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 (APN), called kth-order sum-freedom, that extends a classical 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 $k \leq n$. 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) is easy to address: there exists a simple expression of such sum which shows that it never vanishes. We study in the present paper the case of a vector subspace (a linear subspace), which is much less simple to handle. We show that the sum depends on a coefficient in subspace polynomials. We derive several expressions of this coefficient. Then 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 results on the sums of values of the inverse function over vector subspaces, addressing in particular the cases of dimension at most 3 (equivalently, of co-dimension at most 3). We leave other cases open and provide computer investigation results.

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

Keywords: finite field, multiplicative inverse function, cryptography.

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

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 of the values taken by F over A is nonzero.

In the present paper, we study the behavior relative to this notion of the currently most important example of a vectorial function 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 $\frac{1}{0} = 0$ (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 that it 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 for which values of k it sums to nonzero values over all k-dimensional vector spaces, which is a much more difficult problem, that we only partially solve. It seems that the mathematical study of the sum of the inverse function over all affine subspaces has never been made, while an algorithmic approach exists in [17].

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. We give in Section 5 a rather well structured expression, which is however not simple enough for allowing us to determine all the pairs (n, k) for which the inverse function over $\mathbb{F}_{2^n}$ is kth-order-sum-free. 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 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. 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 $\mathbb{F}_{2^n}$. We address a few other cases of k, and all vector spaces of dimension at most 3 or of co-dimension at most 3 for every n, and all those of dimension 4 or of co-dimension 4 when n is even.

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 $\mathbb{F}_2^m[x_1,\ldots,x_n]/(x_1^2-x_1,\ldots,x_n^2-x_n)$ 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" and not "equal to" to allow 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 affine planes $\{x,y,z,x+y+z\}$ 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[1]), 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, 20, 22, 23, 25, 28, 29, 32, 33, 34]. 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. $\diamond$

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. 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} 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 $L_{E_k}(x) = L_{E_{k-1}}(x) L_{E_{k-1}}(x + a_k) =$

[1] 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.

$L_{E_{k-1}}(x)\left(L_{E_{k-1}}(x)+L_{E_{k-1}}(a_k)\right)$, 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 can be checked by induction that L_{E_k} is linear. Moreover, $L_{E_k}(x)$ equals, up to a multiplicative contant, the determinant of the matrix:

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

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 trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$.

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 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 $Im(L_{E_k})$. ◇

Remark. Let $L^*_{E_k}(x)=\sum_{i=0}^k(b_ix)^{2^{n-i}}$ be the adjoint operator of $L_{E_k}=\sum_{i=0}^k b_ix^{2^i}$, 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 $Im(L^*_{E_k})=E_k^\perp$. ◇

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

3.1.1 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:

- Of course, as observed in [1], we have that $L_{\alpha E}(x)=\alpha^{2^k}L_E(\alpha^{-1}x)$ for every $\alpha\in\mathbb{F}^*_{2^n}$, and that applying the Frobenius automorphism to E results in applying it to each coefficient in $L_E(x)$. It is also proved in this same paper that,

given two vector subspaces E and E' such that $\dim(E) = k \geq \dim(E') = k'$, denoting by 2^j (resp. $2^{j'}$) the second highest degree of the monomials in $L_E(x)$ (resp. $L_{E'}(x)$), we have $\dim(E \cap E') \leq r = \max(j, j' + k - k')$. This is a direct consequence of the relations $L_{E\cap E'}(x) = \gcd(L_E(x), L_{E'}(x)) = \gcd(L_E(x), (L_{E'}(x))^{2^{k-k'}}) = \gcd(L_E(x), L_E(x)+(L_{E'}(x))^{2^{k-k'}})$ and $\deg(L_E(x)+(L_{E'}(x))^{2^{k-k'}}) \leq 2^r$ (the second equality above coming from the fact that $L_E(x)$ 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 $L_E(x) = x^{2^r}+x$, $E' = \ker(tr^n_r), L_{E'}(x) = tr^n_r(x)$ 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, 23] 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 [20], 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 [21], 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:

$n = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, \ldots$).

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 of the multiplicative inverse function taken 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 $i = 0, \ldots, k$, with the convention $b_{k-1,-1} = 0$.
The only monomial in (4) having a nonzero derivative (here we mean the classical derivative of a polynomial function) is x. We have then that $L'_{E_k}(x)$ equals the constant polynomial $b_{k,0} = \prod_{u\in E_k, u\neq 0} u \neq 0$. We also have, by the application of the classical 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 $x = 0$). It equals $\sum_{u\in E_k, u\neq 0} \frac{1}{u}$ and we would like to have a closed form as in the case $x \notin E_k$.

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), the inverse function does not sum to 0 over H. Indeed, according to Theorem 1, it does not sum to 0 over the complement of H in E (which is a coset). Hence, if the inverse function is neither kth-order free nor $(k-1)$th-order free, the $(k-1)$-dimensional vector space over which it sums to zero cannot be a subspace of the k-dimensional vector space over which it sums to zero.

Similarly, for every vector subspace F of $\mathbb{F}_{2^n}$ whose E is a hyperplane, the inverse function does not sum to 0 over F. Indeed, it does not sum to 0 over the complement of E in F.

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

5.1.1 Relating the sum of inverses over E_k and $b_{k,1}$

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 $\phi_k'(x) = \displaystyle\sum_{u\in E_k,u\neq 0}\prod_{v\neq 0, v\neq u}(x+v)$ 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 [25, 33, 34] 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 $b_{k,1} \neq 0$. $\diamond$

5.1.2 Generalization

Proposition 2 *Let $c_1,\dots,c_{n-1}$ be elements of $\mathbb{F}_{2^n}$. If a k-dimensional vector space E_k is included in a vector space E' of equation:*

$$x=\sum_{j=1}^{n-1} c_j x^{2^j}, \tag{7}$$

then we have:

$$\sum_{u\in E_k} u^{-1}=c_1+\sum_{j=k+1}^{n-1} c_j\Big(\sum_{u\in E_k} u^{2^j-2}\Big). \tag{8}$$

Proof. Relation (7) implies, for every $x\in E_k\setminus\{0\}$ and after division by x^2, that $x^{-1}=\sum_{j=1}^{n-1} c_j x^{2^j-2}$. We deduce $\sum_{u\in E_k} u^{-1}=\sum_{j=1}^{n-1} c_j\Big(\sum_{u\in E_k\setminus\{0\}} u^{2^j-2}\Big)$. For $j=1$, $\sum_{u\in E_k\setminus\{0\}} u^{2^j-2}$ equals the sum modulo 2 of 2^k-1 elements equal to 1, and therefore equals 1. For $j\geq 2$, the exponent $2^j-2\geq 2$ has 2-weight $j-1$ and x^{2^j-2} has then algebraic degree $j-1$. We know that a vectorial function of algebraic degree less than k sums to zero over E_k. We have then $\sum_{u\in E_k\setminus\{0\}} u^{2^j-2}=\sum_{u\in E_k} u^{2^j-2}=0$ if $2\leq j\leq k$. The proof is complete. □

Note that the hypothesis of Proposition 2 is always satisfied with $E'=E_k$, for which, since $b_{k,0}\neq 0$, we have $c_j=\frac{b_{k,j}}{b_{k,0}}$ for $j=1,\dots,k$ and $c_{k+1}=\cdots=c_{n-1}=0$. Then we recover the result of Proposition 1.

The result of Proposition 2 is of course much more general than that of Proposition 1, but finding cases of application leading to new results seems challenging.

Indeed, in some cases, the result of Proposition 2 does not give anything new:
(i) When E_k is a subspace of E_{k+1} and we apply firstly Proposition 2 with $c_j=\frac{b_{k+1,j}}{b_{k+1,0}}$ for $j=1,\dots,k+1$ and $c_{k+2}=\cdots=c_{n-1}=0$, and secondly Relation (6) with $k+1$ in the place of k, we get:

$$\sum_{u\in E_k} u^{-1}=\frac{b_{k+1,1}}{b_{k+1,0}}+\frac{1}{b_{k+1,0}}\Big(\sum_{u\in E_k} u^{2^{k+1}-2}\Big)=\sum_{u\in E_{k+1}} u^{-1}+\frac{1}{b_{k+1,0}}\Big(\sum_{u\in E_k} u^{2^{k+1}-2}\Big),$$

and this only provides an alternative expression for $\sum_{u\in E_{k+1}\setminus E_k} u^{-1}$, which we know is non-zero.
(ii) When $c_1=\cdots=c_{l-1}=c_{l+1}=\cdots=c_{n-1}=0$ and $c_l=1$, then E_k being a subspace of the vector space of equation $x=x^{2^l}$, that is of the field $\mathbb{F}_{2^{\gcd(l,n)}}$, we have that $k\leq\gcd(l,n)$ and $\sum_{u\in E_k} u^{-1}=\sum_{u\in E_k} u^{2^l-2}$ equals $\sum_{u\in E_k} u^{2^{\gcd(l,n)}-2}$ (since we have $u^{2^l}=u=u^{2^{\gcd(l,n)}}$ in $\mathbb{F}_{2^{\gcd(l,n)}}$) and this only tells us that addressing $\sum_{u\in E_k} u^{-1}$ can be made within the subfield $\mathbb{F}_{2^{\gcd(l,n)}}$, which is obvious. Changing $c_l=1$ into $c_l\neq 0$ does not change much the situation (then $\mathbb{F}_{2^{\gcd(l,n)}}$ is simply replaced by $\lambda\mathbb{F}_{2^{\gcd(l,n)}}$ for some λ).

There are examples where we get some new information but saying whether the inverse functions sums to zero over E_k is still difficult after having these results:
(i') When E_k is a subspace of E_{k+2} and $c_j = \frac{b_{k+2,j}}{b_{k+2,0}}$ for $j = 1, \ldots, k+2$ and $c_{k+3} = \cdots = c_{n-1} = 0$. We obtain that

$$\begin{aligned}\sum_{u\in E_k} u^{-1} &= \frac{b_{k+2,1}}{b_{k+2,0}} + \frac{b_{k+2,k+1}}{b_{k+2,0}}\Big(\sum_{u\in E_k} u^{2^{k+1}-2}\Big) + \frac{1}{b_{k+2,0}}\Big(\sum_{u\in E_k} u^{2^{k+2}-2}\Big)\\ &= \sum_{u\in E_{k+2}} u^{-1} + \frac{b_{k+2,k+1}}{b_{k+2,0}}\Big(\sum_{u\in E_k} u^{2^{k+1}-2}\Big) + \frac{1}{b_{k+2,0}}\Big(\sum_{u\in E_k} u^{2^{k+2}-2}\Big).\end{aligned}$$

(ii') When $c_{k+1} = \cdots = c_{l-1} = c_{l+1} = \cdots = c_{n-1} = 0$ and $c_l \neq 0$, that is, when E' has equation $x = c_l x^{2^l} + \sum_{j=1}^{k} c_j x^{2^j}$, for some $c_1, \ldots, c_k, c_l \in \mathbb{F}_{2^n}$, then (8) writes $\sum_{u\in E_k} u^{-1} = c_1 + c_l \sum_{u\in E_k} u^{2^l-2}$, while E_k is no more a subspace of a subfield of $\mathbb{F}_{2^l}$ (in fact, l needs no more to be a divisor of n), and to show that the inverse function sums to zero over E_k, it is sufficient to find $c_1, \ldots, c_k, c_l \in \mathbb{F}_{2^n}$ such that $E_k \subseteq E'$ and $c_1 = c_l \sum_{u\in E_k} u^{2^l-2}$. A particular case to be looked at is when $c_1 = \sum_{u\in E_k} u^{2^l-2} = 0$. Note that $\sum_{u\in E_k} u^{2^l-2} = \sum_{x\in\mathbb{F}_{2^n}} 1_{E_k}(x) x^{2^l-2}$ equals the coefficient of $x^{2^n+1-2^l}$ in the univariate form of $1_{E_k}(x)$.

5.2 On the expression of the sum by means of a basis of the vector subspace

The previous subsection only produces a link between the sum of inverses on a vector space and the coefficients of its subspace polynomial. Unlike the case of affine spaces, this connection does not provide a solution so far, and it may only shift the problem. To go further in this direction, we would need a concrete expression for $b_{k,1}$. This is what we are working on in the present subsection.

5.2.1 An expression as a sum of k terms

Relation (3) gives:

$$\begin{aligned}
\phi_k(x) &= x\left(\phi_{k-1}(x)\right)^2 + L_{E_{k-1}}(a_k)\phi_{k-1}(x)\\
&= x\left(\phi_{k-1}(x)\right)^2 + \frac{\phi_k(0)}{\phi_{k-1}(0)}\phi_{k-1}(x),\\
\phi_k(0) &= L_{E_{k-1}}(a_k)\phi_{k-1}(0) = a_k\phi_{k-1}(a_k)\phi_{k-1}(0),\\
\phi'_k(0) &= \left(\phi_{k-1}(0)\right)^2 + \frac{\phi_k(0)}{\phi_{k-1}(0)}\phi'_{k-1}(0),\\
\frac{\phi'_k(0)}{\phi_k(0)} &= \frac{\left(\phi_{k-1}(0)\right)^2}{\phi_k(0)} + \frac{\phi'_{k-1}(0)}{\phi_{k-1}(0)} = \frac{\phi_{k-1}(0)}{a_k\phi_{k-1}(a_k)} + \frac{\phi'_{k-1}(0)}{\phi_{k-1}(0)}\\
&= \dots\\
&= \sum_{i=1}^{k}\frac{\phi_{i-1}(0)}{a_i\phi_{i-1}(a_i)},
\end{aligned}$$

this latter expression being obtained by iteration and using that $\phi_0(x) = 1$. Relation (6) gives then:

Proposition 3 *Let $a_1, \dots, a_k$ be linearly independent elements of $\mathbb{F}_{2^n}$ and $E_k = \langle a_1, \dots, a_k\rangle$ the vector space over $\mathbb{F}_2$ spanned by $a_1, \dots, a_k$. We have:*

$$\begin{aligned}
\sum_{u\in E_k, u\neq 0}\frac{1}{u} &= \sum_{i=1}^{k}\frac{\prod_{u\in E_{i-1}, u\neq 0} u}{\prod_{u\in E_{i-1}}(a_i+u)}\\
&= \frac{1}{a_1} + \frac{a_1}{a_2(a_2+a_1)} + \frac{a_1a_2(a_1+a_2)}{a_3(a_3+a_1)(a_3+a_2)(a_3+a_1+a_2)} + \dots +\\
&\quad \frac{\prod_{u\in E_{k-1}, u\neq 0} u}{\prod_{u\in E_{k-1}}(a_k+u)}.
\end{aligned}$$

This provides an expression of $\sum_{u\in E_k, u\neq 0}\frac{1}{u}$ as a sum of k terms (that are all nonzero), which is more compact than the sum of $2^k - 1$ terms provided by its definition, but does not seem useful for deducing any indication on when $\sum_{u\in E_k, u\neq 0}\frac{1}{u}$ vanishes (except that if the sum of inverses is zero on E_k then it is nonzero on E_{k-1} and on E_{k+1}). Moreover, it is not well structured (in particular, the fact that $\sum_{u\in E_k, u\neq 0}\frac{1}{u}$ is a symmetric function in $a_1, \dots, a_k$ is hidden by the formula).

5.2.2 An expression involving more terms but better structured

We observe that, since $\phi_{k+1}(0) = \phi_k(0)\, L_{E_k}(a_{k+1}) = \phi_k(0)\, a_{k+1}\, \phi_k(a_{k+1})$, and since a_{k+1} can vary in this expression[2] and can then play the role of a variable

[2] It varies outside E_k, but this makes enough points for an interpolation since the degree 2^k of $\phi_{k+1}(0)$ viewed as a polynomial in a_{k+1} is less than the size of the complement of E_k; this restriction on the domain of a_{k+1} therefore does not induce any limitation.

x, the expression of $\phi_k(x)$ can be obtained by replacing k by $k+1$ in any expression we have for $\phi_k(0)$ and a_{k+1} by x in $\phi_{k+1}(0)$ and dividing by $x\,\phi_k(0)$. The coefficient of x in $\phi_k(x)$ (that is, the value of $\phi_k'(0)$) will then be directly deduced.

For this, we need an expression of $\phi_k(0)$, in a form as closed as possible. Note that we have $\phi_2(0) = a_1a_2(a_1+a_2) = a_1^2a_2 + a_1a_2^2 = D_{a_1}D_{a_2}P_2(x)$, where $P_k(x) = x^{2^k-1}$, and $\phi_3(0) = a_1a_2a_3(a_1+a_2)(a_1+a_3)(a_2+a_3)(a_1+a_2+a_3) = a_1a_2^2a_3^4 + a_1a_2^4a_3^2 + a_1^2a_2a_3^4 + a_1^2a_2^4a_3 + a_1^4a_2a_3^2 + a_1^4a_2^2a_3 = D_{a_1}D_{a_2}D_{a_3}P_3(x)$. In the next theorem, we prove that $\phi_k(0) = D_{a_1}\dots D_{a_k}P_k(x)$ for every k. This result has its own interest since it relates the product $b_{k,0}$ of the nonzero elements of E_k to a derivative (while a derivative is naturally related to a sum of values). We deduce an expression of $b_{k,1}$.

Theorem 2 *Let $2 \le k \le n$. Let G_k be the set of bijective functions from $\{1,\dots,k\}$ to $\{0,\dots,k-1\}$ and G_k' the set of bijective functions from $\{1,\dots,k\}$ to $\{0,2,\dots,k\}$. Let E_k be any k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_2^n$ and $(a_1,\dots,a_k)$ a basis of E_k. Let $P_k(x) = x^{2^k-1}$. Then, denoting $\phi_k(x) = \prod_{u\in E_k,u\neq 0}(x+u) = \sum_{i=0}^k b_{k,i}x^{2^i-1}$ and $\mathcal{L}_k(a_1,\dots,a_k) = \sum_{\sigma\in G_k}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$ and $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k) = \sum_{\sigma\in G_k'}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$, we have, for every $x\in\mathbb{F}_{2^n}$:*

$$\phi_k(0) = \prod_{l\in\mathbb{F}_2^k,l\neq 0}\left(\sum_{i=1}^k l_ia_i\right) = D_{a_1}\dots D_{a_k}P_k(x) = \mathcal{L}_k(a_1,\dots,a_k), \tag{9}$$

$$\phi_k(x) = \frac{\sum_{\sigma\in G_{k+1}}\left(\prod_{i=1}^k a_i^{2^{\sigma(i)}}\right)x^{2^{\sigma(k+1)}-1}}{\phi_k(0)}, \tag{10}$$

and

$$\sum_{u\in E_k,u\neq 0}\frac{1}{u} = \frac{\phi_k'(0)}{\phi_k(0)} = \frac{\sum_{\sigma\in G_k'}\prod_{i=1}^k a_i^{2^{\sigma(i)}}}{(\phi_k(0))^2} = \frac{\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)}{(\mathcal{L}_k(a_1,\dots,a_k))^2}. \tag{11}$$

Proof. Relation (9) has been already proved in [11]. Let us show it in a slightly more direct way. We first observe that the polynomial $D_{a_1}\dots D_{a_k}P_k(x)$ is constant since $P_k(x)$ has algebraic degree k. We shall then fix $x=0$. We have $\phi_k(0) = b_{k,0} = \prod_{u\in E_k,u\neq 0}u = \prod_{l\in\mathbb{F}_2^k,l\neq 0}\left(\sum_{i=1}^k l_ia_i\right)$. The value $D_{a_1}\dots D_{a_k}P_k(0)$ equals 0 when $a_1\dots,a_k$ are $\mathbb{F}_2$-linearly dependent (this is true for any polynomial). Hence, each of the factors of $\prod_{l\in\mathbb{F}_2^k,l\neq 0}\left(\sum_{i=1}^k l_ia_i\right)$ (which are pairwise co-prime multivariate polynomials in $a_1,\dots,a_k$) divides $D_{a_1}\dots D_{a_k}P_k(0)$. The set of multivariate polynomials over $\mathbb{F}_{2^n}$ in $a_1,\dots,a_k$ being an integral domain and a unique factorization domain, $\prod_{l\in\mathbb{F}_2^k,l\neq 0}\left(\sum_{i=1}^k l_ia_i\right)$ divides then $D_{a_1}\dots D_{a_k}P_k(0)$.

The two multivariate polynomials $\prod_{l\in\mathbb{F}_2^k,l\neq 0}\left(\sum_{i=1}^k l_ia_i\right)$ and $D_{a_1}\dots D_{a_k}P_k(0)$

are monic. To show they are equal, we only need then to show that they have the same degree. The degree of $\prod_{l\in\mathbb{F}_2^k, l\neq 0}\left(\sum_{i=1}^k l_i a_i\right)$ equals 2^k-1. We have $P_k(x)=\prod_{i=1}^k L_i(x)$, where $L_i(x)=x^{2^{i-1}}$ is linear, which implies $D_{a_1}\dots D_{a_k}P_k(x)=\sum_{\sigma\in S_k}\prod_{i=1}^k L_{\sigma(i)}(a_i)$, where S_k is the symmetric group over $\{1,\dots,k\}$. We have then $D_{a_1}\dots D_{a_k}P_k(x)=\mathcal{L}_k(a_1,\dots,a_k)$. This proves that $D_{a_1}\dots D_{a_k}P_k(0)$ has also degree 2^k-1 as a polynomial in $a_1,\dots,a_k$ and it completes the proof of Relation (9).

Relation (10) is deduced by replacing k by $k+1$ and a_{k+1} by x (see the observations made before the theorem; note that even when $x\in E_k$, it is valid since it writes $0=0$ if $x\neq 0$ and is correct too if $x=0$).

Relation (11) is obtained by calculating the derivative of both sides in (10): $\phi'_k(0)=\frac{\sum_{\sigma\in G_{k+1};\sigma(k+1)=1}\left(\prod_{i=1}^k a_i^{2^{\sigma(i)}}\right)}{\phi_k(0)}$. □

5.2.3 More on $\mathcal{L}$ and $\widetilde{\mathcal{L}}$

The univariate polynomial $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$ is divisible by $L_{E_k}(x)$, where E_k is the vector space generated by $a_1,\dots,a_k$. Indeed (see above), the constant function $D_{a_1}\dots D_{a_{k+1}}P_{k+1}(x)$ vanishes when $a_1,\dots,a_{k+1}$ are linearly dependent and therefore, $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$ vanishes when x is linearly dependent of $a_1,\dots,a_k$, which implies that all the elements of E_k are zeros of $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$. Hence, since $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$ and $L_{E_k}(x)$ have the same degree 2^k, the normalized version of $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$ is equal to $L_{E_k}(x)$ and, since according to the expression of $\mathcal{L}$, the coefficient of x^{2^k} in $\mathcal{L}_{k+1}(a_1,\dots,a_k,x)$ equals $\mathcal{L}_k(a_1,\dots,a_k)$, we have:

$$\frac{\mathcal{L}_{k+1}(a_1,\dots,a_k,x)}{\mathcal{L}_k(a_1,\dots,a_k)}=L_{E_k}(x).$$

Assuming now that $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)=0$, let us fix $a_1,\dots,a_{k-1}$ and consider the univariate polynomial function $x\in\mathbb{F}_{2^n}\mapsto\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$. This linearized polynomial has for zeros the elements of the $\mathbb{F}_2$-vector space E_k generated by $a_1,\dots,a_k$ (indeed[3], all these 2^k elements are zeros and $\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$ has degree 2^k). Hence, $L_{E_k}(x)=\prod_{l\in\mathbb{F}_2^k}\left(x+\sum_{i=1}^k l_i a_i\right)$ divides $\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$, and since these two polynomials have the same degree, the normalized version of $\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$ equals $L_{E_k}(x)$. Note that the coefficient of x^{2^k} in $\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$ equals $\widetilde{\mathcal{L}}_{k-1}(a_1,\dots,a_{k-1})$, by the definition of this polynomial. We have then:

$$\frac{\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)}{\widetilde{\mathcal{L}}_{k-1}(a_1,\dots,a_{k-1})}=L_{E_k}(x).$$

We deduce:

[3] Note that this implies that $\widetilde{\mathcal{L}}_k(a_1,\dots,a_{k-1},x)$ is nonzero at any input x lying outside E_k.

Corollary 1 *For every positive integers $2 \leq k \leq n$ and every $\mathbb{F}_2$-linearly independent elements $a_1, \ldots, a_k$ of $\mathbb{F}_{2^n}$, the following statements are equivalent:*

1. $\sum_{u \in E_k, u \neq 0} \frac{1}{u} = 0$*, where E_k is the vector space spanned by $a_1, \ldots, a_k$,*
2. $\widetilde{\mathcal{L}}_k(a_1, \ldots, a_k) = 0$*,*
3. *The polynomials $\widetilde{\mathcal{L}}_k(a_1, \ldots, a_{k-1}, x)$ and $\left(\widetilde{\mathcal{L}}_{k-1}(a_1, \ldots, a_{k-1})\right) L_{E_k}(x)$ are equal,*

Corollary 1 provides the values of the coefficients $b_{k,i}$ of the linearized polynomial $L_{E_k}(x)$ in the case that $\sum_{u \in E_k, u \neq 0} \frac{1}{u} = 0$. Moreover, in this same case, the function $(a_1, \ldots, a_k, x) \mapsto b_{k,0}\, L_{E_k}(x) = \mathcal{L}_k(a_1, \ldots, a_k)\, L_{E_k}(x)$ equals as we saw already $\prod_{l \in \mathbb{F}_2^k} \left(x + \sum_{i=1}^k l_i a_i\right) \prod_{l \in \mathbb{F}_2^k} \left(\sum_{i=1}^k l_i a_i\right)$, that is, $\mathcal{L}_{k+1}(a_1, \ldots, a_k, x)$.

5.2.4 Some more observations

We now make a series of remarks, which are not essential to the rest of the paper, but which may help subsequent research addressing values of (k, n) not treated in the present work.

Remark. Another way of proving Relation (11) is as follows: $\sum_{\sigma \in G'_k} \prod_{i=1}^k a_i^{2^{\sigma(i)}}$ can be derived from $\mathcal{L}_k(a_1, \ldots, a_k) = \sum_{\sigma \in G_k} \prod_{i=1}^k a_i^{2^{\sigma(i)}} = \prod_{\epsilon \in \mathbb{F}_2^k, \epsilon \neq 0} (\sum_{i=1}^k \epsilon_i a_i)$ as $\sum_{i=1}^k a_i \left(\frac{\partial \mathcal{L}_k(a_1, \ldots, a_k)}{\partial a_i}\right)^2 = \sum_{i=1}^k a_i \sum_{\epsilon \in \mathbb{F}_2^k, \epsilon \neq 0} \epsilon_i \left(\prod_{\eta \in \mathbb{F}_2^k, \eta \neq 0, \epsilon} (\sum_{i=1}^k \epsilon_i a_i)\right)^2 =$ $\sum_{\epsilon \in \mathbb{F}_2^k, \epsilon \neq 0} (\sum_{i=1}^k a_i \epsilon_i) \left(\prod_{\eta \in \mathbb{F}_2^k, \eta \neq 0, \epsilon} (\sum_{i=1}^k \epsilon_i a_i)\right)^2 =$

$$(\mathcal{L}_k(a_1, \ldots, a_k))^2 \sum_{\epsilon \in \mathbb{F}_2^k, \epsilon \neq 0} \frac{1}{\sum_{i=1}^k \epsilon_i a_i} = (\mathcal{L}_k(a_1, \ldots, a_k))^2 \sum_{u \in E_k, u \neq 0} \frac{1}{u},$$

where in the two last expressions, we assume that $a_1, \ldots, a_k$ are linearly independent. ◇

Remark. Let $L_{E_k}(x) = x^{2^k} + \sum_{l=0}^{k-1} b_{k,l}\, x^{2^l}$, then each a_i, for $i = 1, \ldots, k$, satisfies $a_i^{2^k} = \sum_{l=0}^{k-1} b_{k,l}\, a_i^{2^l}$, and the expression $\sum_{\sigma \in G'_k} \prod_{i=1}^k a_i^{2^{\sigma(i)}}$ equals:

$$\sum_{i=1}^k \sum_{\sigma \in G'_k; \sigma(i) = k} \left(\prod_{j \in \{1, \ldots, k\} \setminus \{i\}} a_j^{2^{\sigma(j)}} \right) \left(\sum_{l=0}^{k-1} b_{k,l}\, a_i^{2^l} \right).$$

If $b_{k,1} = 0$, it vanishes since, after the expansion of this latter expression, each monomial in $a_1, \ldots, a_k$ appears twice with the same coefficient. This is coherent with (11).

Remark. We can divide $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)=\sum_{\sigma\in G'_k}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$ by $\mathcal{L}_k(a_1,\dots,a_k)=\sum_{\sigma\in G_k}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$. Indeed, the latter divides the former, since $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)$ is divisible by each a_i, it is multi-linear, and it equals 0 when two variables a_i and a_j are equal; it is then invariant under any transformation of the form $a_i\mapsto a_i+\sum_{j\neq i}\epsilon_j a_j,\ j\neq i,\epsilon_j\in\mathbb{F}_2$ and it is therefore divisible by any nonzero linear combination of the variables. But it seems difficult to determine $Q(a_1,\dots,a_k)=\frac{\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)}{\mathcal{L}_k(a_1,\dots,a_k)}$ for the generic value of k. Moreover, we calculated $Q(a_1,\dots,a_k)$ for $k=2,3,4$, and it has a more complex expression (although of lower degree) than $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)$:
For $k=2$, we have $\widetilde{\mathcal{L}}_2(a_1,a_2)=a_1^4a_2+a_1a_2^4$ and $Q(a_1,a_2)=a_1^2+a_1a_2+a_2^2=(a_1+wa_2)(a_1+w^2a_2)$, where w is a primitive element of $\mathbb{F}_4$ (if n is odd, then we consider this latter product as over $\mathbb{F}_{2^{2n}}$). We find again that it can vanish if and only if n is even.
For $k=3$, we have $\widetilde{\mathcal{L}}_3(a_1,a_2,a_3)=\sum_{s\in S_3}a_{s(1)}^8a_{s(2)}^4a_{s(3)}$ and $Q(a_1,a_2,a_3)=(\sum_{s\in S_3}a_{s(1)}^4a_{s(2)}^2)+a_1a_2a_3(\sum_{i=1}^3a_i^3)+(a_1^2a_2^2a_3^2)$ where S_3 is the symmetric group over $\{1,2,3\}$.
For $k=4$, we have $\widetilde{\mathcal{L}}_4(a_1,a_2,a_3,a_4)=\sum_{s\in S_4}a_{s(1)}^{16}a_{s(2)}^8a_{s(3)}^4a_{s(4)}$ and

$$Q(a_1,a_2,a_3,a_4)=$$

$$\Big(\sum_{s\in S_4}a_{s(1)}^8a_{s(2)}^4a_{s(3)}^2\Big)+\Big(a_1a_2a_3a_4\sum_{i\neq j=1}^4a_i^7a_j^3\Big)+$$

$$\Big(a_1^2a_2^2a_3^2a_4^2\sum_{i=1}^4a_i^6\Big)+\Big(a_1^2a_2^2a_3^2a_4^2\sum_{i=1}^4\prod_{j\neq i}a_j^2\Big),$$

where S_4 is the symmetric group over $\{1,2,3,4\}$.
For showing that the multiplicative inverse (n,n)-function is not kth-order sum-free for some value of k, we can either try to prove that $\widetilde{\mathcal{L}}_k(a_1,\dots,a_k)$ vanishes for at least one k-tuple $(a_1,\dots,a_k)$ of linearly independent elements of $\mathbb{F}_{2^n}$ or that $Q(a_1,\dots,a_k)$ vanishes for at least one k-tuple $(a_1,\dots,a_k)$ of linearly independent elements of $\mathbb{F}_{2^n}$. Even for $k=3$, it is rather complex to do so; actually we found a proof for $k=3$ but we do not give it because there is a simpler one that we shall see later. ◇

5.3 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 $f(x)=\sum_{i=0}^{2^n-1}\delta_ix^i\in\mathbb{F}_{2^n}[x]/(x^{2^n}+x)$; $\delta_i\in\mathbb{F}_{2^n}$ be the univariate representation[4] of f.

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

We have that $\sum_{u\in supp(f)\setminus\{0\}} \frac{1}{u} = \sum_{x\in\mathbb{F}_{2^n}} x^{2^n-2}f(x) = \delta_0 \sum_{x\in\mathbb{F}_{2^n}} x^{2^n-2} + \delta_1 \sum_{x\in\mathbb{F}_{2^n}} x^{2^n-1} + \sum_{i=2}^{2^n-1} \delta_i \sum_{x\in\mathbb{F}_{2^n}} x^{i-1}$. Among $x^{2^n-2}, x^{2^n-1}, x, x^2, \dots, x^{2^n-2}$ the only monomial of algebraic degree n is x^{2^n-1}. This implies:

$$\sum_{u\in E\setminus\{0\}} \frac{1}{u} = \delta_1 \sum_{x\in\mathbb{F}_{2^n}} x^{2^n-1} = \delta_1, \tag{12}$$

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 let us see, by several approaches, how the univariate representation of the indicator can be calculated.

5.3.1 A first way to obtain the univariate representation of the indicator of a vector space

Every k-dimensional $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^n}$ is the intersection of $(n-k)$ $\mathbb{F}_2$-linearly independent linear hyperplanes. This gives $f(x) = \prod_{j=1}^{n-k}(1 + tr_n(u_j x))$ (mod $x^{2^n} + x$), where the $u_j \in \mathbb{F}_{2^n}$ are $\mathbb{F}_2$-linearly independent (more precisely, where $(u_1, \dots, u_{n-k})$ is a basis of the orthogonal of E). The coefficient of x in this polynomial equals

$$\sum_{t\in T'; \sum_{j=1}^{n-k} 2^{t(j)}; \equiv 1 \pmod{2^n-1}} \prod_{j=1}^{n-k} u_j^{2^{t(j)}},$$

where $T' = \{-\infty, 0, \dots, n-1\}^{n-k}$ is the set of all functions from $\{1, \dots, n-k\}$ to $\{-\infty, 0, \dots, n-1\}$, with the convention $2^{-\infty} = 0$. This method is efficient only when k is close to n.

5.3.2 A second way

We start from the subspace polynomial $L_E(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$ (where, if E has dimension k, then $b_{k+1} = \cdots = b_{n-1} = 0$). We have:

$$\begin{aligned}
f(x) &= 1 + \Big(L_E(x)\Big)^{2^n-1} \pmod{x^{2^n}+x} \\
&= 1 + \Big(\sum_{i=0}^{n-1} b_i x^{2^i}\Big)^{\sum_{j=0}^{n-1} 2^j} \pmod{x^{2^n}+x} \\
&= 1 + \prod_{j=0}^{n-1}\Big(\sum_{i=0}^{n-1} b_i^{2^j} x^{2^{i+j \pmod n}}\Big) \pmod{x^{2^n}+x} \\
&= 1 + \sum_{t\in T}\Big(\prod_{j=0}^{n-1} b_{t(j)}^{2^j}\Big) x^{\sum_{j=0}^{n-1} 2^{t(j)+j \pmod n}} \pmod{x^{2^n}+x},
\end{aligned}$$

where $T = \{0,\dots,n-1\}^{\{0,\dots,n-1\}}$ is the set of all functions from $\{0,\dots,n-1\}$ (more precisely, $\mathbb{Z}/n\mathbb{Z}$) to itself (if we know k, we can take $T = \{0,\dots,k\}^{\{0,\dots,k\}}$). The coefficient of x in this expression equals:

$$\sum_{t\in T;\sum_{j=0}^{n-1} 2^{t(j)+j} \equiv 1 \pmod{2^n-1}} \Big(\prod_{j=0}^{n-1} b_{t(j)}^{2^j}\Big),$$

and we know from Relation (6) and Proposition 4 that this expression equals in fact $b_1 b_0^{2^n-2}$ (which may be difficult to prove directly). This method is efficient only when k is small.

Remark. It seems difficult to conversely derive the polynomial $L_E(x)$ from the indicator of E. ◇

5.3.3 A third way

We express by means of the univariate form of the indicator the fact that a non-empty subset of $\mathbb{F}_{2^n}$ is a $\mathbb{F}_2$-vector space if and only if it is preserved by addition. This writes "$f(x) = 1$ and $f(y) = 1$ imply $f(x+y) = 1$", and we have then:

Proposition 5 *Let f be any Boolean function over $\mathbb{F}_{2^n}$, then f is the indicator of an $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^n}$ if and only if the bivariate Boolean function $(x,y) \in \mathbb{F}_{2^n}^2 \mapsto f(x)f(y)(1+f(x+y))$ is identically zero, that is, the two Boolean functions $f(x)f(y)$ and $f(x)f(y)f(x+y)$ coincide.*

Let then $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ be the univariate representation of $f(x)$. We assume that $a_0 = 1$ (since if f is the indicator of a vector space, then $f(0) = 1$). We also assume that $a_{2^n-1} = 0$, since we know that the only vector space whose indicator has algebraic degree n is $\{0\}$ (we know then that $f(x) = x^{2^n-1} + 1$; this case which corresponds to $k = 0$ is not interesting for our purpose). The necessary and sufficient condition in Proposition 5 writes then:

$$\left(\sum_{i=0}^{2^n-2} a_i x^i\right)\left(\sum_{j=0}^{2^n-2} a_j y^j\right) \equiv$$

$$\left(\sum_{u=0}^{2^n-2} a_u x^u\right)\left(\sum_{v=0}^{2^n-2} a_v y^v\right)\left(\sum_{w=0}^{2^n-2} a_w (x+y)^w\right) \pmod{x^{2^n}+x, y^{2^n}+y}.$$

For every $i, j \in \{0, \dots, 2^n - 2\}$, the coefficient of $x^i y^j$ in $f(x)f(y)$ equals $a_i\, a_j$, and in $f(x)f(y)f(x+y) \pmod{x^{2^n}+x, y^{2^n}+y}$, it equals the sum of the coefficients of $x^i y^j$, $x^{i+2^n-1} y^j$, $x^i y^{j+2^n-1}$ and $x^{i+2^n-1} y^{j+2^n-1}$ in $f(x)f(y)f(x+y)$. The coefficient of $x^i y^j$ in $f(x)f(y)f(x+y)$ equals the sum of the products $a_u a_v a_w \binom{w}{k}$ where $u + k = i$ and $v + w - k = j$, that is, the sum of the products $a_u a_v a_w \binom{w}{i-u}$ where $u + v + w = i + j$ that is, the sum of the products $a_u a_v a_w \binom{w}{j-v}$ where $u + v + w = i + j$. We have then (still assuming $a_0 = 1$ and $a_{2^n-1} = 0$) that f is the indicator of a vector space if and only if:

$$\forall i, j \in \{1, \dots 2^n - 2\}, a_i\, a_j =$$

$$\sum_{u,v,w \in \{1,\dots,2^n-2\}; u+v+w=i+j; 0\le u\le i, 0\le v\le j} a_u\, a_v\, a_w \binom{w}{i-u} +$$

$$\sum_{u,v,w \in \{1,\dots,2^n-2\}; u+v+w=i+2^n-1+j; 0\le u\le i} a_u\, a_v\, a_w \binom{w}{i+2^n-1-u} +$$

$$\sum_{u,v,w \in \{1,\dots,2^n-2\}; u+v+w=i+j+2^n-1; 0\le v\le j} a_u\, a_v\, a_w \binom{w}{i-u} +$$

$$\sum_{u,v,w \in \{1,\dots,2^n-2\}; u+v+w=i+j+2^{n+1}-2} a_u\, a_v\, a_w \binom{w}{i+2^n-1-u}. \tag{13}$$

Note indeed that, since $a_0 = 1$, the cases "$i = j = 0$", "$i = 0$ and $j > 0$" and "$i > 0$ and $j = 0$" write respectively $1 = 1$, $a_j = a_j$ and $a_i = a_i$.
This approach may be adapted for trying to build vector spaces over which the inverse function sums to 0, since we can add then the condition $a_1 = 0$ and try to build f satisfying Condition (13).

6 The kth-order-sum-freedom of multiplicative inverse function

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.

Trying to address general values of k, let $a_1, \ldots, a_k$ be $\mathbb{F}_2$-linearly independent elements of $\mathbb{F}_2^n$. Denoting again by E_k the k-dimensional vector space they span; given x, let us see whether $\sum_{u \in E}(x+u)^{-1}$ equals 0 or not.

6.1 Case of an affine space $x+E$, where E is a linear space and $x \notin E$

Theorem 1 shows that the sum $\sum_{u\in E} \frac{1}{x+u}$ is nonzero. Hence, determining whether the multiplicative inverse function is kth-order-sum-free reduces to addressing the case $x \in E$, that is, to determining whether the inverse function sums to nonzero values over all k-dimensional vector subspaces of $\mathbb{F}_{2^n}$.

6.2 Case of a linear space ($x \in E$), first observations and first results

We begin with an observation in the next lemma, which potentially gives a tool for studying the kth-order-sum-freedom of the multiplicative inverse function, but for which it seems to us difficult to deduce concrete consequences. We give it for the case some further work could provide interesting corollaries. Recall that the notation $w_2(\cdot)$ has been introduced in Section 2.

Lemma 1 *Given $2 \le k \le n$, if there exists $d \in \{2, \ldots, 2^n-2\}$ such that $w_2(d) > n-k$, and there exists a k-dimensional $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^n}$ such that the set $E' = \{u^d, u \in E\}$ is also a k-dimensional $\mathbb{F}_2$-subspace, then the multiplicative inverse function is not kth-order-sum-free.*

Proof. We have $\sum_{x\in E'} x^{2^n-2} = \sum_{x\in E} x^{(2^n-2)\,d} = \sum_{x\in E} x^{2^n-1-d}$. Since $w_2(2^n-1-d) = n - w_2(d) < k$, the algebraic degree of the power function x^{2^n-1-d} is strictly less than k, and it sums then to 0 over E. □

Lemma 1 applies for $d = 2^n-2$ and k a divisor of n (we take then $E = E' = \mathbb{F}_{2^k}$), and this does not tell us anything new. It is the only values of k which can work with $d = 2^n-2$ since we know from [18] that (as we already recalled) the multiplicative inverse function maps no affine space A to an affine space except when A is the multiplicative coset of a subfield of $\mathbb{F}_{2^n}$.
Another example of application, also for a divisor k of n, is when $k \ge 2$ and $d = 2^n - 2^k + 1$ (which has 2-weight $n-k+1$). We can then take $E = E' = \mathbb{F}_{2^k}$

(equality coming from the fact that $\gcd(d, 2^k - 1) = \gcd(\gcd(d, 2^n - 1), 2^k - 1) = \gcd(2^k - 2, 2^k - 1) = 1$, and here is where $k \geq 2$ is necessary). But here again this application of the lemma does not tell us anything new in terms of the kth-order-sum-freedom of the multiplicative inverse function.
It seems difficult to find power functions and vector spaces mapped by them onto vector spaces of the same dimension.

Remark. There is an obvious case where the inverse function sums to zero over a vector subspace E: when E is stable under the inversion of its nonzero elements. This corresponds to $d = 2^n - 2$ and $E' = E$ in Lemma 1. But this case does not bring anything new, since the corresponding ϕ_E function (see Subsection 5.1.1) satisfies then $\phi_E(x) = \prod_{u \in E, u \neq 0}(x + u) = \prod_{u \in E, u \neq 0}(x + \frac{1}{u}) = \frac{x^{2^k - 1}}{\prod_{u \in E, u \neq 0} u} \prod_{u \in E, u \neq 0}(\frac{1}{x} + u) = \frac{1}{\prod_{u \in E, u \neq 0} u} \widetilde{\phi_E}(x)$, where $\widetilde{\phi_E}(x)$ is the reciprocal polynomial of $\phi_E(x)$. Then writing $\phi_E(x) = \sum_{i=0}^{k} b_{k,i} x^{2^i - 1}$, we have $\phi_E(x) = \frac{1}{\prod_{u \in E, u \neq 0} u} \sum_{i=0}^{k} b_{k,i} x^{2^k - 2^i}$ and then, if $b_{k,i} \neq 0$ then $2^k - 2^i$ must equal $2^j - 1 \pmod{2^n - 1}$ for some j and then it is easily seen that E must be a subfield of $\mathbb{F}_{2^n}$. ◇

Remark. We can also consider the case of subspaces E stable under squaring (that is, equal to a union of cyclotomic classes in $\mathbb{F}_{2^n}$). Inversion and squaring commuting, we have that $\sum_{u \in E; u \neq 0} \frac{1}{u} = \left(\sum_{u \in E; u \neq 0} \frac{1}{u}\right)^2 \in \mathbb{F}_2$. We do not see what other condition on E could imply that the value 1 is impossible for $\sum_{u \in E; u \neq 0} \frac{1}{u}$, but since $\sum_{u \in E; u \neq 0} \frac{1}{u}$ lives then in $\mathbb{F}_2$ instead of in $\mathbb{F}_{2^n}$, this increases the probability of finding such E satisfying $\sum_{u \in E; u \neq 0} \frac{1}{u} = 0$ (for instance in future computer investigations). Note that E is stable under squaring if and only if $L_E(x^2) = (L_E(x))^2$, that is, the polynomial $L_E(x)$ belongs to $\mathbb{F}_2[x]$. We shall see in the remark after Proposition 8 that, unfortunately, this restriction does not allow to address all situations. ◇

Let us make a second observation for which it seems also difficult to deduce concrete consequences and that we propose for future attempts. Recall from [21] that, for every power q of a prime and every m, the polynomial $x^{q^m} - x$ equals the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide m. Then (as already observed in [1]) if $q^r - 1$ divides m and $x^{q^r - 1} + x^{q-1} + 1$ is irreducible, then $x^{q^r} + x^q + x$ is a subspace polynomial over $\mathbb{F}_{q^m}$ (of course, this can be extended to any irreducible polynomial of the form $x^{q^r - 1} + \sum_{i=1}^{r-1} a_i x^{q^i - 1} + a_0$). Note that, if $q \geq 3$, then $x^{q^r} + x^q + x$ has zero coefficient of x^2. This can then be applied with $q = 2^l$ where $l \geq 2$, taking $n = ml$ and $k = rl$:

Lemma 2 *Let $n = ml$ and $k = rl$ for some positive integers m, k, l, where $l \geq 2$. If $2^k - 1$ divides m and and $x^{q^r - 1} + x^{q-1} + 1$ is irreducible over $\mathbb{F}_{2^l}$, then $x^{2^k} + x^{2^l} + x$ is a subspace polynomial with no term in x^2 and the multiplicative inverse function is then not kth-order-sum-free.*

Note that we have $\gcd(k,n) \geq l \geq 2$ in Lemma 2.

6.2.1 When k is not co-prime with n

We move now to a general result showing that if k is not-coprime with n, then the multiplicative inverse function cannot be kth-order-sum-free. We can indeed generalize the observation that the inverse function sums to zero over $\mathbb{F}_2$-subspaces being subfields of $\mathbb{F}_{2^n}$:

Proposition 6 *If* $\gcd(k,n) = l \neq 1$ *and* $\mathcal{E}$ *is 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* k*th-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 $\sum_{u\in\mathcal{E}\setminus\{0\}}\frac{1}{u} = \sum_{a\in P}\frac{1}{a}\left(\sum_{u\in\mathbb{F}^*_{2^l}}\frac{1}{u}\right) = 0$. □

Proposition 6 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.

6.2.2 Generalization of Proposition 6

Proposition 7 *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* k*th-order-sum-free. This happens for instance 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* $\mathbb{F}_2$ *of the form* $\left\{\sum_{i\in I}\lambda^i; I\subseteq\{0,\ldots,2^n-2\}\right\}$ *where* $\lambda\neq 0,1$.

Proof. If E_k is stable under multiplication by $\lambda\neq 0,1$, 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 $E_k =< G >$ be the k-dimensional $\mathbb{F}_2$-vector subspace generated by G, we have that E_k is invariant under multiplication by λ and $\langle G\rangle = \left\{\sum_{i\in I}\lambda^i; I\subseteq\{0,\ldots,2^n-2\}\right\}$. □

Remark. Proposition 7, even if it covers Proposition 6 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 $\gcd(2^k-1,2^n-1)\neq 1$, that is, $\gcd(k,n)\neq 1$. ⋄

6.3 Case of a linear space ($x \in E$), general observations

6.3.1 A first characterization

According to Theorem 2, we have:

Corollary 2 *Let $2 \leq k \leq n$. The multiplicative inverse function over $\mathbb{F}_{2^n}$ is kth-order-sum-free if and only if the function:*

$$\widetilde{\mathcal{L}}_k(a_1, \ldots, a_k) = \sum_{\sigma \in G'_k} \prod_{i=1}^{k} a_i^{2^{\sigma(i)}}, \tag{14}$$

where G'_k is the set of bijective functions from $\{1, \ldots, k\}$ to $\{0, 2, \ldots, k\}$, vanishes only at the $2^{kn} - (2^n - 1)(2^n - 2) \ldots (2^n - 2^{k-1})$ k-tuples $(a_1, \ldots, a_k) \in (\mathbb{F}_{2^n})^k$ whose terms are $\mathbb{F}_2$-linearly dependent elements of $\mathbb{F}_{2^n}$.

Indeed, if $a_1, \ldots, a_k$ are $\mathbb{F}_2$-linearly dependent, we can express one of them as a linear combination over $\mathbb{F}_2$ of the others, and after expanding the resulting expression, all terms cancel each others; and if they are independent, then Theorem 2 completes the proof.

6.3.2 Sum freedom overs 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 8 *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 Proposition 6, 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?

6.4 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 3 *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*

$$\sum_{u\in E\oplus F;u\neq 0}\frac{1}{u}=\sum_{u\in E;u\neq 0}\frac{1}{u}+\left(\prod_{u\in E,u\neq 0}u\right)\sum_{v\in L_E(F);v\neq 0}\frac{1}{v}, \tag{15}$$

where $L_E(x)=\prod_{u\in E}(x+u)$ 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:

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

And 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 linear bijective from F to $L_E(F)$. □

A first consequence dealing with complementary dimensions Corollary 3 implies that the property for the inverse function of being kth-order-sum-free is invariant under the transformation $k \mapsto n-k$:

Corollary 4 *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.

Indeed, 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}). According to Corollary 3, we have:

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

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. We have also that if E_k is such that $\sum_{u\in E_k,u\neq 0}\frac{1}{u}=0$ and if E_l is 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. Corollary 4 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 $\mathbb{F}_{2^m}$. ◇

A second consequence on the sums of divisors of n Corollary 3 implies that if k is the sum of two divisors of n (and is then possibly co-prime with n), then the inverse function is not kth-order sum-free:

Corollary 5 *Let $n\geq 6$ be divisible by two integers $l\geq 2$ and $r\geq 2$ such that $lr<n$. The inverse function is not $(l+r)$th-order-sum-free.*

Proof. Corollary 3 with $E=\mathbb{F}_{2^l}$ writes: for $\mathbb{F}_{2^l}\cap F=\{0\}$, we have

$$\sum_{u\in\mathbb{F}_{2^l}\oplus F;u\neq 0}\frac{1}{u}=\sum_{w\in F;w\neq 0}\frac{1}{w^{2^l}+w}=\sum_{v\in L_E(F);v\neq 0}\frac{1}{v},\tag{16}$$

where $L_E(x)=x^{2^l}+x$. The vector space $E'=L_E(F)$ can be any $\mathbb{F}_2$-subspace of $L_E(\mathbb{F}_{2^n})=\{w^{2^l}+w;\ w\in\mathbb{F}_{2^n}\}$, that is, of 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 $\mathbb{F}_{2^l}$. Let $(e_1,\dots,e_r)$ be a basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$. The vector space $\{a\in\mathbb{F}_{2^n};tr_l^n(e_1a)=\cdots=tr_l^n(e_ra)=0\}$ is the intersection of r vector subspaces of dimension $n-l$ over $\mathbb{F}_2$, and since $n>lr$, it has then dimension at least 1, i.e. contains at least one nonzero element a. The r elements $e_1a,\dots,e_ra$ of $\ker(tr_l^n)$ are $\mathbb{F}_2$-linearly independent and generate the $\mathbb{F}_2$-vector subspace $E'=a\mathbb{F}_{2^r}$ satisfying $\sum_{v\in E',v\neq 0}\frac{1}{v}=0$. This completes the proof. □

Let us now provide a new result which is the most effective one in this paper on the sum-freedom of the inverse function.

Corollary 6 *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 $j\in\{1,\dots,\frac{n}{r}-l\}$ or of the form $r+jl$ where $j\in\{1,\dots,\frac{n}{l}-r\}$, 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 $k\in\{2,4,\dots,l-1\}\cup\llbracket l,n-l\rrbracket\cup\{n-l+1,n-l+3,\dots,n-2\}$, 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 $k\in\llbracket 2,n-2\rrbracket$.

Proof. We have seen that $L_{\mathbb{F}_{2^l}}(\mathbb{F}_{2^n})$ 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 3 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 Proposition 6 and Corollary 3, 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 $j=1,\dots,\frac{n}{r}-l$. This completes the first part (the case " k divisible by l or by r" being covered by Proposition 6). The second part is a direct consequence by taking $r=2$ (since all the odd numbers between l and $n-l$ write $l+jr=l+2j$ where $j=1,\dots,\frac{n}{r}-l=\frac{n}{2}-l$). The last sentence is by taking $l=3$. □

6.5 Case of a linear space ($x\in E$), characterizations

Recall that, thanks to Proposition 6, we need "only" to address the case where k and n are co-prime (and the case where n is a prime number seems more difficult, since when n is composite, Corollaries 4-6 give also information). We shall not be able to address all cases of (k,n). We know that for $k=n-1$, the inverse function is kth-order-sum-free. Theorem 2 gives a rather well structured expression of $\sum_{u\in E\setminus\{0\}}\frac{1}{u}$ but it seems difficult to exploit it for completely clarifying the situation. Note that we have $\sum_{u\in E\setminus\{0\}}\frac{1}{u}=(D_{a_1}\cdots D_{a_k}H_k)(0)$, where $H_k(x)=x^{1+4+8+\cdots+2^k}=x^{2^{k+1}-3}$. Summarizing what we have and observing that $x^{2^{k+1}-3}$ has algebraic degree k, as an (n,n)-function, we have:

Proposition 9 *For every $2\leq k\leq n$, the following statements are equivalent:*

1. *The multiplicative inverse function over $\mathbb{F}_{2^n}$ is kth-order-sum-free.*

2. *$\sum_{u\in E,u\neq 0}\frac{1}{u}$ is nonzero for every k-dimensional $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^n}$.*

3. *The restriction of function x^{2^n-2} to every k-dimensional subspace of $\mathbb{F}_{2^n}$, viewed as a (k,n)-function, has algebraic degree k.*

4. *No* k*th-order derivative* $D_{a_1}\dots D_{a_k}F$ *of the multiplicative inverse function* F *with* $a_1,\dots,a_k$ $\mathbb{F}_2$*-linearly independent vanishes.*

5. *No* k*th-order derivative* $D_{a_1}\dots D_{a_k}F$ *of the multiplicative inverse function* F *with* $a_1,\dots,a_k$ $\mathbb{F}_2$*-linearly independent vanishes at 0.*

6. $\sum_{u\in E} u^{2^{k+1}-3}$ *is nonzero for every* k*-dimensional* $\mathbb{F}_2$*-subspace* E *of* $\mathbb{F}_{2^n}$*.*

7. *The restriction of function* $H_k(x) = x^{2^{k+1}-3}$ *to every* k*-dimensional* $\mathbb{F}_2$*-subspace of* $\mathbb{F}_{2^n}$*, viewed as a* (k,n)*-function, has algebraic degree* k*.*

8. *No* k*th-order derivative* $D_{a_1}\dots D_{a_k}H_k$ *of the function* $H_k(x) = x^{2^{k+1}-3}$ *with* $a_1,\dots,a_k$ $\mathbb{F}_2$*-linearly independent vanishes (such derivative is constant).*

9. *The function* $H_k(x) = x^{2^{k+1}-3}$ *is* k*th-order-sum-free.*

10. *The symmetric multi-linear function*

$$\widetilde{\mathcal{L}}_k : (a_1,\dots,a_k) \in \mathbb{F}_{2^n}^k \mapsto \sum_{\sigma\in G'_k} \prod_{i=1}^{k} a_i^{2^{\sigma(i)}},$$

where G'_k *is the set of bijective functions from* $\{1,\dots,k\}$ *to* $\{0,2,\dots,k\}$*, vanishes if and only if* $a_1,\dots,a_k$ *are* $\mathbb{F}_2$*-linearly dependent.*

Remark.
Proposition 9 (item 10) shows again that the multiplicative inverse function over $\mathbb{F}_{2^n}$ is second-order-sum-free if and only if n is odd, since we have $a_1^4a_2 + a_1a_2^4 = a_2^5(b^4+b)$, where $b = \frac{a_1}{a_2} \in \mathbb{F}_{2^n}\setminus\mathbb{F}_2$; the equation $b^4+b=0$ is the characteristic equation of $\mathbb{F}_4$, and $\mathbb{F}_4\setminus\mathbb{F}_2$ is empty if and only if n is odd.
For $k=3$, the symmetric multi-linear function $\widetilde{\mathcal{L}}_k$ becomes $(a_1,a_2,a_3)\in\mathbb{F}_{2^n}^k \mapsto a_1^8a_2^4a_3 + a_1^8a_2a_3^4 + a_1^4a_2^8a_3 + a_1^4a_2a_3^8 + a_1a_2^4a_3^8 + a_1a_2^8a_3^4$, and we deduce again that if n is divisible by 3, then the multiplicative inverse function is not third-order-sum-free (take a_1,a_2,a_3 in $\mathbb{F}_{2^3}$ and use that $a_i^8 = a_i$). We can then restrict ourselves to $\gcd(3,n)=1$, and then, after dividing by $a_1a_2a_3$ and observing that the function x^7 is a permutation of $\mathbb{F}_{2^n}$, we have that the multiplicative inverse function is third-order-sum-free if and only if, for every $\mathbb{F}_2$-linearly independent a_1,a_2,a_3 in $\mathbb{F}_{2^n}$, we have $\frac{a_1^3+a_3^3}{a_1^7+a_3^7} \neq \frac{a_2^3+a_3^3}{a_2^7+a_3^7}$. Note that, replacing a_1 and a_2 by a_1a_3 and a_2a_3, respectively, this is equivalent to: for every a_1,a_2 such that a_1,a_2 and 1 are $\mathbb{F}_2$-linearly independent in $\mathbb{F}_{2^n}$, we have $\frac{a_1^3+1}{a_1^7+1} \neq \frac{a_2^3+1}{a_2^7+1}$. In other words, we can have $\frac{x^3+1}{x^7+1} = \frac{y^3+1}{y^7+1}$ (with $x,y\neq 1$) only if $y=x$ or $y=x+1$. In both these latter cases, we do have $\frac{x^3+1}{x^7+1} = \frac{y^3+1}{y^7+1}$, since for $y=x+1$, it writes $\frac{x^3+1}{x^7+1} = \frac{x^3+x^2+x}{x^7+x^6+x^5+x^4+x^3+x^2+x}$ (with $x\neq 0,1$) which is always satisfied. Hence, the condition is equivalent to saying that the function $\frac{x^3+1}{x^7+1}$ is injective over some (any) linear hyperplane H not containing 1. It would be possible to

address this condition but this would lead to technical calculations, while we shall see in Subsection 6.7 another approach which is simpler and will solve the case $k=3$ (see Corollary 8) and will then clarify whether $\frac{x^3+1}{x^7+1}$ is injective over H without having to make these claculations. $\diamond$

6.6 Case of a linear space ($x \in E$), a special class of vector spaces

Let E be a k-dimensional $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^n}$ included in (and possibly equal to) a vector subspace of equation:

$$x^{2^{k+1}} = \alpha x + \beta x^2 + \sum_{j\in J} x^{2^j},$$

where J is some fixed subset of $\{2,\ldots,k\}$ and $\alpha, \beta \in \mathbb{F}_{2^n}$. Then raising to the fourth power the relation $\mathcal{L}_k(a_1,\ldots,a_k) = \sum_{\sigma\in G_k}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$ (where G_k is the set of bijective functions from $\{1,\ldots,k\}$ to $\{0,\ldots,k-1\}$), replacing in the resulting expression $a_i^{2^{k+1}}$ by $\alpha a_i + \beta a_i^2 + \sum_{j\in J} a_i^{2^j}$ for each i, and using that $\widetilde{\mathcal{L}}_k(a_1,\ldots,a_k) = \sum_{\sigma\in G'_k}\prod_{i=1}^k a_i^{2^{\sigma(i)}}$ (where G'_k is the set of bijective functions from $\{1,\ldots,k\}$ to $\{0,2,\ldots,k\}$), we obtain the relation

$$(\mathcal{L}_k(a_1,\ldots,a_k))^4 = \alpha\widetilde{\mathcal{L}}_k(a_1,\ldots,a_k) + \beta(\mathcal{L}_k(a_1,\ldots,a_k))^2,$$

plus an expression which vanishes since, after its expansion, each monomial in $a_1,\ldots,a_k$ appears twice in it with the same coefficient. Assuming $a_1,\ldots,a_k$ linearly independent (that is, $\mathcal{L}_k(a_1,\ldots,a_k)\neq 0$) and $\alpha\neq 0$, we have then $\widetilde{\mathcal{L}}_k(a_1,\ldots,a_k)=0$ if and only if $\mathcal{L}_k(a_1,\ldots,a_k)=\beta^{2^{n-1}}$, with $\beta\neq 0$. This may allow to address some cases that are difficult to handle in another way.

6.7 Case of a linear space ($x \in E$), large values of k

We shall now see 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 $\sum_{u\in E\setminus\{0\}}\frac{1}{u}$ equals the coefficient of x in the univariate representation of the indicator function $1_E(x)$. Let $(u_1,\ldots,u_{n-k})$ be a basis of $E^\perp = \{y\in\mathbb{F}_{2^n}; tr_n(x\,y)=0, \forall x\in E\}$. We have seen in Subsection 5.3 that $1_E(x)=\prod_{i=1}^{n-k}(1+tr_n(u_i\,x)) = \sum_{b\in\{-\infty,0,\ldots,n-1\}^{n-k}}\left(\prod_{i=1}^{n-k}u_i^{2^{b_i}}\right)x^{\sum_{i=1}^{n-k}2^{b_i}}$, where by convention $2^{-\infty}=0$, and that the coefficient of x equals then:

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

We find again that for $k = n-1$, this coefficient, equal to: $\sum_{b\in\{-\infty,0,\dots,n-1\};2^b\equiv 1 \pmod{2^n-1}} u_1^{2^b} = u_1$, is nonzero and the inverse function is $(n-1)$th-order-sum-free.

For $k = n-2$, the coefficient of x is $\sum_{b\in\{-\infty,0,\dots,n-1\}^2;2^{b_1}+2^{b_2}\equiv 1 \pmod{2^n-1}} u_1^{2^{b_1}}u_2^{2^{b_2}} = u_1^{2^0}u_2^{2^{-\infty}} + u_1^{2^{-\infty}}u_2^{2^0} + u_1^{2^{n-1}}u_2^{2^{n-1}} = u_1 + u_2 + \left(u_1u_2\right)^{\frac{1}{2}} = u_2\left(1 + \left(\frac{u_1}{u_2}\right)^{\frac{1}{2}} + \frac{u_1}{u_2}\right)$. 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 deduce (but we knew it already thanks to Corollary 4):

Proposition 10 *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.*

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

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

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

Denoting $x = u_1, y = u_2, z = u_3$, we are led to:

Proposition 11 *Let $n \geq 5$, then the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not $(n-3)$th-order-sum-free if and only if the equation:*

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

admits solutions (x,y,z) such that x, y, z are $\mathbb{F}_2$-linearly independent.

We can assume without loss of generality that $z = 1$ (and then $x, y, x+y \notin \mathbb{F}_2$), since the equation is invariant when we multiply each variable by the same nonzero factor, and denoting $t = y^2+y+1$, we have $t \neq 1$ and the equation becomes:

$$x^4 + tx^2 + (t+1)x + t^2 = 0. \tag{17}$$

Note that the fact that $x \notin \mathbb{F}_2 \cup (y+\mathbb{F}_2)$, does not eliminate any solution x when n is odd, since then $t \notin \mathbb{F}_2$ and none of the elements $0, 1, y, y+1$ can be a solution of the equation. When n is even, we can have $t = 0$ (when y equals a primitive element of $\mathbb{F}_4$), but it is clear that, for every $n \geq 6$, there exist values of $t \notin \mathbb{F}_2$ such that $tr_n(t+1) = 0$ (so that there exists $y \notin \mathbb{F}_2$ such that $y^2+y+1 = t$) and such that Equation (17) has solutions.

Corollary 7 *For every $n \geq 6$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not $(n-3)$th-order-sum-free.*

Corollaries 4 and 7 allow to state:

Corollary 8 *For every $n \geq 6$, the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not third-order-sum-free.*

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

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

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

Denoting $x = u_1, y = u_2, z = u_3$ and taking $u_4 = 1$, we are led to:

Proposition 12 *Let $n \geq 6$, then the multiplicative inverse function over $\mathbb{F}_{2^n}$ is not $(n-4)$th-order-sum-free if and only if the equation:*

$$x^4+y^4+z^4+1+x^2y^2+x^2z^2+x^2+y^2z^2+y^2+z^2+xyz^2+xy^2z+x^2yz+xy+xy^2+$$

$$x^2y+xz+xz^2+x^2z+yz+yz^2+y^2z+xyz=0$$

admits solutions (x,y,z) such that x,y,z and 1 are $\mathbb{F}_2$-linearly independent.

Probably the condition of Proposition 12 can be satisfied for every $n \geq 8$ (for $n \leq 7$ we have $n-4 \leq 3$ and the situation is clear) since we have only one equation and three variables, on which the condition of being linearly independent together with 1 is not very restrictive. According to Corollary 4, the inverse function would then be neither $(n-4)$th-order-sum-free nor 4th-order-sum-free, but we did not find a general proof of this.

We were able to address the case of n even. In that case, we have seen that a plane $E = \{0, a_1, a_2, a_1+a_2\}$ is such that $\sum_{u\in E, u\neq 0} u^{-1} = 0$ if and only if $a_1^2 + a_1a_2 + a_2^2 = 0$, that is, $\frac{a_2}{a_1} \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Moreover, we have $L_E(x) = x(x+a_1)(x+a_2)(x+a_1+a_2) = x^4 + (a_1^2+a_1a_2+a_2^2)\,x^2 + (a_1^2a_2+a_1a_2^2)\,x$. Assuming that $\frac{a_2}{a_1} \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have then $a_2 = a_1w$ where $w^2 = w+1$, and then $L_E(x) = x^4 + a_1^3x$. Let $F = \{0, a_3, a_4, a_3+a_4\}$ be a second plane with a trivial intersection with E. Then, if $(L_E(a_3))^2 + L_E(a_3)L_E(a_4)) + (L_E(a_4))^2 = 0$, that is, if $L_E(a_3) = wL_E(a_4)$ or $L_E(a_3) = w^2L_E(a_4)$, Corollary 3 provides a 4-dimensional vector space $E \oplus F$ such that $\sum_{u\in E\oplus F, u\neq 0} u^{-1} = 0$. Denoting $u = \frac{a_3}{a_1}$ and $v = \frac{a_4}{a_1}$, the relations $L_E(a_3) = wL_E(a_4)$ and $L_E(a_3) = w^2L_E(a_4)$ write $u^4+u = w(v^4+v)$ and $u^4+u = w^2(v^4+v)$, and we deduce that if for instance the former equation, which writes $(u+wv)^4+u+wv = 0$, that is, $u+wv \in \mathbb{F}_4$, has solutions $u, v \in \mathbb{F}_{2^n} \setminus \mathbb{F}_4$ such that $u+v \notin \mathbb{F}_4$, then the multiplicative inverse function is not 4th-order sum-free. Seeing now u and v in $\mathbb{F}_{2^n}/\mathbb{F}_4$, the condition becomes $u+wv = 0, u \neq 0, v \neq 0, u+v \neq 0$ and it is satisfiable as soon as $n \geq 6$, since the two lines of equations $u+wv = 0$ and $u+v = 0$ intersect only in $(0,0)$ and none is reduced to $\{(0,0)\}$. Hence:

Table 1: Values of k for which we known that x^{-1} is not kth-order-sum-free

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

Proposition 13 *Let $n \geq 6$ be even. Then the multiplicative inverse function is neither 4th-order sum-free nor $(n-4)$th-order sum-free.*

The cases $k = 5, \ldots, n-5$ could be studied similarly as in Proposition 12, but we miss a proof of the fact that the inverse function is not kth-order sum-free for any such value.

We display in Table 1 with "✓" each value of k for which we can prove that the multiplicative inverse function is kth-order-sum-free and with "¬" when we can prove with the results in this paper that it is not kth-order-sum-free. We write "-" when k is larger than n.

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 are missing mathematical results explaining these investigation results for $n = 11$ and $k = 4, \ldots, 7$.

6.8 Case of a linear space ($x \in E$), a last observation

There is another possible approach: given an $\mathbb{F}_2$-subspace E of $\mathbb{F}_{2^n}$ admitting a basis $(a_1, \ldots, a_k)$, all four (n, n)-functions

$$S_E(x) = \sum_{u \in E} (x+u)^{-1} = D_{a_1} \cdots D_{a_k} F(x),$$

$$T_E(x) = \left(\prod_{u \in E \setminus \{0\}} u \right) \left(\prod_{u \in E} (x+u)^{-1} \right) = \left(\prod_{u \in E \setminus \{0\}} u \right) \left(F \left(\prod_{u \in E} (x+u) \right) \right),$$

$$\Sigma_E(x) = \sum_{u \in E} (x+u)^{2^k - 1} = D_{a_1} \cdots D_{a_k} P_k(x), \text{ where } P_k(x) = x^{2^k - 1},$$

and

$$\Gamma_E(x) = \sum_{u \in E} (x+u)^{2^{k+1} - 3} = D_{a_1} \cdots D_{a_k} Q_k(x), \text{ where } Q_k(x) = x^{2^{k+1} - 3},$$

are constant on each coset of E.
According to Theorem 1, S_E, T_E and Σ_E coincide on $\mathbb{F}_{2^n} \setminus E$ and according to Proposition 9 (item 10), S_E and Γ_E coincide on E. The constant value taken by function T_E on E is zero. We wish to determine for which k the value of S_E is nonzero on E for every E of dimension k. Let E' be any $(n-k)$-dimensional vector space whose sum with E is direct (and equals then $\mathbb{F}_{2^n}$). Then since S_E has algebraic degree at most $n-k-1$ (being the k-th order derivative of a function of degree $n-1$), its restriction to E' sums to zero. We have then that $S_E(0) = \sum_{u \in E \setminus \{0\}} \frac{1}{u}$ is nonzero if and only if the two functions S_E and T_E do not coincide at 0, or equivalently, the restriction of T_E to E' does not sum to zero, that is, has algebraic degree $n-k$. Since T_E is constant on every coset of E, it is equivalent to say that T_E itself has algebraic degree $n-k$ (indeed, up to a linear transformation, we can take $E' = \mathbb{F}_2^{n-k}$, and T_E depends then only on its $n-k$ first coordinates).

Proposition 14 *Let $k \leq n$ be positive integers and let F be the multiplicative inverse function over $\mathbb{F}_{2^n}$. Let E be any k-dimensional $\mathbb{F}_2$-subspace of $\mathbb{F}_{2^n}$. Then we have $\sum_{u \in E} F(u) = \sum_{u \in E} u^{-1} = \sum_{u \in E; u \neq 0} \frac{1}{u} \neq 0$ if and only if the function $F\left(\prod_{u \in E}(x+u)\right) = \prod_{u \in E}(x+u)^{-1} = F \circ L_E(x)$ has algebraic degree $n-k$.*

Acknowledgement

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 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, Patrick Solé for his indications, Gregor Leander for his kind information about the integral attack, as well as Xiang-Dong Hou and Alexandr Polujan for useful references.

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. Preprint, 2023.

[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] 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.

[18] 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.

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

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

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

[22] 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.

[23] 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.

[24] 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).

[25] 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.

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

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

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

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

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

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

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

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

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