On the confusion and diffusion properties of Maiorana–McFarland’s and extended Maiorana–McFarland’s functions

Claude Carlet

INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France

Received 12 November 2002; accepted 12 August 2003

Abstract

A practical problem in symmetric cryptography is finding constructions of Boolean functions leading to reasonably large sets of functions satisfying some desired cryptographic criteria. The main known construction, called Maiorana–McFarland, has been recently extended. Some other constructions exist, but lead to smaller classes of functions. Here, we study more in detail the nonlinearity and the resiliency of the functions produced by all these constructions. Further we see how to obtain functions satisfying the propagation criterion (among which bent functions) with these methods, and we give a new construction of bent functions based on the extended Maiorana–McFarland’s construction.

Keywords: Cryptography; Stream ciphers; Boolean functions, Nonlinearity; Bent; Resilient

1. Introduction

Boolean functions play a central role in the security of stream ciphers and of block ciphers. The resistance of the cryptosystems to the known attacks can be quantified through some fundamental parameters of the Boolean functions used in them. This leads to criteria \([28,33,42]\) these cryptographic functions must satisfy.

A Boolean function on \(n\) variables is an \(F_2\)-valued function on \(F_2^n\), where \(n\) is a positive integer. In practical cryptography, \(n\) is often small. But even for small values of \(n\), searching for good cryptographic functions by visiting a nonnegligible part of
all Boolean functions on \( n \) variables is computationally impossible since their number \( 2^n \) is too large if \( n \geq 6 \) (for instance, for \( n = 7 \), it would need billions of times the age of the universe on a work-station). Thus, we need constructions of Boolean functions satisfying all necessary cryptographic criteria. Before describing the known constructions, we recall what are these cryptographic criteria.

The design of conventional cryptographic systems relies on two fundamental principles introduced by Shannon [41]: confusion and diffusion. Diffusion consists in spreading out the influence of a minor modification of the input data over all outputs. Confusion aims at concealing any algebraic structure in the system. It is closely related to the complexity of the involved Boolean functions (but the kind of complexity needed in cryptographic framework is different from what is relevant, for instance, to circuit theory). Two main complexity criteria exist for cryptographic Boolean functions: the algebraic degree and the nonlinearity. They quantify, from two different viewpoints, the difference between the considered Boolean functions (the sums of linear functions and constants—the simplest functions, from cryptographic viewpoint). Any Boolean function \( f \) on \( n \) variables admits a unique algebraic normal form (ANF):

\[
f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1, \ldots, n\}} a_I \prod_{i \in I} x_i,
\]

where the \( a_I \)'s are in \( F_2 \) and where the additions are computed in \( F_2 \) (i.e. modulo 2). We call the algebraic degree of \( f \), and we denote by \( d^a f \), the degree of its algebraic normal form (the affine functions are those functions of algebraic degrees at most 1). All cryptographic functions must have high algebraic degrees (see [4,23,25,28,35]).

The Hamming weight \( w_H(f) \) of a Boolean function \( f \) on \( n \) variables is the size of its support \( \{ x \in F_2^n : f(x) = 1 \} \). The Hamming distance \( d_H(f, g) \) between two Boolean functions \( f \) and \( g \) is the Hamming weight of their difference \( f + g \) (this sum is computed modulo 2). The nonlinearity of \( f \) is its minimum distance to all affine functions. We denote by \( N_f \) the nonlinearity of \( f \). All cryptographic functions must have high nonlinearities to resist the correlation and linear attacks [4,27]. A Boolean function \( f \) is called bent if its nonlinearity equals \( 2^{n-1} - 2^{n/2-1} \), which is the maximum possible value (obviously, \( n \) must be even). Then, its distance to every affine function equals \( 2^{n-1} \pm 2^{n/2-1} \). This property can also be stated in terms of the discrete Fourier (or Hadamard) transform of \( f \) defined on \( F_2^n \) as \( \hat{f}(u) = \sum_{x \in F_2^n} f(x)(-1)^{x \cdot u} \) (where \( x \cdot u \) denotes the usual inner product \( x \cdot u = \sum_{i=1}^n x_i u_i \) and where the sum is computed in \( Z \), that is, not mod 2). But it is more easily stated in terms of the Walsh transform of \( f \), that is, the Fourier transform of the “sign” function \( \chi_f(x) = (-1)^{f(x)} \), equal to \( \hat{\chi}_f(u) = \sum_{x \in F_2^n} (-1)^{f(x) + x \cdot u} \). \( f \) is bent if and only if \( \hat{\chi}_f(u) \) has constant magnitude \( 2^{n/2} \) (see [26,34]). Indeed, the Hamming distances between any Boolean function \( f \) and the affine functions \( u \cdot x \) and \( u \cdot x + 1 \) are equal to \( 2^{n-1} - \frac{1}{2} \hat{\chi}_f(u) \) and \( 2^{n-1} + \frac{1}{2} \hat{\chi}_f(u) \). And we have:

\[
N_f = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |\hat{\chi}_f(u)|. \tag{1}
\]
Bent functions have algebraic degrees upper bounded by $n/2$. They are characterized by the fact that their derivatives $D_a f(x) = f(x) + f(x + a)$, $a \neq 0$, are all balanced, i.e. have weight $2^{n-1}$. Hence, they provide the highest possible level of diffusion. But cryptographic functions themselves must be balanced, so that the systems using them resist statistical attacks [35]. Bent functions are not balanced. The propagation criterion $PC$, introduced by Bart Preneel [33] and related to the property of diffusion of the cryptosystems using Boolean functions, leads to a hierarchy on Boolean functions whose highest (i.e. $n$th) level is made of all bent functions, and whose $l$th levels ($l \leq n - 3$ if $n$ is even, $l \leq n - 1$ if $n$ is odd) contain balanced functions. The Boolean function $f$ on $n$ variables satisfies $PC(l)$ (the propagation criterion of degree $l$) if the derivative $D_a f$ is balanced for every nonzero $a \in F_2^n$ of weight smaller than or equal to $l$ (the weight of a binary word is the number of its nonzero components). To allow diffusion, Boolean functions used in some stream ciphers and in block ciphers must satisfy $PC(l)$ with $l$ as large as possible [32,33]. The only known upper bound on the algebraic degrees of general $PC(l)$ functions is $n - 1$.

The last (but not least) diffusion criterion considered in this paper is resiliency. It plays a central role in stream ciphers: in the standard model of these ciphers (see [42]), the outputs to $n$ linear feedback shift registers are the inputs of a Boolean function, called combining function. The output to the function produces the keystream, which is then bitwisely xored with the message to produce the cipher. Some divide-and-conquer attacks exist on this method of encryption (see [4,21,22,43]). To resist these attacks, the system must use a combining function whose output distribution probability is unaltered when any $m$ of the inputs are kept constant [43], with $m$ as large as possible. This property, called $m$th order correlation-immunity [42], is characterized by the set of zero values in the Walsh spectrum [46]: $f$ is $m$th order correlation-immune if and only if $\hat{\gamma}_f(u) = 0$, i.e. $\hat{f}(u) = 0$, for all $u \in F_2^n$ such that $1 \leq w_H(u) \leq m$, where $w_H(u)$ denotes the Hamming weight of the $n$-bit vector $u$. Balanced $m$th order correlation-immune functions are called $m$-resilient functions. They are characterized by the fact that $\hat{\gamma}_f(u) = 0$ for all $u \in F_2^n$ such that $0 \leq w_H(u) \leq m$.

Siegenthaler’s inequality [42] states that any $m$th order correlation immune function on $n$ variables has algebraic degree at most $n - m$, that any $m$-resilient function ($0 \leq m < n - 1$) has algebraic degree smaller than or equal to $n - m - 1$ and that any $(n - 1)$-resilient function has algebraic degree 1. Sarkar and Maitra [37] have shown that the nonlinearity of any $m$-resilient function ($m \leq n - 2$) is divisible by $2^{m+1}$ and is therefore upper bounded by $2^{n-1} - 2^{m+1}$ (see also [44,48]). If a function achieves this bound, then it also achieves Siegenthaler’s bound [44]. More precisely, if $f$ is $m$-resilient and has algebraic degree $d$, then its nonlinearity is divisible by $2^{m+1} + \lfloor \frac{n-m-2}{d} \rfloor$ (see [8,13]) and can therefore be equal to $2^{n-1} - 2^{m+1}$ only if $d = n - m - 1$. Moreover, if an $m$-resilient function achieves nonlinearity $2^{n-1} - 2^{m+1}$, then the Walsh spectrum of the function has then three values (such functions are called “three-valued”; see [2], or “plateaued”, see [47]), these values are 0 and $\pm 2^{m+2}$. Indeed, the distances between the function and affine functions being between $2^{n-1} - 2^{m+1}$ and $2^{n-1} + 2^{m+1}$ they must be equal to $2^{n-1} - 2^{m+1}$, $2^{n-1}$ and
$2^{n-1} + 2^{m+1}$ because of the divisibility result of Sarkar and Maitra. We shall say that an $m$-resilient function achieves the best possible nonlinearity if its nonlinearity equals $2^{n-1} - 2^{m+1}$.

If $2^{n-1} - 2^{m+1}$ is greater than the best possible nonlinearity of all balanced functions (and in particular if it is greater than the best possible nonlinearity of all Boolean functions) then, obviously, this bound can be improved. In the case $n$ is even, the best possible nonlinearity of all Boolean functions being equal to $2^{n-1} - 2^{n/2-1}$ and the best possible nonlinearity of all balanced functions being smaller than $2^{n-1} - 2^{n/2-1}$, Sarkar and Maitra deduce that $N_f \leq 2^{n-1} - 2^{n/2-1} - 2^{m+1}$ for every $m$-resilient function $f$ with $m \leq n/2 - 2$. In the case $n$ is odd, they state that $N_f$ is smaller than or equal to the highest multiple of $2^{m+1}$ which is less than or equal to the best possible nonlinearity of all Boolean functions (which is strictly smaller than $2^{n-1} - 2^{n/2-1}$ for every $n$; it is equal to $2^{n-1} - 2^{(n-1)/2}$ if $n \leq 7$ and strictly greater if $n \geq 15$, see [29]). These upper bounds have been improved successively in [8,13].

A vector $a \in \mathbb{F}_2^n$ is called a linear structure for an $n$-variable function $f$ if the derivative $D_a f(x) = f(x) + f(x + a)$ is constant. Nonlinear cryptographic functions used in block ciphers should have no nonzero linear structure (see [20]). The existence of nonzero linear structures for the functions implemented in stream ciphers could not be used in attacks, yet; but the existence of nonzero linear structures for such functions is a potential risk.

High-order resilient functions (resp. high degree PC functions) with high algebraic degrees and high nonlinearities are needed for applications, but designing constructions of Boolean functions meeting these cryptographic criteria is still a crucial challenge nowadays in symmetric cryptography. We observe some imbalance in the knowledge on cryptographic functions. Examples of $m$-resilient functions achieving the best possible nonlinearities (and thus the best algebraic degrees) have been obtained for small values of $n$ and for every $m \geq 0.6n$ ($n$ being then not limited) [31,36,37,45]. But these examples give very limited numbers of functions (they are often defined recursively or obtained after a computer search) and these functions often have cryptographic weaknesses such as linear structures. Designing constructions leading to large numbers of functions permits to choose, in applications, cryptographic functions satisfying specific constraints. The trivial methods, like variable permutation, of obtaining several Boolean functions from one function $f$, apart from the fact that they do not increase sufficiently their numbers, do not permit to achieve such specific constraints if $f$ does not. Constructing large numbers of cryptographic functions makes also more efficient those cryptosystems in which these functions themselves are parts of the secret keys. Obviously, the known “good” Boolean functions on $n$ variables will always be an insignificant proportion of the total number of functions; but the number of $n$-variable Boolean functions being huge, the number of good functions can however become sufficiently large for including these functions into the keys. The present paper is a contribution to this aim (as well as [12], which has been written later). It has some intersection with [9], but goes further in this direction.
2. Remark on the upper bound on the nonlinearities of resilient functions

As noted in [9,14], for \( m < n/2 - 2 \), except for small values of \( n \), an upper bound on the nonlinearity of \( m \)-resilient functions can be given, which is potentially better than the bounds recalled in the introduction (whatever is the evenness of \( n \)). Let us see more precisely how. Sarkar–Maitra’s divisibility bound shows that \( \tilde{\mu}(a) = \phi(a) \cdot 2^{m+2} \) where \( \phi(a) \) is integer-valued. But Parseval’s relation

\[
\sum_{a \in \mathbb{F}_2^n} \tilde{\mu}^2(a) = 2^{2n}
\]

and the fact that \( \tilde{\mu}(a) \) is null for every word \( a \) of weight \( \leq m \) implies

\[
\sum_{a; \ w(a) > m} \phi^2(a) = 2^{2n-2m-4}
\]

and thus

\[
\max_{a \in \mathbb{F}_2^n} |\phi(a)| \geq \sqrt{\frac{2^{2n-2m-4}}{2^n - \sum_{i=0}^{m} \binom{n}{i}^2}} = \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^{m} \binom{n}{i}}}. 
\]

Thus we have \( \max_{a \in \mathbb{F}_2^n} |\phi(a)| \geq \left[ \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^{m} \binom{n}{i}}} \right] \) (where \( \lceil u \rceil \) denotes the smallest integer greater than or equal to \( u \)) and this implies:

\[
N_f \leq 2^{n-1} - 2^{m+1} \left[ \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^{m} \binom{n}{i}}} \right]. \tag{2}
\]

When \( n \) is even, this number is always less than or equal to \( 2^{n-1} - 2^{n/2-1} - 2^{m+1} \) (given by Sarkar and Maitra [37]) because \( \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^{m} \binom{n}{i}}} \) being strictly greater than \( 2^{n/2-m-2} \) and \( 2^{n/2-m-2} \) being an integer, since \( m \leq n/2 - 2 \), the number \( \left[ \frac{2^{n-m-2}}{\sqrt{2^n - \sum_{i=0}^{m} \binom{n}{i}}} \right] \) is at least \( 2^{n/2-m-2} + 1 \). And when \( n \) increases, the bound above is smaller than \( 2^{n-1} - 2^{n/2-1} - 2^{m+1} \) for an increasing number of values of \( m \leq n/2 - 2 \) (but this improvement does not appear when we compare the values we obtain with this bound to the values indicated in the table they give in [37], because the values of \( n \) considered in this table are small).

When \( n \) is odd, it is difficult to say if inequality (2) is better than the bound given by Sarkar and Maitra, because their bound involves a value which is unknown for \( n \geq 9 \) (the best possible nonlinearity of all Boolean functions). In any case, this makes (2) better usable than their bound.
We know (see [26, p. 310]) that\[ P_m i = \frac{C_0}{C_1} X_{2nH_2\left(\frac{m}{n}\right)} \sqrt{\frac{8m}{8m(1-m/n)}} \],
where $H_2(x)$ is the so-called binary entropy function $-x \log_2(x) - (1-x) \log_2(1-x)$ and satisfies $H_2\left(\frac{1}{2}-x\right) = 1 - 2x^2 \log_2 e + o(x^2)$. Thus we have
\[
N_f \leq 2^{n-1} - 2^{m+1} \left[ \frac{2^{n-m-2}}{2^n - \frac{2^{nH_2(m/n)}}{\sqrt{8m(1-m/n)}}} \right].
\]

3. Maiorana–McFarland’s, Dillon’s and Dobbertin’s constructions and their properties

Some constructions of cryptographic functions define them without needing previously defined cryptographic functions in smaller numbers of variables. These primary constructions lead in practice to wider classes of functions than secondary (i.e. recursive) constructions (recall that the number of Boolean functions in $n-1$ variables is only equal to the square root of the number of Boolean functions in $n$ variables). Unfortunately, the known primary constructions of Boolean functions themselves (see [6]) do not lead to very large classes of functions. In fact, only one reasonably large class of Boolean functions is known, whose elements can be analyzed with respect to the cryptographic criteria recalled above.

3.1. Maiorana–McFarland’s construction

3.1.1. The original Maiorana–McFarland’s class

It is the set (see [18]) of all the (bent) Boolean functions on the vectorspace $F_2^n = \{(x, y), x, y \in F_2^n\}$ ($n$ even) of the form
\[
f(x, y) = x \cdot \pi(y) + g(y) = \sum_{i=1}^{n/2} x_i \pi_i(y) + g(y),
\]
where $\pi$ is any permutation on $F_2^n$, where $\pi_1, \ldots, \pi_{n/2}$ are its coordinate functions, and where $g$ is any Boolean function on $F_2^n$. Notice that $f$, considered as a binary vector of length $2^n$ (through its truth-table), can be viewed as the concatenation of affine functions on $F_2^{n/2}$. Indeed, if for instance we arrange all binary words of length $n$ in reverse lexicographic order, then the truth-table of $f$ is the concatenation of the restrictions of $f$ obtained by fixing the value of $y$ and letting $x$ freely range over $F_2^{n/2}$. These restrictions are affine.

It is a simple matter to see that the bijectivity of $\pi$ is a necessary and sufficient condition for the bentness of $f$ (see relation (6) below). But the generalized version of this construction below will permit us to obtain other bent functions in a similar framework.
3.1.2. The (general) Maiorana–McFarland’s class

It has been introduced in [1], based on the same principle of concatenating affine functions: let \( r \) be an integer such that \( n \geq r \); denote \( n - r \) by \( s \); let \( g \) be any Boolean function on \( F_2^s \) and \( \phi \) any mapping from \( F_2^s \) to \( F_2^r \). Then we define the function:

\[
f_{\phi, g}(x, y) = x \cdot \phi(y) + g(y) = \sum_{i=1}^{r} x_i \phi_i(y) + g(y), \quad x \in F_2^r, \ y \in F_2^s,
\]

where \( \phi_i(y) \) is the \( i \)th coordinate of \( \phi(y) \). This extension has been introduced to produce resilient functions (see below). But we first recall that it can be used to produce functions satisfying the propagation criterion.

**Propagation criterion:** The derivative \( D_{(a,b)}(x,y) \) of a function of the form (5) being equal to \( x \cdot D_b\phi(y) + a \cdot \phi(y + b) + D_bg(y) \), the function satisfies \( PC(l) \) under the sufficient condition that:

1. for every nonzero \( b \in F_2^s \) of weight smaller than or equal to \( l \) and every vector \( y \in F_2^s \), the vector \( D_b\phi(y) \) is nonzero, or equivalently every set \( \phi^{-1}(u) \), \( u \in F_2^s \) either is empty or is a singleton or has minimum distance strictly greater than \( l \);

2. every linear combination of at most \( l \) coordinate functions of \( \phi \) is balanced.


**Bentness:** The sufficient conditions above do not permit to obtain new bent functions, since they lead, when \( l = n \), to the functions of the original class of Maiorana–McFarland. Indeed, \( \phi \) has then to be injective, because of condition 1, and uniformly distributed, because of condition 2. But bent functions can be obtained in a more general framework. Astonishingly enough, this observation has never been made before.

**Proposition 1.** Let \( n = r + s \) \((r \leq s)\) be even. Let \( \phi \) be any mapping from \( F_2^s \) to \( F_2^r \) such that, for every \( a \in F_2^s \), the set \( \phi^{-1}(a) \) is an \((n - 2r)\)-dimensional affine subspace of \( F_2^n \). Let \( g \) be any Boolean function on \( F_2^s \) whose restriction to \( \phi^{-1}(a) \) (viewed as a Boolean function on \( F_2^{n-2r} \) via an affine isomorphism between \( \phi^{-1}(a) \) and this vector-space) is bent for every \( a \in F_2^s \). Then \( f_{\phi, g} \) is bent on \( F_2^n \).

**Proof.** For every Maiorana–McFarland’s function \( f_{\phi, g} \), every \( a \in F_2^s \) and every \( b \in F_2^s \), we have

\[
\widehat{f_{\phi, g}}(a, b) = 2^r \sum_{y \in \phi^{-1}(a)} (-1)^{g(y)+b \cdot y},
\]

since every (affine) function \( x \mapsto f_{\phi, g}(x, y) + a \cdot x + b \cdot y \) either is constant (if \( \phi(y) = a \)) or is balanced (if \( \phi(y) \neq a \)) and contributes then for 0 in the sum \( \sum_{x \in F_2^n, y \in F_2^s} (-1)^{f_{\phi, g}(x,y)+x \cdot a+y \cdot b} \). Thus \( f_{\phi, g} \) is bent if and only if \( r \leq n/2 \) and \( \sum_{y \in \phi^{-1}(a)} (-1)^{g(y)+b \cdot y} = \pm 2^{n/2-r} \) for every \( a \in F_2^s \) and every \( b \in F_2^s \). The hypothesis on \( \phi \) and \( g \) is a sufficient condition for that. \( \square \)
Notice that this construction is easy to use for generating potentially new bent functions: the choice of any partition of $F_2^n$ in $(n-2r)$-dimensional flats and of a bent function on each of these flats leads to a bent function. Further (possibly difficult) work has still to be done for proving that some functions constructed this way lie outside all known classes of bent functions.

Resiliency: We recall now how Maiorana–McFarland’s construction can be used to design resilient functions: if every element in $\phi(F_2^n)$ has Hamming weight strictly greater than $k$, then $f_{\phi,g}$ is $m$-resilient with $m \geq k$ (in particular, if $\phi(F_2^n)$ does not contain the null vector, then $f_{\phi,g}$ is balanced). This is a direct consequence of relation (6).

Algebraic degree and nonlinearity: The algebraic degree of $f_{\phi,g}$ is $s + 1 = n - r + 1$ if and only if $\phi$ has algebraic degree $s$ (i.e. if at least one of its coordinate functions has algebraic degree $s$), which is possible only if $k = \min \{w_H(\phi(y)) : y \in F_2^n\} - 1$ satisfies $k \leq r - 2$, since if $k = r - 1$ then $\phi$ is constant. Otherwise, the algebraic degree of $f_{\phi,g}$ is at most $s$. Thus, if the resiliency order $m$ equals $k$, then the algebraic degree of $f_{\phi,g}$ reaches Siegenthaler’s bound $n - m - 1$ if and only if either $m = r - 2$ and $\phi$ has algebraic degree $s = n - m - 2$ or $m = r - 1$ and $g$ has algebraic degree $s = n - m - 1$. There are cases where $m > k$ (see below) and ways of increasing the degree by modifying the construction (see [36]).

Relations (1) and (6) lead straightforwardly to a general lower bound on the nonlinearity of Maiorana–McFarland’s functions (first observed in [39]):

$$N_{f_{\phi,g}} \geq 2^{n-1} - 2^{r-1} \max_{a \in F_2^r} |\phi^{-1}(a)|$$  \hspace{1cm} (7)

(where $|\phi^{-1}(a)|$ denotes the size of the pre-image $\phi^{-1}(a)$). This bound is tight if $\phi^{-1}(a)$ has size at most 2, for every $a \in F_2^n$. When $\phi$ does not have this property, the bound is weak (see [36] for some improvement). A recent upper bound

$$N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1} \left[ \max_{a \in F_2^r} |\phi^{-1}(a)| \right]$$  \hspace{1cm} (8)

obtained in [9] (and generalized in the present paper, see Theorem 2) strengthens the bound $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1}$ previously obtained in [15,16]. It has led to a characterization of the parameters for which Maiorana–McFarland’s functions $f_{\phi,g}$ such that $w_H(\phi(y)) > k$ for every $y$ and achieving best possible nonlinearity $2^{n-1} - 2^{k+1}$ can exist.

The inequality $N_{f_{\phi,g}} \leq 2^{n-1} - 2^{r-1} \left[ \sum_{i=k+1}^{r} \binom{r}{i} \binom{2^{i/2}+1}{i} \right]$ implied by relation (8) implies in its turn either that $r = k + 1$ or $r = k + 2$.

If $r = k + 1$ then $\phi$ is the constant $(1, \ldots, 1)$ and $n \leq k + 3$. Either $s = 1$ and $g(y)$ is then any function in one variable or $s = 2$ and $g$ is then any function of the form $y_1y_2 + l(y)$ where $l$ is affine (thus, $f$ is quadratic). If $r = k + 2$, then $\phi$ is injective, $n \leq k + 2 + \log_2(k + 3)$, $g$ is any function in $n - k - 2$ variables and $d^o f_{\phi,g} \leq 1 + \log_2(k + 3)$. 

A simple example of \( k \)-resilient Maiorana–McFarland’s functions such that \( N_{f,y} = 2^{n-1} - 2^{k+1} \) (and thus achieving Sarkar et al.’s bound) can be given (see [9]) for any \( r \geq 2 \) and for \( k = r - 2 \).

In [9] is also shown that for every even \( n \leq 10 \), Sarkar et al.’s bound with \( m = n/2 - 2 \) can be achieved by Maiorana–McFarland’s functions. And an example of functions with high nonlinearities but not achieving Sarkar et al.’s bound is given: for every \( n \equiv 1 \mod 4 \), there exist Maiorana–McFarland’s \( \frac{n-1}{4} \)-resilient functions on \( F_2^n \) with nonlinearity equal to \( 2^{n-1} - 2^{\frac{n-1}{2}} \).

**Proposition 2.** Let \( f_{\phi,g} \) be defined by (5).

1. Assume that every element in \( \phi(F_2^n) \) has Hamming weight strictly greater than \( k \) and that, for every \( a \in F_2^n \) of weight \( k + 1 \), either the set \( \phi^{-1}(a) \) is empty or it has an even size and the restriction of \( g \) to this set is balanced. Then \( f_{\phi,g} \) is \( m \)-resilient with \( m \geq k + 1 \). Under this hypothesis, if \( f_{\phi,g} \) achieves the best possible nonlinearity \( 2^{n-1} - 2^{k+2} \), then \( r \leq k + 2 \).

   If \( r = k + 1 \) then \( \phi \) is the constant \( (1, \ldots, 1) \) (and \( g \) is balanced); either \( s = 2 \) and \( g \) and \( f \) are affine or \( s = 3 \) and \( g \) has nonlinearity 2.

   If \( r = k + 2 \) then \( n \leq k + 4 + \log_2(k + 3) \) and \( d^o f \leq 2 + \log_2(k + 3) \).

2. Assume in addition that:
   a. for every \( a \in F_2^n \) of weight \( k + 1 \) and every \( i \in \{1, \ldots, s\} \), denoting by \( H_i \) the linear hyperplane of equation \( y_i = 0 \) in \( F_2^n \), either the set \( \phi^{-1}(a) \cap H_i \) is empty or it has an even size and the restriction of \( g \) to this set is balanced;
   b. for every \( a \in F_2^n \) of weight \( k + 2 \), either the set \( \phi^{-1}(a) \) is empty or it has an even size and the restriction of \( g \) to this set is balanced.

   Then \( f_{\phi,g} \) is \( m \)-resilient with \( m \geq k + 2 \). Under this hypothesis, if \( f_{\phi,g} \) achieves the best possible nonlinearity \( 2^{n-1} - 2^{k+3} \), then \( r \leq k + 3 \).

   If \( r = k + 1 \), then \( 3 \leq s \leq 5 \) and \( \phi \) takes constant value \( (1, \ldots, 1) \). If \( s = 3 \) then \( g \) and \( f \) are affine. If \( s = 4 \), then \( g \) has nonlinearity 4. If \( s = 5 \) then \( g \) has nonlinearity 12.

   If \( r = k + 2 \) then \( n \leq k + 6 + \log_2(k + 3) \) and \( d^o f \leq 3 + \log_2(k + 3) \).

   If \( r = k + 3 \) then \( n \leq k + 5 + \log_2((k+3)/2) + k + 4 \) and \( d^o f \leq 2 + \log_2((k+3)/2) + k + 4 \).
empty or the restriction of \( g \) to \( \phi^{-1}(a) \) takes the same number of times the values 0 and 1 (this is possible thanks to the fact that \( \phi^{-1}(a) \) has an even size), this sum is null. Thus \( f_{\phi,g} \) is \( m \)-resilient with \( m \geq k + 1 \).

If \( N_{f_{\phi,g}} = 2^{n-1} - 2^{k+2} \), then according to inequality (8), we must have
\[
\max_{a \in F_2'} |\phi^{-1}(a)| \leq 2^{k-r+3},
\]
and thus \( r \leq k + 2 \) since \( \max_{a \in F_2'} |\phi^{-1}(a)| \) is greater than or equal to 2.

If \( r = k + 1 \), then \( \phi \) takes constant value \( (1, \ldots, 1) \); hence \( \phi^{-1}(1, \ldots, 1) = F_2' \). Equality \( N_{f_{\phi,g}} = 2^{n-1} - 2^{k+2} \) and relations (1) and (6) imply
\[
\max_{b \in F_2'} \sum_{y \in F_2'} (-1)^{g(y)+b \cdot y} = 4.
\]
Thus \( s \geq 2 \). If \( s = 2 \) then \( g \) and \( f \) are affine. If \( s = 3 \), then \( g \) has nonlinearity 2. The case \( s = 4 \) is impossible since \( g \), being balanced, cannot be bent.

If \( r = k + 2 \) then \( \max_{a \in F_2'} |\phi^{-1}(a)| \leq 4 \) and therefore \( 2^r \) is smaller than or equal to 4 times the number \( r + 1 \) of all words of weights at least \( k + 1 = r - 1 \), i.e. \( s \leq 2 + \log_2(r + 1) \) and thus \( n \leq k + 4 + \log_2(k + 3) \) which implies \( d^s f \leq 2 + \log_2(k + 3) \) because of Siegenthaler’s inequality.

2. To prove that \( f_{\phi,g} \) is \( m \)-resilient with \( m \geq k + 2 \) under the additional hypothesis, the ordered pairs \((a,b)\) we still have to consider are those such that \( a \) has weight \( k + 1 \) and \( b \) has weight 1, and those such that \( a \) has weight \( k + 2 \) and \( b \) is null. According to relation (6), the conditions \( a \) and \( b \) are clearly sufficient, since
\[
\sum_{y \in \phi^{-1}(a)} (-1)^{g(y)+y} = 2 \sum_{y \in \phi^{-1}(a) \cap H_1} (-1)^{g(y)} - \sum_{y \in \phi^{-1}(a)} (-1)^{g(y)} = 2 \sum_{y \in \phi^{-1}(a) \cap H_1} (-1)^{g(y)}.
\]
If \( N_{f_{\phi,g}} = 2^{n-1} - 2^{k+3} \), then according to inequality (8), we must have
\[
\max_{a \in F_2'} |\phi^{-1}(a)| \leq 2^{k-r+4},
\]
and thus \( r \leq k + 3 \) since \( \max_{a \in F_2'} |\phi^{-1}(a)| \) is greater than or equal to 2.

If \( r = k + 1 \), then \( \phi \) takes constant value \( (1, \ldots, 1) \); hence \( \phi^{-1}(1, \ldots, 1) = F_2' \). Equality \( N_{f_{\phi,g}} = 2^{n-1} - 2^{k+3} \) and relations (1) and (6) imply
\[
\max_{b \in F_2'} \sum_{y \in F_2'} (-1)^{g(y)+b \cdot y} = 8.
\]
Thus \( s \geq 3 \). If \( s = 3 \) then \( g \) and \( f \) are affine. If \( s = 4 \), then \( g \) has nonlinearity 4. If \( s = 5 \) then \( g \) has nonlinearity 12. The case \( s = 6 \) is impossible since \( g \), being balanced, cannot be bent.

If \( r = k + 2 \) then \( \max_{a \in F_2'} |\phi^{-1}(a)| \leq 16 \) and therefore \( 2^r \) is smaller than or equal to 16 times the number \( r + 1 \) of all words of weights at least \( r - 1 \), i.e. \( s \leq 4 + \log_2(r + 1) \) and thus \( n \leq k + 6 + \log_2(k + 3) \) which implies \( d^s f \leq 3 + \log_2(k + 3) \) because of Siegenthaler’s inequality.

If \( r = k + 3 \) then \( \max_{a \in F_2'} |\phi^{-1}(a)| \leq 4 \) and therefore \( 2^r \) is smaller than or equal to 4 times the number \( (r - 2) + r + 1 \) of all words of weights at least \( r - 2 \), i.e. \( s \leq 2 + \log_2(r - 2) + r + 1 \) and thus \( n \leq k + 5 + \log_2(k^2 + k + 4) \) which implies \( d^s f \leq 2 + \log_2(k^2 + k + 4) \) because of Siegenthaler’s inequality. □

Remark. More generally, assume that for every vector \( a \in F_2' \) whose Hamming weight \( w_H(a) \) is smaller than or equal to some integer \( l \), either the set \( E_a \) is empty or
for every $b \in F_2^n$ of weight at most $l - \omega(b)$, the restriction of $g(y) + y \cdot b$ to $E_a$ is balanced, then, $f_{\phi, g}$ is $l$-resilient.

In [9] is given a way of obtaining Maiorana–McFarland’s functions satisfying the hypothesis of Proposition 2 and having high nonlinearities.

But the results of Proposition 2 show that except in extreme cases, Maiorana–McFarland’s functions cannot reach Sarkar–Maitra’s bound. This is not astonishing, because Maiorana–McFarland’s construction is general whereas the functions achieving Sarkar–Maitra’s bound are often peculiar. A different way of modifying Maiorana-McFarland’s construction has been introduced in [30].

### 3.2. Dillon’s construction

In [18] is introduced by J. Dillon the class of bent functions called $PSap: F_{2^n}^2$ is identified to the Galois field $F_{2^r}$; $PSap$ is the set of all the functions of the form

$$f(x, y) = g(xy^{2^{n-2}})$$

(i.e. $g(x)$ with $x = 0$ if $x = 0$ or $y = 0$) where $g$ is a balanced Boolean function on $F_{2^r}$ (Dillon also assumes that $g(0) = 0$ but it is not necessary).

The idea of this construction is used in [16] to obtain a construction of resilient functions: let $k$ and $r$ be non-negative integers and $n \geq r$; the vector space $F_2^n$ is identified to the Galois field $F_{2^r}$. Let $g$ be any Boolean function on $F_{2^r}$ and $\phi$ an $F_2$-linear mapping from $F_2^n$ to $F_{2^r}$; set $a \in F_2^n$ and $b \in F_2^r$ such that, for every $y$ in $F_2^n$ and every $z$ in $F_{2^r}$, $a + \phi(y)$ is nonzero and $\phi^*(z) + b$ has weight greater than $k$, where $\phi^*$ is the adjoint of $\phi$. Then the function

$$f(x, y) = g\left(\frac{x}{a + \phi(y)}\right) + b \cdot y; \quad \text{where } x \in F_{2^n}, \ y \in F_2^n$$

(9)

is $m$-resilient with $m \geq k$. The algebraic degree of $f$ is difficult to study but can be optimal. Similar bounds on the nonlinearities of these functions can be proved as for Maiorana–McFarland’s functions:

$$2^{n-1} - 2^{s-1} \max_{b \in F_2^n} |\phi^{-1}(b)| \leq N_f \leq 2^{n-1} - 2^{s-1} \sqrt{\max_{a \in F_2^n} |\phi^{s-1}(a)|}.$$  

Indeed, we have, for every $a \neq 0$ and $b$ (see [6])

$$\tilde{\chi}_f(a, b) = 2^s \sum_{z \in F_2^{s-1}(b+\phi^{-1}(a))} (-1)^{\text{tr}(az)+\phi(z)}.$$  

The same computations as in the proof of Proposition 2 give the desired inequalities. It then follows similar observations as for Maiorana–McFarland’s construction (with the restriction that $\phi^*$ is linear) on the ability of the functions of the form (5) to have nonlinearities near Sarkar–Maitra’s bound. But this class has few elements (since $\phi$ is linear).
3.3. Dobbertin’s construction

In [19], Hans Dobbertin studies an interesting method for modifying bent functions into balanced functions with high nonlinearities (see also [40]). He observes that all known bent functions on $F_2^n$ ($n$ even) are affinely equivalent to functions $f(x, y)$, $x \in F_2^{n/2}$, $y \in F_2^{n/2}$ such that $f(x, 0)$ is constant on $F_2^{n/2}$ (recall that two functions $f$ and $g$ on $F_2^n$ are called affinely equivalent if there exists a linear isomorphism $L$ from $F_2^n$ to $F_2^n$ and a vector $a$ such that $f(x) = g(L(x) + a)$ for every input $x \in F_2^n$; the functions have then the same algebraic degree and the same nonlinearity, but they may have different orders of resiliency and different degrees of propagation criterion). He calls normal the functions which, up to affine equivalence, are constant on the set $F_2^{n/2} \times \{0\}$. A nonnormal bent function has been found only recently (see [3]).

Let $f$ be null (for instance) on $F_2^{n/2} \times \{0\}$ and let $g$ be any balanced function on $F_2^{n/2}$, then the function $h(x, y) = f(x, y) + \delta_0(y)g(x)$, where $\delta_0$ is the Dirac symbol ($\delta_0(y) = 1$ if and only if $y = 0$) is balanced. Moreover:

$$\widetilde{\xi}_h(a, b) = 0 \text{ if } a = 0 \text{ and } \widetilde{\xi}_h(a, b) = \widetilde{\xi}_f(a, b) + \widetilde{\xi}_g(a) \text{ otherwise.} \quad (10)$$

If $n' \leq 13$ is odd and $n = 2^k n'$, then the best known (but perhaps not the best possible) nonlinearity that can be obtained by using Dobbertin’s method is $2^{n-1} - 2^{n/2-1} - 2^{n/4-1} - \cdots - 2^{n/2^k-1} - 2^{(n'-1)/2}$. Indeed, for every odd $n'$, there exists a balanced (quadratic) function on $F_2^n$ with nonlinearity $2^{d-1} - 2^{(n'-1)/2}$ and no balanced function with better nonlinearity is known, since $n' \leq 13$.

Unfortunately, we have the following:

**Proposition 3.** Dobbertin’s construction cannot produce $m$-resilient functions with $m > 0$, and it cannot produce functions satisfying $PC(l)$ with $l \geq n/2$.

**Proof.** The function $h$ above cannot be $m$-resilient with $m > 0$ according to relation (10), since $\widetilde{\xi}_g(a)$ should equal $\pm 2^n/2$ for every word $a$ of weight 1, and $g$ being a function defined on $F_2^{n/2}$, there cannot exist two different values of $a$ such that $\widetilde{\xi}_g(a)$ equals $\pm 2^n/2$.

The function $h$ cannot satisfy $PC(l)$ with $l \geq n/2$ either since it is shown in [7] that a function $h$ on $F_2^n$ satisfies $PC(l)$ if and only if for every vector $u$ of weight at least $n - l$ and every vector $v$:

$$\sum_{w \leq u} \widetilde{\xi}_h^2(w + v) = 2^{n+w}u(u), \quad (11)$$

where $w \leq u$ means that the support of vector $u$ includes the support of vector $w$. This condition cannot be satisfied here if $l \geq n/2$: if $u$ is for instance the vector with the first $n/2$ coordinates equal to 0 and with the last $n/2$ coordinates equal to 1, and if $v = 0$, we have $\widetilde{\xi}_h^2(w) = 0$ for every $w \leq u$, according to relation (10), and relation (11) cannot be satisfied. □
3.4. Remark on the numbers of constructed functions

The class of bent functions produced by the original Maiorana–McFarland’s construction (resp. the class of balanced or resilient functions produced by the Maiorana–McFarland’s construction) is far the widest class, compared to the classes obtained with the other usual constructions. The number of bent functions of the form (4) equals \((2^{n/2})! \times 2^{2^{n/2}}\) and is asymptotically equivalent to \(\left(\frac{2^{n/2} \cdot 1}{e}\right)^{2^{n/2}} \sqrt{2^{n/2}}\) according to Stirling’s formula, while the only other important construction of bent functions, \(PS_{ap}\), leads only to \(\left(\frac{2^{n/2}}{2^{n/2} - 1}\right)^{2^{n/2} + 1/2} \sqrt{n} 2^{n/2}\) functions. And the situation of resilient functions is still more explicit. However, the number of provably bent, balanced or resilient Maiorana–McFarland’s functions seems negligible with respect to the total number of functions with the same properties. For bent functions, this is only a conjecture, since the number of bent functions is unknown (only an upper bound exists [11]). For balanced functions, it can be checked: for every positive integer \(r\), the number of balanced Maiorana–McFarland’s functions obtained by choosing \(\phi\) such that \(\phi(y) \neq 0\) for every \(y\) equals \(2^{r+1} - 2\) \(2^{2^{r-1}}\) and is smaller than or equal to \(2^{2^{r-1}}\) since \(r \geq 1\). It is quite negligible with respect to the number \(\left(\frac{2^n}{2^{n-1}}\right) \approx \frac{2^{2^{n+1/2}}}{\sqrt{n} 2^{n}}\) of all balanced functions on \(F_2^n\). The number of \(k\)-resilient Maiorana–McFarland’s functions obtained by choosing \(\phi\) such that \(w_H(\phi(y)) > k\) for every \(y\) equals \(\left[2 \sum_{i=k+1}^{2^n} \left(\frac{2^n}{i}\right)^{2^{n-i}}\right]\) and is probably also very small compared to the number of all \(k\)-resilient functions. But this number is unknown. Three complementary upper bounds on the number of all \(k\)-resilient functions improve upon all previous bounds [10,11,38]. However, they are probably still far from the real number.

4. The extended Maiorana–McFarland’s class

The restrictions of Maiorana–McFarland’s functions obtained by fixing \(y\) in their input being affine, there is a risk that this be used in future attacks. It is important, when designing cryptographic functions, to anticipate possible new attacks (this is what Rothaus did when introducing the notion of nonlinearity by studying bent functions; the linear attack was not known yet). Also, Maiorana– McFarland’s functions have high divisibilities of their Fourier and Walsh spectra, and there is also a risk that this property be used in attacks, as it is used in [5] to attack block ciphers. For this reason, a construction was proposed in [9]. The functions it produces are concatenations of quadratic functions (i.e. functions which are either affine or of algebraic degree 2) instead of, just, affine functions. This makes them harder to study than Maiorana– McFarland’s functions but they are more numerous and have not the same drawback.
4.1. Definition and Walsh spectrum

**Definition 1.** Let $n$ and $r$ be positive integers such that $r < n$. Denote the integer part \( \lfloor \frac{n}{2} \rfloor \) by $t$ and $n - t$ by $s$. Let $\psi$ be a mapping from $F_2^n$ to $F_2^t$ and let $\psi_1, \ldots, \psi_r$ be its coordinate functions. Let $\phi$ be a mapping from $F_2^n$ to $F_2^t$ and let $\phi_1, \ldots, \phi_r$ be its coordinate functions. Let $g$ be a Boolean function on $F_2^n$. The function $f_{\psi, \phi, g}$ is defined on $F_2^n = F_2^t \times F_2^t$ as

$$f_{\psi, \phi, g}(x, y) = \sum_{i=1}^{t} x_{2i-1}x_{2i}\psi_i(y) + x \cdot \phi(y) + g(y)$$

$$= \sum_{i=1}^{t} x_{2i-1}x_{2i}\psi_i(y) + \sum_{j=1}^{r} x_j\phi_j(y) + g(y); \quad x \in F_2^t, \ y \in F_2^t.$$

Maiorana–McFarland’s functions correspond to the case where $\psi$ is the null mapping. The following theorem is proved in [9].

**Theorem 1.** Let $f_{\psi, \phi, g}$ be defined as in Definition 1. Then for every $a \in F_2^t$ and every $b \in F_2^t$ we have

$$\widehat{f_{\psi, \phi, g}}(a, b) = \sum_{y \in E_a} 2^{-w_1(\psi(y))} \left(-1\right)^{\sum_{i=1}^{t} (\phi_{2i-1}(y) + a_{2i-1})(\phi_{2i}(y) + a_{2i}) + g(y) + y \cdot b},$$

where $E_a$ is the superset of $\phi^{-1}(a)$ equal if $r$ is even to

$$\{y \in F_2^{t}\} \forall i \leq t, \ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i})\},$$

and if $r$ is odd to

$$\left\{ y \in F_2^{t}\right\} \left\{ \forall i \leq t, \ \psi_i(y) = 0 \Rightarrow (\phi_{2i-1}(y) = a_{2i-1} \text{ and } \phi_{2i}(y) = a_{2i})\} \right\}.$$
4.2. Cryptographic properties of the constructed functions

In this section, we study the behavior of the functions \( f_{\psi, \phi, g} \) with respect to the cryptographic criteria.

4.2.1. Algebraic degree

Let \( f_{\psi, \phi, g} \) be defined as in Definition 1. The algebraic degree of \( f_{\psi, \phi, g} \) clearly equals \( \max(2 + d^s \psi_1, \ldots, 2 + d^s \psi_r, 1 + d^s \phi_1, \ldots, 1 + d^s \phi_r, d^s g) \). It is upper bounded by \( 2 + s \).

4.2.2. Nonlinearity

The next theorem was given in [9] without proof. It generalizes to the extended Maiorana–McFarland’s functions the bounds proved in [9] for Maiorana–McFarland’s functions.

**Theorem 2.** Let \( f_{\psi, \phi, g} \) be defined as in Definition 1. Denote by \( M \) the maximum weight of \( \psi(y), \ y \in F_2^s \), and by \( M' \) its minimum weight. Then the nonlinearity \( N_{f_{\psi, \phi, g}} \) of \( f_{\psi, \phi, g} \) satisfies

\[
2^{n-1} - 2^{r-M'-1} \max_{a \in F_2^s} |E_a| \leq 2^{n-1} - \max_{a \in F_2^s} \sum_{y \in E_a} 2^{r-w_H(\psi(y))} \leq N_{f_{\psi, \phi, g}} \\
\leq 2^{n-1} - \max_{a \in F_2^s} \sqrt{\sum_{y \in E_a} 2^{2r-2w_H(\psi(y))}} \\
\leq 2^{n-1} - 2^{r-M'-1} \max_{a \in F_2^s} \sqrt{|E_a|}
\]

where \( |E_a| \) denotes the size of the set \( E_a \) defined in Theorem 1.

**Proof.** According to Theorem 1, for every \( a \in F_2^s \) and every \( b \in F_2^s \), we have

\[
\mathcal{H}_{\psi, \phi, g}(a, b) = \sum_{y \in E_a} 2^{r-w_H(\psi(y))} (-1)^{\sum_{i=1}^r (\psi_{2i-1}(y) + a_{2i-1}) + \phi_{2i}(y) + g(y) + y \cdot b}.
\]

Thus we have \( \max_{a \in F_2^s} \mathcal{H}_{\psi, \phi, g}(a, b) \leq \max_{a \in F_2^s} \sum_{y \in E_a} 2^{r-w_H(\psi(y))} \leq 2^{r-M'} \max_{a \in F_2^s} |E_a| \) and, according to relation (1) we deduce \( N_{f_{\psi, \phi, g}} \geq 2^{n-1} - \max_{a \in F_2^s} \sum_{y \in E_a} 2^{r-w_H(\psi(y))} \geq 2^{n-1} - 2^{r-M'-1} \max_{a \in F_2^s} |E_a| \).

For every real-valued function \( h \) on \( F_2^s \) and for every subset \( E \) of \( F_2^s \), the sum

\[
\sum_{b \in F_2^s} \left( \sum_{y \in E} h(y)(-1)^yb \right)^2
\]
equals:

\[
\sum_{y, z \in E} h(y)h(z) \left( \sum_{b \in F_2^s} (-1)^{b(y+z)} \right) = 2^s \sum_{y \in E} h^2(y)
\]

(indeed, \( \sum_{b \in F_2^s} (-1)^{b(y+z)} \) is null if \( y \neq z \)).
The maximum of a set of values being always greater than or equal to its mean, we deduce \( \max_{b \in F_2^k} \left( \sum_{y \in E} h(y)(-1)^{y \cdot b} \right)^2 \geq \sum_{y \in E} h^2(y) \) and therefore here

\[
\max_{b \in F_2^k} \sum_{y \in E_a} 2^{r-w_H(y)}(-1)^{ \sum_{i=1}^r (\phi_{2j-1}(y)+a_{2j-1})(\phi_{2j+1}(y)+a_{2j})+g(y)+y \cdot b} \geq \sqrt{\sum_{y \in E_a} 2^{2r-2w_H(y)}} \geq 2^{r-M} \sqrt{|E_a|}.
\]

Hence,

\[
\max_{a \in F_2^M} |\mathcal{F}_{f_{\psi,\phi,a}}(a,b)| \geq \max_{a \in F_2^M} \sqrt{\sum_{y \in E_a} 2^{2r-2w_H(y)}} \geq 2^{r-M} \max_{a \in F_2^M} \sqrt{|E_a|}.
\]

Hence, \( N_{f_{\psi,\phi,a}} \) is upper bounded by \( 2^{n-1} - \frac{1}{2} \max_{a \in F_2^M} \sqrt{\sum_{y \in E_a} 2^{2r-2w_H(y)}} \) and thus by \( 2^{n-1} - 2^{r-M-1} \max_{a \in F_2^M} \sqrt{|E_a|} \).

**Remark.** The left and the right handsides of the inequality of Theorem 2 are similar to the same inequalities for Maiorana–McFarland’s functions. The additional division, by respectively \( 2^M \) and \( 2^M \), contributes to increase the nonlinearity. But the replacement of \( \max_{a \in F_2^M} |\phi^{-1}(a)| \) by \( \max_{a \in F_2^M} |E_a| \) contributes to reduce it (the value of \( \max_{a \in F_2^M} |E_a| \) can obviously be much greater than \( \max_{a \in F_2^M} |\phi^{-1}(a)| \)). It is difficult to determine whether the combined actions of these two modifications result in a reduction or an increase of the nonlinearity. The mean of \( |E_a| \) is upper bounded by \( 2^{2M} \max_{a \in F_2^M} |\phi^{-1}(a)| \) but it is difficult to bound \( \max_{a \in F_2^M} \sqrt{|E_a|} \).

### 4.2.3. Balancedness and resiliency

The following theorem was proved in [9].

**Theorem 3.** Let \( f_{\psi,\phi,a} \) be defined as in Definition 1 and let \( k \) be a nonnegative integer. If for every vector \( a \) of weight smaller than or equal to \( k \) we have \( E_a = \emptyset \) then \( f_{\psi,\phi,a} \) is \( m \)-resilient with \( m \geq k \).

For every \( y \in F_2^n \), denote by \( I_y \) the set of indices equal to: \( \{ j \leq 2t/\psi_{\frac{2}{2}}(y) = 0 \) and \( \phi_j(y) = 1 \} \) if \( r \) is even, or if \( r \) is odd and if \( \phi_r(y) = 0 \);

\[
\{ j \leq 2t/\psi_{\frac{2}{2}}(y) = 0 \) and \( \phi_j(y) = 1 \} \cup \{ r \) if \( r \) is odd and \( \phi_r(y) = 1 \).
\]

A sufficient condition for the fact that \( E_a \) is empty for all \( a \in F_2^k \) such that \( w_H(a) \leq k \) is that, for every \( y \in F_2^n \), \( I_y \) has size strictly greater than \( k \) (then \( f_{\psi,\phi,a} \) is \( m \)-resilient with \( m \geq k \); in particular, if for every \( y \in F_2^n \), the set \( I_y \) is not empty, then \( f_{\psi,\phi,a} \) is balanced).

The proof of this theorem is a direct consequence of the fact that for every \( y \in E_a \) and every index \( j \in I_y \), we have \( a_j = 1 \).

In the case of Maiorana–McFarland’s functions, the condition of Theorem 3 reduces to the fact that every element in \( \phi(F_2^k) \) has Hamming weight strictly greater
than \( k \), since all coordinate functions of \( \psi \) are null. It can be translated similarly in the general case.

**Corollary 1.** Let \( f_{\psi,\phi,g} \) be defined as in Definition 1 and let \( k \) be a non-negative integer. Consider the mapping \( \Phi \) from \( F_2^n \) to \( F_2^n \) whose \( j \)-th coordinate function for \( j \leq 2t \) equals the product of the Boolean functions \( \phi_j \) and \( 1 + \psi_{\left[\frac{j}{2}\right]} \) and whose \( r \)-th coordinate function equals \( \phi_r \) if \( r \) is odd. If the image of every element in \( F_2^n \) by \( \Phi \) has Hamming weight strictly greater than \( k \), then \( f_{\psi,\phi,g} \) is \( m \)-resilient with \( m \geq k \).

In particular, if the image of every element in \( F_2^n \) by \( \Phi \) is nonzero, then \( f_{\psi,\phi,g} \) is balanced.

**Remark**

- The Maiorana–McFarland’s function \( f_{\phi,g} : (x,y) \mapsto x \cdot \Phi(y) + g(y) \) is naturally associated to \( f_{\psi,\phi,g} \). If the image of every element in \( F_2^n \) by \( \Phi \) has Hamming weight strictly greater than \( k \), then \( f_{\phi,g} \) is also \( m \)-resilient with \( m \geq k \). Notice that we have \( y \in \Phi^{-1}(a) \) if and only if for every \( j \leq 2t \):
  \[
  \begin{cases}
  a_j = 1 \Rightarrow \psi_{\left[\frac{j}{2}\right]}(y) = 0 \text{ and } \phi_j(y) = 1 = a_j, \\
  a_j = 0 \Rightarrow \psi_{\left[\frac{j}{2}\right]}(y) = 1 \text{ or } \phi_j(y) = 0 = a_j, \text{ and } \phi_r(y) = a_r \text{ if } r \text{ is odd.}
  \end{cases}
  \]

  Hence, \( \Phi^{-1}(a) \) is in general not included in \( \Phi^{-1}(a) \) (take \( a_j = 0 \), \( \psi_{\left[\frac{j}{2}\right]}(y) = 1 \) and \( \phi_j(y) = 1 \) for some \( j \)), then we can have \( y \in \Phi^{-1}(a) \) and \( y \notin \Phi^{-1}(a) \).

- **Restrictions on functions achieving Sarkar–Maitra’s bound:** It is difficult to characterize those functions \( f_{\psi,\phi,g} \) which achieve Sarkar–Maitra’s bound. But we can prove some necessary conditions.
Proposition 4. Let \( f_{\psi, \phi, g} \) be defined as in Definition 1. Assume that \( E_a \) is empty for all \( a \in F_2^n \) such that \( w_H(a) \leq k \). If \( f_{\psi, \phi, g} \) achieves the best possible nonlinearity \( 2^{n-1} - 2^{k+1}, \) then \( k + 1 \leq r \leq k + M + 2, \) where \( M \) denotes the maximum weight of \( \psi(y) \).

If \( r = k + 1 \) then \( f_{\psi, \phi, g} \) is a Maiorana–McFarland’s function.

If \( k + 2 \leq r \leq k + M + 2, \) then \( E_a \) has size at most \( 2^{2k-2r+2M+4} \) for every \( a \) and \( 2^{n+r-2k-2M-4} \leq \sum_{i=k+1}^{r} (\cdot)^i \).

Proof. The property \( r \geq k + 1 \) is obvious since there must exist \( a \) such that \( E_a \neq \emptyset \). If \( N_{f_{\psi, \phi, a}} = 2^{n-1} - 2^{k+1} \), we have \( \sqrt{\max_{a \in F_2^n} |E_a|} \leq 2^{k-r+M+2} \), according to Theorem 2 and hence \( r \leq k + M + 2 \) since \( \max_{a \in F_2^n} |E_a| \geq 1 \).

If \( r = k + 1 \), then it is a simple matter to see that \( \psi \) takes null value and that \( \phi \) takes constant value \((1, \ldots, 1)\). Then \( f_{\psi, \phi, g} \) is a Maiorana–McFarland’s function and has been studied in [9].

If \( k + 2 \leq r \leq k + M + 2, \) then, \( E_a \) having size 0 if \( w_H(a) \leq k \) and size at most \( 2^{2k-2r+2M+4} \) otherwise, we deduce \( 2^r \leq 2^{2k-2r+2M+4} \sum_{i=k+1}^{r} (\cdot)^i \). □

Methods for constructing highly nonlinear resilient functions from Definition 1:

If for any \( a \in F_2^n \), the set \( E_a \) equals \( \phi^{-1}(a) \) (i.e. is minimal) and if every element in \( \phi(F_2^n) \) has Hamming weight strictly greater than \( k \) then \( f_{\psi, \phi, g} \) and \( f_{\phi, g} \) are both at least \( k \)-resilient. Since, for every \( a \in F_2^n \) and \( b \in F_2^n \), \( \overline{f_{\phi, g}}(a, b) \) equals \( 2^r \sum_{y \in \phi^{-1}(a)} (-1)^{g(y)+b \cdot y} \) and \( \overline{f_{\psi, \phi, g}}(a, b) \) equals \( \sum_{y \in \psi^{-1}(a)} 2^r - w_H(\psi(y)) (-1)^{g(y)+b \cdot y} \), the nonlinearity of \( f_{\psi, \phi, g} \) can be smaller than that of \( f_{\psi, \phi, g} \).

- Let \( k \) be some positive integer. Assume that for every vector \( a \in F_2^n \) whose Hamming weight \( w_H(a) \) is smaller than or equal to \( k \), either the set \( E_a \) is empty or for every \( b \in F_2^n \) of weight at most \( k - w_H(a) \), the restriction to \( E_a \) of the function \( \sum_{i=1}^{r} (\phi_{2i-1}(y) + a_{2i-1})(\phi_{2i}(y) + a_{2i}) + g(y) + y \cdot b \) is balanced (for example, the restriction of \( \phi \) to \( E_a \) is constant and the restriction of \( g + b \cdot y \) to \( E_a \) is balanced). Assume also that \( \psi(y) \) has constant weight on \( E_a \). Then, according to Theorem 1, \( f_{\psi, \phi, g} \) is \( k \)-resilient.

Moreover, if every non-empty set \( E_a \) is a flat and if, for some \( \lambda \), every such restriction achieves nonlinearity greater than or equal to \( \frac{|E_a|}{2} - \lambda \) (we assume this value is achieved for some \( a \) then \( 2^{n-1} - 2^{r-M} \lambda \leq N_{f_{\psi, \phi, a}} \leq 2^{n-1} - 2^{r-M} \lambda \), where \( M \) (resp. \( M' \)) is the maximum (resp. minimum) weight of \( \psi(y), y \in F_2^n \).

- In [9] is described another method and examples of functions achieving good trade-offs between resiliency and nonlinearity are also given:
  - For any \( n = 2m \) with \( m \) odd, there exists \( f_{\psi, \phi, g} \) balanced with nonlinearity \( 2^{n-1} - 2^{n/2-1} - 2^{(n/2-1)/2} \). This is the best known nonlinearity for these parameters.
for every $n$ even, let $k$ be such that $\sum_{i=0}^{k} \binom{n/2-2}{i} \leq 2^{n/2-2}$. Then there exists $f_{\psi, \phi, g}$ $k$-resilient with nonlinearity $2^{n-1} - 2^{n/2-1} - 2^{n/2-2}$.

Such characteristics were not obtained in [31,36,37,45].

4.2.4. Propagation criterion

Let us compute the derivatives of $f_{\psi, \phi, g}$. For every $a \in F_2^n$ and every $b \in F_2^n$, we have

$$D_{(a,b)}f_{\psi, \phi, g}(x, y) = \sum_{i=1}^t x_{2i-1} x_{2i} D_b \psi_i(y) + \sum_{i=1}^t (a_{2i-1} x_{2i} + x_{2i-1} a_{2i} + a_{2i-1} a_{2i}) \psi_i(y + b) + x \cdot D_b \phi(y) + a \cdot \phi(y + b) + D_b g(y).$$

Thus, $D_{(a,b)}f_{\psi, \phi, g}(x, y)$ belongs to the extended Maiorana–McFarland’s class and has the form $f_{D_b \psi, a, h_{a,b}}(x, y)$ where for every $i \leq t$, the $(2i - 1)$th coordinate function of $\Psi_{a,b}$ equals $a_{2i} \psi_i(y + b) + D_b a_{2i-1}(y)$, its $(2i)$th coordinate function equals $a_{2i-1} \psi_i(y + b) + D_b \phi_{2i}(y)$, and where $h_{a,b}(y) = \sum_{i=1}^t (a_{2i-1} a_{2i} \psi_i(y + b) + a \cdot \phi(y + b) + D_b g(y)$. We deduce from Corollary 1:

**Proposition 5.** Let $f_{\psi, \phi, g}$ be defined as in Definition 1. For every $(a, b) \in F_2^n \times F_2^n$, denote by $\Phi_{a,b}$ the function from $F_2^n$ to $F_2^n$ whose $(2i - 1)$th coordinate for $i \leq t$ equals the product of the Boolean functions $a_{2i} \psi_i(y + b) + D_b a_{2i-1}(y)$ and $D_b \psi_i(y) + 1$, whose $(2i)$th coordinate function equals the product of the Boolean functions $a_{2i-1} \psi_i(y + b) + D_b \phi_{2i}(y)$ and $D_b \psi_i(y) + 1$ and whose $r$th coordinate function equals $D_b \phi_r(y)$ if $r$ is odd. If, for every $(a, b)$ of weight at most 1, the image of every element in $F_2^n$ by $\Phi_{a,b}$ is nonzero, then $f_{\psi, \phi, g}$ satisfies $PC(l)$.

4.2.5. Plateaued and bent functions

Let $f_{\psi, \phi, g}$ be defined as in Definition 1. According to Theorem 1, if $E_a$ has size 0 or 1 (respectively 0 or 2) for every $a$ and if $\psi$ has constant weight, then $f_{\psi, \phi, g}$ is plateaued (i.e. has a Walsh spectrum with three values, 0 and $\pm \lambda$).

In particular, if $E_a$ has size 1 for every $a$ and if for some integer $k$, taking $r = n/2 + k$ and $s = n/2 - k$, we have $w_1(\psi(y)) = k$ for every $y \in F_2^n$, then $f_{\psi, \phi, g}$ is bent.

This condition is satisfied by every function of the form

$$x_1 x_2 + \cdots + x_{2k-1} x_{2k} + x \cdot \phi(y) + g(y),$$

where the mapping $\phi = (\phi_1, \ldots, \phi_r)$ is such that the mapping $y \in F_2^n \mapsto (\phi_{2k+1}(y), \ldots, \phi_r(y))$ is one to one.

It is also possible to design bent functions from the extended Maiorana–McFarland’s class with nonconstant mappings $\psi$: 
A new construction of bent functions: Take (for instance) \( r \) even (thus \( s = r - 2k \) is also even). Let \((F_j)_{1 \leq j \leq 2^s}\) be a partition of \( F_2^s \), where the \( F_j \)'s are flats of the form \( \{x \in F_2^s; \ x_i = u^j_i, \ \forall i \in I_j\} \), where \( I_j \) is a subset of \( \{1, \ldots, n\} \) of size \( s \) (thus, each \( F_j \) has size \( 2^{r-s} \)) such that \( 2i - 1 \in I_j \iff 2i \in I_j \) for every \( i \) (this is possible since \( s \) is even) and where the vector \( u^j \) belongs to \( F_2^d \). For every \( y \in F_2^s \), choose injectively \( j = 1, \ldots, 2^s \); then, for every \( i \leq r/2 \), set \( \psi_i(y) = 0 \) if \( 2i - 1 \in I_j \) (and \( 2i \in I_j \)) and set \( \psi_i(y) = 1 \) otherwise; choose \( \phi(y) \) in \( F_j \). Then for every function \( g \), the function \( f_{\phi,\psi,g} \) is such that \( E_a \) has size 1 for every \( a \). Indeed, \( E_a \) is the singleton \( \{\phi^{-1}(a)\} \) because the condition \( \psi_j(y) = 0 \Rightarrow \phi_{2j-1}(y) = a_{2j-1} \) and \( \phi_{2j}(y) = a_{2j} \) implies that \( \phi(y) = a \), since \((F_j)_{1 \leq j \leq 2^s}\) is a partition of \( F_2^s \). We have also \( w_4(\psi(y)) = k \) for every \( y \in F_2^s \). Thus \( f_{\phi,\psi,g} \) is bent.

A way of obtaining such a partition \((F_j)_{1 \leq j \leq 2^r}\) is by taking the \( F_j \)'s equal to the cosets of \( \{(0, \ldots, 0)\} \times F_2^{2^k} \). The set \( I_j \) is then independent of \( j \); this would lead to functions linearly equivalent to the functions \((12)\). But, starting from this simple partition, we can modify it to obtain a partition such that \( I_j \) depends on \( j \). For instance, choose \( j_1, j_2, j_3 \) and \( j_4 \) such that the vectors \( u^{j_1}, u^{j_2}, u^{j_3} \) and \( u^{j_4} \) coincide in \( s - 2 \) coordinates \((F = F_{j_1} \cup F_{j_2} \cup F_{j_3} \cup F_{j_4} \) is then a flat); choose two indices \( 2l_0 - 1 \) and \( 2l_0 \) greater than \( s \) and replace \( F_{j_1}, F_{j_2}, F_{j_3} \) and \( F_{j_4} \) respectively by \( \{x \in F; \ x_{2l_0-1} = 0 \ \text{and} \ x_{2l_0} = 1\} \), \( \{x \in F; \ x_{2l_0-1} = 0 \ \text{and} \ x_{2l_0} = 0\} \), \( \{x \in F; \ x_{2l_0-1} = 1 \ \text{and} \ x_{2l_0} = 1\} \). This does not change the property of \((F_j)_{1 \leq j \leq 2^r}\) of being a partition but it changes \( I_{j_1}, I_{j_2}, I_{j_3} \) and \( I_{j_4} \).

It remains to be proven that new bent functions can be obtained through this construction. But in any case, this method of construction is new.

References


[30] E. Pasalic, S. Maitra, A Maiorana–McFarland type construction for resilient Boolean functions on $n$ variables ($n$ even) with nonlinearity $> 2^{n-1} - \frac{2^n}{2^2} + \frac{2^n}{2}$, Proceedings of the Workshop on Coding and Cryptography, Versailles, France, 2003, pp. 365–374.


Further reading