A New Characterization of Almost Bent Functions

Anne Canteaut[1], Pascale Charpin[1], and Hans Dobbertin[2]

[1] INRIA - projet CODES
BP 105, 78153 Le Chesnay, France
{Anne.Canteaut,Pascale.Charpin}@inria.fr
[2] German Information Security Agency
P.O.Box 20 03 63, 53133 Bonn, Germany
dobbertin@skom.rhein.de

Abstract. We study the functions from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$ for odd m which oppose an optimal resistance to linear cryptanalysis. These functions are called almost bent. It is known that almost bent functions are also almost perfect nonlinear, *i.e.* they also ensure an optimal resistance to differential cryptanalysis but the converse is not true. We here give a necessary and sufficient condition for an almost perfect nonlinear function to be almost bent. This notably enables us to exhibit some infinite families of power functions which are not almost bent.

1 Introduction

This paper is devoted to the study of the functions f from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$ which achieve the highest possible nonlinearity. This means that any non-zero linear combination of the Boolean components of f is as far as possible from the set of Boolean affine functions with m variables. When m is odd, the highest possible value for the nonlinearity of a function over $\mathbf{F}_{2^m}$ is known and the functions achieving this bound are called almost bent. These functions play a major role in cryptography; in particular their use in the S-boxes of a Feistel cipher ensure the best resistance to linear cryptanalysis. It was recently proved [5] that the nonlinearity of a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$ corresponds to the minimum distance of the dual of a linear code $\mathcal{C}_f$ of length $(2^m - 1)$. In particular when f is a power function, $f : x \mapsto x^s$, this code $\mathcal{C}_f$ is the cyclic code $\mathcal{C}_{1,s}$ of length $(2^m - 1)$ whose zeros are α and α^s (α denotes a primitive element of $\mathbf{F}_{2^m}$). It was also established [6] that if a function over $\mathbf{F}_2^m$ for odd m ensures the best resistance to linear cryptanalysis, it also ensures the best resistance to differential cryptanalysis. For the associated code $\mathcal{C}_f$, this means that if its dual (or orthogonal) code, denoted by $\mathcal{C}_f^\perp$, has the highest possible minimum distance, then $\mathcal{C}_f$ has minimum distance at least 5. But the reciprocal does not hold. Using Pless power moment identities [22] and some ideas due to Kasami [13], we make this condition necessary and sufficient by adding a requirement on the divisibility of the weights of $\mathcal{C}_f^\perp$. Since the divisibility of the weights of the cyclic code $\mathcal{C}_{1,s}^\perp$ is completely determined by McEliece's theorem [17], the determination of the values of s such that the power function $x \mapsto x^s$ is almost bent on $\mathbf{F}_{2^m}$ is now

L. Knudsen (Ed.): FSE'99, LNCS 1636, pp. 186–200, 1999.

reduced to a combinatorial problem. This notably yields a very fast algorithm for checking if a power function over $\mathbf{F}_{2^m}$ is almost bent, even for large values of m. McEliece's theorem can also be used for proving that $\mathcal{C}_{1,s}^{\perp}$ contains a codeword whose weight does not have the appropriate divisibility. We are then able to prove that, for some infinite families of values of s the power function $x \mapsto x^s$ is not almost bent on $\mathbf{F}_{2^m}$.

The next section recalls the link between the weight distribution of the duals of cyclic codes with two zeros and the nonlinearity of a function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$. In Section 3 we develop a new theoretical tool for studying the weight distribution of some linear codes, which generalizes some ideas due to Kasami. Combined with McEliece's theorem, this method provides a new characterization of almost bent power mappings. Section 4 then focuses on power functions $x \mapsto x^s$ over $\mathbf{F}_{2^m}$ for odd m when the exponent s can be written as $s = 2^{\frac{m-1}{2}} + 2^i - 1$. This set of exponents contains the values which appear in both Welch's and Niho's almost bent functions. We here prove that for most values of i, $x \mapsto x^{2^{\frac{m-1}{2}}+2^i-1}$ is not almost bent on $\mathbf{F}_{2^m}$. In Section 5 we finally give a very simple necessary condition on the exponents s providing almost bent power functions on $\mathbf{F}_{2^m}$ when m is not a prime; in this case we are able to eliminate most values of s. We also prove that the conjectured almost perfect nonlinear function $x \mapsto x^s$ with $s = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ over $\mathbf{F}_{2^{5g}}$ is not almost bent.

2 Almost Bent Functions and Cyclic Codes with Two Zeros

2.1 Almost Perfect Nonlinear and Almost Bent Functions

Let f be a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2^m$. For any $(a, b) \in \mathbf{F}_2^m \times \mathbf{F}_2^m$, we define

$$\delta_f(a,b) = \#\{x \in \mathbf{F}_2^m,\ f(x+a) + f(x) = b\}$$
$$\lambda_f(a,b) = |\#\{x \in \mathbf{F}_2^m,\ a \cdot x + b \cdot f(x) = 0\} - 2^{m-1}|$$

where $\cdot$ is the usual dot product on $\mathbf{F}_2^m$. These values are of great importance in cryptography especially for measuring the security of an iterated block cipher using f as a round permutation [6]. A differential attack [2] against such a cipher exploits the existence of a pair (a, b) with $a \neq 0$ such that $\delta_f(a, b)$ is high. Similarly a linear attack [16] is successful if there is a pair (a, b) with $b \neq 0$ such that $\lambda_f(a, b)$ is high. The function f can then be used as a round function of an iterated cipher only if both

$$\delta_f = \max_{a \neq 0} \max_b \delta_f(a,b) \quad \text{and} \quad \lambda_f = \max_a \max_{b \neq 0} \lambda_f(a,b)$$

are small. Moreover if f defines the S-boxes of a Feistel cipher, the values of δ_f and λ_f completely determine the complexity of differential and linear cryptanalysis [21,20].

Proposition 1. *[21] For any function $f : \mathbf{F}_2^m \to \mathbf{F}_2^m$,*

$$\delta_f \geq 2 \ .$$

In case of equality f is called almost perfect nonlinear *(APN).*

Proposition 2. *[24,6] For any function* $f : \mathbf{F}_2^m \to \mathbf{F}_2^m$,

$$\lambda_f \geq 2^{\frac{m-1}{2}} \ .$$

In case of equality f *is called* almost bent *(AB).*

Note that this minimum value for $\lambda_f$can only be achieved if m is odd. For even m, some functions with $\lambda_f = 2^{\frac{m}{2}}$ are known and it is conjectured that this value is the minimum [23, p. 603].

From now on the vector space $\mathbf{F}_2^m$ is identified with the finite field $\mathbf{F}_{2^m}$. The function f can then be expressed as a unique polynomial of $\mathbf{F}_{2^m}[X]$ of degree at most $(2^m - 1)$. Note that the values of δ_f and λ_f are invariant under both right and left compositions by a linear permutation of $\mathbf{F}_{2^m}$. Similarly, if f is a permutation, $\delta_f = \delta_{f^{-1}}$ and $\lambda_f = \lambda_{f^{-1}}$. We can then assume that $f(0) = 0$ without loss of generality.

Both APN and AB properties can also be expressed in terms of error-correcting codes. We use standard notation of the algebraic coding theory (see [15]). The (Hamming) weight of any vector $x \in \mathbf{F}_2^n$ is denoted by $wt(x)$. Any linear subspace of $\mathbf{F}_2^n$ is called a binary linear code of length n and dimension k and is denoted by $[n, k]$. Any $[n, k]$-linear code $\mathcal{C}$ is associated with its dual $[n, n-k]$-code, denoted by $\mathcal{C}^\perp$:

$$\mathcal{C}^\perp = \{x \in \mathbf{F}_2^n, \ \ x \cdot c = 0 \ \forall c \in \mathcal{C}\} \ .$$

Any $r \times n$ binary matrix H defines an $[n, n-r]$-binary linear code $\mathcal{C}$:

$$\mathcal{C} = \{c \in \mathbf{F}_2^n, \ cH^T = 0\}$$

where H^T is the transposed matrix of H. We then say that H is a parity-check matrix of $\mathcal{C}$. The proofs of the following results are developed by Carlet, Charpin and Zinoviev in [5]:

Theorem 1. *Let* f *be a function from* $\mathbf{F}_{2^m}$ *into* $\mathbf{F}_{2^m}$ *with* $f(0) = 0$. *Let* $\mathcal{C}_f$ *be the linear binary code of length* $2^m - 1$ *defined by the* $2m \times (2^m - 1)$*-parity-check matrix*

$$H_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \dots & f(\alpha^{2^m-2}) \end{pmatrix} \ , \tag{1}$$

where each entry is viewed as a binary column vector of length m *and* α *is a primitive element of* $\mathbf{F}_{2^m}$. *Then*

(i) $\lambda_f = 2^{m-1}$ *if and only* $\dim \mathcal{C}_f > 2^m - 1 - 2m$ *or* $\mathcal{C}_f^\perp$ *contains the all-one vector.*

(ii) If $\dim \mathcal{C}_f = 2^m - 1 - 2m$,

$$\lambda_f = \max_{c \in \mathcal{C}_f^\perp, c \neq 0} |2^{m-1} - wt(c)| \ .$$

In particular, for odd m, f *is AB if and only if for any non-zero codeword* $c \in \mathcal{C}_f^\perp$,

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq wt(c) \leq 2^{m-1} + 2^{\frac{m-1}{2}} \ .$$

(iii) f is APN if and only if the code $\mathcal{C}_f$ has minimum distance 5.

Tables 1 (resp. 2) give all known and conjectured values of exponents s (up to equivalence) such that the power function $x \mapsto x^s$ is APN (resp. AB). AB power permutations also correspond to pairs of maximum-length sequences with preferred crosscorrelation [23].

Table 1. Known and conjectured APN power functions x^s on $\mathbf{F}_{2^m}$ with $m = 2t + 1$

	exponents s	status
quadratic functions	$2^i + 1$ with $\gcd(i, m) = 1$ and $1 \le i \le t$	proven [10,19]
Kasami's functions	$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 1$ and $2 \le i \le t$	proven [14]
inverse function	$2^{2t} - 1$	proven [19,1]
Welch's function	$2^t + 3$	proven [9]
Niho's function	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	proven [8]
Dobbertin's function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ if $m = 5i$	conjectured [8]

Table 2. Known AB power permutations x^s on $\mathbf{F}_{2^m}$ with $m = 2t + 1$

	exponents s	status
quadratic functions	$2^i + 1$ with $\gcd(i, m) = 1$ and $1 \le i \le t$	proven [10,19]
Kasami's functions	$2^{2i} - 2^i + 1$ with $\gcd(i, m) = 1$ and $2 \le i \le t$	proven [14]
Welch's function	$2^t + 3$	proven [4,3]
Niho's function	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	proven [12]

2.2 Weight Divisibility of Cyclic Codes

We now give some properties of binary cyclic codes since the linear code $\mathcal{C}_f$ associated to a power function $f : x \mapsto x^s$ on $\mathbf{F}_{2^m}$ is a binary cyclic code of length $(2^m - 1)$ with two zeros. We especially focus on the weight divisibility of the duals of such codes.

Definition 1. *A linear binary code $\mathcal{C}$ of length n is cyclic if for all codewords $(c_0, \ldots, c_{n-1})$ in $\mathcal{C}$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathcal{C}$.*

If each vector $(c_0, \ldots, c_{n-1}) \in \mathbf{F}_2^n$ is associated with the polynomial $c(X) = \sum_{i=0}^{n-1} c_i X$î in $\mathcal{R}_n = \mathbf{F}_2^n[X]/(X^n - 1)$, any binary cyclic code of length n is an ideal of $\mathcal{R}_n$. Since $\mathcal{R}_n$ is a principal domain, any cyclic code $\mathcal{C}$ of length n is generated

by a unique monic polynomial g having minimal degree. This polynomial is called the generator polynomial of the code and its roots are the zeros of $\mathcal{C}$. The defining set of $\mathcal{C}$ is then the set

$$I(\mathcal{C}) = \{i \in \{0, \cdots, 2^m - 2\} |\ \alpha^i \text{ is a zero of } \mathcal{C}\} \ .$$

where α is a primitive element of $\mathbf{F}_{2^m}$. Since $\mathcal{C}$ is a binary code, its defining set is a union of 2-cyclotomic cosets modulo $(2^m - 1)$, $Cl(a)$, where $Cl(a) = \{2^j a \bmod (2^m - 1)\}$. From now on the defining set of a binary cyclic code of length $(2^m - 1)$ is identified with the representatives of the corresponding 2-cyclotomic cosets modulo $(2^m - 1)$. The linear code $\mathcal{C}_f$ associated to the power function $f : x \mapsto x^s$ on $\mathbf{F}_{2^m}$ is defined by the following parity-check matrix:

$$H_f = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^s & \alpha^{2s} & \dots & \alpha^{(2^m-2)s} \end{pmatrix} \ .$$

It then consists of all binary vectors c of length $(2^m - 1)$ such that $cH_f^T = 0$, *i.e.*

$$c(\alpha) = \sum_{i=0}^{2^m-2} c_i \alpha^i = 0 \text{ and } c(\alpha^s) = \sum_{i=0}^{2^m-2} c_i \alpha^{is} = 0 \ .$$

The code $\mathcal{C}_f$ is therefore the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$.

Definition 2. *A binary code $\mathcal{C}$ is said* 2^ℓ-divisible *if the weight of any of its codewords is divisible by 2^ℓ. Moreover $\mathcal{C}$ is said* exactly 2^ℓ-divisible *if, additionally, it contains at least one codeword whose weight is not divisible by $2^{\ell+1}$.*

The following theorem due to McEliece reduces the determination of the exact weight divisibility of binary cyclic codes to a combinatorial problem:

Theorem 2. *[17] A binary cyclic code is exactly 2^ℓ-divisible if and only if ℓ is the smallest number such that $(\ell + 1)$ nonzeros of $\mathcal{C}$ (with repetitions allowed) have product 1.*

We now focus on primitive cyclic codes with two zeros and on the exact weight divisibility of their duals. We denote by $\mathcal{C}_{1,s}$ the binary cyclic code of length $(2^m - 1)$ with defining set $Cl(1) \cup Cl(s)$. The nonzeros of the cyclic code $\mathcal{C}_{1,s}^\perp$ are the elements α^{-i} with $i \in Cl(1) \cup Cl(s)$. Then $(\ell + 1)$ nonzeros of $\mathcal{C}_{1,s}^\perp$ have product 1 if and only if there exist $I_1 \subset Cl(s)$ and $I_2 \subset Cl(1)$ with $|I_1| + |I_2| = \ell + 1$ and

$$\prod_{k \in I_1 \cup I_2} \alpha^{-k} = 1 \iff \sum_{k \in I_1 \cup I_2} k \equiv 0 \bmod (2^m - 1)$$

We consider both integers u and v defined by their 2-adic expansions: $u = \sum_{i=0}^{m-1} u_i 2^i$ and $v = \sum_{i=0}^{m-1} v_i 2^i$ where $u_i = 1$ if and only if $2^i s \bmod (2^m - 1) \in I_1$ and $v_i = 1$ if and only if $2^i \bmod (2^m - 1) \in I_2$. Then we have

$$\sum_{k \in I_1 \cup I_2} k \equiv \sum_{i=0}^{m-1} u_i 2^i s + \sum_{i=0}^{m-1} v_i 2^i \bmod (2^m - 1) \equiv 0 \bmod (2^m - 1)$$

The size of I_1 (resp. I_2) corresponds to $w_2(u) = \sum_{i=0}^{m-1} u_i$ which is the 2-weight of u (resp. v). McEliece's theorem can then be formulated as follows:

Corollary 1. *The cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^m - 1)$ is exactly 2^ℓ-divisible if and only if for all (u, v) such that $0 \leq u \leq 2^m - 1$, $0 \leq v \leq 2^m - 1$ and*

$$us + v \equiv 0 \bmod (2^m - 1),$$

we have $w_2(u) + w_2(v) \geq \ell + 1$.

Since $v \leq 2^m - 1$, the condition $us + v \equiv 0 \bmod (2^m - 1)$ can be written $v = (2^m - 1) - (us \bmod (2^m - 1))$. This leads to the following equivalent formulation:

Corollary 2. *The cyclic code $\mathcal{C}_{1,s}^{\perp}$ of length $(2^m - 1)$ is exactly 2^ℓ-divisible if and only if for all u such that $0 \leq u \leq 2^m - 1$,*

$$w_2(A(u)) \leq w_2(u) + m - 1 - \ell$$

where $A(u) = us \bmod (2^m - 1)$.

3 Characterization of Almost Bent Functions

As previously seen the nonlinearity of a function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ is related to the weight distributions of some linear binary codes of length $(2^m - 1)$ and dimension $2m$. We here give some general results on the weight distributions of linear codes having these parameters. Our method uses Pless power moment identities [22] and some ideas due to Kasami [13, th. 13] (see also [5, th. 4]). The weight enumerator of a linear code $\mathcal{C}$ of length n is the vector $(A_0, \ldots, A_n)$ where A_i is the number of codewords of weight i in $\mathcal{C}$.

Theorem 3. *Let $\mathcal{C}$ be a $[2^m - 1, 2^m - 2m - 1]$ linear binary code with minimum distance $d \geq 3$. Assume that the dual code $\mathcal{C}^{\perp}$ does not contain the all-one vector $\mathbf{1} = (1, \cdots, 1)$. Let $A = (A_0, \cdots, A_{2^m-1})$ (resp. $B = (B_0, \cdots, B_{2^m-1})$) be the weight enumerator of $\mathcal{C}^{\perp}$ (resp. $\mathcal{C}$). Then we have*

(i) If w_0 is such that $A_w = A_{2^m-w} = 0$ for all $0 < w < w_0$, then

$$6(B_3 + B_4) \leq (2^m - 1)\left[(2^{m-1} - w_0)^2 - 2^{m-1}\right]$$

where equality holds if and only if $A_w = 0$ for all $w \notin \{0, w_0, 2^{m-1}, 2^m - w_0\}$.

(ii) If w_1 is such that $A_w = A_{2^m-w} = 0$ for all $w_1 < w < 2^{m-1}$, then

$$6(B_3 + B_4) \geq (2^m - 1)\left[(2^{m-1} - w_1)^2 - 2^{m-1}\right]$$

where equality holds if and only if $A_w = 0$ for all $w \notin \{0, w_1, 2^{m-1}, 2^m - w_1\}$.

Proof. The main part of the proof relies on the first Pless power moment identities [22]. The first four power moment identities on the weight distribution of the $[2^m-1, 2m]$-code $\mathcal{C}^\perp$ are:

$$\sum_{w=0}^{n} wA_w = 2^{2m-1}(2^m-1),$$
$$\sum_{w=0}^{n} w^2A_w = 2^{3m-2}(2^m-1),$$
$$\sum_{w=0}^{n} w^3A_w = 2^{2m-3}\left((2^m-1)^2(2^m+2) - 3!B_3\right),$$
$$\sum_{w=0}^{n} w^4A_w = 2^{2m-4}\left(2^m(2^m-1)(2^{2m}+3\cdot 2^m-6) + 4!\ (B_4-(2^m-1)B_3)\right)$$

Let us consider the numbers $I_\ell = \sum_{w=1}^{2^m-1}(w-2^{m-1})^\ell A_w$. Since for ℓ even

$$(w-2^{m-1})^\ell = ((2^m-w)-2^{m-1})^\ell\ ,$$

we have for any even ℓ:

$$I_\ell = \sum_{w=1}^{2^m-1}(w-2^{m-1})^\ell A_w = \sum_{w=1}^{2^{m-1}-1}(w-2^{m-1})^\ell (A_w + A_{2^m-w})\ .$$

Note that the codeword of weight zero is not taken in account in the sum above. Recall that $\mathcal{C}^\perp$ does not contain the all-one codeword. By using the four power moments, we obtain the following values for I_2 and I_4:

$$I_2 = 2^{2m-2}(2^m-1)$$
$$I_4 = 2^{2m-2}\left[6(B_3+B_4) + 2^{m-1}(2^m-1)\right]$$

This implies

$$\begin{aligned}\mathcal{I}(x) = I_4 - x^2I_2 &= \sum_{w=1}^{2^{m-1}-1}(w-2^{m-1})^2\left((w-2^{m-1})^2-x^2\right)(A_w+A_{2^m-w})\\ &= 2^{2m-2}\left[6(B_3+B_4) + (2^m-1)(2^{m-1}-x^2)\right]\end{aligned}$$

The w-th term in this sum satisfies:

$$\begin{aligned}(w-2^{m-1})^2\left((w-2^{m-1})^2-x^2\right) &< 0 \ \text{ if } 0<|2^{m-1}-w|<x\\ &= 0 \ \text{ if } w\in\{2^{m-1}, 2^{m-1}\pm x\}\\ &> 0 \ \text{ if } |2^{m-1}-w|>x\end{aligned}$$

This implies that, if $A_w = A_{2^m-w} = 0$ for all w such that $0<w<w_0$, all the terms in $\mathcal{I}(2^{m-1}-w_0)$ are negative. Then we have

$$6(B_3+B_4) + (2^m-1)\left[2^{m-1}-(2^{m-1}-w_0)^2\right] \le 0$$

with equality if and only if all terms in the sum are zero. This can only occur when $A_w = 0$ for all $w \notin \{0, w_0, 2^{m-1}, 2^m - w_0\}$.

Similarly, if $A_w = A_{2^m-w} = 0$ for all w such that $w_1 < w < 2^{m-1}$, all the terms in $\mathcal{I}(2^{m-1} - w_1)$ are positive. Then we have

$$6(B_3 + B_4) + (2^m - 1)\left[2^{m-1} - (2^{m-1} - w_1)^2\right] \geq 0$$

with equality if and only if all terms in the sum are zero, *i.e.* if $A_w = 0$ for all $w \notin \{0, w_1, 2^{m-1}, 2^m - w_1\}$. ◇

Let us now suppose that m is odd, $m = 2t + 1$. We give a necessary and sufficient condition on $f : \mathbf{F}_{2^m} \to \mathbf{F}_{2^m}$ to be almost bent.

Theorem 4. *Let m be an odd integer and let f be a function from $\mathbf{F}_{2^m}$ into $\mathbf{F}_{2^m}$ such that $\lambda_f \neq 2^{m-1}$. Then f is AB if and only if f is APN and the code $\mathcal{C}_f^\perp$ defined in Theorem 1 is $2^{\frac{m-1}{2}}$-divisible.*

Proof. Let $(A_0, \cdots, A_{2^m-1})$ (resp. $(B_0, \cdots, B_{2^m-1})$) be the weight enumerator of $\mathcal{C}_f^\perp$ (resp. $\mathcal{C}_f$) and let w_0 be the smallest w such that $0 < w < 2^{m-1}$ and $A_w + A_{2^m-w} \neq 0$ for all $0 < w < w_0$. According to Theorem 1 *(ii)*, f is AB if and only if $w_0 = 2^{m-1} - 2^{\frac{m-1}{2}}$. Since $\lambda_f \neq 2^{m-1}$, we deduce from Theorem 1 *(i)* that the code $\mathcal{C}_f$ has dimension $2^m - 2m - 1$ and that $\mathcal{C}_f^\perp$ does not contain the all-one vector. Since the minimum distance of $\mathcal{C}_f$ is obviously greater than 3, Theorem 3 can be applied. The announced condition is sufficient: if $w_0 = 2^{m-1} - 2^{\frac{m-1}{2}}$ we have that $B_3 + B_4 = 0$ according to Theorem 3 *(i)*. This means that $\mathcal{C}_f$ has minimum distance 5 (*i.e.* f is APN). Moreover all nonzero weights of $\mathcal{C}_f^\perp$ lie in $\{2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$. The code $\mathcal{C}_f^\perp$ is therefore $2^{\frac{m-1}{2}}$-divisible.

The condition is also necessary since, for any w such that $2^{m-1} - 2^{\frac{m-1}{2}} < w < 2^{m-1}$, both integers w and $2^{m-1} - w$ are not divisible by $2^{\frac{m-1}{2}}$. The condition on the divisibility of the weights of $\mathcal{C}_f^\perp$ then implies that $A_w + A_{2^m-w} = 0$ for all w such that $2^{m-1} - 2^{\frac{m-1}{2}} < w < 2^{m-1}$. If f is APN, $\mathcal{C}_f$ does not contain any codeword of weight 3 and 4. The lower bound given in Theorem 3 *(ii)* (applied with $w_1 = 2^{m-1} - 2^{\frac{m-1}{2}}$) is then reached. It follows that the weight of every codeword in $\mathcal{C}_f^\perp$ lies in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$ and therefore that f is AB. ◇

When f is a power function, $f : x \mapsto x^s$, the corresponding code C_f is the binary cyclic code $\mathcal{C}_{1,s}$ of length $(2^m - 1)$ with defining set $\{1, s\}$. The weight divisibility of the corresponding dual code can therefore be obtained by applying McEliece's theorem, as expressed in Corollary 2. This leads to the following characterization of AB power functions:

Corollary 3. *Let $m = 2t + 1$. Assume that the power function $f : x \mapsto x^s$ on $\mathbf{F}_{2^m}$ has no affine component. Then f is AB on $\mathbf{F}_{2^m}$ if and only if f is APN on $\mathbf{F}_{2^m}$ and*

$$\forall u, \;\; 1 \leq u \leq 2^m - 1, \;\; w_2(A(u)) \leq t + w_2(u) \tag{2}$$

where $A(u) = us \bmod (2^m - 1)$.

Condition (2) is obviously satisfied when $w_2(u) \geq t+1$. Moreover, if $\gcd(s, 2^m - 1) = 1$ (*i.e.* if $x \mapsto x^s$ is a permutation), the condition also holds for all u such that $w_2(u) = t$. Using that

$$A(u2^i \bmod (2^m - 1)) = 2^i A(u) \bmod (2^m - 1),$$

we deduce that Condition (2) must only be checked for one element in each cyclotomic coset. Note that if u is the smallest element in its cyclotomic coset and $w_2(u) < t$, we have $u \leq 2^{m-2} - 1$. This result provides a fast algorithm for checking whether an APN power function is AB, and then for finding all AB power functions on $\mathbf{F}_{2^m}$. There are roughly $\frac{2^{m-1}}{m}$ cyclotomic representatives u such that $w_2(u) \leq t$ and each test requires one modular multiplication on m-bit integers and two weight computations. Condition (2) can then be checked with around 2^m elementary operations and at no memory cost.

The 2-weight of s obviously gives an upper bound on the weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ (obtained for $u = 1$ in Corollary 2). Using this result, we immediately recover the condition on the degree of AB functions given in [5, Theorem 1] in the particular case of power functions.

Corollary 4. *Let m be an odd integer. If the power permutation $f : x \mapsto x^s$ is AB on $\mathbf{F}_{2^m}$, then*

$$\text{degree}(f) = w_2(s) \leq \frac{m+1}{2} \ .$$

4 Power Functions $x \mapsto x^s$ on $\mathbf{F}_2^m$ with $s = 2^{\frac{m-1}{2}} + 2^i - 1$

In his 1968 paper [11], Golomb mentioned a conjecture of Welch stating that for $m = 2t+1$, the power function $x \mapsto x^s$ with $s = 2^t + 3$ is AB on $\mathbf{F}_{2^m}$. Niho [18] stated a similar conjecture for $s = 2^t + 2^{\frac{t}{2}} - 1$ when t is even and $s = 2^t + 2^{\frac{3t+1}{2}} - 1$ when t is odd. Note that all of these exponents s can be written as $2^t + 2^i - 1$ for some i. Since both Welch's and Niho's functions are APN [9,8], Corollary 3 leads to the following formulation of Welch's and Niho's conjectures:
Let $m = 2t + 1$ be an odd integer. For all u such that $1 \leq u \leq 2^m - 1$, we have

$$w_2((2^t + 2^i - 1)u \bmod (2^m - 1)) \leq t + w_2(u) \tag{3}$$

for the following values of i: $i = 2$, $i = t/2$ for even t and $i = (3t+1)/2$ for odd t. We proved that Condition (3) is satisfied in the Welch case ($i = 2$) [4,3]. More recently Xiang and Hollmann used this formulation for proving Niho's conjecture [12]. We here focus on all other values of s which can be expressed as $s = 2^t + 2^i - 1$ for some i. We prove that for almost all of these values $x \mapsto x^s$ is not AB on $\mathbf{F}_{2^m}$. This result is derived from both following lemmas which give an upper bound on the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$.

Lemma 1. *Let $m = 2t+1$ be an odd integer and $s = 2^t + 2^i - 1$ with $2 < i < t-1$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. If 2^ℓ denotes the exact divisibility of $\mathcal{C}_{1,s}^{\perp}$, we have*

- *if* $t \equiv 0 \bmod i$ *and* $i \neq t/2$, *then* $\ell \leq t-1$,
- *if* $t \equiv 1 \bmod i$, *then* $\ell \leq t-i+2$,
- *if* $t \equiv r \bmod i$ *with* $1 < r < i$, *then* $\ell \leq t-i+r$.

Proof. Let $t = iq+r$ with $r < i$ and $A(u) = (2^t+2^i-1)u \bmod 2^m-1$. McEliece's theorem (Corollary 2) implies that $\mathcal{C}_{1,s}^{\perp}$ is at most 2^ℓ-divisible if there exists an integer $u \in \{0,\ldots,2^m-1\}$ such that $w_2(A(u)) = w_2(u)+2t-\ell$. We here exhibit an integer u satisfying this condition for the announced values of ℓ.

- We first consider the case $r \neq 0$. Let $u = 2^t + 2^{r-1}\sum_{k=1}^{q} 2^{ik} + 1$. Then $w_2(u) = q+2$ and we have

$$A(u) = 2^{2t} + 2^{t+r-1}\sum_{k=1}^{q} 2^{ik} + 2^{t+i} + (2^{t+i-1} - 2^{i+r-1}) + (2^i - 1)\ . \quad (4)$$

  If $r > 1$, we have $t+i < t+r-1+ik \leq 2t-1$ for all k such that $1 \leq k \leq q$. All terms in (4) are then distinct. It follows that

$$w_2(A(u)) = 1+q+1+(t-r)+i = w_2(u)+t-r+i\ .$$

  If $r = 1$, we obtain

$$A(u) = 2^{2t} + 2^t\sum_{k=2}^{q} 2^{ik} + 2^{t+i+1} + 2^{t+i-1} - 1\ .$$

  In this case

$$w_2(A(u)) = 1+(q-1)+1+(t+i-1) = w_2(u)+t+i-2\ .$$

- Suppose now that $r = 0$ and $i \neq t/2$. Since $i < t$, we have $q > 2$. Let $u = 2^{t+i} + 2^{t+2} + 2^t + 2^{i+2}\sum_{k=0}^{q-2} 2^{ik} + 1$. Using that $i > 2$, we deduce that $i+2+ik \leq i(q-1)+2 \leq t-i+2 < t$ for all $k \leq q-2$. It follows that $w_2(u) = q+3$. Let us now expand the corresponding $A(u)$:

$$A(u) = 2^{2t} + \sum_{k=0}^{q-3} 2^{t+2+(k+2)i} + 2^{t+2i} + 2^{t+i+3} - 2^{i+2} + 2^i + 2^{i-1} + 1\ . \quad (5)$$

  If $i > 2$, all values of k such that $0 \leq k \leq q-3$ satisfy $t+2i < t+2+(k+2)i < 2t$. We then deduce that, if $q > 2$, all the terms in (5) are distinct except if $i = 3$. It follows that, for any $i > 3$,

$$w_2(A(u)) = 1+(q-2)+1+(t+1)+3 = w_2(u)+t+1\ .$$

  For $i = 3$, we have

$$A(u) = 2^{2t} + \sum_{k=0}^{q-3} 2^{t+3k+8} + 2^{t+7} - 2^5 + 2^3 + 2^2 + 1\ .$$

  In this case

$$w_2(A(u)) = 1+(q-2)+(t+2)+3 = w(u)+t+1\ .$$

◇

Lemma 2. *Let $m = 2t+1$ be an odd integer $s = 2^t + 2^i - 1$ with $t+1 < i < 2t$. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$. If 2^ℓ denotes the exact divisibility of $\mathcal{C}_{1,s}^\perp$, we have*

- *if $t+1 < i < \frac{3t+1}{2}$, then $\ell \leq m - i$,*
- *if $\frac{3t+1}{2} < i < 2t-1$, then $\ell \leq 2(m-i) - 1$,*
- *if $i = 2t-1$, then $\ell \leq 3$.*

Proof. Let $A(u) = (2^t + 2^i - 1)u \bmod (2^m - 1)$. Exactly as in the proof of the previous lemma, we exhibit an integer $u \in \{0, \ldots, 2^m - 1\}$ such that $w_2(A(u)) = w_2(u) + 2t - \ell$ for the announced values of ℓ. We write $i = t + j$ where $1 < j < t$.

- We first consider the case $t + 1 < i < \frac{3t+1}{2}$. Let $u = 2^t + 2^{j-1} + 1$. Then $w_2(u) = 3$ and

$$A(u) = 2^{2t} + 2^{t+2j-1} + 2^{t+j} + 2^{t+j-1} - 1 \ . \tag{6}$$

  Since $j < \frac{t+1}{2}$, we have that $2t > t + 2j - 1$. All the terms in (6) are therefore distinct. We deduce

$$w_2(A(u)) = 3 + (t + j - 1) = w_2(u) + i - 1 \ .$$

- We now focus on the case $\frac{3t+1}{2} < i \leq 2t - 1$. Let $u = 2^t + 2^j + 1$. Then $w_2(u) = 3$ and

$$A(u) = 2^{2t} + 2^{t+j+1} - 2^{j-1} + 2^{2j-t-1} - 1 \ . \tag{7}$$

  Since $\frac{t+1}{2} < j < t$, we have $0 < 2j - t - 1 < j - 1$. If $j \neq t - 1$, all the exponents in (7) are distinct. It follows that

$$w_2(A(u)) = 1 + (t + 2) + (2j - t - 1) = w_2(u) + 2(i - t) - 1 \ .$$

  If $j = t - 1$, we have

$$A(u) = 2^{2t+1} - 2^{j-1} + 2^{2j-t-1} - 1 \ .$$

  In this case

$$w_2(A(u)) = (2t + 1) - (t - j) = w_2(u) + 2t - 3 \ .$$

◇

From both lemma 1 and 2 we deduce the following theorem:

Theorem 5. *Let $m = 2t + 1$ be an odd integer and let $s = 2^t + 2^i - 1$ with $i \in \{1, \ldots, 2t\}$. The only values of i such that $x \mapsto x^s$ is AB on $\mathbf{F}_{2^m}$ are $1, 2, \frac{t}{2}, t, t+1, \frac{3t+1}{2}, 2t$ and maybe $t - 1$.*

Proof. If $i \notin \{1, 2, \frac{t}{2}, t-1, t, t+1, \frac{3t+1}{2}, 2t\}$, $\mathcal{C}_{1,s}^\perp$ is not 2^t-divisible since the upper bounds given in both previous lemmas are strictly less than t. It follows from Theorem 4 that the corresponding power functions are not AB. Moreover $x \mapsto x^s$ is AB for $i \in \{1, 2, \frac{t}{2}, t, t+1, \frac{3t+1}{2}, 2t\}$:

- $i = 1$ corresponds to a quadratic function,
- $i = 2$ corresponds to the Welch's function,
- $i = t$ corresponds to the inverse of a quadratic function since $(2^{t+1} - 1)(2^t + 1) \equiv 2^t \bmod 2^m - 1$.
- $i = t + 1$ corresponds to a Kasami's function since $2^t(2^{t+1} + 2^t - 1) \equiv 2^{2t} - 2^t + 1 \bmod 2^m - 1$.
- $i = 2t$ gives an s which is in the same 2-cyclotomic coset as $2^{t+1} - 1$.
- $i = \frac{t}{2}$ or $i = \frac{3t+1}{2}$ corresponds to the Niho's function. ◇

The only unresolved case is then $i = t-1$. In accordance with our simulation results for $m \leq 39$ we conjecture that the dual of the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, 2^t + 2^{t-1} - 1\}$ is exactly 2^t-divisible. For $m = 5$ and $m = 7$ the function $x \mapsto x^s$ for $s = 2^t + 2^{t-1} - 1$ is AB since it respectively corresponds to a quadratic function and to the Welch function. On the contrary it is known that this power function is not APN when 3 divides m since $\mathcal{C}_{1,s}$ has minimum distance 3 in this case [7, Th. 5]. We actually conjecture that for any odd $m \geq 9$ the function $x \mapsto x^s$ with $s = 2^t + 2^{t-1} - 1$ is not APN on $\mathbf{F}_{2^m}$.

5 AB Power Functions on $\mathbf{F}_{2^m}$ when m Is Not a Prime

We now focus on AB power functions on $\mathbf{F}_{2^m}$ when m is not a prime. We show that in this case the nonlinearity of $x \mapsto x^s$ on $\mathbf{F}_{2^m}$ is closely related to the nonlinearity of the power $x \mapsto x^{s_0}$ on $\mathbf{F}_{2^g}$ where g is a divisor of m and $s_0 = s \bmod (2^g - 1)$.We first derive an upper bound on the exact weight divisibility of $\mathcal{C}_{1,s}^{\perp}$ from the exact weight divisibility of the code $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^g - 1)$.

Proposition 3. *Let g be a divisor of m. Let $\mathcal{C}_{1,s}$ be the binary cyclic code of length $(2^m - 1)$ with defining set $\{1, s\}$ and $\mathcal{C}_0$ the binary cyclic code of length $(2^g - 1)$ with defining set $\{1, s_0\}$ where $s_0 = s \bmod (2^g - 1)$. Assume that $\mathcal{C}_0^{\perp}$ is exactly 2^ℓ-divisible. Then $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible.*

Proof. Let $s = s_0 + a(2^g - 1)$. We here use McEliece's theorem as expressed in Corollary 1. If $\mathcal{C}_0^{\perp}$ is exactly 2^ℓ-divisible, there exists a pair of integers (u_0, v_0) with $u_0 \leq 2^g - 1$ and $v_0 \leq 2^g - 1$ such that

$$u_0 s_0 + v_0 \equiv 0 \bmod 2^g - 1 \text{ and } w_2(u_0) + w_2(v_0) = \ell + 1$$

Let us now consider both integers u and v defined by

$$u = u_0 \frac{2^m - 1}{2^g - 1} \text{ and } v = v_0 \frac{2^m - 1}{2^g - 1}$$

For $s = s_0 + a(2^g - 1)$, the pair (u, v) satisfies

$$us + v = u_0 a(2^m - 1) + \frac{2^m - 1}{2^g - 1}(u_0 s_0 + v_0) \equiv 0 \bmod (2^m - 1) .$$

Since $\frac{2^m-1}{2^g-1} = \sum_{i=0}^{m/g-1} 2^{ig}$ and both u_0 and v_0 are less than $2^g - 1$, we have

$$w_2(u) + w_2(v) = \frac{m}{g}\,(w_2(u_0) + w_2(v_0)) = \frac{m}{g}(\ell + 1)\ .$$

We then deduce that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible. ◇

We now derive a necessary condition on the values of the exponents which provide AB power functions.

Theorem 6. *Let m be an odd integer. The power function $x \mapsto x^s$ is not AB on $\mathbf{F}_{2^m}$ if there exists a divisor g of m with $g > 1$ satisfying one of the following conditions:*

1. $\exists i,\ 0 \le i < g,\ \ s \equiv 2^i \bmod (2^g - 1)$,
2. $s_0 = s \bmod (2^g - 1) \neq 2^i$ *and the dual of the cyclic code of length* $(2^g - 1)$ *with defining set* $\{1, s_0\}$ *is not* $2^{\frac{g-1}{2}}$*-divisible.*

Proof. Theorem 4 provide a necessary condition for obtaining an AB power function on $\mathbf{F}_{2^m}$: this function has to be APN and $\mathcal{C}_{1,s}^{\perp}$ has to be $2^{\frac{m-1}{2}}$-divisible. When $s \equiv 2^i \bmod (2^g - 1)$, it is known [7] that the cyclic code $\mathcal{C}_{1,s}$ has minimum distance 3. It follows that $x \mapsto x^s$ is not APN in this case. Suppose now that the dual of the cyclic code of length $(2^g - 1)$ with defining set $\{1, s_0\}$ is exactly 2^ℓ-divisible. According to the previous theorem we have that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m}{g}(\ell+1)}$-divisible. If $\mathcal{C}_{1,s}^{\perp}$ is $2^{\frac{m-1}{2}}$-divisible, it therefore follows that

$$\frac{m-1}{2} \le \frac{m}{g}(\ell + 1) - 1\ .$$

This gives

$$\ell + 1 \ge \frac{g(m+1)}{2m} > \frac{g-1}{2}$$

since $(m+1)g > m(g-1)$. This implies that $\mathcal{C}_0^{\perp}$ is $2^{\frac{g-1}{2}}$-divisible. ◇

Example 1. We search for all AB power permutations on $\mathbf{F}_{2^{21}}$. We here use that the cyclic codes $\mathcal{C}_{1,s_0}^{\perp}$ of length $(2^7 - 1)$ are at most 4-divisible when $s_0 \in \{7, 19, 21, 31, 47, 55, 63\}$ (and for their cyclotomic conjugates). Amongst the 42340 possible pairs of exponents (s, s^{-1}) such that $\gcd(s, 2^{21} - 1) = 1$ (up to equivalence), only 5520 satisfy both conditions expressed in Corollary 4 and Theorem 6. By testing the weight divisibility of the corresponding cyclic codes as described in Corollary 3 we obtain that only 20 such pairs correspond to a 2^{10}-divisible code $\mathcal{C}_{1,s}^{\perp}$. The corresponding values of $\min(s, s^{-1})$ are:

$$\{3, 5, 13, 17, 33, 241, 257, 993, 1025, 1027, 1055, 3071, 8447\}$$
$$\cup\ \{171, 16259, 31729, 49789, 52429, 123423, 146312\}\ .$$

The exponents lying in the first set are known to provide AB functions (see Table 2). We finally check that the power functions corresponding to the second set of exponents are not APN.

We now exhibit another family of power functions which are not AB:

Proposition 4. *Let m be an odd integer. If there exists a divisor g of m such that s satisfies*

$$s \equiv -s_0 \bmod \frac{2^m-1}{2^g-1} \text{ with } 0 < s_0 < \frac{2^m-1}{2^g-1} \text{ and } w_2(s_0) \leq \frac{1}{2}\left(\frac{m}{g}-3\right)$$

then the power function $x \mapsto x^s$ is not AB on $\mathbf{F}_{2^m}$.

Proof. If the power function $x \mapsto x^s$ is AB on $\mathbf{F}_{2^m}$, we have that the dual of the cyclic code $\mathcal{C}_{1,s}$ of length (2^m-1) with defining set $\{1,s\}$ is $2^{\frac{m-1}{2}}$-divisible. We here use McEliece's theorem as formulated in Corollary 2. Let $u = 2^g - 1$. Then we have

$$A(u) = us \bmod 2^m - 1 = (2^m-1) - (2^g-1)s_0 \ .$$

We obtain that $w_2(A(u)) = m - w_2((2^g-1)s_0)$. Since $w_2((2^g-1)s_0) \leq g w_2(s_0)$, this implies that

$$\begin{aligned} w_2(A(u)) &\geq m - g w_2(s_0) \\ &\geq w_2(u) + m - g(w_2(s_0)+1) > w_2(u) + \frac{m-1}{2} \end{aligned}$$

when $w_2(s_0) \leq \frac{1}{2}\left(\frac{m}{g}-3\right)$. It follows that $\mathcal{C}_{1,s}^{\perp}$ is not $2^{\frac{m-1}{2}}$-divisible. ◇

The third author conjectured that for $m = 5g$ the function $x \mapsto x^s$ with $s = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ is APN on $\mathbf{F}_{2^m}$ [8]. The previous corollary implies:

Proposition 5. *Let m be an odd integer such that $m = 5g$. The power function $x \mapsto x^s$ with $s = 2^{4g} + 2^{3g} + 2^{2g} + 2^g - 1$ is not AB on $\mathbf{F}_{2^m}$.*

Proof. Since $s = \frac{2^{5g}-1}{2^g-1} - 2$, we apply the previous corollary with $s_0 = 2$ and $m/g = 5$ using that

$$w_2(s_0) = 1 = \frac{1}{2}\left(\frac{m}{g}-3\right) \ .$$

◇

References

1. T. Beth and C. Ding. On almost perfect nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 65–76. Springer-Verlag, 1993.
2. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.
3. A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. Submitted.
4. A. Canteaut, P. Charpin, and H. Dobbertin. Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs: conjecture de Welch. *Comptes Rendus de l'Académie des Sciences de Paris*, t. 328, Série I, pages 173–178, 1999.

5. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15:125–156, 1998.
6. F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT'94*, number 950 in Lecture Notes in Computer Science, pages 356–365. Springer-Verlag, 1995.
7. P. Charpin, A. Tietäväinen, and V. Zinoviev. On binary cyclic codes with minimum distance $d = 3$. *Problems of Information Transmission*, 33(4):287–296, 1997.
8. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information and Computation*, 1998. To appear.
9. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 1998. To appear.
10. R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Transactions on Information Theory*, 14:154–156, 1968.
11. S.W. Golomb. Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences. *Information Sciences*, 1:87–109, 1968.
12. H.D.L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Submitted.
13. T. Kasami. Weight distributions of Bose-Chaudhuri-Hocquenghem codes. In *Proceedings of the conference on combinatorial mathematics and its applications*, pages 335–357. The Univ. of North Carolina Press, 1968.
14. T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.
15. F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland, 1977.
16. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science. Springer-Verlag, 1994.
17. R.J. McEliece. Weight congruence for p-ary cyclic codes. *Discrete Mathematics*, 3:177–192, 1972.
18. Y. Niho. *Multi-valued cross-correlation functions between two maximal linear recursive sequences*. PhD thesis, Univ. Southern California, 1972.
19. K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 55–64. Springer-Verlag, 1993.
20. K. Nyberg. Linear approximation of block ciphers. In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT'94*, number 950 in Lecture Notes in Computer Science. Springer-Verlag, 1994.
21. K. Nyberg and L.R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, number 740 in Lecture Notes in Computer Science, pages 566–574. Springer-Verlag, 1993.
22. V. Pless. Power moment identities on weight distributions in error-correcting codes. *Info. and Control*, 3:147–152, 1963.
23. D.V. Sarwate and M.B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, 68(5):593–619, 1980.
24. V.M. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12:197–201, 1971.