On the vector subspaces of $\mathbb{F}_{2^n}$ over which the multiplicative inverse function sums to zero

Claude Carlet*,

University of Bergen, Department of Informatics, 5005 Bergen, Norway

University of Paris 8, Department of Mathematics, 93526 Saint-Denis, France.

E-mail: claude.carlet@gmail.com, Orcid: 0002-6118-7927

Abstract

We study the behavior of the multiplicative inverse function (which plays an important role in cryptography and in the study of finite fields), with respect to a recently introduced generalization of almost perfect nonlinearity (APNness), called kth-order sum-freedom, that extends a classic characterization of APN functions, and has also some relationship with integral attacks. This generalization corresponds to the fact that a vectorial function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ sums to a nonzero value over every k-dimensional affine subspace of $\mathbb{F}_2^n$, for some $k \leq n$ (APNness corresponds to $k = 2$). The sum of the values of the inverse function $x \in \mathbb{F}_{2^n} \mapsto x^{2^n-2} \in \mathbb{F}_{2^n}$ over any affine subspace A of $\mathbb{F}_{2^n}$ not containing 0 (*i.e.* being not a vector space) has been addressed, thanks to a simple expression of such sum, which shows that it never vanishes. We study in the present paper the case of vector (i.e. linear) subspaces, which is much less simple to handle. The sum depends on a coefficient in subspace polynomials. We study for which values of k the multiplicative inverse function can sum to nonzero values over all k-dimensional vector subspaces. We show that, for every k not co-prime with n, it sums to zero over at least one k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. We study the behavior of the inverse function over direct sums of vector spaces and we deduce that the property of the inverse function to be kth-order sum-free happens for k if and only if it happens for $n - k$. We derive several other results and we show that the set of values k such that the inverse function is not kth-order sum-free is stable when adding two values of k whose product is smaller than n (and when subtracting two values under some conditions). We clarify the case of dimension at most 4 (equivalently, of co-dimension at most 4) and this allows to address, for every n, all small enough values of k of the form $3a + 4b$.

Note: Some of the results in this paper have been presented without proof in the Conference Fq15 (without proceedings), June 2023, Paris, France.

*The research of the author is partly supported by the Norwegian Research Council

Keywords: finite field, multiplicative inverse function, cryptography.

1 Introduction

The important notion on (n, m)-functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ called almost perfect nonlinearity (APNness) (see e.g. [10]) has been recently generalized in [11]: given $2 \leq k \leq n$ and m, an (n, m)-function F is called kth-order sum-free if, for every k-dimensional affine subspace (i.e. k-flat) A of $\mathbb{F}_2^n$, the sum $\sum_{x \in A} F(x)$ of the values taken by F over A is nonzero.

In the present paper, we study the behavior relative to this notion of one of the currently most important examples of vectorial functions for cryptography, namely the (multiplicative) inverse function, defined over $\mathbb{F}_{2^n}$ as

$$F(x) = x^{2^n-2},$$

that is, $F(x) = \frac{1}{x}$, with the convention $\frac{1}{0} = 0$ (the function $F(x)$ will be in some cases denoted by x^{-1}, as it is usual). Recall that this function is used in the S-boxes of the Advanced Encryption Standard (AES, see [16]), that is nowadays the symmetric cryptosystem for civil use employed in all domains of every-day life in the whole world (*e.g.* internet), and also in banking, etc. We shall recall from [11] that the inverse function behaves in a particular way with respect to sum-freedom, since it sums to a nonzero value over every affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ that is not a vector subspace. We study in the present paper for which values of k this function sums to nonzero values over all k-dimensional vector spaces, which is a much more difficult problem to study for vector spaces than for those affine spaces that are not vector spaces, and that we shall only very partially solve. It seems that the mathematical study of the sum of the values taken by the inverse function over all affine subspaces has never been made, while an algorithmic approach exists in [18].

The paper is organized as follows. After preliminaries in Section 2, we give in Section 3 some results on the so-called subspace polynomials that will be useful in the whole paper. In Section 4, we recall an expression found in [11], in the form of a ratio with a very simple numerator, of the sum of values taken by the inverse function over affine spaces that are not vector spaces. This expression shows that this sum is never zero. In the case of vector spaces, finding a simple expression is more difficult. In Section 5, we address the case of $\mathbb{F}_{2^l}$-subspaces of $\mathbb{F}_{2^n}$ where $l \geq 2$ is a divisor of n. We deduce that, for every k not co-prime with n, the multiplicative inverse function sums to zero over at least one k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ and is then not kth-order sum-free. We derive a formula valid for any direct sum of vector spaces, which allows to prove that the inverse function is kth-order sum-free if and only if it is $(n-k)$th-order sum-free and showing some stability under addition and subtraction of the set of values of k such that the inverse function is not kth-order sum-free. We address, for all n, the cases where k is at most 4 or at least $n-4$. We finally give computer investigation results on the kth-order sum-freedom of the inverse (n, n)-function for $n \leq 12$ and all k.

2 Preliminaries

Let n and m be two positive integers. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n,m)-functions and when n and m are not specified, they are called vectorial functions. Every (n,m)-function F admits a unique algebraic normal form, that is, a representation as a multivariate polynomial in the algebra[1] $\mathbb{F}_2^m[x_1,\ldots,x_n]/(x_1^2-x_1,\ldots,x_n^2-x_n)$ of the form:

$$F(x)=\sum_{I\subseteq\{1,\ldots,n\}} a_I \prod_{i\in I} x_i = \sum_{I\subseteq\{1,\ldots,n\}} a_I\, x^I;\ x=(x_1,\ldots,x_n)\in\mathbb{F}_2^n, a_I\in\mathbb{F}_2^m.$$

The global degree of this multivariate polynomial, that is, $\max\{|I|; a_I\neq 0\}$, is called the algebraic degree of F and denoted by $d_{alg}(F)$. Any vectorial function F is affine (that is, satisfies $F(x)+F(y)+F(z)+F(x+y+z)=0$ for every $x,y,z\in\mathbb{F}_2^n$) if and only if it has an algebraic degree at most 1. Similarly, we call quadratic a function having an algebraic degree at most 2. We write "at most 2" and not "equal to 2" because this allows simplifying some statements. Note that thanks to this definition, affine functions are particular quadratic functions. In general, for some positive integer r, a function F has algebraic degree at most r if and only if it sums to zero over every affine space of dimension $k>r$. In particular, an (n,m)-function has (maximum) algebraic degree n if and only if it sums to a nonzero value over $\mathbb{F}_2^n$.

In the present paper, $\mathbb{F}_2^n$ will be endowed with the structure of the field $\mathbb{F}_{2^n}$. This is of course possible because $\mathbb{F}_{2^n}$ being an n-dimensional vector space over $\mathbb{F}_2$, every element $x\in\mathbb{F}_{2^n}$ can be identified with the binary vector $(x_1,\ldots,x_n)$ of its coordinates with respect to a fixed basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then, (n,n)-functions viewed from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ can be uniquely represented by their univariate representation:

$$F(x)=\sum_{i=0}^{2^n-1}\delta_i x^i\in\mathbb{F}_{2^n}[x]/(x^{2^n}+x);\ \delta_i\in\mathbb{F}_{2^n}. \tag{1}$$

Indeed, the function mapping such a polynomial of degree at most 2^n-1 to the corresponding function from $\mathbb{F}_{2^n}$ to itself is linear injective, and its domain and co-domain have the same dimension. The existence and uniqueness of this representation extends to (n,m)-functions when m divides n (and in particular to Boolean functions, for which $m=1$), since $\mathbb{F}_{2^m}$ is then a subfield of $\mathbb{F}_{2^n}$. For $m=n$, we call power functions the functions of univariate representation $F(x)=x^i$. It can be proved (see e.g. [10]) that the algebraic degree of any function F given by (1) equals the largest 2-weight $w_2(i)$ of those exponents i whose coefficients δ_i are nonzero, where the 2-weight is the Hamming weight of the binary expansion.

A vectorial function is called APN if it sums to nonzero values over all the

[1] We need to make the quotient by the ideal generated by the $x_i^2-x_i$ for having uniqueness; the variables x_i represent bits, and are then equal to their squares; concretely, this limits the exponents of the variables to at most 1.

affine planes $\{x, y, z, x + y + z\}$ (x, y, z distinct) of the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. This leads to the generalization called kth-order sum-freedom, in which the dimension 2 of affine planes is replaced by dimension $k \leq n$.

3 Preliminary results involving linearized polynomials

3.1 Subspace polynomials

Let E_k be any k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ (i.e. an element of the Grassmannian space of index k over $\mathbb{F}_{2^n}$). Then it is well-known that the function

$$L_{E_k}(x) = \prod_{u \in E_k} (x + u) \tag{2}$$

is $\mathbb{F}_2$-linear (*i.e.* is a linearized polynomial). It is the only normalized polynomial of degree 2^k whose zeros are the elements of E_k. Polynomials of this form are often called *subspace polynomials over* $\mathbb{F}_{2^n}$ (and sometimes specified as kernel-subspace polynomials or subspace-vanishing polynomials); they play roles in many domains of discrete applied mathematics and coding theory (e.g. finding an element of high multiplicative order in a finite field), affine dispersers and extractors (i.e. Boolean functions that behave pseudorandomly when their domain is restricted to any particular affine space of a dimension bounded from below[2]), computational complexity, sub-linear proof verification, cyclic subspace codes for random network coding, the list decoding of Reed-Solomon codes and rank-metric codes, see [1, 2, 4, 5, 6, 7, 14, 15, 23, 25, 26, 28, 31, 32, 35, 36, 37]. They are those normalized linearized polynomials over $\mathbb{F}_{2^n}$ which split over $\mathbb{F}_{2^n}$ and have simple zeros (equivalently, which divide $x^{2^n} + x$, and still equivalently, whose kernel size in $\mathbb{F}_{2^n}$ equals the degree).

Remark. The coefficient of x in $L_{E_k}(x)$ equals $\prod_{u \in E_k, u \neq 0} u \neq 0$. Every normalized linearized polynomial over $\mathbb{F}_{2^n}$ is a subspace polynomial over some Galois extension of $\mathbb{F}_{2^n}$ if and only if its coefficient of x is nonzero, but we are interested in the subspace polynomials over $\mathbb{F}_{2^n}$ precisely. $\diamond$

Let us recall some properties of subspace polynomials which may be useful in future papers. If E_k is defined as the kernel of some linearized polynomial $L(x)$ over $\mathbb{F}_{2^n}$, then $L_{E_k}(x) = \gcd(L(x), x^{2^n} + x)$ and if $L(x)$ splits over $\mathbb{F}_{2^n}$, then $L(x) = (L_{E_k}(x))^{2^r}$ for some r, k. It is also observed (for instance in [4]) that the image spaces of all subspace polynomials of degree 2^k are all the $(n-k)$-dimensional vector subspaces of $\mathbb{F}_2^n$ (and are then also viewed in [4] as so-called image-subspace polynomials). Moreover, if the image space of L_{E_k} equals E'_{n-k}

[2]In the case of dispersers, these restrictions must be non-constant, and in the case of extractors, they must lie at a Hamming distance from balanced functions which is bounded above by some given number.

then the image space of $L_{E'_{n-k}}$ equals E_k (we shall recall the proof of this fact below) and $L_{E_k} \circ L_{E'_{n-k}}(x) = L_{E'_{n-k}} \circ L_{E_k}(x) = x^{2^n} + x$.

Given a basis $(a_1, \ldots, a_n)$ of $\mathbb{F}_2^n$, the sequence $(L_{E_k})_{2 \leq k \leq n}$ where E_k equals the vector space $< a_1, \ldots, a_k >$ satisfies a recurrence relation: for $k \geq 2$, assuming that $L_{E_{k-1}}$ is linear, we have $L_{E_k}(x) = L_{E_{k-1}}(x) L_{E_{k-1}}(x + a_k) = L_{E_{k-1}}(x) \left(L_{E_{k-1}}(x) + L_{E_{k-1}}(a_k)\right)$, and therefore:

$$L_{E_k}(x) = \left(L_{E_{k-1}}(x)\right)^2 + L_{E_{k-1}}(a_k) L_{E_{k-1}}(x) \tag{3}$$

is also linear. Note that Relation (3) is also valid for $k = 1$ if we assume that $L_0(x) = x$. This is how it can be checked by induction that L_{E_k} is linear. Moreover, $L_{E_k}(x)$ equals, up to a multiplicative constant, the determinant of the so-called Moore matrix:

$$\begin{bmatrix} x & x^2 & \ldots & x^{2^k} \\ a_1 & a_1^2 & \ldots & a_1^{2^k} \\ \vdots & \vdots & \ldots & \vdots \\ a_k & a_k^2 & \ldots & a_k^{2^k} \end{bmatrix}.$$

When k divides n and $E_k = \mathbb{F}_{2^k}$, we have $L_{E_k}(x) = x^{2^k} + x$. More generally, for every $l \leq n$, if $L(x) = x^{2^l} + x$, then $\gcd(L(x), x^{2^n} + x) = x^{2^k} + x$ with $k = \gcd(l, n)$. And denoting $F_k = L(\mathbb{F}_{2^n})$, it is easily seen that $L_{F_k}(x) = tr_k^n(x)$, where $tr_k^n(x)$ is the relative trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$: $tr_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}$.

Remark. $c = L_{E_{k-1}}(a_k)$ is the unique nonzero element of $L_{E_{k-1}}(E_k)$ (since $E_k \setminus E_{k-1} = a_k + E_{k-1}$), and, denoting by tr_n the absolute trace function over $\mathbb{F}_{2^n}$ (that is, tr_1^n): $tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$, we have $tr_n\left(\frac{L_{E_k}(x)}{c^2}\right) = 0$ for every $x \in \mathbb{F}_{2^n}$, since $\frac{L_{E_k}(x)}{c^2} = \left(\frac{L_{E_{k-1}}(x)}{c}\right)^2 + \frac{L_{E_{k-1}}(x)}{c}$. Hence, $Im(L_{E_k}) = L_{E_k}(\mathbb{F}_{2^n})$ is included in the hyperplane $\{0, \frac{1}{c^2}\}^\perp = \{x \in \mathbb{F}_{2^n}; tr_n(xy) = 0, \forall y \in \{0, \frac{1}{c^2}\}\}$. In fact, E_k and L_{E_k} being invariant when changing the order in which we write the elements of the chosen basis of E_k, we can obtain this way several elements in the dual of $Im(L_{E_k})$. $\diamond$

Remark. Let $L^*_{E_k}(x) = \sum_{i=0}^{k} (b_i x)^{2^{n-i}}$ be the adjoint operator of $L_{E_k} = \sum_{i=0}^{k} b_i x^{2^i}$, satsifying $L^*_{E_k}(u) \cdot x = u \cdot L_{E_k}(x), \forall u, x \in \mathbb{F}_{2^n}$ (where $u \cdot x = tr_n(ux)$). For every $u \in \mathbb{F}_{2^n}$ and $x \in E_k$, we have then $L^*_{E_k}(u) \cdot x = 0$ and the image set of $L^*_{E_k}$ is then included in $E_k^\perp$. Since these two vector spaces have the same dimension (because L_{E_k} and $L^*_{E_k}$ are known to have the same rank), we have then $Im(L^*_{E_k}) = E_k^\perp$. $\diamond$

Remark. Let E and F be two vector spaces having a trivial intersection. Then, denoting by $E \oplus F$ their direct sum, we have $L_{E \oplus F}(x) = \prod_{u \in E; v \in F}(x + u + v) = \prod_{v \in F} L_E(x + v) = \prod_{v \in F}(L_E(x) + L_E(v)) = L_{L_E(F)}(L_E(x))$. $\diamond$

Main known properties of subspace polynomials Despite the number of papers where subspace polynomials are addressed and used, little is known on them. Let us summarize:
- In [1] are observed the obvious facts that $L_{\alpha E_k}(x) = \alpha^{2^k} L_{E_k}(\alpha^{-1}x)$ for every $\alpha \in \mathbb{F}_{2^n}^*$, and that applying the Frobenius automorphism to E_k results in applying it to each coefficient in $L_{E_k}(x)$. It is also proved in this same paper that, given two vector subspaces E_k and $E_{k'}$ such that $\dim(E_k) = k \geq \dim(E_{k'}) = k'$, denoting by 2^j (resp. $2^{j'}$) the second highest degree of the monomials in $L_{E_k}(x)$ (resp. $L_{E_{k'}}(x)$), we have $\dim(E_k \cap E_{k'}) \leq r = \max(j, j' + k - k')$. This is a direct consequence of the relations $L_{E_k \cap E_{k'}}(x) = \gcd(L_{E_k}(x), L_{E_{k'}}(x)) = \gcd(L_{E_k}(x), (L_{E_{k'}}(x))^{2^{k-k'}}) = \gcd(L_{E_k}(x), L_{E_k}(x) + (L_{E_{k'}}(x))^{2^{k-k'}})$ and $\deg(L_{E_k}(x) + (L_{E_{k'}}(x))^{2^{k-k'}}) \leq 2^r$ (the second equality above coming from the fact that $L_{E_k}(x)$ splits and has simple zeros).
- It is observed in [4] that at least one coefficient is nonzero among any $n - k$ consecutive coefficients b_i in $L_{E_k}(x)$, which is straightforward by considering $\gcd(x^{2^n} + x, (L_{E_k}(x))^{2^j})$ for some j, since a nonzero polynomial of degree less than 2^k cannot have 2^k zeros.
- It is shown in [7, 4] that, if E is an $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^n}$ and $E' = L_E(\mathbb{F}_{2^n})$, then $E = L_{E'}(\mathbb{F}_{2^n})$. Indeed, the monic (formal) polynomial $L_{E'} \circ L_E(X) \in \mathbb{F}_{2^n}[X]$ having degree 2^n and vanishing on $\mathbb{F}_{2^n}$ equals $X^{2^n} + X$. Hence, we have $L_E \circ L_{E'} \circ L_E(X) = L_E(L_{E'} \circ L_E(X)) = L_E(X^{2^n} + X) = L_E(X^{2^n}) + L_E(X) = (L_E(X))^{2^n} + L_E(X)$ and the polynomial $\phi(X) = L_E \circ L_{E'}(X) + X^{2^n} + X$ composed on the right by $L_E(X)$ equals then the zero polynomial in $\mathbb{F}_{2^n}[X]$. This implies that $\phi(X)$ is the zero polynomial since otherwise, denoting its degree by d, the term in $X^{2^k d}$ could not be cancelled in the polynomial $\phi \circ L_E(X) \in \mathbb{F}_{2^n}[X]$. The equality $L_E \circ L_{E'}(X) = X^{2^n} + X$ implies that $L_{E'}(\mathbb{F}_{2^n})$ is included in E and this completes the proof since these two vector spaces have the same dimension by the fundamental theorem of linear algebra. Note that this then proves that $L_{E'}$ and L_E commutate (which is not straightforward from their definitions). A particular case is when r divides n and $E = \mathbb{F}_{2^r}$. Then $L_E(x) = x^{2^r} + x$, $E' = \ker(tr_r^n), L_{E'}(x) = tr_r^n(x)$ and $E \cap E' = \{x^{2^r} + x; x \in \mathbb{F}_{2^{\gcd(2r,n)}}\}$ is trivial if $\frac{n}{r}$ is odd and non-trivial if $\frac{n}{r}$ is even.
- The linearized polynomials L_{E_k} are characterized in [15, 26] by means of companion matrices.

3.2 Particular case of subspace polynomials with coefficients in $\mathbb{F}_2$

The linearized polynomial $L_{E_k}(x)$ has all its coefficients in $\mathbb{F}_2$ if and only if E_k is invariant under the Frobenius automorphism $x \mapsto x^2$. We know, see [23], that such a linearized polynomial $\sum_{i=0}^k b_i x^{2^i}$, $b_i \in \mathbb{F}_2$, is a divisor of $x^{2^n} + x$ if and only if the so-called associated polynomial $\sum_{i=0}^k b_i x^i$ is a divisor of $x^n + 1$. If n is odd then we know, see [24], that this is equivalent to the fact that it is the generator polynomial of a binary cyclic code of length n, and it equals

the product of minimal polynomials $M_j(x) = \prod_{i \in C_j}(x + \beta^i)$, where j ranges over a set of representatives of cyclotomic classes $C_j = \{j, 2j, 2^2 j, \dots\}$ in $\mathbb{Z}/n\mathbb{Z}$ and β is a primitive nth root of unity in $\mathbb{F}_{2^m}$, where m is the smallest positive integer such that n divides $2^m - 1$. Note that the number of these cyclotomic classes (and hence, the maximal number of the minimal polynomials which are factors of $L_{E_k}(x)$) may be as small as 2 (this happens with some primes: $n = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, \dots$).

4 Sums of the values taken by the inverse function over affine spaces not containing 0

In [11], we obtained an explicit expression of the sum of the values taken by the multiplicative inverse function over affine subspaces of $\mathbb{F}_{2^n}$ that are not vector subspaces, which allowed us to prove that such sum is always nonzero. We recall this result after briefly recalling how it was obtained.
Let E_k still be any k-dimensional vector subspace of $\mathbb{F}_{2^n}$. According to (3), $L_{E_k}(x)$ has the form:

$$L_{E_k}(x) = \sum_{i=0}^{k} b_{k,i} x^{2^i}, \tag{4}$$

where $b_{k,k} = 1$ and $b_{k,i} = b_{k-1,i-1}^2 + L_{E_{k-1}}(a_k)\, b_{k-1,i}$, for every $i = 0, \dots, k$, with the convention $b_{k-1,-1} = 0$.
The only monomial in (4) having a nonzero derivative (here we mean the classic derivative of a polynomial function) is x. We have then that $L'_{E_k}(x)$ equals the constant $b_{k,0} = \prod_{u \in E_k, u \neq 0} u \neq 0$. We also have, by the application of the classic formula on the derivative of a product, that $L'_{E_k}(x) = \sum_{u \in E_k} \prod_{v \in E_k, v \neq u}(x+v)$ and for $x \notin E_k$, this gives $L'_{E_k}(x) = \left(\sum_{u \in E_k} \frac{1}{x+u}\right) L_{E_k}(x)$. We deduced then:

Theorem 1 *[11] For every $0 \leq k \leq n$, let E_k be any k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ and let $F(x) = x^{2^n-2} = x^{-1}$ be the multiplicative inverse function over $\mathbb{F}_{2^n}$. We have:*

$$\forall x \notin E_k, \sum_{u \in E_k} F(x+u) = \sum_{u \in E_k} \frac{1}{x+u} = \frac{\prod_{u \in E_k, u \neq 0} u}{\prod_{u \in E_k}(x+u)} = \frac{b_{k,0}}{L_{E_k}(x)} \neq 0, \tag{5}$$

where $L_{E_k}(x) = \prod_{u \in E_k}(x+u)$ and $b_{k,0}$ is its coefficient of x.

5 Sums of the values taken by the inverse function over vector subspaces of $\mathbb{F}_{2^n}$

Let us now study the value of $\sum_{u \in E} F(x+u)$ when $x \in E$ (hence, without loss of generality, when $x = 0$). We study then $\sum_{u \in E_k, u \neq 0} \frac{1}{u}$.

Remark. Theorem 1 shows that, for every $\mathbb{F}_2$-vector subspace E of $\mathbb{F}_{2^n}$ such that $\sum_{u\in E,u\neq 0}\frac{1}{u}=0$ and every linear hyperplane H of E (that is, any vector subspace of E of co-dimension 1), we have $\sum_{u\in H,u\neq 0}\frac{1}{u}\neq 0$ (since $\sum_{u\in E\setminus H}\frac{1}{u}\neq 0$). Hence, if the inverse function is neither kth-order sum-free nor $(k-1)$th-order sum-free, the $(k-1)$-dimensional vector spaces over which it sums to zero cannot be subspaces of the k-dimensional vector spaces over which it sums to zero.
Similarly, for every vector subspace F of $\mathbb{F}_{2^n}$ containing E as a hyperplane, we have $\sum_{u\in F,u\neq 0}\frac{1}{u}\neq 0$, since $\sum_{u\in F\setminus E}\frac{1}{u}\neq 0$.
In particular, for every divisor $m\geq 2$ of n, every linear hyperplane H of $\mathbb{F}_{2^m}$ and every $(m+1)$-dimensional vector subspace F containing $\mathbb{F}_{2^m}$, the inverse function does not sum to 0 over H nor over F. $\diamond$

5.1 Relation with subspace polynomials

Let $\phi_k(x)=\prod_{u\in E_k,u\neq 0}(x+u)$ and $\phi_0(x)=1$. According to Relation (4), we have $\phi_k(x)=\sum_{i=0}^{k}b_{k,i}x^{2^i-1}$. Then $\phi_k(0)=\prod_{u\in E_k,u\neq 0}u=b_{k,0}$ and $\phi_k'(x)=\sum_{i=1}^{k}b_{k,i}x^{2^i-2}$ and therefore $\phi_k'(0)=b_{k,1}$, while the formula on the derivative of a product gives $\phi_k'(x)=\sum_{u\in E_k,u\neq 0}\prod_{v\neq 0,v\neq u}(x+v)$ and then:

$$\sum_{u\in E_k,u\neq 0}\frac{1}{u}=\frac{\phi_k'(0)}{\phi_k(0)}=\frac{b_{k,1}}{b_{k,0}}. \tag{6}$$

Proposition 1 *Let E be any $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. The sum $\sum_{u\in E,u\neq 0}\frac{1}{u}$ is equal to 0 if and only if the coefficient of x^2 in the linearized polynomial $L_E(x)=\prod_{u\in E}(x+u)$ equals 0.*

According to Proposition 1, studying the kth-order sum-freedom of the inverse function results in studying if some linearized polynomials of degree 2^k can have their coefficient of x nonzero, their coefficient of x^2 equal to 0, and 2^k distinct zeros in $\mathbb{F}_{2^n}$. The results of [28, 36, 37] may be helpful from this regard but they do not allow to really solve the general problem.

Remark. Another viewpoint on Proposition 1, which sheds a different light on the result, is as follows. The relation $\sum_{i=0}^{k}b_{k,i}x^{2^i}=0$ is satisfied by every element of E_k. Dividing this relation by $b_{k,0}x^2$ for $x\neq 0$ gives $x^{-1}=\frac{\sum_{i=1}^{k}b_{k,i}x^{2^i-2}}{b_{k,0}}$. Since $0^{-1}=0$ and $\frac{\sum_{i=1}^{k}b_{k,i}x^{2^i-2}}{b_{k,0}}$ equals $\frac{b_{k,1}}{b_{k,0}}$ for $x=0$, we have then, for every $x\in E_k$: $x^{-1}=\frac{b_{k,1}\delta_0(x)+\sum_{i=1}^{k}b_{k,i}x^{2^i-2}}{b_{k,0}}$, where $\delta_0(x)=x^{2^n-1}+1$ is the Dirac (or Kronecker) symbol, and this latter function on E_k, viewed as a k-variable Boolean function, has algebraic degree k (and hence sums to a nonzero value over E_k) if and only if $b_{k,1}\neq 0$. $\diamond$

5.2 Determining the kth-order sum-freedom of multiplicative inverse function for some values of k

We have seen that for $n \geq 3$ odd, the inverse function is second-order sum-free and for $n \geq 2$ even, it is not. The inverse (n,n)-function being a permutation it is not nth-order sum-free and since its restriction to any subfield $\mathbb{F}_{2^k}$ is the multiplicative inverse (k,k)-function, for every divisor k of n, the inverse (n,n)-function is not kth-order sum-free (this generalizes the fact that if n is even, then the inverse function is not APN). The inverse function is $(n-1)$th-order sum-free, thanks to Theorem 1 and the fact that it is not nth-order sum-free (i.e. it sums to 0 over $\mathbb{F}_{2^n}$). Hence there are values of k for which the inverse function is kth-order sum-free and values for which it is not.

According to Theorem 1, determining whether the multiplicative inverse function is kth-order sum-free for some k reduces to determining whether the inverse function sums to nonzero values over all k-dimensional vector subspaces of $\mathbb{F}_{2^n}$.

Note that when a function is not kth-order sum-free (which, for $k \in \{3,\ldots,n-3\}$, is the case of inverse function, seemingly, as we shall see), it is good (but it seems rather difficult for inverse function in general) to determine all k-dimensional subspaces over which the inverse function sums to 0 (or at least determine their number), as this is done for various functions for $k=2$ in [22], in relation with APNness (this reference uses the term of *vanishing k-flats* for such affine spaces). This could be done for $k \in \{3,\ldots,n-3\}$ in future papers.

5.2.1 When k is not co-prime with n

We now show that, when $\gcd(k,n) > 1$, the inverse function sums to zero over some k-dimensional vector spaces, and is then not kth-order sum-free. This generalizes the property that the inverse function sums to zero over subfields of $\mathbb{F}_{2^n}$ different from $\mathbb{F}_2$, and is then not kth-order sum-free when $k \geq 2$ divides n:

Theorem 2 *If $\gcd(k,n) = l > 1$, let $\mathcal{E}$ be any $\frac{k}{l}$-dimensional $\mathbb{F}_{2^l}$-subspace of $\mathbb{F}_{2^n}$, then $\sum_{u\in\mathcal{E};u\neq 0} \frac{1}{u} = 0$; the multiplicative inverse function is then not kth-order sum-free.*

Proof. $\mathcal{E}\setminus\{0\}$ is the disjoint union of the elements of the $(\frac{k}{l}-1)$-dimensional projective space P equal to the set of equivalence classes in $\mathcal{E}\setminus\{0\}$ under the equivalence relation "$a \sim b$ if $\frac{a}{b} \in \mathbb{F}_{2^l}$". Each element in P having the form $a\,\mathbb{F}_{2^l}^*$, we have then $\sum_{u\in\mathcal{E}\setminus\{0\}} \frac{1}{u} = \sum_{a\in P} \frac{1}{a}\left(\sum_{u\in\mathbb{F}_{2^l}^*} \frac{1}{u}\right) = 0$. □

Theorem 2 settles the case of a rather large number of values of k when n is composite (of course, it is useless when n is a prime). Thanks to it, we need now only to address the case where k and n are co-prime.

Generalization of Theorem 2

Proposition 2 *Let k be the dimension of any $\mathbb{F}_2$-vector subspace E_k of $\mathbb{F}_{2^n}$ stable under multiplication by some $\lambda \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, then the multiplicative inverse function is not kth-order sum-free. In particular, if k equals the (additive) rank of any non-trivial multiplicative subgroup G of $\mathbb{F}_{2^n}$, that is, if it equals the dimension of any vector subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ generated by the powers λ^i of some $\lambda \neq 0, 1$, the multiplicative inverse function is not kth-order sum-free.*

Proof. If E_k is stable under multiplication by λ, then we have $\sum_{u \in E_k; u \neq 0} \frac{1}{u} = \sum_{u \in E_k; u \neq 0} \frac{1}{\lambda u} = \frac{1}{\lambda} \sum_{u \in E_k; u \neq 0} \frac{1}{u}$ with $\frac{1}{\lambda} \neq 1$ and therefore $\sum_{u \in E_k; u \neq 0} \frac{1}{u} = 0$. If k equals the (additive) rank of a non-trivial multiplicative subgroup G of $\mathbb{F}_{2^n}$, then let λ be a generator of G and let E_k be the k-dimensional $\mathbb{F}_2$-vector subspace generated by G, we have that E_k is invariant under multiplication by λ. □

Remark. Proposition 2, even if it covers Theorem 2 as a particular case, does not allow to address more values of k. Indeed, we need to have $\prod_{u \in E_k; u \neq 0} u = \prod_{u \in E_k; u \neq 0} (\lambda u) = \lambda^{2^k - 1} \prod_{u \in E_k; u \neq 0} u$ and since $\prod_{u \in E_k; u \neq 0} u \neq 0$, this implies that $\lambda^{2^k - 1} = 1$, which (because $\lambda \neq 1$) requires that $\gcd(2^k - 1, 2^n - 1) > 1$, that is, $\gcd(k, n) > 1$. ◇

Sum-freedom over subfields and superfields If the inverse function over $\mathbb{F}_{2^n}$ is not kth-order sum-free, then for every r, the inverse function over $\mathbb{F}_{2^{rn}}$ is not kth-order sum-free either, since the restriction to $\mathbb{F}_{2^n}$ of the inverse function over $\mathbb{F}_{2^{rn}}$ equals the inverse function over $\mathbb{F}_{2^n}$. Moreover:

Proposition 3 *For every $k \geq 2$, and every $n \geq k$, there exists a positive integer r such that the multiplicative inverse function over $\mathbb{F}_{2^{rn}}$ is not kth-order sum-free.*

This result is straightforward, since we know that, $\mathrm{lcm}(k, n)$ being a multiple of k, the multiplicative inverse function over $\mathbb{F}_{2^{\mathrm{lcm}(k,n)}}$ is not kth-order sum-free. We can even take r smaller than $\frac{\mathrm{lcm}(k,n)}{n}$ when k is composite, thanks to Theorem 2, by taking for r any divisor of k larger than 1.
But let us give an alternative proof which will provide additional insight on the question. According to Proposition 1, the multiplicative inverse function over $\mathbb{F}_{2^{rn}}$ is kth-order sum-free if and only if, for every k-dimensional $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^{rn}}$, the coefficient of x^2 in the polynomial $L(x) = \prod_{u \in E}(x + u)$ is nonzero. The set of such polynomials, for r ranging over $\mathbb{N}^*$, equals the set of linearized polynomials $L(x)$ of degree 2^k over the algebraic closure of $\mathbb{F}_{2^n}$ which have simple zeros. Note that such linearized polynomial has simple zeros in the algebraic closure if and only if its coefficient of x is nonzero (indeed, the polynomial derivative of a linearized polynomial equals the constant polynomial equal to this coefficient). Among such polynomials, some have their coefficient of x^2 equal to zero.
The open question is: for which values of k and n, the value of r can be taken equal to 1?

5.2.2 A result on direct sums of $\mathbb{F}_2$-subspaces of $\mathbb{F}_{2^n}$ and its consequences

Theorem 1 implies the following corollary.

Corollary 1 *Let $1 \leq l \leq k \leq n$ and let E, F be $\mathbb{F}_2$-subspaces of $\mathbb{F}_{2^n}$ with a trivial intersection, and of respective dimensions l and $k-l$, then*

$$\sum_{u \in E \oplus F; u \neq 0} \frac{1}{u} = \sum_{u \in E; u \neq 0} \frac{1}{u} + \left(\prod_{u \in E, u \neq 0} u \right) \sum_{v \in L_E(F); v \neq 0} \frac{1}{v}, \tag{7}$$

where $\oplus$ denotes the direct sum, $L_E(x) = \prod_{u \in E}(x+u)$ and $L_E(F)$ (equal to $L_E(E \oplus F)$) is the $(k-l)$-dimensional vector space equal to the image of F by L_E.
Given an $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^n}$, the vector space $L_E(F)$ can be any $(k-l)$-dimensional $\mathbb{F}_2$-subspace of the $(n-l)$-dimensional space $L_E(\mathbb{F}_{2^n})$

Proof. By hypothesis, L_E is injective over F, because F has trivial intersection with the kernel E of L_E. According to Theorem 1, we have:

$$\begin{aligned}
\sum_{u \in E \oplus F; u \neq 0} \frac{1}{u} &= \sum_{u \in E; u \neq 0} \frac{1}{u} + \sum_{w \in F; w \neq 0} \sum_{u \in E} \frac{1}{w+u} \\
&= \sum_{u \in E; u \neq 0} \frac{1}{u} + \sum_{w \in F; w \neq 0} \frac{\prod_{u \in E, u \neq 0} u}{L_E(w)} \\
&= \sum_{u \in E; u \neq 0} \frac{1}{u} + \left(\prod_{u \in E, u \neq 0} u \right) \sum_{w \in F; w \neq 0} \frac{1}{L_E(w)} \\
&= \sum_{u \in E; u \neq 0} \frac{1}{u} + \left(\prod_{u \in E, u \neq 0} u \right) \sum_{v \in L_E(F); v \neq 0} \frac{1}{v}.
\end{aligned}$$

Given an $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^n}$ and any $(k-l)$-dimensional $\mathbb{F}_2$-subspace E' of $L_E(\mathbb{F}_{2^n})$, there exists a $(k-l)$-dimensional $\mathbb{F}_2$-subspace F of $\mathbb{F}_{2^n}$ with trivial intersection with E such that $L_E(F) = E'$, since L_E is a bijective linear map from F to $L_E(F)$. This completes the proof. □

Remark. Corollary 1 can be extended to more than two vector spaces. For instance, let E, F, G be three vector spaces that are in a direct sum, then:

$$\begin{aligned}
\sum_{u \in E \oplus F \oplus G; u \neq 0} \frac{1}{u} &= \sum_{u \in E; u \neq 0} \frac{1}{u} + \\
&\left(\prod_{u \in E, u \neq 0} u \right) \left(\sum_{v \in L_E(F); v \neq 0} \frac{1}{v} + \left(\prod_{v \in L_E(F), v \neq 0} v \right) \sum_{w \in L_{L_E(F)}(L_E(G)); w \neq 0} \frac{1}{w} \right).
\end{aligned} \tag{8}$$

Indeed, by applying Corollary 1, we obtain: $\sum_{u\in E\oplus F\oplus G;u\neq 0}\frac{1}{u}=\sum_{u\in E;u\neq 0}\frac{1}{u}+\left(\prod_{u\in E,u\neq 0}u\right)\left(\sum_{v\in L_E(F\oplus G);v\neq 0}\frac{1}{v}\right)$, and since, by injectivity, we have that $L_E(F\oplus G)=L_E(F)\oplus L_E(G)$, we obtain $\sum_{u\in E\oplus F\oplus G;u\neq 0}\frac{1}{u}=\sum_{u\in E;u\neq 0}\frac{1}{u}+\left(\prod_{u\in E,u\neq 0}u\right)\left(\sum_{v\in L_E(F)\oplus L_E(G);v\neq 0}\frac{1}{v}\right)$ and we can then apply again (7), which gives (8). ◇

A first consequence dealing with complementary dimensions Corollary 1 implies that the property for the inverse function of being kth-order sum-free is invariant under the transformation $k\mapsto n-k$:

Theorem 3 *Let $2\leq k\leq n-2$ be such that the inverse function is not kth-order sum-free. Let E_k be a k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$ such that $\sum_{u\in E_k;u\neq 0}\frac{1}{u}=0$ and let $E_{n-k}=L_{E_k}(\mathbb{F}_{2^n})$. Then we have $\sum_{v\in E_{n-k};v\neq 0}\frac{1}{v}=0$ and the inverse function is not $(n-k)$th-order sum-free.*
Thus, kth-order sum-freedom and $(n-k)$th-order sum-freedom are equivalent for the multiplicative inverse function.

Proof. Let F_{n-k} be a vector space whose image by L_{E_k} equals E_{n-k} and having dimension $n-k$ (i.e. having a trivial intersection with the kernel E_k of L_{E_k} and whose direct sum with E_k equals $\mathbb{F}_{2^n}$). According to Corollary 1, we have:

$$\sum_{u\in E_k;u\neq 0}\frac{1}{u}+\left(\prod_{u\in E_k,u\neq 0}u\right)\sum_{v\in E_{n-k};v\neq 0}\frac{1}{v}=\sum_{u\in E_k\oplus F_{n-k};u\neq 0}\frac{1}{u}=\sum_{u\in\mathbb{F}_{2^n}^*}\frac{1}{u}=0,$$

and therefore, since $\sum_{u\in E_k;u\neq 0}\frac{1}{u}=0$ and $\prod_{u\in E_k,u\neq 0}u\neq 0$, we have:
$\sum_{v\in E_{n-k};v\neq 0}\frac{1}{v}=0$. □

Remark. Let E_k be such that $\sum_{u\in E_k,u\neq 0}\frac{1}{u}=0$ and let E_l be a subspace of E_k. Then $\sum_{u\in E_l,u\neq 0}\frac{1}{u}=0$ if and only if $\sum_{u\in E_{k-l},u\neq 0}\frac{1}{u}=0$, where $E_{k-l}=L_{E_l}(E_k)$. ◇

Remark. Theorem 3 and the fact that, if the inverse function is not kth-order sum-free over a given field, then the same happens on any of its Galois extensions, shows that if n divides an integer m and the multiplicative inverse function is not kth-order sum-free over $\mathbb{F}_{2^n}$ then it is neither kth-order sum-free nor $(n-k)$th-order sum-free nor $(m-k)$th-order sum-free, nor $(m-n+k)$th-order sum-free over $\mathbb{F}_{2^m}$. ◇

Remark. Theorem 3 can also be deduced from Relation (6) and the polynomial equality, recalled in Subsection 3.1, that (without any reduction by, for instance, $x^{2^n}+x$):

$$L_{E_k}\circ L_{E_{n-k}}(x)=L_{E_{n-k}}\circ L_{E_k}(x)=x^{2^n}+x.$$

Indeed, according to this double equality, and since the coefficient of x^2 in $x^{2^n}+x$ equals 0 and the coefficient of x in $L_{E_k}(x)$ is nonzero as well as that of x in

$L_{E_{n-k}}(x)$, the coefficient of x^2 in $L_{E_k}(x)$ equals zero if and only if the coefficient of x^2 in $L_{E_{n-k}}(x)$ equals zero. $\diamond$

A second consequence, on the structure of the set K of values k such that the inverse function is not kth-order sum-free The following lemma will allow us to show the stability of K under addition and subtraction, with constraints.

Lemma 1 *Let U and V be two vector subspaces of the vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. If $(n - \dim U)(\dim V) < n$, then there exists a nonzero element $a \in \mathbb{F}_{2^n}$ such that $a\,V \subset U$.*

Proof. Let $U^\perp$ be the orthogonal of U with respect to the inner product $x \cdot y = tr_n(xy)$, where tr_n is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. Let $(e_1, \ldots, e_{n-\dim U})$ be a basis of $U^\perp$. For every $x \in \mathbb{F}_{2^n}$, we have $x \in U$ if and only if $tr_n(x\,e_i) = 0$ for every $i \in \{1, \ldots, n - \dim U\}$. Let $(f_1, \ldots, f_{\dim(V)})$ be a basis of V. Since the intersection between any d-dimensional vector subspace of $\mathbb{F}_{2^n}$ and any linear hyperplane of $\mathbb{F}_{2^n}$ has dimension at least $d-1$, the vector space $\{a \in \mathbb{F}_{2^n}; \forall i \in \{1, \ldots, n - \dim U\}, \forall j \in \{1, \ldots, \dim V\}, tr_n(a\,e_i f_j) = 0\}$ has dimension at least $n - (n - \dim U)\dim V > 0$. There exists then a nonzero element a in this vector space, satisfying for every element $v \in V$, that $tr_n(a\,e_i v) = 0$ for every i, that is, $a\,v$ belongs to U. This completes the proof. $\square$.

We deduce the following two results.

Theorem 4 *Let $n \geq 6$ and let two integers $l \geq 2$ and $r \geq 2$ be such that $lr < n$. If the inverse function is not lth-order sum-free nor rth-order sum-free, then it is not $(l + r)$th-order sum-free.*

Proof. Let E of dimension l and V of dimension r be two vector spaces such that $\sum_{u \in E, u \neq 0} \frac{1}{u} = \sum_{v \in V, v \neq 0} \frac{1}{v} = 0$. We can apply Lemma 1 with $U = L_E(\mathbb{F}_{2^n})$. Indeed, the dimension of U equals $n - l$ and the hypothesis of Lemma 1 is then satisfied. Let a be nonzero and such that $a\,V \subset U$. Since L_E induces an isomorphism from $\mathbb{F}_{2^n}/E$ to $L_E(\mathbb{F}_{2^n})$, there exists an $\mathbb{F}_2$-subspace F of $\mathbb{F}_{2^n}$ of dimension r such that $E \cap F = \{0\}$ and $L_E(F) = a\,V$. We have then $\sum_{v \in L_E(F); v \neq 0} \frac{1}{v} = 0$ and Corollary 1 implies then $\sum_{u \in E \oplus F; u \neq 0} \frac{1}{u} = 0$. This completes the proof. $\square$

Hence, the set K defined above is stable under the addition of small enough elements (in particular of elements strictly smaller than $\sqrt{n}$). We deduce from Theorem 4:

Corollary 2 *Let $n \geq 6$ and let r, l be two integers such that $n - 2 \geq r \geq l \geq 2$ and $l\,(n - r) < n$. If the inverse function is not lth-order sum-free nor rth-order sum-free, then it is not $(r - l)$th-order sum-free.*

Proof. Applying (thanks to Theorem 3) Theorem 4 with $n-r$ instead of r gives that if $l\,(n-r) < n$ and the inverse function is not lth-order sum-free nor rth-order sum-free, then it is not $(l+n-r)$th-order sum-free and then again according to Theorem 3, it is not $(r-l)$th-order sum-free. □

Remark. There is also a direct proof of Corollary 2 which has its own interest. Let E and U be two vector spaces of dimensions l and r, respectively, and such that $\sum_{u\in U, u\neq 0} \frac{1}{u} = \sum_{v\in E, v\neq 0} \frac{1}{v} = 0$. According to Lemma 1 with $V = E$, there exists $a \neq 0$ such that $a\,E \subset U$. Let then F be a vector subspace of U with a trivial intersection with $a\,E$ and such that $(a\,E) \oplus F = U$. Then the dimension of F equals $r-l$ and Corollary 1 shows that the inverse function sums to 0 over the $(r-l)$-dimensional vector space $L_{aE}(F)$, which proves the result. ⋄

Of course, we can apply Theorem 4 and Corollary 2 iteratively. For instance, let three integers $l \geq 2$, $r \geq 2$ and $s \geq 2$ be such that $lr < n$ and $(l+r)s < n$, then if the inverse function is not lth-order sum-free nor rth-order sum-free nor sth-order sum-free, then it is not $(l+r+s)$th-order sum-free.

A third consequence when n is composite We now give another consequence of Corollary 1 which can cover many values of k when n is composite.

Theorem 5 *Let n be any positive integer divisible by the product lr of two numbers larger than or equal to 2. Then $L_{\mathbb{F}_{2^l}}(\mathbb{F}_{2^n})$ contains an $(\frac{n}{r}-l)$-dimensional $\mathbb{F}_{2^r}$-vector subspace of $\mathbb{F}_{2^n}$ and for every k divisible by l or by r or of the form $l+jr$ where $j \in \{1,\ldots,\frac{n}{r}-l\}$ or of the form $r+jl$ where $j \in \{1,\ldots,\frac{n}{l}-r\}$, the multiplicative inverse function is not kth-order sum-free.*
In particular, for n even and divisible by an odd integer $l \geq 3$, for every $k \in \{2,4,\ldots,l-1\} \cup [\![l, n-l]\!] \cup \{n-l+1, n-l+3,\ldots,n-2\}$, the multiplicative inverse function is not kth-order sum-free. For instance, if n is divisible by 6, then the multiplicative inverse function is not kth-order sum-free for $k \in [\![2, n-2]\!]$.

Proof. We have that $L_{\mathbb{F}_{2^l}}(x) = x + x^{2^l}$ and therefore $L_{\mathbb{F}_{2^l}}(\mathbb{F}_{2^n})$ equals the kernel of the relative trace function $tr_l^n(x) = x + x^{2^l} + x^{2^{2l}} + x^{2^{3l}} + \cdots + x^{2^{n-l}}$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^l}$. This kernel includes as an $\mathbb{F}_2$-vector subspace the kernel of the relative trace function $tr_{rl}^n(x) = x + x^{2^{rl}} + x^{2^{2rl}} + \cdots + x^{2^{n-rl}}$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{rl}}$, because $tr_l^n = tr_l^{rl} \circ tr_{rl}^n$. Since tr_{rl}^n is $\mathbb{F}_{2^{rl}}$-linear, this latter kernel is an $\mathbb{F}_{2^{rl}}$-vector subspace of dimension $\frac{n}{rl} - 1$ of $\mathbb{F}_{2^n}$ and therefore an $\mathbb{F}_{2^r}$-vector subspace of $\mathbb{F}_{2^n}$, of dimension $(\frac{n}{r} - l)$.
Let us then apply Corollary 1 to $E = \mathbb{F}_{2^l}$ and to any $\mathbb{F}_2$-subspace F of $\mathbb{F}_{2^n}$ having a trivial intersection with E and whose image by $L_{\mathbb{F}_{2^l}}$ is an $\mathbb{F}_{2^r}$-vector subspace of the kernel of tr_{rl}^n. Thanks to Theorem 2 and Corollary 1, we have then $\sum_{u\in\mathbb{F}_{2^l}\oplus F} \frac{1}{u} = 0$ and $\mathbb{F}_{2^l} \oplus F$ can have for dimension over $\mathbb{F}_2$ any number of the form $l+jr$ where $j = 1,\ldots,\frac{n}{r}-l$. This completes the first part (the case " k divisible by l or by r" being covered by Theorem 2). The second part is a direct consequence by taking $r = 2$ (since all the odd numbers between l and

$n-l$ can be written as $l+jr = l+2j$ where $j = 1, \ldots, \frac{n}{r} - l = \frac{n}{2} - l)$. The last sentence is by taking $l = 3$. □

5.2.3 Viewing vector spaces as the supports of their indicators

Let $f(x)$ be any Boolean function and let $supp(f) = \{x \in \mathbb{F}_{2^n}; f(x) = 1\}$ be its support. Let $f(x) = \sum_{i=0}^{2^n-1} \delta_i x^i \in \mathbb{F}_{2^n}[x]/(x^{2^n}+x)$; $\delta_i \in \mathbb{F}_{2^n}$, be the univariate representation[3] of f.
We have that $\sum_{u \in supp(f)\setminus\{0\}} \frac{1}{u} = \sum_{x \in \mathbb{F}_{2^n}} x^{2^n-2} f(x) = \delta_0 \sum_{x \in \mathbb{F}_{2^n}} x^{2^n-2} + \delta_1 \sum_{x \in \mathbb{F}_{2^n}} x^{2^n-1} + \sum_{i=2}^{2^n-1} \left(\delta_i \sum_{x \in \mathbb{F}_{2^n}} x^{i-1}\right)$.
Among the monomials $x^{2^n-2}, x^{2^n-1}, x, x^2, \ldots, x^{2^n-2}$ the only one of algebraic degree n is x^{2^n-1}, and we know that if a Boolean or vectorial function has algebraic degree less than n, then it sums to zero over $\mathbb{F}_{2^n}$. This implies:

$$\sum_{u \in E\setminus\{0\}} \frac{1}{u} = \delta_1 \sum_{x \in \mathbb{F}_{2^n}} x^{2^n-1} = \delta_1, \tag{9}$$

that is:

Proposition 4 *Let f be any Boolean function over $\mathbb{F}_{2^n}$, then $\sum_{u \in supp(f)\setminus\{0\}} \frac{1}{u}$ equals the coefficient of x in the univariate representation of $f(x)$.*

For instance, for $f(x) = tr_n(x)$, we have $\delta_1 = 1$ and then $\sum_{u \in supp(f)\setminus\{0\}} \frac{1}{u} = 1$.

Proposition 4 leads to the question of characterizing the univariate representation of the indicators of $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$. We shall unfortunately leave this question open in general, but we will see a consequence of Proposition 4 in the next subsection.

5.2.4 On large values of k

We show now that large values of k can be addressed more easily than small ones (and since kth-order sum-freedom is equivalent to $(n-k)$th-order sum-freedom, studying the former is a simpler way for addressing the latter). We have, according to Proposition 4 that $\sum_{u \in E_k\setminus\{0\}} \frac{1}{u}$ equals the coefficient of x in the univariate representation of the indicator function $1_{E_k}(x)$. Let $(u_1, \ldots, u_{n-k})$ be a basis of ${E_k}^{\perp} = \{y \in \mathbb{F}_{2^n}; tr_n(x\,y) = 0, \forall x \in E_k\}$. We have $1_{E_k}(x) = \prod_{i=1}^{n-k}(1 + tr_n(u_i\,x)) = \sum_{b \in \{-\infty,0,\ldots,n-1\}^{n-k}} \left(\prod_{i=1}^{n-k} u_i^{2^{b_i}}\right) x^{\sum_{i=1}^{n-k} 2^{b_i}}$, where by convention $2^{-\infty} = 0$, and that the coefficient of x equals then:

$$\sum_{\substack{b \in \{-\infty,0,\ldots,n-1\}^{n-k};\\ \sum_{i=1}^{n-k} 2^{b_i} \equiv 1 \pmod{2^n-1}}} \left(\prod_{i=1}^{n-k} u_i^{2^{b_i}}\right).$$

[3]Since f is Boolean, the univariate representation of f can be written (not in a unique way) in the form $\delta_0 + tr_n(\sum_{i=0}^{2^n-1} c_i x^i)$; $c_i \in \mathbb{F}_{2^n}$, but we shall not use this.

Note that for $k = n-2$, the coefficient of x is $\sum_{\substack{b\in\{-\infty,0,\ldots,n-1\}^2;\\ 2^{b_1}+2^{b_2}\equiv 1 \pmod{2^n-1}}} u_1^{2^{b_1}} u_2^{2^{b_2}} =$ $u_1^{2^0} u_2^{2^{-\infty}} + u_1^{2^{-\infty}} u_2^{2^0} + u_1^{2^{n-1}} u_2^{2^{n-1}} = u_1 + u_2 + \left(u_1 u_2\right)^{\frac{1}{2}} = u_2\left(1 + \left(\frac{u_1}{u_2}\right)^{\frac{1}{2}} + \frac{u_1}{u_2}\right)$. Since the polynomial $1 + x + x^2$ has no zero in $\mathbb{F}_{2^n}$ for n odd, and has for zeros the two primitive elements $w, w^2 = w+1$ of $\mathbb{F}_4$ for n even, and since in the latter case, u_1 and u_2 can be $\mathbb{F}_2$-linearly independent while satisfying $\left(\frac{u_1}{u_2}\right)^{\frac{1}{2}} = w$, we can see that for $n \geq 4$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is $(n-2)$th-order sum-free if and only if n is odd, which is coherent with what we know about APNness and Theorem 3.

For $k = n-3$, the coefficient of x equals

$$\sum_{b\in\{-\infty,0,\ldots,n-1\}^3; 2^{b_1}+2^{b_2}+2^{b_3}\equiv 1 \pmod{2^n-1}} u_1^{2^{b_1}} u_2^{2^{b_2}} u_3^{2^{b_3}} =$$

$$u_1 + u_2 + u_3 + u_1^{2^{n-1}} u_2^{2^{n-1}} + u_1^{2^{n-1}} u_3^{2^{n-1}} + u_2^{2^{n-1}} u_3^{2^{n-1}} + u_1^{2^{n-2}} u_2^{2^{n-2}} u_3^{2^{n-1}} + u_1^{2^{n-2}} u_2^{2^{n-1}} u_3^{2^{n-2}} + u_1^{2^{n-1}} u_2^{2^{n-2}} u_3^{2^{n-2}}.$$

Denoting $x = u_1, y = u_2, z = u_3$ and raising to the fourth power, we have that, for $n \geq 6$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not $(n-3)$th-order sum-free if and only if the equation:

$$x^4 + x^2(y^2 + z^2 + yz) + x(y^2 z + yz^2) + y^4 + z^4 + y^2 z^2 = 0$$

admits solutions (x, y, z) such that x, y, z are $\mathbb{F}_2$-linearly independent (for $n = 5$, we know that the inverse function is 2nd-order sum-free, since n is odd).
Since this polynomial is homogeneous (of degree 4), we can assume without loss of generality that $z = 1$ (and the condition that x, y, z are $\mathbb{F}_2$-linearly independent writes then $x, y, x + y \notin \mathbb{F}_2$), since the equation is invariant when we multiply each variable by the same nonzero factor. Denoting $t = y^2 + y + 1$, the condition above becomes:

$$x^4 + tx^2 + (t+1)x + t^2 = 0, \tag{10}$$

with $tr_n(t+1) = 0$, $t \neq 1$ and $x + x^2 \notin \{0, t+1\}$. It is clear that, for n large enough (say, $n \geq 13$), there exist values of (x, t) satisfying this, since (10) writes $t^2 + (x + x^2)t + x + x^4 = 0$, which is equivalent to

$$\left(\frac{t}{x+x^2}\right)^2 + \frac{t}{x+x^2} = \frac{x+x^4}{x^2+x^4}, \tag{11}$$

and has two solutions t if and only if x is such that $tr_n\left(\frac{x+x^4}{x^2+x^4}\right) = 0$, and the number of pairs (x, t) satisfying (11) and $tr_n(t+1) = 0$ is then larger than the number of pairs (x, t) such that $t = 1$ or $x + x^2 \in \{0, t+1\}$. This completes the proof of the next corollary (thanks to Theorem 3), since the computer investigations we give below show that the result is also true for $n \in [6, 12]$.

Theorem 6 *For every $n \geq 6$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is neither third-order sum-free, nor $(n-3)$th-order sum-free.*

For $k = n-4$, the coefficient of x equals

$$\sum_{b\in\{-\infty,0,\ldots,n-1\}^4;2^{b_1}+2^{b_2}+2^{b_3}+2^{b_4}\equiv 1 \pmod{2^n-1}} u_1^{2^{b_1}} u_2^{2^{b_2}} u_3^{2^{b_3}} u_4^{2^{b_4}} =$$

$$\sum_{i=1}^{4} u_i + \sum_{1\leq i<j\leq 4} u_i^{2^{n-1}} u_j^{2^{n-1}} + \sum_{\substack{1\leq i<j\leq 4;1\leq k\leq 4\\ k\neq i,j}} u_i^{2^{n-2}} u_j^{2^{n-2}} u_k^{2^{n-1}} +$$

$$+ \sum_{\substack{1\leq i<j\leq 4;1\leq k\neq l\leq 4;\\ k,l\neq i,j}} u_i^{2^{n-3}} u_j^{2^{n-3}} u_k^{2^{n-2}} u_l^{2^{n-1}} + u_1^{2^{n-2}} u_2^{2^{n-2}} u_3^{2^{n-2}} u_4^{2^{n-2}}.$$

Denoting $x = u_1, y = u_2, z = u_3$ and taking $u_4 = 1$, we are led for $n \geq 6$ to the equation:

$$x^8 + x^4(y^4 + z^4 + y^2z^2 + y^2 + z^2 + 1 + yz + yz^2 + y^2z)+$$

$$x^2(y^2z^4 + y^4z^2 + y^2z^2 + y^2 + y^4 + z^2 + z^4 + yz + yz^4 + y^4z)+$$

$$x(yz^2 + yz^4 + y^2z + y^4z + y^2z^4 + y^4z^2)+$$

$$y^2z^2 + y^2z^4 + y^4z^2 + y^8 + z^8 + y^4 + z^4 + y^4z^4 + 1 = 0.$$

We need then to find four elements a, b, c, d of $\mathbb{F}_{2^n}$ such that there exist x, y, z such that x, y, z and 1 are linearly independent, and satisfying:

$$\begin{cases} x^8 + ax^4 + bx^2 + cx + d = 0 \\ y^4 + z^4 + y^2z^2 + y^2 + z^2 + yz + yz^2 + y^2z = a + 1 \\ yz\big(y + z + (y + z)^3\big) + y^2z^2\big(y + z + (y + z)^2\big) = a + b + 1 \\ a + b + c + 1 = 0 \\ a^2 + d = 0. \end{cases}$$

That is, we need to find two elements a, b of $\mathbb{F}_{2^n}$ such that there exist x, y, z such that x, y, z and 1 are linearly independent, and satisfying:

$$\begin{cases} x^8 + ax^4 + bx^2 + (a + b + 1)x + a^2 = 0 \\ y^4 + z^4 + y^2z^2 + y^2 + z^2 + yz + yz^2 + y^2z = a + 1 \\ yz\big(y + z + (y + z)^3\big) + y^2z^2\big(y + z + (y + z)^2\big) = a + b + 1. \end{cases} \tag{12}$$

Lemma 2 *If there exist y, z such that:*

- *y, z and 1 are linearly independent over $\mathbb{F}_2$,*
- *for some $a \neq 0$, and b, the two last equations in System (12) are satisfied, and the first equation has eight distinct solutions.*

then the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not $(n-4)$th-order sum-free.

Proof. We want to show that, under these hypotheses, at least one solution x of (12) is such that x, y, z and 1 are linearly independent. Suppose this is not the case. Since y, z and 1 are linearly independent and the first equation in (12) has eight distinct solutions, these eight solutions are the elements of the vector space generated by y, z and 1. This implies that $x^8 + ax^4 + bx^2 + (a+b+1)x + a^2 = x(x+y)(x+z)(x+1)(x+y+z)(x+y+1)(x+z+1)(x+y+z+1)$. The term not involving x after the expansion of the right-hand side of this equality equaling 0, while it is nonzero on the left-hand side, we arrive to a contradiction. □

The double condition that $a \neq 0$ and the first equation in (12), which is a linear non-homogeneous equation, has eight distinct solutions, is equivalent to saying that these eight solutions are the elements of a 3-dimensional affine space that is not a vector space. There are $(2^{n-3}-1)\frac{(2^n-1)(2^n-2)(2^n-4)}{(2^3-1)(2^3-2)(2^3-4)}$ (roughly proportional to 2^{4n}) possible linear equations of degree 8 corresponding to such a situation. The fact that the two last coefficients equal $a+b+1$ and a^2 where a, b are the two other coefficients selects a part of them of size roughly proportional to 2^{2n}. There would be different cases to consider for concretely showing this; we do not develop more, since another proof has been found (after a previous version of the present paper was on iacr ePrint Archive), which will be given in the forthcoming paper [19].
Denoting $yz = p$ and $y + z = s$, the second and third equations in (12) become

$$\begin{cases} s^4 + s^2 + p^2 + p(s+1) = a + 1 \\ \big(p^2 + p(s+1)\big)(s^2 + s) = a + b + 1, \end{cases}$$

which is equivalent to:

$$\begin{cases} p^2 + p(s+1) = s^4 + s^2 + a + 1 \\ \big((s^2+s)^2 + a + 1\big)(s^2 + s) = a + b + 1. \end{cases}$$

The first equation has solutions p, given s, if and only if $\frac{s^4+s^2+a+1}{s^2+1}$ has trace 0 (which is not very selective) and many solutions to the second equation satisfy this condition and correspond to y, z such that y, z and 1 are linearly independent. The hypothesis of Lemma 2 is then satisfied by a large number of solutions for $n \geq 13$. And for $6 \leq n \leq 12$, our computational results below show the existence of solutions as well. We deduce, using again Theorem 3:

Theorem 7 *For every $n \geq 6$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is neither fourth-order sum-free, nor $(n-4)$th-order sum-free.*

Theorem 7, and Theorem 4 successively applied for the pairs:

$$(l, r) = (4, 4), (8, 4), \ldots, (4(b-1), 4), (4b, 3), (3 + 4b, 3) \ldots, (3(a-1) + 4b, 3)$$

show:

Corollary 3 *For all numbers k of the form $3a + 4b$ such that $16(b-1) < n$ and $3\big(3(a-1) + 4b\big) < n$ with $a \in \mathbb{N}^*, b \in \mathbb{N}$, the inverse function is not kth-order sum-free nor $(n-k)$th-order sum-free.*

Table 1: The kth-order sum-free status of the inverse function for small n

n \ k	1	2	3	4	5	6	7	8	9	10	11	12
6	✓	¬	¬	¬	✓	¬						
7	✓	✓	¬	¬	✓	✓	¬					
8	✓	¬	¬	¬	¬	¬	✓	¬				
9	✓	✓	¬	¬	¬	¬	✓	✓	¬			
10	✓	¬	¬	¬	¬	¬	¬	¬	✓	¬		
11	✓	✓	¬	¬	¬	¬	¬	¬	✓	✓	¬	
12	✓	¬	¬	¬	¬	¬	¬	¬	¬	¬	✓	¬

The cases $k = 5, \ldots, n-5$ could be studied similarly, but the number of variables $x, y, z, \ldots$, and the number of equations in the related system of equations of unknowns $a, b, c, \ldots$, increasing with k, the amount of work would increase as well, and an idea (to be found) for addressing all $k \in \{3, \ldots, n-3\}$ with less calculations would be nicer.

5.2.5 Computer investigation

A computer investigation has been made with the kind help of Stjepan Picek. For each pair (n, k) where $n \in [\![6, 12]\!]$ and $k \in [\![3, n-3]\!]$, a k-dimensional vector space E has been found such that $\sum_{u \in E, u \neq 0} \frac{1}{u} = 0$. We display in Table 1 with "✓" each value of k for which the multiplicative inverse function is kth-order sum-free and with "¬" when it is not.
All these investigation results are explained for every k by the theorems above.

Note that for $n = 8$, which is particularly interesting because of AES, we know mathematically the status of all values of k (for $k = 7$ the inverse function is kth-order sum-free, and for $k = 2$, it is not as we know and for $k = 3, 4, 5, 6$, it is not, according to Theorem 6, Theorem 2, Theorem 3, Theorem 2 or 3, respectively).

5.3 Perspectives

Given the computer investigations above, it seems that, for $k \in \{3, \ldots, n-3\}$, the inverse function is not kth-order sum-free. We leave open the problem of proving or disproving this fact (we tend to think it is true).
Considering now other functions than the inverse function, there is an example, given in [11], of a class of (n, n)-functions such that, for any $k \geq 2$ and any $n \geq k$, one of the (n, n)-functions in the class, namely the function x^{2^k-1}, is kth order sum-free (we have then, for every k, an infinite class of kth order sum-free functions). We leave open the question of finding (infinite classes of)

(n,n)-functions being kth order sum-free for several values of $k \in \{3,\ldots,n-3\}$ (note that, for n odd, the inverse function is kth order sum-free for two values of k: 2 and $n-2$). We would even more like to find examples of (n,n)-functions being kth order sum-free for an unbounded number of values of k.

Acknowledgements

This paper is devoted to the memory of Kai-Uwe Schmidt, who made considerably progress our understanding of Boolean functions (in parallel to his well-known works on many other topics) and solved very difficult open problems on them.

We thank Xiang-Dong Hou for his detailed reading of the paper which helped improving it, and for useful references. We also thank the anonymous reviewers, thanks to whom the presentation of the paper could be reorganized in a more direct way. We thank for their kind help Lilya Budaghyan and Stjepan Picek for providing computer investigation results, Gary McGuire for his nice suggestions, Sihem Mesnager for her useful information, Alexandr Polujan for useful references and Patrick Solé for his indications.

References

[1] E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv. Subspace polynomials and cyclic subspace codes. *IEEE Transactions on Information Theory* 62(3), pp.1157-1165, 2016.

[2] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan and S. Vadhan. Short PCPs verifiable in polylogarithmic time. *20th Annual IEEE Conference on Computational Complexity (CCC'05)*, pp. 120-134, 2005.

[3] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan and S. Vadhan. Robust PCPs of proximity, shorter PCPs, and applications to coding. *SIAM Journal on Computing* 36 (4), pp. 889-974, 2006.

[4] E. Ben-Sasson and S. Kopparty. Affine dispersers from subspace polynomials. *SIAM Journal on Computing* 41(4), pp. 880-914, 2012.

[5] E. Ben-Sasson, S. Kopparty and J. Radhakrishnan. Subspace polynomials and list decoding of Reed-Solomon codes. *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pp. 207-216, 2006.

[6] E. Ben-Sasson and M. Sudan. Simple PCPs with poly-log rate and query complexity. *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pp. 266-275, 2005.

[7] E. Berlekamp, *Algebraic Coding Theory,* McGraw-Hill, New York, 1968.

[8] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science* 765, pp. 65-76, 1994.

[9] C. Carlet. Characterizations of the differential uniformity of vectorial functions by the Walsh transform, *IEEE Transactions on Information Theory* 64 (9), pp. 6443-6453, 2018. (preliminary version available in *IACR Cryptology ePrint Archive* http://eprint.iacr.org/ 2017/516, 2017).

[10] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.

[11] C. Carlet. Two generalizations of almost perfect nonlinearity. *IACR ePrint Archive* 2024/841.

[12] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT 1994, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.

[13] W. YC. Chen and J. D. Louck. The combinatorial power of the companion matrix. *Linear Algebra and Its Applications* 232, pp. 261-278, 1996.

[14] Q. Cheng, S. Gao and D. Wan. Constructing high order elements through subspace polynomials. *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1457-1463, 2012.

[15] B. Csajbók, G. Marino, O. Polverino and F. Zullo. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications* 56, pp.109-130, 2019.

[16] J. Daemen and V. Rijmen. AES proposal: Rijndael, 1999. See http://www.quadibloc.com/crypto/co040401.htm

[17] J. Daemen and V. Rijmen. Understanding two-round differentials in AES. *Proceedings of International Conference on Security and Cryptography for Networks, Lecture Notes in Computer Science* 4116, pp. 78-94, 2006.

[18] R. Dargazany, K. Hörnes and M. Itskov. A simple algorithm for the fast calculation of higher order derivatives of the inverse function. *Applied Mathematics and Computation* 221, pp. 833-838, 2013.

[19] A. Ebeling, X.-D. Hou, A. Rydell and S. Zhao. On sum-free functions. Preprint, 2024.

[20] N. Kolomeec and D. Bykov. On the image of an affine subspace under the inverse function within a finite field. *Designs, Codes and Cryptograhy* Volume 92, pp. 467-476, 2024.

[21] S. Lang, *Cyclotomic fields I and II*. Graduate Texts in Mathematics 121, Springer-Verlag, New York, 1990.

[22] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stănică. Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. *IEEE Transactions on Information Theory* 66 (11), pp.7101-7112, 2020.

[23] R. Lidl and H. Niederreiter. *Finite Fields* (vol. 20), Cambridge university press, 1997.

[24] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland. 1977.

[25] G. McGuire and D. Mueller. Some results on linearized trinomials that split completely. *Proceedings of Finite Fields and their Applications Fq14*, pp.149-164, 2020.

[26] G. McGuire and J. Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications* 57, pp.68-91, 2019.

[27] S. Mesnager. *Linear Codes from Functions*, Chapter 20 in "A Concise Encyclopedia 1419 Coding Theory" CRC Press/Taylor and Francis Group (Publisher), London, New York, 2021 (94 pages).

[28] S. Mesnager, K. H. Kim, M. S. Jo. On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic Boolean functions. *Cryptography and Communications* 12 (4), pp. 659-674, 2020.

[29] K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[30] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[31] O. Ore. On a special class of polynomials. *Transactions of the American Mathematical Society* 35 (3), pp.559-584, 1933

[32] O. Ore. Contributions to the theory of finite fields. *Transactions of the American Mathematical Society* 36 (2), pp.243-274, 1934.

[33] K.U. Schmidt. Nonlinearity measures of random Boolean functions. *Cryptography and Communications* 8, pp.637-645, 2016.

[34] K.U. Schmidt. Asymptotically optimal Boolean functions. *Journal of Combinatorial Theory, Series A*, 164, pp.50-59, 2019.

[35] A. Wachter-Zeh. Bounds on list decoding of rank-metric codes. *IEEE Transactions on Information Theory* 59 (11), pp. 7268-7277, 2013.

[36] B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*, 22:79 – 100, 2013.

[37] C. Zanella. A condition for scattered linearized polynomials involving Dickson matrices. *Journal of Geometry*, 110.3:50, 2019.