Cryptography and Communications (2024) 16:285–308
https://doi.org/10.1007/s12095-023-00661-3

RESEARCH

A lower bound for differential uniformity by multiplicative complexity & bijective functions of multiplicative complexity 1 over finite fields

Matthias Johann Steiner[1]

Received: 17 May 2022 / Accepted: 30 June 2023 / Published online: 15 August 2023

Abstract
The multiplicative complexity of an S-box over a finite field is the minimum number of multiplications needed to implement the S-box as an arithmetic circuit. In this paper we fully characterize bijective S-boxes with multiplicative complexity 1 up to affine equivalence over any finite field. We show that under affine equivalence in odd characteristic there are two classes of bijective functions and in even characteristic there are three classes of bijective functions with multiplicative complexity 1. Moreover, in (Jeon et al., Cryptogr. Commun., **14**(4), 849-874 (2022)) A-boxes where introduced to lower bound the differential uniformity of an S-box over $\mathbb{F}_2^n$ via its multiplicative complexity. We generalize this concept to arbitrary finite fields. In particular, we show that the differential uniformity of a (n, m)-S-box over $\mathbb{F}_q$ is at least q^{n-l}, where $\lfloor \frac{n-1}{2} \rfloor + l$ is the multiplicative complexity of the S-box.

Keywords Arithmetic circuit · Multiplicative complexity · M-box · S-box · Differential uniformity

Mathematics Subject Classification (2010) 94A60

1 Introduction

A natural performance measure for boolean circuits is the so-called multiplicative complexity, the minimal number of AND gates needed to implement a circuit as AND-XOR-NOT circuit. Though, for the design of boolean ciphers and hash functions the multiplicative complexity was only of minor concern in the past, because circuit implementations can be replaced by look-up tables. A prime example is the AES [1] S-box that operates on the finite field with 2^8 elements

$$\begin{aligned} S : \mathbb{F}_{2^8} &\to \mathbb{F}_{2^8}, \\ x &\mapsto x^{2^8-2}, \end{aligned}$$

✉ Matthias Johann Steiner
matthias.steiner@aau.at

[1] Cybersecurity, Alpen-Adria Universität Klagenfurt, Universitätsstraße 65-67, Klagenfurt am Wörthersee 9020, Austria

which can be implemented via a look-up table of size $2^8 \times 2^8$.

On the other hand, with the advancement of Zero-Knowledge (ZK) and Multi-Party Computation (MPC) multiplicative complexity became the major performance measure for cryptographic primitives that implement these protocols. First we note that ZK and MPC protocols operate on "big" finite fields $\mathbb{F}_q$ where typically $q \geq 2^{64}$ and in principle q can be a prime number instead of a power of two. If q is a prime, then the analog of the AND gate is simply the multiplication gate which multiplies two elements, hence the name multiplicative complexity. Obviously, for fields of this size the memory requirement of look-up tables is too big, so one has to implement the circuit of a cryptographic primitive. The raison d'être for multiplicative complexity as performance measure is that for ZK protocols based on "MPC-in-the-head" the signature size increases proportionally to the number of multiplication gates in the underlying cryptographic primitive [2]. Also, for MPC protocols based on Yao's garbled circuit [3, 4] the computational complexity depends on the number of multiplication gates in the underlying primitive.

Cryptographic primitives for efficient implementation of ZK and MPC are called *Arithmetization-Oriented* (AO) primitives. Examples of AO primitives are LowMC [5], `MiMC` [6], `GMiMC` [7], Hades [8], Jarvis [9], Poseidon [10], Vision and Rescue [11], Rescue-Prime [12] and `Ciminion` [13]. Although a lot of AO designs have already been proposed, their cryptanalysis is not well-understood yet. First, one has to generalize known cryptanalytic techniques over $\mathbb{F}_2$ or $\mathbb{F}_{2^n}$ to prime fields $\mathbb{F}_p$. Second, attack vectors that have been a minor concern in the past may become a viable threat, in particular Gröbner basis attacks [14]. Lastly, although most AO designs are very generic, so they can be instantiated over arbitrary finite fields, instantiating them over field extensions $\mathbb{F}_{2^n}$ can reduce the security compared to an instantiation over a prime field $\mathbb{F}_p$ of similar size. As example, let us take a look at `MiMC` whose keyed round function is defined as

$$\begin{aligned} R_i : \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{F}_q, \\ (x, k) &\mapsto (x + k + c_i)^3 , \end{aligned}$$

where $c_i \in \mathbb{F}_q$ is a round constant. Note that cubing induces a permutation if and only if $\gcd(3, q-1) = 1$. If we decide for $q = 2^n$ instead of a prime, then suddenly we have two possible models for `MiMC`. From the theory of finite fields it is well-known that

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q^n$$

as $\mathbb{F}_q$-vector spaces. So instead of the natural `MiMC` model over $\mathbb{F}_{2^n}$, we can also model it over $\mathbb{F}_2^n$, but over $\mathbb{F}_2$ one has an unique tool to analyze functions: the so-called algebraic normal form. Analysis of the degree growth of the algebraic normal form of `MiMC` yielded a slower than expected degree growth. Consequently, this property was exploited to mount a key recovery attack via a generalized higher-order differential attack on `MiMC` over binary fields [15].

Finally, for vectorial boolean functions

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

there already exists an established literature that connects multiplicative complexity with security parameters [16–19]. Therefore, the aim of this paper is to extend tools to analyze properties of functions via multiplicative complexity over binary fields to arbitrary finite fields.

1.1 Preliminaries & notation

In this paper, with $p \in \mathbb{Z}$ we always denote a prime number and with $q = p^e$ a prime power where $e \geq 1$. With $\mathbb{F}_q$ we denote the finite field with q elements, and with $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ we denote the cyclic group of invertible elements. By $\operatorname{char}(\mathbb{F}_q)$ we denote the characteristic of the field $\mathbb{F}_q$, i.e., the number of ones such that

$$1 + \ldots + 1 = 0$$

in $\mathbb{F}_q$. If $\mathbb{F}_q$ is clear from context, then we call a function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ a (n, m)-S-box. Matrices $\mathbf{M} \in \mathbb{F}_q^{n \times n}$ are denoted with bold capital letters, vectors are with lower capital letters $\mathbf{v} \in \mathbb{F}_q^n$, and the matrix-vector product is denoted as $\mathbf{M}\mathbf{v}$. We denote the canonical basis of $\mathbb{F}_q^n$ with $\mathbf{e}_1, \ldots, \mathbf{e}_n$, and the group of invertible $n \times n$ matrices over $\mathbb{F}_q$ is denoted as $\mathrm{GL}_n(\mathbb{F}_q)$. Since multiplications play a special role in this paper, we denote with $x \cdot y$ only the product of field elements $x, y \in \mathbb{F}_q$.

1.1.1 Arithmetic circuits

To properly define multiplicative complexity over arbitrary finite fields we need a proper generalization of AND-XOR-NOT logic. Any function $F : \mathbb{F}_2^n \to \mathbb{F}_2$ can be constructed using only AND-XOR-NOT, on the other hand any function over a finite field can be expressed as polynomial. Moreover, one can express AND-XOR-NOT with the following polynomials

$$\mathrm{AND}(x, y) = x \cdot y, \qquad \mathrm{XOR}(x, y) = x + y, \qquad \mathrm{NOT}(x) = x + 1.$$

Our route to generalize Boolean logic will be through polynomials. Any function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ can be represented by a polynomial, moreover if we restrict the degree in each variable to be less than q, then the polynomial representing the function is unique. Therefore, we call the $\mathbb{F}_q$-algebra $\mathbb{F}_q[\mathbf{X}_n] = \mathbb{F}_q[x_1, \ldots, x_n] / \left(x_1^q - x_1, \ldots, x_n^q - x_n\right)$ the algebra of polynomial valued functions. Moreover, we will use the terms function and polynomial synonymously throughout this paper.

Definition 1.1 *Let $\mathbb{F}_q$ be a finite field. We call a polynomial in two variables $f \in \mathbb{F}_q[x, y]$ a binary gate. We call a finite subset of binary gates $\mathcal{F} \subset \mathbb{F}_q[x, y]$ a generating set, if any polynomial valued function $g \in \mathbb{F}_q[\mathbf{X}_n]$, where $n \geq 1$, can be constructed using only $x_1, \ldots, x_n$ and $\mathcal{F}$.*

To construct any polynomial we definitely need a gate that represents multiplication, a gate that represents addition and a gate that adds a constant term, but if q is a prime power, then we need to introduce an additional gate, which will be called the cyclic gate, to construct all polynomials. The following theorem certainly is well-known, though we need it to properly define multiplicative complexity, and we need the explicit construction in the proof to generalize [16, Lemma 6].

Theorem 1.2 *Let $\mathbb{F}_q$ be a finite field, and let $\alpha \in \mathbb{F}_q^\times$ be a generator. Then the gates*

$$\begin{aligned} \mathrm{MUL}(x, y) &= x \cdot y, & \mathrm{CON}(x) &= x + 1, \\ \mathrm{ADD}(x, y) &= x + y, & \mathrm{CYC}(x) &= \alpha \cdot x \end{aligned}$$

form a generating set.

Proof Let $m = \beta \cdot x_1^{m_1} \cdots x_n^{m_n} \in \mathbb{F}_q[\mathbf{X}_n]$ be a monomial. Note that any x^k can be iteratively constructed via $x^k = \text{MUL}\left(x^{k-1}, x\right)$, so we can construct the monomials $x_1^{m_1}, \ldots, x_n^{m_n}$ via iterated MUL gates and their product again via iteration of MUL gates. For $\beta \in \mathbb{F}_q^\times$ there exists an $i \geq 0$ such that $\beta = \alpha^i$. So after constructing $x_1^{m_1} \cdots x_n^{m_n}$ we apply CYC i-times to arrive at m. If we have two monomials $m, n \in \mathbb{F}_q[\mathbf{X}_n]$, then we can construct their sum $m+n$ via ADD. So we can construct any polynomial with constant term 0 using only MUL-ADD-CYC. Let $f, g \in \mathbb{F}_q[\mathbf{X}_n]$ be such that $f(0) = \beta \in \mathbb{F}_q^\times$ and $g = f - \beta$. If $\beta = 1$ then $f = \text{CON}(g)$, so let's assume $\beta \neq 1$. We again can find an $i, j \geq 0$ such that $\alpha^i = \beta$ and $\alpha^j = (1-\beta)$. Now we apply the gates

$$\text{ADD}\left(\text{CYC}^{(j)}(g), \text{CYC}^{(i)}\left(\text{CON}(g)\right)\right) = (1-\beta)\cdot g + \beta \cdot (g+1) = g + \beta,$$

and the claim follows. □

Remark 1.3 1. If q is a prime, then the gate CYC is redundant, because for any $\beta \in \{0, \ldots, q-1\}$ and any monomial $m = x_1^{m_1} \cdots x_n^{m_n}$ we can construct $\beta \cdot m$ by $(\beta-1)$-fold application of ADD, i.e., $\beta \cdot m = \text{ADD}\left((\beta-1)\cdot m, m\right)$.
2. If $q = 2$, then the gates MUL, ADD, CON reduce to the Boolean gates AND, XOR, NOT.

Now we can define multiplicative complexity over any finite field.

Definition 1.4 *Let $\mathbb{F}_q$ be a finite field, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. The multiplicative complexity* $\text{MC}(F)$ *of F is defined as the minimum number of* MUL *gates needed to implement F in a* ADD-MUL-CON-CYC *circuit.*

1.1.2 Differential uniformity

Differential cryptanalysis is one of the most important tools of modern cryptography [20] which studies how a difference in input values can effect the resulting difference in output values. The key measure to quantify whether a function is weak to differential cryptanalysis is the so-called differential uniformity.

Definition 1.5 *Let $\mathbb{F}_q$ be a finite field, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function.*

(1) The differential distribution table of F at $\mathbf{a} \in \mathbb{F}_q^n$ and $\mathbf{b} \in \mathbb{F}_q^m$ is defined as

$$\delta_F(\mathbf{a}, \mathbf{b}) = \left|\{\mathbf{x} \in \mathbb{F}_q^n \mid F(\mathbf{x}+\mathbf{a}) - F(\mathbf{x}) = \mathbf{b}\}\right|.$$

(2) The differential uniformity of F is defined as

$$\delta(F) = \max_{\substack{\mathbf{a} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}, \\ \mathbf{b} \in \mathbb{F}_q^m}} \delta_F(\mathbf{a}, \mathbf{b}).$$

1.1.3 Notions of equivalence

By linear functions we refer to functions that are given via matrix multiplication, and by affine functions we refer to functions that are given via matrix multiplication and addition of a non-zero constant. Throughout this paper we will characterize functions between vector spaces over finite fields with respect to the following equivalence notions.

Definition 1.6 *Let $\mathbb{F}_q$ be a finite field, and let $F, G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be two functions.*

(1) F and G are said to be linearly equivalent if there exist two linear permutations $A_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $A_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $A_1 \circ F = G \circ A_2$.
(2) F and G are said to be affine equivalent if there exist two affine permutations $A_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $A_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $A_1 \circ F = G \circ A_2$.
(3) F and G are said to be extended-affine equivalent if there exist two affine permutations $A_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $A_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and an affine function $A_3 : \mathbb{F}_q^m \to \mathbb{F}_q^n$ such that $F(\mathbf{x}) = (A_2 \circ G \circ A_1)(\mathbf{x}) + A_3(\mathbf{x})$.

It is easy to see that these notions indeed define equivalence classes, moreover they preserve differential uniformity as well as multiplicative complexity.

1.2 Contributions

In the first part of this paper (Section 2) we extend the characterization of bijective functions with multiplicative complexity 1 up to affine equivalence from [16] to arbitrary finite fields. We show that in odd characteristic there are two classes of bijective functions and in even characteristic there are three classes of bijective functions up to affine equivalence.

Theorem 1.7 (Theorems 2.6 and 2.11) *Let $\mathbb{F}_q$ be a finite field, let $n \geq 3$, let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a bijective function with multiplicative complexity* 1*, and let*

$$\begin{aligned} \Lambda_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_{n-1} \cdot x_n, x_2, \ldots, x_n), \end{aligned}$$

$$\begin{aligned} \Theta_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_2^2, x_2, \ldots, x_n), \end{aligned}$$

$$\begin{aligned} \Gamma_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1^2, x_2, \ldots, x_n). \end{aligned}$$

Then,

(1) ([16, Theorem 1]) for $q = 2$, F is affine equivalent to Λ_n.
(2) for $q = 2^m$ and $m \geq 2$, F is affine equivalent to either Λ_n, Θ_n or Γ_n.
(3) for q odd, F is affine equivalent to either Λ_n or Θ_n.

If $q \neq 2$, then we obtain the following characterization in dimension 2.

Corollary 1.8 (Corollaries 2.7 and 2.12) *Let $\mathbb{F}_q$ be a finite field, let $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ be a bijective function with multiplicative complexity* 1*, and let*

$$\begin{aligned} \Theta_2 : \mathbb{F}_q^2 &\to \mathbb{F}_q^2, \\ (x_1, x_2) &\mapsto (x_1 + x_2^2, x_2), \end{aligned} \qquad \text{and} \qquad \begin{aligned} \Gamma_2 : \mathbb{F}_q^2 &\to \mathbb{F}_q^2, \\ (x_1, x_2) &\mapsto (x_1^2, x_2). \end{aligned}$$

Then,

(1) for $q = 2^m$ and $m \geq 2$, F is affine equivalent to either Θ_2 or Γ_2.
(2) for q odd, F is affine equivalent to Θ_2.

In [19] the differential uniformity of a boolean function was lower bounded via its multiplicative complexity. In the second part of this paper (Section 3) we generalize their techniques to arbitrary finite fields. In particular, we derive the following lower bound for the differential uniformity in terms of multiplicative complexity.

Corollary 1.9 (Corollary 3.9) *Let $\mathbb{F}_q$ be a finite field, and let S be a (n, m)-S-box.*

(1) If $\mathrm{MC}(S) \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, then $\delta(S) = q^n$.
(2) If $\mathrm{MC}(S) = \left\lfloor \frac{n-1}{2} \right\rfloor + l$, then $\delta(S) \geq q^{n-l}$ for all $l \geq 0$.

Though, we also have to note that the number of multiplications is in general not an indicator whether also $\delta(S) < q^n$. In Example 3.7 we present an S-box over finite fields $\mathbb{F}_q$, where $q > 2$, with an arbitrary number of multiplications that always has maximal differential uniformity.

2 Bijective functions with multiplicative complexity 1

In this section we characterize bijections $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with multiplicative complexity 1 up to affine equivalence.

2.1 Products of affine permutation polynomials

We call a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ such that $f(x) = \sum_{i=1}^n a_i \cdot x_i + a$, where $a_i, a \in \mathbb{F}_q$, an affine polynomial. As preparation, we need to establish that the product of two affine permutation polynomials is not a permutation polynomial.

Definition 2.1 ([21, 7.34. Definition]) *Let $\mathbb{F}_q$ be a finite field. A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is called a permutation polynomial in n indeterminates over $\mathbb{F}_q$ if the equation $f(x_1, \ldots, x_n) = \alpha$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $\alpha \in \mathbb{F}_q$.*

Remark 2.2 In the computer science literature for characteristic 2 a function represented by a permutation polynomial is commonly called a balanced function.

Moreover, with the notion of orthogonal systems, see [21, 7.35. Definition], it is easy to see that any non-constant affine polynomial is a multivariate permutation polynomial.

That the product of two non-constant affine polynomials is not a permutation polynomial follows as corollary to two theorems of Niederreiter [22]. Two polynomials $f, g \in \mathbb{F}_q[x_1, \ldots, x_n]$ are said to be equivalent if they can be transformed into each other via an affine change of variables $\mathbf{x} = \mathbf{A}\mathbf{y} + \mathbf{c}$, where $\mathbf{A} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ and $\mathbf{c} \in \mathbb{F}_q^n$.

Lemma 2.3 *Let $\mathbb{F}_q$ be a finite field, let $p = \mathrm{char}\left(\mathbb{F}_q\right)$, and let $f, g \in \mathbb{F}_q[x_1, \ldots, x_n]$ be non-constant affine polynomials.*

(1) If $p = 2$ and $g \neq \alpha \cdot f$, where $\alpha \in \mathbb{F}_q^\times$, then $f \cdot g$ is not a permutation polynomial.
(2) If $p > 2$, then $f \cdot g$ is not a permutation polynomial.

Proof For (1), by [22, Theorem 3] a polynomial h of degree at most 2 in n variables in characteristic $p = 2$ is a permutation polynomial if and only if h is equivalent to a polynomial of the form $\hat{h}(x_1, \ldots, x_{n-1}) + x_n$ or $\hat{h}(x_1, \ldots, x_{n-1}) + x_n^2$. Let us now consider the product

$$h(\mathbf{x}) = f(\mathbf{x}) \cdot g(\mathbf{x}) = \left(\sum_{i=1}^n a_i x_i + a\right) \cdot \left(\sum_{i=1}^n b_i x_i + b\right). \tag{1}$$

First we observe that if $g = \alpha \cdot f$, where $\alpha \in \mathbb{F}_q^\times$, then $h = \alpha \cdot f^2$. In characteristic two squaring induces a permutation, so h is a permutation polynomial. Therefore, we have to rule this case out. Now we do a case distinction on different values for the constant terms $a, b \in \mathbb{F}_q$.

Suppose $a, b = 0$, we have to make sure that for all variables x_i such that x_i^2 is present in h at least one mixed term $x_i \cdot x_j$, $i \neq j$, is present, then the decomposition fails. Suppose there exists a variable for which all mixed terms vanish, say x_1, but x_1^2 is present in the product. Then we must have that

$$\begin{aligned} a_1 \cdot b_2 + a_2 \cdot b_1 &= 0, \\ &\vdots \\ a_1 \cdot b_n + a_n \cdot b_1 &= 0. \end{aligned}$$

Of course, if $b_j \neq 0$, then also $a_j \neq 0$. Now we pick two indices $k, l \geq 2$ such that $a_k, b_l \neq 0$. We want to show that $a_k \cdot b_l + a_l \cdot b_l = 0$. We consider the equations

$$\begin{aligned} a_1 \cdot b_k + a_k \cdot b_1 &= 0, \\ a_1 \cdot b_l + a_l \cdot b_1 &= 0, \\ &\Longrightarrow \\ a_1 \cdot b_k \cdot a_l + a_k \cdot b_1 \cdot a_l &= 0, \\ a_1 \cdot b_l \cdot a_k + a_l \cdot b_1 \cdot a_k &= 0, \\ &\Longrightarrow \\ a_1 \cdot (a_k \cdot b_l + a_l \cdot b_k) &= 0. \end{aligned}$$

Hence, the mixed term $x_k \cdot x_l$ must also vanish. So, if all mixed terms in h that contain x_1 vanish but $a_1 \cdot b_1 \neq 0$, then all mixed terms in h must vanish. Consequently,

$$f(\mathbf{x}) \cdot g(\mathbf{x}) = \left(\sum_{i=1}^{n} a_i \cdot b_i \cdot x_i^2 \right) = \left(\sum_{i=1}^{n} (a_i \cdot b_i)^{1/2} x_i \right)^2,$$

and therefore $g = \alpha \cdot f$, where $\alpha \in \mathbb{F}_q^\times$.

Now suppose $a \neq 0$ and $b = 0$, then any linear term of the product polynomial h must be present in a quadratic or mixed term, so the decomposition fails. By symmetry, we can conclude the same for $a = 0$ and $b \neq 0$.

For the last case $a, b \neq 0$, we rewrite

$$h(\mathbf{x}) = \hat{f}(\mathbf{x}) \cdot \hat{g}(\mathbf{x}) + b \cdot \hat{f}(\mathbf{x}) + a \cdot \hat{g}(\mathbf{x}) + a \cdot b,$$

where $\hat{f} = f - a$ and $\hat{g} = g - b$. Now we have to do a subcase distinction, if $b \cdot \hat{f} + a \cdot \hat{g} = 0$, then we can pass to the first case $\hat{a}, \hat{b} = 0$ to conclude that if h is a permutation polynomial, then $\hat{g} = \alpha \cdot \hat{f}$, where $\alpha \in \mathbb{F}_q^\times$. Consequently, this implies that $\alpha \cdot a + b = 0$ and that

$$g = \hat{g} + b = \alpha \cdot \hat{f} + \alpha \cdot a = \alpha \cdot f.$$

On the other hand, if $b \cdot \hat{f} + a \cdot \hat{g} \neq 0$, then a decomposition of the form

$$h = \hat{h}(x_1, \ldots, x_{n-1}) + \lambda \cdot x_n,$$

$\lambda \in \mathbb{F}_q^\times$, is impossible, because if the linear monomial x_n is present in h, then the variable x_n must also be present in at least one quadratic term of h. So, the decomposition must be of the form

$$h = \hat{h}(x_1, \ldots, x_{n-1}) + \lambda \cdot x_n^2,$$

$\lambda \in \mathbb{F}_q^\times$, then we require that

$$a_n \cdot b + b_n \cdot a_n = 0.$$

Thus, the product $\hat{f} \cdot \hat{g}$ may not contain any mixed terms with the variable x_n, but again this already implies that $\hat{g} = \alpha \cdot \hat{f}$ and also $\alpha \cdot a + b = 0$.

Finally, if $g = \alpha \cdot f$, then this property is invariant under any invertible affine coordinate change of the product polynomial $h = f \cdot g$. Further, any affine coordinate change of h will end up in one of the discussed cases. We have now established that if $h = f \cdot g$ is equivalent to a permutation polynomial, then $g = \alpha \cdot f$, where $\alpha \in \mathbb{F}_q$. By negation, if $g \neq \alpha \cdot f$, then h cannot be equivalent to a permutation polynomial.

For (2), by [22, Theorem 2] a polynomial f of degree at most 2 in n variables in characteristic $p > 2$ is a permutation polynomial if and only if f is equivalent to a polynomial of the form $g(x_1, \ldots, x_{n-1}) + x_n$. Again we do a case distinction. If $a, b = 0$, then trivially such a decomposition cannot exist.

Now suppose $a \neq 0$ and $b = 0$, then any linear term of the product must be present in a quadratic or mixed term so the decomposition fails. By symmetry, we can conclude the same for $a = 0$ and $b \neq 0$.

If $a, b \neq 0$, assume that x_1 is present in h. Now let us try to do the composition with x_1. If $a_1, b_1 \neq 0$, then x_1^2 must also be present in h, so the decomposition is impossible. Hence, either $a_1 \neq 0$ and $b_1 = 0$ or $a_1 = 0$ and $b_1 \neq 0$. If one of them is non-zero, then there still must be a mixed term $x_1 \cdot x_j$, $j \neq 1$, present in h since f and g are non-constant. (Also, recall that the mixed terms containing x_1 can only be canceled if $a_1, b_1 \neq 0$.) So the decomposition fails.

Again, under any invertible affine change of coordinates we end up in one of the three cases. □

2.2 Odd characteristic

In [16, Lemma 4] a description of all bijections over $\mathbb{F}_2^n$ with multiplicative complexity 1 and constant term $\mathbf{0}$ was given. Our first major step is to extend this result, though in odd characteristic we also need to account for squaring.

Lemma 2.4 *Let $\mathbb{F}_q$ be a finite field with* $\operatorname{char}\left(\mathbb{F}_q\right) \neq 2$. *Any bijective function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $F(\mathbf{0}) = \mathbf{0}$, and multiplicative complexity* 1, *can be written in the form*

$$F(\mathbf{x}) = \mathbf{M}\mathbf{x} + \Big(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right) \Big)\mathbf{d},$$

where $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, *and* $\mathbf{a}^\intercal \mathbf{M}^{-1} \mathbf{d} = \mathbf{b}^\intercal \mathbf{M}^{-1} \mathbf{d} = 0$.

Proof It is easy to see that any function of this form has multiplicative complexity at most 1, and that the expression covers all functions over $\mathbb{F}_q^n$ that can be realized with a single $\mathbb{F}_q$ multiplication. So it is left to show that the conditions are necessary.

For a contradiction suppose that $\mathbf{M}$ is singular, and let $\mathbf{u} \in \ker(\mathbf{M})$ be non-zero. For the pair $(\mathbf{x}_1, \mathbf{x}_2 = \mathbf{x}_1 + \mathbf{u})$ we have that $\mathbf{M}\mathbf{x}_1 = \mathbf{M}\mathbf{x}_2$. On the other hand, if F is a bijection, then we must have that $F(\mathbf{x}_1) \neq F(\mathbf{x}_2)$ or equivalently $F(\mathbf{x}_1) - F(\mathbf{x}_2) \neq \mathbf{0}$. Therefore, we have

that

$$\begin{aligned} F(\mathbf{x}_1) - F(\mathbf{x}_2) = \Big(\left(\mathbf{a}^\intercal \mathbf{x}_1\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}_1\right) - \left(\mathbf{a}^\intercal \mathbf{x}_2\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}_2\right) \Big) \mathbf{d} \neq \mathbf{0} \\ \Rightarrow \left(\mathbf{a}^\intercal \mathbf{x}_1\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}_1\right) \neq \left(\mathbf{a}^\intercal \mathbf{x}_2\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}_2\right). \end{aligned} \tag{2}$$

Let $g(\mathbf{x}) = (\mathbf{a}^\intercal \mathbf{x}) \cdot (\mathbf{b}^\intercal \mathbf{x})$, and suppose that g is not a permutation polynomial. Then there exists $\alpha \in \mathbb{F}_q$ such that $\left|g^{-1}(\alpha)\right| > q^{n-1}$. For every $\mathbf{x} \in g^{-1}(\alpha)$ we define the sequence

$$\mathbf{s}_{\mathbf{x}}^{(j)} = \begin{cases} \mathbf{x}, & j = 0, \\ \mathbf{x} + \beta^{j-1}\mathbf{u}, & 1 \leq j \leq q-1, \end{cases}$$

where $\beta \in \mathbb{F}_q^\times$ is a generator. For each $\mathbf{x}$ and all $j \neq k$ the elements $\mathbf{s}_{\mathbf{x}}^{(j)}$ and $\mathbf{s}_{\mathbf{x}}^{(k)}$ are pairwise distinct but $\mathbf{M}\mathbf{s}_{\mathbf{x}}^{(j)} = \mathbf{M}\mathbf{s}_{\mathbf{x}}^{(k)}$. So by (2) we have that $g(\mathbf{x}) \neq g\left(\mathbf{s}_{\mathbf{x}}^{(j)}\right)$ for $1 \leq j \leq q-1$. Suppose that for distinct $\mathbf{x}_1, \mathbf{x}_2 \in g^{-1}(\alpha)$ there exist $j \neq k$ such that $\mathbf{s}_{\mathbf{x}_1}^{(j)} = \mathbf{s}_{\mathbf{x}_2}^{(k)}$, then $\mathbf{x}_2 = \mathbf{x}_1 + \beta^l \mathbf{u}$ for some $1 \leq l \leq q-1$ or $\mathbf{x}_2 = \mathbf{x}_1$. So either $\mathbf{x}_2 \notin g^{-1}(\alpha)$ or $\mathbf{x}_2 = \mathbf{x}_1$, a contradiction for both cases. Therefore, for distinct $\mathbf{x}_1, \mathbf{x}_2$ the corresponding sequences are distinct. In particular, we have that

$$\begin{aligned} S &= \left\{ \left\{ \mathbf{s}_{\mathbf{x}}^{(j)} \right\}_{1 \leq j \leq q-1} \mid \mathbf{x} \in g^{-1}(\alpha) \right\} \subset g^{-1}(\alpha)^{\complement}, \\ |S| &= (q-1) \cdot \left|g^{-1}(\alpha)\right|. \end{aligned}$$

Thus,

$$q^n = \left|g^{-1}(\alpha)\right| + \left|g^{-1}(\alpha)^{\complement}\right| \geq \left|g^{-1}(\alpha)\right| + |S| = q \cdot \left|g^{-1}(\alpha)\right| > q^n.$$

A contradiction, so g has to be a permutation polynomial. But this is a contradiction to Lemma 2.3 (2), so $\mathbf{M}$ cannot be singular.

For another contradiction, assume that $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} \neq 0$ or $\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{d} \neq 0$. Without loss of generality we can assume that $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} = 1$ (and similar for $\mathbf{b}$). By assumption F is a bijection, if we substitute $\mathbf{y} = F(\mathbf{x})$, then it is easy to see that $\mathbf{a}^\intercal \mathbf{M}^{-1} F(\mathbf{x})$ is also a permutation polynomial (cf. [21, 7.39. Corollary]). Expanding the product we see that

$$\begin{aligned} \mathbf{a}^\intercal \mathbf{M}^{-1} F(\mathbf{x}) &= \mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{M}\mathbf{x} + \Big(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right) \Big) \mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} \\ &= \mathbf{a}^\intercal \mathbf{x} + \left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right) \\ &= \left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(1 + \mathbf{b}^\intercal \mathbf{x}\right). \end{aligned}$$

On the other hand, by Lemma 2.3 (2) the product of two affine polynomials cannot be a permutation polynomial.

It is left to show that every such F is indeed a bijection. Now suppose that F is not a bijection, but the conditions for $\mathbf{a}$, $\mathbf{b}$, $\mathbf{d}$ and $\mathbf{M}$ are satisfied. Let

$$G(\mathbf{x}) = \mathbf{M}^{-1}\mathbf{x} - \Big(\left(\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \Big) \mathbf{d},$$

then a simple computation, see Appendix A, yields that $(F \circ G)(\mathbf{x}) = (G \circ F)(\mathbf{x}) = \mathbf{x}$. So F has a right and a left inverse, a contradiction. So F has to be a bijection. □

The next lemma is trivial, though we state it for completeness.

Lemma 2.5 *Let $\mathbb{F}_q$ be a finite field, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a bijective function. Then F is affine equivalent to $F_{\mathbf{c}} = F + \mathbf{c}$ with $\mathbf{c} \in \mathbb{F}_q^n$.*

Now we are ready to prove the generalization of [16, Theorem 1] in odd characteristic.

Theorem 2.6 *Let $\mathbb{F}_q$ be a finite field with* $\operatorname{char}\left(\mathbb{F}_q\right) \neq 2$, *let $n \geq 3$, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a bijective function with multiplicative complexity* 1. *Then F is affine equivalent to either*

$$\begin{aligned} \Lambda_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_{n-1} \cdot x_n, x_2, \ldots, x_n), \end{aligned}$$

or

$$\begin{aligned} \Theta_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_2^2, x_2, \ldots, x_n). \end{aligned}$$

Proof By Lemma 2.5 and transitivity of affine equivalence we can restrict the proof to functions with constant term equal to zero, i.e., $F(\mathbf{0}) = \mathbf{0}$. Let $\mathbf{e}_i \in \mathbb{F}_q^n$ have a 1 on the i-th position and else zeros. With Lemma 2.4 we can express Λ_n as

$$\mathbf{M} = \mathbf{I}_{n\times n}, \quad \mathbf{a} = \mathbf{e}_{n-1}, \quad \mathbf{b} = \mathbf{e}_n, \quad \mathbf{d} = \mathbf{e}_1,$$

and similar for Θ_n

$$\mathbf{M} = \mathbf{I}_{n\times n}, \quad \mathbf{a} = \mathbf{b} = \mathbf{e}_{n-1}, \quad \mathbf{d} = \mathbf{e}_1.$$

For $i \neq j$ one clearly has that $\mathbf{e}_i^\intercal \mathbf{I}_{n\times n} \mathbf{e}_j = 0$. Now we have to show that for any permissible choice of generators $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ from Lemma 2.4 we can find two invertible matrices $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ such that either $F(\mathbf{x}) = \mathbf{B}\Lambda_n(\mathbf{A}\mathbf{x})$ or $F(\mathbf{x}) = \mathbf{B}\Theta_n(\mathbf{A}\mathbf{x})$. In particular, if $\mathbf{a} \neq \alpha \cdot \mathbf{b}$, where $\alpha \in \mathbb{F}_q^\times$, then we show equivalence to Λ_n and if $\mathbf{a} = \alpha \cdot \mathbf{b}$, then we show equivalence to Θ_n.

First let's assume that $\mathbf{a} \neq \alpha \cdot \mathbf{b}$. Let $\mathbf{A} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ be arbitrary, we denote the rows of $\mathbf{A}$ by $\mathbf{u}_i^\intercal = \mathbf{e}_i^\intercal \mathbf{A}$. Let $\mathbf{B} = \mathbf{M}\mathbf{A}^{-1}$, then we have

$$\begin{aligned} F(\mathbf{x}) = \mathbf{B}\Lambda_n(\mathbf{A}\mathbf{x}) &= \mathbf{B}\mathbf{A}\mathbf{x} + \left(\left(\mathbf{u}_{n-1}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{u}_n^\intercal \mathbf{x}\right)\right)\mathbf{B}\mathbf{e}_1 \\ &= \mathbf{M}\mathbf{x} + \left(\left(\mathbf{u}_{n-1}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{u}_n^\intercal \mathbf{x}\right)\right)\left(\mathbf{M}\mathbf{A}^{-1}\mathbf{e}_1\right). \end{aligned}$$

By comparing these equations with Lemma 2.4 we must require that $\mathbf{u}_{n-1} = \mathbf{a}$, $\mathbf{u}_n = \mathbf{b}$, and $\mathbf{M}\mathbf{A}^{-1}\mathbf{e}_1 = \mathbf{d}$. Since $\mathbf{a}, \mathbf{b} \neq \mathbf{0}$ and $\mathbf{a} \neq \alpha \cdot \mathbf{b}$ we can conclude that the last two rows of $\mathbf{A}$ are linearly independent. Since $\mathbf{M}$ is invertible, we also have that $\mathbf{A}^{-1}\mathbf{e}_1 = \mathbf{M}^{-1}\mathbf{d}$. Now we see that

$$\mathbf{u}_i^\intercal \mathbf{M}^{-1}\mathbf{d} = \mathbf{e}_i^\intercal \mathbf{A}\mathbf{A}^{-1}\mathbf{e}_1 = \begin{cases} 1, & i = 1, \\ 0, & i \neq 1. \end{cases} \tag{3}$$

The conditions $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} = \mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{d} = \mathbf{0}$ from Lemma 2.4 guarantee that these conditions hold for $\mathbf{u}_{n-1} = \mathbf{a}$ and $\mathbf{u}_n = \mathbf{b}$. We can always choose the remaining $n - 3$ rows such that all u_i are linearly independent and (3) holds. E.g., we can choose $\mathbf{u}_1 = \mathbf{e}_1$ and the remaining basis vectors. If we have a conflict $\mathbf{u}_j \cdot \mathbf{M}^{-1}\mathbf{d} = \alpha \neq 0$, then we replace the vector with $\alpha^{-1}\mathbf{u}_j - \mathbf{u}_1$.

For $\mathbf{a} = \alpha \cdot \mathbf{b}$, let us first take a look at

$$F(\mathbf{x}) = \mathbf{M}\mathbf{x} + \alpha \cdot \left(\mathbf{a}^\intercal \mathbf{b}\right)^2 \mathbf{d}.$$

Let $\mathbf{N} = \alpha^{-1} \cdot \mathbf{1}_{n\times n}$, then we pass to $\mathbf{N}F(\mathbf{x})$. So without loss of generality we can assume that $\mathbf{a} = \mathbf{b}$, now we can in principle use the same strategy as in the first case to construct the affine equivalence to Θ_n, though we have one more row of $\mathbf{A}$ which can be chosen freely. □

Corollary 2.7 *Let $\mathbb{F}_q$ be a finite field with* $\operatorname{char}\left(\mathbb{F}_q\right) \neq 2$*, and let $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ be a bijective function with multiplicative complexity* 1*. Then F is affine equivalent to*

$$\begin{aligned}\Theta_2 : \mathbb{F}_q^2 &\to \mathbb{F}_q^2,\\ (x_1, x_2) &\mapsto (x_1 + x_2^2, x_2).\end{aligned}$$

Remark 2.8 Let $\operatorname{char}\left(\mathbb{F}_q\right) > 2$ and $\alpha \in \mathbb{F}_q^\times$, and suppose that for a bijective function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $\mathrm{MC}(F) = 1$ we have a decomposition as in Lemma 2.4. If $\mathbf{a} \neq \alpha \cdot \mathbf{b}$, then F is affine equivalent to Λ_n, and if $\mathbf{a} = \alpha \cdot \mathbf{b}$, then F is affine equivalent to Θ_n.

For completeness, let us discuss that Λ_n and Θ_n are not affine equivalent. Since only three variables are used in a non-trivial way it suffices to do the argument for $n = 3$. Assume that there exist matrices $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ such that

$$\Theta_3(\mathbf{x}) = \mathbf{B}\Lambda_3(\mathbf{A}\mathbf{x}). \tag{4}$$

Denote with $\mathbf{a}_i \in \mathbb{F}_q^n$ the row vectors of $\mathbf{A}$, then

$$\Lambda_3(\mathbf{A}\mathbf{x}) = \begin{pmatrix} \mathbf{a}_1\mathbf{x} + (\mathbf{a}_2\mathbf{x}) \cdot (\mathbf{a}_3\mathbf{x}) \\ \mathbf{a}_2\mathbf{x} \\ \mathbf{a}_3\mathbf{x} \end{pmatrix}. \tag{5}$$

In the first component we must have the monomial x_2^2, but all other quadratic monomials must vanish since we cannot cancel them via $\mathbf{B}$. Then our only possible choice is

$$\mathbf{a}_2 = (0, \alpha, 0)\,, \tag{6}$$

$$\mathbf{a}_3 = (0, \beta, 0)\,, \tag{7}$$

where $\alpha, \beta \in \mathbb{F}_q^\times$, but then $\mathbf{A}$ is singular.

2.3 Even characteristic

For binary fields $\mathbb{F}_{2^n}$ with $n \geq 2$ squaring induces a proper permutation, hence for the characterization of bijections with multiplicative complexity 1 we also have to account for this case.

As preparation, we need a matrix decomposition from linear algebra. This decomposition was also used in [19, §2.2], since the authors did not provide a reference for this decomposition and we could not find it in the standard literature available to us, we provide a proof here.

Lemma 2.9 *Let k be a field, and let $\mathbf{M}, \mathbf{N} \in k^{n\times m}$ be matrices such that $\mathbf{M}$ is the reduced row echelon form of $\mathbf{N}$. Then there exist matrices $\mathbf{A} \in \mathrm{GL}_n(k)$ and $\mathbf{B} \in \mathrm{GL}_m(k)$ such that $\mathbf{N} = \mathbf{A}\mathbf{M}$ and $\mathbf{N} = \mathbf{M}\mathbf{B}$.*

Proof Let $\operatorname{rank}(\mathbf{M}) = r$, any of the r row vectors of $\mathbf{M}$ can be expressed as linear combinations of row vectors of $\mathbf{N}$. We fill these combinations into the first r rows of $\mathbf{A}$. Note that these rows have to be linearly independent, if they were not, then we could express at least one non-zero row of $\mathbf{M}$ as linear combination of the other rows, a contradiction. Let $\mathbf{m}_i$ and $\mathbf{n}_i$ denote the row vectors of $\mathbf{M}$ and $\mathbf{N}$ respectively, for all $s > r$ we have that $\mathbf{n}_1, \ldots, \mathbf{n}_s$ are linearly dependent. For every $r < s \leq n$ we use such a linear dependence equation with

$\alpha_s \neq 0$ and $\alpha_t = 0$, where α_s is the coefficient of $\mathbf{n}_s$ in the combination and $s < t \leq n$, and fill these coefficients into $\mathbf{A}$. Clearly, we have that rank $(\mathbf{A}) > r$, because at least the $(r+1)^{\text{th}}$ row is independent from the first r rows. Denote with $\mathbf{a}_i = (a_{1,i}, \ldots, a_{m,i})$ the row vectors of $\mathbf{A}$ and suppose that rank $(\mathbf{A}) = s < n$, then

$$\mathbf{a}_{s+1} = \sum_{i=1}^{s} \beta_i \mathbf{a}_i, \tag{8}$$

for some $\beta_i \in k$. By construction of $\mathbf{A}$ we now have that

$$\begin{aligned}\mathbf{0} &= \sum_{j=1}^{m} a_{j,s+1}\mathbf{n}_j = \sum_{j=1}^{m}\sum_{i=1}^{s} \beta_i a_{j,i}\mathbf{n}_j = \sum_{i=1}^{s} \beta_i \sum_{j=1}^{m} a_{j,i}\mathbf{n}_j \\ &= \sum_{i=1}^{r} \beta_i \sum_{j=1}^{m} a_{j,i}\mathbf{n}_j = \sum_{i=1}^{r} \beta_i \mathbf{m}_i.\end{aligned}$$

The second equality follows from (8), the third follows because we can always interchange finite sums, the fourth follows because for $i > s$ the $\mathbf{n}_j$'s sum up to $\mathbf{0}$, and the last equality follows from the construction of the first r rows of $\mathbf{A}$. The $\mathbf{m}_i$'s are a basis of the row space of $\mathbf{N}$, therefore $\beta_i = 0$ for all i. Consequently,

$$\mathbf{a}_{s+1} = \sum_{i=r+1}^{s} \beta_i \mathbf{a}_i,$$

but this is impossible because $\mathbf{a}_{s+1}$ has a non-zero component which is zero for all $\mathbf{a}_i$ in the sum. A contradiction, so $\mathbf{A}$ has to be of full rank.

For the second decomposition, the reduced row echelon form $\mathbf{N}$ is an upper triangle matrix, therefore $\mathbf{N}^\intercal$ is a lower triangle matrix which obviously has a lower triangle reduced row echelon form. Our proof of the decomposition $\mathbf{N} = \mathbf{AM}$ works equally well for a matrix $\mathbf{N}'$ in lower triangle reduced row echelon form. So let $\mathbf{N}'$ be the lower triangle reduced row echelon form of $\mathbf{M}^\intercal$, then

$$\mathbf{N} = \left(\mathbf{N}'\right)^\intercal = \left(\mathbf{B}^\intercal \mathbf{M}^\intercal\right)^\intercal = \mathbf{MB}.$$

□

Now we can prove the analog of Lemma 2.4 in even characteristic.

Lemma 2.10 *Let $\mathbb{F}_q$ be a finite field with* $\operatorname{char}\left(\mathbb{F}_q\right) = 2$ *and $q \geq 4$, and let $\alpha \in \mathbb{F}_q^\times$. Any bijective function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $F(\mathbf{0}) = \mathbf{0}$, and multiplicative complexity 1, can be written in the form*

$$F(\mathbf{x}) = \mathbf{Mx} + \left(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)\right)\mathbf{d},$$

where

(1) $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $\mathbf{a} \neq \alpha \cdot \mathbf{b}$, $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, *and* $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} = \mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{d} = 0$, *or*

(2) $\mathbf{a}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $\mathbf{a} = \alpha \cdot \mathbf{b}$, $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, *and* $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} = 0$, *or*

(3) $\mathbf{a}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $\mathbf{a} = \alpha \cdot \mathbf{b}$, $\mathbf{M} \in \mathbb{F}_q^{n \times n}$ *has rank $n-1$, the matrix* $\begin{pmatrix}\mathbf{M} \\ \mathbf{a}^\intercal\end{pmatrix}$ *has rank n, and if $\mathbf{A} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ is the invertible matrix such that $\mathbf{N} = \mathbf{AM}$ is the reduced row echelon form of $\mathbf{M}$, then $\mathbf{Ad}$ has a non-zero entry on the zero row of $\mathbf{N}$.*

Proof As in odd characteristic, it is easy to see that any function of these forms has multiplicative complexity at most 1, and that the expressions cover all functions over $\mathbb{F}_q^n$ that can be realized with a single $\mathbb{F}_q$ multiplication. The arguments for necessity when $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ are identical to Lemma 2.4, though this time we apply Lemma 2.3 (1).

So let $\mathbf{M} \notin \mathrm{GL}_n\left(\mathbb{F}_q\right)$ and assume that we are given an equation

$$F(\mathbf{x}) = \mathbf{M}\mathbf{x} + \alpha \cdot \left(\mathbf{a}^\mathsf{T}\mathbf{x}\right)^2 \mathbf{d} = \mathbf{c}, \tag{9}$$

with $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$. By Lemma 2.9 there exists a matrix $\mathbf{A} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ such that $\mathbf{N} = \mathbf{A}\mathbf{M}$ is in reduced row echelon form. Thus, we can rewrite the previous equation system as

$$\mathbf{N}\mathbf{x} + \left(\mathbf{a}^\mathsf{T}\mathbf{x}\right)^2 \mathbf{A}\mathbf{d} = \mathbf{A}\mathbf{c}. \tag{10}$$

For the system to admit a unique solution we need n equations, so if j is the index of a zero row of $\mathbf{N}$, then we must have that $(\mathbf{A}\mathbf{d})_j \neq 0$. Suppose that rank $(\mathbf{M}) \leq n-2$, then $\mathbf{N}$ has at least two zero rows, then (10) has two linearly dependent quadratic equations, i.e., the system does not admit a unique solution. Therefore, we must have that rank $(M) = n-1$. Now let us explicitly write out the system of equations

$$\sum_{\substack{k=1 \\ i \neq j}}^{n} N_{i,k} \cdot x_k + \hat{d}_i \cdot \left(\mathbf{a}^\mathsf{T}\mathbf{x}\right)^2 = \hat{c}_i, \quad 1 \leq i < n$$

$$\hat{d}_n \cdot \left(\mathbf{a}^\mathsf{T}\mathbf{x}\right)^2 = \hat{c}_n,$$

where $\hat{\mathbf{d}} = \mathbf{A}\mathbf{d}$ and $\hat{\boldsymbol{c}} = \mathbf{A}\mathbf{c}$. We can use the last equation to transform the system into $n-1$ linear equations and one quadratic equation. Moreover, in characteristic 2 squaring induces a permutation, i.e., by raising the last equation to the power $q/2$ we can find a unique $\tilde{c}_j \in \mathbb{F}_q$ such that

$$\mathbf{a}^\mathsf{T}\mathbf{x} = \tilde{c}_j.$$

So we can transform the system of equations into a linear one which admits a solution if and only if the matrix $\begin{pmatrix} \mathbf{A}\mathbf{M} \\ (\mathbf{A}\mathbf{d})_n \mathbf{a}^\mathsf{T} \end{pmatrix}$ has rank n. Obviously, this is also equivalent to the matrix $\begin{pmatrix} \mathbf{M} \\ \mathbf{a}^\mathsf{T} \end{pmatrix}$ having full rank.

Now suppose that the conditions for one of the three cases are satisfied, but F is not a bijection. For each case we already derived a unique procedure to find a unique solution to (9). (For the first two cases again see Appendix A.) A contradiction, so F has to be a bijection. □

Now we can generalize [16, Theorem 1] to field extensions of $\mathbb{F}_2$.

Theorem 2.11 *Let $\mathbb{F}_q$ be a finite field with* $\mathrm{char}\left(\mathbb{F}_q\right) = 2$ *and $q \geq 4$, let $n \geq 3$, and let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a bijective function with multiplicative complexity* 1. *Then F is affine*

equivalent to either

$$\begin{aligned}\Lambda_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n,\\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_{n-1} \cdot x_n, x_2, \ldots, x_n),\end{aligned}$$

or

$$\begin{aligned}\Theta_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n,\\ (x_1, \ldots, x_n) &\mapsto (x_1 + x_2^2, x_2, \ldots, x_n),\end{aligned}$$

or

$$\begin{aligned}\Gamma_n : \mathbb{F}_q^n &\to \mathbb{F}_q^n,\\ (x_1, \ldots, x_n) &\mapsto (x_1^2, x_2, \ldots, x_n).\end{aligned}$$

Proof In the situations (1) and (2) of Lemma 2.10 we can use the same strategy as in Theorem 2.6 to establish affine equivalence with Λ_n and Θ_n respectively. So we only have to prove case (3). Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ be such that $\mathbf{a} = \alpha \cdot \mathbf{b}$, where $\alpha \in \mathbb{F}_q^\times$. Then

$$F(\mathbf{x}) = \mathbf{M}\mathbf{x} + \alpha \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)^2 \mathbf{d}.$$

Let $\mathbf{N} = \alpha^{-1} \cdot \mathbf{1}_{n\times n}$, then

$$\mathbf{N}\mathbf{F}(\mathbf{x}) = \alpha^{-1} \cdot \mathbf{M}\mathbf{x} + \left(\mathbf{b}^\intercal \mathbf{x}\right)^2 \mathbf{d}.$$

So without loss of generality we can assume that $\mathbf{a} = \mathbf{b}$.

Let us now construct the affine equivalence. Γ_n can be written as

$$\Gamma_n(\mathbf{x}) = \begin{pmatrix} 0 & 0 & \ldots & 0\\ 0 & 1 & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & 1 \end{pmatrix} \mathbf{x} + \left(\mathbf{e}_1^\intercal \mathbf{x}\right)^2 \mathbf{e}_1$$

We want to find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ such that $F(\mathbf{x}) = \mathbf{B}\Gamma_n(\mathbf{A}\mathbf{x})$. We require that $\mathbf{e}_1^\intercal \mathbf{A} = \mathbf{a}^\intercal$ and $\mathbf{B}\mathbf{e}_1 = \mathbf{d}$. Without loss of generality we can assume that

$$\mathbf{M} = \begin{pmatrix} \mathbf{M}_1\\ \mathbf{0}^\intercal\\ \mathbf{M}_2 \end{pmatrix}.$$

If $\mathbf{M}$ is not of this form, then we apply Lemma 2.9 to find $\mathbf{C} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ such that $\mathbf{N} = \mathbf{C}\mathbf{M}$ is in row echelon form of rank $n-1$, so it has a zero row. Since we try to find equivalence up to affine transformations we can replace $F(\mathbf{x})$ by $\mathbf{C}F(\mathbf{x})$ and permute the components of the resulting mapping. Moreover, we must have that

$$\mathbf{M} = \begin{pmatrix} \mathbf{M}_1\\ \mathbf{0}^\intercal\\ \mathbf{M}_2 \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{d} & \mathbf{b}_2 & \ldots & \mathbf{b}_n \end{pmatrix}}_{=\mathbf{B}} \begin{pmatrix} 0 & 0 & \ldots & 0\\ 0 & 1 & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & 1 \end{pmatrix} \underbrace{\begin{pmatrix} \mathbf{a}^\intercal\\ \mathbf{a}_2^\intercal\\ \vdots\\ \mathbf{a}_n^\intercal \end{pmatrix}}_{=\mathbf{A}} = \begin{pmatrix} \mathbf{0} & \mathbf{b}_2 & \ldots & \mathbf{b}_n \end{pmatrix} \begin{pmatrix} \mathbf{a}^\intercal\\ \mathbf{a}_2^\intercal\\ \vdots\\ \mathbf{a}_n^\intercal \end{pmatrix}.$$

Let j be the index of the zero row of $\mathbf{M}$, for the $\mathbf{b}_i$'s we pick all canonical unit vectors $\mathbf{e}_i$ except for $\mathbf{e}_j$. Note that $\mathbf{d}_j \neq 0$, else we would not have a permutation in Lemma 2.10, and henceforth $\mathbf{B}$ has full rank. Now the last equation becomes

$$\begin{pmatrix} \mathbf{M}_1 \\ \mathbf{0}^\intercal \\ \mathbf{M}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{e}_1 & \dots & \mathbf{e}_{j-1} & \mathbf{e}_{j+1} & \dots & \mathbf{e}_n \end{pmatrix} \begin{pmatrix} \mathbf{a}^\intercal \\ \mathbf{a}_2^\intercal \\ \vdots \\ \mathbf{a}_n^\intercal \end{pmatrix} = \begin{pmatrix} \mathbf{a}_2^\intercal \\ \vdots \\ \mathbf{a}_j^\intercal \\ \mathbf{0}^\intercal \\ \mathbf{a}_{j+1}^\intercal \\ \vdots \\ \mathbf{a}_n^\intercal \end{pmatrix}.$$

By the conditions from Lemma 2.10 the matrix on the left-hand side has rank $n-1$, so we have a unique solution for the $\mathbf{a}_i$'s. Finally, by construction

$$\mathbf{A} = \mathbf{D} \begin{pmatrix} \mathbf{M}_1 \\ \mathbf{a}^\intercal \\ \mathbf{M}_2 \end{pmatrix},$$

where $\mathbf{D} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ is a suitable reordering of the rows, has full rank. □

Corollary 2.12 *Let $\mathbb{F}_q$ be a finite field with $\mathrm{char}\left(\mathbb{F}_q\right) = 2$ and $q \geq 4$, and let $F : \mathbb{F}_q^2 \to \mathbb{F}_q^2$ be a bijective function with multiplicative complexity 1. Then F is affine equivalent to either*

$$\begin{aligned} &\Theta_2 : \mathbb{F}_q^2 \to \mathbb{F}_q^2, \\ &(x_1, x_2) \mapsto (x_1 + x_2^2, x_2), \end{aligned} \quad \textit{or} \quad \begin{aligned} &\Gamma_2 : \mathbb{F}_q^2 \to \mathbb{F}_q^2, \\ &(x_1, x_2) \mapsto (x_1^2, x_2). \end{aligned}$$

Remark 2.13 Let $\mathrm{char}\left(\mathbb{F}_q\right) = 2, q \geq 4$ and $\alpha \in \mathbb{F}_q^\times$, and suppose that for a bijective function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $\mathrm{MC}(F) = 1$ we have a decomposition as in Lemma 2.10. If $\mathbf{a} \neq \alpha \cdot \mathbf{b}$, then F is affine equivalent to Λ_n, if $\mathbf{a} = \alpha \cdot \mathbf{b}$ and $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, then F is affine equivalent to Θ_n, and if $\mathbf{a} = \alpha \cdot \mathbf{b}$ and $\mathbf{M} \notin \mathrm{GL}_n\left(\mathbb{F}_q\right)$, then F is affine equivalent to Γ_n.

For completeness, let us again discuss that Λ_n, Θ_n and Γ_n are not affine equivalent. For Λ_n and Θ_n the argument is identical to the one in odd characteristic, see the end of Section 2.2. For Θ_n and Γ_n it suffices to reduce to $n = 2$, note that for all $a, b \in \mathbb{F}_q^\times$ one has

$$(a \cdot x_1 + b \cdot x_2)^2 = a^2 \cdot x_1^2 + b^2 \cdot x_2^2. \tag{11}$$

Thus, any affine change of coordinates for Γ_2 is unable to produce the required polynomial $x_1 + x_2^2$. For Λ_n and Γ_n is suffices to reduce to $n = 3$. Let $\mathbf{A} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$ and denote with $\mathbf{a}_i \in \mathbb{F}_q^n$ its rows. Note that

$$\left(\sum_{i=1}^{3} \mathbf{a}_i \mathbf{x_i}\right)^2$$

cannot contain any monomial $x_i \cdot x_j$, where $i \neq j$. So one can never produce the required polynomial $x_1 + x_2 \cdot x_3$.

3 M-Boxes and differential uniformity

In [19] a new tool was introduced to describe properties of a (n, m)-S-box S over $\mathbb{F}_2$: the associated A-box S_A. Conceptually, the A-box S_A collects all AND-gates of a AND-XOR-NOT circuit that implements S in a vector. Then one can construct S from S_A by applying an affine function. Since we want to generalize this tool to arbitrary finite fields we will define the so-called M-box which contains all multiplications of an arithmetic circuit for an S-box.

3.1 Expansion–compression lemma

In [16, Lemma 6] a process was given to construct any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with multiplicative complexity $\mathrm{MC}(F) \leq c$ and $F(\mathbf{0}) = \mathbf{0}$ by extending iteratively with single multiplications to $\mathbb{F}_q^{n+c}$ and then contracting back to $\mathbb{F}_2^n$ via a linear map. The proof of [16, Lemma 6] can be applied over any finite field, for completeness we summarize the main idea of the proof. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be any function with multiplicative complexity $\mathrm{MC}(F) \leq c$, by Theorem 1.2 we have a circuit for F using at most c many MUL gates. Iteratively, we compute each MUL gate and append its output to $\mathbf{x}$, this way we end up with a vector $\mathbf{z} \in \mathbb{F}_q^{n+c}$ which contains all monomials that are present in the polynomial vector representation of F. Now one can apply a linear function to construct F. Moreover, with this lemma we have a well-defined procedure to extract all multiplications in an S-box into a new associated function.

Lemma 3.1 (Expansion–Compression Lemma [16, Lemma 6]) *Let $\mathbb{F}_q$ be a finite field, let*

$$\begin{aligned} E_n : \mathbb{F}_q^n &\to \mathbb{F}_q^{n+1}, \\ \mathbf{x} &\mapsto \left(\mathbf{x}, (\mathbf{a}^\intercal \mathbf{x}) \cdot (\mathbf{b}^\intercal \mathbf{x})\right), \end{aligned}$$

with $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, and let $C_{m,n} : \mathbb{F}_q^m \to \mathbb{F}_q^n$ be a linear map. Any function $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $F(\mathbf{0}) = \mathbf{0}$, and multiplicative complexity $\mathrm{MC}(F) \leq c$ can be written as composition

$$F = C_{n+c,n} \circ E_{n+c-1} \circ \cdots \circ E_n.$$

We will refer to the E_i's as expansion functions. Moreover, we denote the vectors that define the i^{th} expansion function by $\mathbf{b}_i$ and $\mathbf{b}_{i+1}$ and refer to them as i^{th} partner vectors. The tuple $(\mathbf{b}_1, \ldots, \mathbf{b}_{2k+1})$ will be called the partner tuple.

3.2 Definition of the M-box

With Lemma 3.1 we can decompose any (n, m)-S-box S with $\mathrm{MC}(S) \leq k$ into an expansion part and a compression part. (We now allow affine transformations in the compression to adjust for the constant term.) The output of the expansion part consists of two parts, n elements for the input $\mathbf{x} \in \mathbb{F}_q^n$, we call this part the identity part, and k elements that are the output of MUL gates, we call this part the multiplication part or simply MUL-part. We can interpret the MUL-part as a (n, k)-S-box, which we therefore define as an *M-box*. We denote the M-box associated to an S-box S by S_M, obviously we have also that $\mathrm{MC}(S_M) \leq k$. Let's formalize the concept of M-boxes in mathematical terms.

Definition 3.2 (M-box, cf. [19, Definition 1]) *Let $\mathbb{F}_q$ be a finite field, and Let $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{y} \in \mathbb{F}_q^k$ be the input and output, respectively, of a (n, k)-S-box S_M. For $2k$ vectors $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{F}_q^n, \ldots, \mathbf{b}_{2k}, \mathbf{b}_{2k+1} \in \mathbb{F}_q^{n+k}$ that satisfy the following inductive properties, S_M is called a (n, k)-M-box.*

(i) $y_1 = \left(\mathbf{b}_1^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}_2^\intercal \mathbf{x}\right)$.
(ii) *For* $2 \leq i \leq k$, $y_i = \left(\mathbf{b}_i^\intercal \left(\mathbf{x}, y_1, \ldots, y_{i-1}\right)\right) \cdot \left(\mathbf{b}_{i+1}^\intercal \left(\mathbf{x}, y_1, \ldots, y_{i-1}\right)\right)$.

For a (n,k)*-M-box* S_M, $\mathbf{b}_{2i-1}$ *and* $\mathbf{b}_{2i}$ *are called the* i^{th} *partner vectors for all* i, *and* $(\mathbf{b}_1, \ldots, \mathbf{b}_{2k})$ *is called the partner tuple of* S_M.

Provided a circuit $\mathcal{C}_S$ for the (n,m)-S-box S such that $\mathrm{MC}(S) \leq k$ is given, then it is straight-forward to extract a circuit $\mathcal{C}_{S_M}$ for a corresponding (n,k)-M-box S_M. We build $\mathcal{C}_{S_M}$ inductively in k layers. First we collect all the multiplication gates in $\mathcal{C}_S$, then we pick one multiplication gate which can be built only with linear combinations of the input $\mathbf{x} \in \mathbb{F}_q^n$. In the first layer of $\mathcal{C}_{S_M}$ we now construct the multiplication gate and denote its output by y_1. Next we pick a multiplication gate that only requires $\mathbf{x}$ and y_1 as input, then we construct this gate in the second layer of $\mathcal{C}_{S_M}$ and denote its output by y_2. Inductively, we now run-through all remaining multiplication gates until we have constructed all multiplication gates of $\mathcal{C}_S$. This yields a circuit for $\mathcal{C}_{S_M}$. Of course from the construction of $\mathcal{C}_{S_M}$ we can also extract a set of suitable partner vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{2k-1}, \mathbf{b}_{2k}$.

3.3 Equivalence classes of M-boxes

For this section we fix some notation, with $T_\mathbf{A} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ we will always denote a linear function $T_\mathbf{A}(\mathbf{x}) = \mathbf{A}\mathbf{x}$, where $\mathbf{A} \in \mathbb{F}_q^{n \times m}$.

Using Lemma 3.1 and Definition 3.2 we can decompose a (n,m)-S-box S as

$$S(\mathbf{x}) = T\Big(\big(\mathbf{x}, S_M(\mathbf{x})\big)\Big) + \mathbf{c}, \tag{12}$$

for a (n,k)-M-box S_M, a linear function $T : \mathbb{F}_q^{m+k} \to \mathbb{F}_q^n$, and $\mathbf{c} \in \mathbb{F}_q^n$. The linear function T can be further decomposed into a M-box part and an identity part, i.e., there are $T_\mathbf{N} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and $T_{\mathbf{N}'} : \mathbb{F}_q^k \to \mathbb{F}_q^m$ such that

$$T\Big(\big(\mathbf{x}, S_M(\mathbf{x})\big)\Big) = T_\mathbf{N}(\mathbf{x}) + T_{\mathbf{N}'}\big(S_M(\mathbf{x})\big). \tag{13}$$

(Note that in the last equation we considered the natural extension of $T_\mathbf{N}$ and $T_{\mathbf{N}'}$ to $\mathbb{F}_q^{n+k} \to \mathbb{F}_q^m$.) With Lemma 2.9 we can further rewrite (13) as

$$T\Big(\big(\mathbf{x}, S_M(\mathbf{x})\big)\Big) = T_\mathbf{N}(\mathbf{x}) + (T_\mathbf{D} \circ T_\mathbf{M} \circ S_M)(\mathbf{x}), \tag{14}$$

where $\mathbf{M} \in \mathbb{F}_q^{m \times k}$ is a matrix in reduced row echelon form and $\mathbf{D} \in \mathrm{GL}_m\left(\mathbb{F}_q\right)$. I.e., we have established extended-affine equivalence between S and $T_\mathbf{M} \circ S_M$. We technically summarize this construction in the following theorem which generalizes [19, Theorem 1].

Theorem 3.3 *Let* $\mathbb{F}_q$ *be a finite field. For any* (n,m)*-S-box* S *with* $\mathrm{MC}(S) \leq k$, *there exists a matrix* $\mathbf{M} \in \mathbb{F}_q^{m \times k}$ *in reduced row echelon form and a* (n,k)*-M-box* S_M *such that* $T_\mathbf{M} \circ S_M$ *is extended-affine equivalent to* S. *If* $\mathrm{MC}(S) = k$, *then* S_M *is called suitable for* S.

Now let's characterize equivalence for M-boxes. For two linear permutations $T_\mathbf{A} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $T_\mathbf{B} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ a (n,m)-M-box S_M is clearly linearly equivalent to $T_\mathbf{B} \circ S_M \circ T_\mathbf{A}$. Substituting this equivalence into (14) we obtain that

$$T_\mathbf{D} \circ T_\mathbf{M} \circ S_M = T_\mathbf{D} \circ T_\mathbf{M} \circ T_\mathbf{B} \circ S_M \circ T_\mathbf{A} = T_{\mathbf{D}'} \circ T_{\mathbf{M}'} \circ S_M \circ T_\mathbf{A} \tag{15}$$

for an invertible matrix $\mathbf{D}' \in \mathbb{F}_q^{m \times m}$, and a matrix $\mathbf{M}' \in \mathbb{F}_q^{m \times k}$ in reduced row echelon form. Therefore, we can reduce our search for equivalent M-boxes to $S_M \circ T_\mathbf{A}$ which leads to the generalization of [19, Theorem 2].

Theorem 3.4 *Let $\mathbb{F}_q$ be a finite field. For a (n,k)-M-box S_M and a linear permutation $T_{\mathbf{L}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, let $S'_M = S_M \circ T_{\mathbf{L}}$, which is a M-box linearly equivalent to S_M. If $(\mathbf{b}_1, \ldots, \mathbf{b}_{2k})$ is a partner tuple of S_M, then the following $(\mathbf{b}'_1, \ldots, \mathbf{b}'_{2k+1})$ is a partner tuple of S'_M such that*

$$\begin{aligned} \mathbf{b}'_{2i-1} &= T_{\mathbf{L}_i^\intercal}(\mathbf{b}_{2i-1}), \\ \mathbf{b}'_{2i} &= T_{\mathbf{L}_i^\intercal}(\mathbf{b}_{2i}), \end{aligned}$$

where $\mathbf{L}_i = \begin{pmatrix} \mathbf{L} & \mathbf{0}_{n\times(i-1)} \\ \mathbf{0}_{(i-1)\times n} & \mathbf{I}_{(i-1)\times(i-1)} \end{pmatrix}$ *for* $1 \le i \le k$.

Proof The proof of [19, Theorem 2] does not depend on $\mathbb{F}_2$, therefore we can apply it for any finite field. For a thorough presentation we repeat the arguments. We denote with $S_M(\mathbf{x}) = \mathbf{y}$ and $S_M \circ T_{\mathbf{L}}(\mathbf{x})(\mathbf{x}) = (z_1, \ldots, z_k)$. Now we expand the inductive definition of the M-box to obtain

$$\begin{aligned} z_1 &= \left(\mathbf{b}_1^\intercal T_{\mathbf{L}}(\mathbf{x})\right) \cdot \left(\mathbf{b}_2^\intercal T_{\mathbf{L}}(\mathbf{x})\right) \\ &= \left(T_{\mathbf{L}^\intercal}(\mathbf{b}_1)^\intercal \mathbf{x}\right) \cdot \left(T_{\mathbf{L}^\intercal}(\mathbf{b}_2)^\intercal \mathbf{x}\right). \end{aligned}$$

So $T_{\mathbf{L}^\intercal}(\mathbf{b}_1)$ and $T_{\mathbf{L}^\intercal}(\mathbf{b}_2)$ become new partner vectors and we denote

$$\mathbf{b}'_1 = T_{\mathbf{L}^\intercal}(\mathbf{b}_1), \quad \mathbf{b}'_2 = T_{\mathbf{L}^\intercal}(\mathbf{b}_2).$$

Continuing,

$$\begin{aligned} z_2 &= \left(\mathbf{b}_3^\intercal\left(T_{\mathbf{L}}(\mathbf{x}), z_1\right)\right) \cdot \left(\mathbf{b}_4^\intercal\left(T_{\mathbf{L}}(\mathbf{x}), z_1\right)\right) \\ &= \left(\mathbf{b}_3^\intercal T_{\mathbf{L}_1}(\mathbf{x}, z_1)\right) \cdot \left(\mathbf{b}_4^\intercal T_{\mathbf{L}_1}(\mathbf{x}, z_1)\right) \\ &= \left(T_{\mathbf{L}_1^\intercal}(\mathbf{b_3})^\intercal(\mathbf{x}, z_1)\right) \cdot \left(T_{\mathbf{L}_1^\intercal}(\mathbf{b_4})^\intercal(\mathbf{x}, z_1)\right), \end{aligned}$$

where

$$\mathbf{L}_2 = \begin{pmatrix} \mathbf{L} & \mathbf{0}_{n\times 1} \\ \mathbf{0}_{1\times n} & \mathbf{1}_{1\times 1} \end{pmatrix}.$$

Again, we denote

$$\mathbf{b}'_3 = T_{\mathbf{L}_2^\intercal}(\mathbf{b}_3), \quad \mathbf{b}'_4 = T_{\mathbf{L}_2^\intercal}(\mathbf{b}_4).$$

Inductively repeating this process we obtain that

$$\begin{aligned} \mathbf{L}_i &= \begin{pmatrix} \mathbf{L} & \mathbf{0}_{n\times(i-1)} \\ \mathbf{0}_{(i-1)\times n} & \mathbf{I}_{(i-1)\times(i-1)} \end{pmatrix}, \\ \mathbf{b}'_{2i-1} &= T_{\mathbf{L}_i^\intercal}(\mathbf{b}_{2i-1}) \\ \mathbf{b}'_{2i} &= T_{\mathbf{L}_i^\intercal}(\mathbf{b}_{2i}) \\ z_i &= \left(\mathbf{b'_{2i-1}}^\intercal(\mathbf{x}, z_1, \ldots, z_{i-1})\right) \cdot \left(\mathbf{b'_{2i}}^\intercal(\mathbf{x}, z_1, \ldots, z_{i-1})\right). \end{aligned}$$

This yields a (n,k)-M-box $S'_M = S_M \circ T_{\mathbf{L}}$. □

3.4 Lower bounds of differential uniformity via multiplicative complexity

Since differential uniformity is invariant under extended-affine equivalence it suffices to consider a (n,m)-S-box $S = T_{\mathbf{M}} \circ S_M$ with a suitable M-box S_M and a matrix $\mathbf{M}$ in reduced row echelon form. Moreover, differential uniformity is preserved under affine equivalence,

therefore without loss of generality we can assume that the affine permutations from the extended-affine equivalence are the identity permutations and that S is constant free. I.e.,

$$S = T_{\mathbf{M}} \circ S_M + T_{\mathbf{C}}, \tag{16}$$

where $T_{\mathbf{C}}$ is a linear function. So, for any $\mathbf{x}, \mathbf{a} \in \mathbb{F}_q^n$ we have that

$$S(\mathbf{x}+\mathbf{a}) - S(\mathbf{x}) = T_{\mathbf{M}} \circ \big(S_M(\mathbf{x}+\mathbf{a}) - S_M(\mathbf{x})\big) + T_{\mathbf{C}}(\mathbf{a}). \tag{17}$$

Consequently, for any $\mathbf{b} \in \mathbb{F}_q^m$ and $\hat{\mathbf{b}} = T_{\mathbf{M}}(\mathbf{b}) + T_{\mathbf{C}}(\mathbf{a})$ we have the following inclusion of sets

$$\begin{aligned}
&\left\{\mathbf{x} \in \mathbb{F}_q^n \mid S_M(\mathbf{x}+\mathbf{a}) - S_M(\mathbf{x}) = \mathbf{b}\right\} \\
\subseteq &\left\{\mathbf{x} \in \mathbb{F}_q^n \mid T_{\mathbf{M}} \circ \big(S_M(\mathbf{x}+\mathbf{a}) - S_M(\mathbf{x})\big) = T_{\mathbf{M}}(\mathbf{b})\right\} \\
= &\left\{\mathbf{x} \in \mathbb{F}_q^n \mid T_{\mathbf{M}} \circ \big(S_M(\mathbf{x}+\mathbf{a}) - S_M(\mathbf{x})\big) = \hat{\mathbf{b}} - T_{\mathbf{C}}(\mathbf{a})\right\} \\
= &\left\{\mathbf{x} \in \mathbb{F}_q^n \mid S(\mathbf{x}+\mathbf{a}) - S(\mathbf{x}) = \hat{\mathbf{b}}\right\}.
\end{aligned}$$

Moreover, this inclusion of sets implies that

$$\begin{aligned}
\delta(S) = \delta(T_{\mathbf{M}} \circ S_m + T_{\mathbf{C}}) &\geq \delta_S\big(\mathbf{a}, \hat{\mathbf{b}}\big) \\
&\geq \delta_{S_M}\big(\mathbf{a}, T_{\mathbf{M}}(\mathbf{b})\big) \geq \delta_{S_M}(\mathbf{a}, \mathbf{b}),
\end{aligned}$$

which also implies that

$$\delta(S) \geq \delta(S_M). \tag{18}$$

Hence, to prove lower bounds on S-boxes it suffices to prove lower bounds for (suitable) M-boxes. Note that technically we never used the assumption that S_M is suitable to derive Inequality (18). Though, we will see in Theorem 3.8 that with suitable M-boxes we derive the highest upper bounds.

For partner vectors $\mathbf{b}_i$ of a M-box we denote with $\mathbf{b}_i|^n$ the restriction to the first n entries of $\mathbf{b}_i$. The input difference vectors $\mathbf{a}$ such that $(\mathbf{b}_i|^n)^\mathsf{T}\,\mathbf{a} = 0$ form a vector space which will be called complementable space. In the following lemma, which generalizes [19, Lemma 1], we collect the key properties of complementable spaces.

Lemma 3.5 *Let $\mathbb{F}_q$ be a finite field, and let S_M be a (n,k)-M-box. Define the set $\mathcal{C}_{S_M} \subset \mathbb{F}_q^n$ of all $\mathbf{a} \in \mathbb{F}_q^n$ satisfying $(\mathbf{b}_i|^n)^\mathsf{T}\,\mathbf{a} = 0$ for all partner vectors $\mathbf{b}_i$ to be a complementable space of S_M. The complementable space $\mathcal{C}_{S_M}$ has the following properties.*

(1) For $\mathbf{a} \in \mathcal{C}_{S_M}$, $S_M(\mathbf{a}) = \mathbf{0}$.
(2) For $\mathbf{a} \in \mathcal{C}_{S_M}$ and $\mathbf{x} \in \mathbb{F}_q^n$, $S_M(\mathbf{x}) = S_M(\mathbf{x}+\mathbf{a})$.
(3) If there is a non-zero vector in $\mathcal{C}_{S_M}$, then $\delta(S_M) = q^n$.

Proof The proof of [19, Lemma 1] does not depend on $\mathbb{F}_2$ therefore we can apply it for any finite field. For a thorough presentation we repeat the arguments. For (1), let $\mathbf{a} \in \mathcal{C}_{S_M}$ and $S_M = (f_1, \ldots, f_k)$. By assumption

$$f_1(\mathbf{a}) = \big(\mathbf{b}_1^\mathsf{T}\mathbf{a}\big) \cdot \big(\mathbf{b}_2^\mathsf{T}\mathbf{a}\big) = 0,$$

inductively we now continue

$$f_i(\mathbf{a}) = \big(\mathbf{b}_{2i-1}^\mathsf{T}(\mathbf{a}, \mathbf{0}_{i-1})\big) \cdot \big(\mathbf{b}_{2i}^\mathsf{T}(\mathbf{a}, \mathbf{0}_{i-1})\big) = 0.$$

Therefore, $S_M(\mathbf{a}) = \mathbf{0}$.

For (2), let $S_M(\mathbf{x}) = (y_1, \ldots, y_k)$ and $S_M(\mathbf{x}+\mathbf{a}) = (y'_1, \ldots, y'_k)$. We show per induction that $y_i = y'_i$. For $i = 1$,

$$\begin{aligned} y'_1 &= \left(\mathbf{b}_1^\intercal\,(\mathbf{x}+\mathbf{a})\right) \cdot \left(\mathbf{b}_2^\intercal\,(\mathbf{x}+\mathbf{a})\right) \\ &= \left(\mathbf{b}_1^\intercal\mathbf{x} + \mathbf{b}_1^\intercal\mathbf{a}\right) \cdot \left(\mathbf{b}_2^\intercal\mathbf{x} + \mathbf{b}_2^\intercal\mathbf{a}\right) \\ &= \left(\mathbf{b}_1^\intercal\mathbf{x}\right) \cdot \left(\mathbf{b}_2^\intercal\mathbf{x}\right) = y_1. \end{aligned}$$

Suppose now that the claim is true for $2 \leq i \leq k-1$, then

$$\begin{aligned} y'_i &= \left(\mathbf{b}_{2i-1}^\intercal\left(\mathbf{x}+\mathbf{a}, y'_1, \ldots, y'_{i-1}\right)\right) \cdot \left(\mathbf{b}_{2i}^\intercal\left(\mathbf{x}+\mathbf{a}, y'_1, \ldots, y'_{i-1}\right)\right) \\ &= \left(\mathbf{b}_{2i-1}^\intercal\,(\mathbf{x}+\mathbf{a}, y_1, \ldots, y_{i-1})\right) \cdot \left(\mathbf{b}_{2i}^\intercal\,(\mathbf{x}+\mathbf{a}, y_1, \ldots, y_{i-1})\right) \\ &= \left(\mathbf{b}_{2i-1}^\intercal\,(\mathbf{x}, y_1, \ldots, y_{i-1}) + \left(\mathbf{b}_{2i-1}|^n\right)^\intercal\mathbf{a}\right) \cdot \left(\mathbf{b}_{2i}^\intercal\,(\mathbf{x}, y_1, \ldots, y_{i-1}) + \left(\mathbf{b}_{2i}|^n\right)^\intercal\mathbf{a}\right) \\ &= y_i\,. \end{aligned}$$

Lastly, (3) follows from (2) because $S_M(\mathbf{x}+\mathbf{a}) = S_M(\mathbf{a})$ for all $\mathbf{x} \in \mathbb{F}_q^n$, so $\delta(S_M) = \delta_{S_M}(\mathbf{a}, \mathbf{0}) = q^n$. □

So, for k large enough can one ensure that $\mathcal{C}_{S_M} = \{\mathbf{0}\}$? We already mentioned that $\mathcal{C}_{S_M}$ is a linear space. We define the matrix of transposed truncated partner vectors as

$$\mathbf{A} = \left(\mathbf{b}_1|^n \ \ldots\ \mathbf{b}_{2k+1}|^n\right)^\intercal, \tag{19}$$

then by definition we can view $\mathcal{C}_{S_M}$ as the following kernel

$$\mathcal{C}_{S_M} = \ker(\mathbf{A}) = \left\{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{A}\mathbf{x} = \mathbf{0}\right\}. \tag{20}$$

If k is increased by one, then two more rows are appended to $\mathbf{A}$. For the complementable space to be trivial we need that $\operatorname{rank}(\mathbf{A}) = n$. Therefore, we have the necessary condition that

$$k > \left\lfloor \frac{n-1}{2} \right\rfloor. \tag{21}$$

This leads to the generalization of [19, Theorem 3].

Theorem 3.6 *Let $\mathbb{F}_q$ be a finite field, and let S_M be a (n,k)-M-box. If $k \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, then $\delta(S_M) = q^n$.*

In [19, §3.1] it was established that this condition is sufficient over $\mathbb{F}_2$. Essentially, this is due to $x^2 = x$ in $\mathbb{F}_2$. Unfortunately, this condition cannot be sufficient over other finite fields as one can see from the following counterexample.

Example 3.7 Let $\mathbb{F}_q$ be a finite field. We consider the map

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} (x_1+x_2)\cdot x_3 \\ \left((x_1+x_2)\cdot x_3\right)^2 \\ \vdots \\ \left((x_1+x_2)\cdot x_3\right)^{2k} \end{pmatrix},$$

for some $k \geq 1$. For any finite field with $q > 2$ this defines an $(3, k+1)$-M-box. Obviously, for $k \geq 1$ we have more than $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$ multiplications. On the other hand, for any $k \geq 1$ the matrix of the restricted partner vectors has only two non-zero vectors.

We conclude that over finite fields different from $\mathbb{F}_2$ having many multiplications does not suffice, we need *sufficiently many elementary multiplications* for the complementable space to be trivial. We will shortly revisit this notion in Section 3.5 and prove an efficient criterion for an S-box not having sufficiently many elementary multiplications.

On the other hand, the lower bound from [19, Theorem 4] can be generalized independently from this observation.

Theorem 3.8 *Let $\mathbb{F}_q$ be a finite field, and let S_M be a (n,k)-M-box. If $k = \left\lfloor \frac{n-1}{2} \right\rfloor + l$, then $\delta(S_M) \geq q^{n-l}$ for all $l \geq 0$.*

Proof We can generalize the proof of [19, Theorem 3], though we have to account for more than two field elements. We do induction on l, for $l = 0$ we can apply Theorem 3.6. Now suppose that the theorem holds for $l > 0$, we consider a $(n, k+1)$-M-box S_M, where $k = \left\lfloor \frac{n-1}{2} \right\rfloor + l$. If we consider $S_M|_k$, i.e., S_M without the last MUL gate, then by our induction hypothesis $\delta(S_M|_k) \geq q^{n-l}$. On the other hand, we have the following equality of sets

$$\begin{aligned}&\left\{\mathbf{x} \in \mathbb{F}_q^n \mid S_M|_k(\mathbf{x}+\mathbf{a}) - S_M|_k(\mathbf{x}) = \mathbf{b}\right\}\\ &= \bigcup_{\alpha \in \mathbb{F}_q} \left\{\mathbf{x} \in \mathbb{F}_q^n \mid S_M(\mathbf{x}+\mathbf{a}) - S_M(\mathbf{x}) = (\mathbf{b}, \alpha)\right\}.\end{aligned}$$

We can now conclude from the pigeonhole principle that at least for one $\alpha \in \mathbb{F}_q$ we have that $\delta_{S_M}\big(\mathbf{a}, (\mathbf{b}, \alpha)\big) \geq q^{n-l-1}$. Therefore, we have that $\delta(S_M) \geq q^{n-l-1}$. □

One should keep in mind that only if the M-box has sufficiently many elementary multiplications, then the inequality could become non-trivial, else the differential uniformity is always maximal.

Combining Theorems 3.3, 3.6, 3.8 we now obtain the generalization of [19, Corollary 1].

Corollary 3.9 *Let $\mathbb{F}_q$ be a finite field, and let S be a (n,m)-S-box.*

(1) If $\mathrm{MC}(S) \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, then $\delta(S) = q^n$.
(2) If $\mathrm{MC}(S) = \left\lfloor \frac{n-1}{2} \right\rfloor + l$, then $\delta(S) \geq q^{n-l}$ for all $l \geq 0$.

3.5 An efficient criterion for not sufficiently many elementary multiplications

In the previous section we observed in Example 3.7 that only multiplications with linear combinations of $x_1, \ldots, x_n$ have the potential to lower the differential uniformity. For practical considerations one would like to have criteria to efficiently determine whether an S-box has sufficiently many elementary multiplications or not. In the following proposition we show that at least for the latter case it can be sufficient to simply look at the monomials in the components of the S-box.

Proposition 3.10 *Let $\mathbb{F}_q$ be a finite field, and let S be a (n,m)-S-box, and let $\mathcal{M} \in \mathbb{F}_q[x_1, \ldots, x_n]$ be the set of all non-linear monomials that are present in the components of S. If there exists an x_i which is not present in any monomial of $\mathcal{M}$, then S has maximal differential uniformity $\delta(S) = q^n$.*

Proof We implement S with the M-box S_M which constructs every monomial independently. (I.e., the product $(x_1 + x_2) \cdot x_3$ is implemented via $(x_1 \cdot x_3, x_2 \cdot x_3)$.). Since x_j is not present in any component of S_M it is obvious that all partner vectors of S_M are zero on the i^{th} component. So by Lemma 3.5 S_M has maximal differential uniformity. □

We note that this criterion has a rather trivial proof too, since any such (n, m)-S-box can also be considered as $(n-1, m)$-S-box via extended-affine equivalence and being constant in one component implies maximal differential uniformity. Though, to showcase the theory developed in this paper we proved it via the M-box.

We provide evidence that a converse positive criterion like "every variable x_i divides at least one monomial in $\mathcal{M}$, then the differential uniformity is less than q^n" won't be true in general as it is quite simple to find a counterexample.

Example 3.11 (cf. [23, §4.3]) Let $\mathbb{F}_q$ be finite field, and let $f \in \mathbb{F}_q[x]$ be a polynomial with $\deg(f) \geq 2$. We consider the Lai–Massey permutation

$$\mathcal{F}_{\mathrm{LM}} : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + f(x_1 - x_2) \\ x_2 + f(x_1 - x_2) \end{pmatrix}.$$

Clearly, we can find for both variables monomials that are divisible by them. On the other hand, the Lai–Massey permutation is affine equivalent to the Feistel permutation

$$\mathbf{A} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ F(x_1, x_2) = \begin{pmatrix} x_1 \\ x_2 + f(x_1) \end{pmatrix},$$

then $F_{\mathrm{LM}} = T_{\mathbf{B}} \circ F \circ T_{\mathbf{A}}$.

4 Conclusions

In this paper, we fully characterized bijective functions with multiplicative complexity 1 over finite fields. We also extended the techniques of [19] to study differential uniformity in terms of the associated M-box. We want to mention that in [19, §4] an algorithm was described to find S-boxes over $\mathbb{F}_2^n$ which satisfy the lower bound on differential uniformity in Corollary 3.9. In principle, one could come up with a similar algorithm for arbitrary finite fields $\mathbb{F}_q$, though for large n or q this method becomes computationally infeasible.

Acknowledgements The author would like to thank the anonymous reviewers for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper.

Funding Open access funding provided by University of Klagenfurt. Matthias Steiner was supported by the KWF under project number KWF-3520|31870|45842.

Declarations

Competing Interests The author declares no competing interests.

Appendix A

A simple calculation

Let $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$, $\mathbf{M} \in \mathrm{GL}_n\left(\mathbb{F}_q\right)$, $\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{d} = \mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{d} = 0$, and let

$$F(\mathbf{x}) = \mathbf{M}\mathbf{x} + \Big(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)\Big)\mathbf{d},$$
$$G(\mathbf{x}) = \mathbf{M}^{-1}\mathbf{x} - \Big(\left(\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}\right)\Big)\mathbf{M}^{-1}\mathbf{d}.$$

We first observe that

$$\mathbf{a}^\intercal G(\mathbf{x}) = \mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}, \qquad \mathbf{a}^\intercal \mathbf{M}^{-1} F(\mathbf{x}) = \mathbf{a}^\intercal \mathbf{x},$$
$$\mathbf{b}^\intercal G(\mathbf{x}) = \mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}, \qquad \mathbf{b}^\intercal \mathbf{M}^{-1} F(\mathbf{x}) = \mathbf{b}^\intercal \mathbf{x}.$$

Then

$$\begin{aligned}
&(F \circ G)(\mathbf{x}) = \\
&\quad = \mathbf{M}\left(\mathbf{M}^{-1}\mathbf{x} - \left(\left(\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}\right)\right)\mathbf{M}^{-1}\mathbf{d}\right) \\
&\qquad + \left(\left(\mathbf{a}^\intercal G(\mathbf{x})\right) \cdot \left(\mathbf{b}^\intercal g(\mathbf{x})\right)\right)\mathbf{d} \\
&\quad = \mathbf{x} - \left(\left(\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}\right)\right)\mathbf{d} + \left(\left(\mathbf{a}^\intercal \mathbf{M}^{-1}\mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1}\mathbf{x}\right)\right)\mathbf{d} \\
&\quad = \mathbf{x},
\end{aligned}$$

and similar

$$\begin{aligned}
&(G \circ F)(\mathbf{x}) = \\
&\quad = \mathbf{M}^{-1}\left(\mathbf{M}\mathbf{x} + \left(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)\right)\mathbf{d}\right) \\
&\qquad - \left(\left(\mathbf{a}^\intercal \mathbf{M}^{-1} F(\mathbf{x})\right) \cdot \left(\mathbf{b}^\intercal \mathbf{M}^{-1} F(\mathbf{x})\right)\right)\mathbf{M}^{-1}\mathbf{d} \\
&\quad = \mathbf{x} + \left(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)\right)\mathbf{M}^{-1}\mathbf{d} - \left(\left(\mathbf{a}^\intercal \mathbf{x}\right) \cdot \left(\mathbf{b}^\intercal \mathbf{x}\right)\right)\mathbf{M}^{-1}\mathbf{d} \\
&\quad = \mathbf{x}.
\end{aligned}$$

References

1. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard, 2nd edn. Information Security and Cryptography. Springer, Berlin, Heidelberg (2020). https://doi.org/10.1007/978-3-662-60769-5
2. Chase, M., Derler, D., Goldfeder, S., Orlandi, C., Ramacher, S., Rechberger, C., Slamanig, D., Zaverucha, G.: Post-quantum zero-knowledge and signatures from symmetric-key primitives. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. CCS'17, pp. 1825–1842. Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3133997
3. Yao, A.C.-C.: How to generate and exchange secrets. In: 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), pp. 162–167 (1986). https://doi.org/10.1109/SFCS.1986.25
4. Songhori, E.M., Hussain, S.U., Sadeghi, A.-R., Schneider, T., Koushanfar, F.: TinyGarble: Highly compressed and scalable sequential garbled circuits. In: 2015 IEEE Symposium on Security and Privacy, pp. 411–428 (2015). https://doi.org/10.1109/SP.2015.32
5. Albrecht, M.R., Rechberger, C., Schneider, T., Tiessen, T., Zohner, M.: Ciphers for MPC and FHE. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015, pp. 430–454. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_17

6. Albrecht, M., Grassi, L., Rechberger, C., Roy, A., Tiessen, T.: MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016, pp. 191–219. Springer, Berlin, Heidelberg (2016).https://doi.org/10.1007/978-3-662-53887-6_7
7. Albrecht, M.R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A., Schofnegger, M.: Feistel structures for mpc, and more. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) Computer Security – ESORICS 2019, pp. 151–171. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-29962-0_8
8. Grassi, L., Lüftenegger, R., Rechberger, C., Rotaru, D., Schofnegger, M.: On a generalization of substitution-permutation networks: The HADES design strategy. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020, pp. 674–704. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45724-2_23
9. Ashur, T., Dhooghe, S.: MARVELlous: a STARK-Friendly Family of Cryptographic Primitives. Cryptology ePrint Archive, Report 2018/1098 (2018). https://ia.cr/2018/1098
10. Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., Schofnegger, M.: Poseidon: A new hash function for Zero-Knowledge proof systems. In: 30th USENIX Security Symposium (USENIX Security 21), pp. 519–535. USENIX Association, United States (2021). https://www.usenix.org/conference/usenixsecurity21/presentation/grassi
11. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of symmetric-key primitives for advanced cryptographic protocols. IACR Trans. Symmetric Cryptol. 2020(3), 1–45 (2020). https://doi.org/10.13154/tosc.v2020.i3.1-45
12. Aly, A., Ashur, T., Ben-Sasson, E., Dhooghe, S., Szepieniec, A.: Design of symmetric-key primitives for advanced cryptographic protocols. IACR Trans. Symmetric Cryptol. 2020(3), 1–45 (2020). https://doi.org/10.13154/tosc.v2020.i3.1-45
13. Dobraunig, C., Grassi, L., Guinet, A., Kuijsters, D.: Ciminion: Symmetric encryption based on Toffoli-gates over large finite fields. In: Canteaut, A., Standaert, F.-X. (eds.) Advances in Cryptology – EUROCRYPT 2021, pp. 3–34. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77886-6_1
14. Albrecht, M.R., Cid, C., Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C., Schofnegger, M.: Algebraic cryptanalysis of stark-friendly designs: Application to marvellous and mimc. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, pp. 371–397. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34618-8_13
15. Eichlseder, M., Grassi, L., Lüftenegger, R., Øygarden, M., Rechberger, C., Schofnegger, M., Wang, Q.: An algebraic attack on ciphers with lowdegree round functions: Application to full mimc. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, pp. 477–506. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64837-4_16
16. Zajac, P., Jókay, M.: Multiplicative complexity of bijective 4x4 S-boxes. Cryptogr. Commun. **6**(3), 255–277 (2014). https://doi.org/10.1007/s12095-014-0100-y
17. Zajac, P.: Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity. Des. Codes Cryptogr. **82**(1), 43–56 (2017). https://doi.org/10.1007/s10623-016-0256-x
18. Boyar, J., Find, M.G.: Multiplicative complexity of vector valued boolean functions. Theoret. Comput. Sci. **720**, 36–46 (2018). https://doi.org/10.1016/j.tcs.2018.02.023
19. Jeon, Y., Baek, S., Kim, H., Kim, G., Kim, J.: Differential uniformity and linearity of S-boxes by multiplicative complexity. Cryptogr. Commun. **14**(4), 849–874 (2022). https://doi.org/10.1007/s12095-021-00547-2
20. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) Advances in Cryptology-CRYPTO' 90, pp. 2–21. Springer, Berlin, Heidelberg (1991). https://doi.org/10.1007/3-540-38424-3_1
21. Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Encyclopedia of mathematics and its applications. Cambridge Univ. Press, Cambridge (1997)
22. Niederreiter, H.: Permutation polynomials in several variables over finite fields. Proc. Japan Acad. **46**(9), 1001–1005 (1970). https://doi.org/10.2183/pjab1945.46.1001
23. Roy, A., Steiner, M.: An Algebraic System for Constructing Cryptographic Permutations over Finite Fields. arXiv. V6 (2022). https://doi.org/10.48550/ARXIV.2204.01802