On the Non-linearity of Power Functions

Philippe Langevin, Pascal Véron

Designs, Codes and Cryptography, 37, 31–43, 2005

On the Non-linearity of Power Functions

PHILIPPE LANGEVIN langevin@univ-tln.fr
GRIM, Université de Toulon, France

PASCAL VÉRON veron@univ-tln.fr
GRIM, Université de Toulon, France

Communicated by: A. Pott

Received January 31, 2003; Revised April 20, 2004; Accepted June 30, 2004

Abstract. We study the Boolean functions arising from power functions by means of Stickelberger's congruences on Gauss sum. We obtain a new criterion for high non-linearity of such boolean functions in terms of permutation polynomials. Finally, a new characteristic property of Gold exponents is given.

Keywords: Gauss sums, Boolean funcitons

AMS Classification: 06E30

1. Non-Linearity

Let L be a finite field of order $q := 2^m$. Let μ be the canonical additive character of L mapping $x \in L$ to $\mu(x) = (-1)^{\mathrm{Tr}_L(x)}$, where Tr_L is the absolute trace form of L. The *Fourier coefficient* of a polynomial $f \in L[X]$ at the point $a \in L$ is defined by

$$\widehat{f}(a) = \sum_{x \in L} \mu\big(f(x) + ax\big).$$

It is also the *Walsh coefficient* of the Boolean function $x \mapsto \mathrm{Tr}_L\big(f(x)\big)$. The Hamming distance between this *Boolean function corresponding* to f, and the linear form $x \mapsto \mathrm{Tr}_L(ax)$ is equal to $(q - \widehat{f}(a))/2$. The minimal distance between $\mathrm{Tr}_L \circ f$ and the set of all affine functions from L into $\mathbf{F}_2$ is called the *nonlinearity* of f. The nonlinearity of f, usually denoted by $\mathrm{NL}(f)$, is given by

$$\mathrm{NL}(f) = 2^{m-1} - \frac{1}{2}\,\mathrm{R}(f), \tag{1}$$

where $\mathrm{R}(f) := \sup_{a \in \mathbf{F}_2^m} |\widehat{f}(a)|$ is the *spectral amplitude* of f. Several interesting problems and conjectures arise from the study of non-linearity of polynomials and more specially in the case of monomials also called power functions. Questions that come from different frameworks: cyclic codes with two zeroes, correlation of sequences, Boolean functions and graphs theory [9]. See [2] for a complete list of references. Most of the papers about the nonlinearity of monomial use McEliece's theorem [10,27] on the divisibility of weights of cyclic codes. The main goal of that

paper consists in applying directly Stickelberger's congruences on Gauss sums [33] to explore the nonlinearity of power functions.

2. Cryptographic Parameters

In their article on cryptanalysis and Boolean functions [7], Chabaud and Vaudenay define two important parameters that measure the resistance of polynomials against two sort of attacks.

Following [7], for all $(a, b) \in L^2$, we denote by $\lambda_f(a, b)$ the Fourier coefficient of the polynomial $b f(x)$. The first parameter measures the resistance against the *linear cryptanalysis*, it is defined by $\Lambda(f) = \sup_{a,b \neq 0} \lambda_f(a, b)$. The best resistance is achieved by the polynomials that minimize Λ. Note that if f is a permutation of L then $\Lambda(f)$ is nothing other than the spectral amplitude of f. Let γ be a primitive root of L and let τ be an integer. The Fourier coefficient of bf at γ^τ is nothing other than the τ-th crosscorrelation coefficient (up to unity) between the sequences $\left[\mu\left(bf(\gamma^i)\right)\right]_{i=0}^{q-1}$ and $\left[\mu(\gamma^i)\right]_{i=0}^{q-1}$. It follows from an old result by Sidelnikov [32] that

$$\Lambda(f)^2 \geq 2q. \tag{2}$$

If the equality occurs then the degree of L over $\mathbf{F}_2$ is necessarily odd and the spectrum of f is composed of the three values: $-\sqrt{2q}$, 0, and $+\sqrt{2q}$. In that case, the function is said to be *almost bent* (AB-property).

For all $(u, v) \in L^2$, let $\delta_f(u, v)$ be the number of solutions of the equation $f(x + u) + f(x) = v$. The second parameter, defined by $\Delta(f) := \sup_{(u,v) \in L^\times \times L} \delta_f(u, v)$, measures the resistance of f against the *differential cryptanalysis*. Clearly,

$$\Delta(f) \geq 2. \tag{3}$$

The best resistance is achieved by the polynomials satisfying $\Delta(f) = 2$. In that case, the polynomial is said *almost perfect nonlinear* (APN-property).

The next identity comes from Fourier analysis. It provides a link between these two notions.

$$\sum_{a,b \in L} \lambda_f(a, b)^4 = q^2 \sum_{u,v \in L} \delta_f(u, v)^2. \tag{4}$$

Proof. Sketch.

$$\begin{aligned}\sum_{a,b \in L} \lambda_f(a, b)^4 &= q \sum_{b \in L} \sum_{x+y+z+t=0} \mu\left(bf(x) + bf(y) + bf(z) + bf(t)\right) \\ &= q^2 \sum_{\substack{x+y+z+t=0 \\ f(x)+f(y)+f(z)+f(t)=0}} 1 \quad = q^2 \sum_{u,v \in L} \delta_f(u, v)^2.\end{aligned}$$

■

All these notions are simplified in the context of power functions $x \mapsto x^s$, and still more when s is prime to $q-1$. In all the case, the unsolved main problems come from the natural questions: what is the spectral amplitude, say $L(s,q)$ of the power function $x \mapsto x^s$ over the field of order q? What is the minimal value $L(q)$ of the $L(s,q)$? What are the *good exponents* s such that $L(s,q) = L(q)$?

3. Power Functions

Let s be a positive integer, $1 \le s \le q-2$. The Fröbenius automorphism of L shows that the spectrum of x^s, as well as the APN-character of s, do not depend on the cyclotomic class of s modulo $q-1$.

$$s' \sim s \Longleftrightarrow \exists j, \quad s' = 2^j s \pmod{q-1}.$$

The inversion does not change the character APN of an invertible exponent. We says that two (invertible) exponents s' and s are equivalents if $s' \sim s$ or $s' \sim s^{-1}$. Let us denote by $\mathrm{wt}(s)$ the numbers of bits equal to 1 in the binary expansion of s. It is well known that the degree of the Boolean function corresponding to x^s is less or equal to $\mathrm{wt}(s)$, see e.g [5]. More precisely, if $r_1, r_2, \ldots, r_w$ are the positions of nonzeroes bits of s i.e. $s = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_w}$, the algebraic normal form of $\mathrm{Tr}_L \circ x^s$ in an arbitrary normal basis $(b_1, b_2, \ldots, b_m)$ of L is

$$f(x_1, x_2, \ldots, x_m) = \sum_{i_1, i_2, \ldots, i_w} x_{i_1} x_{i_2}, \ldots, x_{i_w} \mathrm{Tr}_L(b_{i_1 \oplus r_1} b_{i_2 \oplus r_2}, \ldots, b_{i_w \oplus r_w}), \tag{5}$$

where $\oplus$ is the addition modulo m.

In general, the degree of a Boolean function whose all the Walsh coefficients are all divisible by 2^v has degree less or equal to $m - v + 1$, see e.g. [5], one can even say a little bit more [26]. Thus, the weight of an exponent s satisfying the AB-property must be less or equal to $(m+1)/2$. We will see in Lemma 2 that an AB-exponent is necessarily invertible, and thus must satisfy a pair of inequalities

$$\mathrm{wt}(s) \le \frac{m+1}{2}, \quad \text{and} \quad \mathrm{wt}(1/s) \le \frac{m+1}{2}.$$

The group $(\mathbf{Z}/m\mathbf{Z})^*$ acts also over the set of exponents. The action of λ (prime to m) on the exponent s is defined by:

$$s^{(\lambda)} = \sum_{i=1}^{w} 2^{\lambda r_i}. \tag{6}$$

It is easy to see that the quadratic part of the Boolean functions associated to the exponents s and $s^{(\lambda)}$ are equivalents under the action of the general linear group of $\mathrm{GL}_m(\mathbf{F}_2)$. Often, the spectrums of s and $s^{(\lambda)}$ are the same, but, it seems difficult to say more between the nonlinearity of s and $s^{(\lambda)}$.

4. Quadratic Forms

Let Q be a quadratic form of the $\mathbf{F}_2$-space L. By definition, there exists a bilinear symmetric form ϕ such that:

$$\forall x, y \in L, \quad Q(x+y) = Q(x) + Q(y) + \phi(x, y). \tag{7}$$

One reduces the study of Q to that of its *kernel* K (or *radical*) i.e. The orthogonal space of L with respect of ϕ, defined by

$$K := \{y \in L \mid \forall x \in L, \quad \phi(x, y) = 0\}.$$

Let us recall that Q is linear over K and also that the bilinear form ϕ is a symplectic form, that is $\phi(x, x) = 0$, for all $x \in L$. The square of the character sum $\Sigma := \sum_{x \in L} (-1)^{Q(x)}$ depends essentially on the dimension, say k, of the kernel of Q.

$$\begin{aligned}\Sigma^2 &= \sum_{x \in L} (-1)^{Q(x)} \sum_{y \in L} (-1)^{Q(y)} = \sum_{x, y \in L} (-1)^{Q(x)+Q(y)} \\ &= \sum_{x, y \in L} (-1)^{Q(x+y)+\phi(x,y)} = \sum_{x, z \in L} (-1)^{Q(z)+\phi(x,z)} \\ &= q \sum_{z \in K} (-1)^{Q(z)}.\end{aligned}$$

Hence, the later square is equal to zero or $\pm 2^{(m+k)/2}$ according to whether Q is defective or not. In the classical terminology [12], Q is defective if its restriction to K is not identically equal to 0.

4.1. Gold Exponents

The spectrum of the quadratic form corresponding to the exponent $2^r + 1$ have been determined by Gold [17] in the context of M-sequences. Let us consider the *Gold exponent* $s = 2^r + 1$. The power function x^s is APN if and only if $(r, m) = 1$. More precisely, see [29],

$$\Delta(x^{2^r+1}) = 2^{(r,m)}.$$

For any $a \in L$, the Boolean function $Q_a : x \mapsto \mathrm{Tr}_L(x^s + ax)$ is a quadratic form whose the symplectic form is

$$\phi(x, y) = \mathrm{Tr}_L\left(x^{2^r} y + x y^{2^r}\right),$$

since the bilinear form $(x, y) \mapsto \mathrm{Tr}_L(xy)$ is not degenerate, the orthogonal space of L with respect to ϕ is equal to $K := \{x \mid x^{2^r} + x^{2^{-r}} = 0\}$, which is nothing but the intermediate field of dimension $(2r, m)$. It follows from the calculation of the above section that the spectral amplitude of the power function x^s is equal to $2^{(m+(2r,m))/2}$.

4.2. Kasami Exponents

Kasami calculated the spectrum of an exponent of the form $2^{2r}-2^r+1$ in the context of codes [21]. The links between the exponents of Kasami and the theory of the quadratic forms was highlighted by Dobbertin in [16]. Let us assume $(r,m)=1$. The starting trick consists in the use of change of variables $x \leftarrow x^{2^r+1}$ in the calculation of the Fourier coefficient of $x^{2^{2r}-2^r+1}$:

$$\sum_{x\in L} \mu\left(x^{2^{2r}-2^r+1}+ax\right)=\sum_{x\in L} \mu\left(x^{2^{3r}+1}+ax^{2^r+1}\right) \tag{8}$$

The dimension of the kernel of the quadratic form $x \mapsto \mathrm{Tr}_L(x^{2^{3r}+1}+ax^{2^r+1})$ may be greater than 1. But, in that case, the the quadratic form is defective [13], thus, the Fourier coefficient is equal to zero.

5. The Odd Case

From the above sections,

$$\sqrt{2q} \le L(q) \le 2\sqrt{q},$$

with equality on the left hand side in the case of L has an odd dimension. On the other side, one does not know the true value of $L(q)$ when the dimension of L is even. Several conjectures are still open [3,19,30], one of the most famous (Welch's conjecture) claims the equality on the right hand side, see [31]. Thus, the odd case is easier than the even one in the sense that we know the true value of $L(q)=\sqrt{2q}$. The problem consists in finding the set of all the good exponents.

LEMMA 1. *In odd case, a power APN function is one-to-one.*

Proof. Following a very simple but elegant argument due to Dobbertin. If s is not prime with $q-1$ then there exists $x \neq 1$ in L such that $x^s=1$ that verifies

$$\left(\frac{x}{x+1}\right)^s+\left(\frac{1}{x+1}\right)^s=0=\left(\frac{x^2}{x^2+1}\right)^s+\left(\frac{1}{x^2+1}\right)^s,$$

and APN property would imply one of the two quadratic relations $x=x^2$ or $x^2+x+1=0$ which is absurd since the degree of L is odd. ∎

At the end of the Sixties, Golomb mentioned a conjecture of Welch concerning the crosscorrelation function of binary M-sequences. In our context this conjecture claims that the spectrum of the monomial with exponent

$$2^{(m-1)/2}+3, \quad \text{(Welch exponent)} \tag{9}$$

is composed of three values $\{-\sqrt{2q}, 0, +\sqrt{2q}\}$.

The proof of the Welch's conjecture was made about 30 years later by Canteaut, Charpin and Dobbertin. The starting point is the next proposition. In general, all the Fourier coefficients of a polynomial are even integers. We say that f is r-divisible if the dyadic valuation of the Fourier coefficients of f are greater or equal to r.

PROPOSITION 5.1. *A polynomial has the AB-property iff it has the APN-property and is* $(m+1)/2$*-divisible.*

It is a consequence of identity (4), see [2].

In [8] Cusick and Dobbertin prove the APN-property of the exponent (9). In [2], Charpin, Canteaut and Dobbertin use McEliece's theorem to prove that the $(m+1)/2$-divisibility of this exponent. The proof is rather technical. All together with Proposition 51, show that the Welch expoenent is good.

PROBLEM 1. *The boolean function associated to the Welch exponent has degree* 3. *Find a new proof using the "theory" of cubic forms.*

Let r be the residue such that $4r \equiv -1 \pmod{m}$. At the beginning of the Seventies, Niho conjectured the exponent of the form

$$2^{2r} + 2^r - 1. \tag{10}$$

In [8], Cusik and Dobbertin proved the APN-property of the Niho exponent. It is a good exponent since the divisibility by $\sqrt{2q}$ of the Fourier coefficients has been obtained by Hollmann and Xiang in [20]. Their method is relatively powerful but, once again the proof remains very technical.

Recently, Bringer pointed us out that the trick used by Dobbertin in the case of Kasami exponents applies also in the Niho case. Indeed, by the change of variables $x \longrightarrow x^{2^{2r+1}+2^r+1}$, a cubic form appears in the calculation of the Fourier coefficient Table 1:

$$\sum_{x \in L} \mu(x^{2^{2r}+2^r-1} + ax) = \sum_{x \in L} \mu(x^3 + ax^{2^{2r+1}+2^r+1})$$

As we see, Problem (1) suggests a new proof for the Niho exponent.

The exponents presented in the precedings sections forms a list, see Table 1, of at most $\phi(m)+1$ distinct classes, and the main conjecture is

Table 1. Known good exponents m odd.

Type	s	Condition
Gold	$2^r + 1$	$(r, m) = 1)$
Kasami	$2^{2r} - 2^r + 1$	$(r, m) = 1)$
Welch	$2^{(m-1)/2} + 3$	
Niho	$2^{2r} + 2^r - 1$	$4r \equiv -1 \mod m$

Conjecture 5.1. (Dobbertin). *If s is a good exponent then s has Gold, Kasami, Welch or Niho type.*

6. Application of Stickelberger's Congruences

In the next section, we will use Gauss sums and Stickelberger theorem to analyze the nonlinearity of power functions. Elementary properties of the cyclotomic fields are the main tools, we suggest the references [23] (french) or [25]. We begin by a concrete realization of L has the quotient ring $\mathbf{Z}[\xi]/\wp$, where ξ is the principal $(q-1)$-root of the unity in the field of complex numbers and $\wp$ one of the prime ideal of $\mathbf{Z}[\xi]$ containing 2. It follows that the maps which sends the class of ξ^j on ξ^j defines a multiplicative character of L of order $q-1$. It is the *Teichmüller character* of L, we denote it ω.

By definition,

$$\forall a \in L = Z[\xi]/\wp, \quad a = \omega(a) \mod \wp.$$

Any multiplicative characters of L is a power of ω and a famous theorem of Stickelberger gives a $\wp$-adic estimation of the Gauss sum

$$G_L(\chi) = \sum_{x \in L^\times} \chi(x)\mu(x).$$

THEOREM 6.1. (congruences of Stickelberger). *For any positive integer j the Gauss sum $G_L(\bar{\omega}^j, \mu_L)$ is congruent to $2^{S(j)}$ modulo $\wp^{S(j)+1}$, where $S(j)$ is the sum of the bits of $j \mod n$.*

Let s be an exponent. We use the inversion formula,

$$\mu(z) = \frac{1}{q-1} \sum_{\chi \in \widehat{L^\times}} G_L(\chi)\bar{\chi}(z),$$

to express the Fourier coefficients of the power function $f(x) = x^s$.

$$\begin{aligned}
\widehat{f}(a) &= \sum_{x \in L} \mu_L(x^s + ax) \\
&= 1 + \frac{1}{(q-1)^2} \sum_{x \in L^\times} \sum_{\chi \in \widehat{L^\times}} \sum_{\psi \in \widehat{L^\times}} G_L(\chi)G_L(\psi)\bar{\chi}^s(x)\bar{\psi}(ax) \\
&= \frac{q}{q-1} + \frac{1}{q-1} \sum_{1 \neq \chi \in \widehat{L^\times}} G_L(\chi)G_L(\bar{\chi}^s)\chi^s(a).
\end{aligned}$$

The congruences of Stickelberger show the importance of the distribution of the $V(j) = S(js) + S(-j)$ when j ranges $[0, q-2]$. Let us consider the following notations

Table 2. A numerical example ($m=7$).

s	Type	$1/s$	2	3	4	5	6	7	J
1		1						126	All
3	Gold[1], Kasami[1]	43			7	14	28	28	1
5	Gold[2]	27			7	21	28	14	1
7		55		7		14	35	14	1
9	Gold[3]	15			7	28	21	14	1
11	Welch, Kasami[2]	13			7	28	7	42	9
19		47		7		21	28	14	1
21	Niho	31		7	7	14	21	28	1
23	Kasami[3]	29			21		28	28	1 3 13
63		63	7		21		35		1

$$\nu_s = \min_{1\le j\le q-2} V(j), \quad J_s = \{j \mid V(j)=\nu_s\}, \quad P_s(X) = \sum_{j\in J_s} X^j \in \mathbf{F}_2[X].$$

Remark that since S is invariant under multiplication by 2, then J_s is an union of cyclotomic class modulo $q-1$, as a mapping L over $\mathbf{F}_2$, $P_s(X)$ is an idempotent. In particular, since the dimension of L is odd, we can write $P_s(X) = \mathrm{Tr}_L \circ Q_s(X)$ where $Q_s(X)$ is obtained choosing the minimal representant of each cyclotomic class contained in J_s. See the numerical illustration, Table 2.

PROPOSITION 6.1. *The power function x^s is ν_s-divisible but not more. Moreover, $\widehat{f}(a) \equiv 0 \mod 2^{1+\nu_s}$ if and only if $P_s(a^s)=0$.*

Proof. From Stickelberger theorem,

$$\widehat{f}(a) = 2^{\nu_s}\left[\sum_{j\in J_s} \omega^{js}(a)\right] \pmod{\wp^{1+\nu_s}}$$

Note that $\sum_{j\in J_s} \omega^{js}(a) \equiv P_s(a^s) \pmod{\wp}$. Hence, all the Fourier coefficients have a dyadic valuation greater or equal to ν_s. Since the idempotent $P_s(X^s)$ is not the null polynomial, there exists an element $a\in L$ such that $P_s(a^s)\neq 0$, and the corresponding Fourier coefficient is not divisible by $2^{1+\nu_s}$. ■

Up to now, we do not know any counter-example to the following conjecture.

Conjecture 6.1. If s is invertible modulo $q-1$. The spectrum of x^s contains two Fourier coefficients of dyadic valuation ν_s with distinct signe.

It is not easy to find the J-set of an exponent.

PROPOSITION 6.2. *If s is a Gold exponent the J_s is equal to the cyclotomic class of $-1/j$.*

Proof. Let $s=2^k+1$ be a Gold exponent, and let us consider the power function $f(x)=x^s$. From Section (4.1), the kernel of the quadratic form $x \mapsto \mathrm{Tr}_L(x^s+ax)$ is equal to $\{0,1\}$ whence

$$\mathrm{Tr}_L(a)=0 \Leftrightarrow \hat{f}(a)=0 \Leftrightarrow P_s(a^s)=0.$$

Since $\mathrm{Tr}_L(x)$ and $P_s(x^s)$ are idempotents, we get an equality of polynomials which implies that J_s is equal to the cyclotomic class of $-1/s$. ■

LEMMA 2. *If the power function x^s is $(m+1)/2$-divisible then s is invertible.*

Proof.. If s is not invertible then there exists $z \neq 0$ such that $sz=0$. It follows $S(z) \geq (m+1)/2$ and $S(-z) \geq (m+1)/2$ that is absurd since $S(j)+S(-j)=m$ for all non zero j. ■

THEOREM 6.2. *Let s be an integer. If $v_s=(m+1)/2$ and $P_s(X)$ has 2^{m-1} roots in L then s is a good exponent.*

Proof. Let $f(x)=x^s$. Let $z(a)$ be the integer such that $\widehat{f}(a)=z(a)2^{(m+1)/2}$. Using Parseval identity, we know that $\sum_{a\in L} z(a)^2=2^{m-1}$, since half of the $z(a)$'s are odd, we deduce they are equal to ± 1 and the other are 0. ■

COROLLARY 6.1. *Let s be an exponent such that $v_s=(m+1)/2$. If $Q_s(X)$ is a permutation polynomial of L then s is a good exponent or (equivalently) $x \mapsto x^s$ is AB.*

Initialy the above corollary was design to disprove the Dobbertin's conjecture since it gives a strategy to eventually find new good exponents. Indeed, it suffices (for example) to look for exponents s of weight less or equal to $(m+1)/2$ among those having a J-set reduced to a single cyclotomic class. Unfortunately, we do not find new good exponents in that way up to $m=39$. The Table 3 lists all the good exponents whose the J-set reduces to one cyclotomic class, but not being Gold type. We finish this paper with a nice characterization of Gold exponent in term of J-set.

THEOREM 6.3. *Let s be an integer coprime with $q-1$. The exponent s lies in Gold class if and only if $v_s=(m+1)/2$ and J_s is equal to the cyclotomic class of $1/s$.*

Proof. As we saw before, the condition is necessary. Conversely, if $v_s=(m+1)/2$ and J_s reduces to the cyclotomic class of $1/s$ then the Fourier transform of f is identically equal to zero over the hyper-plane $H=\{a \mid \mathrm{Tr}_L(a)=0\}$. The orthogonal of H with respect to the bilinear form $(x,y) \mapsto \mathrm{Tr}_L(xy)$ is $\mathbf{F}_2$. Using the Poisson summation formula, we get

$$0=\frac{1}{2^{m-1}}\sum_{a\in H}\hat{f}(a)\mu(az)=\mu\big(f(z)\big)+\mu\big(f(z+1)\big),$$

Table 3. All the Good exponents whose the J-set reduces to a single cyclotomic class, not being of the Gold type ($5 \le m \le 39$).

m	s	$1/s$	j	type
5				
7	11	104	9	K W
9	–	–	–	
13	171	7712	1189	K
11	43	1809	293	K
15	–	–	–	
17	683	127041	21141	K
19	2731	516224	84629	K
21	–	–	–	
23	10923	8323329	1387093	K
25	43691	33423872	5548629	K
27	–	–	–	
29	174763	535823361	89303381	K
31	699051	2145388544	357214549	K
33	–	–	–	
35	2796203	4278194177	1428858197	K
37	11184811	4261421056	1420469589	K
39	–	–	–	

whence

$$\mathrm{Tr}_L\left((x+1)^s + x^s\right) = 1$$

but it is possible if and only if the binary weight of s is 2, as we prove in the lemma below. ■

LEMMA 3. *Let L be the Galois field of even order q. Let $0 < s < q-1$ be an integer coprime with $q-1$. If the Boolean function $x \mapsto \mathrm{Tr}_L\left((x+1)^s + x^s\right)$ is constant equal to 1 then the degree of L is odd and the binary weight of s is 2.*

Proof. The degree m of L is odd since $\mathrm{Tr}_L(1) = 1$. Without a loss of generality, we may assume s odd and we denote by w the binary weight of s. We have to prove that $w = 2$. Let us use the binary expansion to identify the integers of the interval $[0, 2^m - 1]$ with the subsets of $\{0, 1, \ldots, m-1\}$ mapping the integer $k = \sum_{i=0}^{m-1} k_i 2^i$ on its support

$$\mathrm{supp}\,(k) = \{i \mid k_i = 1\}.$$

We say that $k \subseteq l$ if and only if the support of k is included in that of l. A well known relation of E. Lucas asserts that $k \subseteq l$ if and only if the binomial coefficient $\binom{l}{k}$ is congruent to 1 modulo 2. Let R be a set of representatives of the cyclotomic

classes modulo $q-1$. By means of Lucas relation,

$$\mathrm{Tr}_L\big((x+1)^s\big)=\sum_{k=0}^{s}\binom{s}{k}\mathrm{Tr}_L(x^k)=\sum_{r\in R}\underbrace{\sum_{k\sim r}\binom{s}{k}}_{C(r)}\mathrm{Tr}_L(x^r),$$

where $C(r)$ is the cardinality of the set $\{x \mid x\sim r, \quad x\subseteq s\}$. Clearly, $C(0)=C(s)=1$ and $C(1)=w$. The linear independence of the Boolean functions $x\mapsto \mathrm{Tr}_L(x^r)$, r varying in R, in conjunction with the equality $\mathrm{Tr}_L\big((x+1)^s+x^s\big)=1$ implies that $C(r)\equiv 0 \pmod 2$, for all $r\in R/\{0,s\}$. In particular, w must be even.

Let y be an integer of weight $w-1$ "included" in s, since $C(y)\equiv 0 \pmod 2$, there exists a shift x of y, such that $x\neq y$ and $x\subseteq s$. Let t be the smallest integer such that $y\equiv 2^t x \pmod{q-1}$, and let us denote by τ the translation $i\mapsto i\oplus t$.

The intersection $Z:=\mathrm{supp}\,(k)\cap\mathrm{supp}\,(l)$ contains $w-2$. We denote by a and b be the integers such that $\mathrm{supp}\,(x)=Z\cup\{a\}$ and $\mathrm{supp}\,(y)=Z\cup\{b\}$. The translation τ induces a one-to-one mapping from $Z\cup\{a\}$ onto $Z\cup\{b\}$ and we can construct a sequence $z_1:=b$, z_2, $\ldots$, $z_r=a$ such that $z_{i-1}=z_i\oplus t$ for all $2\le i\le r$. Let J be the complement of $\{z_1,z_2,\ldots,z_r\}$ with respect to $\mathrm{supp}\,(s)$. We have obtained the decomposition:

$$s=\sum_{i=0}^{r-1}2^{a+it}+\sum_{j\in J}2^j.$$

Moreover, since J is invariant under τ the product $(2^t-1)\sum_{j\in J}2^j$ is equal to zero modulo $q-1$. For a similar reason, since s is not a zero divisor modulo $q-1$, the set $\{z_0,z_1,\ldots,z_r\}$ is not a cycle under τ that is $b\oplus t\neq a$. They are r shifts of 2^a+2^{a+t} included in $\sum_{i=1}^{r}2^{z_i}$. On an other hand, by cyclicity, J contains $|J|$ other shifts.

$$C(2^a+2^{a+t})=r-1+|J|=w-1.$$

Now, the parity of w implies $s=2^a+2^{a+t}$. ■

7. Notations

Sec.	Symbols	Definition	
1	m	a positive integers, mostly odd.	
	L, q	L the field of order $q=2^m$.	
	μ	additive character.	$\mu(x)=(-1)^{\mathrm{Tr}_L(x)}$.
	Tr_L	absolute trace of L over $\mathbf{F}_2$.	
	$f(X)$	a polynomial in $L[X]$.	
	$\widehat{f}(a)$	Fourier coefficient of f at a.	$\sum_{x\in L}\mu\big(f(x)+a.x\big)$.
	$R(f)$	spectral amplitude of f	$\sup_{a\in\mathbf{F}_2^m}\lvert\widehat{f}(a)\rvert$.
	$\mathrm{NL}(f)$	nonlinearity.	
2	$\lambda_f(a,b)$	Fourier coefficient of $bf(X)$.	

	$\Lambda(f)$	$\sup_{a,b\neq 0} \lambda_f(a,b)$.	
	$\delta_f(u,v)$	number of $x \in L$ such that $f(X+u)+f(X)=v$.	
	$\Delta(f)$	$\sup_{u\neq 0,v} \delta_f(u,v)$.	
	s	an exponent.	$0 \leq s \leq q-1$
	$L(s,q)$	spectral amplitude of x^s over L.	
	$L(q)$	$\sup_s L(s,q)$.	
3	(x,y)	GCD of the integers x and y.	
	$i \oplus j$	addition modulo m.	
	$s' \sim s$	cyclotomic equivalence	$\exists j, \quad s' \equiv 2^j s \pmod{q-1}$.
	$\mathrm{wt}(s)$	binary weight of s.	
6	ξ	principal $(q-1)$-root of unity.	$\exp(2i\pi/(q-1))$
	$\wp$	a prime above 2 in $\mathbf{Q}(\xi)$.	
	ω	Teichmüller character defined by $\wp$.	
	$S(j)$	$\mathrm{wt}(j \mod q-1)$.	
	χ	multiplicative character.	
	$G_L(\chi)$	Gauss sum.	
	ν_s	$\min_j S(-j)+S(js)$.	
	J_s	the set $\{j \mid S(-j)+S(js)=\nu_s\}$.	
	$P_s(X)$	the idempotent $\sum_{j\in J_s} X^j$.	

Acknowledgment

Most of the ideas exposed in this paper were obtained during our visit to the university of Saint-Louis in Senegal. A stay on the initiative of Mary Teuw Niane and Oumar Mbodj. We are grateful for the hospitality we received there.

References

1. J. Ax, Zeroes of polynomials over finite fields. *Am. J. Math.*, Vol. 86 (1964) pp. 256–261.
2. A. Canteaut, P. Charpin and P. H. Dobbertin, Binary M-sequences with three-valued crosscorrelation: a proof of the Welch conjecture. *IEEE trans. IT.*, Vol. 46, No. 1 (2000) pp. 4–8.
3. A. Canteaut, P. Charpin and H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions and crosscorrelation of maximum-length sequences. *SIAM J. Discrete Math.*, Vol. 13 (2000) pp. 105–138.
4. W.-C. W. Li, B. Poonen and A. R. Calderbank, A 2-adic approach to the analysis of cyclic codes. *IEEE trans. Inf. Th.*, Vol. 43, No. 3 (1997) pp. 977–986.
5. Claude Carlet Codes de Reed-Muller, codes de Kerdock et de Preparata Phd thesis, Paris VI, 1990.
6. A. R. Calderbank and G. McGuire, Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences. *IEEE trans. Inf. Theory*, Vol. 41, No. 4 (1995) pp. 1153–1155.
7. F. Chabaud and S. Vaudenay, Links between diffrential and linear cryptanalysis. *Eurocrypt 94*, Vol. 950 (1994) pp. 356–365.
8. T. Cusick and H. Dobbertin, Some new 3-valued crosscorrelation functions of binary m-sequences. *IEEE Trans. Inf. Theory*, Vol. 42 (1996) pp. 1238–1240.
9. E. R. van Dam and D. Fon-Der-Flaass, Codes, Graphs and schemes from nonlinear functions. *preprint*, 2000.
10. P. Delsarte, Weight of p-ary Abelian codes. *Philips Res. Rep.*, Vol. 26 (1971) pp. 145–153.
11. P. Delsarte et and R. J. McEliece, Zeros of functions in finite abelian group algebras. *Am. J. Math.*, Vol. 98, (1976) pp. 197–224.

12. J. Dieudonné, *La Géométrie Des Groupes* Classiques, Springer-Verlag (1971).
13. H. Dobbertin, One-to-one highly nonlinear power functions on finite fields. *AAECC*, Vol 9, No. 2 (1998) pp. 139–152.
14. H. Dobbertin, Almost Perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Trans. Inf. Theory*, Vol. 45 (1999) pp. 1271–1275.
15. H. Dobbertin, Almost Perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Inf. Comput.*, Vol. 151 (1999) pp. 57–72.
16. H. Dobbertin, Another Proof of Kasami's Theorem. *Des. Codes Crypt.*, Vol. 11–13 (1999) pp. 177–180.
17. R. Gold, Optimal binary sequences for spread spectrum multiplexing. *IEEE* Vol. IT-13 (1967) pp. 619–621.
18. R. Gold, Maximal recursive sequences with 3-valued crosscorrelation functions. *IEEE trans. Inf. Theory*, Vol. 14 (1968) pp. 154–156.
19. Tor Helleseth, Some results about the crosscorrelation function between two maximal linear sequences. *Discrete Math.*, Vol. 16 (1976) pp. 209–232.
20. H. D. L. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences *Finite Fields th. Appl.*, Vol. 7 (2001) pp. 253–287.
21. T. Kasami, The weight enumerators for several classes of subcodes of the 2-nd Reed-Muller codes. *Inf. Control*, Vol. 18 (1971) pp. 369–394.
22. L. Carlitz and S. Uchiyama, Bounds for exponential sums. *Duke Math.*, Vol. 24 (1957) pp. 37–41.
23. J. R. Joly, Equations et variétés algébriques sur un corps fini. *L'enseignement mathématique*, Vol. xix (1974).
24. G. Lachaud and J. Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *CRAS*, Vol. 305 (1987) pp. 881–883.
25. S. Lang, Cyclotomic fields I and II. *GTM*, Vol. 121 (1990).
26. *Philippe Langevin Rayon de Recouvrement des Codes de Reed-Muller Affines*, Ph.d Thesis, Université de Limoges (1992).
27. R. J. McEliece, Weight congruences for p-ary cyclic codes. *Discr. Math.*, Vol. 3 (1972) pp. 177–192.
28. Y. Niho, *Multi-valued Cross Correlation Functions Between Two Maximal Linear Recursive Sequences*. Ph.D Thesis, University of Southern California (1972).
29. K. Nyberg, *Differentially uniform mappings for cryptography*. Proc. of Eurocrypt '93, LNCS 765, Springer-Verlag (1994) pp. 55–64.
30. B. Poonen, G. McGuire, A. R. Calderbank and M. Rubinstein, On a conjecture of Helleseth's conjecture regarding pairs of binary m-sequences. *IEEE trans. Inf. Theory*, vol. 41, No. 4 (1995) pp. 1153–1155.
31. D. V. Sarwate and M. B. Pursley, Cross correlation properties of pseudo-random and related sequences. *Proc. IEEE*, Vol. 68 (1980) pp. 593–619.
32. V. M. Sidel'Nikov, On the mutual correlation of sequences. *Soviet Math. Dokl.*, Vol. 12 (1971) pp. 197–201.
33. J. Stickelberger, Uber eine verallgemeinerung der kreistheilung. *Math. Ann.*, Vol. 37 (1890) pp. 321–367.