# On the Lower Block Triangular Nature of the Incidence Matrices to Compute the Algebraic Immunity of Boolean Functions

Deepak Kumar Dalai(✉)

School of Mathematical Sciences, NISER, Bhubaneswar 751005, India
deepak@niser.ac.in

**Abstract.** The incidence matrix between two sets of vectors in $\mathbb{F}_2$ has a great importance in different areas of mathematics and sciences. The rank of these matrices are very useful while computing the algebraic immunity(AI) of Boolean functions in cryptography literature [3,7]. With a proper ordering of monomial (exponent) vectors and support vectors, some interesting algebraic structures in the incidence matrices can be observed. We have exploited the lower-block triangular structure of these matrices to find their rank. This structure is used for faster computation of the AI and the low degree annihilators of an $n$-variable Boolean functions than the known algorithms. On the basis of experiments on at least 20 variable Boolean functions, we conjecture about the characterization of power functions of algebraic immunity 1, could verify the result on the AI of $n$-variable inverse S-box presented in [6](i.e., $\lceil 2\sqrt{n} \rceil - 2$), and presented some results on the AI of some important power S-boxes.

**Keywords:** Cryptography · Boolean function · Power function · Algebraic immunity

## 1 Notation

In this section, we introduce the basic notations and definitions which are required to read the later part of the article.

$V_n$: The $n$ dimensional vector space over the two element field $\mathbb{F}_2 = \{0, 1\}$.
$\mathsf{wt}(v)$: The weight of a vector $v = (v_1, v_2, \ldots, v_n) \in V_n$ is $\mathsf{wt}(v) = |\{v_i : v_i = 1\}|$.
$V_{n,d}$: The set of vectors in $V_n$ of weight $d$ or less i.e., $V_{n,d} = \{v \in V_n : \mathsf{wt}(v) \leq d\}$.
$u \subseteq v$: For $u = (u_1, u_2, \ldots, u_n), v = (v_1, v_2, \ldots, v_n) \in V_n$, we denote $u \subseteq v$ if $u_i = 1$ implies $v_i = 1$ for $1 \leq i \leq n$.
$+, \sum$: The addition operators on $\mathbb{F}_2$ or, on reals $\mathbb{R}$, which is context based.
$\mathsf{int}(u)$: The integer value of the binary string representation of the vector $u \in V_n$.

**Ordering of vectors**: If $u, v \in V_n$, then

1. Lexicographic ordering: $u < v$ if $\mathsf{int}(u) < \mathsf{int}(v)$.
2. Weighted ordering: $u <_w v$ if $(\mathsf{wt}(u) < \mathsf{wt}(v))$ or, $(\mathsf{wt}(u) = \mathsf{wt}(v)$ and $\mathsf{int}(u) < \mathsf{int}(v))$.


A. Maletti (Ed.): CAI 2015, LNCS 9270, pp. 79–89, 2015.
DOI: 10.1007/978-3-319-23021-4_8

**Incidence matrix ($M_V^X$)**: For $v, x \in V_n$, $x$ is incident on $v$ if $x \subseteq v$. We denote $v^x = 1$ if $x \subseteq v$ and 0 otherwise. For given two ordered sets of vectors $V, X$, the incidence matrix $M_V^X$ of $V$ on $X$ is defined as $M_V^X[i,j] = v_i^{x_j}$, where $v_i$ and $x_j$ are $i$-th and $j$-th element in $V$ and $X$ respectively. We call $X$ as exponent vector set and $V$ as support vector set.

**Incidence matrix ($M_V^d$)**: If the exponent vector set $X = V_{n,d}$, then the incidence matrix $M_V^X$ is denoted as $M_V^d$.

**Boolean function**: A function $f : V_n \mapsto \mathbb{F}_2$ is called $n$ variable Boolean function. The set of all Boolean functions on $n$-variable is denoted as $B_n$. The polynomial form of a Boolean function can be represented as an element of binary quotient ring on $n$-variables $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$ and this form is called the *algebraic normal form* (ANF) of the Boolean function. The degree of $f \in B_n$ (i.e., $\deg(f)$) is the algebraic degree. We also denote $B_{n,d} = \{f \in B_n : \deg(f) \leq d\}$ and $m_{n,d}$ is the set of all monomials of degree $d$ or less. The evaluations of $f$ at each vector in $V_n$ with an order is known as the *truth table* representation of $f$ and the representation can be viewed as a $2^n$-tuple binary vector. The support set and the weight of $f \in B_n$ is defined as $S(f) = \{v \in V_n : f(v) = 1\}$ and $\mathsf{wt}(f) = |S(f)|$ respectively.

**Algebraic immunity ($\mathsf{AI}$)**: Given $f \in B_n$, a nonzero $g \in B_n$ is called an annihilator of $f$ if $f.g = 0$, i.e., $f(v)g(v) = 0$ for all $v \in V_n$. The set of all annihilators of $f \in B_n$ is denoted by $An(f)$. The algebraic immunity of $f \in B_n$ is defined as $\mathsf{AI}(f) = \min\{\deg(g) : g \in An(f) \cup An(1+f)\}$.

$\mathsf{wt}(M), \mathsf{den}(M)$: The weight and density of an $m \times n$ binary matrix $M$ are defined as $\mathsf{wt}(M) = |\{M[i,j] : M[i,j] = 1\}|$ and $\mathsf{den}(M) = \frac{\mathsf{wt}(M)}{mn}$ respectively.

## 2 Introduction

The incidence matrix $M_V^X$ is an interesting tool in the study of several branches in mathematics and computer sciences like combinatorics, coding theory, cryptography and polynomial interpolation. The incidence matrix $M_V^d$ has an important role in the study of algebraic cryptanalysis. The problem to find the rank of this matrix is equivalent to compute the $\mathsf{AI}$ of a Boolean function [7]. Some algorithms are available in [4,5,7] to find the rank of $M_V^d$ and the solution of the system of equations $M_V^d \gamma = 0$ to find the annihilators of degree $d$ of the Boolean function of support set $V$.

From the point of view of algebraic cryptanalysis, $f \in B_n$ should not be used to design a cryptosystem if $\mathsf{AI}(f)$ is low [1,7]. It is known that for any $f \in B_n$, $\mathsf{AI}(f) \leq \lceil \frac{n}{2} \rceil$. Thus, the target of a good design is to use a $f \in B_n$ such that neither $f$ nor $1 + f$ has an annihilator of degree much less than $\lceil \frac{n}{2} \rceil$.

If $g \in B_n$ is an annihilator of $f \in B_n$ then $g(v) = 0$ for $v \in S(f)$. To find a $d$ or lesser degree annihilator $g \in B_{n,d}$, one has to solve the system of linear equations

$$\sum_{\alpha \in V_n, \mathsf{wt}(\alpha) \leq d} a_\alpha v^\alpha = 0 \quad \text{for } v \in S(f) \quad \text{i.e.,} \quad \sum_{\alpha \in V_n, \mathsf{wt}(\alpha) \leq d, \alpha \subseteq v} a_\alpha = 0 \text{ for } v \in S(f).$$

That is, $M^d_{S(f)}\gamma = 0.$ (1)

where the transpose of $\gamma$ is the unknown row vector $(a_\alpha)$. If $\text{rank}(M^d_{S(f)}) < |m_{n,d}| = \sum_{i=0}^{d} \binom{n}{i}$ then $f$ has a $d$ or lesser degree annihilator.

For $f \in B_n$, the incidence matrix $M^d_{S(f)}$ is a particular case of $M^X_V$, whose rank tells about the $\mathsf{AI}(f)$. In this article, we study the rank of $M^X_V$, with special attention on $M^d_{S(f)}$. Some structures of $M^X_V$, which are not seen in a random binary matrix are addressed in [2]. Thus, the system of equations in Equation 1 can be solved faster as compared to solving an arbitrary system of equations of same order if the algebraic structures in $M^X_V$ are carefully exploited. For example, in [4], some structures have been exploited to make it constant time faster in average case.

In Section 3, we have proposed a technique on the ordering of vectors in $X$ and $V$ which makes the matrix $M^X_V$ and $M^d_{S(f)}$ a lower block triangular. The Section 3.2 and 3.3 contain the main results of this article to reduce the computation time. Experimental results of some important exponent S-boxes are presented in Section 4. On the basis of experiments, we conjecture about the complete characterization of power functions of algebraic immunity 1. We too verified the result on the $\mathsf{AI}$ of inverse power function in [6] till 20 variable Boolean functions which was conjectured in [6]. Some experimental results on some important power functions are too presented in this section.

## 3 Lower-Block Triangular Nature of $M^X_V$

An $n \times m$ matrix $M$ is a lower-block triangular if its form is as

$$M = \begin{pmatrix} M_{11} & M_{12} & \dots & M_{1l} \\ M_{21} & M_{22} & \dots & M_{2l} \\ \dots & \dots & \ddots & \dots \\ M_{l1} & M_{l2} & \dots & M_{ll} \end{pmatrix} \quad (2)$$

where $M_{ij}$ are $n_i \times m_j$ sub-matrices for $1 \leq i, j \leq l$ with $\sum_{i=0}^{l} n_i = n$ and $\sum_{j=0}^{l} m_j = m$ and $M_{i,j}$ are zero sub-matrices for $j > i$.

### 3.1 Using the Ordering $<_w$

Consider two ordered sets of vectors $V, X \subseteq V_n$ with the ordering $<_w$. Let $V^0, V^1, \dots, V^n$ and $X^0, X^1, \dots, X^n$ be the disjoint partitions of $V$ and $X$ such that $V^i = \{v \in V : \mathsf{wt}(v) = i\}$ and $X^i = \{x \in X : \mathsf{wt}(x) = i\}, 0 \leq i \leq n$ respectively. If $v \in V^i$, $x \in X^j$ and $i < j$, it is clear that $v <_w x$ and $x \not\subseteq v$. Hence, from the definition of incidence, we have the following theorem.

**Theorem 1.** *The incidence matrix $M_V^X$ is a lower block triangular matrix with $M_{ij} = M_{V^i}^{X^j}$ on the ordering $<_w$ of elements of $V$ and $X$.*

Since $M_V^X$ is lower block triangular, block wise Gaussian row elimination can be performed to find its rank. Consider that $V$ and $X$ are chosen randomly such that $|V| = |X| = 2^{n-1}$. Here, $|X^i|$ and $|V^i|$ are approximately $\frac{1}{2}\binom{n}{i}$ for $0 \leq i \leq n$. The time complexity for $i$th block wise row elimination is $O(2^n\binom{n}{i}^2)$. Hence, the time complexity for finding the rank of $M_V^X$ is $O(2^n \sum_{i=0}^{n}\binom{n}{i}^2) = O(2^n\binom{2n}{n})$.

For the case of $M_{S(f)}^d$, $X = V_{n,d}$ and $V = S(f)$. So, $|X^i| = \binom{n}{i}$ for $0 \leq i \leq d$ and $|X^i| = 0$ for $d+1 \leq i \leq n$. If $f \in B_n$ is a randomly chosen Boolean function, then $|V^i| \approx \frac{1}{2}\binom{n}{i}$, for $0 \leq i \leq n$. During each block wise row operation of matrix $M_{S(f)}^d$ from down to top, all columns in the block should be eliminated to have the rank equal to the number of columns. So, the same number of rows are eliminated and rest of the rows augmented to the next block of rows. For $0 \leq j < n-d$, no computation is needed for the $j$th block wise row elimination as $|X^{n-j}| = 0$. For $n-d \leq j \leq n$, the number of rows in $j$th block operation is

$$r_j = |V^{n-j}| + (\sum_{i=0}^{j-1}|V^{n-i}| - \sum_{i=n-d}^{j-1}|X^{n-i}|)$$
$$= \sum_{i=0}^{j}|V^{n-i}| - \sum_{i=n-d}^{j-1}|X^{n-i}| \approx \frac{1}{2}\sum_{i=0}^{j}\binom{n}{i} - \sum_{i=n-d}^{j-1}\binom{n}{i}.$$

For $d < \frac{n}{2}$,

$$r_j \approx \frac{1}{2}(\binom{n}{j} + \sum_{i=n-d}^{j-1}\binom{n}{i} + \sum_{i=d+1}^{n-(d+1)}\binom{n}{i} + \sum_{i=n-(j-1)}^{d}\binom{n}{i} + \sum_{i=0}^{n-j}\binom{n}{i}) - \sum_{i=n-d}^{j-1}\binom{n}{i}$$

$$= \frac{1}{2}(\binom{n}{j} + \sum_{i=d+1}^{n-(d+1)}\binom{n}{i} + \sum_{i=0}^{n-j}\binom{n}{i}) = O(2^n).$$

During the $j$th block wise operation, the sub matrix has $r_j$ many rows and $\sum_{i=0}^{n-j}\binom{n}{i}$ many columns and from there $\binom{n}{n-j}$ many columns (and as many rows ) to be eliminated. The time complexity in the $j$th block wise row elimination is $O(r_j\binom{n}{n-j}(\sum_{i=0}^{n-j}\binom{n}{i}))) = O(r_j\binom{n}{j}^2)$ and hence, the time complexity for finding the rank of $M_{S(f)}^d$ is $O(\sum_{j=n-d}^{n}(r_j\binom{n}{j}^2)) = O(2^n\sum_{j=n-d}^{n}\binom{n}{j}^2) = O(2^n\sum_{j=0}^{d}\binom{n}{j}^2)$.

Moreover, as discussed in [2, Section3.2], each sub-matrix is sparser by $O(2^d)$ than a random matrix, which can further be exploited to speed up the process by $O(2^d)$. Moreover, there is advantage in space complexity as only the sub-matrix of size $r_j \times \binom{n}{j} = O(2^n\binom{n}{j})$ is needed during the $j$th block operation in stead of the whole $2^{n-1} \times 2^{n-1}$ matrix.

### 3.2 Using the Ordering $<$

Consider two ordered subsets $V, X$ of $V_n$ with the ordering $<$. Here onwards, we mean the notation $K = 2^k - 1$ and $N = 2^n - 1$. Let $V^0, V^1, \ldots, V^K$, and $X^0, X^1, \ldots, X^K, k \leq n$, be disjoint subsets of $V$ and $X$, partitioned on the value of left most $k$ coordinates of the vectors in $V$ and $X$ respectively. The superscript $i$ of $V^i$ and $X^i$ denotes the integer value of left most $k$-coordinates of vectors in $V$ and $X$. If $v \in V^i$, $x \in X^j$ and $i < j$, then $v < x$ and that implies $x \not\subseteq v$. Let denote $\mathsf{vect}(i)$ is the vector form of binary representation of $i$. Hence, we have the following lemma.

**Lemma 1.** *The incidence matrix $M_{V^i}^{X^j}$ is a zero matrix if $\mathsf{vect}(j) \not\subseteq \mathsf{vect}(i)$ for $0 \leq i, j \leq K$.*

Since $\mathsf{vect}(j) \not\subseteq \mathsf{vect}(i)$ for $j > i$, $M_{V^i}^{X^j}$ is zero matrix for $j > i$ and we have the following theorem.

**Theorem 2.** *The incidence matrix $M_V^X$ is a lower block triangular matrix with $M_{ij} = M_{V^i}^{X^j}$ on the ordering $<$ of elements of $V$ and $X$.*

Since $M_V^X$ is lower block triangular, block wise Gaussian row elimination from down to top can be implemented for reducing the computation time. Hence we have the following results on the rank of $M_V^X$.

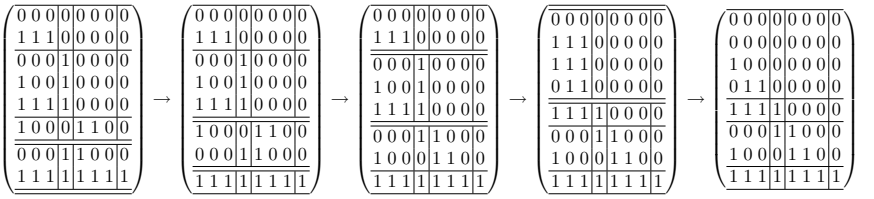
**Corollary 1.** *$rank(M_V^X) < |X|$ iff $rank(M_{\overline{V}}^{\overline{X}}) < |\overline{X}|$ where $\overline{V} = \cup_{i=0}^{p} V^{K-i}$ and $\overline{X} = \cup_{i=0}^{p} X^{K-i}$ for some $0 \leq p \leq K$.*

**Corollary 2.** *If $\sum_{i=0}^{p} |V^{K-i}| < \sum_{i=0}^{p} |X^{K-i}|$ for some $0 \leq p \leq K$, then $rank(M_V^X) < |X|$. Therefore, if $|V| = |X|$ and $\sum_{i=0}^{p} |V^i| > \sum_{i=0}^{p} |X^i|$ for some $0 \leq p \leq K$, then $rank(M_V^X) < |X|$.*

Corollary 2 classifies some Boolean functions of having low $\mathsf{AI}$. It can be used in better way by finding a possible permutation on the variables $x_1, x_2, \ldots, x_n$, such that $\sum_{i=0}^{p} |V^{K-i}| < \sum_{i=0}^{p} |X^{K-i}|$ for a some $p$.

**Corollary 3.** *If $rank(M_V^X) = |X|$ then for every permutation on variables $x_1, x_2, \ldots, x_n$ and $k, p$, $0 \leq k \leq n, 0 \leq p < 2^k$, $\sum_{i=0}^{p} |V^{K-i}| \geq \sum_{i=0}^{p} |X^{K-i}|$.*

*Example 1.* Let $X = \{1, 2, 3, 4, 8, 9, 10, 14\}$ and $V = \{0, 3, 4, 5, 7, 9, 12, 15\}$ be two subsets of $V_4$. Here, the vectors are shown in their integer form. If we fix the left most two coordinates, then $X^0 = \{1, 2, 3\}, X^1 = \{4\}, X^2 = \{8, 9, 10\}, X^3 = \{14\}$ and $V^0 = \{0, 3\}, V^1 = \{4, 5, 7\}, V^2 = \{9\}, V^3 = \{12, 15\}$. Here, $|V^0| + |V^1| = 5$ and $|X^0| + |X^1| = 4$. Hence, following the corollary 2, we have $rank(M_V^X) < |X|$. To find the exact value of $rank(M_V^X)$ the block wise row reduction of $M_V^X$ can be done as following. The block of rows enclosed by double lines are to be reduced.

$M_V^X =$ 

Here $rank(M_V^X) = 6$ i.e., there are two free monomials corresponding to the vectors 2 and 10 in $X$ i.e., $x_2$ and $x_2x_4$. So, there are 2 linearly independent annihilators on the monomials of exponent vectors from $X$ of the Boolean function having support set $V$.

Now consider that $V$ and $X$ are chosen randomly such that $|V| = |X| = \eta$. Fixing $k$ variables, there are $2^k$ blocks of rows of size approximately $\frac{\eta}{2^k}$. The time complexity for row elimination of each block is $O(\eta \times (\frac{\eta}{2^k})^2) = O(\eta^3 2^{-2k})$. Hence, the time complexity for finding the rank of $M_V^X$ is $O(2^k \times \eta^3 2^{-2k}) = O(\eta^3 2^{-k})$. If $|V| = |X| = 2^{n-1}$, the time complexity for finding the rank of $M_V^X$ is $O(2^{3n-k})$. If one fixes all $n$ variables, the theoretical time complexity becomes $O(2^{2n})$, i.e., quadratic time complexity on number of monomials. Moreover, the space complexity for the computation is $O(2^n)$ (i.e., linear) as only one block of rows is needed during the computation. Hence, we have the following theorem.

**Theorem 3.** *For a randomly chosen subsets $V$ and $X$ of $V_n$ such that $|V| = |X| = 2^{n-1}$, the expected time complexity and space complexity to compute the rank of the $2^{n-1} \times 2^{n-1}$ matrix $M_V^X$ is $O(2^{2n})$ and $O(2^n)$ i.e., quadratic time complexity and linear space complexity on the $|X|$ respectively.*

Now we shall discuss about the rank of $M_{S(f)}^d$, which is needed to compute $\mathsf{AI}(f)$ for $f \in B_n$. In this case, $X = V_{n,d}$ and $V = S(f)$. Since the exponent set $X$ is not a random set, the time and space complexity is not expected as the described one in Theorem 3. For $0 \le k \le n$, we have $|X^i| = |V_{n,d}^i| = b_i = \sum_{j=0}^{d-\mathsf{wt}(i)} \binom{n-k}{j}$, $0 \le i < 2^k$. If $f \in B_n$ is randomly chosen, then we have $|V^i| \approx 2^{n-k-1}$, $0 \le i < 2^k$. In each block wise row operation (from down to top) of matrix $M_{S(f)}^d$, every time all columns in the block need to be eliminated. So, the same number of rows are also eliminated and rest of the rows are augmented to the next block of rows. Hence, during the $j$-th block wise row operation, for $0 \le j \le K$, the number of rows is

$$\begin{aligned} r_j &= |V^{K-j}| + \sum_{i=0}^{j-1} (|V^{K-i}| - b_{K-i}) \\ &= \sum_{i=0}^{j} |V^{K-i}| - \sum_{i=0}^{j-1} b_{K-i} \approx (j+1)2^{n-k-1} - \sum_{i=0}^{j-1} b_{K-i}. \end{aligned}$$

At the $j$-th block operation, the sub-matrix contains $r_j$ rows, $c_j = \sum_{i=0}^{K-j} b_i$ columns and $b_{K-j}$ columns from these $c_j$ columns to be eliminated. So, the time

complexity for the $j$th block row elimination is $O(r_j c_j b_{K-j})$ and hence, time complexity to find the rank of $M^d_{S(f)}$ is $O(\sum_{j=0}^{K} r_j c_j b_{K-j})$.

If $k = n$, then the time to compute the rank of $M^d_{S(f)}$ is $O(\sum_{j=0}^{N} r_j c_j b_{N-j})$. In this case $b_i = \sum_{i=0}^{d-\mathsf{wt}(i)} \binom{0}{i} = \begin{cases} 1 \text{ if } \mathsf{wt}(i) \le d \\ 0 \text{ if } \mathsf{wt}(i) > d, \end{cases}$ i.e., $b_{N-j} = \begin{cases} 1 \text{ if } \mathsf{wt}(j) \ge n-d \\ 0 \text{ if } \mathsf{wt}(i) < n-d. \end{cases}$

So,

$$c_j = \sum_{i=0}^{N-j} b_i = \sum_{\substack{0 \le i \le N-j \\ \mathsf{wt}(i) \le d}} 1 = \sum_{i=0}^{d} \binom{n}{i} - \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1$$

and

$$r_j \approx \frac{j+1}{2} - \sum_{i=0}^{j-1} b_{N-i} = \frac{j+1}{2} - \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1.$$

When $\mathsf{wt}(j) < n-d$ i.e., $b_{N-j} = 0$, there is no column to eliminate and hence no operation is done. When $\mathsf{wt}(j) \ge n-d$, i.e., $b_{N-j} = 1$, there is only one column to eliminate. So, the time complexity for $j$-th block operation is $O(r_j c_j)$. Therefore, the time complexity to find the rank of $M^d_{S(f)}$ is $O(\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} r_j c_j)$. Simplifying it, we have

$$\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} r_j c_j = \sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} \left(\frac{j+1}{2} - \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1\right)\left(\sum_{i=0}^{d} \binom{n}{i} - \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1\right)$$

$$\le \sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} \left(\frac{j+1}{2} - \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1\right)\left(\sum_{i=0}^{d} \binom{n}{i}\right).$$

Now, we will find the value of the summation $\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} j$. If $j$ is in the summation, then $j$ has $\mathsf{wt}(j)$ many non-zero positions in the binary expansion of $j$ and each non-zero position $k$ contributes the value $2^k$ to the summation. In the summation, each position occurs $\frac{1}{n}\sum_{i=n-d}^{n} i\binom{n}{i} = \sum_{i=n-d}^{n} \binom{n-1}{i-1}$ many times. So, for $0 \le k < n$, $k$-th position contributes the value $2^k \sum_{i=n-d}^{n} \binom{n-1}{i-1}$ to the summation. Hence, $\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} j = \sum_{i=n-d}^{n} \binom{n-1}{i-1} \sum_{k=0}^{n-1} 2^k = \sum_{i=n-d}^{n} \binom{n-1}{i-1} N$.

So,

$$\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} \frac{j+1}{2} = \frac{1}{2}\left(\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} j + \sum_{i=n-d}^{n} \binom{n}{i}\right) = \frac{1}{2}\left(\sum_{i=n-d}^{n} \binom{n-1}{i-1} N + \sum_{i=n-d}^{n} \binom{n}{i}\right)$$

Now, in the summation $\sum_{\substack{0 \le j \le N \\ \mathsf{wt}(j) \ge n-d}} \sum_{\substack{0 \le i \le j-1 \\ \mathsf{wt}(i) \ge n-d}} 1$, an integer $i$ with $\mathsf{wt}(i) \ge n-d$, is counted $l$ times, where $l = |\{j : i < j \le N, \mathsf{wt}(j) \ge n-d\}|$. Let $i_1 < i_2 < \cdots < N$ are integers with weight at least $n-d$, then $i_1$ is counted

$\sum_{i=n-d}^{n}\binom{n}{i}-1$ times, $i_2$ is counted $\sum_{i=n-d}^{n}\binom{n}{i}-2$ times and so on.
So, $\sum_{\substack{0\le j\le N\\ \mathsf{wt}(j)\ge n-d}}\sum_{\substack{0\le i\le j-1\\ \mathsf{wt}(i)\ge n-d}}1=(\sum_{i=n-d}^{n}\binom{n}{i}-1)+(\sum_{i=n-d}^{n}\binom{n}{i}-2)+\cdots+0$
$=\frac{1}{2}\sum_{i=n-d}^{n}\binom{n}{i}(\sum_{i=n-d}^{n}\binom{n}{i}-1)$.

Hence, $\sum_{\substack{0\le j\le N\\ \mathsf{wt}(j)\ge n-d}} r_jc_j\le(2^n\sum_{i=n-d}^{n}\binom{n}{i}-(\sum_{i=n-d}^{n}\binom{n}{i})^2)\sum_{i=0}^{d}\binom{n}{i}$
$=(\sum_{i=0}^{d}\binom{n}{i})^2\sum_{i=d+1}^{n}\binom{n}{i}$.

**Theorem 4.** *For a randomly chosen Boolean function $f\in B_n$, the expected time complexity and space complexity to compute the rank of the matrix $M^d_{S(f)}$ is $O((\sum_{i=0}^{d}\binom{n}{i})^2\sum_{i=d+1}^{n}\binom{n}{i})$ and $O(\max_{0\le j\le N} r_jc_j)$ respectively.*

Since the simplification of the above expression is not very easy, the time complexity bound given in the Theorem 4 is not a tight upper bound. Hence the theoretical time complexity mentioned in Theorem 4 is not a significant improvement over other algorithms. However, in practice, it is very fast and can be used to compute for $n = 20$. Moreover, exploiting the sparseness of the sub-matrices, the computation speed can further be improved.

### 3.3 Ordering $<$ and Dalai-Maitra Algorithm [4]

As we discussed in above, to find $\mathsf{AI}$ of $f\in B_n$, one needs to compute the rank of $M^d_{S(f)}$. The involutory property of $M^{V_{n,d}}_{V_{n,d}}$ (i.e., $(M^{V_{n,d}}_{V_{n,d}})^2=I$) is exploited to reduce the size of incidence matrix $M^d_{S(f)}$ to compute its rank in Dalai-Maitra algorithm [4]. Instead of computing the rank of $M^d_{S(f)}$ of order $|V_{n,d}|\times|S(f)|$, it is proposed to compute the rank of a smaller matrix $I^d_f$ of order $|S(f)\setminus V_{n,d}|\times|V_{n,d}\setminus S(f)|$. Given a $f\in B_n$ and $d\le n$ the matrix $I^d_f$ is defined as

$$I^d_f[v,x]=\begin{cases}\sum_{i=0}^{d-\mathsf{wt}(x)}\binom{\mathsf{wt}(v)-\mathsf{wt}(x)}{i} \bmod 2 & \text{if } x\subseteq v\\ 0 & \text{if } x\not\subseteq v,\end{cases}$$

where $v\in Y=S(f)\setminus V_{n,d}$ and $x\in Z=V_{n,d}\setminus S(f)$.

**Theorem 5.** *[4] The matrix $M^d_{S(f)}$ is of full rank (i.e., $|V_{n,d}|$) iff the matrix $I^d_f$ is of full rank (i.e., $|Z|$).*

We can see that the order of matrix $I^d_f$ is reduced by half in average in both the number of rows and columns. To find $\mathsf{AI}(f)$, finding rank of $M^d_{S(f)}$ can speed up the process approximately by 8 times. We further speed up the process by observing the lower block triangular nature of $M^d_{S(f)}$ by proper ordering of the vectors in $Y$ and $Z$.

Let the vectors in $Y$ and $Z$ be ordered by $<$. For $0\le k\le n$, let $Y^0,\ldots,Y^{2^k-1}$ and $Z^0,\ldots,Z^{2^k-1}$ be the partitions of $Y$ and $Z$ on their left most $k$ coordinates of vectors in $Y$ and $Z$ respectively. Let denote $I^d_f[Y^i,Z^j]$ be the sub-matrix in $I^d_f$ corresponding to the vector subsets $Y^i$ and $Z^j$.

**Lemma 2.** *The sub-matrix* $I_f^d[Y^i, Z^j]$ *is a zero matrix if* $\mathsf{vect}(j) \nsubseteq \mathsf{vect}(i)$ *for* $0 \leq i, j \leq K$.

Since $\mathsf{vect}(j) \nsubseteq \mathsf{vect}(i)$ for $j > i$, $I_f^d[Y^i, Z^j]$ is zero matrix for $j > i$ and we have the following theorem.

**Theorem 6.** *The matrix* $I_f^d$ *is a lower block triangular matrix with submatrices* $I_{f\,ij}^d = I_f^d[Y^i, Z^j]$, $0 \leq i, j \leq 2^k - 1$ *on the ordering* $<$ *of elements of* $Y$ *and* $Z$.

Comparing the partitions in matrix $M_{S(f)}^d$ in subsection 3.2, here we have $|Y^i| \approx \frac{|V^i|}{2}$ and $|Z^i| \approx \frac{|X^i|}{2}$. Therefore, the computation in this technique is expected to be 8 times faster than the technique described in the earlier subsection. Therefore, the technique presented here is so far the best technique to evaluate $\mathsf{AI}$ of a Boolean function. It is possible to find $\mathsf{AI}$ of a Boolean function of 20 variables or, a few more variables with less memory.

## 4 Experiments on the AI of Power Functions

Since the vector space characteristic of finite field $\mathbb{F}_{2^n}$ can be viewed as $V_n = \mathbb{F}_2^n$, every function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ can be viewed as an ordered collection of $n$ Boolean function. That is, $F(x) = (F_1(x), F_2(x), \cdots, F_n(x))$, where the Boolean functions $F_i$s are called the co-ordinate Boolean functions of $F$. The nonzero linear combination of the co-ordinate functions, (i.e., $\sum_{i=1}^n a_i F_i, a_i \in \mathbb{F}_2$ but not all $a_i$ are zero) are called component Boolean functions of $F$. The component functions of $F$ can too be algebraically represented as $Tr(\lambda F)$ for non-zero constants $\lambda \in \mathbb{F}_{2^n}^*$.

**Definition 1.** *Let* $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ *be a function. The algebraic immunity of* $F$ *is* $\mathsf{AI}(F) = \min_{(a_1,\ldots,a_n)\in V_n \setminus \{(0,\ldots,0)\}} \{\mathsf{AI}(\sum_{i=1}^n a_i F_i)\}$ *i.e., the minimum of* $\mathsf{AI}$ *of the component functions of* $F$.

A function $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is called a power function if $F$ is of the form $F(x) = x^d$ for $x \in \mathbb{F}_{2^n}$ and $d$ is an integer. The degree of power function $x^d$ is defined as the weight of the $\mathsf{vect}(d)$, which is the degree of each component function of $x^d$. In this section, we present some experimental results on the $\mathsf{AI}$ of power functions.

During the experiments, we observed a nice result for power functions of having algebraic immunity 1. It is known that $\mathsf{AI}(x^{d_1}) = \mathsf{AI}(x^{d_2})$ if $d_1$ and $d_2$ are in same 2-cyclotomic coset modulo $2^n - 1$ i.e., $d_2 = 2^i d_1 \bmod 2^n - 1$ for some integer $i$. The size of each 2-cyclotomic coset is a divisor of $n$. It is very clear that the $\mathsf{AI}$ of linear power functions, i.e., $\mathsf{AI}(x^{2^i \bmod 2^n - 1})$, is 1. We present a conjecture on the nonlinear power functions of algebraic immunity 1.

*Conjecture 1.* Let $n \geq 4$ and $x^d$ be a power function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Then $\mathsf{AI}(x^d) = 1$ iff one of the followings happens for $d$.

i. $d \in \{1, 2, \ldots, 2^{n-1}\}$ i.e., $x^d$ is a linear power function.
ii. The size of 2-cyclotomic coset modulo $2^n - 1$ of $d$ is a proper divisor of $n$.

Based on this conjecture, we have the following example and corollary.

*Example 2.* Let take $n = 6$. Here $\mathsf{AI}(x^d) = 1$ iff

1. $d \in \{1, 2, 4, 8, 16, 32\}$ (when $x^d$ is linear) or,
2. $d \in \{9, 18, 36\} \cup \{21, 42\} \cup \{27, 54, 45\}$ (when $x^d$ is not linear).

**Corollary 4.** *If $n$ is prime , then there is no non-linear power functions of algebraic immunity* 1.

Further, using the proposed technique, we computed $\mathsf{AI}$ of some cryptographic important power functions like inverse functions, Kasami exponents and Niho exponents up to 21 variables. The $\mathsf{AI}$ of $n$-variable inverse function, $x^{-1}$, is upper bounded by $\lceil 2\sqrt{n} \rceil - 2$, Kasami and Niho exponents are upper bounded by $\lceil 2\sqrt{n} \rceil$ [8]. Experimentally, we checked that the $\mathsf{AI}$ of the inverse function is exactly $\lceil 2\sqrt{n} \rceil - 2$ for $n \leq 21$ which is proved in [6].

A Kasami exponent $K : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is of the form $x^{2^{2k}-2^k+1}$ for $k \leq \frac{n}{2}$ and $\gcd(n, k) = 1$. The degree of Kasami exponent is $k + 1$. Therefore, $\mathsf{AI}(K) \leq min\{k+1, \lceil 2\sqrt{n} \rceil\}$. The following table presents the experimental result of $\mathsf{AI}(K)$ for the largest $k \leq \frac{n}{2}$ and $\gcd(n, k) = 1$.

| $n$ | $k$ | $\deg(K)$ | $\lceil 2\sqrt{n} \rceil$ | $\mathsf{AI}(K)$ | $n$ | $k$ | $\deg(K)$ | $\lceil 2\sqrt{n} \rceil$ | $\mathsf{AI}(K)$ |
|---|---|---|---|---|---|---|---|---|---|
| 10 | 3 | 4 | 7 | 4 | 14 | 5 | 6 | 8 | 6 |
| 11 | 5 | 6 | 7 | 5 | 15 | 7 | 8 | 8 | 7 |
| 12 | 5 | 6 | 7 | 5 | 16 | 7 | 8 | 8 | 7 |
| 13 | 6 | 7 | 8 | 6 | 17 | 8 | 9 | 9 | 8 |

For odd $n = 2s + 1$, a Niho exponent $N : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ is of the form $x^{2^s+2^{\frac{s}{2}}-1}$ if $s$ is even and $x^{2^{\frac{3s+1}{2}}+2^s-1}$ if $s$ is odd. The degree of Niho exponent is $d = \frac{n+3}{4}$ if $n \equiv 1 \mod 4$ and $d = \frac{n+1}{2}$ if $n \equiv 3 \mod 4$. Therefore, $\mathsf{AI}(N) \leq min\{d, \lceil 2\sqrt{n} \rceil\}$. The following table presents the experimental results of $\mathsf{AI}(N)$.

| $n$ | $\deg(N)$ | $\lceil \sqrt{n} \rceil$ | $\mathsf{AI}(N)$ | $n$ | $\deg(N)$ | $\lceil \sqrt{n} \rceil$ | $\mathsf{AI}(N)$ |
|---|---|---|---|---|---|---|---|
| 9 | 3 | 7 | 3 | 15 | 8 | 8 | 7 |
| 11 | 6 | 7 | 5 | 17 | 5 | 9 | 5 |
| 13 | 4 | 8 | 4 | 19 | 10 | 9 | 9 |

Then we do experiments to find power functions of optimal $\mathsf{AI}$ (i.e., $\lceil \frac{n}{2} \rceil$) and we found that there are power functions of optimal $\mathsf{AI}$ but it becomes rarer as $n$ increases. The experiment is tabulated below.

| $n$ | $m = \lvert\{x^d : \mathsf{AI}(x^d) = \lceil \frac{n}{2} \rceil, 0 \leq d \leq 2^n - 2\}\rvert$ | $\frac{m}{2^n-1}$ | $n$ | $m$ | $\frac{m}{2^n-1}$ |
|---|---|---|---|---|---|
| 3 | 3 | $\approx 0.4286$ | 4 | 4 | $\approx 0.2667$ |
| 5 | 15 | $\approx 0.4839$ | 6 | 12 | $\approx 0.1905$ |
| 7 | 21 | $\approx 0.1654$ | 8 | 48 | $\approx 0.1882$ |
| 9 | 45 | $\approx 0.0881$ | 10 | 260 | $\approx 0.2542$ |
| 11 | 154 | $\approx 0.0752$ | 12 | 1236 | $\approx 0.3018$ |

## References


1. Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345–359. Springer, Heidelberg (2003)
2. Dalai, D.K.: Computing the rank of incidence matrix and algebraic immunity of boolean functions. IACR Cryptology ePrint Archive, p. 273 (2013)
3. Dalai, D.K., Gupta, K.C., Maitra, S.: Results on algebraic immunity for cryptographically significant boolean functions. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 92–106. Springer, Heidelberg (2004)
4. Dalai, D.K., Maitra, S.: Reducing the number of homogeneous linear equations in finding annihilators. In: Gong, G., Helleseth, T., Song, H.-Y., Yang, K. (eds.) SETA 2006. LNCS, vol. 4086, pp. 376–390. Springer, Heidelberg (2006)
5. Didier, F.: Using Wiedemann's algorithm to compute the immunity against algebraic and fast algebraic attacks. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 236–250. Springer, Heidelberg (2006)
6. Feng, X., Gong, G.: On algebraic immunity of trace inverse functions over finite fields with characteristic two. Cryptology ePrint Archive, Report 2013/585 (2013). http://eprint.iacr.org/
7. Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of boolean functions. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 474–491. Springer, Heidelberg (2004)
8. Nawaz, Y., Gong, G., Gupta, K.C.: Upper bounds on algebraic immunity of boolean power functions. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 375–389. Springer, Heidelberg (2006)