Designs, Codes and Cryptography, 37, 319–346, 2005

Highly Nonlinear Resilient Functions Through Disjoint Codes in Projective Spaces

PASCALE CHARPIN Pascale.Charpin@inria.fr
INRIA, project CODES, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France

ENES PASALIC enespasalic@yahoo.se
INRIA, project CODES, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France

Communicated by: J.D. Key

Received February 2, 2004; Revised September 17, 2004; Accepted September 22, 2004

Abstract. Functions which map n-bits to m-bits are important cryptographic sub-primitives in the design of additive stream ciphers. We construct highly nonlinear t-resilient such functions ((n, m, t) functions) by using a class of binary *disjoint codes*, a construction which was introduced in *IEEE Trans. Inform. Theory*, Vol. IT-49 (2) (2003). Our main contribution concerns the generation of suitable sets of such disjoint codes. We propose a deterministic method for finding disjoint codes of length vm by considering the points of $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$. We then obtain some lower bounds on the number of disjoint codes, by fixing some parameters. Through these sets, we deduce in certain cases the existence of resilient functions with very high nonlinearity values. We show how, thanks to our method, the degree and the differential properties of (n, m, t) functions can be improved.

Keywords: Boolean function, n-input m-output function, resilient function, nonlinearity, propagation characteristic, symmetric cryptography, stream cipher, linear code, projective space, complete weight enumerator

AMS Classification: 11T71

1. Introduction

A classical method for constructing key-stream generators is to combine a set of linear feedback shift registers with a nonlinear Boolean function, say f. Then f must fulfill certain properties in order to increase the time/space complexity of different attacks. Common attacks are Siegenthaler correlation attack [29], Berlekamp–Massey linearity synthesis attack [20] and different linear approximation attacks [10]. The main criteria that f should fulfill are: high-nonlinearity, high-algebraic degree, and resiliency of sufficient order. Also the propagation characteristics of f have to be considered.

In a modern design of a stream cipher, functions mapping to a block of output bits appear in many situations. These functions are of the form $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and

are called n-input m-output functions. In block cipher design such functions are referred to as S-boxes. S-boxes is a well-studied subject, and different important criteria have been considered. Since any such function F can be studied by means of its coordinates, which are Boolean functions, these criteria generalize those of Boolean functions.

For the case of Boolean functions ($m = 1$), there is a simple method of generating functions with some fixed resiliency and high nonlinearity, using the so-called Maiorana–McFarland construction [3]. This construction was developed or has been used as a basis for further improvements in e.g. [7, 26, 27]. We now have quite a lot of results for the case $m = 1$ [5, 26].

When $1 < m < n$ the situation is different. A few papers [8, 15, 16, 22, 32] have appeared before, providing nonlinear functions with some resiliency. Here we further develop the approach originally proposed in [15], where a set of disjoint codes has been used for construction of nonlinear resilient functions. However, the major problem with the construction in [15] was the fact that such a set is available through computer search (which becomes infeasible for a moderate cardinality of this set). Using the basic theory of projective spaces, we describe a set of disjoint codes which contains a large number of codes, for some fixed resiliency, and which is easy to handle. In many cases our design will generate resilient functions with much better nonlinearity compared to previous methods.

The paper is organized as follows. Section 2 provides basic definitions and notations both for 1-output and m-output functions, $m > 1$. In Section 3, we recall the known constructions; we explain the method for constructing highly nonlinear n-input m-output t-resilient functions by using disjoint linear codes introduced in [15]. In Section 4, we show how the points of some projective spaces can be fruitfully used in such a construction. We consider (n, m, t) functions. Fixing m and t, we obtain some bounds on the number of disjoint codes (Theorems 5–7). We finally present some numerical values for constructed functions and a comparison with previous constructions [16, 32]. In the last section we explain precisely how algebraic degree and differential properties of (n, m, t) functions can be improved.

Notation

– $\mathbb{F}_{2^m}$ is the finite field of order 2^m,

– β is a primitive root of $\mathbb{F}_{2^m}$,

– $\mathcal{B}_n$ is the set of Boolean functions of n variables,

– $\mathcal{M}_n^m$ is the set of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$,

– `card` E is the cardinal of some set E,

– $E^* = E \setminus \{0\}$,

– $|\Lambda|$ is the absolute value of any real value Λ,

– # [,] is defined before Table 1.

2. Preliminaries

In this paper, we study the cryptographic properties of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ where $1 < m < n$. We will denote by $\mathcal{M}_n^m$ the set of such functions. We denote by $\mathcal{B}_n$ the set of Boolean functions of n variables, i.e., the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

Any $F \in \mathcal{M}_n^m$ can be regarded as composed of m Boolean functions, its m-output *coordinate functions*. More generally, a *component function* of F is a nonzero linear combination of its coordinate functions. Thus we will often set $F = (f_1, \ldots, f_m)$ where $f_i \in \mathcal{B}_n$. A Boolean function f can be expressed in algebraic normal form (ANF), i.e., there are unique binary constants $\lambda_0, \lambda_1, \ldots, \lambda_{12}, \ldots, \lambda_{12\ldots n}$ such that:

$$f(x_1, \ldots, x_n) = \lambda_0 + \lambda_1 x_1 + \cdots + \lambda_n x_n + \lambda_{12} x_1 x_2 + \lambda_{13} x_1 x_3 + \cdots + \lambda_{12\ldots n} x_1 x_2 \cdots x_n, \tag{1}$$

where addition and multiplication are in $\mathbb{F}_2$.

Definition 1. The algebraic degree of f, denoted $\deg(f)$, is defined to be the maximum degree appearing in its ANF.

Many properties for Boolean functions are studied through the Walsh transform.

Definition 2. The Walsh transform of $f \in \mathcal{B}_n$ is defined to be the real-valued function $\mathcal{F}$:

$$\omega \in \mathbb{F}_2^n \mapsto \mathcal{F}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \omega \cdot x}, \tag{2}$$

where the *dot product* of vectors x and ω is defined as $x \cdot \omega = x_1 \omega_1 + \cdots + x_n w_n$.

We say that the Boolean function f *is balanced* if the probability of $f(x) = 1$ is the same as the probability of $f(x) = 0$. Alternatively, using the Walsh transform, f is balanced if and only if $\mathcal{F}(0) = 0$. For two functions of $\mathcal{B}_n$, say f and g, the Hamming distance between them is defined as

$$d_H(f, g) = \mathtt{card}\{x \mid f(x) \neq g(x), x \in \mathbb{F}_2^n\}. \tag{3}$$

Definition 3. The *nonlinearity* of $f \in \mathcal{B}_n$, denoted by $\mathcal{N}(f)$, is defined as

$$\mathcal{N}(f) = \min_{g \in \mathcal{A}_n} d_H(f, g), \tag{4}$$

where $\mathcal{A}_n$ is the set of all affine functions of n variables,

$$\mathcal{A}_n = \left\{ a_0 + \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{F}_2, 0 \leq i \leq n \right\}.$$

The nonlinearity of f can be obtained through the Walsh transform as follows:

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |\mathcal{F}(\omega)|. \tag{5}$$

Finding Boolean functions with maximal nonlinearity is an important and well studied problem. For n even, maximal nonlinearity is obtained by the *bent functions* [19, 25]. For n odd, maximal nonlinearity is only known for $n < 9$, and determining it for $n \geq 9$ looks as very hard challenge [23, 24]. Since bent functions are not balanced, another hard open problem is to find the maximum nonlinearity for balanced functions when n is even [11].

Now the next definition concerns the function's ability not to leak information to the output when a subset of the input variables is kept fixed. The so-called *resiliency* was characterized in the Walsh transform domain by Xiao and Massey [33].

Definition 4. A function $f \in \mathcal{B}_n$ is resilient of order t (t-resilient) if and only if

$$\mathcal{F}(\omega) = 0 \quad \text{for all } \omega \in \mathbb{F}_2^n \quad \text{such that } 0 \leq wt(w) \leq t, \tag{6}$$

where $wt(\omega)$ denotes the Hamming weight of ω, i.e., the number of ones in ω.

This paper will be directed towards the study of trade-offs between resiliency and nonlinearity for functions of $\mathcal{M}_n^m$. As any $F \in \mathcal{M}_n^m$ is fully defined through its component functions, we are going to state the cryptographic properties of such F, generalizing the previous properties. We start with a formal definition of resilient functions.

Definition 5. Let $F \in \mathcal{M}_n^m$; let t be a positive integer such that $t \leq n - m$. The vector x, describing $\mathbb{F}_2^n$, is $x = (x_1, x_2, \ldots, x_n)$ where $x_i \in \mathbb{F}_2$.

1. Let $T = \{j_1, \ldots, j_t\}$ be any subset of $\{1, \ldots, n\}$ and $\{i_1, \ldots, i_{n-t}\} = \{1, \ldots, n\} - T$, where T has cardinality t. Then F is said to be unbiased with respect to (w.r.t.) T if for every $(a_1, \ldots, a_t) \in \mathbb{F}_2^t$

   $$F(x_1, x_2, \ldots, x_n)|_{x_{j_1} = a_1, \ldots, x_{j_t} = a_t}$$

   runs through all the vectors in $\mathbb{F}_2^m$, each 2^{n-m-t} times, when $(x_{i_1}, \ldots, x_{i_{n-t}})$ runs through $\mathbb{F}_2^{n-t}$. The function F is said to be unbiased when $F(x)$ takes all values in $\mathbb{F}_2^m$, each 2^{n-m} when x runs through $\mathbb{F}_2^n$.
2. F is said to be an (n, m, t)-resilient function if F is unbiased w.r.t. every subset T of $\{1, \ldots, n\}$ of cardinality t. The parameter t is called the resiliency of the function.

The next theorem gives the relationship between a resilient function and its component functions. This comes from the next lemma, which is well-known and called the *XOR Lemma* [32]. The proof of this lemma can be found in a more general context in [17, Theorem 7.37]. In order to replace Definition 5 in this context, we recall a basic property.

Let $F \in \mathcal{M}_n^m$, $F = (f_1, f_2, \ldots, f_m)$ and $1 \le m \le n$, where each f_i is in $\mathcal{B}_n$. Then $f_1, f_2, \ldots, f_m$ is said to be an orthogonal system of polynomials if for each $(a_1, a_2, \ldots, a_m)$ *in* $\mathbb{F}_2^m$

$$f_1(x_1, \ldots, x_n) = a_1, \ldots, f_m(x_1, \ldots, x_n) = a_m$$

has exactly 2^{n-m} solutions in $\mathbb{F}_2^n$ (Definition 7.35, [17]). According to Definition 5, F is *unbiased* if it runs through all the vectors in $\mathbb{F}_2^m$, each 2^{n-m} times, when $(x_1, \ldots, x_n)$ runs through $\mathbb{F}_2^n$. Thus F is *unbiased* if and only if $f_1, f_2, \ldots, f_m$ is an orthogonal system of Boolean functions.

LEMMA 1. *A function* $F = (f_1, f_2, \ldots, f_m)$, *where* $f_i \in \mathcal{B}_n, 1 \le i \le m$, *is unbiased if and only if all nonzero linear combinations of the functions* $f_1, \ldots, f_m$ *are balanced.*

Hence, an immediate consequence of the previous lemma is the following.

THEOREM 1. *Let t, m such that* $t + m \le n$. *A function* $F = (f_1, f_2, \ldots, f_m)$ *is an* (n, m, t)*-resilient function if and only if all nonzero linear combinations of* $f_1, f_2, \ldots, f_m$ *are* $(n, 1, t)$*-resilient functions,* i.e., *are t-resilient functions of* $\mathcal{B}_n$.

Proof. By definition, F is an (n, m, t)-resilient function if and only if, by fixing any set of t variables, F becomes a function F' such that:

$$F' : \mathbb{F}_2^{n-t} \mapsto \mathbb{F}_2^m \quad \text{and} \quad F' \text{is unbiased.}$$

From Lemma 1 this means that any component function of F' is balanced. From Definition 4, this is equivalent to say that any component function of F is a t-resilient Boolean function. ∎

Nonlinearity of $F \in \mathcal{M}_n^m$, introduced in [21], follows in a similar manner.

Definition 6. The nonlinearity of $F = (f_1, f_2, \ldots, f_m)$, denoted by $\mathcal{N}(F)$, is defined as the minimum among the nonlinearities of all its component functions:

$$\mathcal{N}(F) = \min_{b \in \mathbb{F}_2^m, b \neq 0} \mathcal{N}(f^{(b)}), \quad f^{(b)} = \sum_{i=1}^{m} b_i f_i. \tag{7}$$

Similarly, the *algebraic degree* of $F = (f_1, f_2, \ldots, f_m)$ is defined as the minimum of degrees of component functions of F, namely,

$$\deg(F) = \min_{b \in \mathbb{F}_2^m, b \neq 0} \deg(f^{(b)}), \quad f^{(b)} = \sum_{i=1}^{m} b_i f_i. \tag{8}$$

Remark 1. In accordance with (7) and (8), we get bounds on $\mathcal{N}(F)$ and on $\deg(F)$ by means of known bounds on resilient Boolean functions. For instance, recall the bound on the divisibility of $f \in \mathcal{B}_n$, which is t-resilient of degree r[4]:

$$\mathcal{F}(\omega) \equiv 0 \pmod{2^{t+2+\lfloor \frac{n-t-2}{r} \rfloor}}, \quad \forall \omega \in \mathbb{F}_2^n.$$

Assume that F is an (n, m, t)-resilient function; we then deduce

$$\mathcal{N}(F) \leq 2^{n-1} - 2^{t+1+\lfloor \frac{n-t-2}{r} \rfloor}, \tag{9}$$

where r is obtained from (8). This bound is significant for $t \geq n/2 - 2$ and then $m \leq n/2 + 2$; actually it is only significant for $n/2 - 2 \leq t \leq n/2$ and then $n/2 \leq m \leq n/2 + 2$. Indeed, it is well-known[1] that the resiliency t is upper bounded by

$$t \leq \left\lfloor \frac{2^{m-1} n}{2^m - 1} \right\rfloor - 1. \tag{10}$$

This upper bound, which implies $t \leq n/2$, is tighter than the bound derived directly from the definition of resiliency ($t \leq n - m$). For instance, for $n = 10, m = 2$ the equation (10) gives $t \leq 5$, whereas the trivial bound only indicates that $t \leq 8$.

3. Resilient Functions in $\mathcal{M}_n^m$ and Linear Codes

The connection between linear resilient functions and linear codes was established in [2, 9], and the equivalence between resilient functions and large set of orthogonal arrays was considered in [30]. The most simple construction for resilient functions of $\mathcal{M}_n^m$ uses linear error-correcting codes. Then any bound on binary linear code leads to some bound on resiliency. According to this construction, it is convenient to define *linear resilient functions* which are simply resilient functions whose coordinates functions and any nonzero linear combination of these are linear.

Recall that any *linear binary code* C of length n is a subspace of $\mathbb{F}_2^n$; thus it is defined by any *generating matrix* whose rows form a basis of C. The *minimum distance* of C is the smallest Hamming weight of its nonzero codewords. Such a code C of length n, dimension m and minimum distance δ is said to be an $[n, m, \delta]$ binary code.

THEOREM 2 [1]. *Let C be an $[n, m, t+1]$ binary code. Let $\mathcal{G}$ be an $m \times n$ generating matrix of C. Define $F \in \mathcal{M}_n^m$ by*

$$F(x_1, \ldots, x_n) = \mathcal{G} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Then F is an (n, m, t)-resilient function. Such a function F is said to be a linear resilient function. In other words, there exists a linear (n, m, t)-resilient function if and only if there exists a linear $[n, m, t+1]$ code.

[1] This has been proved in [12]; see another proof in [1].

Note that a class of functions reaching the upper bound in (10) is easily derived by applying Theorem 2 to the Simplex code, which is a linear $[2^m - 1, m, 2^{m-1}]$ code [22]. For clarity, we now explain Theorem 2 by an example using the [7, 3, 4] Simplex code.

EXAMPLE 1. *Let* C *be a* [7,3,4] *binary linear code with generating matrix*

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Thus we can define a (7, 3, 3)-resilient function $F \in \mathcal{M}_7^3$ which is linear:

$$F(x_1, \ldots, x_7) = \begin{cases} f_1 = x_1 + x_4 + x_5 + x_6, \\ f_2 = x_2 + x_4 + x_5 + x_7, \\ f_3 = x_3 + x_4 + x_6 + x_7. \end{cases}$$

Any linear combination g of the f_i is a linear function with at least four terms, since the minimum distance of C is 4. Thus, any g is clearly 3-resilient. And the bound (10) is reached since $(7 \times 4)/7 - 1 = 3 = t$. ■

3.1. Linear-like Resilient Functions

By applying any nonlinear permutation to any linear resilient function, one easily generalizes the previous construction. This was exploited by Zhang and Zheng in [32].

Let F be a linear (n, m, t)-resilient function and let P be any permutation on $\mathbb{F}_2^m$. Then the function $H = P \circ F$ is an (n, m, t)-resilient function which is nonlinear. Indeed if F satisfies Definition 5, item 2, this holds for $P \circ F$, as soon as P is a permutation on $\mathbb{F}_2^m$. Note that this holds even if F is not linear and independently of the value of t; indeed the value of t comes from the number of terms in the linear component functions of F.

Set $F = (f_1, \ldots, f_m)$ and $P = (p_1, \ldots, p_m)$ where $f_i \in \mathcal{B}_n$ and $p_i \in \mathcal{B}_m$. Since the f_i are linear and linearly independent, we obtain a basis of $\mathbb{F}_2^n$ by taking for each $i, 1 \le i \le m$,

$$u_i = (f_i(x), x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n),$$

which we complete with $u_{m+1}, \ldots, u_n$. Let us denote by V the m-dimensional subspace defined by the $n - m$ equations $u_{m+1} = \cdots = u_n = 0$. Thus we get

$$H(x) = (p_1(f_1(x)), \ldots, p_m(f_m(x))) = P(u_1, \ldots, u_m),$$

which is independent from $u_{m+1}, \ldots, u_n$. This is to say that the restrictions of H on V and on its cosets are equal to P. Note that H is linear if and only if P is linear too. Thus the Theorem 3 of [32] can be stated more precisely:

THEOREM 3. *Let $H = P \circ F$, where F is a linear (n, m, t)-resilient function and P is any permutation on $\mathbb{F}_2^m$. Then we have*:

- *there is an m-dimensional subspace V of $\mathbb{F}_2^n$ such that the restrictions of H on the cosets of V are equal to P*;
- *the image of H, an $m \times 2^n$ matrix on $\mathbb{F}_2$, can be viewed as a concatenation of 2^{n-m} times $\mathbb{F}_2^m$, each part being equal to $P(V)$*;
- *the degree of H equals the degree of P*;
- *the nonlinearity of H equals $2^{n-m}\mathcal{N}(P)$.*
  We will say that H is a linear-like (n, m, t)-resilient function.

From the previous construction, we get an (n, m, t)-resilient function H, which is nonlinear but can be written, up to a linear permutation as $(P, \ldots, P)$ (2^{n-m} times the chosen permutation P). One can say that, in a certain sense, the period of the sequence produced by $H(x)$ could be short. Moreover the degree and the nonlinearity are strongly bounded by the parameters of P. The authors of [32] proposed the design of nonlinear $(2^m - 1, m, 2^{m-1} - 1)$ resilient functions with a nonlinearity of at least $2^{2^m-2} - 2^{2^m-1-(m/2)}$ and the algebraic degree $m - 1$.

3.2. *A Construction of Highly Nonlinear (n, m, t)-Resilient Functions*

In [16], concatenation of resilient functions with bent functions was used in order to obtain nonlinear resilient functions of $\mathcal{M}_n^m$. Another approach has been taken in [15] where disjoint linear codes has been used for the same purpose. The main problem which is still unsolved is the way of finding such disjoint codes, relying only on a computer search for such codes. In a recent work [22] the known construction methods have been merged into a general construction technique that uses the existence of a single linear code with certain parameters. This technique has been later modified in [14] slightly improving the results in [22] by utilizing all the $2^k - 1$ nonzero codewords of a linear $[u, k, t+1]$ code rather than only 2^{k-1}.

In this section, we recall the construction of t-resilient functions $F \in \mathcal{M}_n^m$ with high nonlinearity introduced in [15]. The next lemma enables us to use all the nonzero codewords of a linear code.

LEMMA 2. [15]. *Let C be any binary $[u, m, \delta]$ linear code, with generating matrix $\mathcal{G}$. Let β be a primitive element in the field $\mathbb{F}_{2^m}$ providing the polynomial basis $(1, \beta, \ldots, \beta^{m-1})$ of $\mathbb{F}_{2^m}$. Define the linear bijection $\phi: \mathbb{F}_{2^m} \mapsto C$ by*

$$\phi(a_0 + a_1\beta + \cdots + a_{m-1}\beta^{m-1}) = (a_0 \cdots a_{m-1})\mathcal{G}$$

(*simply by encoding $(a_0, \ldots, a_{m-1})$*). *Consider the $2^m - 1 \times m$ matrix*:

$$\mathcal{A}=\begin{pmatrix} \phi(1) & \phi(\beta) & \cdots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \cdots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi(\beta^{2^m-2}) & \phi(1) & \cdots & \phi(\beta^{m-2}) \end{pmatrix}.$$

Then, for any nonzero linear combination of columns of the matrix $\mathcal{A}$, each nonzero codeword of C appears exactly once.

According to the previous lemma, we can obtain nonlinear functions F and then improve the construction of Theorem 2. We explain this, by an example.

EXAMPLE 2. *We extend the discussion presented in Example* 1. *The code C has seven nonzero codewords. Then, using the matrix $\mathcal{A}$. of Lemma* 2, *we can construct the component functions, say $f_i, i=1,\ldots,3$, by concatenating the linear functions corresponding to the elements in the ith column of $\mathcal{A}$.*

This could give us an output of length 7×2^7. However we only use four rows of $\mathcal{A}$, since the input space is always a power of two. This enables a construction of F, where $F(y,x):\mathbb{F}_2^2\times\mathbb{F}_2^7\cdot\mapsto\mathbb{F}_2^3$.

Let us for $0\le i\le 6$ define the linear functions $\ell_i(x)=\phi(\beta^i)\ .\ x$, where $x=(x_1,\ldots,x_7)$ and "$\cdot$" is the scalar product in $\mathbb{F}_2^7$. Then, with the four first lines of $\mathcal{A}$, define $F(y,x)$ by its coordinate functions:

$$f_1=(y_1+1)(y_2+1)\ell_0(x)+(y_1+1)y_2\ell_1(x)+y_1(y_2+1)\ell_2(x)+y_1y_2\ell_3(x),$$
$$f_2=(y_1+1)(y_2+1)\ell_1(x)+(y_1+1)y_2\ell_2(x)+y_1(y_2+1)\ell_3(x)+y_1y_2\ell_4(x),$$
$$f_3=(y_1+1)(y_2+1)\ell_2(x)+(y_1+1)y_2\ell_3(x)+y_1(y_2+1)\ell_4(x)+y_1y_2\ell_5(x).$$

Due to the properties of $\mathcal{A}$, any linear combination of the f_i, say g, is a concatenation of four linear functions in $\mathcal{B}_7$; these functions have at least four terms and are two by two different (from Lemma 2). Thus g is 3 resilient and as a consequence of Theorem 1 F is 3-resilient too. Hence F is a (9, 3, 3) nonlinear function with $\mathcal{N}_F=2^8-2^6=192$, which is readily checked. ■

Definition 7. [15]. Let $\{C_1,C_2,\ldots,C_s\}$ be a set of linear binary codes with the same parameters $[u,m,\delta]$. It is called a set of disjoint codes if it is such that

$$C_i\cap C_j=\{0\},\quad 1\le i<j\le s.$$

Definition 8. Let us consider the set of binary linear codes of length u, dimension m and minimum distance δ. Let $\mathcal{D}$ be the set of sequences of disjoint codes, as defined in Definition 7. Then we denote by $M(u,m,\delta)$ the maximal cardinality of elements of $\mathcal{D}$.

In [15], two lower bounds on $M(u, m, \delta)$ were derived. However, these bounds only state the existence of a set of disjoint codes of cardinality at least $M(u, m, \delta)$, These results are only of theoretical importance since no deterministic method was suggested for finding such codes. Our interest is for constructible sets of $[u, m, \delta]$ disjoint codes with high cardinality and easy to handle. All the ideas of using disjoint codes may be summarized by the following result due to Johansson and Pasalic [15].

THEOREM 4. [15]. *If there exists a set of linear* $[u, m, t+1]$ *disjoint codes with cardinality* $[2^{n-u}/(2^m-1)]$ *then there exists an* (n, m, t)*-résilient function* F *with nonlinearity*

$$\mathcal{N}(F) = 2^{n-1} - 2^{u-1}.$$

The proof of Theorem 4 is to be found in [15] but for convenience we briefly recapture the main idea of this construction. Also, the next example will further clarify the construction method based on disjoint codes. It concerns the construction of a (9, 2, 3) nonlinear resilient function based on the existence of sufficiently many disjoint [6, 2, 4] linear codes.

Any linear $[u, m, t+1]$ code provides $2^m - 1$ nonzero codewords that can be used by means of Lemma 2. Thus one concatenates t-resilient linear functions since the minimum distance of the code is $t+1$ and only nonzero codewords are used (see Theorem 2). Then to construct a function $F \in \mathcal{M}_n^m$, we obviously need 2^{n-u} such codewords (since $F(x)$ takes 2^n values). Hence supplied with at least $\lceil 2^{n-u}/2^{m-1} \rceil$ disjoint linear codes we will be able to concatenate these t-resilient linear functions by means of Lemma 2 to obtain F. Remark that the nonlinearity value only depends on the length of the codes used. Then having the set of disjoint codes at our disposal the aim is to construct F with n as large as possible.

EXAMPLE 3. *Consider the construction of a* 3*-resilient function* $F \in \mathcal{M}_9^2$,

$$F : (y, x) \in \mathbb{F}_2^3 \times \mathbb{F}_2^6 \mapsto F(y, x) \in \mathbb{F}_2^2$$

based on the set of disjoint [6, 2, 4] *linear codes. Using the sane notation as in Theorem* 4 *we have* $n = 9, u = 6, m = 2$ *and* $t = 3$. *Hence we need* $\lceil 2^3/(2^2-1) \rceil = 3$ *disjoint* [6, 2, 4] *linear codes. We take three such codes* C_1, C_2, C_3 *whose generator matrices are given by,*

$$\mathcal{G}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \mathcal{G}_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad \mathcal{G}_3 \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Then we can form, from each $\mathcal{G}_i$, its matrix $\mathcal{A}_i$ (of Lemma 2). Consider now the concatenation of the three matrices $\mathcal{A}_i$, since we need $2^{n-u} = 8$ lines only, we do not take the last line of $\mathcal{A}_3$. Note that the first three rows of $\mathcal{A}$ are derived from

C_1 by means of Lemma 2, the next three rows of $\mathcal{A}$ are obtained from C_2 and finally the last two rows from C_3.

$$\mathcal{A}=\left(\begin{array}{c}(111100)\ (001111)\\(001111)\ (110011)\\(110011)\ (111100)\\\hline(011110)\ (100111)\\(100111)\ (111001)\\(111001)\ (011110)\\\hline(010111)\ (101101)\\(101101)\ (111010)\end{array}\right).$$

Then we define the function $F=(f_1, f_2)$ as $F(y,x)=(A_y^1\cdot x, \mathcal{A}_y^2\cdot x)$. Here, for any fixed y the entry $\mathcal{A}_y^i, i=1,2$, corresponds to the $[y]$-th row and the i-th column of $\mathcal{A}$, where $[y]$ is a decimal representation of $y\in\mathbb{F}_2^{n-u}$.

The function F is a (9, 2, 3)-resilient function with nonlinearity $\mathcal{N}_F=224$. It is easily verified that the linear combinations of the vectors in each row of $\mathcal{A}$ yield new vectors all having the weight greater than or equal to four. Furthermore, none of the vectors appears more than once in each column of $\mathcal{A}$ or in any linear combination of $\mathcal{A}$'s columns. Thus, F is. 3-resilient and the nonlinearity of F is given by,

$$\mathcal{N}_F=2^{n-1}-2^{u-1}=224. \qquad \blacksquare$$

Obviously there is a room for extension of Theorem 4 by using a set of disjoint linear codes of not necessarily same dimension.

COROLLARY 1. *If there exists a set* $\mathcal{C}=\{C_i|i\in I\}$ *of linear* $[u, m_i, t+1]$ *disjoint codes such that* $\sum_{i\in I}(2^{m_i}-1)/2^{n-u}\geq 1$, *then there exists a t-resilient function* $F\in\mathcal{M}_n^m$, *where* $m=\min_{i\in I} m_i$, *with nonlinearity*

$$\mathcal{N}(F)=2^{n-1}-2^{u-1}.$$

4. Disjoint Codes through Counting the Points in Projective Spaces

We first give a brief background on projective spaces in our context. Let F_{2^m} be a finite field of order 2^m, and let V be a ν-dimensional vector space over the field $\mathbb{F}_{2^m}$. Then, let us consider the following equivalence relation on the elements of V^*. For any pair $(x, y)\in V^*\times V^*$:

$$x\sim y \iff \exists\lambda\in\mathbb{F}_{2^m}^* \quad \text{such that} \quad \lambda x=y.$$

The relation $\sim$ divides the elements of V^* into the set of $(2^{\nu m}-1)/(2^m-1)$ equivalence classes, called *points*. This set of points is called the $(\nu-1)$ dimensional

projective space over $\mathbb{F}_{2^m}$, and is denoted by $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$. Note that any point in $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$, can be regarded as an m-dimensional vector subspace of $\mathbb{F}_2^{vm}$ with the all-zero vector discarded. This identification is obtained by introducing a natural isomorphism between $\mathbb{F}_{2^m}$ and $\mathbb{F}_2^m$.

In other words, we can consider any point as a linear code C of length v over $\mathbb{F}_{2^m}$ but also as a linear code C' of length vm and dimension m over $\mathbb{F}_2$. For instance, consider $x = (x_0, \ldots, x_{v-1})$ in V^*. Let β be a primitive root of $\mathbb{F}_{2^m}$; so $\langle 1, \beta, \ldots, \beta^{m-1} \rangle$ is a basis of $\mathbb{F}_{2^m}$. The class of x, a point, is here identified to a $[v, m]$-code C with generator matrix

$$\mathcal{G} = \begin{bmatrix} x_0 & \ldots & \ldots & x_{v-1} \\ \beta x_0 & \ldots & \ldots & \beta x_{v-1} \\ \ldots & \ldots & \ldots & \ldots \\ \beta^{m-1} x_0 & \ldots & \ldots & \beta^{m-1} x_{v-1} \end{bmatrix}.$$

Since each entry of $\mathcal{G}$ is in $\mathbb{F}_{2^m}$, it can be seen as a codeword of length m providing a $[vm, m]$-code C', Note that in coding theory the code C' is usually called the *binary image of the code* C.[2] By definition, the elements of $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$, and therefore the codes derived from points, are two by two disjoint.

Thus the basic idea, when using projective spaces for our purpose of finding disjoint $[u, m, t+1]$-codes over $\mathbb{F}_2$, is to work in $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$, when $u = vm$. That is, to count such disjoint codes is equivalent to counting the points in $\mathbf{PG}(v-1, \mathbb{F}_{2^m})$ such that the derived $[vm, m]$-code has minimum distance $t+1$.

We will see in the next developments that it is easy to characterize such points. For instance, the points of weight $t+1$ are suitable. Note that, at the first sight, the condition $u \geq v(t+1)$ seems necessary. It is not the case, since there exist points of weight t whose binary images have weight greater than $t+1$.

Recall that β is some primitive element of $\mathbb{F}_{2^m}$, the finite field of order $2^m, m > 2$. Then each element β^i of $\mathbb{F}_{2^m}^*$ will be represented by means of the basis $\langle 1, \beta, \ldots, \beta^{m-1} \rangle$, providing the natural isomorphism between $\mathbb{F}_{2^m}$ and $\mathbb{F}_2^m$:

$$\mathcal{I} : \beta^j \in \mathbb{F}_{2^m} \mapsto (a_0, \ldots, a_{m-1}) \in \mathbb{F}_2^m, \quad \text{where} \quad \beta^j = \sum_{i=0}^{m-1} a_i \beta^i. \tag{11}$$

The vector $(a_0, \ldots, a_{m-1})$ is called *the binary image of* β^j. Note that the Hamming weight of β^j equals 1 while the Hamming weight of its binary image equals $\sum_{i=0}^{m-1} a_i$. We need to define this more generally.

Definition 9. Let $v = (v_1, \ldots, v_r)$ be a vector of $\mathbb{F}_{2^m}^r$. The binary image of v is defined by expanding (11):

$$\mathcal{I}(v) = (\mathcal{I}(v_1), \ldots, \mathcal{I}(v_r)).$$

[2] See an elementary presentation in [18], Chapter 10, Section 5.

We call binary Hamming weight of v, and denote by $wt_2(v)$, the Hamming weight of the binary image of v: $wt_2(v) = wt(\mathcal{I}(v))$.

Let C be a linear $[r, m]$-code on F_{2^m} with basis $\langle e_0, \ldots, e_{m-1}\rangle$. The binary image of C, denoted $\mathcal{I}(C)$, is the linear $[rm, m]$-code with basis $\langle \mathcal{I}(e_0), \ldots, \mathcal{I}(e_{m-1})\rangle$.

LEMMA 3. *Let β denotes a primitive element of $\mathbb{F}_{2^m}$. Consider any point of* $\mathbf{PG}(1, \mathbb{F}_{2^m})$*, identified to a* $[2, m]$*-code C, with representative* $(1, \beta^\ell)$ *for some* $\ell \in [1, 2^m - 2]$.

Then the code $\mathcal{I}(C)$ is a $[2m, m, \delta]$ binary code such that $\delta \geq 3$ if and only if ℓ is such that $m \leq \ell \leq 2^m - m - 1$, where $m > 2$.

Proof. By fixing the polynomial basis of $\mathbb{F}_2^m$ to be $\langle 1, \beta, \ldots, \beta^{m-1}\rangle$, any $\beta^i \in \mathbb{F}_{2^m}$ is such that $wt_2(\beta^i) = 1$ if and only if $i \in [0, m-1]$. By definition, C is the set of the codewords $(\beta^i, \beta^{i+\ell}, i \in [0, 2^m - 2]$, where $i + \ell$ is calculated modulo $2^m - 1$.

Clearly, $\mathcal{I}(C)$ has minimum distance at least three if and only if at least one element of the pair $(i, i + \ell)$ is not in $[0, m-1]$, for all i. If $\ell \in [m, 2^m - m - 1]$ then $i + \ell \in [m, 2^m - 1]$, for all $i \in [0, m-1]$. Conversely, assume that

$$i \in [0, m-1] \quad \Longrightarrow \quad m \leq i + \ell \pmod{2^m - 1}.$$

Setting $i = 0$, we get $m \leq \ell$. On the other hand, if $\ell > 2^m - m - 1$ then there is $i \in [1, m-1]$ such that $\ell + i = 2^m - 1$, i.e. $\ell + i \equiv 0$, a contradiction. Thus $\ell \leq 2^m - m - 1$. ∎

4.1. Lower Bound on the Number of Disjoint $[tm, m, t+1]$ Codes

We first derive a bound on $M(tm, m, t+1)$, by counting some points of $\mathbf{PG}(t-1, \mathbb{F}_{2^m})$.

THEOREM 5. *The number of disjoint binary $[tm, m, t+1]$-codes derived from the points of* $\mathbf{PG}(t-1, \mathbb{F}_{2^m})$ *is lower bounded by:*

$$M^{lb}(tm, m, t+1) = (2^m - 2m) \sum_{i=0}^{t-2} (2m-1)^i (2^m - 1)^{t-2-i}.$$

This leads to a lower bound on the number , $M(tm, m, t+1)$, introduced in Definition 8.

Proof. Set $I = [m, 2^m - m - 1)$; note that I has cardinality $2^m - 2m$. Now we want to count *many* points of $\mathbf{PG}(t-1, \mathbb{F}_{2^m})$ which produce $[tm, m, t+1]$-codes. We consider the points Λ whose representatives $(\lambda_1, \ldots, \lambda_t)$ satisfy:

1. $\lambda_i \neq 0$ for all $i \in [1, t]$,
2. there is at least one pair (λ_r, λ_s) with representative $(1, \beta^\ell)$, $\ell \in I$.

The first condition implies that Λ, as well as any element of its class, is such that $wt(\Lambda)=t$. The second condition implies that each corresponding binary image has weight at least $t+1$, according to Lemma 3.

The most convenient way to count such points is to fix, say $\lambda_1=1$, and consider the points of the form $(1,\lambda_2,\ldots,\lambda_t)$. Clearly, any choice of $(\lambda_2,\ldots,\lambda_t)\in(\mathbb{F}_{2^m}^*)^{t-1}$ gives a distinct point, hence one disjoint code.

By choosing $\lambda_2=\beta^i$ for $i\in I$, we may take any $(\lambda_3,\ldots,\lambda_t)\in(\mathbb{F}_{2^m}^*)^{t-2}$ This gives $(2^m-2m)(2^m-1)^{t-2}$ points. When selecting $\lambda_2=\beta^j$ for $j\notin I$, we have to select $\lambda_3=\beta^i$ for $i\in I$ and the remaining $t-3$ coordinates are chosen arbitrary from $(\mathbb{F}_{2^m}^*)^{t-3}$. This gives a general recursion of the form $(2^m-2m)(2m-1)^k(2^m-1)^{t-2-k}$, for $k=1,\ldots,t-2$.

Summarizing this, we may write

$$M^{lb}(tm,m,t+1)=(2^m-2m)(2^m-1)^{t-2}+(2^m-2m)\sum_{k=1}^{t-2}(2m-1)^k(2^m-1)^{t-2-k},$$

which can be rewritten as stated. ■

Remark 2. By the previous theorem we proved implicitly that for $t=2$, $M^{lb}(2m,m,3)$, which is equal to 2^m-2m, is exactly the number of $[2m,m,3]$ disjoint codes derived from $\mathbf{PG}(2,\mathbb{F}_{2^m})$. For $t=3$ then $M^{lb}(3m,m,4)=(2^m-2m)(2^m+2m-2)$ and this property holds for $m\le 3$ too. It is obvious for $m=2$; for $m=3$, see that $(0,1,\beta^\ell)$ has binary weight 4 if and only if $wt_2(\beta^\ell)=3$ but there is only one such vector.

Moreover, a simple way for describing a large set of disjoint codes is indicated by the proof of Theorem 5. ■

EXAMPLE 4. *We work in* $\mathbf{PG}(2,\mathbb{F}_{2^3})$ *in order to construct a large set of disjoint* [9, 3, 4] *codes. According to Theorem 5, we get*: $M^{lb}(9,3,4)=2(7+5)=24$. *So we obtain* 24 *disjoint* [9, 3, 4] *codes. Now we are going to express precisely these* 24 *points in* $\mathbf{PG}(2,\mathbb{F}_{2^3})$.

We proceed as in the proof of Theorem 5. Note that here $I=\{3,4\}$. We choose those points Λ such that $wt(\Lambda)=3$. Moreover, any element $(\lambda_1,\lambda_2,\lambda_3)$ of the class of Λ must satisfy $wt_2(\lambda_1,\lambda_2,\lambda_3)\ge 4$, (with notation of Definition 9). Thus we choose the points of the form $\Lambda=(1,\lambda_2,\lambda_3)$ where at least one λ_j is equal to β^i for $i\in\{3,4\}$, More precisely:

$$P=\{(1,\beta^i,\beta);\, i\in I,\beta\in\mathbb{F}_{2^3}^*\}\cup\{(1,\beta^j,\beta^i);\, j\notin I, i\in I\}.$$

The set P contains 24 distinct points; therefore 24 disjoint [9, 3, 4] binary codes can be derived. Now we apply Theorem 4 with $u=9, m=3$ and $t=3$. We look for the largest n satisfying $[2^{n-u}/(2^m-1)]\le 24$. This gives $n-u=7$, that is $n=16$.

Note that we can choose 19 arbitrary codes as $2^7 \leq 19 * 7$. Finally we are able to construct a $(16 = 9 + 7, 3, 3)$ function F with nonlinearity $2^{15} - 2^8$. ■

Remark 3. It can be verified that a (9, 3, 3) function F with nonlinearity $2^{15} - 2^8$ cannot be constructed by any other known method. It is enough to consider the currently best known method in [14]. Applying this method one uses a code of shortest length, i.e. a [7, 3, 4] code, together with an highly nonlinear function $G \in \mathcal{M}_9^3$. As given in [14, Theorem 8], the nonlinearity of the resulting (16, 3, 3) function is

$$\mathcal{N}(F) = 2^{n-1} - 2^{u-1} \times \texttt{effect},$$

where $\texttt{effect} = 2^{m+1} = 2^4$ for $u = 7$, implying $\mathcal{N}(F) = 2^{15} - 2^{10}$. ■

4.2. *Lower Bound on the Number of Disjoint* $[tm, m, t+r]$ *Codes,* $r \geq 2$

In the previous section, we have considered a special case of constructing $[tm, m, t+1]$ codes by selecting suitable points in $\mathbf{PG}(t-1, \mathbb{F}_{2^m})$. Now we extend this result to the case of disjoint $[tm, m, t+r]$ codes where $r \geq 2$. The main idea is that we can also select the points Λ whose binary weight satisfies $wt(\Lambda) < t$ provided that the coordinates of Λ fulfill certain conditions. This means that even the special case treated in the previous section is only a lower bound (tight for projective spaces of relatively small dimension) since we may also consider the points Λ of weight smaller than t.

OPEN PROBLEM 1. *In general, deriving the exact number of points for arbitrary dimension v of the projective space and for any t seems to be a hard combinatorial problem. Note the connection with the determination of complete weight enumerators of non binary linear codes* [18, *ch.* 5, *Section* 6]. *This is left as an important research problem since any significant improvement over the bounds given in this paper has an immediate consequence in getting functions with better cryptographic properties.*

Hence in the sequel we only propose the lower bounds on the number of disjoint codes leaving the derivation of an exact value of disjoint codes, based on counting the suitable points in a projective space, as an open problem.

THEOREM 6. *Let* $t \geq 4, m \geq 3$ *be given positive integers. Set* $t = 2r + \ell$, *for* $r \geq 2$ *and a nonnegative integer* ℓ. *Then the number of disjoint* $[u = tm, m, t+r]$ *codes is lower bounded by*

$$M(tm, m, t+r) \geq M^{lb}(tm, m, t+r) = (2^m - 2m)^r (2m-1)^{r-1} \binom{2r-1}{r} (2^m - 1)^{\ell},$$

where $M(tm, m, t+r)$ *is introduced in Definition* 8.

Proof. To obtain disjoint $[tm, m]$ linear codes we consider the points in $\mathbf{PG}(t-1, \mathbb{F}_{2^m})$. Now set again $I = [m, 2^m - m - 1]$ and denote $J = [0, 2^m - 2] \backslash I$; thus $\mathtt{card}\, I = 2^m - 2m$ and $\mathtt{card}\, J = 2m - 1$. From Lemma 3, we know that a point $(1, \beta^e)$ is such that all its representatives satisfy $wt_2((\beta^j, \beta^{i+j})) \geq 3$ if and only if $e \in I$. We consider points $\Lambda = (\lambda_1, \ldots, \lambda_t)$ which satisfy:

1. $\lambda_i \neq$ for all $i \in [1, t]$,
2. There are at least r disjoint pairs of coordinates, say $(\lambda_{i_1}, \lambda_{i_{r+1}}), \ldots, (\lambda_{i_r}, \lambda_{i_{2r}})$, with a representative $(1, \beta^e), e \in I$, for each $(\lambda_{i_j}, \lambda_{i_{j+r}})$, $j = 1, \ldots, r$.

The first condition implies that $wt((\lambda_1, \ldots, \lambda_t)) = t$ and this property holds for any element of the class of Λ. The second condition implies that each corresponding binary image has weight at least $t + r$. Indeed by item 2 we have:

$$wt_2((\lambda_{i_1}, \ldots, \lambda_{i_r}, \lambda_{i_{r+1}}, \ldots, \lambda_{i_{2r}})) \geq 3r, \quad 1 \leq i_1 \neq \cdots \neq i_r \leq t.$$

Then the total weight of the binary image is

$$wt_2((\lambda_1, \ldots, \lambda_t)) = wt_2((\lambda_i, \ldots, \lambda_{i_{2r}})) + wt_2((\lambda_{i_{2r+1}}, \ldots, \lambda_{i_t})) \geq 3r + t - 2r = t + r.$$

According to Lemma 3, this holds for any representative. Now we are going to count a subset of points Λ.

We consider the points of the form $\Lambda = (1, \lambda_2, \ldots, \lambda_{2r}, \lambda_{2r+1}, \ldots, \lambda_t)$, where the coordinates $\lambda_{2r+1}, \ldots, \lambda_t$ may be chosen arbitrary from $(\mathbb{F}_{2m}^*)^\ell$ provided that $1, \lambda_2, \ldots, \lambda_{2r}$ are such that they form r disjoint pairs of coordinates with a representative $(1, \beta^e), e \in I$. Since $\lambda_1 = 1$ is fixed, we can choose r coordinates,

$$\lambda_{k_1}, \lambda_{k_2}, \ldots, \lambda_{k_r}, \quad 2 \leq k_1 \neq k_2 \neq \cdots \neq k_r \leq 2r,$$

such that each pair $(1, \lambda_{k_1}), (\lambda_{k_r+2}, \lambda_{k_2}), \ldots, (\lambda_{k_{2r}}, \lambda_{k_r})$ has a representative of the form $(1, \beta^e)$ with $e \in I$. Here $1 \leq k_{r+i} \neq k_i \leq 2r$ for $i = 2, \ldots, r$. Note that fixing $\lambda_1 = 1$ ensures that we choose distinct points Λ if the remaining $t - 1$ coordinates are not all the same.

The r coordinates, $\lambda_{k_l}, \lambda_{k_2} \ldots, \lambda_{k_r}$, are chosen in $\binom{2r-1}{r}$ different ways, and for any given placement their values are chosen in $(2^m - 2m)$ ways (cardinality of I). The remaining $r - 1$ coordinates, $\lambda_{k_{r+2}}, \ldots, \lambda_{k_{2r}}$, among the first $2r$ coordinates, are then chosen from the alphabet of cardinality $(2m - 1)$ (cardinality of J). Choosing coordinates in such a way together with the fact that $\lambda_1 = 1$ is kept fixed ensure that we select distinct points satisfying items 1 and 2 above. Since the last ℓ coordinates are selected arbitrary from $\mathbb{F}_{2^m}^*$, this gives a total number of choices:

$$M^{lb}(tm, t + r) = (2^m - 2m)^r (2m - 1)^{r-1} \binom{2r-1}{r} (2^m - 1)^\ell,$$

as stated. ∎

4.3. *Disjoint Codes of Smaller Minimum Distance*

We now utilize the results derived above in a more general framework. More precisely we now consider disjoint codes of length $u = mv$ and minimum distance $t+1$ with $v > t$.

THEOREM 7. *Let $u = mv$, for some positive integers m, v. Let t such that $0 \le t \le v-1$. Then the cardinality of a set of disjoint $[u, m, t+1]$ linear codes is lower bounded by,*

$$M(u, m, t+1) \ge \sum_{i=t+1}^{v} \binom{v}{i} (2^m - 1)^{i-1} + \binom{v}{t} M^{lb}(mt, m, t+1). \tag{12}$$

Proof. We first estimate the cardinality of the set

$$\Lambda^{t+1} = \{\Lambda \in \mathbf{PG}(v-1, \mathbb{F}_{2^m}) | wt(\Lambda) \ge t+1\}$$

as any such point corresponds to one $[vm, m, t+1]$ code. Clearly, there are $\binom{v}{i}$ choices of Λ for $wt(\Lambda) = i, t+1 \le i \le v$. Now for any such choice, the number of distinct points is $(2^m - 1)^i / (2^m - 1)$ and we obtain the first sum in (12).

It remains to estimate the number of points of weight t which produce a code of minimum distance $t+1$. There are $\binom{v}{t}$ v-tuples of weight t. Since $v-t$ coordinates are fixed to be zero the number of points resulting in codes of minimum distance $t+1$ is computed as in Theorem 5 by evaluating $M^{lb}(mt, m, t+1)$. This gives the second term on the right in (12), which concludes the proof. ∎

EXAMPLE 5. *Assume that we need to find as many as possible disjoint* [12, 3, 4] *linear codes in order to construct an* (*n*, 3, 3)*-resilient function by means of Theorem* 4. *From Theorem* 7, *putting $m = 3, v = 4$ and $t = 3$, we have*

$$M(12, 3, 4) \ge 7^3 + \binom{4}{3} M^{\ell b}(9, 3, 4) = 343 + 4 \cdot 24 = 439.$$

Thus, with notation of Theorem 4, we need $[2^{n-u}/7]$ disjoint codes to construct an (*n*, 3, 3)-resilient function F with $u = 12$. We have $7 \times 439 = 3073$ and $2^{11} \le 3073 \le 2^{12}$. Thus we take $n - u = 11$, that is $n = 23$. Then we need 293 disjoint [12, 3, 4] linear codes only (among the 439 suitable codes), as $2^{11} = 292 * 7 + 4$. Finally we are able to construct F, a (23, 3, 3)-resilient function with nonlinearity $\mathcal{N}(F) = 2^{22} - 2^{11}$. Note that a Boolean function with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ is usually said *almost optimal* and our function reach this value for $m = 3$ and $t = 3$. Actually it is the best nonlinearity for the functions obtained by Maiorana–McFarland construction. ∎

Note that a trivial upper bound on the cardinality of the set of disjoint $[u, 2, t+1]$ codes, denoted by $M^{ub}(u, 2, t+1)$, is given by,

$$M^{ub}(u, 2, t+1) = \left\lfloor \frac{\sum_{i=t+1}^{u} \binom{u}{i}}{3} \right\rfloor. \tag{13}$$

This bound is easily derived by counting all vectors in $c \in \mathbb{F}_2^u$, such that $wt(c) \geq t+1$. The lower bounds, given by Theorems, 5 and 7, seems to be very tight for relatively small m and t, as shown in the following example.

EXAMPLE 6. *We illustrate the tightness of the bound derived in Theorem* 7. *Assume* $v=3, m=2, t=1$, *i.e., we compare the lower and upper bound on the number of disjoint* [6, 2, 2] *linear codes. Then we obtain, from Theorem* 7, $M(6, 2, 2) \geq 18$ *while* $M^{ub}(6, 2, 2) = 19$.

4.4. Further Extensions and a Nonlinearity Comparison

The method described above works fine when the length of codes u have a nontrivial prime decomposition. Obviously, for prime u there will be no disjoint codes through this technique. To circumvent this restriction we can utilize simple techniques of combining two codes as follows. Let $\mathcal{G}_1, \mathcal{G}_2$ be generator matrices for $[u_1, m, t_1+1]$ and $[u_2, m, t_2+1]$ codes, respectively. Then the code defined by a generator matrix

$$\mathcal{G} \begin{pmatrix} \mathcal{G}_1 & 0 \\ 0 & \mathcal{G}_2 \end{pmatrix} \tag{14}$$

is a $[u_1+u_2, 2m, \min\{t_1, t_2\}+1]$ linear code. Then denoting by $\mathcal{C}_1, \mathcal{C}_2$ the sets of disjoint $[u_1, m, t+1]$ and $[u_2, m, t+1]$ linear codes, respectively, we may construct $\mathtt{card}\,\mathcal{C}_1 \times \mathtt{card}\,\mathcal{C}_2$ disjoint $[u_1+u_2, 2m, t+1]$ linear codes.

To increase the minimum distance, one may consider the lengthening of the type $\mathcal{G} = (\mathcal{G}_1 | \mathcal{G}_2)$ which gives $[u_1+u_2, m, t]$, where $t \geq t_1+t_2+2$. As above, this method also generates $\mathtt{card}\,\mathcal{C}_1 \times \mathtt{card}\,\mathcal{C}_2$ disjoint $[u_1+u_2, m, t]$ linear codes.

The following example will demonstrate that a careful use of these ideas may give significant improvements upon some best known results even at the first sight this is not possible by a straightforward application of Theorem 7 or Theorem 5.

EXAMPLE 7. *The construction of* (36, 8, t) *functions of high nonlinearity has been discussed a lot in the literature* [14, 15, 22]. *Here we only consider the case* $t=2$. *Since* $m=8$ *it seems that we must look for* [24, 8, 3] *which cannot give any improvement upon the currently highest known nonlinearity* $2^{35} - (9/16)\, 2^{20}$.

On the other hand, finding sufficiently many disjoint [20, 8, 3] codes will enable us to construct a function with nonlinearity $2^{35} - 2^{19}$. As any [20, 8, 3] linear code

Table 1. Lower bound on the number of disjoint linear codes.

#[6,3,2]=7	#[6,3,3]=2	#[9,3,3]=55	#[9,3,4]=24
#[8,4,2]=15	#[8,4,3]=8	#[12,4,3]=249	#[16,4,3]=4323
#[10,5,3]=22	#[15,5,3]=1027	#[15,5,4]=880	#[12,6,3]=52

gives $2^8 - 1$ nonzero codewords, we need at least $[2^{16}/255] = 258$ such codes. We compute the number of [12, 4, 3] and [8, 4, 3] disjoint codes. Denoting these sets by $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, we obtain,

$$\mathtt{card}\,\mathcal{C}_1 = 249 \quad \text{and } \mathtt{card}\,\mathcal{C}_2 = 8.$$

This gives 249·8 disjoint [20, 8, 3] codes (using $\mathcal{G}$ as in (14)) which is more than enough for the construction of (36, 8, 2) function with $\mathcal{N}(F) = 2^{35} - 2^{19}$. Also note that using 1029 such codes we can obtain a (38, 8, 2) function with the nonlinearity $\mathcal{N}_F = 2^{37} - 2^{19}$. ■

Table 1 gives some further examples on the lower bound on the number of disjoint linear codes of relatively small size. In this table, $\#[u, m, \delta]$ is the number of disjoint linear codes of length u, dimension m and minimal distance δ.

From these codes we construct in many cases the functions with best known nonlinearity for given inputs n, m, t. These codes are utilized in the same manner as in the Examples 1–3. Some of these functions and the corresponding codes are listed in the Table 2, where the nonlinearity of our functions is compared to those presented in [14].

We interpret the entries in the table as follows. The first item in the first row specify the parameters of disjoint codes used (the cardinality is given in Table 1), and n is the number of input variables. Then the comparison with [14] is made using these parameters: for given parameters of the code $[u, m, t+1]$ we compare in the second row the nonlinearities of (n, m, t) functions of our method and the design proposed in [14]. The first entry in the second row is the nonlinearity obtained by our method, whereas the second entry (separated by the comma) is the nonlinearity of [14]. Note that the first and the third column make a comparison to different sizes of input space. For instance the values $n = 23$[21] means that we compare the nonlinearity of our (23, 4, 2) function with the nonlinearity of a (21, 4, 2) function in [14].

5. Additional Properties of (*n, m, t*) Functions from Disjoint Codes

In accordance with Theorem 4, the existence of a set of disjoint $[u, m, t+1]$ linear codes of cardinality $r \geq \lceil 2^{n-u}/(2^m - 1) \rceil$ enables us to construct an (n, m, t) function F with nonlinearity $2^{n-1} - 2^{u-1}$. In this section, we assume that such a set

Table 2. Nonlinearity comparison with the results in [14].

[12,4,3]; n=23[21]	[10,5,3]; n=19	[15,5,4]; n=29[25]	[12,6,3]; n=23
$(2^{22} - 2^{11}), (2^{20} - \frac{3}{4}2^{12})$	$(2^{18} - 2^9), (2^{18} - \frac{5}{8}2^{12})$	$(2^{28} - 2^{14}), (2^{24} - \frac{5}{8}2^{15})$	$(2^{22} - 2^{11}), (2^{22} - \frac{19}{32}2^{14})$

$\mathcal{C}$ is available by counting the points in $\mathbf{PG}(u-1, \mathbb{F}_{2^m})$, a construction which we introduced in Section 4.

5.1. *Definition of Functions*

Let us denote by F any (n, m, t) function obtained trough the proof of Theorem 4, by using disjoint $[u, m, t+1]$ linear codes. We implicitly suppose that

$$n \geq 4, \quad 1 \leq t \leq n-3, \quad t \leq u \leq n-1, \quad 1 \leq m \leq u.$$

According to the proof of Theorem 4 in [15], the function F is as follows defined:

$$F : (y, x) \in \mathbb{F}_2^{n-u} \times \mathbb{F}_2^u \longmapsto \begin{cases} \ell_1(y) \cdot x \\ \vdots \\ \ell_m(y) \cdot x, \end{cases} \tag{15}$$

where each ℓ_i, $1 \leq i \leq m$, is a mapping from $\mathbb{F}_2^{n-u}$ to $\mathbb{F}_2^u$, each vector $\ell_i(y)$ (for any fixed y) defining a linear Boolean functions of u variables by scalar product with x. Thus each output-vector is in $\mathbb{F}_2^m$. Moreover, each $\ell_i(y)$ must be of weight at least $t+1$ and this must hold for any linear combination of the vectors $\ell_i(y)$. One then deduces that the order of resiliency is equal to t. The nonlinearity is equal to $2^{n-1} - 2^{u-1}$ if and only if for any such combination, any pair (y, y') gives two different codewords of weight at least $t+1$. All these conditions are satisfied when we apply Lemma 2 to each code of any set

$$\mathcal{C} = \{C_0, \ldots, C_{r-1}\}$$

of r disjoint $[u, m, t+1]$ linear codes, with $r \geq [2^{n-u}/(2^m - 1)]$.

It is important to notice that the function F is such that all its components are Maiorana–McFarland functions of $\mathcal{B}_n$, as introduced in [3, Proposition 4.2]. Moreover, all have the same nonlinearity; more precisely, these functions all have as Walsh spectrum the set $\{0, \pm 2^u\}$. Any such function produces a codeword, say X, of length 2^n which is a concatenation of 2^{n-u} balanced codewords of length 2^u and weight 2^{u-1}, say X_i, for i in the range $[1, 2^{n-u}]$. Each codeword corresponds to a linear function with resiliency order $\geq t$ (see more explanations in [6, 7]).

These codewords X_i are arranged by means of Lemma 2. Since $2^{n-u}/(2^m - 1)$ is never an integer, set

$$2^{n-u} = (r-1)(2^m - 1) + \gamma, \quad 0 < \gamma \leq 2^m - 2. \tag{16}$$

The codewords $X_{i(2^m-1)+1}, \ldots, X_{(i+1)(2^m-1)}$, $0 \leq i \leq r-2$, are the nonzero codewords of C_i. The codewords $X_{(r-1)(2^m-1)+1}, \ldots, X_{(r-1)(2^m-1)+\gamma}$ are γ different nonzero codewords of C_{r-1}.

Now we are going to express the algebraic form of the m-output coordinate functions of F. Set $F = (f_1, \ldots, f_m)$. For any code C_i, $i = 0, \ldots, r-1$, we construct

the corresponding matrix $A^{(i)}$, which is defined by Lemma 2 and denoted by A there. Now, for a given $y \in \mathbb{F}_2^{n-u}$ we define its decimal representation:

$$[y] = k(2^m - 1) + e, \quad 0 \le k \le r-1, \quad 0 \le e \le 2^m - 2. \tag{17}$$

We put then an order $\mathcal{C}$, since k corresponds to $A^{(k)}$. Moreover, $A_e^{(k)}$ will denote the eth row of $A^{(k)}$. More precisely we denote by $A_{e,j}^{(k)}$ the entry corresponding to the eth row and jth column, for $e = 0, \ldots, 2^m - 2$, $j = 1, \ldots, m$. Thus we express the $\ell_j(y)$ of (15) as:

$$\ell_j(y) \cdot x = A_{e,j}^{(k)} \cdot x, \quad x \in \mathbb{F}_2^u.$$

Then we easily derive the algebraic normal form of the functions $f_j, 1 \le j \le m$, by summing over $\mathbb{F}_2^{n-u}$, that is

$$f_j(y, x) = \sum_{\tau \in \mathbb{F}_2^{n-u}} \left(\prod_{s=1}^{n-u} (y_s + \tau_s + 1) \right) A_{e_\tau, j}^{(k_\tau)} \cdot x, \tag{18}$$

where for any $\tau = (\tau_1, \ldots, \tau_{n-u}) \in \mathbb{F}_2^{n-u}$,the indices k_τ, e_τ, are uniquely determined through $[\tau] = k_\tau(2^m - 1) + e_\tau$.

5.2. *Algebraic Degree*

Note that our construction completely coincides with the method in [15] except that instead of computer search for disjoint codes we propose a deterministic method. However, an exact value of algebraic degree has not been examined in [15].

It is important to notice that the degree of any $F \in \mathcal{M}_n^m$, constructed by means of concatenating codewords of a certain number disjoint $[u, m, t+1]$ linear codes is always upper bounded by $\deg(F) \le n - u + 1$. This is easily verified by noting that any restriction of $F(y, x)$ obtained by fixing $y \in \mathbb{F}_2^{n-u}$ is a linear function in $x \in \mathbb{F}_2^u$. Our purpose is to obtain $\deg(F) = n - u + 1$. As already mentioned $\gamma > 0$ in (16). This means that we only use γ rows from $A^{(r-1)}$. The choice of these rows will turn out to be of crucial importance when deriving results on algebraic degree. However, for convenience of notation, we may always consider a permuted version of $A^{(r-1)}$ such that these γ rows are listed in increasing order.

Remark 4. Actually, we may use any permutation of the rows of $A^{(i)}$ for $i = 0, \ldots, r-2$ also including the permutation of the chosen γ rows of $A^{(r-1)}$. Hence we may obtain a huge number of distinct functions having the same cryptographic properties.

To prove the main result we need an easy technical result stated without proof.

LEMMA 4. *Let U any m-dimensional subspace of $\mathbb{F}_2^u$, $2 \le m \le n$. Then $\sum_{u \in U} u = \mathbf{0}$. In particular, $\sum_{c \in C} c = \mathbf{0}$ for any linear code C of dimension $m \ge 2$.*

THEOREM 8. *Let $\mathcal{C} = \{C_0, \ldots, C_{r-2}, C_{r-1}\}$ be a set of disjoint $[u, m, t+1]$ linear codes and $A^{(0)}, \ldots, A^{(r-2)}, A^{(r-1)}$ its corresponding codeword matrices. Let r, γ be positive integers satisfying $(r-1)(2^m-1)+\gamma = 2^{n-u}$ for $\gamma \in [1, 2^m-2]$. Define $F \in \mathcal{M}_n^m$, $F = (f_1, \ldots, f_m)$ where the f_j are given by* (18). *Then it is always possible to choose the rows of $A^{(i)}, i = 0, \ldots, r-1$, such that $deg(F) = n-u+1$.*

Proof. Consider the ANF of the functions f_j given by (18). Then, looking at the expansion of $\prod_{s=1}^{n-u}(y_s + \tau_s + 1)$, we note that each term of maximum degree, say $y_1 y_2 \cdots y_{n-u} x_\ell$ for some $\ell \in [1, u]$, is present in the algebraic normal form of f_j if and only if

$$\sum_{\tau \in \mathbb{F}_2^{n-u}} A_{e_{\tau,j}}^{(k_\tau)} \neq (0, \ldots, 0) \text{ in } \mathbb{F}_2^u, \tag{19}$$

Moreover, according to the definition of $\deg(F)$, (8), this property must hold when any linear combination of the f_j is considered. This means that we need to choose the codes $C_0, \ldots, C_{r-1}$ such that condition in (19) and its expansion are satisfied.

We take all the rows of $A^{(0)}, \ldots, A^{(r-2)}$ and some specific γ rows of $A^{(r-1)}$. By Lemma 4,we have for any fixed $k, 0 \le k \le r-2$,

$$\sum_{e=0}^{2^m-2} A_{e,j}^{(k)} = (0, \ldots, 0)$$

for any j, and this holds for any linear combination of the $A_{e,j}^{(k)}$(on j). Indeed, from Lemma 2, any nonzero linear combination of the columns of $A^{(k)}$ is a permutation of the nonzero codewords of C_k, for any k. Then we need to choose γ rows of matrix $A^{(r-1)}$ in such a manner that

$$\sum_{l=1}^{\gamma} \sum_{j=1}^{m} b_j A_{s_l,j}^{(r-1)} \neq (0, \ldots, 0), \quad \forall b \in \mathbb{F}_2^m \backslash \{0\}, \tag{20}$$

where $0 \le s_1 \neq s_2 \neq \cdots \neq s_\gamma \le 2^m - 2$.

Let us denote by $p(x)$ the primitive polynomial of degree m defining the field $\mathbb{F}_{2^m}$, and let β such that $p(\beta) = 0$.

By Lemma 2, the rows of $A^{(r-1)}$ are constructed via multiplication shifts: any sth row of $A^{(r-1)}$ is equal to $(\phi(\beta^s), \ldots, \phi(\beta^{s+m-1}))$, where ϕ is a linear bijection from $\mathbb{F}_{2^m}$ to C_{r-1} satisfying $\phi(0) = 0$. Then instead of $\phi(\beta^s)$ we may consider β^s. First we have to choose γ rows of $A^{(r-1)}$ (indices $s_1, \ldots, s_\gamma$) such that

$$\underbrace{(\beta^{s_1} + \beta^{s_2} + \cdots + \beta^{s_\gamma})}_{g(\beta)} \neq 0.$$

We may simply choose

$$g(x) = 1 + x + \cdots + x^{\gamma-1} = \frac{1+x^\gamma}{1+x}.$$

Since $p(x)$ is the minimal polynomial of β, $g(\beta)=0$ if and only if p divides g. But, if p divides g then $p(x)$ is a factor of $1+x^\gamma$ implying $\beta^\gamma=1$, which contradicts the fact that β is a primitive root. Note that the choice of g does not depend of the choice of p. Now the condition (20) is equivalent to

$$(b_0+b_1\beta+\cdots+b_{m-1}\beta^{m-1})(1+\beta+\cdots+\beta^{\gamma-1})\neq 0 \quad \forall b\in\mathbb{F}_2^m, \quad b\neq 0$$

which is obviously satisfied. ■

We illustrate this method with a detailed example, using previous notation.

EXAMPLE 8. *Consider using a set $\mathcal{C}$ of disjoint* [9, 3, 3] *codes in construction of an* (n,m,t) *function F with $n=17, m=3$ and $t=2$. In Table* 1, *we find* $\#[9,3,3]=55$. *Since* $2^{n-u}=28=36\cdot 7+4$ *we need a subset of* 37 *codes of $\mathcal{C}$, say* $\{C_0,\ldots,C_{36}\}$. *We use fully the codes* $C_i, 0\le i\le 35$, (*that is all the rows of associated matrices* $A^{(0)},\ldots,A^{(35)}$), *and only* 4 *rows of* $A^{(36)}$. *Now β is a root of the primitive polynomial* $p(x)=x^3+x+1$, *used to define the field* $\mathbb{F}_{2^3}$, *and* $g(x)=1+x+x^2+x^3$. *Note that g is of weight 4. Then one can check that choosing the first four rows of* $A^{(36)}$ *will provide a function of degree* $n-u+1=9$. *These four rows of* $A^{(36)}$ *are given by*

$$B^{(36)}=\begin{pmatrix}\phi(1) & \phi(\beta) & \phi(\beta^2)\\ \phi(\beta) & \phi(\beta^2) & \phi(\beta^3)\\ \phi(\beta^2) & \phi(\beta^3) & \phi(\beta^4)\\ \phi(\beta^3) & \phi(\beta^4) & \phi(\beta^5)\end{pmatrix}=\begin{pmatrix}c_0 & c_1 & c_2\\ c_1 & c_2 & c_0+c_1\\ c_2 & c_0+c_1 & c_1+c_2\\ c_0+c_1 & c_1+c_2 & c_0+c_1+c_2\end{pmatrix},$$

where the c_i form a basis of C_{36}. Then we compute

$$\sum_{i=0}^{3} B_{i,1}^{(36)}\cdot x=c_2\cdot x, \quad \sum_{i=0}^{3} B_{i,2}^{(36)}\cdot x=(c_o+c_1)\cdot x, \quad \sum_{i=0}^{3} B_{i,3}^{(36)}\cdot x=(c_1+c_2)\cdot x,$$

corresponding to each function $f_j, 1\le j\le 3$, which also gives $\sum_{j=1}^{3} b_j \sum_{i=0}^{3} B_{i,j}^{(36)}\cdot x\neq 0$ *for any nonzero* $b\in\mathbb{F}_2^3$. *Alternatively, it can be checked that* $(b_0 1+b_1\beta+b_2\beta^2)(1+\beta+\beta^2+\beta^3)$ *is not zero, for any choice of nonzero b. Hence, we have constructed a* (17, 3, 2) *function F, with nonlinearity* $2^{16}-2^8$, *and whose degree is* $n-u+1=9$.

5.3. *A Comparison Related to Algebraic Degree*

For a comparison we only concentrate on the class of functions of very high-nonlinearity derived in [14]. In most of the cases a simple modification of the Zhang and Zheng construction [32], as described in [14], will provide functions of highest algebraic degree. For instance, referring back to Example 8, based on the existence of a [17, 12, 3] linear code the Zhang and Zheng method will provide a (17, 12, 2) function F' such that $\mathcal{N}(F')=2^{16}-2^{11}$ and $\deg(F')=m-1=11$. Then discarding 9 output variables will yield a (17, 3, 2) function with nonlinearity

$2^{16}-2^{11}$. Thus, a higher-algebraic degree is traded-off against a lower nonlinearity when compared to the function in Example 8.

A class of highly nonlinear functions has been derived in [14] using a direct sum composition of the form $H(x, y)=F(x)\oplus G(y)$, where $F:\mathbb{F}_2^u \to \mathbb{F}_2^m$ is a linear (u, m, t) function derived from a $[u, m, t+1]$ linear code. Again, for given m, t the length u is chosen to be the smallest possible. The function $G:\mathbb{F}_2^{n-u} \to \mathbb{F}_2^m$ is such that its nonlinearity is a highest known. Then clearly the algebraic degree of H is determined by the degree of G. When G is bent ($\mathcal{N}(G)=2^{n-u-1}-2^{(n-u)/2-1}$), which occurs for even $n-u \geq 2m$, this degree is upper bounded by $(n-u)/2$. Our approach uses the concatenation of linear functions in u'-variables, where in general $u' > u$ since we cannot find a set of disjoint codes of shortest length for given m, t. However, a proper choice of the codes/codewords used will always result in a function of degree $n-u'+1$. Hence in the case that G is bent, the method of [14] will provide functions of degree $\leq (n-u)/2$ compared to $n-u'+1$ in our case.

It can be checked by computation that $n-u'+1 > (n-u)/2$ is always fulfilled for the examples given in Table 2. Even in the case when G is not bent, having degree $(n-u)/2 < d \leq n-u$, in certain cases when d is smaller than $n-u$ our method is still favorable.

5.4. *Differential Properties*

The differential properties (sometimes called autocorrelation properties) measure the unbalancedness of the function's derivative in direction a. More formally, for any Boolean function $f \in \mathcal{B}_n$ its derivative with respect to nonzero $a \in \mathbb{F}_2^n$ is defined as

$$D_a f(x) = f(x) + f(x+a), \quad a \in \mathbb{F}_2^{n*}. \tag{21}$$

The worst case arises when $D_a f(x)$ is constant, that is $D_a f(x)=0$ or 1, for some nonzero a. Such an a is called a linear structure of f. This feature should be avoided in a well-designed cipher and furthermore it is of interest to choose f such that the absolute value of the differential spectra,

$$\max_{a\in\mathbb{F}_2^{n*}} \left| \sum_{x\in\mathbb{F}_2^n} (-1)^{D_a f(x)} \right|$$

is minimized.

In the case of function $F \in \mathcal{M}_n^m$, the derivatives may be defined with respect to the nonzero linear combination of its coordinates functions $f_1, \ldots, f_m$. Hence, for any $b \in \mathbb{F}_2^{m^*}$ we consider the Boolean function $f^{(b)}(x)=\sum_{j=1}^m b_i f_i(x)$ and define $D_a f^{(b)}$ as in (21). Then similarly to the Boolean case we may look for the maximum absolute value of the spectra,

$$\max_{a\in\mathbb{F}_2^{n*},b\in\mathbb{F}_2^{m*}}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{D_a f^{(b)}(x)}\right|. \tag{22}$$

To deduce the differential properties of the construction based on a set $\mathcal{C}$ of disjoint codes we recall that for any fixed $y\in\mathbb{F}_2^{n-u}$ each component function $f^{(b)}(y,x)$ is a linear function in x, that is $f^{(b)}(y,x)=c\cdot x$ for a fixed y and for some c which is a codeword of some code in $\mathcal{C}$. Furthermore, due to the construction method these linear functions are pairwise distinct since the codewords from the set of disjoint codes are used in a non repeated manner, that is $f^{(b)}(y,x)\neq f^{(b)}(y'',x)$ for any $y'\neq y''$. From now on we denote by f any such component function; clearly our next results on f hold for any choice of b.

To avoid a cumbersome mathematical notation it is convenient to represent any function f as a concatenation of linear functions. As before we use the set $\mathcal{C}=\{C_0,\ldots,C_{r-2},C_{r-1}\}$ of disjoint $[u,m,t+1]$ linear codes, using all the rows of the associated matrices of $C_0,\ldots,C_{r-2}$ and only γ rows of the matrix $A^{(r-1)}$ (see also the proof of Theorem 8). Then we write

$$f=l_0^0||\cdots||l_{2^m-2}^0||\cdots||l_0^{r-2}||\cdots||l_{2^m-2}^{r-2}||l_0^{r-1}||\cdots||l_{\gamma-1}^{r-1},$$

where the superscript i of l indicates that $l_0^i,\ldots,l_{2^m-2}^i$ are defined by means of the nonzero codewords in C_i. More precisely, denoting the codewords of C_i as $c_0,\ldots,c_{2^m-2}$, the set $\{l_0^i,\ldots,l_{2^m-2}^i\}$ is equivalent to the set $\{c_{\sigma(o)}\cdot x,\ldots,c_{\sigma(2^m-2)}\cdot x\}$, where σ is a permutation of indices that can be deduced from the matrix $A^{(i)}$.

Regarding the derivatives of f we note that $D_{e,a}f(y,x)=f(y+e,x+a)+f(y,x)$ is a balanced function for any nonzero e. This is verified by noticing that any $e\neq 0$ induces a permutation of the codewords such that for any fixed y

$$D_{e,a}f(y,x)=f(y+e,x+a)+f(y,x)=c_i\cdot(x+a)+c_j\cdot x=(c_i+c_j)\cdot x+c_i\cdot a,$$

which is an affine function for c_i,c_j which are codewords each of some code of $\mathcal{C}$, $c_i\neq c_j$. Hence for $e\neq 0$, $D_{e,a}f(y,x)$ is balanced for any fixed y and consequently $\sum_{y,x}(-1)^{D_{e,a}f(y,x)}=0$.

The case $e=0$ is a little bit harder to analyze, thus we only give the upper bound on the value $\sum_{y,x}(-1)^{D_{e,a}f(y,x)}$. Note that $e=0$ means that codewords are not permuted which gives that for a fixed y we have

$$D_{0,a}f(y,x)=f(y,x+a)+f(y,x)=c_i\cdot(x+a)+c_i\cdot x=c_i\cdot a.$$

Thus for fixed y the function $D_{0,a}f(y,x)$ is constant. We deduce, taking $c_1,\ldots,c_\gamma\in C_{r-1}^*$:

$$\sum_{y\in\mathbb{F}_2^{n-u}}\sum_{x\in\mathbb{F}_2^u}(-1)^{D_{0,a}f(y,x)}=\sum_{j=0}^{r-2}\sum_{c\in C_j^*}\sum_{x\in\mathbb{F}_2^u}(-1)^{c\cdot a}+\sum_{i=1}^{\gamma}\sum_{x\in\mathbb{F}_2^u}(-1)^{c_i\cdot a}$$

$$= \sum_{j=0}^{r-2} \sum_{x \in \mathbb{F}_2^u} \sum_{c \in C_j^*} (-1)^{c \cdot a} + 2^u \sum_{i=1}^{\gamma} (-1)^{c_i \cdot a}$$
$$-(r-1)2^u + 2^u \sum_{i=1}^{\gamma} (-1)^{c_i \cdot a},$$

where we use that for any subspace V we have $\sum_{v \in V^*} (-1)^{v \cdot a} = -1$ for any $a \neq 0$. Then considering the worst case for which we assume that $c_i \cdot a = 1$ for all i, we get

$$\left| \sum_{y,x} (-1)^{D_{0,a} f(x,y)} \right| \leq (r-1+\gamma)2^u.$$

Hence we have proved the following.

THEOREM 9. *For an (n, m, t) function F constructed by means of a set of r disjoint $[u, m, t+1]$ linear codes the derivatives of any component f of F satisfy,*

$$\sum_{y,x} (-1)^{D_{e,a} f(x,y)} = 0, \quad \text{for all } e \neq 0, \tag{23}$$

$$\max_a \left| \sum_{y,x} (-1)^{D_{0,a} f(x,y)} \right| \leq (r-1+\gamma)2^u, \quad a \neq 0, \tag{24}$$

where $2^{n-u} = (r-1)(2^m - 1) + \gamma$. ■

Thus it turns out that the differential properties could be better if we use a set of disjoint codes of small cardinality but of larger dimension. Also a small value for γ seems better in this context. Actually to sharpen the above bound for $e = 0$ seems possible for constructions with small parameters. In any case the exact upper bound can be easily computed. Due to the conditions imposed by high algebraic degree the rows of $A^{(r-1)}$ should be chosen with respect both to the algebraic degree and to a minimum absolute value of derivatives.

References

1. J. Bierbrauer, K. Gopalakrishnan and R. D. Stinson, Bounds for resilient functions and orthogonal arrays. In *Advances in Cryptology—CRYPTO'94*, vol. LNCS 839, Springer-Verlag (1994) pp. 247–256.
2. C. H. Bennet, G. Brassard and J. M. Robert, Privacy amplification by public discussion, *SIAM Journal on Computing*, Vol. 24 (1988) pp. 210–229.
3. P. Camion, C. Carlet, P. Charpin and N. Sendrier, On correlation-immune functions. In *Advances in Cryptology—EUROCRYPT'91*, Vol. LNCS 547, Springer-Verlag (1991) pp. 86–100.
4. C. Carlet, On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. In *Sequences and their Applications - SETA '01*, *Discrete Mathematics and Theoretical Computer Science*, Springer-Verlag (2001) pp. 131–144.

5. C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction. In *Advances in Cryptology - CRYPT0 2002*, Lecture Notes in Computer Science, 2442, pp. 549–564.
6. P. Charpin and E. Pasalic, On propagation characteristics of resilient functions. In *Selected Areas in Cryptography—SAC 2002*, LNCS, 2595, Springer-Verlag (2003) pp. 356–365.
7. S. Chee, S. Lee, D. Lee and H. S. Sung, On the correlation immune functions and their nonlinearity. In *Advances in Cryptology—ASIACRYPT'96*, Vol. LNCS, 1163, Springer-Verlag (1996) pp. 232–243.
8. J. H. Cheon, Nonlinear vector resilient functions. In *Advances in Cryptology—CRYPTO 2001*, Vol. LNCS, 2139, Springer-Verlag (2001) pp. 181–195.
9. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky, The bit extraction problem or t-resilient functions. In *26th IEEE Symposium on Foundations of Computer Science*, (1985) pp. 396–407.
10. G. Xiao, C. Ding and W. Shan, *The Stability Theory of Stream Ciphers*, Vol. LNCS, 561. Springer-Verlag (1991).
11. H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption, Cambridge Security Workshop*, Vol. LNCS, 1008, Springer-Verlag (1994) pp. 61–74.
12. J. Friedman, On the bit extraction problem. In *33rd IEEE Symposium on Foundations of Computer Science*, (1982) pp. 314–319.
13. K. Gopalakrishnan and R. D. Stinson, Three characterization of nonbinary correlation immune and resilient functions, *Des. Codes Cryptogr.*, Vol. 5(3) (1995) pp. 241–251.
14. K. C. Gupta and P. Sarkar, Improved constructions of nonlinear resilient S-boxes. In *Advances in Cryptology—ASIACRYPT 2002*, Vol. LNCS, 2501, Springer-Verlag (2002) pp. 466–483.
15. T. Johansson and E. Pasalic, A construction of resilient functions with high nonlinearity, *IEEE Trans. on Inform. Theory*, IT-49(2) (2003).
16. K. Kurosawa, T. Satoh and K. Yamamoto, Highly nonlinear t-resilient functions, *Journal of Universal Computer Science* Vol. 3(6) (1997) pp. 721–729.
17. R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, Vol. 20, Cambridge University Press, Cambridge (1983).
18. F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam (1977).
19. W. Meier and O. Staffelbach, Nonlinearity criteria of cryptographic functions. In *Advances in Cryptology—EUROCRYPT'88*, Vol. LNCS, 330, Springer-Verlag (1988) pp. 549–562.
20. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton (1997).
21. K. Nyberg, On the construction of highly nonlinear permutations. In *Advances in Cryptology—EUROCRYPT'92*, Vol. LNCS 658, Springer-Verlag (1992) pp. 92–98.
22. E. Pasalic and S. Maitra, Linear codes in generalized construction of resilient functions with very high nonlinearity. *IEEE Trans. Inform. Theory*, Vol. IT-48(8) (2002) pp. 2182–2191.
23. N. J. Patterson and D. H. Wiedemann, The covering radius of the (2^{15}, 16) Reed-Muller code is at least 16276, *IEEE Trans. on Inform. Theory* Vol. IT-29(3) (1983) pp. 354–356.
24. N. J. Patterson and D. H. Wiedemann, Correction to – the covering radius of the (2^{15}, 16) Reed-Muller code is at least 16276, *IEEE Trans. Inform. Theory* Vol. IT-36(2) (1990) p. 443.
25. O. S. Rothaus, On bent functions, *J. Combin. Theory, Series A*, Vol. 20 (1976) pp. 300–305.
26. P. Sarkar and S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology—EUROCRYPT 2000*, Vol. LNCS 1807, Springer-Verlag (2000) pp. 485–506.
27. P. Sarkar and S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology—CRYPTO 2000*, Vol. LNCS 1880, Springer-Verlag (2000) pp. 515–532.
28. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptograpic applications. *IEEE Trans. Inform. Theory* Vol. IT-30 (1984) pp. 776–780.

29. T. Siegenthaler, Decrypting a class of stream ciphers using cipher-text only. *IEEE Trans. Computers*, Vol. C-34 (1985) pp. 81–85.
30. D. R. Stinson, Resilient functions and large sets of orthogonal arrays, In *Congressus Numeranitium*, Vol. 92 (1993) pp. 105–110.
31. Y. Tarannikov, On resilient Boolean functions with maximal possible nonlinearity. In *Proceedings of Indocrypt*, Vol. LNCS 1977, Springer-Verlag (2000) pp. 19–30.
32. X. M. Zhang and Y. Zheng, Cryptographically resilient functions, *IEEE Trans. Inform. Theory*, Vol. IT-43(5) (1997) pp. 1740–1747.
33. G.-Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inform. Theory*, Vol. IT-34(5) (1988) pp. 569–571.