On Degree-d Zero-Sum Sets of Full Rank

Christof Beierle*, Alex Biryukov, Aleksei Udovenko†

SnT and CSC, University of Luxembourg, Luxembourg
firstname.lastname@uni.lu

December 10, 2018

Abstract

A set $S \subseteq \mathbb{F}_2^n$ is called degree-d zero-sum if the sum $\sum_{s \in S} f(s)$ vanishes for all n-bit Boolean functions of algebraic degree at most d. Those sets correspond to the supports of the n-bit Boolean functions of degree at most $n-d-1$. We prove some results on the existence of degree-d zero-sum sets of full rank, i.e., those that contain n linearly independent elements, and show relations to degree-1 annihilator spaces of Boolean functions and semi-orthogonal matrices. We are particularly interested in the smallest of such sets and prove bounds on the minimum number of elements in a degree-d zero-sum set of rank n.

The motivation for studying those objects comes from the fact that degree-d zero-sum sets of full rank can be used to build linear mappings that preserve special kinds of *nonlinear invariants*, similar to those obtained from orthogonal matrices and exploited by Todo, Leander and Sasaki for breaking the block ciphers Midori, Scream and iScream.

Keywords: Boolean function, annihilator, orthogonal matrix, nonlinear invariant, trapdoor cipher, symmetric cryptography

1 Introduction

After the introduction of *linear cryptanalysis* in [13] as a powerful method to attack symmetric cryptographic primitives, people started studying how to generalize this method in order to exploit *nonlinear approximations* for cryptanalysis, see, e.g., [6] and [11]. While it might be easier to find a nonlinear approximation over parts of the primitive, e.g., over an S-box of small size, a crucial problem in nonlinear cryptanalysis is to find nonlinear approximations that hold true for the *whole round function* of the primitive. An example that exploits nonlinear approximations that are preserved over the whole round function is *bilinear cryptanalysis* over Feistel ciphers [4].

*The work of Christof Beierle was funded by the *SnT Cryptolux RG* budget.

†The work of Aleksei Udovenko was funded by the *Fonds National de la Recherche* Luxembourg (project reference 9037104).

More recently, an interesting solution for the above problem was described by Todo, Leander and Sasaki in [18] for round functions that can be described in terms of an LS-design [5]. Let one round of a substitution-permutation cipher operating on n S-boxes of t-bit length be given as depicted in Figure 1 and let the linear layer $L^{(t)} \colon \mathbb{F}_2^{nt} \to \mathbb{F}_2^{nt}$ only XOR the outputs of the S-boxes, i.e., each $(y_1, \ldots, y_n)$ for $y_j \in \mathbb{F}_2^t$ is mapped to $(z_1, \ldots, z_n)$ where $z_j = \sum_{i=1}^{n} \alpha_{i,j} y_i$ for particular $\alpha_{i,j} \in \mathbb{F}_2$. In that case, $L^{(t)}$ can be defined by

$$L = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \ldots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n,1} & \alpha_{n,2} & \ldots & \alpha_{n,n} \end{bmatrix} .$$

Todo *et al.* observed that if L is orthogonal, then for *any* t-bit Boolean function f of algebraic degree less than or equal to 2 it is

$$f(y_1) + f(y_2) + \cdots + f(y_n) = f(z_1) + f(z_2) + \cdots + f(z_n) \; . \tag{1}$$

This fact was used to successfully cryptanalyze the block ciphers Midori, Scream and iScream in a weak key setting. Indeed, if f is any invariant function for the S-box S, i.e., if for all $x \in \mathbb{F}_2^t$, $f(x) = f(S(x))$, and if $\deg(f) \leq 2$, one obtains an invariant function for the whole round according to Equation 1.

An interesting question is whether the property of L being orthogonal is also necessary for Equation 1 to hold for all f with degree upper-bounded by 2. More generally, we would like to understand the necessary and sufficient properties of the linear layer that preserve such invariants in the case when $\deg(f) \leq d$ for $d > 2$. Although the existence of a non-trivial[1] linear layer for which Equation 1 holds for all f with $\deg f \leq d$ is totally unclear, such a construction would be of significant interest. On the one hand, it would deepen the knowledge on how to design strong symmetric cryptographic primitives and to avoid possible attacks and could on the other hand be useful in order to design symmetric *trapdoor ciphers* to be used as public-key schemes, see, e.g., [2, 15, 17]. The idea would be to hide a nonlinear approximation as the trapdoor information. If the linear layer is designed such that it preserves *all invariants* of a special form, e.g., all functions of degree at most d, the specification of the linear layer would not leak more information on the particular invariant and thus on the trapdoor. There could also be applications besides cryptography, so the above problem might be of independent interest.

1.1 Our Contribution

In this work we answer the above question and consider the case of $L \in \mathbb{F}_2^{n \times m}$, i.e., the number of outputs (m) might be different than the number of inputs (n). We precisely characterize the matrices that preserve *all* invariants of the form similar as given in Equation 1, i.e.,

$$f(y_1) + \cdots + f(y_n) = f(z_1) + \cdots + f(z_m) + f(0) \cdot (m + n \mod 2) \; , \tag{2}$$

[1] By *non-trivial* we mean that the matrix L is not a permutation matrix.

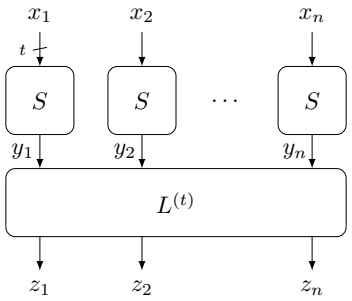

Figure 1: The round function of a substitution-permutation cipher based on an LS-design.

where the degree of f is upper bounded by d and we call such matrices *degree-d sum-invariant*. We show that such matrices can be build from zero-sum sets of rank n, i.e., they correspond to the n-bit Boolean functions of degree at most $n-d-1$ which admit no linear annihilator. This characterization is obtained in Propositions 2, 3 and 4. Our results imply that $m \geq n$ and, for the case of $d = 2$, the property of L being (semi-)orthogonal is not only sufficient, but also necessary. Moreover, we obtain an interesting characterization of orthogonal matrices over $\mathbb{F}_2$, i.e., $L \in \mathbb{F}_2^{n\times n}$ is orthogonal if and only if in every $2 \times 2n$ submatrix of $\left[\begin{array}{c|c} I_n & L \end{array}\right]$, each column occurs an even number of times.

Besides showing the link between degree-d zero-sum sets and degree-d sum-invariant matrices, we study degree-d zero-sum sets of full rank in more detail. We are in particular interested in the smallest of such sets. Let $F(n,d)$ denote the minimum number of elements in a degree-d zero-sum set of rank n. The following theorem summarizes our main results.

Theorem 1. *Let $n, d \in \mathbb{N}$ with $n > d \geq 1$. Then the following properties of $F(n,d)$ hold.*

(i) $F(n,d) = \min\{\mathrm{wt}(g) \mid g \in \mathcal{B}_{n,n-d-1} \setminus \{0\}$ *with* $\dim \mathrm{AN}_1(g) \leq 1\}$.

(ii) $F(n,1) = n + 2 - (n \mod 2)$ *and, for* $n = 4$ *or* $n > 5$, $F(n,2) = 2n$. *As exceptions,* $F(3,2) = 8$ *and* $F(5,2) = 12$.

(iii) $F(d+1,d) = F(d+2,d) = 2^{d+1}$. *Moreover,* $F(d+3,d) = 3 \cdot 2^d$ *and* $F(2d+4,d) = 2^{d+2}$. *For* $d+4 \leq n \leq 2d+3$,

$$F(n,d) = 2^{2d-n+4}(2^{n-d-2} - 1)\ .$$

(iv) for any fixed d, the sequence $F(n,d)$ is increasing, i.e., $F(n+1,d) \geq F(n,d)$.

(v) for $n_1, n_2 > d$, the inequality

$$F(n_1 + n_2, d) \leq F(n_1, d) + F(n_2, d)$$

holds. Moreover, for $d \geq 2$, it is

$$F(n+d, d-1) \leq F(n,d) \leq 2F(n-1, d-1) \ .$$

The last inequality implies that, for $n \geq 4$, $F(n,3) \geq 2n+6$.

We prove the above values by providing a construction of the corresponding zero-sum sets (resp. Boolean functions). In case where we only prove an upper bound, we provide a construction that meets this bound. Table 1 shows the values and bounds for $F(n,d)$ for $n \leq 30$ and $d \leq 10$.

The last inequality in Theorem 1 implies that any degree-d sum-invariant matrix $L \in \mathbb{F}_2^{n \times n}$ for $d \geq 3$ must be a permutation matrix. In other words, the observation of Todo *et al.* cannot be extended for higher-degree invariants without L being expanding.

1.2 Organization

In Section 2, we fix our notation and recall basic properties of Boolean functions. We also recall the observations made in [18] with regard to orthogonal matrices and the preservation of degree-2 invariants. For motivating the remainder of the paper, we directly present an example construction of an expanding linear mapping that preserves higher-degree invariants.

In Section 3, we show equivalent characterizations of degree-d zero-sum sets and explain the links between degree-d sum-invariant matrices and degree-d zero-sum sets.

We study minimal degree-d zero-sum sets in Section 4 and prove the results summarized in Theorem 1. We further summarize the implications to degree-d sum-invariant matrices in Section 5. Finally, the paper is concluded in Section 6.

2 Preliminaries

By $\mathbb{N}$ we denote the set of natural numbers $\{1, 2, \dots\}$ and by $\mathbb{F}_2$ we denote the field with two elements, i.e., $\{0, 1\}$. We represent elements in $\mathbb{F}_2^n$ as row vectors and we denote by e_i the i-th unit vector. For a vector $u = (u_1, \dots, u_n) \in \mathbb{F}_2^n$ let $\mathrm{wt}(u) \coloneqq |\{i \in \{1, \dots, n\} \mid u_i = 1\}|$ denote the *Hamming weight* of u. For a Boolean function f, we denote by $\mathrm{wt}(f)$ the Hamming weight of the value vector of f. For a set $S \subseteq \mathbb{F}_2^n$, the *indicator* of S is defined as the Boolean function $\mathbb{1}_S : \mathbb{F}_2^n \to \mathbb{F}_2$ for which $\mathbb{1}_S(x) = 1$ if and only if $x \in S$.

Let $\mathcal{B}_{n,d}$ denote the set of n-bit *Boolean functions* $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ of algebraic degree at most d. Any Boolean function $f \in \mathcal{B}_{n,d}$ can be uniquely represented as a multivariate polynomial in $\mathbb{F}_2[x_1, \dots, x_n]/(x_1^2 + x_1, \dots, x_n^2 + x_n)$ through its *algebraic normal form (ANF)*. That is,

$$f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u \ ,$$

where $x = (x_1, \dots, x_n), u = (u_1, \dots, u_n)$ and $x^u \coloneqq \prod_{i=1}^n x_i^{u_i}$. Because the algebraic degree is upper bounded by d, it is $a_u = 0$ for all u with $\mathrm{wt}(u) > d$. Any Boolean

function with algebraic degree at most 1 is said to be *affine* and an affine function f with $f(0) = 0$ is said to be *linear*. The algebraic degree of the zero-function is defined to be $-\infty$. We use the symbol $\preceq$ to denote the partial ordering on $\mathbb{F}_2^n$ defined by $x \preceq u$ if and only if, for all $i \in \{1, \ldots, n\}$, $x_i \leq u_i$.

For any two vectors $x, y \in \mathbb{F}_2^n$, we denote by $x \odot y \coloneqq (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_2^n$ the *Hadamard product* of x and y. The *inner product* of x and y is given by

$$\langle x, y \rangle \coloneqq \sum_{i=1}^{n} x_i y_i = \mathrm{wt}(x \odot y) \mod 2 .$$

We generalize this notion to one vector or more than two vectors in the following sense. Let $x_1, \ldots, x_d \in \mathbb{F}_2^n$. Then we define

$$\langle x_1, \ldots, x_d \rangle \coloneqq \sum_{i=1}^{n} \prod_{j=1}^{d} x_{j,i} = \mathrm{wt}(x_1 \odot \cdots \odot x_d) \mod 2 .$$

We use $\mathbb{F}_2^{n \times m}$ to denote the set of matrices in $\mathbb{F}_2$ with n rows and m columns. The $n \times n$ identity matrix will be denoted by I_n. Any matrix $L \in \mathbb{F}_2^{n \times m}$ defines a linear mapping $\varphi \colon \mathbb{F}_2^n \to \mathbb{F}_2^m,\ x \mapsto xL$. We denote by $L^\top$ the transpose of the matrix L. L_i denotes the i-th row of L.

2.1 Higher-Order Derivatives, Affine Equivalence and Algebraic Immunity of Boolean Functions

For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and a vector $\alpha \in \mathbb{F}_2^n$, we denote the function $\delta_\alpha f : \mathbb{F}_2^n \to \mathbb{F}_2$ to be the *derivative* of f with respect to α, given by $\delta_\alpha f(x) \coloneqq f(x) + f(x + \alpha)$. It is well known that $\deg \delta_\alpha f \leq \deg f - 1$ for any Boolean function f and any α, see [12]. The derivation can be iterated multiple times resulting in a *higher-order derivative*. For d linearly independent vectors $\alpha_1, \ldots, \alpha_d \in \mathbb{F}_2^n$ it holds that

$$\delta_{\alpha_1} \ldots \delta_{\alpha_d} f(x) = \sum_{z \in \mathrm{span}(\alpha_1, \ldots, \alpha_d)} f(x + z) .$$

If the vectors $\alpha_1, \ldots, \alpha_d$ are linearly dependent, then the derivative is equal to zero.

Boolean functions have several applications in cryptography, e.g., for designing stream ciphers. In order to resist algebraic attacks, the notion of algebraic immunity was introduced in 2004 as follows.

Definition 1 (Algebraic immunity [14])**.** *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$. An n-bit Boolean function $g \neq 0$ is called an* annihilator *of f, if $fg = 0$. The set of annihilators of f together with $g = 0$ forms a vector space, denoted by $\mathrm{AN}(f)$. We denote by $\mathrm{AN}_d(f)$ the subspace of annihilators of f with algebraic degree at most d together with the zero-function. The* algebraic immunity *of f, denoted $\mathrm{AI}(f)$, is defined as the minimum k for which $\mathrm{AN}_k(f) \cup \mathrm{AN}_k(f + 1) \neq \{0\}$.*

An important concept for Boolean function is the notion of affine equivalence.

Definition 2 (Affine Equivalence)**.** *Two Boolean functions* $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *are called* affine equivalent *if there exists a linear bijection* $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *and a vector* $c \in \mathbb{F}_2^n$ *such that* $g = f \circ (\varphi + c)$*. If* $c = 0$*,* f *and* g *are called* linear equivalent*.*

It is well known that the weight, the algebraic degree and the dimensions of the annihilator spaces (and thus the algebraic immunity) are invariant under affine equivalence.

2.2 Orthogonal Matrices and Preservation of Nonlinear Invariants

In [18], Todo, Leander and Sasaki introduced the *nonlinear invariant attack* and successfully distinguished the block ciphers Midori, Scream and iScream from a random permutation for a significant fraction of weak keys. For an n-bit permutation $G\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, the main idea consists in finding a non-constant n-bit Boolean function f and a constant $\varepsilon \in \mathbb{F}_2$ such that

$$\forall x \in \mathbb{F}_2^n\colon f(x) = f(G(x)) + \varepsilon \ .$$

Such a function f is called an *invariant* for G. In order to find an invariant for the cipher, Todo *et al.* observed that if $L \in \mathbb{F}_2^{n\times n}$ is an orthogonal matrix, i.e., if $\langle xL, yL\rangle = \langle x, y\rangle$ for all $x, y \in \mathbb{F}_2^n$, then for all Boolean functions $f \in \mathcal{B}_{t,2}$ it is

$$\forall X \in \mathbb{F}_2^{t\times n}\colon \sum_{i=1}^{n} f\big((X^\top)_i\big) = \sum_{j=1}^{n} f\big(((XL)^\top)_j\big) \ . \tag{3}$$

In other words, *any* Boolean function $f\colon \mathbb{F}_2^t \to \mathbb{F}_2$ of algebraic degree at most 2 gives rise to an invariant over the linear layers of Midori, Scream and iScream of the form $(x_1, \ldots, x_n) \mapsto f(x_1) + \cdots + f(x_n)$, where n denotes the number of S-boxes, t denotes the bit length of the S-box and $x_i \in \mathbb{F}_2^t$.

We illustrate this from a slightly different point of view on the example of the linear layer used in Midori (see [1]), which is defined by the following matrix:

$$L = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \ . \tag{4}$$

It is easy to see that L is orthogonal. Thus, according to Equation 3, for *any* $f \in \mathcal{B}_{t,2}$ and all $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^t$, the following equation holds:

$$\begin{aligned} &f(x_1) + f(x_2) + f(x_3) + f(x_4) = \\ &f(x_2 + x_3 + x_4) + f(x_1 + x_3 + x_4) + f(x_1 + x_2 + x_4) + f(x_1 + x_2 + x_3) \ . \end{aligned}$$

We now consider an alternative way of proving this. The arguments of f form an affine subspace of dimension 3, namely $x_1 + \mathrm{span}(x_1 + x_2, x_1 + x_3, x_1 + x_4)$. Therefore, the equation is equivalent to

$$\delta_{x_1+x_2}\delta_{x_1+x_3}\delta_{x_1+x_4} f(x_1) = 0 \ , \tag{5}$$

which is clearly true for any $f \in \mathcal{B}_{t,2}$ and any x_1, x_2, x_3, x_4 since all third-order derivatives of a quadratic function are equal to zero. This observation gives new insights on how to generalize the linear layer in order to preserve *higher-degree invariants*.

Proposition 1. *Let $d \geq 2$ be an integer. Then there exists a matrix $L \in \mathbb{F}_2^{n \times m}$ with $n = d + 2, m = 2^{d+1} - d - 2$ and full rank n such that for any $t \geq 1$ and any $f \in \mathcal{B}_{t,d}$, the following property holds:*

$$\forall X \in \mathbb{F}_2^{t \times n} \colon \sum_{i=1}^{n} f\big((X^\top)_i\big) = \sum_{j=1}^{m} f\big(((XL)^\top)_j\big) \,. \tag{6}$$

An example of such L is given by a matrix with columns taken as all vectors from $\mathbb{F}_2^n$ with an odd Hamming weight greater or equal to 3.

Proof. For any $t \geq 1$ and any $x_0, \ldots, x_{d+1} \in \mathbb{F}_2^t$ consider the $(d+1)$-dimensional affine subspace

$$V = x_0 + \operatorname{span}(x_0 + x_1, x_0 + x_2, \ldots, x_0 + x_{d+1}) \,.$$

For any Boolean function f of degree d, any $(d+1)$-th derivative vanishes. Therefore, $\sum_{v \in V} f(v) = 0$. This can be equivalently written as

$$\begin{aligned} & f(x_0) + f(x_1) + \ldots + f(x_{d+1}) = \\ &= \sum_{\substack{I \subseteq \{1,\ldots,d+1\} \\ |I| \geq 2 \text{ even}}} f(x_0 + \sum_{i \in I} x_i) + \sum_{\substack{I \subseteq \{1,\ldots,d+1\} \\ |I| \geq 3 \text{ odd}}} f(\sum_{i \in I} x_i) \\ &= \sum_{\substack{I \subseteq \{0,\ldots,d+1\} \\ |I| \geq 3 \text{ odd}}} f(\sum_{i \in I} x_i) \,. \end{aligned} \tag{7}$$

The right-hand side contains $2^{d+1} - d - 2$ applications of f. Let Y be the set of the linear functions defining the arguments of f in the right-hand side of Equation 7, i.e.,

$$Y = \left\{ \sum_{i \in I} x_i \;\middle|\; I \subseteq \{0, \ldots, d+1\},\ |I| \geq 3 \text{ odd} \right\} \,,$$

and let L be the matrix corresponding to the linear function mapping $(x_0, x_1 \ldots, x_{d+1})$ to $(y_1, y_2 \ldots, y_{2^{d+1}-d-2})$, where $y_i \in Y$ and all y_i are pairwise different. Then, Equation 7 is equivalent to Equation 3 with the described L.

Since $m \geq n \geq 4$, any unit vector from $\mathbb{F}_2^n$ can be expressed a linear combination of 3 columns of L, e.g., $(1,0,0,0,\ldots,0) = (1,1,1,0,\ldots,0) + (1,0,1,1,\ldots,0) + (1,1,0,1,\ldots,0)$. We conclude that L has full rank n. □

Example 1. *For $d = 2$ we obtain the orthogonal matrix given in Equation 4. For $d = 3$ we obtain an expanding linear mapping $\varphi : \mathbb{F}_2^5 \to \mathbb{F}_2^{11}$ defined by the following 5×11*

matrix L:

$$L = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

3 Degree-d Zero-Sum Sets and Sum-Invariant Matrices

A natural question to ask is which other linear mappings have a similar property as given in Equation 6. To answer this question, we study *degree-d zero-sum sets* as a generalization of the above problem.

Definition 3 (Degree-d Zero-Sum Set)**.** *Let $S \subseteq \mathbb{F}_2^n$ and let $d \in \mathbb{N}$. We call S to be* degree-d zero-sum *if, for all $f \in \mathcal{B}_{n,d}$,*

$$\sum_{s \in S} f(s) = 0\,. \tag{8}$$

We define $\mathrm{rank}(S)$ *to be the maximum number of linearly independent elements in S and denote by $\mathrm{ZS}^d_{n\times m}$ the set of degree-d zero-sum sets with m elements and rank n.*

We first show the following equivalent characterizations of degree-d zero-sum sets.

Proposition 2. *Let $S = \{s_1, \ldots, s_k\} \subseteq \mathbb{F}_2^n$ and let $d \in \mathbb{N}$. Let $\mathbb{M}_S \in \mathbb{F}_2^{n\times k}$ be any matrix (up to a permutation of the columns) the columns of which correspond to the elements of S, i.e., $\mathbb{M}_S = \left[\; s_1^\top \;\middle|\; \ldots \;\middle|\; s_k^\top \;\right]$. Then the following statements are equivalent:*

(i) *S is a degree-d zero-sum set.*

(ii) *k is even and, for any choice of d (not necessarily distinct) rows $r_1, \ldots, r_d$ of $\mathbb{M}_S$, it is $\langle r_1, \ldots, r_d\rangle = 0$.*

(iii) *in every $d \times k$ submatrix of $\mathbb{M}_S$, each column occurs an even number of times.*

(iv) $\deg(\mathbb{1}_S) \leq n - d - 1$.

(v) *for all $t \geq 1$ and all $f \in \mathcal{B}_{t,d}$, $\forall X \in \mathbb{F}_2^{t\times n}$: $\sum_{s\in S} f(sX^\top) = 0$.*

In particular, the degree-d zero-sum sets in $\mathbb{F}_2^n$ are exactly the supports of the n-bit Boolean functions of degree at most $n - d - 1$. Therefore, any non-empty degree-d zero-sum set must contain at least 2^{d+1} elements.

Proof. To prove $(i) \Rightarrow (ii)$, let

$$\mathbb{M}_S = \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix}$$

with $r_i \in \mathbb{F}_2^k$. Let $l_1, \ldots, l_d$ be d (not necessarily distinct) row indices and consider the monomial function $f \in \mathcal{B}_{n,d},\ x \mapsto \prod_{i=1}^{d} x_{l_i}$, which has degree d. From Equation 8, it must be

$$0 = \sum_{s \in S} f(s) = \sum_{s \in S} \prod_{i=1}^{d} s_{l_i} = \langle r_{l_1}, \ldots, r_{l_d} \rangle \ .$$

Clearly, k must be even because $\sum_{s \in S} 1 = 0$.

$(ii) \Rightarrow (iii)$: We first see that any $1 \times k$ submatrix of $\mathbb{M}_S$ contains each element in $\mathbb{F}_2$ an even number of times. Indeed, let r be any row in $\mathbb{M}_S$. From (ii) we know that $\mathrm{wt}(r) \mod 2 = \langle r \rangle = 0$ and thus r contains an even number of 1's. Because k is even, it must also contain an even number of 0's. We now use induction on the number of rows. Let $d' < d$ such that $(ii) \Rightarrow (iii)$ holds for d'. Let us choose an arbitrary $(d'+1) \times k$ submatrix $H = [m_{i,j}]_{1 \le i \le d'+1, 1 \le j \le k}$ of $\mathbb{M}_S$. We define $H^{(0)} \coloneqq [m^{(0)}_{i,j}]$ to be the submatrix of H that is obtained by selecting exactly the columns $m_{\star,j}$ of H for which $m_{d'+1,j} = 0$. Similarly, let $H^{(1)} \coloneqq [m^{(1)}_{i,j}]$ be the submatrix of H that is obtained by selecting exactly the columns $m_{\star,j}$ of H for which $m_{d'+1,j} = 1$. We have already seen from the initial step that both $H^{(0)}$ and $H^{(1)}$ must contain an even number of columns (otherwise the row $m_{d'+1,\star}$ would have an odd weight). From (ii), we know that

$$\begin{aligned} 0 &= \langle m_{1,\star}, \ldots, m_{d',\star}, m_{d'+1,\star} \rangle = \langle m^{(0)}_{1,\star}, \ldots, m^{(0)}_{d'+1,\star} \rangle + \langle m^{(1)}_{1,\star}, \ldots, m^{(1)}_{d'+1,\star} \rangle \\ &= \langle m^{(1)}_{1,\star}, \ldots, m^{(1)}_{d',\star} \rangle = \langle m^{(0)}_{1,\star}, \ldots, m^{(0)}_{d',\star} \rangle \ . \end{aligned}$$

Because of the induction hypothesis, $H^{(0)}$ and $H^{(1)}$ contain each column an even number of times and therefore, every column of H occurs an even number of times.

$(iii) \Rightarrow (iv)$: Let $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) \ge n - d$. Because of (iii), $|\{s \in S \mid s \preceq u\}|$ is even. It follows that

$$|\{s \in S \mid s \preceq u\}| \mod 2 = \sum_{s \preceq u} \mathbb{1}_S(s) = 0$$

and thus, the monomial x^u doesn't occur in the ANF of $\mathbb{1}_S$. Since this holds for all u with $\mathrm{wt}(u) \ge n - d$, the algebraic degree of $\mathbb{1}_S$ is at most $n - d - 1$.

$(iv) \Rightarrow (v)$: Let $f \in \mathcal{B}_{t,d}$ be an arbitrary function of degree at most d. Observe that

$$\forall X \in \mathbb{F}_2^{t \times n} \quad \sum_{s \in \mathbb{F}_2^n} \mathbb{1}_S \cdot f(sX^\top) = 0 \ , \tag{9}$$

because $\deg \mathbb{1}_S \cdot (f \circ X) \le \deg \mathbb{1}_S + \deg f \le n-1$. Here, $f \circ X$ denotes the n-bit Boolean function $s \mapsto f(sX^\top)$. Equation 9 can equivalently be written as

$$\forall X \in \mathbb{F}_2^{t \times n} \quad \sum_{s \in S} f(sX^\top) = 0 \ ,$$

which proves (v). The implication $(v) \Rightarrow (i)$ follows by letting $t = n$ and $X = I_n$.

To see that any non-empty degree-d zero-sum set contains at least 2^{d+1} elements, we use the fact that any non-zero Boolean function of degree at most $n-d-1$ has a weight at least $2^{n-(n-d-1)} = 2^{d+1}$. □

It is worth remarking that the property of being degree-d zero-sum is invariant under the application of an injective linear mapping. Indeed, if $\varphi\colon \mathrm{span}(S) \to \mathbb{F}_2^{n'}$ is an injective linear function on the subspace $\mathrm{span}(S)$ of dimension $\mathrm{rank}(S)$, then $|\varphi(S)| = |S|$ and if S is degree-d zero-sum, so is $\varphi(S)$. Further, $\mathrm{rank}(\varphi(S)) = \mathrm{rank}(S)$. Therefore, without loss of generality, we can represent a zero-sum set $S \in \mathrm{ZS}_{n\times m}^d$ as a subset of $\mathbb{F}_2^n$ and given by the columns of an $n \times m$ matrix $\mathbb{M}_S$ of the form

$$\mathbb{M}_S = \left[\ I_n \ \middle|\ L\ \right] \tag{10}$$

for an $L \in \mathbb{F}_2^{n\times(m-n)}$. We say that a zero-sum set (resp. a matrix $\mathbb{M}_S$) given in the representation of Equation 10 is in *systematic form*. We are in particular interested in the properties of such matrices L that define zero-sum sets in $\mathrm{ZS}_{n\times m}^d$ in the above way. For instance, such an L can only exist if m is even. We generalize this by introducing the notion of a *degree-d sum-invariant matrix* as follows.

Definition 4 (Degree-d Sum-Invariant Matrix)**.** *A matrix $L \in \mathbb{F}_2^{n\times m}$ is called* degree-d sum-invariant *if, for all $t \geq 1$ and all $f \in \mathcal{B}_{t,d}$,*

$$\forall X \in \mathbb{F}_2^{t\times n}\colon \sum_{i=1}^{n} f\big((X^\top)_i\big) = \sum_{j=1}^{m} f\big(((XL)^\top)_j\big) + \varepsilon_{m+n} f(0)\ , \tag{11}$$

where $\varepsilon_{m+n} = (m+n) \mod 2$.

Proposition 3. *Let $L \in \mathbb{F}_2^{n\times m}$ be a linear mapping and let $d \in \mathbb{N}$. Then the following statements are equivalent:*

(i) L is degree-d sum-invariant.

(ii) The columns of the matrix $\widehat{\mathbb{M}_L}$ occurring with odd multiplicity define a degree-d zero-sum set, where

$$\begin{cases} \widehat{\mathbb{M}_L} \coloneqq \left[\ I_n \ \middle|\ L\ \right] \in \mathbb{F}_2^{n\times(m+n)}, & \text{if } m+n \text{ is even}\,; \\ \widehat{\mathbb{M}_L} \coloneqq \left[\ I_n \ \middle|\ L \ \middle|\ 0\ \right] \in \mathbb{F}_2^{n\times(m+n+1)}, & \text{if } m+n \text{ is odd}\,. \end{cases} \tag{12}$$

(iii) For all $x_1, \ldots x_d \in \mathbb{F}_2^n$ it is $\langle x_1, \ldots, x_d\rangle = \langle x_1 L, \ldots, x_d L\rangle$.

Moreover, if L fulfills (i) and if $d \geq 2$, then $n \leq m$, $LL^\top = I_n$ and L must have full rank n.

Proof. We first prove $(i) \Rightarrow (ii)$. If $m+n$ is even, then Equation 11 is equivalent to

$$\forall X \in \mathbb{F}_2^{t\times n}\colon \sum_{i=1}^{n} f\big(e_i X^\top\big) + \sum_{j=1}^{m} f\big((L^\top)_j X^\top\big) = 0\ , \tag{13}$$

where e_i denotes the i-th unit vector. If there is a j for which $(L^\top)_j$ is equal to a unit vector e_k, then $f((L^\top)_j X^\top) = f(e_k X^\top)$ and the two terms cancel in Equation 13.

Similarly, if there exist two different j_1, j_2 such that $(L^\top)_{j_1} = (L^\top)_{j_2}$, then $f((L^\top)_{j_1} X^\top)$ and $f((L^\top)_{j_2} X^\top)$ cancel out. This is another way of saying that the columns of the matrix $\widehat{\mathbb{M}_L} = \left[\begin{array}{c|c} I_n & L \end{array}\right]$ occurring with odd multiplicity define a degree-d zero-sum set.

If $m+n$ is odd, then $\varepsilon_{m+n} = 1$ and Equation 11 can be written as

$$\forall X \in \mathbb{F}_2^{t\times n}\colon \sum_{i=1}^{n} f\big(e_i X^\top\big) + \sum_{j=1}^{m} f\big((L^\top)_j X^\top\big) + f(0X^\top) = 0\ .$$

This is equivalent to say that the columns of the $n \times (m+n+1)$ matrix $\widehat{\mathbb{M}_L} = \left[\begin{array}{c|c|c} I_n & L & 0 \end{array}\right]$ occurring with odd multiplicity define a degree-d zero-sum set.

$(ii) \Rightarrow (iii)$. If the columns of $\widehat{\mathbb{M}_L}$ occurring with odd multiplicity define a degree-d zero sum set, then, because of Proposition 2, any d (not necessarily distinct) rows $[e_{l_1} \mid L_{l_1}], \ldots, [e_{l_d} \mid L_{l_d}]$ of $\widehat{\mathbb{M}_L}$ fulfill

$$\langle [e_{l_1} \mid L_{l_1}], \ldots, [e_{l_d} \mid L_{l_d})] \rangle = 0\ ,$$

which is equivalent to $\langle e_{l_1}, \ldots, e_{l_d}\rangle = \langle e_{l_1}L, \ldots, e_{l_d}L\rangle$. Because of the linearity of the inner product, i.e., $\langle x_1 + x_1', x_2, \ldots, x_d\rangle = \langle x_1, x_2, \ldots, x_d\rangle + \langle x_1', x_2, \ldots, x_d\rangle$, the statement follows.

$(iii) \Rightarrow (i)$. If there are $f_1, f_2 \in \mathcal{B}_{t,d}$ such that Equation 11 holds for both f_1 and f_2, then it clearly holds for f_1+1 and for f_1+f_2 as well. Therefore, without loss of generality, let $f \in \mathcal{B}_{t,d}$ be a monomial function, i.e., $f(z) = \prod_{k=1}^{d} z_{l_k}$ for $1 \le l_1 \le \cdots \le l_d \le t$. Let $X \in \mathbb{F}_2^{t\times n}$. Then,

$$\sum_{i=1}^{n} f((X^\top)_i) = \sum_{i=1}^{n}\prod_{k=1}^{d} (X^\top)_{i,l_k} = \langle X_{l_1}, \ldots, X_{l_d}\rangle$$

and

$$\sum_{j=1}^{m} f(((XL)^\top)_j) + \varepsilon_{m+n} f(0) = \sum_{j=1}^{m}\prod_{k=1}^{d} ((XL)^\top)_{j,l_k} = \langle X_{l_1}L, \ldots, X_{l_d}L\rangle\ .$$

It follows that if L preserves all generalized inner products of d elements, then L is degree-d sum-invariant.

If L fulfills the equivalent statements (i) - (iii), then, for all $x, y \in \mathbb{F}_2^n$, it is

$$xy^\top = \langle x, y\rangle = \langle xL, yL\rangle = xL(yL)^\top = xLL^\top y\ .$$

It follows that $LL^\top$ must be the identity and thus, L must have full rank n. □

This result shows a relation between degree-d sum-invariant matrices and semi-orthogonal matrices. A matrix $L \in \mathbb{F}_2^{n\times m}$ with $n \le m$ is called *semi-orthogonal* if $LL^\top = I_n$. Indeed, we have shown that a matrix is degree-2 sum-invariant if and only if

it is semi-orthogonal.[2] Because of the above relation, the degree-$(d+1)$ sum-invariant matrices might also be called *d-th order semi-orthogonal*.

The invertible semi-orthogonal matrices are exactly the *orthogonal* matrices and the orthogonal matrices in dimension n form a multiplicative group, called the *orthogonal group*. With the above equivalences, we obtain an interesting characterization of the orthogonal groups over $\mathbb{F}_2$.

Corollary 1. *A matrix $L \in \mathbb{F}_2^{n\times n}$ is orthogonal if and only if in each $2 \times 2n$ submatrix of $\left[\begin{array}{c|c} I_n & L \end{array}\right]$, each column occurs an even number of times.*

3.1 Relation to Orthogonal Arrays

Proposition 2 points out a relation between degree-d zero-sum sets and orthogonal arrays.

Definition 5 (Orthogonal Array [7])**.** *An $m \times n$ matrix M with entries from a finite set of cardinality k is said to be an* orthogonal array with k levels, strength d and index λ*, denoted $OA(m, n, k, d)$, if every $m \times d$ submatrix of M contains each d-tuple exactly λ times as a row. Without loss of generality, we will assume that M is a matrix with elements in $\mathbb{Z}_k$.*

For our purposes we are only interested in the case of $k = 2$. We directly obtain the following.

Corollary 2. *Let $S \subseteq \mathbb{F}_2^n$. If $\mathbb{M}_S^\top$ is an $OA(|S|, n, 2, d)$ such that 2^{d+1} divides $|S|$ (i.e., if the index λ is even), then S is a degree-d zero-sum set.*

As an example, for $d = 3$, there is a well-known construction of orthogonal arrays from Hadamard matrices (see, e.g., [7, pp. 145–148]). A *Hadamard matrix* of order n is a matrix $H \in \mathbb{Z}^{n\times n}$ which can only take values in $\{-1, 1\}$ and which fulfills $H^\top H = nI_n$. For a matrix M with elements in $\{-1, 1\}$, we denote by $\widetilde{M}$ the $\mathbb{F}_2$ matrix obtained from M by replacing -1 with 0, i.e., we define $\widetilde{M}$ to be the result of $\frac{1}{2}(M + 1)$, interpreted in $\mathbb{F}_2$.

If H is a Hadamard matrix of order $8k$ for $k \in \mathbb{N}$, it is well known that

$$\left[\begin{array}{c} \widetilde{H} \\ \widetilde{-H} \end{array}\right]$$

is an $OA(16k, 8k, 2, 3)$ of even index (see [8, Theorem 4.16]). Therefore, it defines a degree-3 zero-sum set $S \subseteq \mathbb{F}_2^{8k}$ with $16k$ elements. However, its rank can be at most $4k$ (see [16, Proposition 2]) and we are interested in the zero-sum sets of full rank.

[2] We only consider matrices with $n \leq m$. If $L \in \mathbb{F}_2^{n\times m}$ with $n > m$, L would be defined to be semi-orthogonal if $L^\top L = I_m$. Then, L is semi-orthogonal if and only if $L^\top$ is degree-2 sum-invariant.

4 Minimal and Maximal Zero-Sum Sets

In this section we study zero-sum sets of particular rank n and prove results on their existence. We are particularly interested in the smallest of such sets, defined in the following sense.

Definition 6. *We denote by $F(n,d)$ the minimum number $m \in \mathbb{N}$ for which there exists an $S \in \mathrm{ZS}^d_{n\times m}$. We call a zero-sum set* minimal *if it is contained in $\mathrm{ZS}^d_{n\times F(n,d)}$. Analogously, a zero-sum set $S \in \mathrm{ZS}^d_{n\times m}$ is called* maximal *if $\mathrm{ZS}^d_{n'\times m} = \varnothing$ for all $n' > n$.*

Note that $F(n,d)$ is only defined if $n > d$ as otherwise, the only degree-d zero-sum set in $\mathbb{F}_2^n$ is the empty set. We first characterize the zero-sum sets of particular rank n in terms of Boolean functions.

4.1 Relations between Zero-Sum Sets and Affine Annihilators of Boolean Functions

The first three existence results are presented in Propositions 4, 5 and 6 and outline the link between zero-sum sets and the dimensions of degree-1 annihilator spaces of Boolean functions.

Proposition 4. *There exists a degree-d zero-sum set $S \in \mathrm{ZS}^d_{n\times m}$ if and only if there exists a Boolean function $h \in \mathcal{B}_{n,n-d-1}$ with $\mathrm{wt}(h) = m$ and $\dim \mathrm{AN}_1(h) \leq 1$.*

Proof. Let us assume that $S \in \mathrm{ZS}^d_{n\times m}$ is given in systematic form, i.e., it can be represented as in Equation 10. Then, $S = \mathrm{supp}(h)$ for a Boolean function $h \in \mathcal{B}_{n,n-d-1}$ for which $\forall i \in \{1,\ldots,n\} : h(e_i) = 1$. Such a function cannot have a linear annihilator and therefore, any $a \in \mathrm{AN}_1(h) \setminus \{0\}$ must be of the form $a = \ell + 1$ for a linear Boolean function ℓ. It follows that $\dim AN_1(h) \leq 1$.

Let now $h \in \mathcal{B}_{n,n-d-1}$ with $\mathrm{wt}(h) = m$ and $\dim \mathrm{AN}_1(h) \leq 1$. Let $a \in \mathrm{AN}_1(h) \setminus \{0\}$. If $a = \ell + 1$ for a linear function ℓ, then h has no linear annihilator. If a is linear, we fix a constant $c \in \mathbb{F}_2^n$ for which $a(c) = 1$ and consider the function $h_c \colon x \mapsto h(x+c) \in \mathcal{B}_{n,n-d-1}$ which is affine-equivalent to h and thus has the same weight. It is easy to verify that $a+1$ is an affine annihilator for h_c. Because the dimensions of the annihilator spaces are invariant under affine equivalence, h_c has no linear annihilators. Therefore, without loss of generality, we can assume that h has no linear annihilator. Let $S = \mathrm{supp}(h) \subseteq \mathbb{F}_2^n$ be the support of h and consider a matrix $\mathbb{M}_S$ the columns of which form exactly the set S. Since h has no linear annihilator, there is no linear combination of rows of $\mathbb{M}_S$ that is equal to zero. We conclude that $\mathbb{M}_S$ has full rank n and $S \in \mathrm{ZS}^d_{n\times m}$. □

Proposition 5. *Given a function $h \in \mathcal{B}_{n,n-d-1}$ with $\mathrm{wt}(h) = m$ and $\mathrm{AN}_1(h) = \{0\}$, it is possible to construct a zero-sum set in $\mathrm{ZS}^d_{(n+1)\times m}$.*

Proof. Consider the function

$$h' : \mathbb{F}_2^{n+1} \to \mathbb{F}_2, (x_1,\ldots,x_{n+1}) \mapsto x_{n+1}h(x_1,\ldots,x_n) \ .$$

Note that h' has degree at most $n-d$. Further, h' has no linear annihilator. Otherwise, by setting $x_{n+1}=1$, we would obtain that h has an annihilator of algebraic degree 1, contradicting $\mathrm{AN}_1(h)=\{0\}$. By Proposition 4, we can construct $S\in \mathrm{ZS}^d_{(n+1)\times m}$. □

A converse statement is true for maximal zero-sum sets.

Proposition 6. *Let $n\geq 2$ and let $S\in \mathrm{ZS}^d_{(n+1)\times m}$ be maximal. Then, $\mathbb{1}_S$ is linear equivalent to a function $h\in\mathcal{B}_{n+1,n-d}$ of the form*

$$h(x_1,\ldots,x_{n+1}) = x_{n+1}\cdot g(x_1,\ldots,x_n)\ , \tag{14}$$

where $g\in\mathcal{B}_{n,n-d-1}$ with $\mathrm{wt}(g)=\mathrm{wt}(h)=m$ and $\mathrm{AN}_1(g)=\{0\}$. Further, if $m<2^{n-1}$, then $\mathrm{AI}(g)\geq 2$.

Proof. Let $\mathbb{M}_S$ be a matrix which columns correspond to the elements of S. Because S is maximal, the vector subspace of $\mathbb{F}_2^m$ spanned by the rows of $\mathbb{M}_S$ must contain the all-1 vector $1_m \coloneqq (1,1,\ldots,1)$. Otherwise, one would obtain a zero-sum set in $\mathrm{ZS}^d_{(n+2)\times m}$ defined by the matrix

$$\begin{bmatrix} \mathbb{M}_S \\ 1_m \end{bmatrix}.$$

Therefore, we can apply a linear permutation A on the columns of $\mathbb{M}_S$ such that $\mathbb{1}_{A(S)} = h$ where $h\in\mathcal{B}_{n+1,n-d}$ is of the form as given in Equation 14 with $g\in\mathcal{B}_{n,n-d-1}$ and $\mathrm{wt}(g)=\mathrm{wt}(h)$. It is left to show that $\mathrm{AN}_1(g)=\{0\}$.

Clearly, g cannot have a linear annihilator. We assume now that g has an annihilator of degree 1 of the form $(x_1,\ldots,x_n)\mapsto 1+\sum_{i=1}^n a_i x_i$. Then, $g(x)=0$ for all x with $\sum_{i=1}^n a_i x_i = 0$. Let j be such that $a_j=1$. For the linear permutation $Q:\mathbb{F}_2^n\to\mathbb{F}_2^n$, $Q(x_1,\ldots,x_n)=(x_1,\ldots,x_{j-1},\sum_{i=1}^n a_i x_i, x_{j+1},\ldots,x_n)$, we have

$$g(Q(x_1,\ldots,x_n)) = x_j\cdot g'(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$$

for a function $g'\in\mathcal{B}_{n-1,n-d-2}$. But this means that h is linear-equivalent to a function of the form $(x_1,\ldots,x_{n+1})\mapsto x_{n+1}\cdot x_n\cdot g'(x_1,\ldots,x_{n-1})$, which has a linear annihilator $x_{n+1}+x_n$. We get a contradiction and conclude that $\mathrm{AN}_1(g)=\{0\}$.

If $m<2^{n-1}$, it is easy to see that $g+1$ cannot admit an annihilator of algebraic degree 1. Suppose that $a\in\mathrm{AN}_1(g+1)\setminus\{0\}$. Then, $\mathrm{wt}(a)=2^{n-1}$ and $ag=a$, which is impossible. □

As Proposition 6 only holds for maximal zero-sum sets we cannot use it to establish an equivalence between minimal degree-d zero-sums of rank $n+1$ and n-bit Boolean functions of degree $n-d-1$ with algebraic immunity at least 2 and minimum weight. We therefore propose the following question:

Question 1. *Let $S\in\mathrm{ZS}^d_{n\times m}$ be minimal. What are necessary and sufficient conditions for S to be maximal?*

4.2 Minimal Zero-Sum Sets: Bounds and Values for $F(n, d)$

In order to derive values for $F(n, d)$, we basically have to study the Boolean functions that admit at most one annihilator of algebraic degree 1 and find those of minimum weight. Indeed, from Proposition 4, we know that

$$F(n,d) = \min\{\mathrm{wt}(g) \mid g \in \mathcal{B}_{n,n-d-1} \setminus \{0\} \text{ with } \dim \mathrm{AN}_1(g) \leq 1\} .$$

For $d = 1$ and $d = 2$ we can easily determine the cardinalities of minimal degree-d zero-sum sets, as stated in Propositions 7 and 8. The proofs also provide a construction for a minimal zero-sum set. While the proof for $d = 1$ is rather trivial, the proof for $d = 2$ relies on the relation between degree-2 zero-sum sets and semi-orthogonal matrices.

Proposition 7. *For $n \geq 2$, $F(n, 1) = n + 2 - (n \mod 2)$.*

Proof. Consider a zero-sum set $S \in \mathrm{ZS}^1_{n\times m}$ and its matrix in systematic form. Each row must have an even weight, therefore there must be at least one extra column besides the identity part, i.e. $m \geq n + 1$. Furthermore, m must be even and the proposition follows. □

Proposition 8. *For $n = 4$ and for $n > 5$, it is $F(n, 2) = 2n$. Further, $F(3, 2) = 8$ and $F(5, 2) = 12$.*

Proof. Let $n \geq 3$ and m be minimal such that there exists an $S \in \mathrm{ZS}^2_{n\times m}$. Let further $L \in \mathbb{F}_2^{n\times(m-n)}$ such that S is in systematic form with $\mathbb{M}_S = [I_n|L]$. As $\mathbb{M}_S$ cannot contain any repeated columns, it is $\mathbb{M}_S = \widehat{\mathbb{M}_L}$ and thus, L must be semi-orthogonal and $n \leq (m - n)$. It follows that $F(n, 2) = m \geq 2n$.

Let now $n = 4$ or $n \geq 6$. To prove the existence of an $S \in \mathrm{ZS}^2_{n\times 2n}$, we observe that if $L \in \mathbb{F}_2^{n\times n}$ is an orthogonal matrix for which each column has weight larger than 1, $\widehat{\mathbb{M}_L}$ defines a degree-2 zero-sum set of size $2n$ and rank n according to Proposition 3. It is left to show that, for any dimension $n = 4$ or $n \geq 6$, there exists an orthogonal matrix for which no column corresponds to a unit vector. We are going to distinguish four cases. Let us define the orthogonal matrices M_4 and M_6 as

$$M_4 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \quad M_6 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} .$$

Case 1 ($n = 0 \mod 4$): The block-diagonal matrix $\mathrm{diag}(M_4, \ldots, M_4)$ which contains M_4 as its diagonal blocks is orthogonal and each column weight is equal to 3.

Case 2 ($n = 2 \mod 4$): Because $n > 5$, it is $n = 4k + 6$ for $k \geq 0$ and the matrix $\mathrm{diag}(M_6, M_4, M_4, \ldots, M_4)$ is orthogonal and each column has weight at least 3.

Case 3 ($n = 3 \mod 4$): Because $n > 5$, it is $n = 4k+3$ for $k \geq 1$ and the two matrices $D_1 = \mathrm{diag}(1, 1, 1, M_4, M_4, \ldots, M_4)$ and $D_2 = \mathrm{diag}(M_4, 1, 1, \ldots, 1)$ are orthogonal. Their product is orthogonal and of the form

$$D_1 D_2 = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & \ldots & 0 \\ \hline \multicolumn{4}{c|}{\mathrm{A}} & \multicolumn{4}{c}{\mathrm{D}} \end{array}\right], \tag{15}$$

where D is the $4k \times (4k-1)$ submatrix of $\mathrm{diag}(M_4, \ldots, M_4)$ omitting the first column. It is obvious that each column has weight at least 3.

Case 4 ($n = 1 \mod 4$): Because $n > 5$, it is $n \geq 9$ and $n = 4k + 6 + 3$ for $k \geq 0$. The two matrices $D_1 = \mathrm{diag}(1, 1, 1, M_6, M_4, \ldots, M_4)$ and $D_2 = \mathrm{diag}(M_4, 1, 1, \ldots, 1)$ are orthogonal. Their product is orthogonal and of the form given in Equation 15 with D as the $(4k+6) \times (4k+6-1)$ submatrix of $\mathrm{diag}(M_6, M_4, M_4, \ldots, M_4)$ omitting the first column. It is obvious that each column has weight at least 3.

For $n = 3$ we use that any degree-d zero-sum set must contain at least 2^{d+1} elements. Thus, $F(n, 2) \geq 8$. We obtain $F(3, 2) = 8$ because $\mathbb{F}_2^3$ is a degree-2 zero-sum set.

For $n = 5$, assume that there exists an orthogonal matrix $L \in \mathbb{F}_2^{5\times 5}$ which does not have a unit vector as its row (or column). From point (*iii*) of Proposition 2 it follows that any 2×5 submatrix of L must contain an odd number of columns equal to each of $(0, 1), (1, 0), (0, 0)$ and an even number of columns equal to $(1, 1)$ (same applies for rows of any 5×2 submatrix of L). It follows that, up to a permutation of rows, L has the following form:

$$L = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & . & . & . \\ 1 & 1 & . & . & . \\ 1 & 1 & . & . & . \end{bmatrix}. \tag{16}$$

It is easy to see that it is not possible to complete this matrix such that all 2×5 and 5×2 submatrices satisfy the condition. Therefore, $F(5, 2) > 10$. Moreover, it is easy to verify that

$$\mathbb{M}_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

defines a zero-sum set in $\mathrm{ZS}^2_{5\times 12}$, thus $F(5, 2) = 12$. □

Proposition 9 below presents a simple way to construct a $d+1$ zero-sum set of rank $n+1$ from a degree-d zero-sum set of rank n. This construction might be used to derive an upper bound on $F(n, d)$.

Proposition 9. *If there exists an $S \in \mathrm{ZS}^d_{n\times m}$, one can construct a zero-sum set $S' \in \mathrm{ZS}^{d+1}_{(n+1)\times 2m}$. In particular, for $n > d+1$, $F(n, d) \leq 2F(n-1, d-1)$.*

Proof. If $S \in \mathrm{ZS}^d_{n\times m}$, then the columns of the matrix

$$\left[\begin{array}{c|c} 0\ \ldots\ 0 & 1\ \ldots\ 1 \\ \mathbb{M}_S & \mathbb{M}_S \end{array}\right]$$

define a degree-$(d+1)$ zero-sum set S' with $2m$ elements of rank $n+1$. We remark that both sets S and S' have essentially the same indicator function, only the domain dimension is different. □

Note that the upper bound on $F(n,d)$ given by this construction is not always tight. Let $S \subseteq \mathbb{F}_2^9$ be such that $\mathbb{1}_S(x) = x_1(x_2x_3x_4x_5 + x_6x_7x_8x_9)$. It easy to verify that $S \in \mathrm{ZS}^3_{9\times 30}$. It follows that $F(9,3) \leq 30 \neq 2F(8,2) = 32$. The corresponding matrix $\mathbb{M}_S$ is given by:

$$\mathbb{M}_S = \left[\begin{array}{cccccccccccccccccccccccccccccc}
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&1&1&1&0&0&0&0&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right].$$

Proposition 10. *For any $d \in \mathbb{N}$ and $n_1, n_2 > d$, $F(n_1+n_2, d) \leq F(n_1, d) + F(n_2, d)$.*

Proof. If $S_1 \in \mathrm{ZS}^d_{n_1\times m_1}, S_2 \in \mathrm{ZS}^d_{n_2\times m_2}$, then the columns of the matrix

$$\mathbb{M}_S = \left[\begin{array}{c|c} & 0\ \ldots\ 0 \\ \mathbb{M}_{S_1} & \vdots \\ & 0\ \ldots\ 0 \\ \hline 0\ \ldots\ 0 & \\ \vdots & \mathbb{M}_{S_2} \\ 0\ \ldots\ 0 & \end{array}\right]$$

repeating an odd number of times define a degree-d zero-sum set S with at most m_1+m_2 elements of rank n_1+n_2. More precisely, if both S_1 and S_2 contain the zero vector, then the resulting zero-sum set has size m_1+m_2-2 due to the zero-vector being cancelled by the repetition. Otherwise, S has size m_1+m_2. □

Proposition 11. *Let $d \geq 2$. If there exist an $S \in \mathrm{ZS}^d_{n\times m}$, one can construct a zero-sum set in $\mathrm{ZS}^{d-1}_{(n+d)\times m}$. In particular, for $n > d$, $F(n,d) \geq F(n+d, d-1)$.*

Proof. Let $\mathbb{M}_S = \left[\ I_n | L\ \right]$ be a matrix for S in systematic form. By reordering the rows of $\mathbb{M}_S$, one can bring it into the form

$$\left[\begin{array}{c|c|c|c} 1\ldots1 & 1 & 0\ldots0 & 0\ldots0 \\ A & 0 & B & I_{n-1} \end{array}\right], \tag{17}$$

where $A \in \mathbb{F}_2^{(n-1)\times m_1}$ and $B \in \mathbb{F}_2^{(n-1)\times m_2}$ for some m_1, m_2 with $m_1 + m_2 + n = m$. Moreover, m_1 cannot be zero because the first row must have an even weight. We see that $\left[\begin{array}{c|c} A & 0 \end{array}\right]$ must define a degree-$(d-1)$ zero-sum set in $\mathbb{F}_2^{n-1}$, i.e., $\left[\begin{array}{c|c} A & 0 \end{array}\right] = \mathbb{M}_T$ for a $T \in \mathrm{ZS}^{d-1}_{r\times(m_1+1)}$. This is simply because the Hadamard product of any $d-1$ rows of $\left[\begin{array}{c|c} A & 0 \end{array}\right]$ can be expressed as the Hadamard product of d rows of $\mathbb{M}_S$, i.e., the $d-1$ rows at the same positions as those of $\left[\begin{array}{c|c} A & 0 \end{array}\right]$ and the first row $[11\ldots100\ldots0]$. We conclude that $m_1 = |T| \geq 2^d$ and thus, $r \geq d$.

Let $v_1, \ldots, v_d$ be d linearly independent rows of A and consider the matrix

$$\left[\begin{array}{c|c|c|c} 1\ldots1 & 1 & 0\ldots0 & 0\ldots0 \\ A & 0 & B & I_{n-1} \\ v_1 & 0 & 0\ldots0 & 0\ldots0 \\ v_2 & 0 & 0\ldots0 & 0\ldots0 \\ \vdots & \vdots & \vdots & \vdots \\ v_d & 0 & 0\ldots0 & 0\ldots0 \end{array}\right],$$

which must define a zero-sum set in $\mathrm{ZS}^{d-1}_{(n+d)\times m}$ by the same argument as above, i.e., the Hadamard product of any $d-1$ rows can be expressed as the Hadamard product of d rows of $\mathbb{M}_S$. It is also easy to see that no linear combination of rows can be equal to zero, i.e. the constructed set has full rank $n+d$. □

Using the above result and Proposition 8, we can prove a lower bound on $F(n,3)$ as follows.

Corollary 3. *For $n \geq 4$ it is $F(n,3) \geq 2n+6$.*

So far, we were able to characterize the minimal degree-d zero-sum sets for $d = 1$ and $d = 2$ and proved some inequalities for the general case. Further, we can use the following classification theorem by Kasami, Tokura and Azumi in order to derive some more exact values of $F(n,d)$.

Theorem 2 ([9, 10])**.** *Let $r \geq 2$ and let $f \in \mathcal{B}_{n,r} \setminus \{0\}$ with $\mathrm{wt}(f) < 2^{n-r+1}$. Then f is affine equivalent to either (i) or (ii), where*

(i) $f = x_1 \ldots x_{r-2}(x_{r-1}x_r + x_{r+1}x_{r+2} + \ldots + x_{r+2\ell-3}x_{r+2\ell-2}), n \geq r + 2\ell - 2$

(ii) $f = x_1 \ldots x_{r-\ell}(x_{r-\ell+1} \ldots x_r + x_{r+1} \ldots x_{r+\ell}), r \geq \ell, n \geq r + \ell$.

A direct application leads to the following results.

Proposition 12 (Values of $F(n,d)$ for $n \leq 2d+4$)**.** *(i)* $F(d+1,d) = 2^{d+1}$.

(ii) $F(d+2,d) = 2^{d+1}$ *and the minimal zero-sum sets in $\mathbb{F}_2^{d+2}$ correspond to the Boolean functions of algebraic degree* 1.

(iii) $F(d+3,d) = 3 \cdot 2^d$ *and the minimal zero-sum sets in $\mathbb{F}_2^n$ correspond to the Boolean functions affine equivalent to $x \mapsto x_1x_2 + x_3x_4$.*

(iv) *For* $d+4 \leq n \leq 2d+3$, $F(n,d) = 2^{2d-n+4}(2^{n-d-2}-1) = \mathrm{wt}(h_{n,d})$, *where*

$$r = n-d-1, h_{n,d}\colon (x_1,\ldots,x_n) \mapsto x_1(x_2x_3\ldots x_r + x_{r+1}x_{r+2}\ldots x_{2r-1}) \ .$$

(v) $F(2d+4,d) = 2^{d+2} = \mathrm{wt}(g_d)$, *where:*

$$g_d\colon (x_1,\ldots,x_{2d+4}) \mapsto x_1(x_2x_3\ldots x_{d+3} + (x_2+1)x_{d+4}x_{d+5}\ldots x_{2d+4}) \ .$$

Proof. For $d \in \mathbb{N}, d < n$, let us define the set

$$S_{n,d} \coloneqq \{g \in \mathcal{B}_{n,d} \setminus \{0\} \text{ with } \dim \mathrm{AN}_1(g) \leq 1\} \ .$$

From Proposition 4 we know that $F(n,d) = \min\{\mathrm{wt}(g) \mid g \in S_{n,n-d-1}\}$. Therefore, we trivially obtain $F(d+1,d) = 2^{d+1}$. $S_{d+2,1}$ is the set of $(d+2)$-bit Boolean functions of algebraic degree 1 (together with the constant-1 function) and thus $F(d+2,d) = 2^{d+1}$.

To obtain the minimum weight of functions in $S_{d+3,2}$, we first note that every Boolean function of algebraic degree 2 of the minimum weight 2^{d+1} must be affine equivalent to a monomial function, i.e., $x \mapsto x_1x_2$ (see Proposition 12 of [3]). As this monomial function admits the annihilators $x \mapsto x_1+1$ and $x \mapsto x_2+1$, the minimum weight in $S_{d+3,d}$ must be at least $2^{d+2}-2^d$ (see, e.g., [3, p. 70] for the possible weights of quadratic Boolean functions). This weight is obtained by the function $x \mapsto x_1x_2+x_3x_4$, which clearly is in $S_{d+3,2}$. To see that all other functions in $S_{d+3,2}$ of minimum weight are affine equivalent to it, it is enough to see that all of the functions $q_{n,\ell}\colon (x_1,\ldots,x_n) \mapsto x_1x_2+x_3x_4+\cdots+x_{2\ell-1}x_{2\ell}$ with $\ell \geq 3$ have a strictly larger weight. Indeed, by induction on ℓ, it can be easily shown that $\mathrm{wt}(q_{n,\ell}) = 2^{n-1}-2^{n-\ell-1}$.

Let now $d+4 \leq n \leq 2d+3$. It is easy to see that $h_{n,d} \in S_{n,n-d-1}$. Further, its weight can be computed as

$$\mathrm{wt}(h_{n,d}) = 2^{d+1}+2^{d+1}-2^{2d-n+4} = 2^{2d-n+4}(2^{n-d-2}-1) \ .$$

It is left to show that $h_{n,d}$ is an element of minimum weight in $S_{n,n-d-1}$. Let therefore be $h' \in S_{n,n-d-1}$ with $\mathrm{wt}(h') \leq \mathrm{wt}(h_{n,d})$. Since $\mathrm{wt}(h_{n,d}) < 2^{n-(n-d-1)+1} = 2^{d+2}$ the assumptions of Theorem 2 are fulfilled and h' would be affine equivalent to one of the forms given in cases (i) and (ii) of Theorem 2. If $n \geq d+5$, Case (i) corresponds to a Boolean function of the form $x \mapsto x_1x_2g$ which admits $x \mapsto x_1+1$ and $x \mapsto x_2+1$ as degree-1 annihilators. For $n = d+4$, Case (i) corresponds to a function of the form $x \mapsto x_1(x_2x_3+x_4x_5+\cdots+x_{2\ell}x_{2\ell+1}) = x_1g$ for $g \in S_{n,2}$ and, therefore, its weight must be at least $2^{n-2}-2^{n-4} = 2^{2d-n+4}(2^{n-d-2}-1)$.

Otherwise, h' must be affine equivalent to one of the functions given in Case (ii). Since it cannot admit two annihilators of algebraic degree 1, it must be affine equivalent to either $x \mapsto x_1(x_2x_3\ldots x_r+x_{r+1}x_{r+2}\ldots x_{2r-1}) = h_{n,d}$ or $g_{n,d}\colon x \mapsto x_1x_2\ldots x_r+x_{r+1}x_{r+2}\ldots x_{2r}$, where $r = n-d-1$. As $\mathrm{wt}(g_{n,d}) = 2^{2d-n+3}(2^{n-d-1}-1) > \mathrm{wt}(h_{n,d}) = 2^{2d-n+3}(2^{n-d-1}-2)$, statement (iv) follows.

It is easy to see that $\mathrm{wt}(g_d) = 2^{d+2}$, i.e. $F(2d+4,d) \leq 2^{d+2}$. By Proposition 9 and (iv) of this proposition, $F(2d+4,d) \geq F(2d+5,d+1)/2 = (2^{d+2}-1)$. Since $F(2d+4,d)$ has to be even, statement (v) follows. □

We are now going to show that, for any fixed d, the sequence $F(n,d)$ is increasing with n. For that, we need the following lemma.

Lemma 1. *For $n > 2d+3$, we have $F(n,d) \leq \frac{2^n}{n+1}$.*

Proof. By repeatedly applying Proposition 9 and by Proposition 8, we obtain

$$F(n,d) \leq 2^{d-1}(n-d+2) = 2^n \frac{n-d+2}{2^{n-d+1}} \ .$$

It is left to show that $\frac{n-d+2}{2^{n-d+1}} \leq \frac{1}{n+1}$. We know that

$$(n+1)(n-d+2) < (2n-2d-2)(n-d+2) = 2(n-d-1)(n-d+2) \leq 2^{n-d+1} \ ,$$

which is true for $n-d \geq 5$. The latter is guaranteed by $n \geq 2d+4$ and $d \geq 1$. This proves the statement. □

Proposition 13. *For $n > d+1$, it is $F(n,d) \geq F(n-1,d)$.*

Proof. We prove this statement by induction on d. If $d = 1$ and $d = 2$, the statement is obviously true by Propositions 7 and 8. Let thereby $d \geq 3$ and assume that the statement is true for $d-1$.

Let $S \in \mathrm{ZS}^d_{n\times m}$ be a minimal zero-sum set, i.e., $m = F(n,d)$, such that $\mathbb{M}_S$ can be given as in Equation 17 for $A \in \mathbb{F}_2^{(n-1)\times m_1}$ and $B \in \mathbb{F}_2^{(n-1)\times m_2}$ with m_1, m_2 such that $m_1 + m_2 + n = m$. Let $m' \coloneqq m_2 + n - 1$. We see that $[B|I_{n-1}]$ must define a degree-$(d-1)$-zero-sum set in $\mathbb{F}_2^{n-1}$, i.e., $[B|I_{n-1}] = \mathbb{M}_T$ for a $T \in \mathrm{ZS}^{d-1}_{(n-1)\times m'}$. This is because every $(d-1)\times m'$ submatrix of $\mathbb{M}_T$ must occur an even number of times (from the property of S being a degree-d zero-sum set) and, since $\mathbb{M}_T$ contains I_{n-1}, it must have rank $n-1$. We now distinguish two cases.

Case 1 ($m' \leq \frac{m}{2}$): In that case we directly obtain

$$m = F(n,d) \geq 2F(n-1,d-1) \geq 2F(n-2,d-1) \geq F(n-1,d) \ ,$$

where the second estimation follows from the induction hypothesis and the last one follows from Proposition 9.

Case 2 ($m' > \frac{m}{2}$): We first remark that if $n \leq 2d+3$, the statement directly follows from Proposition 12. For example, for $n \geq d+5$,

$$F(n,d) = 2^{d+2} - 2^{2d-n+4} \geq 2^{d+2} - 2^{2d-n+5} = F(n-1,d) \ .$$

Let us therefore assume that $n > 2d+3$. Note that in the matrix $\mathbb{M}_S$, we can add the first row $[11\ldots100\ldots0]$ to any other row and would obtain an equivalent zero-sum set. This operation does not change the right part of $\mathbb{M}_S$ containing I_{n-1}. Indeed, it allows us to obtain a zero-sum set $S_c \in \mathrm{ZS}^d_{n\times m}$ represented by

$$\mathbb{M}_{S_c} = \left[\begin{array}{c|c|c|c} 1\ldots1 & 1 & 0\ldots0 & 0\ldots0 \\ A + c^\top & c^\top & B & I_{n-1} \end{array}\right]$$

for any $c \in \mathbb{F}_2^{n-1}$. Let us denote by R the set of columns of A together with the zero column vector. Our statement to prove follows if we can guarantee the existence of a vector $\tilde{c}$ such that, for all $v \in (R + \tilde{c}^\top)$, $\mathrm{wt}(v) \geq 2$. Then, we would obtain a zero-sum set in $\mathrm{ZS}^d_{(n-1)\times m''}$ defined by

$$\left[\ A + \tilde{c}^\top \ \middle|\ \tilde{c}^\top \ \middle|\ B \ \middle|\ I_{n-1}\ \right]$$

as there won't be any cancellation between $[A + \tilde{c}^\top \mid c^\top]$ and I_{n-1}. Indeed, such a vector must always exist. Assume that, for all $c \in \mathbb{F}_2^{n-1}$, there exists a $v \in (R + \tilde{c}^\top)$ with weight at most 1. This is equivalent to say that the covering radius of the set R is equal to 1. By a simple counting argument it follows that $|R| \geq \frac{2^{n-1}}{n}$. On the other hand, it is

$$|R| = m - m' < F(n,d) - \frac{F(n,d)}{2} = \frac{1}{2}F(n,d) \leq \frac{2^{n-1}}{n+1}\ ,$$

where the last inequality follows from the previous lemma. □

5 Implications for Degree-*d* Sum-Invariant Matrices

In this section, we point out the implications of the above results on degree-d sum-invariant matrices. The most interesting implication is that any bijective degree-3 sum-invariant matrix must be trivial. As the linear layer of a block cipher based on an LS-design certainly has to be bijective, this shows that one cannot extend the observation of Todo *et al.* to invariants of degree higher than two.

Corollary 4. *Let $L \in \mathbb{F}_2^{n\times n}$ be a degree-d sum-invariant matrix for $d \geq 3$. Then L must be a permutation matrix.*

Proof. Let us assume a degree-3 sum-invariant matrix $L \in \mathbb{F}_2^{n\times n}$ and let $\widehat{\mathbb{M}_L}$ be given by

$$\widehat{\mathbb{M}_L} = \left[\ I_n \ \middle|\ L\ \right] \in \mathbb{F}_2^{n\times 2n}\ .$$

By Proposition 3, the columns of $\widehat{\mathbb{M}_L}$ occurring an odd number of times correspond to a degree-3 zero-sum set $S \subseteq \mathbb{F}_2^n$. Note that the unit columns of I_n do not repeat inside I_n. Therefore, after removing the even occurrences of each column, the number of columns left in I_n will be not smaller than the number of columns left in L. It follows that $\mathrm{rank}(S) \geq |S|/2$. This is only possible if S is empty and thus L is a permutation matrix. □

Consider a degree-d sum-invariant matrix L and consider the matrix $\widehat{\mathbb{M}_L}$ defined as in Proposition 3:

$$\begin{cases} \widehat{\mathbb{M}_L} \coloneqq \left[\ I_n \ \middle|\ L\ \right] \in \mathbb{F}_2^{n\times(m+n)}, & \text{if } m+n \text{ is even;} \\ \widehat{\mathbb{M}_L} \coloneqq \left[\ I_n \ \middle|\ L \ \middle|\ 0\ \right] \in \mathbb{F}_2^{n\times(m+n+1)}, & \text{if } m+n \text{ is odd,} \end{cases} \tag{18}$$

where it is shown that the columns of $\widehat{\mathbb{M}_L}$ occurring and odd number of times define a degree-d zero-sum set. Because of the cancellations, the size and the rank of the zero-sum set may be lower. We deduce the following decomposition of sum-invariant matrices.

Proposition 14. *Let $L \in \mathbb{F}_2^{n\times m}$ be a degree-d sum-invariant matrix such that no column of L is equal to zero. Then, up to permutations of rows and columns, L can be expressed in the following form:*

$$L = \left[\begin{array}{c|c|c|c} A & \begin{array}{c} 0 \\ \hline I_k \end{array} & M & M \end{array}\right], \tag{19}$$

where k, t are some integers, $M \in \mathbb{F}_2^{n\times t}$, $A \in \mathbb{F}_2^{n\times(m-2t-k)}$, and the columns of A do neither contain unit vectors nor repetitive columns. Such integers k, t are unique. Consider the matrix $\widehat{A}$:

$$\begin{cases} \widehat{A} \coloneqq \left[\begin{array}{c|c} \begin{array}{c} I_{n-k} \\ \hline 0 \end{array} & A \end{array}\right] \in \mathbb{F}_2^{n\times(m+n-2t-2k)}, & \text{if } m+n \text{ is even;} \\ \widehat{A} \coloneqq \left[\begin{array}{c|c|c} \begin{array}{c} I_{n-k} \\ \hline 0 \end{array} & A & 0 \end{array}\right] \in \mathbb{F}_2^{n\times(m+n-2t-2k+1)}, & \text{if } m+n \text{ is odd.} \end{cases} \tag{20}$$

The columns of the matrix $\widehat{A}$ are pairwise distinct and form a degree-d zero-sum set.

Proof. The columns of $\widehat{\mathbb{M}_L}$ occurring an odd number of times form a degree-d zero-sum set. The columns of I_n may only cancel with columns from L. Let k be the number of unit vectors occurring an odd number of times in L. Let A be the matrix consisting of the columns of L that are repeated an odd number of times and which are not unit vectors. It follows that L can be expressed in the form given in Equation 19. Now consider the matrix $\widehat{\mathbb{M}_L}$. After removing even repetitions of columns, the matrix will be equal to $\widehat{A}$. It follows that the columns of $\widehat{A}$ define a degree-d zero-sum set.

To show uniqueness of k, t, first recall that A must not contain unit vectors. It follows that all columns of L occurring an even number of times must be in M, and all columns occurring an odd number of times must be either in A or in I_k depending only on the column weight. □

5.1 Minimum Expansion Rate

We have shown that for $d \geq 3$, there exist no bijective degree-d sum-invariant matrices. However, there exist rectangular degree-d sum-invariant matrices resulting in expanding linear mappings. A natural problem would be to find a degree-d sum-invariant matrix with a minimum expansion rate.

Definition 7 (Expansion Rate)**.** *The* expansion rate *of a matrix $L \in \mathbb{F}_2^{n\times m}$ is the ratio $\frac{m}{n}$.*

Note that, given a degree-d sum-invariant matrix $L \in \mathbb{F}_2^{n\times m}$, we can always build a a degree-d sum-invariant matrix in $\mathbb{F}_2^{(n+1)\times(m+1)}$ of the form

$$\begin{bmatrix} L & 0 \\ 0 & 1 \end{bmatrix}.$$

Therefore, by repetitively extending any matrix L by unit vectors in the above way, we can construct a matrix with an expansion rate arbitrarily close to 1. Indeed, the permutation matrices have an expansion rate of exactly 1. Therefore, by the *minimum expansion rate* for a degree-d sum-invariant matrix of fixed d, we refer to the minimum expansion rate over all degree-d sum-invariant matrices that do not contain a unit vector as a column.

It is clear that for $d = 2$ the minimum expansion rate is 1 and is achieved by orthogonal matrices. For $d \geq 3$ the minimum expansion rate is an open problem. It corresponds to the minimum value of $\frac{F(n,d)}{n} - 1$. Among the established values of $F(n, d)$ the minimum expansion rate is achieved for $F(d+2, d) = 2^{d+1}$, i.e. by the matrices from the construction given in Proposition 1. We conjecture that this is indeed the optimal expansion rate.

Conjecture 1. *Let $d \geq 3$. The minimum expansion rate of a degree-d sum-invariant matrix is equal to $\frac{2^{d+1}-d-2}{d+2}$.*

6 Conclusion and Open Problems

In this work we have revealed the precise properties of the linear layer used in LS-designs that allow to preserve nonlinear invariants of a similar form than those observed by Todo *et al.* As a negative result, we have shown that it is not possible to construct such an LS-design block cipher that generalizes the invariants to be preserved up to algebraic degree 3. Those results were obtained by studying the Boolean functions of minimum weight that admit no linear annihilator.

An interesting open question is stated in Question 1. That is, can we understand in which cases the minimal degree-d zero-sum sets are also maximal? A more general and indeed remarkable result would be to derive exact formulas for $F(n, d)$ in those cases where we were only able to provide upper and lower bounds. Indeed, solutions to those problems would have interesting implications such as understanding the minimum expansion rate of degree-d sum-invariant matrices and deriving equivalences between degree-d zero-sum sets and Boolean functions with algebraic immunity at least 2.

References

[1] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni. Midori: A block cipher for low energy. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015*, volume 9453 of *Lecture Notes in Computer Science*, pp. 411–436. Springer, Berlin, Heidelberg, 2015.

[2] A. Bannier and E. Filiol. Partition-based trapdoor ciphers. In *Partition-Based Trapdoor Ciphers*. InTech, 2017.

[3] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. In Y. Crama and P. Hammer, editors, *Boolean Methods and Models*. Cambridge University Press, 2007.

[4] N. Courtois. Feistel schemes and bi-linear cryptanalysis. In M. Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pp. 23–40. Springer, Berlin, Heidelberg, 2004.

[5] V. Grosso, G. Leurent, F.-X. Standaert, and K. Varici. LS-designs: Bitslice encryption for efficient masked software implementations. In C. Cid and C. Rechberger, editors, *Fast Software Encryption*, volume 8540 of *Lecture Notes in Computer Science*, pp. 18–37. Springer, Berlin, Heidelberg, 2015.

[6] C. Harpes, G. G. Kramer, and J. L. Massey. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT'95*, volume 921 of *Lecture Notes in Computer Science*, pp. 24–38. Springer, Berlin, Heidelberg, 1995.

[7] A. Hedayat, N. Sloane, and J. Stufken. *Orthogonal Arrays*. Springer Series in Statistics. Springer New York, 1999.

[8] A. Hedayat and W. Wallis. Hadamard matrices and their applications. *Ann. Stat.*, 6(6):1184–1238, 1978.

[9] T. Kasami and N. Tokura. On the weight structure of Reed-Muller codes. *IEEE Transactions on Information Theory*, 16(6):752–759, 1970.

[10] T. Kasami, N. Tokura, and S. Azumi. On the weight enumeration of weights less than 2.5d of Reed-Muller codes. *Information and Control*, 30(4):380–395, 1976.

[11] L. R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT'96*, volume 1070 of *Lecture Notes in Computer Science*, pp. 224–236. Springer, Berlin, Heidelberg, 1996.

[12] X. Lai. Higher order derivatives and differential cryptanalysis. In R. E. Blahut, D. J. Costello, U. Maurer, and T. Mittelholzer, editors, *Communications and Cryptography. The Springer International Series in Engineering and Computer Science (Communications and Information Theory)*, volume 276, pp. 227–233. Springer, Boston, MA, 1994.

[13] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pp. 386–397. Springer, Berlin, Heidelberg, 1994.

[14] W. Meier, E. Pasalic, and C. Carlet. Algebraic attacks and decomposition of boolean functions. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pp. 474–491. Springer, Berlin, Heidelberg, 2004.

[15] J. Patarin and L. Goubin. Asymmetric cryptography with s-boxes. In Y. Han, T. Okamoto, and S. Qing, editors, *Information and Communication Security*, volume 1334 of *Lecture Notes in Computer Science*, pp. 369–380. Springer, Berlin, Heidelberg, 1997.

[16] K. T. Phelps, J. Rifà, and M. Villanueva. Hadamard codes of length $2^t s$ (s odd). Rank and kernel. In M. P. C. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 3857 of *Lecture Notes in Computer Science*, pp. 328–337. Springer, Berlin, Heidelberg, 2006.

[17] V. Rijmen and B. Preneel. A family of trapdoor ciphers. In E. Biham, editor, *Fast Software Encryption*, volume 1267 of *Lecture Notes in Computer Science*, pp. 139–148. Springer, Berlin, Heidelberg, 1997.

[18] Y. Todo, G. Leander, and Y. Sasaki. Nonlinear invariant attack. In J. Cheon and T. Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, volume 10032 of *Lecture Notes in Computer Science*, pp. 3–33. Springer, Berlin, Heidelberg, 2016.

A Values and Bounds for $F(n, d)$

In the following table we describe known exact values or known bounds of $F(n, d)$ for $n \in \{2, \ldots, 30\}$ and $d \in \{1, \ldots, 10\}$. The exact values come from Propositions 7, 8 and 12. The lower bounds come from Propositions 11 and 9. The upper bounds come from Proposition 10. We remark that for $F(2d + 5, d)$ the upper bound is obtained by using a slightly different construction. We use the same diagonal construction but fill the free space with 1s. Consider the matrix $\widehat{\mathbb{M}_S}$ given by

$$\mathbb{M}_S = \left[\begin{array}{c|c} & 1 \ \ldots \ 1 \\ \mathbb{M}_{S_1} & \vdots \\ & 1 \ \ldots \ 1 \\ \hline 1 \ \ldots \ 1 & \\ \vdots & \mathbb{M}_{S_2} \\ 1 \ \ldots \ 1 & \end{array}\right],$$

where $S_1 \in \mathrm{ZS}^d_{(d+1)\times F(d+1,d)}$, $S_2 \in \mathrm{ZS}^d_{(d+4)\times F(d+4,d)}$ and both $\widehat{\mathbb{M}_{S_1}}, \widehat{\mathbb{M}_{S_2}}$ contain a column $(1, \ldots, 1)$ so that two columns repeat in $\widehat{\mathbb{M}_S}$. Note that the row span of S_1 does not contain a row $(1, \ldots, 1)$ and thus $\mathrm{rank}(\widehat{\mathbb{M}_S}) = \mathrm{rank}(\widehat{\mathbb{M}_{S_1}}) + \mathrm{rank}(\widehat{\mathbb{M}_{S_2}}) = 2d + 5$. The columns of $\widehat{\mathbb{M}_S}$ form a zero-sum set from $\mathrm{ZS}^d_{(2d+5)\times(5\cdot 2^d-2)}$.

Table 1: This table shows the values of $F(n,d)$ for $n \in \{2,\ldots,30\}$ and $d \in \{1,\ldots,10\}$. In cases where the exact value is not known, $[a,b]$ denotes that $a \leq F(n,d) \leq b$.

n, d	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	4									
3	4	8								
4	6	8	16							
5	6	12	16	32						
6	8	12	24	32	64					
7	8	14	24	48	64	128				
8	10	16	28	48	96	128	256			
9	10	18	30	56	96	192	256	512		
10	12	20	32	60	112	192	384	512	1024	
11	12	22	[32,38]	62	120	224	384	768	1024	2048
12	14	24	[32,40]	64	124	240	448	768	1536	2048
13	14	26	[32,44]	[64,78]	126	248	480	896	1536	3072
14	16	28	[34,46]	[64,80]	128	252	496	960	1792	3072
15	16	30	[36,48]	[64,88]	[128,158]	254	504	992	1920	3584
16	18	32	[38,54]	[64,92]	[128,160]	256	508	1008	1984	3840
17	18	34	[40,56]	[64,94]	[128,176]	[256,318]	510	1016	2016	3968
18	20	36	[42,60]	[64,96]	[128,184]	[256,320]	512	1020	2032	4032
19	20	38	[44,62]	[64,110]	[128,188]	[256,352]	[512,638]	1022	2040	4064
20	22	40	[46,64]	[64,112]	[128,190]	[256,368]	[512,640]	1024	2044	4080
21	22	42	[48,70]	[64,120]	[128,192]	[256,376]	[512,704]	[1024,1278]	2046	4088
22	24	44	[50,72]	[64,124]	[128,222]	[256,380]	[512,736]	[1024,1280]	2048	4092
23	24	46	[52,76]	[64,126]	[128,224]	[256,382]	[512,752]	[1024,1408]	[2048,2558]	4094
24	26	48	[54,78]	[64,128]	[128,240]	[256,384]	[512,760]	[1024,1472]	[2048,2560]	4096
25	26	50	[56,80]	[64,142]	[128,248]	[256,446]	[512,764]	[1024,1504]	[2048,2816]	[4096,5118]
26	28	52	[58,86]	[66,144]	[128,252]	[256,448]	[512,766]	[1024,1520]	[2048,2944]	[4096,5120]
27	28	54	[60,88]	[68,152]	[128,254]	[256,480]	[512,768]	[1024,1528]	[2048,3008]	[4096,5632]
28	30	56	[62,92]	[70,156]	[128,256]	[256,496]	[512,894]	[1024,1532]	[2048,3040]	[4096,5888]
29	30	58	[64,94]	[72,158]	[128,286]	[256,504]	[512,896]	[1024,1534]	[2048,3056]	[4096,6016]
30	32	60	[66,96]	[74,160]	[128,288]	[256,508]	[512,960]	[1024,1536]	[2048,3064]	[4096,6080]