# Modifying Boolean Functions to Ensure Maximum Algebraic Immunity

Konstantinos Limniotis, Nicholas Kolokotronis, *Member, IEEE*, and Nicholas Kalouptsidis

***Abstract*—The algebraic immunity of cryptographic Boolean functions is studied in this paper. Proper modifications of functions achieving maximum algebraic immunity are proved, in order to yield new functions of also maximum algebraic immunity. It is shown that the derived results apply to known classes of functions. Moreover, two new efficient algorithms to produce functions of guaranteed maximum algebraic immunity are developed, which further extend and generalize known constructions of functions with maximum algebraic immunity.**

***Index Terms*—algebraic attack, algebraic immunity, annihilators, Boolean functions, cryptography**

## I. Introduction

Boolean functions constitute important building blocks for cryptographic systems, either as S-boxes in block ciphers or as filter/combiner functions in stream ciphers. The security of these systems is mainly attributed to the properties of the underlying functions. More precisely, cryptographic Boolean functions need to satisfy specific criteria, such as balancedness or high nonlinearity, in order to ensure resistance against cryptanalytic attacks.

Among the attacks that have received great attention over the last years is the so-called algebraic attack, which exploits the structure of the underlying functions to construct an overdefined system of nonlinear multivariate equations that will allow to determine the secret key [11]. As a result of the analysis derived in [17], the following property is stated as a prerequisite for any function $f$ in order to prevent algebraic attacks: there should not be a function $g$ of low degree satisfying either $f * g = 0$ or $(f + 1) * g = 0$. This observation leads to the definition of the *algebraic immunity* as a significant cryptographic criterion for Boolean functions that relates to the minimum degree of functions satisfying the above condition. If such a low degree function $g$ exists, then an algebraic attack may take place. Moreover, an algebraic attack can be more easily mounted if many linearly independent (rather than only one) such low degree functions exist [11].

Part of this work was presented at the IEEE International Symposium on Information Theory, Saint Petersburg, Russia, July 31–August 6, 2011.

K. Limniotis is with the Hellenic Data Protection Authority, Kifissias 1–3, 11523, Athens, Greece (e-mail: klimniotis@dpa.gr), and with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, University Campus, 15784 Athens, Greece (e-mail: klimn@di.uoa.gr).

N. Kolokotronis is with the Department of Computer Science and Technology, University of Peloponnese, End of Karaiskaki Str., 22100 Tripolis, Greece (e-mail: nkolok@uop.gr).

N. Kalouptsidis is with the Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, University Campus, 15784 Athens, Greece (e-mail: kalou@di.uoa.gr).

There are many open problems that should be addressed in the design of cryptosystems that are immune to algebraic attacks [2]. An important open issue is the construction of Boolean functions achieving the maximum possible algebraic immunity. Several constructions of such functions are provided in the literature. The first one is the *majority* function, described in [13], which is a symmetric function; other constructions of symmetric functions having maximum algebraic immunity are also given in [1], [20], [9] (note that when the number of the variables is odd, then the only symmetric function with maximum algebraic immunity is the majority function [19]). However, the symmetry property poses a risk from a cryptographic point of view and, thus, constructions of non-symmetric functions of maximum algebraic immunity are of high importance. Several such constructions have been given in [3], [4], [14], [22], [7]; unfortunately, most of the functions do not present high nonlinearity, whereas others are non-balanced. Further constructions, providing functions with higher nonlinearities, are given in [5], [24], [21], [25] (as is pointed out though in [8], the first construction in [24] coincides with the construction in [5]). Finally, functions with odd number of variables and maximum algebraic immunity are constructed in [15]; however, this construction, although it covers the entire space of functions with maximum algebraic immunity, is more theoretical than practical. In general, constructing functions with maximum algebraic immunity (without sacrificing other cryptographic criteria) still remains an active research area.

Algebraic attacks may be further improved by exploiting linear relations among the keystream bits; this approach, called *fast algebraic attack*, was first proposed in [12]. Fast algebraic attacks may be efficiently applied to cryptographic systems that are resistant to conventional algebraic attacks; however, they require knowledge of consecutive keystream bits (which is not needed in algebraic attacks). Amongst the known families of functions achieving maximum algebraic immunity, those proposed in [5], [21] seem to behave well against fast algebraic attacks. A maximum value for the algebraic immunity is also a necessary (though not sufficient) condition for withstanding such attacks [18].

In this paper, new results are proved for efficiently constructing cryptographic Boolean functions having maximum algebraic immunity. Our analysis is based on exploring the behavior of functions with maximum algebraic immunity when some entries of their truth table are altered. First, we prove that proper slight modifications yield functions whose algebraic immunity is at least maximum minus one; this result agrees with the heuristic arguments presented in [6] indicating that a random Boolean function has high algebraic immunity

with a high probability. Next we proceed by further proving sufficient conditions to ensure that the functions obtained via the aforementioned modification have maximum algebraic immunity, whereas the cases of odd and even number of variables are treated separately. Hence, these results further strengthen the existing constructions of cryptographic functions with maximum algebraic immunity by providing the means to appropriately modify such functions so as to ensure that the algebraic immunity does not decrease. In the process, the proposed analysis yields two new efficient algorithms providing functions with maximum algebraic immunity. The first one is based on proper modifications of the majority function and it extends the construction in [22] (which is restricted to the class of rotation symmetric Boolean functions), whereas it generalizes the construction given in [7] (for the case of even number of variables) to the odd case. The second algorithm, which applies to functions of odd number of variables, is based on proper modifications of the functions that have been recently proposed in [21], [25]. For the first case, the Algebraic Normal Form (i.e. multivariate representation) of the functions is being considered, whereas for the second algorithm the support of the function is decribed as a set of powers of a primitive element over a finite field (i.e. the univariate representation of functions is used).

The paper is organized as follows; the basic definitions and the notation used are introduced in Section II. Section III presents the behavior of the functions with maximum algebraic immunity if one or two entries of their truth table are modified. This section forms the basis to identify sufficient conditions to ensure that such modifications do not decrease the algebraic immunity; such conditions are proved in Section IV, whereas an algorithm is provided for constructing functions with maximum algebraic immunity. This algorithm is based upon the special structure of the majority function and generalizes other known constructions lying in the same context. In addition, by considering the univariate polynomial representation of Boolean functions, we construct in Section V another efficient algorithm for generating new functions of odd number of variables and maximum algebraic immunity, via appropriate modifications of the functions given in [21], [25]. Finally, concluding remarks are given in Section VI.

## II. Preliminaries

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, where $\mathbb{F}_2 = \{0, 1\}$ is the binary field. The set of Boolean functions on $n$ variables is denoted by $\mathbb{B}_n$. The truth table of $f$ is the binary vector

$$\boldsymbol{f} = (f(0, 0, \ldots, 0), f(0, 0, \ldots, 1), \ldots, f(1, 1, \ldots, 1))$$

of length $2^n$, also denoted by $f$ for simplicity. The Boolean function $f \in \mathbb{B}_n$ is said to be *balanced* if $\mathrm{wt}(f) = 2^{n-1}$. The *support* of a Boolean function $f \in \mathbb{B}_n$ is defined as $\mathrm{supp}(f) = \{\boldsymbol{b} \in \mathbb{F}_2^n : f(\boldsymbol{b}) = 1\}$. We also define the support of a vector $\boldsymbol{b} \in \mathbb{F}_2^n$ as $\mathrm{supp}(\boldsymbol{b}) = \{1 \le i \le n : b_i = 1\}$.

Any $n$-variable Boolean function $f$ is uniquely expressed by the *Algebraic Normal Form* (ANF) as

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} c_{\boldsymbol{v}} \boldsymbol{x}^{\boldsymbol{v}} \tag{1}$$

where the sum is taken modulo 2, $c_{\boldsymbol{v}} \in \mathbb{F}_2$ and $\boldsymbol{x}^{\boldsymbol{v}} = \prod_{i=1}^n x_i^{v_i}$. The *degree* $\deg(f)$ of $f$ is the highest number of variables that appear in a monomial in its ANF.

Since there is a natural correspondence between the $n$-th dimensional vector space $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$, a function $f \in \mathbb{B}_n$ can also be represented by a univariate polynomial from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$

$$f(x) = \sum_{i=0}^{2^n-1} \beta_i x^i$$

where $\beta_0, \beta_{2^n-1} \in \mathbb{F}_2$ and $\beta_{2i} = (\beta_i)^2 \in \mathbb{F}_{2^n}$ for $1 \le i \le 2^n - 2$; this polynomial is associated with a Mattson-Solomon polynomial of $f$ [16, p. 401].

The complement of a binary variable $x$ will be denoted by $\overline{x} = x + 1$, where "+" represents addition modulo 2. Any variable, in either complemented or uncomplemented form, is called *literal*. Similarly, if $\boldsymbol{b} \in \mathbb{F}_2^n$, we write $\overline{\boldsymbol{b}} \triangleq \boldsymbol{b} + \mathbf{1}$, where $\mathbf{1}$ is the all-one vector of length $n$. For any Boolean function $f \in \mathbb{B}_n$ and a vector $\boldsymbol{b} \in \mathbb{F}_2^n$, a *minterm* $x_{\boldsymbol{b}}$ is defined as $x_{\boldsymbol{b}} = (x_1 + \overline{b}_1) \cdots (x_n + \overline{b}_n)$. Hence, a minterm is a product of literals where each of the variables appears once. Clearly, $x_{\boldsymbol{b}} \in \mathbb{B}_n$ and $x_{\boldsymbol{b}}(\boldsymbol{a}) = 1$ if and only if $\boldsymbol{a} = \boldsymbol{b}$. Any product of $k \le n$ literals, considered as a Boolean function with $n$ variables, is the *indicator* (or *characteristic function*) of a flat of dimension $n - k$. Moreover, if $\boldsymbol{a} \in \mathbb{F}_2^n$ is $n$-tuple representation of an element $\alpha^i \in \mathbb{F}_{2^n}$ (in terms of some fixed basis - e.g. polynomial), where $\alpha$ is a primitive element over $\mathbb{F}_{2^n}$, we also write the corresponding minterm as $x_{\alpha^i}$.

If $E$ is a linear subspace of $\mathbb{F}_2^n$, we denote by $f|_E$ the restriction of $f$ on $E$. Then $f$ is decomposed as follows

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{a} \in E^\perp} \vartheta_{\boldsymbol{a}+E}(\boldsymbol{x})\, f|_{\boldsymbol{a}+E}(\boldsymbol{x}) \tag{2}$$

where $E^\perp$ is the orthogonal complement of $E$ and $\vartheta_{\boldsymbol{a}+E}$ is the indicator of the flat $\boldsymbol{a}+E$, that is $\vartheta_{\boldsymbol{a}+E}(\boldsymbol{x}) = 1 \Leftrightarrow \boldsymbol{x} \in \boldsymbol{a}+E$.

*Definition 1:* For any $f \in \mathbb{B}_n$, its nonlinearity $\mathsf{nl}(f)$ is defined as

$$\mathsf{nl}(f) = \min_{g \in \mathbb{B}_n : \deg(g) \le 1} \mathrm{wt}(f + g)\,.$$

*Definition 2:* Given $f \in \mathbb{B}_n$, we say that $g \in \mathbb{B}_n$ is an annihilator of $f$ if and only if $g$ lies in the set $\mathcal{AN}(f) = \{g \in \mathbb{B}_n : f * g = 0\}$, where $*$ denotes the multiplication (point-wise product) of Boolean functions.

From the analysis of [11], [17] it becomes evident that a cryptographic Boolean function $f$ should neither have low degree multiples nor low degree annihilators; otherwise, it is probable that an algebraic attack can be successfully mounted. As it is proved in [17], these requirements are equivalent to saying that $f$ has high algebraic immunity.

*Definition 3:* The algebraic immunity $\mathsf{AI}_n(f)$ of $f \in \mathbb{B}_n$ is the minimum degree of all nonzero annihilators of $f$ and $f + 1$.

A well-known result, first proved in [11], is that $\mathsf{AI}_n(f) \le \lceil \frac{n}{2} \rceil$ for all $f \in \mathbb{B}_n$.

A simple class of functions achieving the maximum algebraic immunity consists of the so-called majority functions [13], namely:

*Proposition 1:* Let $f \in \mathbb{B}_n$ and $\epsilon \in \mathbb{F}_2$. Then

$$f(\boldsymbol{x}) = \begin{cases} 0, & \text{if } \mathrm{wt}(\boldsymbol{x}) < \frac{n}{2}, \\ \epsilon, & \text{if } \mathrm{wt}(\boldsymbol{x}) = \frac{n}{2} \text{ (and } n \text{ is even)}, \\ 1, & \text{if } \mathrm{wt}(\boldsymbol{x}) > \frac{n}{2}, \end{cases}$$

is called majority function and satisfies $\mathsf{AI}_n(f) = \lceil \frac{n}{2} \rceil$.

Amongst several constructions of Boolean functions achieving maximum algebraic immunity, the one of [5] is of high importance since it also satisfies several other cryptographic criteria. This construction is described as follows:

*Proposition 2:* Let $n > 1$ be an integer and $\alpha$ be a primitive element of the finite field $\mathbb{F}_{2^n}$. If $f \in \mathbb{B}_n$ with $\mathrm{supp}(f) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^{n-1}-2}\}$, then $\mathsf{AI}_n(f) = \lceil \frac{n}{2} \rceil$.

The above construction provides functions whose support consists of consecutive powers of a primitive element $\alpha$ over $\mathbb{F}_{2^n}$. Generalizations of this construction have been recently given in [21], [25], based on the univariate representation of functions; to describe these, we first need to recall some notation from [21], [25] (which will be used in the sequel).

A *cyclotomic coset* modulo $2^n - 1$ is defined as $I_d = \{d, 2d, \ldots, 2^{n_d-1}d\}$, where $n_d$ is the smallest integer such that $2^{n_d}d \equiv d \pmod{2^n - 1}$, and the smallest element $j$ in $I_d$ is referred to as *coset leader*. The set containing all coset leaders modulo $2^n - 1$ will be denoted by $I$. We also denote by $m_d(x)$ the *minimal polynomial* of $\alpha^d$ over $\mathbb{F}_2$ (whose roots are the elements of $I_d$). Next we define the polynomial

$$R_d(x) = \prod_{i \in I, \mathrm{wt}(i) = d} m_{2^n-1-i}(x) = \prod_{i : \mathrm{wt}(i) = n-d} (x - \alpha^i)$$

for $1 \leq d \leq n-1$, where $R_n(x) = x+1$ and $R_0(x) = x$. We also define the product

$$R_{d_1,d_2}(x) = \prod_{i=d_1}^{d_2} R_i(x)$$

for $0 \leq d_1 \leq d_2 \leq n$. It is clear that, for $d_1 < d_2$,

$$R_{d_1+1,d_2}(x) = 1 + r_1 x + r_2 x^2 + \ldots + r_{E-1} x^{E-1} + x^E \quad (3)$$

where $E = \sum_{i=d_1+1}^{d_2} \binom{n}{i}$ (and $r_i \in \mathbb{F}_2$, $i = 1, \ldots, E-1$).

Since $r_0 = r_E = 1$, the following $\sum_{i=0}^{d_1} \binom{n}{i} \times \sum_{i=0}^{d_2} \binom{n}{i}$ matrix

$$\boldsymbol{R}_{d_1+1,d_2} = \begin{pmatrix} r_0 & r_1 & \ldots & r_E & 0 & \ldots & 0 \\ 0 & r_0 & \ldots & r_{E-1} & r_E & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & \vdots & \vdots & \ldots & 0 \\ 0 & 0 & \ldots & \vdots & \vdots & \ldots & r_E \end{pmatrix} \quad (4)$$

is of full rank $\sum_{i=0}^{d_1} \binom{n}{i}$. Next we enumerate each column of $\boldsymbol{R}_{d_1+1,n-1}$, where the first column is considered as the 0-th column (and, thus, the last is the $(2^n-2)$-th column). For a given function $f \in \mathbb{B}_n$, let $\boldsymbol{R}^{1_f}_{d_1+1,n-1}$ be the sub-matrix of $\boldsymbol{R}_{d_1+1,n-1}$ such that the $j$-th column of $\boldsymbol{R}_{d_1+1,n-1}$ belongs to $\boldsymbol{R}^{1_f}_{d_1+1,n-1}$ if and only if $\alpha^j \in \mathrm{supp}(f)$; the sub-matrix $\boldsymbol{R}^{0_f}_{d_1+1,n-1}$ is similarly defined.

*Theorem 1 ([21]):* There exists $g \in \mathcal{AN}(f)$ with $\deg(g) \leq d$ if and only if

$$\sum_{i=0}^{d} \binom{n}{i} > \mathrm{rank}(\boldsymbol{R}^{1_f}_{d_1+1,n-1})$$

*Proposition 3 ([21]):* Let $n > 1$ be an integer and $\alpha$ be a primitive element of the finite field $\mathbb{F}_{2^n}$. If $f \in \mathbb{B}_n$ with $\mathrm{supp}(f) = \{1, \alpha, \alpha^2, \ldots, \alpha^{\delta_n - 1}\} \cup S$, where

- $S \subset \{\alpha^{\delta_n}, \ldots, \alpha^{\delta_n + \hat{\delta}_n + 1}\}$ and $|S| = 2^{n-1} - \delta_n$,
- $\delta_n = \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$,
- $\hat{\delta}_n = \binom{n}{\lceil \frac{n}{2} \rceil}$,

then $\mathsf{AI}_n(f) = \lceil \frac{n}{2} \rceil$.

Is is shown in [25] that specific modifications of any function constructed via Proposition 3 yield other functions of maximum algebraic immunity; these are further discussed (and extended) in Section V.

## III. General Concepts of Modification Strategies

In this section we prove that proper slight modifications of any function $f \in \mathbb{B}_n$ with maximum algebraic immunity $\lceil \frac{n}{2} \rceil$ yields functions which are bound to have maximum or almost maximum (that is $\lfloor \frac{n}{2} \rfloor$) algebraic immunity. Moreover, it is shown that the lowest degree annihilator of any such modified function with algebraic immunity $\lfloor \frac{n}{2} \rfloor$ is unique. These results, apart from their own significance, form the basic building blocks to derive proper modifications of functions ensuring maximum algebraic immunity, which are subsequently described in Section IV.

We first present a preliminary result that is subsequently used; this result does not depend on the parity of $n$.

*Lemma 1:* Let $f \in \mathbb{B}_n$ have no nonzero annihilators of degree less than $k$, $1 < k \leq \deg(f)$, and let $\boldsymbol{a} \in \mathbb{F}_2^n$ be such that $f(\boldsymbol{a}) = 0$. Then, the function $h = f + x_{\boldsymbol{a}}$ does not have nonzero annihilators of degree less than $k$.

*Proof:* Note that $h(\boldsymbol{x}) = f(\boldsymbol{x})$ for all $\boldsymbol{x} \neq \boldsymbol{a}$, whereas $h(\boldsymbol{a}) = 1$. Hence, $\mathcal{AN}(h) \subset \mathcal{AN}(f)$. ∎

The following result is also well-known [2].

*Proposition 4:* If $n$ is odd, then $f \in \mathbb{B}_n$ has maximum algebraic immunity $\frac{n+1}{2}$ if and only if $f$ is balanced and has no nonzero annihilators of degree less than $\frac{n+1}{2}$.

If $n$ is even, then things are different; a necessary (but not sufficient) condition for $f$ to have maximum algebraic immunity $\frac{n}{2}$ is that [3]

$$|\mathrm{wt}(f) - 2^{n-1}| \leq \tbinom{n-1}{n/2}$$

Based on the above, we prove the following which extends the result of [23, Corollary 4.1] stating that $\mathsf{AI}_n(f + x_{\boldsymbol{0}}) = \frac{n-1}{2}$ (where $\boldsymbol{0} \in \mathbb{F}_2^n$ is the all-zero vector) for all $f \in \mathbb{B}_n$ with $\mathsf{AI}_n(f) = \frac{n+1}{2}$ and $n$ odd.

*Proposition 5:* Let $f \in \mathbb{B}_n$, where $n$ is odd, having maximum algebraic immunity $\frac{n+1}{2}$, and let $\boldsymbol{a} \in \mathbb{F}_2^n$ be such that $f(\boldsymbol{a}) = 1$. Then the function $h = f + x_{\boldsymbol{a}}$ satisfies

$$\mathsf{AI}_n(h) = \frac{n-1}{2}$$

and, moreover, it has a unique annihilator $u$ of degree $\frac{n-1}{2}$.

*Proof:* Note that $(f+1)(\boldsymbol{a}) = 0$ and, consequently, Lemma 1 implies that the function $h+1$ has no nozero annihilators of degree less than $\frac{n+1}{2}$. We shall first prove that there exists nonzero $u \in \mathcal{AN}(h)$ with $\deg(u) < \frac{n+1}{2}$. Let us assume that such function does not exist. Hence, the function $h$ has also the maximum possible algebraic immunity $\frac{n+1}{2}$. However, since $h$ is clearly not balanced (recall that $f$ is necessarily balanced), we get a contradiction due to Proposition 4.

Next, we shall prove that the annihilator $u$ of the function $h$ satisfying $\deg(u) \leq \frac{n-1}{2} < \frac{n+1}{2}$ is unique. Note that any such $u$ (as any annihilator of $h$) satisfies

$$h * u = 0 \Rightarrow (f + x_{\boldsymbol{a}}) * u = 0 \Rightarrow f * u = x_{\boldsymbol{a}} * u.$$

The fact $\deg(u) < \mathsf{AI}_n(f)$ implies that $x_{\boldsymbol{a}} * u$ can not be identically zero and, since the weight of the Boolean function $x_{\boldsymbol{a}}$ is 1, we necessarily get

$$f * u = x_{\boldsymbol{a}}\,. \tag{5}$$

If there existed $u' \neq u$ with $\deg(u') < \mathsf{AI}_n(f)$ and $f*u' = x_{\boldsymbol{a}}$, then we would obtain $f * (u + u') = 0$, which contradicts the fact that $\mathsf{AI}_n(f) = \frac{n+1}{2}$. Thus, the function $u \in \mathcal{AN}(h)$ satisfying $\deg(u) < \frac{n+1}{2}$ is unique.

Since $f(\boldsymbol{a}) = 1$, we have $x_{\boldsymbol{a}} = f * x_{\boldsymbol{a}}$ and (5) yields that $f * (u + x_{\boldsymbol{a}}) = 0$, i.e. $u + x_{\boldsymbol{a}} \in \mathcal{AN}(f)$. Let $E$ be a $(n-1)$-dimensional (affine) subspace of $\mathbb{F}_2^n$ not containing vector $\boldsymbol{a}$, such that $E \cup \{\boldsymbol{a} + E\} = \mathbb{F}_2^n$. Then

$$f|_E * (u + x_{\boldsymbol{a}})|_E = 0 \Rightarrow f|_E * u|_E = 0$$

and, since $\mathsf{AI}_n(f) = \frac{n+1}{2}$, its restriction $f|_E$ can not have nonzero annihilators of degree less than $\frac{n-1}{2}$. Thus it holds either $\deg(u|_E) \geq \frac{n-1}{2}$, in which case we immediately get $\deg(u) = \frac{n-1}{2}$, or $u|_E = 0$. Note that we can always find a $(n-1)$-dimensional flat $E$ not containing $\boldsymbol{a}$ for which $u|_E \neq 0$. Indeed, if this was not true then we would be able to find $k > \frac{n-1}{2}$ flats $E_1, \ldots, E_k$ such that $u|_{E_i} = 0$ and $V = \bigcap_i E_i$ be a $(n-k)$-dimensional flat not containing $\boldsymbol{a} \in \mathbb{F}_2^n$; then we would obtain $u = \vartheta_{\boldsymbol{a}+V} u|_{\boldsymbol{a}+V}$ from (2) and $\deg(u) > \frac{n-1}{2}$ (since $u \neq 0$), which contradicts the fact that $\deg(u) \leq \frac{n-1}{2}$. Hence, $\deg(u) = \frac{n-1}{2}$, thus concluding our proof. ∎

In the proof of Proposition 5 we saw that if $u \in \mathcal{AN}(f+x_{\boldsymbol{a}})$ then $u+x_{\boldsymbol{a}} \in \mathcal{AN}(f)$. In particular, the minimum degree such $u$ is associated with one annihilator $g$ (equal to $u + x_{\boldsymbol{a}}$) of $f$ all terms of which, with degree greater than $\frac{n-1}{2}$, coincide with those in the ANF of $x_{\boldsymbol{a}}$.

A direct result from Proposition 5 and Lemma 1 is the following.

*Corollary 1:* If $\mathsf{AI}_n(f) = \frac{n+1}{2}$ and $n$ odd, then

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}}) = \frac{n-1}{2}, \quad \forall \boldsymbol{a} \in \mathbb{F}_2^n,$$

and the annihilator of degree $\frac{n-1}{2}$ is unique.

Corollary 1 implies that the modification of any entry in the truth table of $f \in \mathbb{B}_n$ with maximum algebraic immunity always results in a function of algebraic immunity decreased by 1. The importance of the above results rests with the fact that the annihilator of either $f + x_{\boldsymbol{a}}$ or $f + x_{\boldsymbol{a}} + 1$ with the minimum degree $\frac{n-1}{2}$ is unique, since it is known that an algebraic attack may be more easily mounted if many (rather than only one) low-degree annihilators are determined [11]. Combining the above, we obtain the following result.

*Proposition 6:* Let $n$ be odd and $f \in \mathbb{B}_n$ be such that $\mathsf{AI}_n(f) = \frac{n+1}{2}$. Then, for any $\boldsymbol{a} \in \mathrm{supp}(f)$ and $\boldsymbol{b} \notin \mathrm{supp}(f)$, the function $h = f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ satisfies $\mathsf{AI}_n(h) \geq \frac{n-1}{2}$.

*Proof:* First note that for $g = f + x_{\boldsymbol{a}}$ and $g' = 1 + f + x_{\boldsymbol{b}}$ we get $g(\boldsymbol{b}) = 0$ and $g'(\boldsymbol{a}) = 0$ respectively, whereas both $g, g'$ have algebraic immunity $\frac{n-1}{2}$ and a unique annihilator of such degree, according to Corollary 1. Then, the claim follows by applying Lemma 1 on $g + x_{\boldsymbol{b}}$ (that is $h$) and $g' + x_{\boldsymbol{a}}$ (that is $h+1$). ∎

Proposition 6 implies that any modification of two entries of the truth table of $f \in \mathbb{B}_n$, with $n$ odd and $\mathsf{AI}_n(f) = \frac{n+1}{2}$, such that the resulting function remains balanced yields a function with algebraic immunity at least $\frac{n-1}{2}$. This result agrees with the heuristic results presented in [6] indicating that the algebraic immunity of a random balanced Boolean function with $n$ variables is at least $\lfloor \frac{n}{2} \rfloor$ with very high probability. Moreover, if a function $f$ obtained via Proposition 6 satisfies $\mathsf{AI}_n(f) = \frac{n-1}{2}$ then there is only one annihilator of $f$ with degree $\frac{n-1}{2}$. The same claim holds for $f+1$.

Although the case of even number of variables $n$ is quite different, some of the above results still hold; this is shown next.

*Proposition 7:* Let $f \in \mathbb{B}_n$, where $n$ is even, having maximum algebraic immunity $\frac{n}{2}$, and let $\boldsymbol{a} \in \mathbb{F}_2^n$ be such that $f(\boldsymbol{a}) = 1$. Then,

$$h = f + x_{\boldsymbol{a}}$$

satisfies $\mathsf{AI}_n(h) \geq \frac{n}{2} - 1$. If $\mathsf{AI}_n(h) = \frac{n}{2} - 1$, then $h$ has a unique annihilator $u$ of degree $\frac{n}{2} - 1$ and $u + x_{\boldsymbol{a}} \in \mathcal{AN}(f)$.

*Proof:* According to Lemma 1, $h+1$ does not have annihilators of degree less that $\frac{n}{2}$. To show that $h$ does not have annihilators of degree less that $\frac{n}{2} - 1$ (and if $u \in \mathcal{AN}(f)$ with $\deg(u) = \frac{n}{2} - 1$ does exist, then it is unique) we simply proceed as in the proof of Proposition 5. ∎

A special case of Proposition 7, imposing restrictions on the weight of $f$, was proved in [23, Theorem 4.2] under a different formulation: if $\mathsf{AI}_n(f) = \frac{n}{2}$ and $\mathrm{wt}(f) = 2^{n-1} + (-1)^{f(\mathbf{0})}\binom{n-1}{n/2}$, then $\mathsf{AI}_n(h) = \frac{n}{2} - 1$; that is, only functions whose weight is at the extreme points of the valid range (any function with algebraic immunity $\frac{n}{2}$ can have) are considered.

*Proposition 8:* Let $n$ be even and $f \in \mathbb{B}_n$ be such that $\mathsf{AI}_n(f) = \frac{n}{2}$. Then, for any $\boldsymbol{a} \in \mathrm{supp}(f)$ and $\boldsymbol{b} \notin \mathrm{supp}(f)$, the function

$$h = f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$$

satisfies $\mathsf{AI}_n(h) \geq \frac{n}{2} - 1$; moreover, if annihilators of either $h$ or $h+1$ exist with degree $\frac{n}{2} - 1$, then they are unique.

*Proof:* Direct consequence of Proposition 7 and Lemma 1 (*see* also the proof of Proposition 6). ∎

Concluding this section, we show that modifications of balanced Boolean functions as those described above may result in functions with the maximum possible algebraic degree.

*Corollary 2:* Let $f \in \mathbb{B}_n$ be balanced. Then it is always possible to choose $\boldsymbol{a} \in \mathrm{supp}(f), \boldsymbol{b} \in \mathrm{supp}(f+1)$ such that $\deg(h) = n - 1$, i.e. the maximum possible, where $h = f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$.

*Proof:* Let $y_i$ denote the monomial $y_i = \prod_{j \neq i} x_j$ of degree $n-1$, and let $\boldsymbol{c} \in \mathbb{F}_2^n$ be the vector whose coordinate $c_i$ is the coefficient of $y_i$ in the ANF of $f$, $i = 1, 2, \ldots, n$. By construction, $\deg(h) \leq n-1$, since $f$ is balanced, and therefore the coefficient of $\prod_i x_i$ in the ANF of $x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ is zero. It is straightforward to show that the coefficient of $y_i$ in the ANF of $x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ is equal to $a_i + b_i$. Therefore, we get $\deg(h) = n-1$ if and only if $\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c}$ is nonzero. ∎

## IV. Proper Modifications of Functions

In this section we derive new techniques for generating functions with maximum algebraic immunity. To achieve this goal, we focus on necessary and sufficient conditions to obtain functions with maximum algebraic immunity via Proposition 6 (for the odd case) or Proposition 8 (for the even case).

First, we introduce a partial ordering of vectors in $\mathbb{F}_2^n$ as follows:

$$\boldsymbol{u} \preceq \boldsymbol{v} \Leftrightarrow \mathrm{supp}(\boldsymbol{u}) \subseteq \mathrm{supp}(\boldsymbol{v}),\ \boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n,$$

and we say that $\boldsymbol{u}$ is *smaller than or equal* to $\boldsymbol{v}$ (equivalently, $\boldsymbol{v}$ is *greater than or equal* to $\boldsymbol{u}$). The strict inequality $\prec$ is defined similarly. Moreover, for any set of vectors $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_m\}$ of $\mathbb{F}_2^n$, we say that $\boldsymbol{v}_i$ is a *maximal* element if and only if there is no $1 \leq j \leq m$ such that $\boldsymbol{v}_i \prec \boldsymbol{v}_j$; a *minimal* element is similarly defined. For any function $f \in \mathbb{B}_n$, we also define the following sets:

$$\min_{\preceq}(f) = \{\boldsymbol{a} \in \mathrm{supp}(f) \colon \boldsymbol{b} \preceq \boldsymbol{a} \Rightarrow \boldsymbol{b} = \boldsymbol{a}\ \forall \boldsymbol{b} \in \mathrm{supp}(f)\},$$
$$\max_{\preceq}(f) = \{\boldsymbol{a} \in \mathrm{supp}(f) \colon \boldsymbol{a} \preceq \boldsymbol{b} \Rightarrow \boldsymbol{b} = \boldsymbol{a}\ \forall \boldsymbol{b} \in \mathrm{supp}(f)\}.$$

Clearly, both $\min_{\preceq}(f)$ and $\max_{\preceq}(f)$ are subsets of $\mathrm{supp}(f)$.

Next, the cases of odd and even number of variables will be treated separately.

### A. The odd case

In order to prove sufficient conditions to ensure maximum algebraic immunity, the following Lemma will be used.

*Lemma 2:* With the notation of Proposition 6, let $g = f + x_{\boldsymbol{a}}$ and $g' = 1 + f + x_{\boldsymbol{b}}$. If $u, u'$ are the unique annihilators of $g, g'$ respectively of degree $\frac{n-1}{2}$, then $u(\boldsymbol{a}) = u'(\boldsymbol{b}) = 1$ and

$$\mathsf{AI}_n(h) = \frac{n+1}{2} \Leftrightarrow u(\boldsymbol{b}) = 1 \text{ or } u'(\boldsymbol{a}) = 1\ .$$

*Proof:* The existence and uniqueness of $u, u'$ with degree $\frac{n-1}{2}$ is ensured by Proposition 5. The fact that $u + x_{\boldsymbol{a}} \in \mathcal{AN}(f)$ (*see* proof of Proposition 5) and $f(\boldsymbol{a}) = 1$ implies $(u + x_{\boldsymbol{a}})(\boldsymbol{a}) = 0$ and eventually $u(\boldsymbol{a}) = 1$ ($u'(\boldsymbol{b}) = 1$ is obtained similarly). From the definition of $g, g', h$ and Lemma 1, we get

$$\mathcal{AN}(h) \subset \mathcal{AN}(g) \quad \text{and} \quad \mathcal{AN}(h+1) \subset \mathcal{AN}(g')\ .$$

To ensure that $u \notin \mathcal{AN}(h)$ and $u' \notin \mathcal{AN}(1+h)$, which immediately yields $\mathsf{AI}_n(h) = \frac{n+1}{2}$ due to the uniqueness of $u, u'$, we need to enforce $u(\boldsymbol{b}) = u'(\boldsymbol{a}) = 1$ (since $h(\boldsymbol{b}) = (1+h)(\boldsymbol{a}) = 1$). However, due to Proposition 4, only one of these conditions suffices to give the desired result. ∎

We next prove that there exist specific functions enabling (in a straightforward manner) the selection of vectors $\boldsymbol{a}, \boldsymbol{b}$ such that all the conditions in Lemma 2 are satisfied.

*Theorem 2:* Let $f \in \mathbb{B}_n$ with $n$ odd and $\mathsf{AI}_n(f) = \frac{n+1}{2}$. Then

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n+1}{2} \quad \forall \boldsymbol{b} \prec \boldsymbol{a}$$

where $\boldsymbol{a} \in \min_{\preceq}(f)$ satisfying $\mathrm{wt}(\boldsymbol{a}) \geq \frac{n+1}{2}$; moreover, if such $\boldsymbol{a}$ does exist, then $\mathrm{wt}(\boldsymbol{a}) = \frac{n+1}{2}$.

*Proof:* Let $k = \mathrm{wt}(\boldsymbol{a})$. Note that $f(\boldsymbol{a}) = 1$, $f(\boldsymbol{b}) = 0$ by hypothesis. Let $E$ be the $k$-dimensional subspace $E = \{\boldsymbol{x} \in \mathbb{F}_2^n : \boldsymbol{x} \preceq \boldsymbol{a}\}$ and $g = f + x_{\boldsymbol{a}}$. It is easily seen that $g|_E = f|_E + x_{\boldsymbol{a}}|_E$ is identically zero (due to the minimality of $\boldsymbol{a}$, the function $f|_E$ has weight 1 with $f|_E(\boldsymbol{a}) = 1$). Thus, the indicator of $E$ is a function of degree $n - k < \frac{n+1}{2}$ given by

$$u = \vartheta|_E = \prod_{i \notin \mathrm{supp}(\boldsymbol{a})} (x_i + 1) \Leftrightarrow u(x) = \sum_{\boldsymbol{b} \preceq \boldsymbol{a}} x_{\boldsymbol{b}}$$

that annihilates $g$. Hence, Corollary 1 implies that $\deg(u) = \frac{n-1}{2}$ (and, thus, $k = \frac{n+1}{2}$) and, moreover, $u$ is the unique function with the above properties. Our proof is concluded by noting that $u$ satisfies the conditions of Lemma 2; indeed, $u(\boldsymbol{b}) = 1\ \forall \boldsymbol{b} \prec \boldsymbol{a}$. Thus, according to Lemma 2, $\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n+1}{2}$. ∎

As a result of the above, starting from a given function with maximum algebraic immunity and applying Theorem 2, we may construct a (possibly large) number of functions with maximum algebraic immunity.

The following result is proved along the same lines.

*Theorem 3:* Let $f \in \mathbb{B}_n$ with $n$ odd and $\mathsf{AI}_n(f) = \frac{n+1}{2}$. Then

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n+1}{2} \quad \forall\ \boldsymbol{b} \succ \boldsymbol{a}$$

where $\boldsymbol{a} \in \max_{\preceq}(f)$ satisfying $\mathrm{wt}(\boldsymbol{a}) \leq \frac{n-1}{2}$; moreover, if such $\boldsymbol{a}$ does exist, then $\mathrm{wt}(\boldsymbol{a}) = \frac{n-1}{2}$.

The above two Theorems, in conjunction with Proposition 4, lead to the following result which forms the basis for our proposed construction method.

*Corollary 3:* Let $f \in \mathbb{B}_n$ with $n$ odd and $\mathsf{AI}_n(f) = \frac{n+1}{2}$. If $\boldsymbol{a} \in \mathrm{supp}(f)$, $\boldsymbol{b} \in \mathrm{supp}(1+f)$, with $\boldsymbol{b} \prec \boldsymbol{a}$, satisfy one of

i) $\boldsymbol{a} \in \min_{\preceq}(f)$ and $\mathrm{wt}(\boldsymbol{a}) \geq \frac{n+1}{2}$;
ii) $\boldsymbol{b} \in \max_{\preceq}(1+f)$ and $\mathrm{wt}(\boldsymbol{b}) \leq \frac{n-1}{2}$;

then $f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ has maximum algebraic immunity $\frac{n+1}{2}$.

The above can be applied to known constructions of Boolean functions of maximum algebraic immunity, thus generalizing them and leading to new functions.

*Example 1:* Let $f \in \mathbb{B}_5$ be constructed via Proposition 2, where $\alpha$ is a root of the primitive polynomial $p(x) = x^5 + x^2 + 1$ over $\mathbb{F}_2$. It can be verified that $\boldsymbol{a} = (1\,0\,1\,0\,1)$ is a minimal element of $\mathrm{supp}(1+f)$. Thus, Theorem 2 implies that swapping $\boldsymbol{a}$ with any element $\boldsymbol{b} \prec \boldsymbol{a}$ lying in $\mathrm{supp}(f)$ results in another function with maximum algebraic immunity; namely, since the element of $\mathbb{F}_{2^n}$ with 5-tuple representation $(1\,0\,1\,0\,1)$ is $\alpha^{22}$, we get that any function of the form

$$\mathrm{supp}(f) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}, \alpha^{22}\} \setminus \{s\}$$

where $s \in \{0, 1, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^{10}\}$, has maximum algebraic immunity 3.

We next prove, similarly to the previous analysis, another swapping between $\mathrm{supp}(f)$ and $\mathrm{supp}(f+1)$ which also results in functions with maximum algebraic immunity; this is -

somehow - the inverse swapping of those given in Theorems 2 and 3 and may apply to functions that do not have the properties described in Theorems 2, 3.

*Theorem 4:* Let $f \in \mathbb{B}_n$ with $n$ odd and $\mathsf{AI}_n(f) = \frac{n+1}{2}$. Let us suppose that there exists $\boldsymbol{a} \in \mathrm{supp}(f+1)$ such that

- $\mathrm{wt}(\boldsymbol{a}) \geq \frac{n+1}{2}$,
- all the smaller than $\boldsymbol{a}$ vectors with degree less than $\frac{n+1}{2}$, apart from a vector $\boldsymbol{b}$, also lie in $\mathrm{supp}(f+1)$.

Then,

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n+1}{2}$$

*Proof:* Due to Proposition 5, there exists an annihilator $u$ of $f + x_{\boldsymbol{a}} + 1$ with degree $\frac{n-1}{2}$ (and, due to Lemma 1, the function $f + x_{\boldsymbol{a}}$ does not have nonzero annihilator of degree less than $\frac{n+1}{2}$). Note also that, as it is shown in the proof of Proposition 5, $u(\boldsymbol{a}) = 1$. Moreover, since $(f + x_{\boldsymbol{a}} + 1)(\boldsymbol{w}) = 1$ for all $\boldsymbol{w} \neq \boldsymbol{b}$ such that $\boldsymbol{w} \prec \boldsymbol{a}$, we get that for each such $\boldsymbol{w}$ it holds $u(\boldsymbol{w}) = 0$. Hence, since $u(\boldsymbol{a}) = 1$ and $\deg(u) < \frac{n+1}{2}$, we necessarily get that $u(\boldsymbol{b}) = 1$. The claim follows from Lemma 2. ∎

*Example 2:* Let us consider the following function of maximum algebraic immunity, that can be obtained by the method proposed in [25, Construction 2]:

$$\mathrm{supp}(f) = \{\alpha^{15}, \alpha^{16}, \ldots, \alpha^{30}\} \setminus \{\alpha^{18}\} \cup \{\alpha^{3}\}$$

It can be verified that the element $\alpha^{11} \in \mathrm{supp}(f+1)$, with 5-tuple representation $(1\ 1\ 1\ 0\ 0)$, satisfies the conditions imposed in Theorem 4 (for $\boldsymbol{a} = \alpha^{11}$ and $\boldsymbol{b} = \alpha^{19}$) and, thus, swapping $\alpha^{11}$ with $\alpha^{19} \in \mathrm{supp}(f)$ (with 5-tuple representation $(0\ 1\ 1\ 0\ 0)$) results in another function with also maximum algebraic immunity (this swapping can not be obtained by using the method described in [25]).

In addition, the element $\alpha^{22}$ (with 5-tuple representation $(1\ 0\ 1\ 0\ 1)$) is a minimal element of $\mathrm{supp}(f)$ and, thus, Theorem 2 can be also applied; consequently, we finally get that any function of the form

$$\mathrm{supp}(h) = \mathrm{supp}(f) \setminus \{\alpha^{19}, \alpha^{22}\} \cup \{\alpha^{11}, s\}$$

where $s \in \{0, 1, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^{10}\}$, has maximum algebraic immunity 3.

Note that functions of the highest possible algebraic degree (i.e. $n-1$) can be generated by a proper (each time) selection of the vectors $\boldsymbol{a}, \boldsymbol{b}$ such as to ensure that the condition implied in the proof of Corollary 2 holds. Other cryptographic criteria though, such as nonlinearity, are contingent (apart from the choice of $\boldsymbol{a}, \boldsymbol{b}$) on the properties of the functions that are used as a starting point.

*1) Construction of an iterative algorithm:* Using as a starting point the majority function $f \in \mathbb{B}_n$, Corollary 3 directly results in the development of an iterative algorithm (*see* Alg. 1) that constructs new functions of maximum algebraic immunity. In each step, the algorithm implements the procedure described by Corollary 3 and appropriately swaps elements between the supports of $f$ and $f+1$ to obtain a new function with maximum algebraic immunity. The algorithm outputs a set of Boolean functions $\{f_i\}_{i \geq 1}$, where $f_i$ is obtained at the $i$-th step (line 9 of Alg. 1). An important remark is that functions obtained via Alg. 1 can be efficiently implemented since the ANF of the majority function (our starting point) is easily computed due to its symmetric structure.

**Algorithm 1** Generate Functions of Maximum AI

**input:** odd $n$, majority function $f \in \mathbb{B}_n$
**initialization:** $i \leftarrow 0, f_0 \leftarrow f$

1: $S \leftarrow \mathrm{supp}(f)$ ⫽ vectors of weight $\geq \lceil \frac{n}{2} \rceil$
2: $S' \leftarrow \mathrm{supp}(1+f)$ ⫽ vectors of weight $\leq \lfloor \frac{n}{2} \rfloor$
3: $T \leftarrow \min_{\preceq}(f)$ ⫽ vectors of weight $= \lceil \frac{n}{2} \rceil$
4: $T' \leftarrow \max_{\preceq}(1+f)$ ⫽ vectors of weight $= \lfloor \frac{n}{2} \rfloor$
5: **while** $(T \neq \emptyset) \vee (T' \neq \emptyset)$ **do**
6: $i \leftarrow i + 1$
7: $(\boldsymbol{a}_i, \boldsymbol{b}_i) \in \{S \times S' : \boldsymbol{a}_i \in T \ \vee \boldsymbol{b}_i \in T'\}$ ⫽ choose randomly
8: $f_i \leftarrow f_{i-1} + x_{\boldsymbol{a}_i} + x_{\boldsymbol{b}_i}$ ⫽ swap $\boldsymbol{a}_i, \boldsymbol{b}_i$
9: $S \leftarrow S \setminus \{\boldsymbol{a}_i\}$
10: $S' \leftarrow S' \setminus \{\boldsymbol{b}_i\}$
11: $T \leftarrow T \setminus \{\boldsymbol{v} \in T : \boldsymbol{v} \succ \boldsymbol{b}_i\}$
12: $T' \leftarrow T' \setminus \{\boldsymbol{u} \in T' : \boldsymbol{u} \prec \boldsymbol{a}_i\}$
13: **end**

**output:** functions $\{f_i\}_{i \geq 1} : \mathsf{AI}_n(f_i) = \lceil \frac{n}{2} \rceil$

We further analyze Alg. 1 next. Let us assume that, at step $i$, $f_i$ is obtained from $f_{i-1}$ by swapping $\boldsymbol{a}_i \in \mathrm{supp}(f_{i-1})$ and $\boldsymbol{b}_i \in \mathrm{supp}(f_{i-1}+1)$; then it is easy to see that $\boldsymbol{a}_i$ is necessarily a maximal element of $\mathrm{supp}(1+f_i)$ and $\boldsymbol{b}_i$ is necessarily a minimal element of $\mathrm{supp}(f_i)$. In order to examine whether the vectors $\boldsymbol{a}_i$ or $\boldsymbol{b}_i$ could also be used at step $i+1$, we distinguish between the following cases:

*Case 1:* $\boldsymbol{a}_i \in \min_{\preceq}(f_{i-1})$. Hence, at the beginning of the $i$-th step, $\boldsymbol{a}_i \in T$ (and $f_{i-1}(\boldsymbol{a}_i) = 1$), whereas $f_i(\boldsymbol{a}_i) = 0$ following the execution of line 9. Suppose we want to use $\boldsymbol{a}_i$ at step $i+1$ to obtain a new function. This can be done by

i) applying Theorem 2 on $f_i$; a vector $\boldsymbol{a} \in T$ such that $\boldsymbol{a}_i \prec \boldsymbol{a}$ would be needed (not true, as $\mathrm{wt}(\boldsymbol{a}_i) = \mathrm{wt}(\boldsymbol{a})$),
ii) applying Theorem 3 on $1 + f_i$; then $\boldsymbol{a}_i$ would have to satisfy $\mathrm{wt}(\boldsymbol{a}_i) < \frac{n+1}{2}$ (not true).

*Case 2:* $\boldsymbol{b}_i \in \max_{\preceq}(1+f_{i-1})$. Hence, at the beginning of the $i$-th step, $\boldsymbol{b}_i \in T'$ (and $f_{i-1}(\boldsymbol{b}_i) = 0$), whereas $f_i(\boldsymbol{b}_i) = 1$ following the execution of line 9. Likewise, suppose we want to use $\boldsymbol{b}_i$ at step $i+1$; this can be done by

i) applying Theorem 2 on $f_i$; then $\boldsymbol{b}_i$ would have to satisfy $\mathrm{wt}(\boldsymbol{b}_i) \geq \frac{n+1}{2}$ (not true),
ii) applying Theorem 3 on $1+f_i$; a vector $\boldsymbol{a} \in T'$ such that $\boldsymbol{b}_i \succ \boldsymbol{a}$ would be needed (not true, as $\mathrm{wt}(\boldsymbol{b}_i) = \mathrm{wt}(\boldsymbol{a})$).

Thus, neither $\boldsymbol{a}_i$ nor $\boldsymbol{b}_i$ can be used at step $i+1$. It is also easy to see that $\boldsymbol{a}_i$ and $\boldsymbol{b}_i$ can not be used in any subsequent swapping and, therefore, they can be excluded from the remaining steps; this is reflected in lines 10–11 of Alg. 1. Furthermore, since $\boldsymbol{a}_i \in \max_{\preceq}(1+f_i)$, all elements smaller than $\boldsymbol{a}_i$ in $\mathrm{supp}(1+f_i)$ can not be used by Theorem 3 and are removed from $T'$; similar arguments also hold for $\boldsymbol{b}_i$ and $T$ (*see* lines 12–13 of Alg. 1).

Finally, note that if $\boldsymbol{a}_i \in T$ at the beginning of the $i$-th step of the algorithm, then all $\boldsymbol{u} \prec \boldsymbol{a}_i$ are lying in $S'$ (*see* line 12 of Alg. 1); likewise, all $\boldsymbol{v} \succ \boldsymbol{b}_i$ belong to $S$ if $\boldsymbol{b}_i \in T'$ (*see* line 13 of Alg. 1). Consequently, if at least one of $T, T'$ is non–empty, then there always exists a pair $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ satisfying the conditions of Corollary 3.

TABLE I
GENERATION OF FUNCTIONS $f_i \in \mathbb{B}_5 : \mathsf{AI}_n(f_i) = 3,\ 1 \le i \le 5$

| $i$ | $\boldsymbol{a}_i$ | $\boldsymbol{b}_i$ | removed from $T$ | removed from $T'$ | $\deg(f_i)$ | $\mathsf{nl}(f_i)$ |
|---|---|---|---|---|---|---|
| 0 | | | | | 4 | 10 |
| 1 | 00111 | 00011 | 00111, 01011, 10011 | 00110, 00101, 00011 | 4 | 10 |
| 2 | 11001 | 00001 | 01101, 10101, 11001 | 11000, 10001, 01001 | 4 | 10 |
| 3 | 10111 | 10100 | 10110, 11100 | 10100, 10010 | 3 | 12 |
| 4 | 01110 | 00110 | 01110 | 01100, 01010 | 4 | 10 |
| 5 | 11010 | 10000 | 11010 | – | 4 | 10 |

*Example 3:* For $n = 5$, the constructions of Proposition 1,2 have degree 4 and nonlinearity 10 (whereas their algebraic immunity is the maximum possible, that is 3). Starting with $n = 5$ and the majority function $f \in \mathbb{B}_5$ (Proposition 1), the initialization process of Alg. 1 gives $i = 0, f_0 = f$ and

$$\begin{aligned} T = \{&00111,01011,01101,01110,10011,\\ &10101,10110,11001,11010,11100\}\\ T' = \{&00011,00101,00110,01001,01010,\\ &01100,10001,10010,10100,11000\} \end{aligned}$$

whereas $S, S'$ are defined accordingly.

A summary information of Alg. 1 execution is presented in Table I, along with the algebraic degree and nonlinearity of each function. At the $i$-th step, a pair $(\boldsymbol{a}_i, \boldsymbol{b}_i)$ satisfying the conditions of Corollary 3 is chosen, and a new function with $\mathsf{AI}_n(f_i) = \lceil \frac{5}{2} \rceil = 3$ is computed according to line 9. At the end of Alg. 1, both $T, T'$ are empty.

Note that the functions obtained by Alg. 1 do not necessarily have the same algebraic degree or nonlinearity. Hence the proposed construction is quite general, since the derived functions are not necessarily pairwise affine equivalent.

It should be stressed that modifying the majority functions with odd number of variables was also studied in [7] (*see* Construction 2), but the functions constructed therein do not cover the whole space of functions obtained by Alg. 1. Moreover, it should be also pointed out that Alg. 1 provides all the rotation symmetric Boolean functions of maximum algebraic immunity constructed by the method described in [22, Construction 1].

*Proposition 9:* Let $M_n$ be the number of all functions with algebraic immunity $\frac{n+1}{2}$ obtained by Alg. 1. Then,

$$M_n > \binom{n}{\frac{n+1}{2}} \left( 2^{\frac{n+1}{2}+1} - 2 - \frac{n+1}{2} \right)$$

*Proof:* Let $k = \frac{n+1}{2}$. The initial sets $T, T'$ in Alg. 1 consist of $\binom{n}{k}$ elements. Each vector in $T$ (*resp.* $T'$) has $2^k - 1$ candidate vectors in $S'$ (*resp.* $S$) that can be used to get a new function. Thus, the number of valid swaps at the first step is

$$2\binom{n}{k}\left(2^k - 1\right) - \binom{n}{k}k = \binom{n}{k}\left(2^{k+1} - 2 - k\right)$$

where $\binom{n}{k}k$ is the number of swaps with exactly one element from $T$ and $T'$. ∎

Experimental results for larger values of $n$ show that the functions constructed via Alg. 1 may achieve nonlinearity greater than the nonlinearity of the majority function, which is equal to $2^{n-1} - \binom{n-1}{\lfloor n/2 \rfloor}$ [13]; an upper bound though on the maximum nonlinearity that can be attained still remains to be proved. However, let us recall that the functions derived in [7, Construction 2] constitute a proper subset of those obtained via Alg. 1. It is proved in [7] that the nonlinearity of functions constructed therein is $2^{n-1} - \binom{n-1}{\lfloor n/2 \rfloor} + \Delta(n)$, where $\Delta(n)$ is a function increasing rapidly with $n$; hence, such nonlinearities are also achievable by Alg. 1.

### *B. The even case*

We subsequently prove that specific swaps between $\mathrm{supp}(f)$ and $\mathrm{supp}(f+1)$ for a function $f$ with even number of variables, similar to the swaps described previously for the odd case, suffice to ensure maximum algebraic immunity.

*Theorem 5:* Let $f \in \mathbb{B}_n$ with $n$ even and $\mathsf{AI}_n(f) = \frac{n}{2}$. Suppose there exists $\boldsymbol{a} \in \min_{\preceq}(f)$ such that $\mathrm{wt}(\boldsymbol{a}) \ge \frac{n}{2}$ and $\mathsf{AI}_n(f + x_{\boldsymbol{a}}) = \frac{n}{2}$. Then

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n}{2} \quad \forall\ \boldsymbol{b} \prec \boldsymbol{a}.$$

*Proof:* First note that $f(\boldsymbol{a}) = 1$, $f(\boldsymbol{b}) = 0$ by hypothesis. Moreover, the function $f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ does not have annihilator of degree less than $\frac{n}{2}$ due to Lemma 1. Suppose there exists $u \in \mathcal{AN}(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}} + 1)$ with $\deg(u) < \frac{n}{2}$. Then it necessarily holds $u(\boldsymbol{b}) = 1$ (since, otherwise, $u$ would also be annihilator of $f + x_{\boldsymbol{a}} + 1$, resulting in $\deg(u) \ge \frac{n}{2}$). Moreover, it holds $u(\boldsymbol{v}) = 0\ \forall \boldsymbol{v} \preceq \boldsymbol{a}$ (and $\boldsymbol{v} \ne \boldsymbol{b}$) , since $(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}} + 1)(\boldsymbol{v}) = 1$ by hypothesis (recall that $\boldsymbol{a} \in \min_{\preceq}(f)$). Consequently, considering the ANF of $u$ described in (1), we have that $c_{\boldsymbol{v}} = \sum_{\mu \preceq \boldsymbol{v}} u(\mu)$ and, thus, $c_{\boldsymbol{a}} = 1$, contradicting the fact that $\deg(u) < \frac{n}{2}$; hence, we finally get that $\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n}{2}$. ∎

*Theorem 6:* Let $f \in \mathbb{B}_n$ with $n$ even and $\mathsf{AI}_n(f) = \frac{n}{2}$. Suppose there exists $\boldsymbol{a} \in \max_{\preceq}(f)$ such that $\mathrm{wt}(\boldsymbol{a}) \le \frac{n}{2}$ and $\mathsf{AI}_n(f + x_{\boldsymbol{a}}) = \frac{n}{2}$. Then

$$\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n}{2} \quad \forall\ \boldsymbol{b} \succ \boldsymbol{a}, \mathrm{wt}(\boldsymbol{b}) \ge \frac{n}{2}.$$

*Proof:* Note that $f(\boldsymbol{a}) = 1$, $f(\boldsymbol{b}) = 0$ by hypothesis. Moreover, the function $f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ does not have annihilator of degree less than $\frac{n}{2}$ due to Lemma 1. Working as in Theorem 5, we derive that if there exists $u \in \mathcal{AN}(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}} + 1)$ with $\deg(u) < \frac{n}{2}$, then it holds $u(\boldsymbol{b}) = 1$. Moreover, it holds $u(\boldsymbol{v}) = 0\ \forall \boldsymbol{v} \succeq \boldsymbol{a}$ (and $\boldsymbol{v} \ne \boldsymbol{b}$), since $(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}} + 1)(\boldsymbol{v}) = 1$ by hypothesis (recall that $\boldsymbol{a} \in \max_{\preceq}(f)$). Let us set $u'(x) = u(\overline{x})$ (where it holds $\deg(u) = \deg(u')$). Then $u'(\boldsymbol{v}) = 0\ \forall \boldsymbol{v} \preceq \overline{\boldsymbol{a}}$ (and $\boldsymbol{v} \ne \overline{\boldsymbol{b}}$), whereas $u'(\overline{\boldsymbol{b}}) = 1$ (note that $\overline{\boldsymbol{b}} \prec \overline{\boldsymbol{a}}$). Hence, the claim follows by using the same arguments as those used in Theorem 5. ∎

Clearly, Theorems 5 and 6, which refer to functions of even number of variables, resemble Theorems 2 and 3 respectively (that were proved for the odd case).

*1) Construction of an iterative algorithm:* As in the odd case, the majority function can be also used as a starting point to construct new functions of maximum algebraic immunity via Theorems 5 and 6. Note that the majority function $f \in \mathbb{B}_n$, $n$ even, satisfies $\mathsf{AI}_n(f + x_{\boldsymbol{a}}) = \frac{n}{2}\ \forall \boldsymbol{a} \in \mathbb{F}_2^n$ with $\mathrm{wt}(\boldsymbol{a}) = \frac{n}{2}$ [13]. Hence, by recursively applying Theorems 5 and 6 for proper choices of vectors, we again obtain Alg. 1; hence, this algorithm is independent from the parity on $n$ (and, if $n$ is

even, the input majority function $f$ may have arbitrary value at any $\boldsymbol{a} \in \mathbb{F}_2^n$ with $\mathrm{wt}(\boldsymbol{a}) = \frac{n}{2}$).

It should be pointed out that if Alg. 1 is restricted to the even case, then it coincides with the construction given in [7, Construction 1] which appropriately modifies the majority function with even number of variables (the nonlinearities of some classes of functions obtained via this construction are also discussed therein); however, note that Theorems 5 and 6 are more general and can be possibly applied to other functions.

## V. Further constructions of functions with maximum algebraic immunity

In this section we further elaborate the analysis given in [21], [25] to provide new functions in odd number of variables of maximum algebraic immunity. Again, our analysis is based on proper modifications of functions with maximum algebraic immunity; in the subsequent analysis though, each element in the support of a function $f \in \mathbb{B}_n$ is represented as a power of a primitive element over $\mathbb{F}_{2^n}$ (and not as a vector over $\mathbb{F}_2^n$).

First note that, given a balanced function $f$ in odd number of variables $n$, the sub-matrix $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ given in Section II is square and, due to Theorem 1, $\mathsf{AI}_n(f) = \frac{n+1}{2}$ if and only if it has full rank. Hence, for odd $n$, the function $f$ with

$$\mathrm{supp}(f) = \{1,\ \alpha,\ \ldots,\ \alpha^{2^{n-1}-1}\}$$

has maximum algebraic immunity; in this case, the matrix $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ is upper-triangular. More precisely, this function is explicitly constructed in [21] (*see* Proposition 3, where, for odd $n$, we have $d_n = 2^{n-1}$). Similarly, the function $h$ with

$$\mathrm{supp}(h) = (\alpha^{2^{n-1}-1}\ \alpha^{2^{n-1}}\ \ldots\ \alpha^{2^n-2})$$

has also maximum algebraic immunity; in this case, the matrix $\boldsymbol{R}^{1_h}_{\frac{n+1}{2},n-1}$ is lower-triangular.

More recently, Zeng *et al.* in [25, Construction 1] proved that the aforementioned $f$ can be properly modified by swapping $\alpha^i \in \mathrm{supp}(f)$ and $\alpha^j \in \mathrm{supp}(f+1)$ such that the corresponding matrix $\boldsymbol{R}^{1_{f'}}_{\frac{n+1}{2},n-1}$ of the new function $f'$ remains upper-triangular; similarly, the function $h$ can be appropriately modified such us to ensure that the resulting $\boldsymbol{R}^{1_{h'}}_{\frac{n+1}{2},n-1}$ matrix is lower-triangular (*see* [25, Construction 2]).

Before we recall the above constructions, we shall first introduce some notation; since there is a direct association between the non-zero elements of $\mathbb{F}_{2^n}$ and the columns of $\boldsymbol{R}_{\frac{n+1}{2},n-1}$, we write the $m$-th column of $\boldsymbol{R}_{\frac{n+1}{2},n-1}$ as $\boldsymbol{v}^m = (\boldsymbol{v}_0^m, \boldsymbol{v}_1^m, \ldots, \boldsymbol{v}_{2^{n-1}-1}^m)^T$, that is:

$$\boldsymbol{v}^m = \begin{cases} (r_m\ r_{m-1}\ \ldots r_0\ 0 \ldots 0)^T,\ 0 \le m \le 2^{n-1}-1 \\ (0 \ldots\ 0\ r_E\ r_{E-1} \ldots r_{m-E})^T,\ 2^{n-1} \le m \le 2^n - 2 \end{cases}$$

where the elements $r_i$, $i = 0, \ldots, E$, are determined by (3) and $E = 2^{n-1} - 1$.

The constructions of [25] can be described as follows.

*Proposition 10:* Let us consider the following sets:

$$W \subset \{0, 1, \ldots, 2^{n-1}-1\}$$
$$Y \subset \{2^{n-1}, \ldots, 2^n - 2\}$$
$$\hat{W} \subset \{2^{n-1}-1, \ldots, 2^n - 2\}$$
$$\hat{Y} \subset \{0, 1, \ldots, 2^{n-1}-2\}$$

with $|W| = |Y|$ and $\left|\hat{W}\right| = \left|\hat{Y}\right|$, satisfying the following:

1) For each $w \in W$ there exists unique $y \in Y$ such that for an integer $i$ it holds
$$\boldsymbol{v}_i^w = \boldsymbol{v}_i^y = 1,$$
$$\boldsymbol{v}_{i+\ell}^w = \boldsymbol{v}_{i+\ell}^y = 0\ \forall\ 1 \le \ell \le 2^{n-1} - 1 - i.$$
2) For each $\hat{w} \in \hat{W}$ there exists unique $\hat{y} \in \hat{Y}$ such that for an integer $j$ it holds
$$\boldsymbol{v}_j^{\hat{w}} = \boldsymbol{v}_j^{\hat{y}} = 1,$$
$$\boldsymbol{v}_{j-\ell}^{\hat{w}} = \boldsymbol{v}_{j-\ell}^{\hat{y}} = 0\ \forall\ 1 \le \ell \le j.$$

Then both the functions $f_1, f_2 \in \mathbb{B}_n$, $n$ odd, with

$$\mathrm{supp}(f_1) = \{\alpha^i | i \in (\{0, 1, \ldots, 2^{n-1}-1\} \setminus W) \cup Y\}$$
$$\mathrm{supp}(f_2) = \{\alpha^i | i \in (\{2^{n-1}-1, \ldots, 2^n - 2\} \setminus \hat{W}) \cup \hat{Y}\}$$

have maximum algebraic immunity $\frac{n+1}{2}$.

Next we will further generalize the above constructions, by proving proper modifications of these functions to guarantee maximum algebraic immunity. To achieve this goal, we prove the following result which characterizes the annihilator $u \in \mathcal{AN}(f + x_{\boldsymbol{a}})$ described in Corollary 1.

*Theorem 7:* Let $f \in \mathbb{B}_n$, $n$ odd, with $\mathsf{AI}_n(f) = \frac{n+1}{2}$ and $\mathrm{supp}(f) = (\alpha^{i_1}\ \alpha^{i_2} \ldots\ \alpha^{i_{2^{n-1}}})$. Let also $u$ be the unique annihilator of $f + 1 + x_{\alpha^m}$, where $\alpha^m \in \mathrm{supp}(f+1)$, with degree $\frac{n-1}{2}$. Then it holds $u(\alpha^{i_k}) = 1$, $1 \le k \le 2^{n-1}$, if and only if the solution $\boldsymbol{z}$ of the linear system

$$\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1} \boldsymbol{z}^T = \boldsymbol{v}^m \tag{6}$$

satisfies $\boldsymbol{z}_j = 1$, where $j$ is such that the $j$-th column of $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ is $\boldsymbol{v}^{i_k}$.

*Proof:* First note that (6) has a unique solution, since $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ is of full rank. Hence, if $\mathrm{supp}(\boldsymbol{z}) = (j_1\ j_2\ \ldots j_q)$, then we get that the sum of the $j_1$-th, ..., $j_q$-th columns of $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ give rise to $\boldsymbol{v}^m$ (and this is the only linear combination of columns of $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ having this property). Therefore, replacing any of these $q$ columns in $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ with $\boldsymbol{v}^m$, we get another matrix having also full rank (and, clearly, changing any other column of $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ with $\boldsymbol{v}^m$ would not lead to a full-rank matrix). The claim follows by recalling the properties of the function $u$ described in Lemma 2. ∎

From the above we directly conclude that, for any given function $f$ with maximum algebraic immunity, a pair of vectors $\boldsymbol{a} \in \mathrm{supp}(f)$ and $\boldsymbol{b} \in \mathrm{supp}(f+1)$ such that $\mathsf{AI}_n(f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}) = \frac{n+1}{2}$ can be found (even for fixed $\boldsymbol{a}$ or $\boldsymbol{b}$) by solving a linear system of the form of (6). However, since the dimension of the system is $2^{n-1}$, we get that the overall computational complexity of solving such a system is

**Algorithm 2** Generate Functions of Maximum AI

**input:** odd $n$, $f \in \mathbb{B}_n$ constructed via [21] or [25]
**input:** $\text{supp}(f) = \{\alpha^{j_0}, \ldots, \alpha^{j_{2^{n-1}-1}}\}$, $\alpha^m \notin \text{supp}(f)$
**initialization:** $S \leftarrow \{\}$
1: $\boldsymbol{z} \leftarrow \boldsymbol{0}$ ⫽ all-zero vector of length $2^{n-1}$
2: $i \leftarrow 2^{n-1} - 1$
3: **while** $(i \geq 0)$ **do**
4: $\quad \boldsymbol{z}_i \leftarrow \boldsymbol{v}_i^m$
5: $\quad$ **if** $i \neq 2^{n-1} - 1$ **then**
6: $\quad\quad$ **for** $r = (i+1) \rightarrow 2^{n-1} - 1$ **do**
7: $\quad\quad\quad \boldsymbol{z}_i \leftarrow \boldsymbol{z}_i + \boldsymbol{v}_i^{j_r} * \boldsymbol{z}_r$
8: $\quad\quad$ **end for**
9: $\quad$ **end if**
10: $\quad$ **if** $\boldsymbol{z}_i = 1$ **then**
11: $\quad\quad S \leftarrow S \cup \alpha^{j_i}$
12: $\quad$ **end if**
13: $\quad i \leftarrow i - 1$
14: **end**
**output:** $f_{j_r} \leftarrow f + x_{\alpha^m} + x_{\alpha^{j_r}}$, $\alpha^{j_r} \in S$

$O(2^{3n})$ [10] and, thus, this approach is feasible only for very small values of $n$.

*Remark 1:* It is proved in [14] that a Boolean function with maximum algebraic immunity can be computed by identifying an invertible submatrix of a given $2^{n-1} \times 2^{n-1}$ matrix, whereas the construction in [15] also nessecitates the computation of an inverse matrix of dimension $2^{n-1}$. Hence, the above observation regarding the matrix $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ (which is not considered in [14], [15]) lies in the same context.

The above situation though is greatly simplified by considering the constuctions in [21], [25]. For the functions obtained therein, the matrix $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ is upper-triangular (or lower-triangular); hence, the corresponding linear system can be efficiently solved by a *backward substitution* (or *forward substitution* respectively) approach (*see* e.g. [10]), thus reducing the overall computational complexity to $O(2^{2n})$. Moreover, it should be stressed that, towards constructing new functions of maximum algebraic immunity, we do not necessarily need to fully solve the linear system (6); we simply need to find out a non-zero entry of $\boldsymbol{z}$, as Theorem 7 implies.

The aforementioned procedure is illustrated in Alg. 2. In order to simplify our analysis, we assume that the matrix $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}$ is upper-triangular (the case of lower-triangular matrix can be similarly treated). Alg. 2 implements the backward substitution procedure, to solve the linear system $\boldsymbol{R}^{1_f}_{\frac{n+1}{2},n-1}\boldsymbol{z}^T = \boldsymbol{v}^m$, whereas the support of $\boldsymbol{z}$ constitute the output of the algorithm (elements of the set $S$), indicating the candidates elements from $\text{supp}(f)$ for swapping with $\alpha^m \in \text{supp}(f+1)$.

Alg. 2 proceeds by fully solving the corresponding linear system (that is it computes *all* the possible candidate elements for swapping). Recalling the above discussion though, it should be pointed out that this full execution is not necessary; we may stop whenever at least one entry $\boldsymbol{z}_j$ is found such that $\boldsymbol{z}_j = 1$. Hence, if the outer *while* loop (Line 3) is executed only $k$ times (where $k$ may be significantly smaller than $2^{n-1}$), then the computational complexity of the algorithm is $O(k^2)$.

Similarly to Corollary 2, we next show that the maximum possible algebraic degree (i.e. $n-1$) can be always attained via modifications as those describe above; the following result has been proved in [25, Proposition 1] for the special case of the modifications described in Proposition 10 but, as it can be readily verified, it also holds for our more general modifications.

*Corollary 4:* Let $f \in \mathbb{B}_n$, $n$ odd, constructed via either the methods of [21] or [25]. Then, for any $\boldsymbol{a} \in \text{supp}(f)$, $\boldsymbol{b} \in \text{supp}(f+1)$, the balanced function $h = f + x_{\boldsymbol{a}} + x_{\boldsymbol{b}}$ satisfies $\deg(h) = n-1$ if and only if $\sum_{\boldsymbol{c} \in \text{supp}(h)} h(\boldsymbol{c}) \neq 0$.

Finally, note that the nonlinearity of functions constructed in [21], [25] is expected to be - in general - high (*see* [25, Theorem 2], where a specific family of the derived functions is examined); hence, our approach may also lead to functions of high nonlinearity (clearly, at the worst case, the nonlinearity of functions obtained via Alg. 2 is decreased only by 2 compared to the nonlinearity of the input functions). However, there is still room for further research.

### A. The special case of the function constructed in [21]

Next we confine ourserlves to the function $f$ constructed in [21] (that is $\text{supp}(f) = \{1,\ \alpha,\ \ldots,\ \alpha^{2^{n-1}-1}\}$). In this case, the following result further facilitates the analysis.

*Proposition 11:* Let $0 \leq i_0 < i_1 < \ldots < i_j < 2^{n-1} - 1$ be such that

$$\sum_{k=0}^{j} \boldsymbol{v}^{i_k} = \boldsymbol{v}^m,$$

where $m$ satisfies $2^{n-1} < m < 2^n - 2$, then

$$\sum_{k=0}^{j} \boldsymbol{v}^{i_k+1} = \boldsymbol{v}^{m+1}.$$

*Proof:* Since the matrix $\boldsymbol{R}_{\frac{n+1}{2},n-1}$ is circulant of full rank, it generates a $(N,k)$ cyclic code $\mathcal{C}$, where $N = 2^n - 1$ and $k = 2^{n-1}$. Equivalently, $\boldsymbol{R}_{\frac{n+1}{2},n-1}$ may be considered as a parity-check matrix of the $(N, k-1)$ dual code $\mathcal{C}^{\perp}$ which is also cyclic. Hence, our hypothesis implies that the vector $\boldsymbol{a} = (a_0\ a_1\ \ldots a_{2^n-1})$ satisfying

$$a_i = \begin{cases} 1, \text{ if } i \in \{i_0, \ldots, i_j, m\} \\ 0, \text{ elsewhere} \end{cases}$$

is a codeword of $\mathcal{C}^{\perp}$, since $\boldsymbol{a}\boldsymbol{R}^T_{\frac{n+1}{2},n-1} = \boldsymbol{0}$. Hence, the shifted vector $\boldsymbol{a}' = (a_{2^n-1}\ a_0\ a_1\ \ldots\ a_{2^n-1})$ is also a codeword of $\mathcal{C}^{\perp}$ and, thus, $\boldsymbol{a}'\boldsymbol{R}^T_{\frac{n+1}{2},n-1} = \boldsymbol{0}$, which in turn leads to the desired result. ■

*Example 4:* Let us consider the function $f$ constructed in [21] with $n = 7$, namely $\text{supp}(f) = \{1,\ \alpha,\ \ldots, \alpha^{63}\}$, where $\alpha$ is a primitive element over $\mathbb{F}_{2^7}$. By executing Alg. 2 for any element $\alpha^m \in \{\alpha^{64}, \ldots, \alpha^{126}\}$ lying in $\text{supp}(f+1)$, we get all the possible swaps that may take place in order to preserve the maximum algebraic immunity; these swaps are illustrated in Table II (where the exponents of the corresponding elements are shown). The missing entries in the Table II (for $m = 66, 67, 68, 70, 71$ etc.) can be directly obtained by applying Proposition 11, without executing Alg. 2; hence, for

TABLE II
ALL THE APPROPRIATE SWAPS ON THE FUNCTION
$f : \mathrm{supp}(f) = \{1, \alpha, \ldots, \alpha^{2^{n-1}-1}\}, n = 7$

| $m$ | Candidates for swapping |
|---|---|
| 64 | 63 62 61 60 58 53 51 49 48 47 46 45 43 38 37 34 33 32 31 30 26 24 23 21 16 15 12 11 10 9 8 **6** 5 2 **0** |
| 65 | **60 59** 58 54 53 52 51 50 45 44 43 39 37 35 30 27 26 25 23 22 21 17 15 13 8 **7** 5 3 2 **1** 0 |
| 69 | 61 60 57 56 55 54 53 51 46 45 41 39 38 37 33 32 29 27 25 24 23 19 17 16 15 10 8 7 4 2 0 |
| 72 | 62 61 59 57 56 54 53 51 47 46 45 44 43 42 41 40 38 37 36 35 34 33 31 28 27 24 23 22 21 20 19 18 16 15 13 12 9 8 7 6 3 2 0 |
| 74 | 62 60 59 56 55 51 44 42 40 39 36 35 34 32 31 29 25 22 20 18 17 16 14 12 6 4 0 |
| 76 | **63** 60 57 51 49 48 47 45 44 43 42 41 36 32 30 27 26 23 22 21 20 19 18 15 14 12 11 10 9 5 **0** |
| 77 | 63 62 60 53 52 **51 50 47** 44 42 38 34 32 30 28 27 26 22 20 **19** 13 **9** 8 5 2 **1 0** |
| 78 | 62 60 58 54 52 **49** 47 46 **39** 38 37 35 34 32 30 29 28 **27** 26 24 **20** 16 15 14 12 **11** 8 5 3 1 0 |
| 80 | 63 61 **58** 56 54 53 47 46 45 43 41 40 39 38 36 33 29 28 24 23 22 21 18 17 **15** 14 13 12 11 9 8 7 6 3 0 |
| 81 | 63 61 60 **59** 58 57 55 54 53 51 49 45 44 43 42 41 40 39 38 33 32 **31 29** 26 25 22 21 19 18 14 13 11 7 6 5 4 2 **1** 0 |
| 82 | **63** 59 56 55 54 53 52 51 **50 49** 48 47 44 42 41 40 **39** 38 37 31 **27** 24 **22** 21 20 **19** 16 14 11 10 9 7 3 1 0 |
| 83 | 63 62 61 **58** 57 56 55 54 52 50 **47** 46 42 41 40 39 37 34 33 31 30 28 26 25 24 22 20 17 **16** 9 6 5 4 1 **0** |
| 84 | 61 60 **59** 57 56 55 **49** 46 45 42 41 40 37 35 33 30 29 27 25 24 18 17 16 15 12 11 9 8 7 **1** 0 |
| 87 | 61 **59** 53 52 51 47 46 44 40 37 36 34 31 28 27 26 24 23 20 19 18 16 14 9 8 6 5 4 3 2 0 |
| 90 | **63** 61 60 **58** 56 55 54 53 51 **50** 48 **46** 45 40 39 38 33 32 29 27 24 **22** 19 17 16 15 10 7 3 2 0 |
| 91 | **63** 60 59 **58** 57 56 55 54 53 52 48 45 43 41 40 39 38 37 32 31 28 26 25 24 21 20 18 17 15 12 10 9 6 5 4 3 2 1 **0** |
| 92 | 63 62 **59** 57 56 55 54 51 48 47 45 44 **43** 42 41 40 39 37 34 31 30 29 27 25 24 23 22 19 18 15 13 12 9 8 7 4 3 **1 0** |
| 93 | 62 61 57 56 55 53 52 51 47 44 42 41 40 37 35 34 33 28 25 21 20 19 15 14 13 12 11 6 4 1 0 |
| 95 | 62 61 60 59 57 55 54 51 48 47 45 44 42 39 38 36 35 34 33 32 31 27 26 24 **22** 17 14 13 12 11 10 9 5 3 0 |
| 97 | 60 59 58 57 56 51 50 48 45 44 43 41 40 36 35 32 31 30 29 28 23 21 19 14 13 10 9 8 7 6 0 |
| 101 | 58 55 54 53 52 51 46 44 43 40 39 38 37 36 35 31 30 27 26 25 24 21 18 17 16 15 14 13 9 8 6 5 4 2 0 |
| 107 | 63 62 **59** 57 53 52 **51 50** 48 **47** 44 42 41 38 36 34 27 26 22 20 19 16 14 **9** 5 2 **0** |
| 108 | 62 61 54 **52** 47 46 42 39 38 35 34 33 32 31 30 28 27 26 24 20 17 16 12 11 9 8 5 3 2 **1** 0 |
| 110 | 62 61 60 **58** 56 54 53 51 47 46 45 44 43 41 40 38 36 35 31 29 28 24 23 **22** 21 **19** 18 16 15 14 13 12 9 8 7 6 4 3 0 |
| 112 | **61** 56 55 51 42 40 34 32 25 20 18 17 14 12 0 |
| 115 | 63 62 61 60 59 54 53 51 49 48 47 46 38 35 34 33 32 31 30 28 26 24 20 17 16 12 11 10 9 8 **6** 5 3 2 0 |
| 116 | 58 55 54 53 52 51 50 46 45 43 39 38 37 36 35 30 29 27 26 25 24 23 18 17 16 15 13 8 7 5 4 3 2 1 0 |
| 122 | 63 62 **59** 57 56 53 52 48 47 46 44 42 41 38 37 36 35 34 29 26 22 19 16 15 14 13 12 7 5 2 **0** |
| 123 | 62 61 57 54 51 46 42 39 36 35 34 33 32 31 27 26 24 **21** 20 17 14 13 12 11 10 9 5 3 2 **1** 0 |
| 125 | **62 61** 60 59 58 56 51 **49** 47 46 45 44 43 41 36 35 32 31 30 29 28 24 **22** 21 19 14 13 10 9 8 7 6 **4** 3 0 |

e.g. $m = 113$, the corresponding entries in the Table would be $(62, 57, 56, 52, 43, 41, 35, 33, 26, 21, 19, 18, 15, 13, 1)$ (obtained via an increment by one of the corresponding entries for $m = 112$).

The bold numbers indicate that the corresponding swaps also preserve the nonlinarity of $f$ (being equal to $54$), according to computer computations; all the others swaps result in functions with decreased nonlinearity by 2.

## VI. CONCLUSIONS

The algebraic immunity of Boolean functions was studied in this paper. The behavior of functions of maximum algebraic immunity when they are slightly modified is examined, identifying proper modifications that ensure maximum algebraic immunity of the resulting functions. Applications to known constructions yield new constructions of functions with maximum algebraic immunity, thus generalizing the previous ones; more precisely, the proposed Alg. 1 stands as a direct generalization of the construction of [7], since it also fully covers the odd case, whereas the proposed Alg. 2 further extends the constructions given in [21], [25].

## REFERENCES


[1] A. Braeken, and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," in *Indocrypt 2005*, LNCS 3797, pp. 35–48, Springer, Heidelberg, 2005.

[2] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," in *Int. Workshop on Coding and Cryptography*, pp. 1–11, 2005.

[3] C. Carlet, D. K. Dalai, K. G. Gupta and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3105–3121, 2006.

[4] C. Carlet, "Constructing balanced functions with optimum algebraic immunity," in *IEEE Int. Symp. Inf. Theory*, pp. 451–455, 2007.

[5] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *Asiacrypt 2008*, LNCS 5350, pp. 425–440, Springer, Heidelberg, 2008.

[6] C. Carlet and P. Gaborit, "On the construction of balanced Boolean functions with a good algebraic immunity," in *IEEE Int. Symp. Inf. Theory*, pp. 1101–1105, 2005.

[7] C. Carlet, X. Zeng, C. Li and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," *Des. Codes Cryptogr.*, vol. 52, pp. 303–338, 2009.

[8] C. Carlet, "Comments on "Constructions of cryptographically significant Boolean functions using primitive polynomials"," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4852–4853, 2011.

[9] Y. Chen and P. Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity: construction and analysis," *IEEE Trans. Inf. Theory*, vol. 57, pp. 2522–2538, 2011.

[10] T. H. Cormen, C. E. Leiserson, R. L. Rivest, *Introduction to Algorithms*. MIT Press, 1990.

[11] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Eurocrypt 2003*, LNCS 2656, pp. 345–359, Springer, Heidelberg, 2003.

[12] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology - Crypto 2003*, LNCS 2729, pp. 176–194, Springer, Heidelberg, 2003.

[13] D. K. Dalai, S. Maitra and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," *Des. Codes Cryptogr.*, vol. 40, pp. 41–58, 2006.

[14] N. Li and W. Qi, "Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity," in *Asiacrypt 2006*, LNCS 4284, pp. 84–98, Springer, Heidelberg, 2006.

[15] N. Li, L. Qu, W. Qi, G. Feng, C. Li and D. Xie, "On the construction of Boolean functions with optimal algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1330–1334, 2008.

[16] F. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*. North-Holland, Amsterdam, 1977.

[17] W. Meier, E. Pasalic and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Eurocrypt 2004*, LNCS 3027, pp. 474–491, Springer, Heidelberg, 2004.

[18] E. Pasalic, "Almost fully optimized infinitive classes of Boolean functions resistant to (fast) algebraic cryptanalysis," in *ICISC 2008*, LNCS 5461, pp. 399–414, Springer, Heidelberg, 2008.

[19] L. Qu, C. Li, and K. Feng, "A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2908–2910, 2007.

[20] L. Qu, K. Feng, F. Liu, and L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2406–2412, 2009.

[21] P. Rizomiliotis, "On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation", *IEEE Trans. Inf. Theory*, vol. 56, pp. 4014–4024, 2010.

[22] S. Sarkar and S. Maitra, "Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity," in *AAECC 2007*, LNCS 4851, pp. 271–280, Springer, Heidelberg, 2007.

[23] C. Wang and X. Chen, "On extended algebraic immunity," *Des. Codes Cryptogr.*, vol. 57, pp. 271–281, 2010.

[24] Q. Wang, J. Peng, and H. Kan, "Constructions of cryptographically significant Boolean functions using primitive polynomials", *IEEE Trans. Inf. Theory*, vol. 56, pp. 3048–3053, 2010.

[25] X. Zeng, C. Carlet, J. Shan and L. Hu, "More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks," *IEEE Trans. Inf. Theory*, vol. 57, pp. 6310–6320, 2011.