimension 2. Moreover, X is the intersection of two hypersurfaces of degree $d-3$, thus it has degree $(d-3)^2$. □

The surface X is reducible. Let $X = \bigcup_i X_i$ be its decomposition in absolutely irreducible components.

We embed the affine surface X into a projective space $\mathbb{P}^4(\overline{\mathbb{F}_q})$ with homogeneous coordinates $(x : y : z : t : u)$. Consider the hyperplane at infinity H_∞ defined by the equation $u = 0$ and let X_∞ be the intersection of the projective closure $\overline{X}$ of X with H_∞. Then X_∞ is the intersection of two surfaces in this hyperplane, which are respectively the intersections $S_{1,\infty}$ and $S_{2,\infty}$ of the cylinders S_1 and S_2 with that hyperplane. The homogeneous equations of $S_{1,\infty}$ and $S_{2,\infty}$ are

$$P_{x^d}(x,y,z) = \frac{x^d + y^d + z^d + (x+y+z)^d}{(x+y)(x+z)(y+z)}$$

and

$$P_{x^d}(x,y,t) = \frac{x^d + y^d + t^d + (x+y+t)^d}{(x+y)(x+t)(y+t)}.$$

By Proposition 8, the intersection of the curve X_∞ with the plane $x+z+t=0$ (inside the hyperplane at infinity) is an absolutely irreducible component C' of the curve X_∞ of multiplicity 1, defined over $\mathbb{F}_2$. So the only absolutely irreducible component of $\overline{X}$, say $\overline{X}_1$, which contains C' is defined over $\mathbb{F}_q$.

Proposition 11. *Let $\mathcal{X}$ be an absolutely irreducible projective surface of degree > 1. Then the maximum number of rational points on $\mathcal{X}$ which are contained in the hypersurface $\overline{V} \cup H_\infty$ is*

$$\sharp(\mathcal{X} \cap (\overline{V} \cup H_\infty)) \leq 8(\deg(\mathcal{X})q + 1).$$

Proof. As $\deg(\mathcal{X}) > 1$, the surface $\mathcal{X}$ is not contained in any hyperplane. Thus, a hyperplane section of $\mathcal{X}$ is a curve of degree $\deg(\mathcal{X})$. Using the bound on the maximum number of rational points on a general hypersurface of given degree proved by Serre in [**19**], we get the result. □

Theorem 12. *Let $q = 2^m$. Consider a function $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ of degree $d = 2^r - 1$ with $r \geq 3$. If $31 \leq d < q^{1/8} + 2$, then $\delta(f) > 4$. For $d < 31$, we get $\delta(f) > 4$ for $d = 7$ and $m \geq 22$ and also if $d = 15$ and $m \geq 30$.*

Proof. From an improvement of a result of S. Lang and A. Weil [**15**] proved by S. Ghorpade and G. Lachaud [**11**, section 11], we deduce

$$\begin{aligned} |\#\overline{X}_1(\mathbb{F}_q) - q^2 - q - 1| &\leq ((d-3)^2 - 1)((d-3)^2 - 2)q^{3/2} + 36(2d-3)^5 q \\ &\leq (d-3)^4 q^{3/2} + 36(2d-3)^5 q. \end{aligned}$$

Hence

$$\#\overline{X}_1(\mathbb{F}_q) \geq q^2 + q + 1 - (d-3)^4 q^{3/2} - 36(2d-3)^5 q.$$

Therefore, if

$$q^2 + q + 1 - (d-3)^4 q^{3/2} - 36(2d-3)^5 q > 8((d-3)q + 1),$$

then $\#\overline{X}(\mathbb{F}_q) \geq \#\overline{X}_1(\mathbb{F}_q) > 8((d-3)q+1)$, and hence $\overline{X}_1(\mathbb{F}_q) \not\subset \overline{V} \cup H_\infty$ by Proposition 11. As X is the set of affine points of the projective surface $\overline{X}$, we deduce that $X(\mathbb{F}_q) \not\subset V$ and so the differential uniformity of f is at least 6 from Theorem 3. This condition can be written

$$q - (d-3)^4 q^{1/2} - 36(2d-3)^5 - 8(d-3) > 0.$$

This condition is satisfied when

$$q^{1/2} > d^4 - 12d^3 + 54d^2 + 1044d + 5265 + 25920/d$$

if $d \geq 2$, or $d < q^{1/8} + 2$ if $d \geq 31$. □

References

[1] Y. Aubry and M. Perret, A Weil theorem for singular curves, *Arithmetic, Geometry and Coding Theory,* (Luminy, 1993), Walter de Gruyter, 1-7, Berlin - New-York 1996.

[2] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields, *Finite Fields and Their Applications*, 10 (2004), no. 3, 412-431.

[3] T.P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* 52 (2006), no. 9, 4160-4170.

[4] C. Bracken and G. Leander, New families of functions with differential uniformity of 4, to be published with the *proceedings of the workshop BFCA08*, Copenhague, 2008.

[5] C. Bracken and G. Leander, A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree, preprint, arXiv:0901.1824v1.

[6] L. Budaghyan, C. Carlet and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inform. Theory*, vol. 54, pp. 4218-4229, 2008.

[7] L. Budaghyan, C. Carlet and A. Pott, New constructions of almost perfect nonlinear and almost bent functions. *Proceedings of the Workshop on Coding and Cryptography* 2005, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.

[8] A. Canteaut, Differential cryptanalysis of Feistel ciphers and differentially δ-uniform mappings, *In Selected Areas on Cryptography*, SAC'97, pp. 172-184, Ottawa, Canada, 1997.

[9] C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[10] F. Hernando and G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, *arXiv:0903.2016v1*, [cs.IT] ; (math.AG), 11 march 2009.

[11] S. R. Ghorpade and G. Lachaud, Etale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, *Mosc. Math. J.*, 2 (2002), n. 3, 589-631.

[12] R. Harshorne, Algebraic geometry, Graduate Texts in Math., 52 (1977), Springer-Verlag.

[13] H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC-10 (G Cohen, T. Mora and O. Moreno Eds.)*, Lecture Notes in Computer Science, Vol. 673, Springer-Verlag, NewYork/Berlin 1993.

[14] H. Janwa, G. McGuire and R. M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2), *Applied J. of Algebra*, 178, 665-676 (1995).

[15] S. Lang and A. Weil, Number of points of varieties in finite fields, *Amer. J. Math.* 76, (1954), pp. 819-827.

[16] K. Nyberg, Differentially uniform mappings for cryptography, *Advances in cryptology—Eurocrypt '93* (Lofthus, 1993), 55–64, Lecture Notes in Comput. Sci., n° 765, Springer, Berlin, 1994.

[17] F. Rodier, Bornes sur le degré des polynômes presque parfaitement non-linéaires, *Contemporary Math.*, Vol. 487, 169-181 2009); *arXiv:math/0605232v3* [math.AG], 2 may 2008.

[18] F. Rodier, Bounds on the degrees of APN polynomials, to be published with the proceedings of the workshop BFCA08, Copenhague, 2008.

[19] J. -P. Serre, Lettre à M. Tsfasman, *Astérisque* 198-199-200 (1991), 351-353.

[20] J. F. Voloch, Symmetric cryptography and algebraic curves, *Algebraic Geometry and its Applications*, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 135-141 (2008).

Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France, and, Institut de Mathématiques de Luminy, Marseille, France

E-mail address: yves.aubry@univ-tln.fr and rodier@iml.univ-mrs.fr