Designs, Codes and Cryptography, 15, 125–156 (1998)

Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems

CLAUDE CARLET
GREYC, Université de Caen, 14032 Caen Cedex, France

PASCALE CHARPIN
INRIA,Codes,Domaine de Voluceau-Rocquencourt, BP 105 - 78153, Le Chesnay, France

VICTOR ZINOVIEV
Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow 101447, Russia

Communicated by: D. Jungnickel

Received August 5, 1997; Revised January 27, 1998; Accepted February 4, 1998

Abstract. Almost bent functions oppose an optimum resistance to linear and differential cryptanalysis. We present basic properties of almost bent functions; particularly we give an upper bound on the degree. We develop the "coding theory" point of view for studying the existence of almost bent functions, showing explicitly the links with cyclic codes. We also give new characterizations of almost bent functions by means of associated Boolean functions.

Keywords: almost perfect nonlinear, almost bent, bent, Boolean function, sequence, linear code, cyclic code

1. Introduction

We denote by V_m the set $GF(2)^m$ of all binary words of length m and study the functions from V_m to itself. Let F be such a function, the Fourier transform of F, whose value at $(a,b) \in {V_m}^2$, is equal to:

$$\mu_F(a,b) = \sum_{x \in V_m} (-1)^{\langle b,F(x)\rangle + \langle a,x\rangle} \ , \tag{1}$$

where "$\langle \, , \rangle$" is the usual inner product on V_m, plays a role in several topics of information theory such as

- sequences (e.g. m-sequences, cf. [21]);
- correlation-immune and resilient functions (cf. [6], Theorem 5);
- permutations suitable for block ciphers (cf. [10, 31]).

We focus in this paper on the study of those functions F for which $\mu_F(a,b)$ takes the values 0 and $\pm 2^{\frac{m+1}{2}}$ only (m odd), when a ranges over V_m and b ranges over $V_m^* = V_m \setminus \{0\}$.

This problem is one of most interest in the study of m-sequences: when F is a power function $x \to F(x) = x^t$, viewed as a function from the Galois field $GF(2^m)$ to itself, this corresponds to the fact that two m-sequences $(\alpha^i)_{i=0,\ldots,2^m-2}$ and $(\alpha^{ti})_{i=0,\ldots,2^m-2}$ (where α is a primitive element of $GF(2^m)$) have a *preferred* crosscorrelation function – see a recent result in [5].

It is also a central problem in the study of permutations suitable for DES-like cryptosystems: recall that the functions that oppose an optimum resistance to linear cryptanalysis (cf. [30]) are the *almost bent* (AB) functions (cf. [10]), i.e. those functions such that the maximum of the magnitude of $\mu_F(a,b)$, when a ranges over V_m and b ranges over V_m^*, reaches the lower bound $2^{\frac{m+1}{2}}$, or equivalently those functions such that the minimum distance between the set of all the functions $\langle b, F\rangle,\ b \in V_m^*$, and the set of all affine functions from V_m into $GF(2)$ is the largest. Note that AB functions do not exist when m is even. Chabaud and Vaudenay have re-discovered in [10] the bound quoted above that was originally proved by Sidel'nikov in [35].

AB functions have the property that $\mu_F(a,b)$ takes the values 0 and $\pm 2^{\frac{m+1}{2}}$ only, when a ranges over V_m and b ranges over V_m^*. Any AB function is *almost perfect nonlinear* (APN), i.e. opposes an optimum resistance to differential cryptanalysis (cf. [3, 32]): for any nonzero vector a and any vector b, the equation $F(x) + F(x+a) = b$ admits at most two solutions in V_m.

Recall that Nyberg [32] proposed two examples of APN functions, which are permutations on the space V_m, identified to the Galois field $GF(2^m)$. These permutations are the power functions $x \rightarrow x^{2^i+1}$, where i is co-prime with m, and $x \rightarrow x^{2^m-2}$. Chabaud and Vaudenay observed later that, for odd m, the first one of these functions is AB and the other is not.

Actually these last results are known in coding theory, as properties of some cyclic codes. Moreover, another infinite class of AB permutations can be deduced from Remark 3 of [24], page 379, by Kasami: for any i such that i is co-prime with m, the function $x \rightarrow x^{2^{2i}-2^i+1}$ is AB. Since the work of Kasami, no other infinite class of AB functions was discovered. There exist also two conjectures (cf. [27]). The first one is due to Welch: *the function $F(x) = x^t$, where $t = 2^i + 3$ and $i = (m-1)/2$, is AB.* The second one is due to Niho: *the function $F(x) = x^s$, where $s = 2^i + 2^{\frac{3i+1}{2}} - 1$ if $i = (m-1)/2$ is odd and $s = 2^i + 2^{\frac{i}{2}} - 1$ if $i = (m-1)/2$ is even, is AB.*

In Section 2, we recall the definitions and present some basic properties of APN and AB functions. We study the transformations that let globally invariant the set of AB (resp. APN) functions. Our main result is an upper bound on the degree of any AB function.

In Section 3 we develop another point of view for studying the existence of APN and of AB functions, by using *classical* tools of coding theory. We first recall the characterization, due to Kasami [23], of binary codes with parameters $[2^m-1, 2m, d]$ which are *optimal*, in a certain sense. We later show that these optimal codes correspond to AB functions; therefore we prove that AB functions correspond to uniformly packed codes with external distance three. To conclude, we explain how the primitive cyclic codes appear in this context and how their parameters could be used. Particularly we develop the links with the study of cyclic codes with two zeros.

We give in Section 4 new characterizations of AB functions, by establishing several links between the notion of AB function and that of bent Boolean function. A function F from V_m to V_m being given, we define a Boolean function γ_F on $V_m \times V_m$ such that F is APN if and only if γ_F has weight $2^{2m-1} - 2^{m-1}$ and F is AB if and only if γ_F is bent. We give a sufficient condition for a function F to be AB that involves bent functions on V_{m+1}.

2. AB and APN Functions

Definition 1 *The function F is said to be* almost perfect nonlinear *(APN) if all the equations*

$$F(x) \ + \ F(x+a) \ = \ b \ , \ \ a,b \in V_m \ , \ a \neq 0 \ , \tag{2}$$

have no more than two solutions in V_m.

Clearly, (2) must have then either 0 or 2 solutions.

Definition 2 *The function F is said to be an* almost bent *(AB) function if the numbers $\mu_F(a,b)$, given by (1), are equal to 0 and $\pm 2^{\frac{m+1}{2}}$ only, when $a \in V_m$ and $b \in V_m^*$ (or, equivalently, when $a,b \in V_m;\ (a,b) \neq (0,0)$).*

AB functions exist only when m is odd. *We will always assume m to be odd when we study AB functions*.
Definition 2 does not depend on a particular choice of the inner product in V_m. If we identify V_m with $GF(2^m)$, we can take $\langle x,y\rangle = tr(xy)$ in relation (1), where $tr(x) = x + x^2 + \cdots + x^{2^{m-1}}$ is the trace function from $GF(2^m)$ to $GF(2)$.

2.1. Properties of Stability

Let us recall the properties of stability of APN functions given by Nyberg [32] and give some others. We check that these properties are also valid for AB functions. We give the proofs of the new results, only, since all these results are easy to prove.

Proposition 1 *The right and the left compositions of an APN (resp. AB) function by an affine permutation are APN (resp. AB). The inverse of an APN (resp. AB) permutation is APN (resp. AB).*

Proof: Let F be AB and L be a linear permutation (the case of an affine permutation is similar); $\mu_{L\circ F}(a,b)$ is equal to $\mu_F(a, L^*(b))$ where L^* is the adjoint operator of L (i.e. where for any $x,\ y \in V_m$ we have: $\langle x, L(y)\rangle \ = \ \langle L^*(x), y\rangle$). If "$\langle\, ,\rangle$" is the usual inner product, L^* is the linear permutation whose matrix is transposed of that of L. We have also $\mu_{F\circ L}(a,b) = \mu_F(L^{-1*}(a), b)$ and $\mu_{F^{-1}}(a,b) = \mu_F(b,a)$. ■

Proposition 2 *Let $F(x)$ be an APN function (resp. an AB function) from V_m to itself, and $A(x)$ an affine function. Then the function $F(x) + A(x)$ is APN (resp. AB).*

The proof is straightforward. Notice that Proposition 2 implies the existence of non-bijective AB functions: obviously, for any permutation F, there exist linear functions L such that $F + L$ is non-bijective (choose two distinct vectors u and v and take L such that $L(u) + L(v) = F(u) + F(v)$).
Remark 1. (a) Because of Proposition 2, it is possible to assume without loss of generality that $F(x)$ does not contain a constant term, i.e. $F(0) = 0$.
(b) We conjecture that the following statement holds: *for any AB function F, there exists a linear function L such that $F + L$ is a permutation.*

Let F_1 be a function from V_m to itself and F_2 a permutation on V_m. By definition, $F_1 \circ {F_2}^{-1}$ is APN if and only if, for any nonzero element (a,b) of ${V_m}^2$, the system:

$$\begin{cases} F_1 \circ {F_2}^{-1}(x) + F_1 \circ {F_2}^{-1}(y) &= b \\ x + y &= a \end{cases}$$

admits at most two solutions (x,y).
Changing x and y into $F_2(x)$ and $F_2(y)$, we deduce that the function $F_1 \circ {F_2}^{-1}$ is APN if and only if the system:

$$\begin{cases} F_1(x) + F_1(y) &= b, \\ F_2(x) + F_2(y) &= a \end{cases}$$

admits at most two solutions (x,y). We then deduce.

Proposition 3 *Let F be an APN (resp. AB) function on V_m and L_1, L_2 be two linear functions from ${V_m}^2$ to V_m. Assume that (L_1, L_2) is a permutation on ${V_m}^2$ and that the function $F_2(x) = L_2(F(x), x)$ is a permutation on V_m. Then, the function $F_1 \circ F_2^{-1}$, where $F_1(x) = L_1(F(x), x)$ is APN (resp. AB).*

Proof: Let F be an APN function (for AB functions, see Corollary 5). The function $F_1 \circ F_2^{-1}$ is APN if and only if the following system with unknown (x,y):

$$\begin{cases} F_1(x) + F_1(y) &= b \\ F_2(x) + F_2(y) &= a \end{cases}$$

admits at most two solutions for any nonzero vector (a,b), or equivalently, denoting by (a', b') the unique ordered pair such that $(L_1, L_2)(b', a') = (b, a)$ and applying the inverse permutation of (L_1, L_2), the system:

$$\begin{cases} F(x) + F(y) &= b' \\ x + y = a' \end{cases}$$

admits at most two solutions (x,y) for any nonzero vector (a', b'). ∎

All the transformations we have seen above, that respect APN (resp. AB) property, are particular cases of this general one:
- if $(L_1, L_2)(b,a) = (a,b)$, then $F_1 \circ F_2^{-1}$ is equal to F^{-1};
- if $L_1(b,a)$ and $L_2(b,a)$ depend only on b and a, respectively, this corresponds to the right and left compositions of F by linear permutations;
- if $L_1(b,a) = b + L(a)$ and $L_2(b,a) = a$ where L is any linear function from V_m to itself, then we obtain $F(x) + L(x)$.

2.2. A Bound on the Degree

The notion of AB function is close to that of bent function. Recall that for any positive even m, a Boolean function f on V_m (i.e. a function from V_m to $GF(2)$) is called *bent* if, for every $a \in V_m$, the character sum:

$$\sum_{x\in V_m}(-1)^{f(x)+\langle a,x\rangle}$$

is equal to $\pm 2^{\frac{m}{2}}$. A function F from V_m (m even) to V_k is called *bent* if all the Boolean functions $\langle b,F\rangle$ ($b\in V_k^*$) are bent, i.e. if for any $b\in V_k^*$ and any $a\in V_m$, we have: $\mu_F(a,b)=\pm 2^{\frac{m}{2}}$. Such functions exist if and only if $m\geq 2k$ (cf. [31]).
There exists an upper bound on the algebraic degree of any bent function (cf. [33]). We shall obtain an upper bound on the algebraic degree of any AB function. We first recall what is the algebraic degree of a function.
There exist two representations of a function F from V_m to V_m:

1. In the first one, F is considered as a function from $GF(2^m)$ to itself. It admits a unique representation as a polynomial of degree smaller than 2^m, in one variable over $GF(2^m)$:

$$F(x) \;=\; \sum_{j=0}^{2^m-1}\delta_j x^j\ ,\ \ \delta_j\in GF(2^m)\ . \tag{3}$$

   F is linear if and only if $F(x)$ is a *linearized polynomial* over $GF(2^m)$:

$$\sum_{j=0}^{m-1}\delta_j x^{2^j}\ ,\ \ \delta_j\in GF(2^m)\ . \tag{4}$$

   It is called an affine function if it is the sum of a linear function and of a constant one.

2. In the second one, F is uniquely represented as a polynomial in m variables with coefficients in V_m (that can be identified to $GF(2^m)$):

$$\underline{F}(x_1,\cdots,x_m)=\sum_{u\in V_m}\delta(u)\left(\prod_{j=1}^{m}{x_j}^{u_j}\right).$$

   This polynomial is called the algebraic normal form of F.

The way to obtain one representation from the other is the following: change x into the expression $\sum_{j=1}^m x_j\alpha^{j-1}$, where α is a primitive element of $GF(2^m)$. We have:

$$\begin{aligned}\underline{F}(x_1,...,x_m) &= F(\sum_{j=1}^{m}x_j\alpha^{j-1})\\ &= \sum_{i=0}^{2^m-1}\delta_i\left(\sum_{j=1}^{m}x_j\alpha^{j-1}\right)^i\\ &= \sum_{i=0}^{2^m-1}\delta_i\left(\sum_{j=1}^{m}x_j\alpha^{j-1}\right)^{\sum_{s=0}^{m-1}i_s2^s}\\ &= \sum_{u\in V_m}\delta(u)\left(\prod_{j=1}^{m}{x_j}^{u_j}\right)\ .\end{aligned}$$

The algebraic degree of F is the degree of the polynomial $\underline{F}(x_1, ..., x_m)$. It can be expressed by means of the exponents of $F(x)$.

Definition 3 *Let j be any integer in the range $[0, 2^m - 1]$. Consider the binary expansion of j :*

$$j \;=\; \sum_{s=o}^{m-1} j_s 2^s \;,\; j_s \in \{0,1\} \;.$$

The 2*-weight $w_2(j)$ of j is the number of nonzero coefficients j_s, i.e.* $w_2(j) \;=\; \sum_{s=0}^{m-1} j_s \;.$

Definition 4 *Let $F(x)$ be a polynomial given by expression (3). $F(x)$ has* 2*-degree D if D is the maximum* 2*-weight of its exponents:*

$$D \;=\; max\;\{\; w_2(j) \;:\; 0 \le j \le 2^m - 1,\; \delta_j \neq 0 \;\}. \tag{5}$$

The algebraic degree of F is then equal to the 2-degree of $F(x)$.

It is well known that the algebraic degree of a bent function on V_m is at most $\frac{m}{2}$ (cf. [33]). The following statement gives us also a bound on the algebraic degree of an AB function.

Theorem 1 *Let F be any function on $GF(2^m)$. If F is AB, then the algebraic degree of F is less than or equal to $(m + 1)/2$.*

Proof:

$$\underline{F}(x_1, ..., x_m) \;=\; \sum_{u \in GF(2^m)} \delta(u)\; {x_1}^{u_1} \cdots {x_m}^{u_m} \;.$$

For any nonzero $b \in V_m$ define the Boolean function f:

$$f(x_1, ..., x_m) \;=\; \sum_{u \in GF(2^m)} \langle \delta(u), b \rangle \; {x_1}^{u_1} \cdots {x_m}^{u_m} \;.$$

It is clear that for any b the degree of f is at most equal to the algebraic degree of $F(x)$, and there exists b for which these degrees are equal. Therefore the algebraic degree of F is bounded by $(m+1)/2$ if and only if, for any nonzero $b \in V_m$, the Boolean function $\langle b, F \rangle$ has degree less than or equal to $(m+1)/2$.

Let g be the Möbius transform of f. That is for all $u \in V_m$,

$$g(u) = \sum_{v \in V_m,\; v \preceq u} f(v) \;,$$

this sum being computed in $GF(2)$, and where $v \preceq u$, for binary vectors $v = (v_1, \ldots, v_m)$ and $u = (u_1, \ldots, u_m)$, means that the condition $v_i = 1$ implies $u_i = 1$. One says that *the binary vector u covers the binary vector v*. Let $wt(u)$ denote the Hamming weight of u, i.e. the number of its nonzero symbols. The algebraic normal form of the Boolean function f is equal to (cf. Th. 1, p. 372 in [29]):

$$f(x_1,...,x_m) \ = \ \sum_{u\in V_m} g(u)\left(\prod_{i=1}^{m} x_i^{u_i}\right) \ ,$$

this sum being computed in $GF(2)$. Therefore, to prove the theorem, we have to prove that for any u, such that $wt(u) > (m+1)/2$, the value of $g(u)$ equals zero. Now denote by $\widehat{f}$ the Walsh transform of f:

$$\widehat{f}(u) = \sum_{v\in V_m} f(v)\,(-1)^{\langle u,v\rangle} \ ,$$

the sum being computed in **Z**. Using the inverse transform, we have

$$f(v) = 2^{-m} \sum_{w\in V_m} \widehat{f}(w)(-1)^{\langle v,w\rangle},$$

and then

$$\begin{aligned} g(u) \ &= \ 2^{-m}\sum_{v\preceq u}\sum_{w\in V_m} \widehat{f}(w)\,(-1)^{\langle v,w\rangle} \text{ [mod 2]} \\ &= \ 2^{-m}\sum_{w\in V_m}\widehat{f}(w)\left(\sum_{v\preceq u}(-1)^{\langle v,w\rangle}\right) \text{ [mod 2].} \end{aligned}$$

The set $E_u = \{v \in V_m \,|\, v \preceq u\}$ is a vector subspace of V_m. Its dimension is $wt(u)$. We know that for any subspace E of V_m and any word w, the sum $\sum_{v\in E}(-1)^{\langle v,w\rangle}$ is nonzero if and only if w belongs to the orthogonal of E, that is the linear space

$$\{w \in V_m \mid \forall v \in E,\ \langle v,w\rangle = 0\} \ ,$$

in which case its value is equal to the cardinality $|E|$ of E. The orthogonal space ${E_u}^{\perp}$ is equal to $E_{u+\mathbf{1}}$ where $u+\mathbf{1} = (u_1+1,\ldots,u_m+1)$. So

$$g(u) = 2^{wt(u)-m}\sum_{w\in E_{u+\mathbf{1}}}\widehat{f}(w) \ \text{[mod 2].} \tag{6}$$

Let $f_\chi = (-1)^f$. Since F is AB, for any w, the value at w of the Walsh transform of f_χ is equal either to 0 or to $\pm 2^{\frac{m+1}{2}}$, by definition. But we have $f_\chi = 1-2f$, since f is Boolean. The Walsh transform of the constant function 1 is equal to $2^m\Delta_0$, where $\Delta_0(w)$ is the Dirac symbol: $\Delta_0(w) = 1$ if $w = 0$ and 0 otherwise. Thus, the value at w of the Walsh transform of f_χ is equal to $2^m\Delta_0(w) - 2\widehat{f}$. We deduce that, for any w, the value $\widehat{f}(w)$ is divisible by $2^{\frac{m-1}{2}}$. In accordance with (6), we can deduce that $g(u) = 0$ when $wt(u) > (m+1)/2$.

Note that another proof of this property can be found in [8, Lemma 3]. ■

Theorem 1 permits to give another argument of the fact that the power function x^{2^m-2} is not AB, since its algebraic degree is $m-1$, and to eliminate some possible values of t, for which a function $F(x) = x^t$ cannot be AB.

Theorem 2 *Let $g,\ s$ and m be any integers, where $g, s \geq 2$, $gs < m$, and m is odd. Let t be any integer, $1 < t < 2^m - 1$, which can be presented in the ring $\mathbf{Z}_{2^m-1}$ in the following form:*

$$1 + 2^s + 2^{2s} + \cdots + 2^{gs}. \tag{7}$$

Assume the following conditions:

$$gcd(s, m) = 1,\ \textit{and } m \equiv 1 \ (mod\ g + 1)\ . \tag{8}$$

Then $F(x) = x^t$ is not AB.

The proof is based on the following statement, which gives the exact value of the 2-weight of t^{-1} for all the numbers t of the form above.

Lemma 1 *Let $g,\ s$ and m be any integers, where $g \geq 1,\ s \geq 2$ and $gs < m$, and let t be any integer, $1 < t < 2^m - 1$, which can be presented in the ring $\mathbf{Z}_{2^m-1}$ in the form (7). If m is such that $m \equiv 1\ (mod\ g + 1)$ and if $gcd(s, m) = 1$, then the numbers t and $2^m - 1$ are mutually prime and $w_2(t^{-1}) = (gm + 1)/(g + 1)$.*

Proof: Set $u := (m - 1)/(g + 1)$.
Then we have (equality means congruence modulo $2^m - 1$):

$$\begin{aligned}
-1 &= t\ \frac{1 - 2^s}{2^{s(g+1)} - 1} \\
&= t\ \frac{2^{us(g+1)+s} - 2^s}{2^{s(g+1)} - 1} \\
&= t\ 2^s\ \frac{2^{us(g+1)} - 1}{2^{s(g+1)} - 1} \\
&= t\ 2^s\ \left(1 + 2^{s(g+1)} + 2^{2s(g+1)} + ... + 2^{(u-1)s(g+1)}\right).
\end{aligned}$$

Since $gcd(s, m) = 1$, the numbers $(g + 1)s$ and m are co-prime and any two numbers $i(g + 1)s$ and $j(g + 1)s$ are pairwise non-congruent modulo m for distinct $i, j < m$. Thus $w_2(-1/t) = u$, and consequently $w_2(1/t) = m - u = (gm + 1)/(g + 1)$. ■

Proof of Theorem 2: . According to Lemma 1, under the conditions of the theorem, the number t^{-1} has always 2-weight $(gm + 1)/(g + 1)$ which is more than $(m + 1)/2$ for $g \geq 2$. Now if $F(x) = x^t$ is AB, then, according to Proposition 1, $F^{-1}(x) = x^{t^{-1}}$ is also AB. But then, the 2-degree of $x^{t^{-1}}$ exceeds the upper bound of Theorem 1 and therefore x^t can not be AB. ■

This lemma shows that *the bound of Theorem 1 is tight.* Indeed, for the case $g = 1$, the function $F(x) = x^t = x^{1+2^s}$, which is bijective and AB for any s prime to m, has an inverse $F(x) = x^{t^{-1}}$ (which is also AB by Proposition 1), where $w_2(t^{-1}) = (m + 1)/2$.

2.3. AB mappings of Nonprime Lengths

Assume $n = 2^m - 1$ is not a prime number. For any proper divisor g of n, denote by M_g the set of all the multiples of g in $[0,\ n]$.

Theorem 3 *Let*

$$F(x) \ = \ \sum_{i=0}^{n} \delta_i x^i$$

be any polynomial over $GF(2^m)$ such that the condition $\delta_i \neq 0$ implies $i \in M_g$, where g is an arbitrary divisor of $n = 2^m - 1$. Then $F(x)$ is neither a permutation nor an AB function.

Proof: By hypothesis, there exists a polynomial $G(x)$ such that $F(x) = G(x^g)$. Recall that α is a primitive element of $GF(2^m)$. Let $u = n/g$ and $\beta = \alpha^u$. We have $\beta \neq 1$ and $F(\beta x) = G(\beta^g x^g) = G(x^g) = F(x)$. Thus F is not a permutation. F is constant on each set

$$\{\beta^i x \ : \ i = 0, \cdots, g-1\};\ x \in GF(2^m)^\star\ .$$

All these sets have the same cardinality g and define a partition of $GF(2^m)^\star$; thus, the sum

$$\sum_{x \in GF(2^m)^\star} (-1)^{tr(bF(x))}$$

is divisible by g. We deduce that for every b, g is a divisor of $\mu_F(0,b) \pm 1$. Note that $\mu_F(0,b) = 0$ implies $g = 1$ which contradicts the hypothesis.

Suppose that F is AB. Then $\mu_F(0,b)$ is equal to $\pm 2^{\frac{m+1}{2}}$ and g is a divisor of $2^{\frac{m+1}{2}} \pm 1$, which is impossible since $2^{\frac{m+1}{2}} \pm 1$ and $2^m - 1$ are co-prime. ■

Remark 2. The same arguments show that if a power function $F(x) = x^t$ is AB on $GF(2^m)$, then $F(x)$ is a permutation of $GF(2^m)$. But it is easy to show more generally that if $F(x) = x^t$ is APN on $GF(2^m)$, then $gcd(t, 2^m - 1)$ is equal to 1 if m is odd and to 3 if m is even.

3. AB and APN Functions and Codes

3.1. Preliminary Results from Coding Theory

We use standard notation of the algebraic coding theory (see [29]). The *(Hamming) weight* of any vector $x \in V_n$ is denoted by $wt(x)$, and the *(Hamming) distance* between any two vectors x and y from V_n is denoted by $d(x,y)$. Any linear subspace of V_n of dimension k is called a *binary linear code* C and is denoted by $[n,\ k,\ d]$, where d is the *minimum Hamming distance* of C. For $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ from V_n we denote $\langle x,\ y\rangle\ = x_1y_1 + \cdots + x_ny_n$ a inner product in V_n. Any linear $[n,k,d]$ code C is associated with its *dual* $[n, n-k, d^\perp]$ code denoted by $C^\perp$:

$$C^{\perp} \;=\; \{x \in V_n :\; \langle x, c\rangle \;=\; 0,\, \forall\, c \in C\}\;.$$

Denote by ν_i the number of codewords of C of weight i. The vector $(\nu_0, ..., \nu_n)$ is called the *weight enumerator* of C, and the polynomial

$$W_C(x) \;=\; \sum_{i=0}^{n} \nu_i x^i$$

is called the *weight polynomial* of C. For any binary $(r \times n)$ matrix $\mathcal{H}$ define the linear binary code C of length $n :\; C = \{c \in V_n :\; c\mathcal{H}^{\tau} = 0\}$, where $\mathcal{H}^{\tau}$ is the transposed matrix of $\mathcal{H}$. We say that C is defined by the *parity check matrix* $\mathcal{H}$.

Two binary codes C and C' with same parameters are called *equivalent*, if they coincide, up to the order of codewords, after some permutations of the positions of C'.

Identify a vector $c = (c_0, ..., c_{n-1})$ of V_n with the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. A binary linear $[n,\, k,\, d]$ code is *cyclic*, if it is an ideal of the ring $GF(2)[x]/(x^n - 1)$, of the polynomials over $GF(2)$ modulo $(x^n - 1)$. For any such code C there exists a unique monic polynomial $g(x)$, called the *generator polynomial of* C, such that any element $c(x)$ of C can be uniquely expressed in the form: $c(x) = a(x)g(x)$. Denote by $m_i(x)$ the *minimal polynomial* of α^i over $GF(2)$, where α is a *primitive element* of $GF(2^m)$. For any binary cyclic code C of length $n = 2^m - 1$ we have: $g(x) = m_{i_1}(x) \cdots m_{i_s}(x)$; we say that C is defined by the set $\alpha^{i_j},\; j = 1, ..., s$, called its *zero's set*. When $gcd(u,\; 2^m - 1) = 1$, α^u is a primitive element too. Then the cyclic code with zero's set $\{\alpha^{i_j},\; j = 1, ..., s\}$, is equivalent to the cyclic code whose zero's set is $\{(\alpha^u)^{i_j},\; j = 1, ..., s\}$.

We need to define two classical families of binary cyclic codes. The cyclic code of length $2^m - 1$ whose zero's set is

$$T = \bigcup_{i=1}^{d-1} \{\; \alpha^i,\; \alpha^{2i}, \ldots, \alpha^{2^{m-1} i \bmod n}\; \}$$

is called *the narrow-sense primitive BCH code with designed distance* d. Note that implicitly $\alpha^d \not\in T$. This code is a $(d-1)/2$-error-correcting BCH code (see [29, p.201]). The punctured *Reed-Muller code of length* $n = 2^m - 1$ *and order* r*, denoted by* $\mathcal{R}^*(m, r)$ (see [29, p.383]), is the cyclic code with zero's set

$$\{\alpha^i \;: i = 1, ..., 2^m - 2,\; 1 \le w_2(i) \le m - r - 1\},$$

where $w_2(i)$ is the 2-weight of i (see Definition 3).

The interpretation of AB and APN functions in terms of coding theory is based on the following result, which is actually due to Kasami (Theorem 13 in [23]). We give here a more general presentation, including codes of any dimension. For clarity and because we will use these later, we also give the main elements of the proof.

Theorem 4 *Let C be any linear $[n,\, n-k,\, d]$ code with minimum distance $d \ge 3$, where $n = 2^m - 1$ and m is odd. Assume that the dual code $C^{\perp}$, of dimension k, does not contain the all-one vector $\mathbf{1} = (1, ..., 1)$. Let $\eta = (\eta_0, ..., \eta_n)$ (resp. $\nu = (\nu_0, ..., \nu_n)$) be the weight enumerator of the code $C^{\perp}$ (resp. C). Let w_0 be the smallest w such that*

$$\eta_w \;+\; \eta_{2^m-w} \;\neq\; 0\,,\;\; 0 \;<\; w \;<\; 2^{m-1}\,.$$

Then $k \geq m$ and we have the following properties.
(i) *If $k \geq 2m$ then w_0 satisfies*

$$w_0 \;\leq\; 2^{m-1} - 2^{(m-1)/2}\,.$$

Moreover if w_0 is identical with its upper bound, then $\nu_3 = \nu_4 = 0$, $k = 2m$ and the weight distribution of $C^\perp$ is the same as the weight distribution of the dual of the 2-error-correcting BCH code, which is

Weight: w	*Number of words: η_w*
0	1
$2^{m-1} - 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} + 2^{(m-3)/2})$
2^{m-1}	$(2^m - 1)(2^{m-1} + 1)$
$2^{m-1} + 2^{(m-1)/2}$	$(2^m - 1)(2^{m-2} - 2^{(m-3)/2})$

(ii) *If $m \leq k < 2m$, then the minimum distance of C is at most four. Moreover when $w_0 \geq 2^{m-1} - 2^{(m-1)/2}$, one must have:*

$$\nu_3 + \nu_4 \leq \left((2^{m-1} - 1)(2^{3m-3} - 2^{k+m-3})\right)/(3 \cdot 2^{k-1})\,. \tag{9}$$

Sketch of Proof: . The main part of the proof is obtained by means of the first *Pless power moments* [28], actually the first four power moments of the weight distribution of C (and $C^\perp$):

$$\left.\begin{array}{rcl} \sum_{w=0}^{n} w\eta_w &=& 2^{k-1}n, \\[2ex] \sum_{w=0}^{n} w^2\eta_w &=& 2^{k-2}n(n+1), \\[2ex] \sum_{w=0}^{n} w^3\eta_w &=& 2^{k-3}(n^2(n+3) - 3!\,\nu_3), \\[2ex] \sum_{w=0}^{n} w^4\eta_w &=& 2^{k-4}(n(n+1)(n^2+5n-2) + 4!\,(\nu_4 - n\nu_3))\,. \end{array}\right\} \tag{10}$$

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

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

we have for any even ℓ:

$$I_\ell = \sum_{w=1}^{n}(w - 2^{m-1})^\ell \eta_w = \sum_{w=w_0}^{2^{m-1}-1}(w - 2^{m-1})^\ell(\eta_w + \eta_{2^m-w})\,. \tag{11}$$

Note that the codeword of weight zero is not taken in account in the sum above. Recall that C does not contain the all-one codeword.

The values of I_2 and I_4 are simply obtained by using the four power moments given by (10). We replace n by $2^m - 1$ and obtain

$$I_2 = 2^{k+m-2} - 2^{2m-2} \tag{12}$$

and

$$I_4 = 2^{k+m-4}(3 \cdot 2^m - 2) - 2^{4m-4} + 3 \cdot 2^{k-1}(\nu_3 + \nu_4) \; . \tag{13}$$

Now we consider

$$I_4 - 2^{m-1} I_2 = \sum_{w=w_0}^{2^{m-1}-1} (w - 2^{m-1})^2 \left((w - 2^{m-1})^2 - 2^{m-1}\right)(\eta_w + \eta_{2^m - w}) \; . \tag{14}$$

Note that, if $2^{m-1} - 2^{(m-1)/2} < w \le 2^{m-1} - 1$, then the wth term above is less than or equal to zero. From (12) and (13) we have

$$I_4 - 2^{m-1} I_2 = (2^{m-1} - 1)(2^{k+m-3} - 2^{3m-3}) + 3 \cdot 2^{k-1}(\nu_3 + \nu_4) \; . \tag{15}$$

When $k < m$, the value of I_2 is strictly negative which is impossible, proving that C cannot satisfy the hypothesis of the theorem.

(i) Suppose that $k \ge 2m$. Then, from (15), the value of $I_4 - 2^{m-1} I_2$ cannot be negative. In the sum (14), the terms which correspond to the values of w greater than $2^{m-1} - 2^{(m-1)/2}$, are negative. So the value of w_0 is at most $2^{m-1} - 2^{(m-1)/2}$.

Assume that $w_0 = 2^{m-1} - 2^{(m-1)/2}$. By replacing w_0 by its value in (14), we obtain $I_4 - 2^{m-1} I_2 \le 0$. From (15), the only possibility is $I_4 - 2^{m-1} I_2 = 0$. We deduce from (15) that $k = 2m$ and $\nu_3 + \nu_4 = 0$. Therefore $C^\perp$ has dimension $2m$ and C has minimum distance at least five. Moreover only three values η_w are unknown. They correspond to the following values of w:

$$w = 2^{m-1} \pm 2^{(m-1)/2} \quad \text{and} \quad w = 2^{m-1} \; .$$

Now we apply a classical result which can be found in [28]: *let S be a subset of $\{1, 2, \ldots, n\}$ containing s elements. Then the weight distributions of $C^\perp$ and C are uniquely determined by $\nu_1, \nu_2, \ldots, \nu_{s-1}$ and the η_i with $i \notin S$.*

As $\nu_1 = \nu_2 = \nu_3 = \nu_4 = 0$ and the values η_w are unknown for only three values of w, the weight enumerator of $C^\perp$ (and of C) is unique. Since the 2-error-correcting BCH code satisfies our hypothesis, its weight polynomial is the solution.

(ii) If $k = m$ then $I_2 = 0$, proving that $C^\perp$ has only one weight $w = 2^{m-1}$ – i.e. the code $C^\perp$ has the same weight distribution as the simplex code.

Assume that $m < k < 2m$. If $\nu_3 + \nu_4 = 0$ we obtain from (13),

$$I_4 = 2^{m-4}(3 \cdot 2^{m+k} - 2^{k+1} - 2^{3m}) \; .$$

If $k < 2m - 1$ then $I_4 < 0$, a contradiction. On the other hand (if $k = 2m - 1$), a code $[2^m - 1,\ 2^m - 2m,\ 5]$ does not exist [18] (see also [4]). So the minimum distance of C is at most four.

When $w_0 \geq 2^{m-1} - 2^{(m-1)/2}$, the value of $I_4 - 2^{m-1}I_2$ must be less than or equal to zero (see (14)). We obtain the condition (9) on $\nu_3 + \nu_4$ from (15), completing the proof.

■

Remark 3. Let's explain what the hypotheses of Theorem 4 mean. First, the condition $d \geq 3$ means that any two columns of the parity check matrix of C are distinct. Second, the vector **1** is not in $C^{\perp}$ if and only if C contains some codewords of odd weight.

3.2. Coding Theory Point of View

Definition 5 *Let C be a linear code of length n and denote by $(\eta_0, ..., \eta_n)$ the weight enumerator of its dual $C^{\perp}$. The set $\Omega = \{j \; : \; \eta_j \neq 0, \; 1 \leq j \leq n\}$ is said to be the characteristic set of C. The external distance of C, denoted by θ, is the cardinality of Ω: $\theta = card\, \Omega$.*

Theorem 5 *Let F be any polynomial of the form (3) such that $F(0) = 0$ and let C_F be the $[n = 2^m - 1, k \; , d]$ code defined by the parity check matrix*

$$\mathcal{H}_F = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \ldots & F(\alpha^{n-1}) \end{pmatrix} , \tag{16}$$

where each entry is viewed as a binary vector. Then:
(i) *The code C_F is such that $3 \leq d \leq 5$.*
(ii) *F is APN if and only if $d = 5$.*
(iii) *F is AB if and only if the characteristic set of C_F looks as follows*

$$\Omega = \{ \; 2^{m-1}, \; 2^{m-1} \pm 2^{(m-1)/2} \; \} \; .$$

Proof: First note that, for any mapping F, the dimension k of C_F is such that $k \geq 2^m - 1 - 2m$. Since any two columns of $\mathcal{H}_F$ are distinct, we have that $d \geq 3$. Assume that $d \geq 6$. As the existence of a linear $[n, \; k, \; d]$ code implies the existence of a linear $[n-1, \; k, \; d-1]$ code, the code C_F with parameters $[2^m - 1, \; k, \; 6]$, $k \geq 2^m - 1 - 2m$, provides a linear $[2^m - 2, \; k, \; 5]$ code. But such a code does not exist by [18] (see also [4]). Thus we should have $d \leq 5$, completing the proof of **(i)**.

Let $c = (c_0, \; ..., \; c_{n-1})$ be a binary vector. By the definition of $\mathcal{H}_F$ (see (16)), c belongs to C_F, if and only if it satisfies

$$\sum_{i=0}^{n-1} c_i \alpha^i \; = \; 0 \quad \text{and} \quad \sum_{i=0}^{n-1} c_i F(\alpha^i) \; = \; 0 \; . \tag{17}$$

According to (17), C_F has minimum weight 3 or 4 if and only if there exist four distinct elements, say x, y, x', y', of $GF(2^m)$ such that

$$x \; + \; y \; + \; x' \; + \; y' \; = \; 0 \quad \text{and} \quad F(x) \; + \; F(y) \; + \; F(x') \; + \; F(y') \; = \; 0 \; . \tag{18}$$

The minimum weight is 3, if one of these elements is zero; otherwise it is 4. The equation (2) can be rewritten as follows:

$$x + y = a \quad \text{and} \quad F(x) + F(y) = b\,, \tag{19}$$

where $a \neq 0$ and b are arbitrary elements of $GF(2^m)$. Suppose that there exist two distinct pairs (x, y) and (x', y') which satisfy (19). Of course *distinct* implies that we have here four distinct elements of $GF(2^m)$. The existence of such four elements, for some a and b, is equivalent to the existence of four elements satisfying (18). So we have proved that F is APN if and only if C_F has minimum distance $d \geq 5$. But from **(i)** we have, that $d \leq 5$. So we have proved $(\mathbf{ii})$.

Now set $f(x) = \langle b, F(x)\rangle + \langle a, x\rangle$. Considering the elements of $GF(2^m)$ as binary vectors, we can see that the function f is actually a linear combination of rows of $\mathcal{H}_F$. Hence the numbers

$$\lambda_{a,b} \;=\; \text{card}\,\{\, \alpha^i \mid f(\alpha^i) = 1 \,\}$$

are the weights of codewords of $C_F^{\perp}$ (i.e. the elements of Ω). Assume that F is AB, i.e. $\mu_F(a, b) = 0$ or $\pm 2^{\frac{m+1}{2}}$. First $\mu_F(a, b) = 0$ means that $\lambda_{a,b} = 2^{m-1}$ and therefore $2^{m-1} \in \Omega$. Similarly, the condition $\mu_F(a, b) = \pm 2^{\frac{m+1}{2}}$ means that

$$2\lambda_{a,b} = 2^m \pm 2^{\frac{m+1}{2}}, \quad \text{i.e.}\;\; \lambda_{a,b} = 2^{m-1} \pm 2^{\frac{m-1}{2}} \;\in\; \Omega\,.$$

Thus, we have proved $(\mathbf{iii})$. Note that in (1) the values of $\mu_F(a, 0)$ are not considered. From this point of view they correspond to the codewords of $C_F^{\perp}$ which are generated by the first m rows of $\mathcal{H}_F$. That is the codewords of the *simplex code* which have weight 2^{m-1}.

■

Corollary 1 *Let F be any polynomial (3). Then:*
(i) *If F is APN then the dimension of C_F is equal to $2^m - 2m - 1$.*
(ii) *If F is APN then $C_F^{\perp}$ does not contain the all-one vector.*
(iii) *If F is AB then F is APN.*
(iv) *If F is AB then the weight distribution of $C_F^{\perp}$ is unique and given by Theorem 4,* **(i)**.

Proof: **(i)** Let F be any APN function. In accordance with Theorem 5, C_F is an $[n,\ k,\ d]$ code, with $n = 2^m - 1$, $d = 5$ and $k \geq n - 2m$. If $k = n + 1 - 2m$ then we obtain a linear $[2^m - 1,\ 2^m - 2m,\ 5]$ code, which does not exist [18]. Therefore we should have $k = 2^m - 1 - 2m$.
(ii) Assume that F is APN. Then C_F contains some codewords of weight 5. Since the vector $\mathbf{1} = (1, ..., 1)$ cannot be orthogonal to any codeword of odd weight, $\mathbf{1}$ is not in $C_F^{\perp}$.
(iii) Assume that F is AB. By definition, the dimension of $C_F^{\perp}$ is at most $2m$. Suppose that it is less than $2m$. It means that there are at least one $\beta \neq 0$ and one γ such that $\langle \beta, F(x)\rangle + \langle \gamma, x\rangle = 0$, for all $x \in GF(2^m)$. So $\mu_F(\gamma, \beta) = 2^m$, a contradiction. Moreover the code $C_F^{\perp}$ has exactly three weights, 2^{m-1} and $2^{m-1} \pm 2^{(m-1)/2}$. This implies that the sum in (14) is zero. Since $k = 2m$, we deduce from (15): $\nu_3 = \nu_4 = 0$. Thus F is APN.
(iv) Follows immediately from Theorem 4, **(i)**. ■

For any binary code C denote by ρ its *covering radius*,

$$\rho \;=\; \max_{x\in V_n} \;\min_{c\in C} \{\; d(x,c) \;\} \;.$$

Proposition 4 *Let F be any APN mapping. Then the covering radius ρ of C_F is such that:* $3 \;\leq\; \rho \;\leq\; 4\,.$

Proof: An e-error-correcting code is said to be *perfect* if its covering radius is equal to e. It is well known that there are no binary perfect codes of length $n \geq 7$ with distance 5 (see [29, p. 182]). Since F is APN, the code C_F is a 2-error-correcting code. Assuming that C_F is not a trivial perfect code of length 5, its covering radius ρ is at least 3.

Suppose now that $\rho = 5$ and consider any coset D of C_F of weight 5. According to Corollary 1,**(i)**, the dimension of C_F is $2^m - 1 - 2m$. Therefore the code $D \cup C_F$ is a (linear) code $[2^m - 1,\ k,\ 5]$ with $k = 2^m - 2m$. But such a code does not exist [18]. ■

There is an interesting connection between AB functions and so called uniformly packed codes. We will define these codes in the sense of [1] – see other definitions in [34], [19] and [20].

Definition 6 [1] *Let C be any binary code of length n, with minimum distance $d = 2e+1$ and covering radius ρ. For any $x \;\in\; V_n$ denote by $\zeta_j(x)$ the number of codewords of C at distance j from x. The code C is called* uniformly packed, *if there exist real numbers $h_0,\ h_1, ...,\ h_\rho$ such that for any $x \in V_n$ the following equality holds*

$$\sum_{j=0}^{\rho} h_j\; \zeta_j(x) \;=\; 1\;.$$

A special case of such codes, introduced in [34], corresponds to the case $\rho = e+1$ and

$$h_0 = h_1 = \cdots = h_{e-1} = 1,\; h_e = h_{e+1} = 1/\ell, \tag{20}$$

where ℓ is a positive integer.

Theorem 6 *Let F be any polynomial (3), where m is odd. Then F is AB, if and only if C_F is a uniformly packed code of length $n = 2^m - 1$ with minimum distance $d = 2e+1 = 5$ and covering radius $\rho = e+1 = 3$.*

Proof: Let F be any AB mapping. From Corollary 1,**(iii)**, F is APN. Moreover, according to Theorem 5, C_F has minimum distance 5 and its characteristic set is

$$\Omega = \{(n+1)/2,\; (n+1)/2 \pm \sqrt{(n+1)/2}\}\;.$$

So its external distance θ is equal to 3. Therefore by the well known Delsarte inequality [12] (that *$\rho \leq \theta$ for any code C*), we have $\rho \leq 3$. But from Proposition 4 we have: $\rho \geq 3$, and therefore, $\rho = 3 = \theta$. Now we use the following result [2], [20]: *a code C is uniformly packed, if and only if its covering radius ρ is equal to its external distance θ*. Therefore C_F is a uniformly packed code with $d = 2e+1 = 5$ and $\rho = e+1 = 3$.

For the converse statement, first we recall two results. In [1] it was proved that the 2-error-correcting BCH code of length $n = 2^m - 1$, where m odd, is uniformly packed with parameters (20), where $\ell = (n-1)/6$ and where the roots $\xi_i,\ i = 1,2,3$, of the Lloyd polynomial are:

$$\xi_1 \;=\; \frac{n+1}{2} \;-\; \sqrt{\frac{n+1}{2}},\;\; \xi_2 \;=\; \frac{n+1}{2},\;\; \xi_3 \;=\; \frac{n+1}{2} + \sqrt{\frac{n+1}{2}}\;. \tag{21}$$

Then in [20] it was proved that these codes are the only uniformly packed codes of length $n = 2^m - 1,\ n \geq 31$, (m odd) with $d = 2e + 1 = 5$ and $\rho = e + 1 = 3$. In fact, the uniformly packed codes given in [20] differ from Definition 6, but it is easy to see (and it was mentioned in [20], [2]), that uniformly packed codes with parameters (20) coincide with uniformly packed codes in the sense of [20] when $\lambda + 1 = \mu$ (see p. 23 in [20]).

Since C_F is linear, the values of the roots $\xi_j,\ j = 1,2,3$, give the values of nonzero components of the weight enumerator of the dual code $C_F^{\perp}$, which form the characteristic set Ω of C_F (see Definition 5). Then by Theorem 5,**(iii)**, we obtain that F is AB. ■

According to Theorem 5, if the function F is AB then the weight distribution of C_F is unique, and equal to the weight distribution of the 2-error-correcting BCH code. Now we can say more: such a code C_F is *completely regular*.

Definition 7 *A code C is completely regular, if for any its coset U,*

$$U \;=\; x \;+\; C \;=\; \{x + c \mid c \in C\}\;,$$

the weight distribution of U is uniquely defined by its minimum weight.

It is known that any uniformly packed code with parameters (20) is completely regular [34, Theorem 4] (see also [20, p.23], where this property is proved for a more general class of codes).

Corollary 2 *Let F be any polynomial (3), where m is odd. If F is AB, then C_F is a completely regular code.*

Thus, if F is AB, the weight polynomial $W_U(x)$ of any coset U of C_F is uniquely defined by its minimum weight s. Following [1], we will show how to write out the weight polynomials of the cosets of C_F. The Lloyd's type theorem for uniformly packed codes asserts ([1], Theorem 1) that the existence of a uniformly packed code C of length n with parameters $h_i,\ i = 0,1,\ldots,\rho$, implies that the Lloyd polynomial $L_\rho(x,n)$ of C,

$$L_\rho(x,n) \;=\; \sum_{i=0}^{\rho} h_i\, P_i(x,n)\;,$$

has ρ distinct integral roots between 0 and n. Here $P_k(x,n)$ is the Krawtchouk polynomial of degree k:

$$P_k(x,n) \;=\; \sum_{j=0}^{k} (-1)^{k-j} \binom{n-x}{j} \binom{x}{k-j}\;,$$

where

$$\binom{x}{j} \;=\; \frac{x(x-1)\cdots(x-j+1)}{j!}\;,$$

for any real x. Denote by ξ_i the i-th root of $L_\rho(x,n)$, where $i = 1,\ldots,\rho$. Now suppose that U is an arbitrary coset of C of weight s: $s = min\,\{wt(c)\;:\; c \in U\}$. Denote by $\eta_{(s)} = (\eta_{s,0},\ \eta_{s,1}, ...,\ \eta_{s,n})$ its weight enumerator. The first ρ values of $\eta_{s,j}$ follow from the definition of the uniformly packed code with parameters (20):

$$s \;=\; \begin{cases} 0,...,e-1\;: & \eta_{s,j}=0, \quad \forall\, j \le e+1,\; j \ne s \text{ and } \eta_{s,s}=1\;, \\ e\;: & \eta_{s,j}=0, \quad \forall\, j < s\; \eta_{s,s}=1 \text{ and } \eta_{s,s+1}=\ell-1\;, \\ e+1\;: & \eta_{s,j}=0, \qquad\quad \forall\, j < s \text{ and } \eta_{s,s}=\ell\;. \end{cases} \tag{22}$$

Assuming that we know all the roots ξ_j of the Lloyd polynomial, we can write the weight polynomial $W_s(x)$ of U in the following evident form (Theorem 2, [1]) :

$$W_s(x) \;=\; \frac{|C|(1+x)^n}{2^n} \;+\; \sum_{j=1}^{\rho} \tau_{s,j}(1+x)^{n-\xi_j}(1-x)^{\xi_j}\;, \tag{23}$$

where ρ constants $\tau_{s,j}$ depend on the known coefficients $\eta_{s,j}$ (see(22)) of $W_s(x)$ and are therefore defined by the corresponding system of linear equations. Since the value $\eta_{s,s}$ uniquely defines the weight enumerator $\eta_{(s)}$, any uniformly packed code with $\rho = e+1$ is completely regular. For the case $e = 2$ and $n = 2^m - 1$, m is odd, the weight polynomial $W_C(x) = W_0(x)$ of the code $C = C_F$ looks as follows:

$$\begin{aligned} W_C(x) \;=\; & \tfrac{1}{2(n+1)^2}(2(1+x)^n + n\xi_3(1+x)^{\xi_3-1}(1-x)^{\xi_3} + \\ + \;\; & n(n+3)(1+x)^{\xi_2-1}(1-x)^{\xi_2} \;+\; n\xi_1(1+x)^{\xi_1-1}(1-x)^{\xi_1})\;, \end{aligned} \tag{24}$$

where the roots ξ_i are given by (21).

Corollary 3 *Let F be any APN mapping. Then F is AB if and only if the code C_F has external distance $\theta = 3$.*

Proof: First assume that F is AB. According to Theorem 5, it implies that the weight enumerator of the code $C_F^{\perp}$, has exactly three nonzero components, i.e. C_F has external distance $\theta = 3$ (see Definition 5).

Now assume that the code C_F has minimum distance 5 and external distance 3. According to Proposition 4, C_F has covering radius $\rho \geq 3$. But by the Delsarte inequality , $\rho \leq \theta$ and therefore $\rho = 3$. Since $\rho = \theta$, the code C_F is uniformly packed and the statement follows from Theorem 6 above. ■

3.3. APN Functions and Cyclic Codes

We consider only binary cyclic codes of length $n = 2^m - 1$. In order to establish the connection between the properties of APN (or AB) functions and cyclic codes, it is necessary to define these codes in terms of systems of equations. Any binary vector $c = (c_0,\ ...,\ c_{n-1})$ can be identified to its *support*, also called its *set of locators*. This is the set

$$\{\ \alpha^i \in GF(2^m)^* \mid c_i = 1,\ i = 0, 1, ..., n-1\}\ ,$$

whose cardinality is $wt(c)$. Now we define the *power functions* of any vector c of weight w. Let $\{X_1, \dots, X_w\}$ be the set of locators of c; the power functions $\varphi_k(c)$ of c are :

$$\varphi_k(c)\ =\ \sum_{j=1}^{w} X_j^k \quad ,\quad k \in [1, n]\ . \tag{25}$$

Note that $\varphi_n(c)$ is equal to $wt(c)$ modulo 2.

Definition 8 *Denote by $cl(j)$ the 2-cyclotomic coset of j modulo n. Let T be a set of integers from $[0, n-1]$, which is a union of some cosets $cl(j)$. The binary cyclic code of length n, with zeros set $\{\ \alpha^k \mid k \in T\ \}$, is the set of all vectors c such that $\varphi_k(c) = 0$ for all $k \in T$. The set T is called the defining set of C.*

In this section we assume that $F(x) = \sum \delta_j x^j$ is a polynomial (3), such that $F(0) = 0$. We mentioned in Remark 1 that for the study of APN (or AB) functions we can add this hypothesis without loss of generality. We will explain later why we are then in accordance with the hypotheses of Theorem 4 (see the next lemma).

Now we can construct the code C_F with parity check matrix $\mathcal{H}_F$ (see Theorem 5). Then a vector $c = (c_0, ..., c_{n-1})$ is in C_F if and only if

$$\sum_{i=0}^{n-1} c_i \alpha^i\ =\ 0 \quad \text{and} \quad \sum_{i=0}^{n-1} c_i F(\alpha^i) =\ 0\ .$$

We have clearly that $\sum_{i=0}^{n-1} c_i \alpha^i = \varphi_1(c)$ and

$$\sum_{i=0}^{n-1} c_i F(\alpha^i) = \sum_{i=0}^{n-1} c_i \sum_{j=1}^{n} \delta_j \alpha^{ij}\ =\ \sum_{j=1}^{n} \delta_j \sum_{i=0}^{n-1} c_i (\alpha^i)^j\ =\ \sum_{j=1}^{n} \delta_j \varphi_j(c)\ .$$

Henceforth c is in C_F if and only if

$$\varphi_1(c) = 0 \quad \text{and} \quad \sum_{j=3}^{n} \delta_j \varphi_j(c) = 0 \tag{26}$$

(note that $\varphi_2(c) = (\varphi_1(c))^2 = 0$). Particularly if c is such that $\varphi_1(c) = 0$ and $\varphi_j(c) = 0$ for all $\delta_j \neq 0$, then c is a codeword of C_F. Actually c is contained in a subcode of C_F which is the binary cyclic code, which we denote by B_F, whose zeros are all the elements α^j such that $\delta_j \neq 0$. When $\alpha^n = 1$ is not a zero of B_F, then B_F contains some codewords of odd weight. It means that the all-one vector is not in $B_F^\perp$, implying that $C_F^\perp$ does not contain the all-one vector. Note that 1 is not a zero of B_F if and only if $\delta_n = 0$. Thus we have proved the following property.

Lemma 2 *Let $F(x)$ be a polynomial (3), such that $F(0) = 0$. Denote by I_F the set of exponents j such that $\delta_j \neq 0$. Set*

$$T_F \ = \ \{ \ cl(1) \ \} \cup \{ \ cl(j) \mid j \in I_F \ \} \ .$$

Then the code C_F contains the binary cyclic code B_F of length n whose defining set is T_F. When $\delta_n = 0$, the dual code $C_F^{\perp}$ does not contain the all-one vector.

So we can exhibit a large class of polynomials which cannot be APN.

Theorem 7 *Notation is that of Lemma 2. Let g be any proper divisor of m. Let Λ_g be the set of all integers t, $t \in [1,\ 2^m - 2]$, such that $t \equiv 2^\ell \ (mod\ 2^g - 1)$ for some ℓ, $0 \leq \ell \leq g-1$. If F is such that T_F is a subset of Λ_g, then F is not APN (and therefore not AB).*

Proof: By definition, T_F is a union of 2-cyclotomic cosets. Since Λ_g is invariant under the multiplication by 2 modulo n and contains $cl(1)$, T_F can be a subset of Λ_g.

Let C be the binary cyclic code of length n with defining set Λ_g. It is proved in [11], in a more general context, that the minimum distance of such a code is three. Indeed, consider the vector c whose locators are $\{1, \beta, \beta + 1\}$, where β is any element of $GF(2^g) \setminus \{0, 1\}$. Then for any $t \in \Lambda_g$, $t \equiv 2^\ell \pmod{2^g - 1}$, we have, that:

$$\varphi_t(c) = 1 + \beta^t + (1+\beta)^t = 1 + \beta^{2^\ell} + (1+\beta)^{2^\ell} = 0 \ ,$$

implying that c is a codeword of C. As T_F is contained in Λ_g, C is contained in the cyclic code B_F. From Lemma 2, B_F is contained in C_F, proving that C_F has minimum distance three. In accordance with Theorem 5,**(ii)**, the function F, cannot be APN, and, therefore, F cannot be AB. ■

EXAMPLE 1. For the case $m = 9$ and $g = 3$ let Λ_3 be the set of all integers s, $s \in [1, 510]$, such that s modulo 7 is a power of two. The set Λ_3 is a union of some cyclotomic cosets modulo 511, whose set of representatives, say R, is:

$$R = \left\{ \begin{array}{l} 1, 9, 11, 15, 23, 25, 29, 37, 39, 43, 51, 53, 57, 79, \\ 85, 93, 95, 107, 109, 123, 127, 183, 191, 219, 239 \end{array} \right\} \ .$$

Take any $F(x)$, given by (3), and consider the set I_F of exponents corresponding to nonzero coefficients. If for any $j \in I_F$ some element of the coset $cl(j)$ belongs to R, then $F(x)$ is not APN. For instance, the polynomial x^t is not APN for any $t \in R$.

3.4. The Quadratic Case

Denote by Q_m the set of all integers s, $s \in \{1, ..., 2^m - 1\}$, whose 2-weight is equal to one or two. That is

$$Q_m \ = \ \{ \ 2^k + 2^\ell \mid k \text{ and } \ell \text{ in } [0, m-1] \ \} \ . \tag{27}$$

The polynomial $F(x)$ is said to be *quadratic* if its algebraic degree is equal to 2. It means that $F(x)$ has the following form

$$F(x) = \sum_{j \in Q_m} \delta_j x^j \ , \ \ \delta_j \in GF(2^m) \ . \tag{28}$$

Note that the associated Boolean function f, $f(x) = \langle b, F(x) \rangle + \langle a, x \rangle$ is quadratic (its algebraic normal form is a polynomial of degree 2 in m variables).

Proposition 5 *Let F be a quadratic polynomial (28). Then the code $C_F^{\perp}$ is contained in $\mathcal{R}^*(m, 2)$.*

Proof: Recall that the code $\mathcal{R}^*(m, r)$ (see Section 3) is defined by those α^s, where the integer s, $1 \leq s \leq 2^m - 2$, is such that $1 \leq w_2(s) \leq m - r - 1$. So the set Q_m is exactly the defining set of $\mathcal{R}^*(m, m-3)$. On the other hand, the defining set of $\mathcal{R}^*(m, m-2)$ is $\{cl(1)\}$. Hence C_F is always contained in $\mathcal{R}^*(m, m-2)$, since $\varphi_1(c) = 0$ for any $c \in C_F$ (see (26)).

Consider now the code B_F with defining set T_F (see Lemma 2). By definition, the polynomial $F(x)$ is quadratic if and only if T_F is contained in Q_m, meaning that the cyclic code B_F contains the code $\mathcal{R}^*(m, m-3)$. Then all the elements α^s satisfying $1 \leq w_2(s) \leq m - 3$ are zeros of the dual code $B_F^{\perp}$, proving that $B_F^{\perp}$ is contained in $\mathcal{R}^*(m, 2)$. So we have:

$$\mathcal{R}^*(m, m-3) \subset B_F \subset C_F \quad \Longrightarrow \quad C_F^{\perp} \subset B_F^{\perp} \subset \mathcal{R}^*(m, 2) \ .$$

■

When F is quadratic, there is an interesting expansion of Theorem 4.

Theorem 8 *Let F be a quadratic polynomial (28). Then F is AB if and only if F is APN.*

More generally this property holds when F is such that the code C_F is equivalent to a code C whose dual is in the punctured Reed-Muller code of order two.

Proof: This result is directly obtained from the identities stated in the proof of Theorem 4. Consider any linear code C such that $C^{\perp}$ is in $\mathcal{R}^*(m, 2)$ and whose dimension is $2m$. The weight distribution of the code $\mathcal{R}^*(m, 2)$ is well-known (see [29], Chapter 15). In particular when m is odd, this code has no codewords of weight w such that $2^{m-1} - 2^{(m-1)/2} < w < 2^{m-1}$. Therefore this property holds for any subcode of $\mathcal{R}^*(m, 2)$.

Now the result is deduced from (14) and (15) (where notation is that of Theorem 4). If $\nu_3 = \nu_4 = 0$, with $k = 2m$, we obtain

$$I_4 - 2^{m-1} I_2 = \sum_{w = w_0}^{2^{m-1} - 2^{(m-1)/2}} (w - 2^{m-1})^2 ((w - 2^{m-1})^2 - 2^{m-1})(\eta_w + \eta_{2^m - w}) = 0 \ .$$

Since $C^{\perp}$ has no weight w such that $2^{m-1} - 2^{(m-1)/2} < w < 2^{m-1}$, there are no negative terms in the sum above. This implies that all terms are zero, which means that $\eta_w + \eta_{2^m - w} = 0$, for all w which are not in the set $\{\ 2^{m-1} \pm 2^{(m-1)/2},\ 2^{m-1}\ \}$.

We have already proved that any AB mapping is APN; on the other hand if F is APN then the dimension of $C_F^{\perp}$ equals $2m$ (see Corollary 1). Now we assume that F is APN and that the code C_F is equivalent to a code C whose dual is a subcode of $\mathcal{R}^*(m, 2)$. Then the dual of C_F is equivalent to $C^{\perp}$. The weight polynomial of C_F (resp. $C_F^{\perp}$) is the same as the weight polynomial of C (resp. $C^{\perp}$). Since F is APN, C has minimum distance 5 and, according to the proof above, $C^{\perp}$ has only three weights, $2^{m-1} \pm 2^{(m-1)/2}$ and 2^{m-1}. So F is AB. From Proposition 5, when F is quadratic, the code $C_F^{\perp}$ is itself a subcode of $\mathcal{R}^*(m,2)$, completing the proof. ■

Corollary 4 *Assume that $F(x) = x^k$. Suppose that there is $j = 2^{\ell}+1$ such that $jk = 2^s(2^r+1)$ modulo 2^m-1, for some s and some r.*

Then if F is APN, F is AB.

Proof: In this case the code C_F is a cyclic code with zeros α and α^k (and their conjugates). The transformation above carries C_F to the cyclic code C whose zeros are α^j and α^{jk}. Since j is prime to 2^m-1 it is a permutation which conserves the weight polynomials.

We can deduce that the code C_F is equivalent to a code which is in the Reed-Muller of order two and apply the previous theorem. ■

Remark 4. (a) We have proved in Theorem 1 that the algebraic degree of any AB function is upper bounded by $(m+1)/2$. On the other hand, there are few examples of APN functions which are not AB. The numerical results induce a conjecture, that *any APN function is always AB when its algebraic degree is strictly less than* $(m+1)/2$.
(b) An infinite class of quadratic AB mappings was given by Kasami (see Theorem 10 later). It is strongly conjectured that, *up to equivalence, there are no other quadratic mappings which are AB.*

To conclude this section, we are going to express the property for a quadratic function F to be AB, in terms of a system of equations over $GF(2^m)$. Recall that F is APN if and only if the code C_F has minimum distance 5. When F is quadratic, we have a particular situation: the code C_F contains codewords of weight 4 if and only if it contains codewords of weight 3. We begin by proving this property.

Lemma 3 *Let F be a quadratic polynomial. Then F is AB if and only if the code C_F does not contain any codeword of weight three.*

Proof: When F is AB, then F is APN, implying that C_F has minimum distance five. So C_F cannot contain any codeword of weight three.

For the converse statement we will use the terminology of Section 3.3. Let $\mathrm{c} \in C_F$ of weight three whose support, denoted by $supp(\mathrm{c})$, is the set $\{X_1,\ X_2,\ X_3\}$. By definition, if $\mathrm{c} \in C_F$ then

$$\phi_1(\mathrm{c}) = X_1 + X_2 + X_3 = 0$$

(see (25) and (26)). By adding "0" to the locators set of c, we obtain a linear subspace of $GF(2^m)$ of dimension 2. Similarly, the support of any $\mathrm{c}' \in C_F$ of weight 4 is an affine subspace of $GF(2^m)$ of dimension 2. Its support is a coset of $supp(\mathrm{c}) \cup \{0\}$, for some c satisfying $\phi_1(\mathrm{c}) = 0$:

$$supp(\mathrm{c}') \;=\; \{\nu\} \,\cup\, \{\nu \,+\, X \mid X \in supp(\mathrm{c})\}\;,\;\; \nu \in GF(2^m)\;. \qquad (29)$$

Take $F(x) = \sum_{j\in I} \delta_j x^j$ where $I \subseteq Q_m$ and $\delta_j \neq 0$. Let c' be a codeword of weight 4 of C_F. Recall that $\mathrm{c}' \in C_F$ if and only if

$$\varphi_1(\mathrm{c}') = 0 \quad \text{and} \quad \sum_{j\in I} \delta_j\ \varphi_j(\mathrm{c}') = 0\ .$$

Obviously $\varphi_1(\mathrm{c}') = \varphi_1(\mathrm{c})$. Moreover for any $j \in Q_m$, where $j = 2^k + 2^\ell$, we obtain, using (29),

$$\begin{aligned}\varphi_j(\mathrm{c}') &= \nu^{2^k+2^\ell} + \sum_{i=1}^{3}(\nu + X_i)^{2^k+2^\ell} \\ &= \nu^{2^k+2^\ell} + \sum_{i=1}^{3}\left(\nu^{2^k+2^\ell} + \nu^{2^k}(X_i)^{2^\ell} + \nu^{2^\ell}(X_i)^{2^k} + (X_i)^{2^k+2^\ell}\right) \\ &= \sum_{i=1}^{3}(X_i)^{2^k+2^\ell} = \varphi_j(\mathrm{c}),\end{aligned}$$

since $\sum_{i=1}^{3}(X_i)^{2^s} = 0$ for any s. Thus we have proved that there is $\mathrm{c}' \in C_F$, with $wt(\mathrm{c}') = 4$, if and only if there is $\mathrm{c} \in C_F$ with $wt(\mathrm{c}) = 3$, completing the proof. ■

Theorem 9 *Let F be a quadratic polynomial of the form (28). Then F is AB if and only if for any $k,\ k \in [1, n-1]$, and for any $\nu,\ \nu \in GF(2^m) \setminus \{0,1\}$, the following unequality holds:*

$$\sum_{j\in Q_m, j=2^s+2^\ell, s>\ell} \delta_j\ \alpha^{jk}(\nu^{2^s} + \nu^{2^\ell})\ \neq\ 0\ . \tag{30}$$

Proof: In accordance with Lemma 3, any quadratic polynomial F is AB if and only if C_F does not contain any codeword whose support can be identified with a linear subspace of $GF(2^m)$ of dimension 2. Let $\mathcal{V}$ be the set of such subspaces. The cardinality of $\mathcal{V}$ is well-known to be $(2^m - 1)(2^{m-1} - 1)/3$. There are $2^{m-1} - 1$ elements of $\mathcal{V}$ of the type

$$\{\ 0,\ 1,\ \nu,\ \nu + 1\ \}\ ,\ \ \nu \in GF(2^m) \setminus \{0,1\}\ ,$$

By shifting, for a fixed ν, we obtain $2^m - 1$ subspaces of the type.

$$\{\ 0,\ \alpha^k,\ \alpha^k\nu,\ \alpha^k(\nu + 1)\ \}\ ,\ k \in [0, n-1]. \tag{31}$$

We obtain at all $(2^m - 1)(2^{m-1} - 1)$ subspaces, where each subspace occurs three times. So any element of $\mathcal{V}$ has the form (31) for some ν, corresponding to a codeword that we will denote by $\mathrm{c}_{\nu,k}$.

Let $j \in Q_m$. Since $\varphi_1(\mathrm{c}_{\nu,k}) = 0$, by definition, we have $\varphi_j(\mathrm{c}_{\nu,k}) = 0$ for all $j = 2^s$. Moreover if $j = 2^s + 2^\ell$, $s > \ell$, we have

$$\varphi_j(\mathrm{c}_{\nu,k}) = \alpha^{kj} + (\alpha^k\nu)^j + (\alpha^k(\nu + 1))^j = \alpha^{kj}\left(\nu^{2^s} + \nu^{2^\ell}\right)\ . \tag{32}$$

Now we express the fact, that C_F does not contain any codeword $\mathrm{c}_{\nu,k}$. According to (26), we must have

$$\sum_{j\in Q_m} \delta_j \varphi_j(\mathrm{c}_{\nu,k}) \neq 0\ ,\ \ \nu \in GF(2^m)\setminus\{0,1\},\ \text{and}\ k\in[0,n-1]\ .$$

Since $\varphi_1(\mathrm{c}_{\nu,k}) = 0$ and by using (32), we conclude that the condition above is equivalent to (30), completing the proof. ■

EXAMPLE 2. Suppose that $F(x) = \delta x^j$, $j = 2^s + 2^\ell$ and $s > \ell$. Then (30) is satisfied if and only if $s - \ell$ is prime with m. Indeed we must have

$$\delta\alpha^{kj}(\nu^{2^s} + \nu^{2^\ell}) \neq 0$$

for all ν and for all k. Since $\nu^{2^s} + \nu^{2^\ell} = (\nu^{2^{s-\ell}} + \nu)^{2^\ell}$, it is possible only if the polynomial $x^{2^{s-\ell}} + x$ has only 0 and 1 as roots in $GF(2^m)$. We have again a well known result: *if $t = 2^i + 1$, if m is odd and i and m are co-prime, then the function $F(x) = x^t$ is AB* (see Theorem 10 later).

3.5. AB Functions and Cyclic Codes with Two Zeros

In this section we suppose that $F(x)$ is a power polynomial over $GF(2^m)$, $F(x) = x^t$ where the 2-cyclotomic coset $cl(t)$ has the cardinality m (if it is not satisfied, then F is not APN according to Corollary 1). The code C_F is the binary cyclic code whose zeros are α, α^t and their conjugates. This code is obviously equivalent to any code C whose zeros are α^j and α^{jt}, where jt is computed modulo n, for any j which is co-prime with n. Actually we consider now binary cyclic codes with two zeros α^r and α^s (and their conjugates). Such a code $C_{r,s}$ has the parity check matrix:

$$\mathcal{H}_{r,s} = \begin{pmatrix} 1 & \alpha^r & \alpha^{2r} & \dots & \alpha^{(n-1)r} \\ 1 & \alpha^s & \alpha^{2s} & \dots & \alpha^{(n-1)s} \end{pmatrix} .$$

Although the function F is the most simple here, the problem of finding such functions which are APN (furthermore, which are AB) remains an *hard open problem*. The known AB functions are due to Kasami.

Theorem 10 [23],[24] **(i)** *Let $F(x) = x^{2^i+1}$, where $gcd(i,m) = 1$. Then F is AB.* **(ii)** *Let $r = 2^j + 1$ and $s = 2^{3j} + 1$, where $gcd(j,m) = 1$. Then the code $C_{r,s}$ is equivalent to the code $C_{1,r^{-1}s}$, where the function $F(x) = x^{r^{-1}s} = x^{t(j)},\ t(j) = 2^{2j} - 2^j + 1$, is AB.*

Remark 5. Note that, in Theorem 10, $2^{3j} + 1$ is viewed modulo n; we obtain there all the functions defined for $j \in [1, (m-1)/2]$ and $gcd(j,m) = 1$. Our conjecture is that *for all class of codes $\{\ C_{r,s}\ \}$, where $r = 2^i + 1$ and $s = 2^j + 1$, this is the only situation where the minimum distance is five.*

The only known class of APN functions, which are not AB, is the class of functions $F(x) = x^{-1}$. These functions correspond to the so-called Melas codes, i.e. the codes

$C_{1,-1}$ of length $2^m - 1$, where m is odd. The weights of the corresponding dual codes were determined by Lachaud and Wolfmann [25].

Actually, taking into account the equivalent cyclic codes, the result of Kasami provides a larger class of AB functions. In the following example we consider the length 127, which is the last length for which any AB function of the type $F(x) = x^t$ belongs to a known class.

EXAMPLE 3. Consider codes of length 127. Since 127 is prime, all the integers $1, 2, .., 126$ are partitioned into $126/7 = 18$ cosets. These cosets form a multiplicative group, say $\mathcal{G}_7$, of order 18 under multiplication modulo 127: $cl(i)cl(j) = cl(ij)$ (the coset $cl(3)$ is a generator of this group). It means that there are $\binom{18}{2}$ different choices of unordered pairs $\{r, s\}$ and each such choice defines a code $C_{r,s}$. Under the action of $\mathcal{G}_7$, all these codes are partitioned into 9 orbits $\mathcal{O}_t = \{C_{3^i, t \cdot 3^i} \,:\, i = 0, 1, ...17\}$, consisting of all codes equivalent to $C_{1,t}$.

From Kasami's results (Theorem 10 above) we have three AB functions $F(x) = x^{t(j)}$, $t(j) = 2^{2j} - 2^j + 1$ and $j \in \{1, 2, 3\}$:

$$t(1) = 3\ ,\ \ t(2) = 13\ ,\ \ t(3) = 57\ ,$$

which correspond to the codes $C_{1,t}$ for $t = 3,\ 13$ and 23 (indeed, 57 belongs to $cl(23)$). We have also the three quadratic AB functions: $F(x) = x^{2^i+1}$, $1 \le i \le 3$. Since the first functions of both types coincide (indeed, $t(1) = 2^1 + 1$), it gives five AB functions $F(x) = x^t$ corresponding to five codes $C_{1,t} : t \in \{3,\ 5,\ 9,\ 13,\ 23\ \}$. It is clear that the orbit $\mathcal{O}_t$, corresponding to the code $C_{1,t}$, contains also a code $C_{1,t^{-1}}$. Indeed, the code $C_{s,ts}$ for $s = t^{-1}$, which is in fact $C_{s,1}$, is equivalent to the code $C_{1,t}$, ensuring that the function $F(x) = x^s = x^{t^{-1}}$ is AB too. We have the following five inverse values $s = t^{-1}$:

t	3	5	9	13	23
s	43	27	15	11	29 .

Therefore, we obtain ten AB functions $F(x) = x^t$ of Kasami type, which correspond to the codes $C_{1,t}$ of Kasami type and belong to five orbits $\mathcal{O}_t$, for $t \in \{3, 5, 9, 13, 23\}$. The only one short orbit $\mathcal{O}_{63}$ (which consists of 9 codes) corresponds to the mentioned above Melas code (and give APN functions). The three remaining orbits $\mathcal{O}_t$, for $t \in \{7, 19, 21\}$, consist of codes with minimum distance four. Actually, for $m = 7$ all AB functions $F(x) = x^t$ are of Kasami type. This property holds also for $m = 5$, but not for $m = 9$, where the function $F(x) = x^{19}$ is AB and appears as the first example of AB function, which is not of Kasami type, but corresponds to the conjecture of Welsh.

There are recent works on the classification of codes $C_{r,s}$ via their minimum distances. By using the Weil bound for the number of zeroes of the polynomial of two variables, Janwa et al. [22] characterized several classes of codes $C_{1,t}$ whose minimum distance is at most four. We formulate their main result.

Theorem 11 [22] *For any fixed t satisfying* $t \equiv 3\ (mod\ 4)$ *and* $t > 3$, *there is no infinite family of codes* $C_{1,t}$ *with minimum distance* 5.

Roughly speaking, the work [22] strengthens the conjecture that APN functions are exceptional. A fortiori this conjecture holds for AB functions. It is important to notice that the approach, used in [22], is not connected with the weight enumerators of the duals of the codes $C_{1,t}$, i.e. with the AB property of codes.

On the other hand in [11], the authors focus on the characterization of cyclic codes with minimum distance 3. They introduce some tools that we use now for two results related with two conjectures, already mentioned in Remark 6. In both cases, we characterize a large class of codes with minimum distance at least 4. For the generality we consider any value of m, even or odd.

Proposition 6 *Let $C_{r,s}$ be a binary cyclic code of length $n = 2^m-1$, where m is any integer, $r = 2^i+1$ and $s = 2^j+1, 0 < i < j < m$. For even m assume that $gcd(2^i+1,\ 2^m-1) = 1$. If further $gcd(j+i, m) = gcd(j-i, m) = 1$, then the code $C_{r,s}$ has minimum distance at least four. Otherwise, $C_{r,s}$ has minimum distance three.*

Proof: First notice that for the proof we need the condition $gcd(2^i+1, 2^m-1) = 1$. However this is always satisfied when m is odd. Indeed let us define for any $i,\ 0 < i < m$: $g = gcd(2^i+1,\ 2^m-1)$, $u = gcd(i, m)$ and $h = gcd(2i, m)$. The condition

$$g \mid 2^m - 1 \text{ and } g \mid 2^{2i} - 1$$

implies that g divides $2^h - 1$. For odd m we have $u = h$; thus g divides $2^u - 1$ and $2^u - 1$ divides 2^i-1. Therefore g divides 2^i-1, implying that g divides $(2^i+1)+(2^i-1) = 2^{i+1}$, which is possible only for $g = 1$.

Since $gcd(2^i+1,\ 2^m-1) = 1$, any two columns of the parity check matrix of $C_{r,s}$ are distinct, meaning that there is no codeword of weight 2. As we know, the code $C_{r,s}$ has minimum distance three, if and only if there is a solution (X, Y) of the following system of equations:

$$\begin{aligned} Y^{2^i+1} + X^{2^i+1} + 1 &= 0 \\ Y^{2^j+1} + X^{2^j+1} + 1 &= 0 \end{aligned} \tag{33}$$

where X and Y are in $GF(2^m) \setminus \{0, 1\}$ and $X \neq Y$. We can express Y by means of X, using the first equation of (33). Note that the condition $gcd(2^i+1, 2^m-1) = 1$ implies that this correspondence is one-to-one.

Thus solving (33) is equivalent to solving the following equation with only one indeterminate:

$$(X^{2^i+1} + 1)^{\frac{2^j+1}{2^i+1}} + X^{2^j+1} + 1 = 0\ .$$

or equivalently

$$(X^{2^i+1} + 1)^{2^j+1} + (X^{2^j+1} + 1)^{2^i+1} = 0\ ,$$

which, by expanding the preceding, might be rewritten as:

$$X^{2^j(2^i+1)} + X^{2^i+1} + X^{2^i(2^j+1)} + X^{2^j+1} = 0\ .$$

The polynomial above, say $P(X)$, can be simply factorized:

$$P(X) = (X^{2^{i+j}} + X)(X^{2^j} + X^{2^i}) = (X^{2^{i+j}} + X)(X^{2^{j-i}} + X)^{2^i} .$$

We have proved that the code $C_{r,s}$ has minimum distance three, if and only if $P(X)$ has at least one root in $GF(2^m) \setminus \{0,1\}$. However, the roots of $P(X)$ are the elements of the fields $GF(2^{j+i})$ and $GF(2^{j-i})$. Hence we can conclude that $C_{r,s}$ has minimum distance three, if and only if $gcd(j+i, m) > 1$ or $gcd(j-i, m) > 1$; otherwise the code $C_{r,s}$ has minimum distance four or five. ■

Consider again the codes $C_{1,t}$. It is clear that such a code cannot contain a codeword of weight 2 (see Theorem 5). Suppose that it contains a codeword of weight 3. That means that, up to a shift, the system

$$\begin{cases} Y + X + 1 &= 0 \\ Y^t + X^t + 1 &= 0 \end{cases}$$

has at least one solution (X, Y) in $GF(2^m) \setminus \{0,1\}$, where $X \neq Y$. It is equivalent to say that the polynomial

$$U_t(X) \;=\; 1 \;+\; X^t \;+\; (1+X)^t \tag{34}$$

has at least one root in $GF(2^m) \setminus \{0,1\}$. Moreover if we know the factorization of $U_t(X)$, we can state a necessary and sufficient condition for the code $C_{1,t}$ to have minimum distance three (as we made above in Proposition 6). In [11], the authors obtained such a condition for any $t = 2^u \pm (2^v - 1)$, where v and u are any positive integers, $1 \leq v < u \leq m$.

Theorem 12 *[11] Let $C_{1,t}$ be a binary cyclic code of length $n = 2^m - 1$, where m is any integer, and let $t = 2^u \pm (2^v - 1)$, where u, v ($1 \leq v < u \leq m$) are arbitrary integers. Let*

$$g_1 = \begin{cases} gcd(m, u), & \text{if } t = 2^u + 2^v - 1, \\ gcd(m, u - v), & \text{if } t = 2^u - 2^v + 1, \end{cases} \tag{35}$$

and $g_2 = gcd(m, v)$. Then the code $C_{1,t}$ has minimum distance at least four, if and only if $g_1 = g_2 = 1$, and in all other cases the minimum distance is equal to three.

EXAMPLE 4. As an illustration of the previous theorem, we consider the cyclic codes $C_{1,t}$ for the cases $t = 2^i + 1$ and $t = 2^i + 3$. For the case $t = 2^i + 1$ we have immediately that $U_t(X) = X^{2^i} + X$. The polynomial $U_t(X)$ has roots in $GF(2^m) \setminus \{0,1\}$ if and only if $gcd(m, i) = 1$. When $t = 2^i + 3$ we obtain

$$\begin{aligned} U_t(X) &= 1 + X^{2^i+3} + (1+X)^{2^i+3} \\ &= X^{2^i+2} + X^{2^i+1} + X^{2^i} + X^3 + X^2 + X \\ &= (X^{2^i} + X)(X^2 + X + 1) . \end{aligned}$$

So the set of roots of $U_t(X)$ is the union of the fields $GF(2^2)$ and $GF(2^i)$. The polynomial $U_t(X)$ has no root in $GF(2^m) \setminus \{0,1\}$ if and only if $gcd(i, m) = 1$ and m odd.

4. Bent Functions and AB Functions

This section is devoted to the study of the properties of some Boolean function γ_F associated to the function F and whose definition follows.

Definition 9 *For any function F from V_m to itself, we denote by δ_F the integer-valued function on ${V_m}^2$ whose value at (a,b) is the number of solutions in V_m of the equation $F(x)+F(x+a)=b$. We denote by γ_F the Boolean function on ${V_m}^2$ whose value at (a,b) is 1 if $a \neq 0$ and $\delta_F(a,b) \neq 0$.*

EXAMPLE 5. Take $F(x)=x^{2^i+1}$, where i is co-prime with m. Then for any vectors a and b, $a \neq 0$, $\gamma_F(a,b)$ is equal to 1 if and only if there exists x such that $ax^{2^i}+a^{2^i}x+a^{2^i+1}=b$ or, equivalently

$$\left(\frac{x}{a}\right)^{2^i}+\frac{x}{a}=\frac{b}{a^{2^i+1}}+1.$$

Therefore, we have: $\gamma_F(a,b)=tr\left(\frac{b}{a^{2^i+1}}\right)$ (with $\frac{1}{0}=0$).

EXAMPLE 6. Take now $F(x)=x^{2^m-2}$, then for any nonzero vectors a and b, $\gamma_F(a,b)$ is equal to 1 if and only if there exists $x \neq 0,\ a$, such that $\dfrac{1}{x}+\dfrac{1}{x+a}=b$ (or, equivalently: $\left(\frac{x}{a}\right)^2+\frac{x}{a}=\frac{1}{ab}$). Therefore, we have:

$$\gamma_F(a,b)=tr\left(\frac{1}{ab}\right)+1+\Delta_0(a)+\Delta_0(b)+\Delta_0(a)\Delta_0(b)+\Delta_0(ab+1).$$

Open Question: what is the function γ_F where $F(x)=x^{2^{2i}-2^i+1}$ (with $gcd(i,m)=1$)?

4.1. *Properties of the Function γ_F*

Now we will characterize the APN and AB functions by means of the functions γ_F. In the proof of the next theorem, we will need the following lemma. In the sequel, $\Delta_0(a,b)$ denotes the Dirac symbol at (a,b), whose value is 1 if $(a,b)=(0,0)$ and 0 otherwise.

Lemma 4 *For any APN function F, the Walsh transform of the function $(\gamma_F)_\chi=(-1)^{\gamma_F}$ is equal to $2^{2m}\Delta_0-(\mu_F)^2+2^m$.*

Proof: Since F is APN, δ_F is equal to $2^m\Delta_0+2\,\gamma_F$, according to Definition 1. Since γ_F is Boolean, $(\gamma_F)_\chi$ is equal to $1-2\gamma_F$, that is $1-\delta_F+2^m\Delta_0$.

Now the Walsh transform of the constant function 1 is $2^{2m}\Delta_0$ and that of Δ_0 is the constant function 1. Hence, the Walsh transform of the function $(\gamma_F)_\chi$ is equal to $2^{2m}\Delta_0-\widehat{\delta_F}+2^m$.

It is well known that $\widehat{\delta_F}$ is equal to $(\mu_F)^2$ (cf. for instance [10]) . So, the Walsh transform of the function $(\gamma_F)_\chi$ is equal to $2^{2m}\Delta_0-(\mu_F)^2+2^m$, completing the proof. ■

In the next theorem, we call *dual* of a bent Boolean function f on V_m (cf. definition in Section 2.2) the Boolean function $\tilde{f}$ such that $\widehat{f_\chi} = 2^m\ \widetilde{f}_\chi$. It is a bent function too.

Theorem 13 *Let F be a function from V_m to itself. Then the following properties hold:*

(i) *F is APN if and only if the Boolean function γ_F has weight $2^{2m-1} - 2^{m-1}$.*
(ii) *F is AB if and only if γ_F is bent.*
(iii) *If F is an APN function, then the function $b \rightarrow \gamma_F(a,b)$ is balanced for any nonzero vector a – i.e. it takes equally often the values 1 and 0.*
(iv) *If F is an APN permutation, then the function $a \rightarrow \gamma_F(a,b)$ is balanced for any nonzero vector b.*
(v) *If F is AB, then the function $\widetilde{\gamma_F}$ is the Boolean function whose value at (a,b) is 1 if and only if $b \neq 0$ and $\mu_F(a,b) \neq 0$.*

Proof: **(i)** Obviously, adding all the values of $\delta_F(a,b)$, $b \in V_m$, being same as counting all the elements of V_m, the sum $\sum\limits_{b \in V_m} \delta_F(a,b)$, computed in **Z**, is equal to 2^m, for any a. Therefore

$$\sum_{a \in V_m{}^*,\ b \in V_m} \delta_F(a,b) = 2^{2m} - 2^m. \tag{36}$$

On the other hand, F is APN if and only if

$$\sum_{a \in V_m{}^*,\ b \in V_m} \delta_F(a,b) = 2 \sum_{a \in V_m{}^*,\ b \in V_m} \gamma_F(a,b).$$

So, F is APN if and only if the sum $\sum\limits_{a,b \in V_m} \gamma_F(a,b)$, computed in **Z**, is equal to $2^{2m-1} - 2^{m-1}$.

(ii) According to **(i)**, we may without loss of generality assume that F is APN. Indeed, if F is AB, then it is APN and if γ_F is bent, then its weight is $2^{2m-1} \pm 2^{m-1}$, that is $2^{2m-1} - 2^{m-1}$ since it is bounded by 2^{2m-1}. By definition, γ_F is bent if and only if the Walsh transform of the function $(\gamma_F)_\chi$ is equal to $\pm 2^m$, for every a, b. In fact, according to Parseval's relation, the sum of the squares of the values of the Walsh transform of the function $(\gamma_F)_\chi$ is equal to 2^{4m}. So, γ_F is bent if and only if, for any (a,b) *different from* $(0,0)$, the value at (a,b) of the Walsh transform of the function $(\gamma_F)_\chi$ is equal to $\pm 2^m$. According to Lemma 4, the Walsh transform of the function $(\gamma_F)_\chi$ is equal to:

$$2^{2m}\ \Delta_0 - (\mu_F)^2 + 2^m. \tag{37}$$

We deduce that γ_F is bent if and only if, for any (a,b) different from $(0,0)$, $(\mu_F)^2\,(a,b)$ is equal to 0 or to 2^{m+1}, that is if F is AB.

(iii) The sum $\sum_{b \in V_m} \delta_F(a,b)$ is equal to 2^m and it is also equal to $2\sum_{b \in V_m} \gamma_F(a,b)$ since F is APN.

(iv) If F is a permutation, we can apply **(iii)** to its inverse and deduce **(iv)**, since $\gamma_{F^{-1}}(a,b) = \gamma_F(b,a)$.

(v) The proof is a direct consequence of (37): $\widetilde{\gamma_F}$ equals 1 if and only if the Walsh transform of the function $(\gamma_F)_\chi$ is equal to -2^m, i.e. if and only if μ_F equals $\pm 2^{\frac{m+1}{2}}$. ■

Remark 6.
1. We know that any bent function on ${V_m}^2$ has algebraic degree at most m (see Definition 4). So, when F is AB, γ_F has algebraic degree at most m. That is not true for APN functions (consider $F:\ x \rightarrow x^{2^m-2}$).
2. When F is an AB power function, the bent function γ_F has the form described by H. Dobbertin in [14] under the name of triple-construction.

Corollary 5 *Under the hypothesis of Proposition 3, F is AB if and only if $F_1 \circ F_2^{-1}$ is AB.*

Proof: $\gamma_{F_1 \circ F_2^{-1}}(a,b)$ is equal to 1 if and only if $a \neq 0$ and if there exists (x,y) in $V_m \times V_m$ such that $F_2(x)+F_2(y)=a$ and $F_1(x)+F_1(y)=b$. Thus, $\gamma_{F_1 \circ F_2^{-1}}$ is equal to $\gamma_F \circ L^{-1}$, where $L=(L_1,L_2)$. The function $\gamma_{F_1 \circ F_2^{-1}}$ is therefore bent if and only if γ_F is bent. ■

4.2. The quadratic case revisited

We have already seen that any quadratic APN mapping is AB. We can deduce it also from Theorem 13 and say more, when F is a permutation. Recall that F is quadratic if and only if the function from $V_m \times V_m$ to V_m:

$$\varphi_F(x,y) = F(0)+F(x)+F(y)+F(x+y)$$

is bilinear. Let us show that there exists then a unique permutation G on V_m, such that, for any a and b:

$$\gamma_F(a,b) = \langle G(a), b\rangle.$$

For any nonzero vector a, $F(x)+F(x+a)$ is equal to $\varphi_F(x,a)+F(0)+F(a)$. Therefore, the set $E_a = \{F(x)+F(x+a)\ :\ x \in V_m\}$ is an affine subspace of V_m. Since F is a permutation, E_a does not contain 0. Since F is APN, E_a has cardinality 2^{m-1} and so is an hyperplane. Therefore, there exists a unique vector $G(a)$ such that $E_a = \{y \in V_m |\ \langle G(a), y\rangle = 1\}$. Complete G by setting $G(0)=0$. We have $\gamma_F(a,b) = \langle G(a), b\rangle$ for any vectors a and b. Since F is a permutation, the function $a \rightarrow \gamma_F(a,b)$ is balanced for any nonzero b, which means that G is a permutation. We know that, for every permutation G, the function $(a,b) \rightarrow \langle G(a), b\rangle$ is bent (cf. [13]). Thus, F is AB.

This result is more generally valid for any permutation F such that any space E_a is a flat. Thus, it is true if, for any b, the Boolean function $\langle b, F(x)\rangle$ is partially bent (cf. [7]): we know that, under this condition, for any nonzero a and b, the function $\langle b, F(x)+F(x+a)\rangle$ is either balanced or constant. According to [29], Chapter 13, Lemma 6, this implies that any space E_a is an hyperplane.

Notice that the rather natural conjecture that, for any AB function F and any nonzero b, the function $\langle b, F(x)\rangle$ is partially bent is false: for any nonzero b, the function $\langle b, F(x)\rangle$ would have degree at most $(m-1)/2$ and we know that there exist AB functions F whose algebraic degree is $(m+1)/2$.

We give now a sufficient condition for $F(x)$ to be AB.

Proposition 7 *Let $F(x)$ be a function from V_m to itself. A sufficient condition for $F(x)$ to be AB is that, for any nonzero b in V_m, the Boolean function $\langle b, F(x)\rangle$ is the restriction to V_m of a bent function on V_{m+1}, i.e. there exists a Boolean function $f_b(x)$ on V_m such that the Boolean function: $(x,\epsilon) \to \langle b, F(x)\rangle + \epsilon f_b(x)$ is bent on $V_m \times GF(2)$.*

Proof: We have

$$\sum_{x\in GF(2^m)} (-1)^{\langle b,F(x)\rangle+\langle a,x\rangle} = \frac{1}{2}\left(\sum_{(x,\epsilon)\in GF(2^m)\times GF(2)} (-1)^{\langle b,F(x)\rangle+\epsilon f_b(x)+\langle a,x\rangle} + \sum_{(x,\epsilon)\in GF(2^m)\times GF(2)} (-1)^{\langle b,F(x)\rangle+\epsilon f_b(x)+\langle a,x\rangle+\epsilon} \right).$$

Since the function $\langle b, F(x)\rangle + \epsilon f_b(x)$ is bent, for any a, these two last sums are both equal to $\pm 2^{\frac{m+1}{2}}$; their mean is then equal to $\pm 2^{\frac{m+1}{2}}$ or to 0. ■

Notice that f_b must be balanced for any $b \neq 0$, according to the properties of bent functions, and that it is impossible that $f_b(x) = \langle b, f(x)\rangle$ where $f(x)$ is a function from V_m to V_m: the function $F(x) + \epsilon f(x)$ from $V_m \times GF(2)$ to V_m would be bent, a contradiction since the dimension of $V_m \times GF(2)$ is not twice as great as that of V_m.

Remark 7. **(a)** Let F be any quadratic AB function, then it satisfies the hypothesis of Proposition 7: for any $b \neq 0$, $\langle b, F(x)\rangle$ is an element of the Reed-Muller code of order 2; the symplectic form associated to $\langle b, F(x)\rangle$ has the form $\langle L_b(x), y\rangle$, where L_b is linear (cf. [29], Chapter 15); F being AB, L_b has a kernel E_b of dimension 1; let $c \notin Im(L_b) \bigcup {E_b}^{\perp}$ (such an element always exists since $Im(L_b)$ and ${E_b}^{\perp}$ are linear hyperplanes) then it is a simple matter to check that the function

$$\langle b, F(x)\rangle + \epsilon \langle c, x\rangle$$

has a nondegenerate associated symplectic form, i.e. is bent.

(b) Identify V_m to $GF(2^m)$ and take as inner product $\langle x, y\rangle = tr(xy)$, where tr is the trace function from $GF(2^m)$ to $GF(2)$. If F is a power permutation on $GF(2^m)$, i.e. $F(x) = x^r$ with $gcd(r, 2^m - 1) = 1$, then it is enough to show the existence of f_b for one $b \neq 0$ only.

Acknowledgments

The authors wish to thank Hans Dobbertin for helpful discussions. In particular he indicated some result derived from Theorem 3 (cf. Remark 2) and a simplification of the proof of Lemma 1.

References

1. L.A. Bassalygo, G.V. Zaitsev, and V.A. Zinoviev, Uniformly packed codes, *Problems of Information Transmission*, Vol. 10, No 1 (1974) pp. 9-14.

2. L.A. Bassalygo and V.A. Zinoviev, Remark on uniformly packed codes, *Problems of Information Transmission*, Vol. 13, No 3 (1977) pp. 22-25.
3. E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, Vol. 4, No. 1 (1991) pp. 3-72.
4. A.E. Brouwer and L.M.G.M. Tolhuizen, A Sharpening of the Johnson Bound for Binary Linear Codes, *Designs, Codes and Cryptography*, Vol. 3, No. 1 (1993) pp. 95-98.
5. A.R. Calderbank, G. McGuire, B. Poonen and M. Rubinstein, On a conjecture of Helleseth regarding pairs of binary m-sequences, *IEEE Transactions on Information Theory*, Vol. 42 (1996) pp. 988-990.
6. P. Camion and A. Canteaut, Construction of t-resilient functions over a finite alphabet, Advances in Cryptology, EUROCRYPT'96, Lecture Notes in Computer Science, Springer-Verlag, New York, 1070 (1996) pp. 283-293 .
7. C. Carlet, Partially-bent functions, *Designs Codes and Cryptography*, Vol. 3 (1993) pp. 135-145.
8. C. Carlet, Two new classes of bent functions, Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, Springer-Verlag, New York, 765 (1994) pp. 77-101.
9. T. Cusick and H. Dobbertin, Some new 3-valued crosscorrelation functions of binary m-sequences, *IEEE Transactions on Information Theory*, Vol. 42 (1996) pp. 1238-1240.
10. F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis, Advances in Cryptology, EUROCRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, New York, 950 (1995) pp. 356-365.
11. P. Charpin, A. Tietäväinen and V. Zinoviev, On binary cyclic codes with $d = 3$, *Problems of Information Transmission*, Vol. 33, No. 3 (1997).
12. P. Delsarte, Four Fundamental parameters of a code and their combinatorial significance, *Inf. and Contr.* Vol. 23 (1973) pp. 407-438.
13. J.F. Dillon, Elementary Hadamard Difference Sets, Ph. D. Thesis, Univ. of Maryland (1974).
14. H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, Fast Software Encryption: Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms, Lecture Notes in Computer Science, Springer-Verlag, New York, 1008 (1995) pp. 61-74.
15. H. Dobbertin, One to one highly nonlinear power functions on $GF(2^n)$, preprint.
16. H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$, preprint.
17. H. Dobbertin, Another proof of Kasami's theorem, preprint.
18. S.M. Dodunekov and V.A. Zinoviev, V.A. A note on Preparata Codes, Proceedings of Sixth Intern. Symp. on Information Theory, Moscow - Tashkent Part 2 (1984) pp. 78-80.
19. J.M. Goethals and S.L. Snover, Nearly perfect codes, *Discrete Mathematics*, Vol. 3 (1972) pp. 64-88.
20. J.M. Goethals and H.C.A. Van Tilborg, Uniformly packed codes, *Philips Res. Repts* Vol. 30 (1975) pp. 9-36.
21. T. Helleseth and P.V. Kumar, Sequences with low correlation, *Handbook of coding theory* (V. S. Pless and W. C. Huffman, eds., R. A. Brualdi, asst. ed.), to appear.
22. H. Janwa, G. McGuire and R.M. Wilson Double-error-correcting codes and absolutely irreductible polynomials over $GF(2)$, *Journal of Algebra*, Vol. 178 (1995) pp. 665-676.
23. T. Kasami, Weight distributions of Bose-Chaudhuri-Hocquenghem Codes, *Combinatorial Math. and Applications* (R.C. Bose and T.A. Dowlings, eds.), Univ. of North Carolina Press, Chapel Hill, NC (1969).
24. T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, *Information and Control* Vol. 18 (1971) pp. 369-394.
25. G. Lachaud and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE Transactions on Information Theory*, Vol. 36 (1990) pp. 686-692.
26. R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20*, Cambridge University Press, Cambridge (1983).
27. Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph. D. Thesis, USCEE Rep. 409 (1972).
28. V. Pless, Power moment identities on weight distributions in error-correcting codes, *Info. and Control*, Vol. 6 (1963) pp. 147-152.
29. F.J. Mac Williams and N.J. Sloane, *The theory of error-correcting codes*, Amsterdam, The Netherlands: North Holland (1977).
30. M. Matsui, Linear cryptanalysis method for DES cipher, *Advances in Cryptography, EUROCRYPT'93*, Lecture Notes in Computer Science, Springer-Verlag, New York, 765 (1994) pp. 386-397,.
31. K. Nyberg,Perfect non-linear S-boxes, Advances in Cryptology, EUROCRYPT' 91, Lecture Notes in Computer Science, Springer-Verlag, New York, 547 (1992) pp. 378-386.

32. K. Nyberg, Differentially uniform mappings for cryptography, Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science, Springer-Verlag, New York, 765 (1994) pp. 55-64,.
33. O.S. Rothaus, On Bent Functions, *J. Comb. Theory*, Vol. 20A (1976) pp. 300- 305.
34. N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, Uniformly packed codes, *Problems of Information Transmission*, Vol. 7, No 1 (1971) pp. 38-50.
35. V.M. Sidel'nikov, On the mutual correlation of sequences, *Soviet Math. Dokl.*, Vol. 12 (1971) pp. 197-201