Binary m-Sequences with Three-Valued Crosscorrelation: A Proof of Welch's Conjecture

Anne Canteaut, Pascale Charpin, and Hans Dobbertin

Abstract—**We prove the long-standing conjecture of Welch stating that for odd $n = 2m + 1$, the power function x^d with $d = 2^m + 3$ is maximally nonlinear on GF (2^n) or, in other terms, that the crosscorrelation function between a binary maximum-length linear shift register sequences of degree n and a decimation of that sequence by $2^m + 3$ takes on precisely the three values $-1, -1 \pm 2^{m+1}$.**

Index Terms—**Almost perfect nonlinear mappings, crosscorrelation, maximally nonlinear mappings, McEliece's theorem, power functions, Walsh transform, Welch's conjecture.**

I. Introduction and Preliminaries

In his 1968 paper [7], S. W. Golomb mentioned a conjecture of Welch concerning the crosscorrelation function of binary m-sequences (see also Niho's thesis [11] of 1972). Since that time, crosscorrelation functions have been studied intensively, but Welch's conjecture remained open. A weakened version was recently verified by the third author [5]. Based on this prework we shall finally confirm the Welch conjecture in the present paper. Applying McEliece's powerful theorem on divisible codes we can reduce the problem to an inequality for the Hamming weights of cyclotomic numbers, which actually holds as is demonstrated in the next section.

Let $L = \mathrm{GF}(2^n)$ be the finite field with 2^n elements, where $n = 2m+1$ is odd. A mapping F from L to L is called *almost perfect nonlinear* (APN) if each equation

$$F(t+a) + F(t) = b \qquad (a \in L^*, \, b \in L) \tag{1}$$

has at most two (and therefore either none or precisely two) solutions t in L. We note that an APN power function $F(x) = x^d$ is necessarily one-to-one for odd n, as can be seen easily.

Being APN is a "differential" property. Nevertheless, for odd n it is closely related to another extremal kind of nonlinearity which refers to the Hamming distance to linear mappings. The basic tool for the latter aspect is the *Walsh transform* $f^{\mathcal{W}}$ of a Boolean function $f\colon L \longrightarrow \mathrm{GF}(2)$, which is defined as

$$f^{\mathcal{W}}(a) = \sum_{x \in L} \chi(f(x) + \mathrm{Tr}\,(ax)), \qquad a \in L.$$

Here $\chi(y) = (-1)^{\mathrm{Tr}\,(y)}$ denotes the canonical additive character on GF (2). The $f^{\mathcal{W}}(a)$ are said to be the *Walsh coefficients of* f. If $|f^{\mathcal{W}}(a)|$ is "large" then the linear mapping $\ell_a(x) = \mathrm{Tr}\,(ax)$ (if $f^{\mathcal{W}}(a) > 0$) or its complement (if $f^{\mathcal{W}}(a) < 0$) has a "small" Hamming distance to f, or in other words, is a "good" approximation for f.

Thus a quantitative measure for the linearity of f is given by the maximal absolute value, denoted by $\mathcal{L}(f)$, occurring in the Walsh spectrum of f

$$\mathcal{L}(f) = \max\left\{\left|f^{\mathcal{W}}(a)\right| \,:\, a \in L\right\}.$$

The Walsh transform of $F\colon L \longrightarrow L$ is defined as the collection of all Walsh transforms of component functions of F, i.e., mappings of the form $f_{\mathcal{S}}(x) = \mathrm{Tr}\,(\mathcal{S}F(x))$, $\mathcal{S} \in L^*$. We denote by $\mathcal{W}(F)$ the set of all values occurring in the Walsh spectrum of F, and set

$$\mathcal{L}(F) = \max\{\mathcal{L}(f_{\mathcal{S}}) : \mathcal{S} \in L^*\}.$$

Those F attaining the minimal possible value for $\mathcal{L}(F)$ are called *maximally nonlinear*. This minimum is known to be 2^{m+1} for $n = 2m+1$. From Chabaud and Vaudenay [4, p. 363], we conclude.

Theorem 1: F is maximally nonlinear if and only if $\mathcal{W}(F) = \{0, \pm 2^{m+1}\}$. Moreover, if F is maximally nonlinear then F is APN.

On the other hand, if we take $F(x) = x^d$ with $\gcd(d, 2^n - 1) = 1$ then the Walsh spectrum of F allows us to determine the set of the values of the crosscorrelation function between the following two m-sequences (maximum-length linear shift register sequences): $(s_0, s_1, \cdots, s_i, \cdots)$ and $(s'_0, s'_1, \cdots, s'_i, \cdots)$ with $s_i = \mathrm{Tr}\,(\alpha^{id})$ and $s'_i = \mathrm{Tr}\,(a\alpha^i)$, and where α is a primitive root of L. In 1968, Welch conjectured that the power function x^d for the *Welch exponent*

$$d = 2^m + 3$$

is maximally nonlinear or, in other terms, that the crosscorrelation function between a binary maximum-length linear shift register sequence of degree n and a decimation of that sequence by $2^m + 3$ takes on precisely the three values $-1, -1 \pm 2^{m+1}$.

For this time, Welch's conjecture has been verified numerically for many values of m. Note that there are few classes of power functions that are maximally nonlinear. The most recent results are listed in [2].

Definition 1: The power functions $F(x) = x^d$ with $d = 2^m + 3$, m odd, are called the *Welch power functions*.

A major step toward confirming Welch's conjecture is the following theorem proven in [5].

Manuscript received August 31, 1998; revised June 23, 1999. This work was supported in part by the Katholieke Universiteit Leuven, Belgium. This work was performed while H. Dobbertin was with the Katholieke Universiteit Leuven, ESAT-COSIC, B-3001 Heverlee, Belgium

A. Canteaut and P. Charpin are with INRIA-Rocquencourt, Domaine de Voluceau, B.P. 105, F-78153 Le Chesnay Cedex, France (e-mail: {Anne.Canteaut; Pascale.Charpin}@inria.fr).

H. Dobbertin is with the German Information Security Agency, Bonn, Germany (e-mail: dobbertin@skom.rhein.de).

Communicated by S. W. Golomb, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(00)00361-8.

Theorem 2: Welch power functions are APN.

As mentioned above, the APN property is implied by maximal nonlinearity. Conversely, as we shall demonstrate below, the APN property plus the condition that all Walsh coefficients of $\mathrm{Tr}\,(x^d)$ are divisible by 2^{m+1} implies maximal nonlinearity. We note that there is also another way to prove this fact, namely, by using Kasami's method—we will indicate it in the Appendix at the end of the paper. This method is based on classical results in coding theory which make it possible to prove that under certain hypotheses the Walsh spectrum is unique. In our context these hypotheses are exactly the APN property and the divisibility condition for the Walsh coefficients.

It is well known (see, for instance, [8]) that if x^d is APN then the sum of fourth powers of all Walsh coefficients of $f(x) = \mathrm{Tr}\,(x^d)$ has precisely the value, namely, 2^{3n+1}, which appears in case of maximal nonlinearity, where the Walsh spectrum consists precisely of $\{0, \pm 2^{m+1}\}$. For the reader's convenience we include a proof.[1] We have

$$\begin{aligned}\sum_{a\in L} f^{\mathcal{W}}(a)^4 &= \sum_{a,\,x,\,y,\,z,\,w\in L} \chi(x^d+y^d+z^d+w^d+a(x+y+z+w))\\ &= \sum_{x,\,y,\,z,\,w\in L} \chi(x^d+y^d+z^d+w^d)\\ &\quad\cdot \sum_{a\in L}\chi(a(x+y+z+w)).\end{aligned}$$

We now apply a very common argument. If $x+y+z+w \neq 0$ then $a(x+y+z+w)$, $a\in L$, runs through all elements of L, and, therefore,

$$\sum_{a\in L}\chi(a(x+y+z+w)) = \begin{cases} 0, & \text{if } x+y+z+w \neq 0\\ 2^n, & \text{if } x+y+z+w = 0.\end{cases} \tag{2}$$

We can proceed as follows:

$$\begin{aligned}\sum_{a\in L} f^{\mathcal{W}}(a)^4 &= 2^n\left(\sum_{x,\,y,\,z\in L}\chi(x^d+y^d+z^d+(x+y+z)^d)\right)\\ &= 2^n\left(\sum_{x,\,y\in L}\chi(x^d+y^d+(x+y)^d) + \sum_{x,\,y\in L}\sum_{z\in L^*}\right.\\ &\qquad\left.\cdot\,\chi(z^d((x/z+y/z+1)^d+(x/z)^d+(y/z)^d+1))\right)\\ &= 2^n\left(\sum_{x,\,y\in L}\chi(x^d+y^d+(x+y)^d) - 2^{2n}\right.\\ &\qquad\left.+\sum_{u,\,v,\,z\in L}\chi(z^d((u+v+1)^d+u^d+v^d+1))\right)\end{aligned}$$

by using (2), for $z=0$ and any pair $(x,\,y)$, and next substituting $u = x/z$ and $v = y/z$.

Now $(u+v+1)^d+u^d+v^d+1 = 0$ holds iff either $u = v$ or else

$$\left(\frac{1}{u+v}+1\right)^d + \left(\frac{1}{u+v}\right)^d = \left(\frac{u}{u+v}+1\right)^d + \left(\frac{u}{u+v}\right)^d \tag{3}$$

(by dividing all terms by $(u+v)^d$). In accordance with (1), if x^d is APN then (3) is impossible for four different terms. If x^d is APN then the latter means either $u = 1$ or $v = 1$. Thus there are precisely $3\times(2^n-1)+1$ pairs $(u,\,v)$ satisfying the above equation : $u = v$ or $u = 1$ or $v = 1$. We conclude by using (2) that

$$\sum_{u,\,v,\,z\in L}\chi(z^d((u+v+1)^d+u^d+v^d+1)) = 2^n(3\times(2^n-1)+1).$$

Similarly we can derive

$$\sum_{x,\,y\in L}\chi(x^d+y^d+(x+y)^d) = 2^{n+1}$$

which altogether gives as claimed

$$\sum_{a\in L} f^{\mathcal{W}}(a)^4 = 2^n(2^{n+1}-2^{2n}+3\times 2^{2n}-2^{n+1}) = 2^{3n+1}.$$

Lemma 1: If for an APN power function x^d all Walsh coefficients of $\mathrm{Tr}\,(x^d)$ are divisible by 2^{m+1}, then x^d is maximally nonlinear.

Proof: Assume that $W_i = 2^{m+1}V_i$, $i = 0, 1, \cdots, k-1$, is a sequence listing all absolute values of nonzero coefficients occurring in the spectrum of $\mathrm{Tr}\,(x^d)$, where $V_0 = 1$ and $V_i > 1$ for $1 \le i < k$. Suppose that W_i occurs precisely λ_i times. Let x^d be APN. Then as shown above

$$\sum_{i<k}\lambda_i W_i^4 = \sum_{i<k}\lambda_i 2^{2n+2}V_i^4 = 2^{3n+1}.$$

By Parseval's equation we have

$$\sum_{i<k}\lambda_i W_i^2 = \sum_{i<k}\lambda_i 2^{n+1}V_i^2 = 2^{2n}.$$

Consequently,

$$\sum_{i<k}\lambda_i V_i^4 = \sum_{i<k}\lambda_i V_i^2$$

i.e.,

$$\sum_{i<k}\lambda_i(V_i^4-V_i^2) = \sum_{1\le i<k}\lambda_i(V_i^4-V_i^2) = 0.$$

Since $V_i^4 - V_i^2 > 0$ for $i \ge 1$, all $\lambda_i (i \ge 1)$ must vanish. □

For an arbitrary integer a we denote by $\omega(a)$ the Hamming weight of the binary representation of a and define

$$\omega_n(a) = \omega(a')$$

where a' is the remainder of a modulo $2^n - 1$.

[1] We note that, transferred into a coding theory context, power sums of Walsh coefficients correspond to Pless power moments[12].

McEliece's famous theorem on divisible codes (see [10]) states, transferred into the present context, that

Theorem 3: All Walsh coefficients of $\mathrm{Tr}\,(x^d)$ are divisible by 2^{m+1} if and only if for all nonzero $a < 2^n - 1$

$$\omega_n(a) + \omega_n(-ad) \geq m + 1$$

(recall that $n = 2m + 1$).

II. Proof of Welch's Conjecture: The Missing Link

In the sequel we identify integers with their binary representation. Let $d = 2^m + 3$ denote the Welch exponent. According to Theorem 2, Lemma 1, and Theorem 3 we have to show that $\omega_n(a) + \omega_n(-ad) \geq m + 1$ for all nonzero $a < 2^n - 1$, which is obviously equivalent to

$$\omega_n(ad) - \omega_n(a) \leq m \tag{4}$$

since $\omega_n(-x) = n - \omega_n(x)$ for nonzero x. Of course, we can assume that $\omega_n(a) \leq m$. We represent a in the form

$$a = b + 2^{m+1}c$$

where we assume without loss of generality $b < 2^m$ and $c < 2^{m-1}$. In fact, there exists a pair of positions $(i, i + m \bmod n)$ such that $a_i = a_{i+m} = 0$, since otherwise $\omega_n(a) \geq m + 1$. By a cyclic shift, or in other terms, cyclotomic equivalence, let $i = m$. We conclude

$$ad = (3b + c) + 2^m(b + 6c) \bmod 2^n - 1. \tag{5}$$

Our proof makes use of the evident fact that for arbitrary integers x, y we have

$$\omega(x + y) \leq \omega(x) + \omega(y)$$

with equality iff x and y are *disjoint*, in the sense that $x_i = 0$ or $y_i = 0$ for all i. The same rule holds for ω_n if $x, y < 2^n - 1$.

In view of (5) we shall study the following function H for arbitrary integers (finite bit strings) B, C

$$H(B, C) = \omega(3B + C) + \omega(B + 6C) - \omega(B) - \omega(C).$$

Note that

$$\omega_n(ad) - \omega_n(a) \leq H(b, c)$$

since $\omega_n(ad) \leq \omega(3b+c)+\omega(b+6c)$ and $\omega_n(a) = \omega(b)+\omega(c)$.

We have checked the following lemma with a computer.

Lemma 2: Let

$$B = B_5B_4B_3B_2B_1B_0 \quad \text{and} \quad C = C_5C_4C_3C_2C_1C_0$$

be bit strings of length 6, i.e., integers smaller than 64.

i) Then there is some nonzero $r \leq 6$ such that

$$H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) \leq r.$$

ii) If $B_0 = C_0 = 1$ then there is some nonzero $r \leq 6$, such that

$$H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) < r.$$

For 7-bit strings $B = B_6B_5B_4B_3B_2B_1B_0$ and $C = C_6C_5C_4C_3C_2C_1C_0$ we have:

iii) If $(B_0, C_0) \neq (1, 0)$ then there is some nonzero $r \leq 7$, with

$$H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) < r,$$

or there is some nonzero $r \leq 6$ with

$$H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) = r$$

and $(B_r, C_r) \neq (1, 0)$.

Lemma 3: Let $s \geq 1$. Let

$$B = B_{s-1} \cdots B_0$$
$$C = C_{s-1} \cdots C_0$$

be bit strings of length s, i.e., integers smaller that 2^s.

i) Then

$$H(B, C) \leq s + 2$$

and $H(B, C) = s + 2$ implies $B_0 = 1$, $C_0 = 0$.

ii) If $B_{s-1} = 1$ and $C_{s-1} = 0$ then

$$H(B, C) \leq s + 1$$

and $H(B, C) = s + 1$ implies $B_0 \neq C_0$.

iii) If $s \geq 2$, $B_{s-1} = 1$, and $C_{s-1} = C_{s-2} = 0$, then $H(B, C) = s + 1$ implies $B_0 = 1$, $C_0 = 0$, and $3B + C < 2^{s+1}$.

Proof: For $s \leq 6$ we checked the lemma by direct computations (with computer help). For $s > 6$ we proceed by induction as follows. Given B, C we have by Lemma 2 i) that there is some $0 < r \leq 6$ with $H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) \leq r$. We will use the inequality

$$\begin{aligned} H(B, C) \leq\, & H(B_{s-1} \cdots B_r, C_{s-1} \cdots C_r) \\ & + H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) \end{aligned} \tag{6}$$

and the notations

$$\begin{aligned} B^{(0)} &= B_{s-1} \cdots B_r & B^{(1)} &= B_{r-1} \cdots B_0 \\ C^{(0)} &= C_{s-1} \cdots C_r & C^{(1)} &= C_{r-1} \cdots C_0. \end{aligned}$$

Proof of i): To show $H(B, C) \leq s + 2$, it is sufficient to apply (6) and the induction hypothesis

$$\begin{aligned} H(B, C) &\leq H\left(B^{(0)}, C^{(0)}\right) + H\left(B^{(1)}, C^{(1)}\right) \\ &\leq (s - r + 2) + r = s + 2. \end{aligned}$$

Suppose now that $H(B, C) = s + 2$. This implies clearly $H(B^{(0)}, C^{(0)}) = s - r + 2$ and $H(B^{(1)}, C^{(1)}) = r$. The first equality implies that $(B_r, C_r) = (1, 0)$ (by the induction hypothesis) and, if $(B_0, C_0) \neq (1, 0)$, the second one implies that $(B_r, C_r) \neq (1, 0)$ (Lemma 2-iii)). We then deduce that $(B_0, C_0) = (1, 0)$.

Proof of ii): We similarly have

$$\begin{aligned} H(B, C) &\leq H\left(B^{(0)}, C^{(0)}\right) + H\left(B^{(1)}, C^{(1)}\right) \\ &\leq (s - r + 1) + r = s + 1. \end{aligned}$$

We now assume that $H(B, C) = s+1$ and $B_0 = C_0$ and we distinguish two cases:

- If $B_0 = C_0 = 0$ then $B = B'|0$ and $C = C'|0$. Thus $H(B, C) = H(B', C')$ where $H(B', C') \le s$—by induction since B' and C' have only $s-1$ bits.
- If $B_0 = C_0 = 1$ we apply Lemma 2 ii): we can choose r, $0 < r \le 6$, such that $H(B_{r-1} \cdots B_0, C_{r-1} \cdots C_0) < r$. Since $H(B^{(0)}, C^{(0)}) \le s-r+1$ by induction hypothesis, we obtain

$$H(B, C) < (s-r+1)+r = s+1.$$

In both cases we state a contradiction; so $B_0 \ne C_0$.

Proof of iii: Assume that $H(B, C) = s+1$ with $B_{s-1} = 1$ and $C_{s-1} = C_{s-2} = 0$.

We first prove that $(B_0, C_0) = (1, 0)$. If $H(B, C) = s+1$ there exists $r \le 6$ such that $H(B^{(0)}, C^{(0)}) = s-r+1$ and $H(B^{(1)}, C^{(1)}) = r$. If $s - r \le 2$, the first equality implies that $(B_r, C_r) = (1, 0)$ by induction hypothesis. This also holds when $s = r+1$, since $(B_r, C_r) = (B_{s-1}, C_{s-1}) = (1, 0)$. According to Lemma 2 iii), $(B_r, C_r) = (1, 0)$ and $H(B^{(1)}, C^{(1)}) = r$ can only occur when $(B_0, C_0) = (1, 0)$.

We now prove that our hypothesis implies $3B + C < 2^{s+1}$. Indeed, since $H(B^{(0)}, C^{(0)}) = s-r+1$ then $3B^{(0)} + C^{(0)} < 2^{s-r+1}$: if $s - r \ge 2$ this holds by induction hypothesis, and if $s - r = 1$, $3B^{(0)} + C^{(0)} = 3B_{s-1} + C_{s-1} = 3 < 2^2$. We then obtain:

$$\begin{aligned}3B + C &= \left(3B^{(0)} + C^{(0)}\right)2^r + \left(3B^{(1)} + C^{(1)}\right)\\ &< 2^{s+1} + \left(3B^{(1)} + C^{(1)}\right).\end{aligned}$$

Therefore, either $3B + C < 2^{s+1}$ as desired or $3B + C = 2^{s+1} + \Delta$ for some $0 \le \Delta \le 3(2^r - 1) < 2^{r+2} - 1$ with $r \le 6$. The latter is impossible. In fact, otherwise,

$$\begin{aligned}H(B, C) &= \omega(3B + C) + \omega(B + 6C) - \omega(B) - \omega(C)\\ &= \omega\left(2^{s+1} + \Delta\right) + \omega(B + 6C) - \omega(B) - \omega(C)\\ &\le \omega(\Delta) + 1 + \omega(B + 6C) - \omega(B) - \omega(C)\\ &\le 8 + \omega(6C) - \omega(C)\\ &= 8 + \omega(3C) - \omega(C).\end{aligned}$$

On the other hand, $\omega(3C) - \omega(C) \le (s-2)/2$ if s is even and $\omega(3C) - \omega(C) \le (s-1)/2$ if s is odd. Hence

$$s + 1 = H(B, C) \le 9 + (s-1)/2.$$

We then obtain a contradiction if $s \ge 14$. For $s \le 13$ the statement was verified by computer assistance. □

We are now prepared to confirm (4).

Case 1. $2^{m-1} \le b < 2^m$ and $2^{m-2} \le c < 2^{m-1}$: In this case, $b_{m-1} = 1$ and $c_{m-1} = 0$. By applying Lemma 3 ii), we obtain that $H(b, c) \le m+1$. Suppose now that $H(b, c) = m+1$. Since $b + 6c \ge 2^{m+1}$, we have

$$ad \equiv \left(b + 6c - 2^{m+1}\right)2^m + (3b + c + 1) \bmod \left(2^{2m+1} - 1\right)$$

where the right-hand term of this equality is positive, and

$$\omega_n(ad) \le \omega\left(b + 6c - 2^{m+1}\right) + \omega(3b + c + 1).$$

Using that $2^{m+1} \le b + 6c < 2^{m+2}$, we deduce that

$$\omega(b + 6c - 2^{m+1}) = \omega(b + 6c) - 1.$$

From Lemma 3 ii) we also have that $b_0 \ne c_0$, or, equivalently, that $(3b + c)$ is odd. Then $\omega(3b + c + 1) \le \omega(3b + c)$. We finally get that, if $H(b, c) = m+1$, then

$$\begin{aligned}\omega_n(ad) &\le \omega(b + 6c) - 1 + \omega(3b + c)\\ &\le H(b, c) - 1 \le m.\end{aligned}$$

Case 2. $2^{m-1} \le b < 2^m$ and $c < 2^{m-2}$: In this case, $b_{m-1} = 1$ and $c_{m-1} = c_{m-2} = 0$. By applying Lemma 3 iii), we obtain that $H(b, c) \le m+1$. Suppose now that $H(b, c) = m+1$. Lemma 3 iii) implies that $3b + c < 2^{m+1}$ and $b_0 = 1$. Since $3b + c > 2^m$, its most significant bit is m. By writing

$$ad \equiv (b + 6c + 1)2^m + (3b + c - 2^m) \bmod \left(2^{2m+1} - 1\right)$$

we get

$$\begin{aligned}\omega_n(ad) &\le \omega(b + 6c + 1) + \omega(3b + c - 2^m)\\ &\le \omega(b + 6c) + \omega(3b + c) - 1\\ &\le m\end{aligned}$$

where $\omega(b + 6c + 1) \le \omega(b + 6c)$ comes from the fact that $(b + 6c)$ is odd since $b_0 = 1$.

Case 3. $b < 2^{m-1}$ and $2^{m-2} \le c < 2^{m-1}$: In this case,

$$a' = 2^{m+1}a \bmod (2^{2m+1} - 1) = b2^{m+1} + 2c.$$

Since $2^{m-1} \le 2c < 2^m$, either Case 1 or Case 2 can be applied to a'. We then deduce that

$$\omega_n(ad) = \omega_n(a'd) \le m - \omega_n(a') = m - \omega_n(a).$$

Case 4. $b < 2^{m-1}$ and $c < 2^{m-2}$: If $b < 2^{m-2}$, Lemma 3 i) gives that $H(b, c) \le m$.

If $2^{m-2} \le b < 2^{m-1}$, we have $b_{m-2} = 1$ and $c_{m-2} = 0$. Lemma 3 ii) then implies that $H(b, c) \le m$. □

To summarize, we can state the following theorem, which was originally conjectured by Welch in 1968.

Theorem 4: Welch power functions are maximally nonlinear.

Recently, the third author has shown that *Niho power functions x^d*,

$$d = 2^{2r} + 2^r - 1, \qquad \text{with} \quad 4r + 1 \equiv 0 \bmod n$$

are APN. Niho [11] conjectured that they are even maximally nonlinear. We suspect that our methods, with somewhat more technical effort, could also be applied to confirm Niho's conjecture.

APPENDIX
THE CODING POINT OF VIEW

Consider binary cyclic codes of length $2^n - 1$, $n = 2m+1$, and whose generator polynomial is the product of two minimal polynomials. More precisely, let α be a primitive root of

GF(2^n) and denote by $M_s(X)$ the minimal polynomial of α^s, $1 \leq s \leq 2^{n-1}-1$. Let us denote by C_s the binary cyclic code whose generator is the product $M_1(X)M_s(X)$, $s \neq 2^i$ for all i. Assuming that $\gcd(s,\, 2^n-1)=1$, C_s is a $[2^n-1,\, 2^n-2n-1]$ code whose minimum distance δ_s is in $\{3, 4, 5\}$.

It was shown in [3] that the power function x^s is APN if and only if $\delta_s = 5$. This function is maximally nonlinear on L if and only if the dual of C_s, say $C_s^\perp$, has three nonzero weights only, which are 2^{n-1} and $2^{n-1} \pm 2^m$. Moreover, it is known that if $C_s^\perp$ satisfies this last condition then its weight enumerator is unique and is the same as the weight enumerator of the dual of the two-error-correcting Bose–Chaudhuri–Hocquenghem (BCH) code. The tools introduced by Kasami [9] for his proof can be used for proving Lemma 1—that we rewrite below for codes C_s.

Proposition 1: The code $C_s^\perp$ has only three weights, 2^{n-1} and $2^{n-1} \pm 2^m$, if and only if $\delta_s = 5$ and each weight of $C_s^\perp$ is divisible by 2^m.

Proof: We present a sketch of proof only; a full explanation, in a more general context, will be given in a forthcoming paper [2].

Let $k = 2^n - 1$ and $\eta = (\eta_0, \cdots, \eta_k)$ (respectively, $\nu = (\nu_0, \cdots, \nu_k)$) be the weight enumerator of the code $C_s^\perp$ (respectively, C_s). The proof is based on the study of numbers $I_\ell = \sum_{w=1}^{k} (w - 2^{n-1})^\ell \eta_w$, for some ℓ. We have for any even ℓ

$$I_\ell = \sum_{w=w_0}^{2^{n-1}-1} (w - 2^{n-1})^\ell (\eta_w + \eta_{2^n-w})$$

where w_0 is the minimal weight of $C_s^\perp$. By using the four first power moments of weight enumerator [12], we obtain $I_2 = 2^{3n-2} - 2^{2n-2}$ and

$$I_4 = 2^{3n-4}(3 \cdot 2^n - 2) - 2^{4n-4} + 3 \cdot 2^{2n-1}(\nu_3 + \nu_4).$$

We deduce two expressions of $\mathcal{I} = I_4 - 2^{n-1} I_2$ (where $n = 2m+1$)

$$\begin{aligned} I_4 - 2^{2m} I_2 = &\sum_{w=w_0}^{2^{2m}-1} \left(w - 2^{2m}\right)^2 \left(\left(w - 2^{2m}\right)^2 - 2^{2m}\right) \\ &\cdot (\eta_w + \eta_{2^n-w}) \\ =& \, 3 \cdot 2^{2n-1}(\nu_3 + \nu_4). \end{aligned}$$

Note that the wth term above is less than or equal to zero if and only if w satisfies: $2^{2m} - 2^m \leq w \leq 2^{2m} - 1$ or $\eta_w = \eta_{2^n-w} = 0$.

First $\mathcal{I} = 0$ if and only if $\nu_3 = \nu_4 = 0$, i.e., $\delta_s = 5$. On the other hand, there is no negative term in the first expression of $\mathcal{I}$ when all weights w of $C_s^\perp$ are divisible by 2^m. Since $\mathcal{I} = 0$ when the weights of $C_s^\perp$ are only 2^{n-1} and $2^{n-1} \pm 2^m$, the proof is easily completed. □

Remark: A maximally nonlinear power function is usually said to be *almost bent* (AB) in a cryptographic context. Such a function opposes an optimum resistance to both linear and differential cryptanalysis. An extensive study of APN and AB properties was recently made by Carlet, Charpin, and Zinoviev in [3].

Acknowledgment

The authors wish to thank C. Carlet, T. Helleseth, E. Schulte-Geers, F. Levy-dit-Vehel, and V. Zinoviev for helpful discussions and hints. They would also like to thank the members of the Research Group ESAT-COSIC, especially Prof. B. Preneel, for their hospitality.

References

[1] A. Canteaut, P. Charpin, and H. Dobbertin, “Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs: Conjecture de Welch,” *C.R. Acad. Sci. Paris*, ser. 1, vol. 328, pp. 173–178, 1999.

[2] ——, “Divisibility of cyclic codes and highly nonlinear functions on $\mathbf{F}_{2^m}$,” *SIAM J. Discr. Math*, to be published.

[3] C. Carlet, P. Charpin, and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems,” *Des., Codes Cryptogr.*, vol. 15, pp. 125–156, 1998.

[4] F. Chabaud and S. Vaudenay, “Links between differential and linear cryptanalysis,” in *Advances in Cryptology—EUROCRYPT’94*. ser. Lecture Notes in Computer Science, vol. 950, A. De Santis, Ed. New York, NY: Springer-Verlag, 1995, pp. 356–365.

[5] H. Dobbertin, “Almost perfect nonlinear power functions on GF(2^n): The Welch case,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 1271–1275, May 1999.

[6] ——, “Almost perfect nonlinear power functions on GF(2^n): The Niho case,” *Inform. Comput.*, to be published.

[7] S. W. Golomb, “Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences,” *Inform. Sci.*, vol. 1, pp. 87–109, 1968.

[8] T. Helleseth, “Some results about the cross-correlation function between two maximal linear sequences,” *Discr. Math.*, vol. 16, pp. 209–232, 1976.

[9] T. Kasami, “Weight distributions of Bose–Chaudhuri–Hocquenghem codes,” in *Combinatorial Mathematics and Applications*, R. C. Bose and T. A. Dowlings, Eds. Chapel Hill, NC: Univ. North Carolina Press, 1969, ch. 20.

[10] R. J. McEliece, “Weight congruence for p-ary cyclic codes,” *Discr. Math.*, vol. 3, pp. 177–192, 1972.

[11] Y. Niho, “Multi-valued cross-correlation functions between two maximal linear recursive sequences,” Ph.D. dissertation, Dept. Elec. Eng., Univ. Southern California, Los Angeles, CA, 1972.

[12] V. Pless, “Power moment identities on weight distributions in error-correcting codes,” *Inform. Contr.*, vol. 6, pp. 147–152, 1963.