Characterisation of Bijectivity Preserving Componentwise Modification of S-Boxes

Kaisa Nyberg

Department of Computer Science
Aalto University School of Science, Finland
kaisa.nyberg@aalto.fi

Abstract. Various systematic modifications of vectorial Boolean functions have been used for finding new previously unknown classes of S-boxes with good or even optimal differential uniformity and nonlinearity. Recently, a new method was proposed for modification a component of a bijective vectorial Boolean function by using a linear function. It was shown that the modified function remains bijective under the assumption that the inverse of the function admits a linear structure. A previously known construction of such a modification based on bijective Gold functions in odd dimension is a special case of this type of modification. In this paper, we show that the existence of a linear structure is necessary. Further, we consider replacement of a component of a bijective vectorial Boolean function in the general case. We prove that a permutation on $\mathbb{F}_2^n$ remains bijective if and only if the replacement is done by composing the permutation with an unbalanced Feistel transformation where the round function is any Boolean function on $\mathbb{F}_2^{n-1}$.

1 Introduction

Search for S-boxes that satisfy desirable cryptographic criteria has been under intensive study since they were proposed for use as the main nonlinear component in the construction of cryptographic primitives.

Among other methods, systematic variation of S-boxes has been proposed. In this paper we consider bijective S-boxes and their modification by changing one component in such a way that the new S-box is also a permutation.

Beierle and Leander suggested that an S-box which has one linear component but is otherwise highly nonlinear could be a good starting point when constructing new highly nonlinear S-boxes [BL20]. Further, they give two examples of permutations on $\mathbb{F}_{2^n}$ that have low differential uniformity but one linear component. In odd dimension, their construction is done for the inverse of a Gold function, while in even dimension the starting point is an earlier construction of a 2-to-1 function based on the multiplicative inverse function on $\mathbb{F}_{2^{n-1}}$.

Recently, the example using Gold function was shown to be a special case of a more general method based on the existence of a linear structure of type 1 for a component of the inverse of the permutation [Nyb22]. Since the components of a Gold function have linear structures of type 1, any component of the inverse of a Gold function can be replaced by a linear Boolean function.

The multiplicative inverse function in a finite field does not have linear structures. Therefore the question arises, whether existence of a linear structure is necessary for the construction of permutations with linear components. In this paper we answer this question affirmatively.

More generally, we show that the existence of linear structures is a necessary prerquisite for any componentwise modification of a permutation that preserves bijectivity. In particular, we establish a characterisation of the relationship between two different extensions of a 2-to-1 function in terms of existence of a linear structure of type 1. This characterisation is then further expressed in terms of a Feistel transformation.

Outline. We start by introducing the necessary preliminaries in Section 2. In Section 3 we recall the modification method derived from the existence of a linear structure. The necessity of the existence of a linear structure is proved in Section 4 where also the connection to Feistel transformations is established. Our characterisation of bijectivity preserving componentwise modification is presented in Section 5 and the conclusions are drawn in Section 6.

2 Preliminaries

We consider the vector space $\mathbb{F}_2^n$ of dimension n over $\mathbb{F}_2$ where n is a positive integer. A vector $x \in \mathbb{F}_2^n$ can be represented as an n-tuple $x = (x_1, \dots, x_n)$ of coordinates $x_i \in \mathbb{F}_2$, $i = 1, \dots, n$. We denote by '$\oplus$' the addition in $\mathbb{F}_2^n$. The zero element in $\mathbb{F}_2^n$ is denoted by 0_n, where the subscript is omitted if $n = 1$. For two vectors $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_2^n$ we define an inner product denoted as $x \cdot y$ by setting

$$x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n.$$

The n^{th} coordinate vector $(0, \dots, 0, 1)$ is denoted by e_n. The orthogonal complement of a subspace $U \subset \mathbb{F}_2^n$ is denoted by $U^\perp$.
A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is said to be balanced if the size of its support is equal to 2^{n-1}. This is equivalent to saying that the Walsh transform of f at 0_n is equal to 0.
Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vectorial Boolean function. Given a vector $\beta \in \mathbb{F}_2^m$, $\beta \neq 0$, we define a component of F as the Boolean function

$$x \mapsto \beta \cdot F(x), \ x \in \mathbb{F}_2^n,$$

and denote this function by $\beta \cdot F$. A vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is a permutation (bijection) if and only if all its components are balanced.
Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f is said to have a linear structure if there is a vector $w \in \mathbb{F}_2^n$, $w \neq 0_n$, such that

$$f(x \oplus w) \oplus f(x) = \delta, \text{ for all } x \in \mathbb{F}_2^n,$$

where $\delta \in \mathbb{F}_2$ is a constant [MS89]. Then we say that w is a linear structure of type δ of f.

3 Replacing a Component by a Linear One

Beierle and Leander studied bijective APN Gold functions in odd dimension. They showed that the inverse of such a Gold function, which is APN and has high nonlinearity, can be modified by replacing one component by a linear function in such a way that the resulting modification is also a permutation [BL20].
This construction was studied in [Nyb22] where it was shown that a sufficient prerequisite allowing the linear replacement, is that any component of a Gold function has a linear structure of type 1. Let us restate the result from [Nyb22].

Theorem 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a bijective vectorial Boolean function and assume that one of its components, say $\beta \cdot F$ has a linear structure w of type 1. Let $\alpha \in \mathbb{F}_2^n$ be such that $\alpha \cdot w = 1$ and F^{-1} be modified by replacing the component $\alpha \cdot F^{-1}$ by the linear function $x \mapsto \beta \cdot x$. Then the resulting function is a bijection.*

The main tool for connecting the linear structure to the bijectivity property is the permutation π constructed as follows.

Theorem 2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with a linear structure w of type 1. We define a function $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by setting*

$$(\gamma \cdot \pi)(x) = \gamma \cdot x,\ x \in \mathbb{F}_2^n,$$

for all $\gamma \in \{0, w\}^\perp$. The remaining components are defined by first fixing an $\alpha \in \mathbb{F}_2^n$ such that $\alpha \cdot w = 1$ and then setting

$$\alpha \cdot \pi(x) = f(x),\ x \in \mathbb{F}_2^n.$$

Then π is a permutation.

Example Let f be a Boolean function on $\mathbb{F}_2^n$ of the form

$$f(x_1, \ldots, x_n) = x_n \oplus g'(x_1, \ldots, x_{n-1}). \tag{1}$$

Then $e_n = (0, \ldots, 0, 1)$ is a linear structure of f. The resulting permutation π is given as follows

$$\pi(x_1, \ldots, x_n) = \big(x_1, \ldots, x_{n-1}, x_n \oplus g'(x_1, \ldots, x_{n-1})\big). \tag{2}$$

Such a permutation is known as one round of an unbalanced Feistel network where the round function g' is a Boolean function on $\mathbb{F}_2^{n-1}$. We shall call it the unbalanced $(n-1, 1)$ Feistel transformation.
The goal of this paper is to show that an unbalanced Feistel transformation is essentially the only possible function to be applied on a permutation if bijectivity is desired to be preserved in componentwise modification.

4 A Linear Structure Is Necessary

The second construction of a differentially 4-uniform permutation with null nonlinearity given in [BL20] was obtained by adding a linear component to a known example of a differentially 4-uniform 2-to-1 function.
Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ be a 2-to-1 function. Given a Boolean function f on $\mathbb{F}_2^n$, let us define a function R_f from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ by setting

$$R_f(x) = (S(x), f(x)).$$

As noted in [BL20] the function R_f is a permutation if and only if f is balanced and $S(\mathrm{supp}(f)) = \mathbb{F}_2^{n-1}$. Such f can always be found be dividing the input space into two disjoint sets A and B such that $S|_A$ and $S|_B$ are injections, and setting

$$f(x) = \begin{cases} 0, & \text{if } x \in A \\ 1, & \text{if } x \in B. \end{cases}$$

The question is, can f be chosen to be linear, in other words, can the set A be chosen to be a hyperplane in $\mathbb{F}_2^n$.
In this section we show that if a linear extension exists, then any other bijective extension of S has an inverse which has a component with a linear structure of type 1. More generally, we shall show that a component of a vectorial Boolean function can be replaced by a linear function only if the inverse of the said function has a component with a linear structure.
We start by showing that the existence of a linear structure of type 1 for the function f is necessary in the construction of π given in Theorem 2.

Theorem 3. *Let π be a permutation on $\mathbb{F}_2^n$ such that the component $\gamma \cdot \pi$ is the linear function $x \mapsto \gamma \cdot x$ for all γ in an $(n-1)$-dimensional subspace U of $\mathbb{F}_2^n$. Let $\alpha \notin U$. Then the unique nonzero vector in $U^\perp$ is a linear structure of type 1 of $\alpha \cdot \pi$.*

Proof. Let $w \in \mathbb{F}_2^n$ be the unique non-zero vector such that $w \cdot \gamma = 0$ for all $\gamma \in U$. Then $w \cdot \gamma = 1$ for all $\gamma \in \mathbb{F}_2^n \setminus U$. Since π is a permutation, the functions

$$x \mapsto \alpha \cdot \pi(x) \oplus \gamma \cdot \pi(x) = \alpha \cdot \pi(x) \oplus \gamma \cdot x$$

are balanced for all $\gamma \in U$. Using the inverse Walsh transform we get

$$\begin{aligned}(-1)^{\alpha\cdot\pi(x)} &= 2^{-n} \sum_{\gamma \in \mathbb{F}_2^n} (-1)^{\gamma\cdot x} \sum_{z \in \mathbb{F}_2^n} (-1)^{\alpha\cdot\pi(z)\oplus\gamma\cdot z} \\ &= 2^{-n} \sum_{\gamma \in \mathbb{F}_2^n \setminus U} (-1)^{\gamma\cdot x} \sum_{z \in \mathbb{F}_2^n} (-1)^{\alpha\cdot\pi(z)\oplus\gamma\cdot z},\end{aligned}$$

for all $x \in \mathbb{F}_2^n$. By using this expression for $\pi(x \oplus w)$ we get

$$(-1)^{\alpha\cdot\pi(x\oplus w)} = (-1)^{\gamma\cdot\alpha}(-1)^{\alpha\cdot\pi(x)} = (-1)^{\alpha\cdot\pi(x)\oplus 1},$$

for all $x \in \mathbb{F}_2^n$. □

Corollary 1. *In the context of Theorem 1 a replacement of a component $\alpha \cdot F^{-1}$ by a linear function $x \mapsto \beta \cdot x$ is possible if and only if the component $\beta \cdot F$ has a linear structure w of type 1 such that $\alpha \cdot w = 1$.*

To state another consequence of this result, let us first recall the following property of Boolean functions with a linear structure of type 1, see e.g. [Car21].

Proposition 1. *A Boolean function on $\mathbb{F}_2^n$ has a linear structure of type 1 if and only if it is linearly equivalent to a function of the form*

$$x = (x_1, x_2, \ldots, x_n) \mapsto x_n \oplus g'(x_1, \ldots, x_{n-1}), \tag{3}$$

where g' is a Boolean function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$.

Corollary 2. *A vectorial Boolean function on $\mathbb{F}_2^n$ of the form*

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1}, f(x_1, \ldots, x_n))$$

is a permutation if and only it is an unbalanced $(n-1, 1)$ Feistel transformation as given by Equation (2).

5 Replacing a Component: General Case

More generally, we can ask whether two Boolean functions f and g, for which $R_f = (S, f)$ and $R_g = (S, g)$ are permutations, are somehow related. An answer is given by the following theorem.

Theorem 4. *Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ be a 2-to-1 function and f a Boolean function such that $R_f = (S, f)$ is a permutation. Then f can be replaced by another Boolean function g by preserving bijectivity if and only if the vector e_n is a linear structure of type 1 of the Boolean function $g \circ R_f^{-1}$.*

Proof. Assume first that g gives a permutation R_g. We observe that the first $n-1$ coordinate functions of R_f and R_g are equal and given by S. This holds also when composed with R_f^{-1}. This means that the first $n-1$ coordinate functions of $R_g \circ R_f^{-1}$ are given by

$$S\left(R_f^{-1}(y)\right) = (y_1, \ldots, y_{n-1}),$$

for all $y = (y_1, \ldots, y_{n-1}, y_n) \in \mathbb{F}_2^n$. This means that only the last coordinate functions of the functions $R_g \circ R_g^{-1}$ and $R_g \circ R_f^{-1}$ are different. In the first case it is the linear function $y \mapsto y_n$ and in the second case the function $y \mapsto g\left(R_f^{-1}(y)\right)$. By Theorem 3 we get that $w = e_n$ is a linear structure of $g(R_f^{-1})$.

Assume now that e_n is a linear structure of $g \circ R_f^{-1}$ of type 1. Then we can define a permutation π as in Theorem 2 by choosing $\alpha = e_n$ and setting

$$\pi(y) = \left(y_1, \dots, y_{n-1}, g\left(R_f^{-1}(y)\right)\right).$$

Then $R_g = \pi \circ R_f$ is a permutation. □

Since π is a Feistel transformation, we get the following corollary, from where it follows that any modification of one component of a vectorial Boolean function is essentially done by first using a bijective linear transformation to place the component to be the rightmost coordinate function and then applying an unbalanced Feistel transformation.

Corollary 3. *Let $F = (f_1, \dots, f_n)$ be a permutation on $\mathbb{F}_2^n$. Then $F' = (f_1, \dots, f_{n-1}, g)$ is a permutation if and only if there is a Boolean function g' on $\mathbb{F}_2^{n-1}$ such that*

$$g(x) = f_n(x) \oplus g'\left(f_1(x), \dots, f_{n-1}(x)\right)$$

for all $x \in \mathbb{F}_2^n$.

Proof. We apply Theorem 4 by choosing $R_f = F$. Then the vector e_n is a linear structure of $g \circ F^{-1}$ if and only if there is a Boolean function g' on $\mathbb{F}_2^{n-1}$ such that

$$\left(g \circ F^{-1}\right)(y) = y_n \oplus g'(y_1, \dots y_{n-1}).$$

This equality holds for all $y = (y_1, \dots, y_n) \in \mathbb{F}_2^n$, if and only if it holds for all $x \in \mathbb{F}_2^n$ such that $y = F(x) = (f_1(x), \dots, f_n(x))$. □

We also see that the number of replacements of a component preserving bijectivity is the square root of the total of 2^{2^n} different Boolean functions on $\mathbb{F}_2^n$.

6 Conclusions

We have studied the previously suggested method for replacing a component of a permutation on $\mathbb{F}_2^n$ with a linear one under the assumption that the inverse of the permutation has a linear structure of type 1. We have proved that the existence of the linear structure is necessary for such a modification. More generally, a component f of a permutation F can be replaced by a function g by preserving bijectivity if and only if $g \circ F^{-1}$ has a linear structure of type 1. In concrete terms, this means that a modification of a rightmost component of a permutation will result in a permutation if and only if the modification is done by applying an unbalanced $(n-1, 1)$ Feistel transformation to the permutation.

We hope that this new characterisation may be used to facilitate search of modifications of bijective S-boxes with desired cryptographic criteria.

Acknowledgements

The author thanks Christof Beierle for posing the question about the necessity of the existence of a linear structure for linear replacement of a component.

References

[BL20] Christof Beierle and Gregor Leander. 4-uniform permutations with null nonlinearity. *Cryptogr. Commun.*, 12(6):1133–1141, 2020.

[Car21] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press, 2021.

[MS89] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer, 1989.

[Nyb22] Kaisa Nyberg. Modification of bijective S-boxes with linear structures. Cryptology ePrint Archive, Report 2022/1550, 2022. http://eprint.iacr.org/2022/1550.