4-Uniform Permutations with Null Nonlinearity

Christof Beierle, Gregor Leander

Horst Görtz Institute for IT Security, Ruhr University Bochum, Bochum, Germany
firstname.lastname@rub.de

Abstract

We consider n-bit permutations with differential uniformity of 4 and null nonlinearity. We first show that the inverses of Gold functions have the interesting property that one component can be replaced by a linear function such that it still remains a permutation. This directly yields a construction of 4-uniform permutations with trivial nonlinearity in odd dimension. We further show their existence for all $n = 3$ and $n \geq 5$ based on a construction in [1]. In this context, we also show that 4-uniform 2-1 functions obtained from *admissible sequences*, as defined by Idrisova in [8], exist in every dimension $n = 3$ and $n \geq 5$. Such functions fulfill some necessary properties for being subfunctions of APN permutations. Finally, we use the 4-uniform permutations with null nonlinearity to construct some 4-uniform 2-1 functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ which are not obtained from admissible sequences. This disproves a conjecture raised by Idrisova.

Keywords: Boolean function, Cryptographic S-boxes, APN permutations, Gold functions

1 Introduction

It is well known that an APN function, i.e., a differentially 2-uniform function, must have non-trivial nonlinearity (see, e.g., [3, Prop. 13]). For functions with slightly worse differential properties, this does not necessarily need to hold. In particular, there exist differentially 4-uniform permutations with trivial nonlinearity of 0. Although this is not a new result of ours, we think that it is worth highlighting and studying such functions in more detail. For example, one possible application would be to construct other 4-uniform permutations, but with higher nonlinearity. In particular, one can reduce any permutation with trivial nonlinearity to a 2-1 function of the same uniformity and extend it back to a permutation in many possible ways.

Having a function with differential uniformity d, replacing one component by a linear function trivially yields a function with differential uniformity at most $2d$ and null nonlinearity. However, the crucial part is that the function constructed in that way *is*

This is a preprint of an article published in Cryptography and Communications. The final authenticated version is available online via https://doi.org/10.1007/s12095-020-00434-2.

again a permutation. We were therefore interested in the following question: *Can we find APN permutations for which one component can be replaced by a linear function such that it still remains a permutation?*

In the first part of this work, we show that the inverses of Gold functions (see [7, 9]), i.e., the inverses of power permutations $x \mapsto x^{2^i+1}$ in $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$, have such a property. Thus, they yield a construction of 4-uniform permutations with null nonlinearity. We remark that this observation directly leads to the construction of the APN function CCZ-equivalent to $x \mapsto x^{2^i+1}$ and EA-inequivalent to any power function constructed in [2]. Since the Gold functions are permutations only in odd dimension, we further observe that the differentially 4-uniform 2-1 function constructed in [1], which is defined in even and odd dimension (except for $n = 4$), can also be extended by a linear coordinate in order to obtain a 4-uniform permutation. By showing that such a 2-1 function exists for all $n = 3$ and $n \geq 5$, we therefore conclude that 4-uniform permutations with trivial nonlinearity exist for all $n = 3$ and $n \geq 5$.

In the second part of the paper we focus on 2-1 subfunctions of permutations, that are obtained by discarding one coordinate function. In [8], Idrisova has shown a necessary property on the subfunctions of APN permutations. In particular, for a subfunction $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ of an APN permutation, she showed that, for all non-zero $\alpha \in \mathbb{F}_2^n$, the following two conditions hold:

1. If $\{S(x), S(x+\alpha)\} = \{S(y), S(y+\alpha)\}$, then either $x = y$ or $x = y + \alpha$.
2. If $S(x) = S(x+\alpha)$ and $S(y) = S(y+\alpha)$, then either $x = y$ or $x = y + \alpha$.

We show that the above mentioned 4-uniform 2-1 function family constructed in [1], which is defined for $n = 3$ and $n \geq 5$, always fulfills this necessary property. Therefore, and interestingly, 4-uniform 2-1 functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{n-1}}$ fulfilling this property do not exist only for those n for which we know (at the time of writing) that no APN permutation exists. In her work, Idrisova conjectured that all 4-uniform 2-1 functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^{n-1}}$ fulfill this property. By using the 4-uniform permutations with null nonlinearity constructed in the first part, we provide counterexamples to that conjecture in the final part of the paper.

1.1 Notation and Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ denote the field with two elements and let $\mathbb{F}_{2^n}$ denote its extension field of dimension n. By Tr, we denote the *trace function* over $\mathbb{F}_{2^n}$ relative to $\mathbb{F}_2$, i.e., $\mathrm{Tr}\colon \mathbb{F}_{2^n} \mapsto \mathbb{F}_2, x \mapsto x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$. Note that the trace function is $\mathbb{F}_2$-linear.

A function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called *differentially d-uniform* if d is the smallest number such that, for every $a \in \mathbb{F}_{2^n} \setminus \{0\}$ and every $b \in \mathbb{F}_{2^m}$, the equation $F(x) + F(x+a) = b$ has at most d solutions for $x \in \mathbb{F}_{2^n}$. A differentially 2-uniform function is called *Almost Perfect Nonlinear (APN).* The *nonlinearity* of F, denoted $\mathrm{nl}(F)$, is defined as the minimum Hamming distance of any non-trivial component function to all affine Boolean functions.

There are several well-known equivalence relations on vectorial Boolean functions. The function $G\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called *affine equivalent* to F if there exist affine permutations $A\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $B\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that $F \circ A = B \circ G$. The function G is called *extended affine equivalent* (*EA-equivalent*) to F if there exist affine permutations $A\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $B\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and an affine function $C\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $F \circ A = B \circ (G + C)$. We finally recall the notion of CCZ-eqivalence. Let $\Gamma_F \coloneqq \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ be the *function graph* of F. The functions F and G are called *CCZ-equivalent* (see [4, 2]), if there exist an affine permutation $\mathcal{L}\colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ such that $\Gamma_G = \mathcal{L}(\Gamma_F)$. The differential uniformity and the nonlinearity are invariant under all of the above equivalence relations.

2 Some 4-Uniform Permutations

In this section, we give two example families of differentially 4-uniform permutations with trivial nonlinearity.

2.1 Inverses of Gold Functions: The Case of n Odd

An interesting construction can be obtained by the inverses of quadratic APN power permutations. For those, it is possible to replace a component function by a linear function and still obtain a permutation.

Proposition 1. *Let $n \geq 3$ be odd, let $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$, and let $d = (2^i + 1)^{-1} \bmod 2^n - 1$ with $\gcd(i, n) = 1$. Then, the mapping*

$$G_{\alpha,d}\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad x \mapsto x^d + \mathrm{Tr}(\alpha x^d + x)$$

is a differentially 4-uniform permutation with null nonlinearity. The inverse can be given as

$$G_{\alpha,d}^{-1}\colon x \mapsto x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}(\alpha x + x^{2^i+1}) \ .$$

Proof. To show that $G_{\alpha,d}$ is a permutation, we show that the mapping

$$G'_{\alpha,d}(x) \coloneqq G_{\alpha,d}(x^{2^i+1}) = x + \mathrm{Tr}(\alpha x + x^{2^i+1})$$

is an involution. Indeed, we can write $G'_{\alpha,d}(G'_{\alpha,d}(x))$ as

$$\begin{aligned} & x + \mathrm{Tr}(x^{2^i+1}) + \mathrm{Tr}(\alpha)\mathrm{Tr}(\alpha x + x^{2^i+1}) + \mathrm{Tr}\left(\left(x + \mathrm{Tr}(\alpha x + x^{2^i+1})\right)^{2^i+1}\right) \\ &= x + \mathrm{Tr}(x^{2^i+1}) + \mathrm{Tr}(\alpha)\mathrm{Tr}(\alpha x + x^{2^i+1}) + \mathrm{Tr}(x^{2^i+1}) + \mathrm{Tr}\left(\mathrm{Tr}(\alpha x + x^{2^i+1})\right) \\ &= x + \mathrm{Tr}(\alpha)\mathrm{Tr}(\alpha x + x^{2^i+1}) + \mathrm{Tr}(1)\mathrm{Tr}(\alpha x + x^{2^i+1}) = x \ , \end{aligned}$$

where the last equality follows from the fact that $\mathrm{Tr}(1) = \mathrm{Tr}(\alpha) = 1$ for odd n. The expression for the inverse of $G_{\alpha,d}$ follows because it can be given as $G_{\alpha,d}^{-1}(x) = G'_{\alpha,d}(x)^{2^i+1}$.

The 4-uniformity follows because $x \mapsto x^d$ is APN as the inverse of the APN permutation $x \mapsto x^{2^i+1}$ (see [9]). To see that $\mathrm{nl}(G_{\alpha,d}) = 0$, we observe that $\mathrm{Tr}(x) = \mathrm{Tr}(\alpha \cdot G_{\alpha,d}(x))$. □

Remark 1. *If we define $F_d(x) := x + \mathrm{Tr}(x^d + x)$, the function $H_d(x) := F_d(G_{1,d}^{-1}(x))$ is CCZ-equivalent to $x \mapsto x^d$ by construction via the involution*

$$\mathcal{L}\colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \quad (x,y) \mapsto (y + \mathrm{Tr}(y) + \mathrm{Tr}(x), x + \mathrm{Tr}(x) + \mathrm{Tr}(y))$$

operating on the function graph of $x \mapsto y = x^d$. By using the fact that $H_d(x) = F_d(G'_{1,d}(x)^{2^i+1})$, one can easily see that $H_d(x) = x^{2^i+1} + (x^{2^i} + x)\mathrm{Tr}(x + x^{2^i+1})$, which is equal to the function CCZ-equivalent to $x \mapsto x^{2^i+1}$ and EA- inequivalent to any power function, constructed in [2].

Remark 2. *The existence of differentially 4-uniform permutations with trivial nonlinearity is not a new result. In particular, it was shown in [6] that the mapping*

$$P_n\colon x \mapsto x + x^{2^{\frac{n+1}{2}}-1} + x^{2^n - 2^{\frac{n+1}{2}}+1}$$

is a permutation in $\mathbb{F}_{2^n}$ for odd $n \geq 3$. It was shown in [10] that this permutation is differentially 4-uniform. Although that, to the best of our knowledge, the null nonlinearity of P_n was not mentioned in previous work, it is trivial to observe. It simply holds because P_n is of the form $x \mapsto x + x^{d-1} + (x^{d-1})^d$ for $d = 2^{\frac{n+1}{2}}$ and thus, $\mathrm{Tr}(P_n(x)) = \mathrm{Tr}(x)$. Note that $2^{\frac{n+1}{2}-1}$ is the multiplicative inverse of $2^{\frac{n+1}{2}+1}$ modulo $2^n - 1$, so this construction is also related to Gold functions.

2.2 A Construction Covering the Case of n Even

In [1] Alsalami presented the following family of 4-uniform 2-1 functions, constructed by the finite field inversion.

Proposition 2 ([1])**.** *Let $n \geq 3$ and let $\gamma \in \mathbb{F}_{2^{n-1}}, \gamma \notin \{0,1\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 1$. The function*

$$S_\gamma\colon \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 \to \mathbb{F}_{2^{n-1}}, \quad (x, x_n) \mapsto \gamma^{x_n} x^{2^{n-1}-2}\ ,$$

is a differentially 4-uniform 2-1 function.

Note that such a function S_γ does not exist for $n = 4$, because there is no element $\gamma \in \mathbb{F}_{2^3} \setminus \{0,1\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1})$. More generally, Idrisova remarked in [8] that no 4-uniform 2-1 function from $\mathbb{F}_{2^4}$ to $\mathbb{F}_{2^3}$ exists. However, S_γ exists for all other dimensions $n = 3$ and $n \geq 5$ as shown in the following lemma.

Lemma 1. *For $m = 2$ and $m \geq 4$, there exist an element $\gamma \in \mathbb{F}_{2^m} \setminus \{0,1\}$ with* $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 1$.

Proof. We first consider the case of even m. Since no element in $\mathbb{F}_{2^m} \setminus \{0,1\}$ is self-inverse, $\mathbb{F}_{2^m} \setminus \{0,1\}$ can be partitioned into $2^{m-1}-1$ sets of the form $\{\gamma, \gamma^{-1}\}$. Since exactly half of the elements in $\mathbb{F}_{2^m}$ have trace 1 and since $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$, there are 2^{m-1} elements in $\mathbb{F}_{2^m} \setminus \{0,1\}$ with trace 1. From the pigeonhole principle, there is at least one such set $\{\gamma, \gamma^{-1}\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 1$.

Let now m be odd. Let us define the Boolean functions

$$\iota \colon \mathbb{F}_{2^m} \to \mathbb{F}_2, x \mapsto \mathrm{Tr}(x^{2^m-2}) \quad \kappa \colon \mathbb{F}_{2^m} \to \mathbb{F}_2, x \mapsto \begin{cases} x & \text{if } x \in \mathbb{F}_2 \\ \mathrm{Tr}(x)+1 & \text{if } x \notin \mathbb{F}_2 \end{cases}.$$

Suppose there do not exist $\gamma \in \mathbb{F}_{2^m} \setminus \{0,1\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1})$, then, $\forall \gamma \in \mathbb{F}_{2^m} \setminus \{0,1\}$, it is $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) + 1$ and therefore $\iota = \kappa$ because of the definitions of the above functions. However, it is $\mathrm{nl}(\kappa) \leq 2$, since κ has Hamming distance 2 from the affine function $x \mapsto \mathrm{Tr}(x) + 1$. Further, it is well known that $\mathrm{nl}(\iota) \geq 2^{m-1} - 2^{\frac{m}{2}} - 2$ (see [3, p. 50], [5]). This is a contradiction if $m \geq 5$ and thus, there exists $\gamma \in \mathbb{F}_{2^m} \setminus \{0,1\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1})$.

Suppose that $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 0$. Similarly as in the case of even m, we can partition $\mathbb{F}_{2^m} \setminus \{0,1,\gamma,\gamma^{-1}\}$ into $2^{m-1}-2$ sets of the form $\{\tilde{\gamma}, \tilde{\gamma}^{-1}\}$. Since exactly half of the elements in $\mathbb{F}_{2^m}$ have trace 1 and since $\mathrm{Tr}(0) \neq \mathrm{Tr}(1)$, there are $2^{m-1}-1$ elements in $\mathbb{F}_{2^m} \setminus \{0,1,\gamma,\gamma^{-1}\}$ with trace 1. From the pigeonhole principle, there is at least one such set $\{\tilde{\gamma}, \tilde{\gamma}^{-1}\}$ with $\mathrm{Tr}(\tilde{\gamma}) = \mathrm{Tr}(\tilde{\gamma}^{-1}) = 1$. □

The 2-1 functions S_γ as given in Proposition 2 can trivially be extended to permutation on $\mathbb{F}_{2^n}$. Let $f \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function with $|\mathrm{supp}(f)| = 2^{n-1}$ and $S_\gamma(\mathrm{supp}(f)) = \mathbb{F}_{2^{n-1}}$, the function

$$R_{\gamma,f} \colon \mathbb{F}_2^n \to \mathbb{F}_2^n, \quad x \mapsto (S_\gamma(x), f(x))$$

is a permutation on $\mathbb{F}_{2^n}$. By choosing $f(x) = x_n$, we obtain a 4-uniform permutation with a linear component, i.e., $\mathrm{nl}(R_{\gamma,f}) = 0$.

3 APN Admissible Functions

Let $S = (S_1, \ldots, S_n)$ be a vectorial Boolean function defined by its coordinates $S_i \colon \mathbb{F}_2^n \to \mathbb{F}_2$. For $j \in \{1, \ldots, n\}$, we define $S_{(j)} = (S_1, \ldots, S_{j-1}, S_{j+1}, \ldots, S_n)$ as the subfunction from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ of S obtained by omitting the j-th coordinate. In [8], necessary properties on the subfunctions of APN permutations were given in terms of so-called *admissible sequences*. We slightly reformulate this definition by directly considering the properties of functions and not sequences.

Definition 1 (see [8]). *A 4-uniform 2-1 function $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^{n-1}$ is called* APN admissible*, if, for all non-zero $\alpha \in \mathbb{F}_2^n$, the following two conditions hold:*

1. *If $\{S(x), S(x+\alpha)\} = \{S(y), S(y+\alpha)\}$, then either $x = y$ or $x = y + \alpha$.*

2. If $S(x) = S(x+\alpha)$ and $S(y) = S(y+\alpha)$, then either $x = y$ or $x = y+\alpha$.

The following fact for APN permutation was shown by Idrisova.

Proposition 3 (Prop. 5 of [8])**.** *Let S be a subfunction of an APN permutation, i.e., $S = T_{(j)}$ for an APN permutation $T\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then S is APN admissible.*

3.1 The Existence of APN Admissible Functions

If we have an APN permutation in n bit, one directly obtains an APN admissible function according to Proposition 3 by removing one coordinate. One can ask whether APN admissible functions exist in dimensions for which we don't know APN permutations. For $n = 4$, APN admissible functions do not exist. In the following, we show that APN admissible functions exist for all $n = 3$ and $n \geq 5$ by showing that S_γ is APN admissible.

Proposition 4. *The function S_γ for $\gamma \in \mathbb{F}_{2^{n-1}} \setminus \{0,1\}$ with $\mathrm{Tr}(\gamma) = \mathrm{Tr}(\gamma^{-1}) = 1$ is APN admissible.*

Proof. Since S_γ is 2-1 and 4-uniform, we only need to show that the two conditions of Definition 1 are met. We first show Condition 1. Let $x, y, \alpha \in \mathbb{F}_{2^{n-1}}$ and $x_n, y_n, \alpha_n \in \mathbb{F}_2$ with $(\alpha, \alpha_n) \neq (0,0)$ such that

$$\{S_\gamma(x,x_n), S_\gamma(x+\alpha, x_n+\alpha_n)\} = \{S_\gamma(y,y_n), S_\gamma(y+\alpha, y_n+\alpha_n)\}\ . \tag{1}$$

If $x = 0$, then $S_\gamma(x,x_n) = 0$. Since the only preimages of 0 are $(0,0)$ and $(0,1)$, Equation 1 implies $y = 0$ or $y+\alpha = 0$. It can easily be derived that $(y,y_n) = (0,x_n)$ or $(y,y_n) = (\alpha, x_n+\alpha_n)$ from the fact that $S_\gamma(z,z_n) = S_\gamma(z,z_n+1)$ only holds if $z = 0$. Thus, Condition 1 is met for $x = 0$. A similar argument holds for $y = 0, x+\alpha = 0$, and $y+\alpha = 0$. Let us therefore assume that $x \notin \{0,\alpha\}$ and $y \notin \{0,\alpha\}$. Equation 1 is equivalent to

$$\begin{aligned} &\{x(x+\alpha)y(y+\alpha)S_\gamma(x,x_n), x(x+\alpha)y(y+\alpha)S_\gamma(x+\alpha,x_n+\alpha_n)\} \\ = &\{x(x+\alpha)y(y+\alpha)S_\gamma(y,y_n), x(x+\alpha)y(y+\alpha)S_\gamma(y+\alpha,y_n+\alpha_n)\}\ , \end{aligned}$$

which simplifies to

$$\{\gamma^{x_n}(x+\alpha)y(y+\alpha), \gamma^{x_n \oplus \alpha_n}xy(y+\alpha)\} = \{\gamma^{y_n}x(x+\alpha)(y+\alpha), \gamma^{y_n \oplus \alpha_n}x(x+\alpha)y\}\ .$$

This holds if either

$$\gamma^{x_n}y = \gamma^{y_n}x \quad \text{and} \quad \gamma^{x_n \oplus \alpha_n}(y+\alpha) = \gamma^{y_n \oplus \alpha_n}(x+\alpha)\ ,$$

or

$$\gamma^{x_n}(y+\alpha) = \gamma^{y_n \oplus \alpha_n}x \quad \text{and} \quad \gamma^{x_n \oplus \alpha_n}y = \gamma^{y_n}(x+\alpha)\ .$$

In both of the above cases, by distinguishing all eight cases of (α_n, x_n, y_n), one can derive that either $(x,x_n) = (y,y_n)$ or $(x,x_n) = (y+\alpha, y_n+\alpha_n)$.

To show Condition 2, let $x, y, \alpha \in \mathbb{F}_{2^{n-1}}$ and $x_n, y_n, \alpha_n \in \mathbb{F}_2$ with $(\alpha, \alpha_n) \neq (0,0)$ such that

$$S_\gamma(x, x_n) = S_\gamma(x+\alpha, x_n+\alpha_n) \quad \text{and} \quad S_\gamma(y, y_n) = S_\gamma(y+\alpha, y_n+\alpha_n) \; . \tag{2}$$

Condition 2 is trivially met when $x \in \{0, \alpha\}$ or $y \in \{0, \alpha\}$. Let therefore, again, $x, y \notin \{0, \alpha\}$. Equation 2 is equivalent to

$$\gamma^{x_n}(x+\alpha) = \gamma^{x_n \oplus \alpha_n} x \quad \text{and} \quad \gamma^{y_n}(y+\alpha) = \gamma^{y_n \oplus \alpha_n} y \; .$$

For $\alpha_n = 0$, it follows that $\alpha = 0$, which is a contratiction to $(\alpha, \alpha_n) \neq (0,0)$. For $\alpha_n = 1$, one can easily derive that $(x, x_n) = (y, y_n)$ or $(x, x_n) = (y+\alpha, y_n+\alpha_n)$ by checking all four cases for (x_n, y_n). □

3.2 Idrisova's Conjecture

Idrisova conjectured that every 4-uniform 2-1 function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ is APN admissible [8, Conjecture 2]. That conjecture was experimentally verified for the case $n \leq 4$. We now use the 4-uniform permutations with null nonlinearity defined above to construct counterexamples to that conjecture. The constructions are based on the following observation.

By e_i we denote the i-th unit vector in $\mathbb{F}_2^n$, i.e., $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 is set at position i.

Proposition 5. *Let S be an n-bit permutation with a linear or affine component $\langle \gamma, S \rangle$, $\gamma \in \mathbb{F}_2^n$. Then, for $j \in \{1, \ldots, n\}$, if the vectors*

$$e_1, e_2, \ldots, e_{j-1}, e_{j+1}, e_{j+2}, \ldots, e_n, \gamma$$

are linearly independent, the subfunction $S_{(j)}$ is 2-1 and the differential uniformity of $S_{(j)}$ is equal to the differential uniformity of S.

Proof. W.l.o.g., let $j = n$. It is obvious that $S_{(n)}$ is 2-1. Let $T := \sum_{i=1}^n \gamma_i S_i$, which is linear or affine, i.e., there exists an $\epsilon \in \{0,1\}$ such that, for all $x, y \in \mathbb{F}_2^n$, $T(x) + T(y) = T(x+y) + \epsilon$. Now, let $x, \alpha \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2^{n-1}$ be such that

$$\begin{aligned} &S_{(n)}(x) + S_{(n)}(x+\alpha) \\ &= (S_1(x), \ldots, S_{n-1}(x)) + (S_1(x+\alpha), \ldots, S_{n-1}(x+\alpha)) = \beta \; . \end{aligned}$$

This holds if and only if

$$\begin{aligned} &(S_1(x), \ldots, S_{n-1}(x), T(x)) + (S_1(x+\alpha), \ldots, S_{n-1}(x+\alpha), T(x+\alpha)) \\ &= (\beta, T(\alpha) + \epsilon) \; . \end{aligned}$$

If $e_1, \ldots, e_{n-1}, \gamma$ are linearly independent, the function $(S_1, \ldots, S_{n-1}, T)$ is linear equivalent to S. It follows that the uniformity of $S_{(n)}$ must be equal to the uniformity of S. □

Example 1. *Let $n = 5$ and consider the function $G_{1,3} \colon \mathbb{F}_{2^5} \mapsto \mathbb{F}_{2^5}$. By representing $\mathbb{F}_{2^5}$ as $\mathbb{F}_2[X]/_{(X^5+X^2+1)}$, a representation of $G_{1,3}$ can be given by the look-up table*

$$\begin{aligned} G = [&\mathit{00, 01, 19, 0A, 06, 0E, 0B, 1C, 03, 0D, 05, 1B, 13, 1D, 11, 02,}\\ &\mathit{14, 1E, 10, 1A, 0F, 17, 12, 07, 15, 09, 08, 16, 18, 1F, 0C, 04}]\ . \end{aligned}$$

In this example, $\langle (0,1,0,0,1), G\rangle$ is linear, therefore

$$\begin{aligned} G_{(2)} = [&\mathit{0, 1, 9, 2, 6, 6, 3, C, 3, 5, 5, B, B, D, 9, 2,}\\ &\mathit{C, E, 8, A, 7, F, A, 7, D, 1, 0, E, 8, F, 4, 4}] \end{aligned}$$

is a differentially 4-uniform 2-1 function according to Proposition 5. However, it is $\{G_{(2)}(\mathit{02}), G_{(2)}(\mathit{02} + \mathit{01})\} = \{G_{(2)}(\mathit{0E}), G_{(2)}(\mathit{0E} + \mathit{01})\} = \{\mathit{02}, \mathit{09}\}$, so it is not APN admissible. This is a counterexample to Conjecture 2 of [8].

Example 2. *Let $n = 6$ and let $\mathbb{F}_{2^5}$ be represented as $\mathbb{F}_2[X]/_{(X^5+X^2+1)}$. Let $\gamma = \alpha + 1 \in \mathbb{F}_{2^5}$, where α is a root of $X^5 + X^2 + 1$. By choosing $f(x) = x_n$, the function $R_{\gamma,f}$ has a linear component by construction. It is linear equivalent to*

$$\begin{aligned} R = [&\mathit{00, 23, 13, 3C, 3B, 17, 2E, 34, 1F, 24, 39, 15, 27, 31, 2A, 2D,}\\ &\mathit{3D, 18, 22, 02, 1E, 0B, 38, 05, 11, 3E, 1A, 3F, 25, 33, 14, 08,}\\ &\mathit{20, 21, 12, 01, 09, 1C, 32, 0C, 36, 2C, 0E, 30, 29, 0F, 06, 37,}\\ &\mathit{2B, 0D, 26, 1D, 07, 3A, 28, 2F, 16, 0A, 35, 04, 03, 10, 19, 1B}]\ , \end{aligned}$$

which has the linear component $\langle (1,1,1,1,1,1), R\rangle$. Considering the linear equivalent permutation R allows us to remove an arbitrary *coordinate function in order to obtain a 4-uniform 2-1 function by Proposition 5. In particular,*

$$\begin{aligned} R_{(6)} = [&\mathit{00, 11, 09, 1E, 1D, 0B, 17, 1A, 0F, 12, 1C, 0A, 13, 18, 15, 16,}\\ &\mathit{1E, 0C, 11, 01, 0F, 05, 1C, 02, 08, 1F, 0D, 1F, 12, 19, 0A, 04,}\\ &\mathit{10, 10, 09, 00, 04, 0E, 19, 06, 1B, 16, 07, 18, 14, 07, 03, 1B,}\\ &\mathit{15, 06, 13, 0E, 03, 1D, 14, 17, 0B, 05, 1A, 02, 01, 08, 0C, 0D}] \end{aligned}$$

is differentially 4-uniform and 2-1, but

$$\{R_{(6)}(\mathit{01}), R_{(6)}(\mathit{01} + \mathit{02})\} = \{R_{(6)}(\mathit{10}), R_{(6)}(\mathit{10} + \mathit{02})\} = \{\mathit{11}, \mathit{1E}\}\ ,$$

so it is not APN admissible. This is another counterexample to the Conjecture.

We expect that similar counterexamples can be constructed for all $n \geq 5$.

4 Conclusion

We have seen that 4-uniform permutations with null nonlinearity exist for all $n = 3$ and $n \geq 5$, where an interesting construction can be given by the inverses of Gold functions.

Moreover, 4-uniform 2-1 functions obtained from *admissible sequences*, as defined by Idrisova, exist for all $n = 3$ and $n \geq 5$. It is interesting to observe that $n = 4$ defines a special case for which none of the above exist.

For future work it would be interesting to find more constructions of 4-uniform permutations with null nonlinearity and use them to construct 4-uniform permutations (or even APN permutations) with high nonlinearity. Such a construction can be achieved by the following procedure: Let F be a 4-uniform permutation in n bit with trivial nonlinearity.

1. Choose a permutation G affine equivalent to F.
2. Discard a coordinate of G to obtain a 4-uniform 2-1 function G' from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ by Proposition 5.
3. Choose an n-bit Boolean function f with $|\mathrm{supp}(f)| = 2^{n-1}$ for which $G'(\mathrm{supp}(f)) = \mathbb{F}_2^{n-1}$ and construct the permutation $H\colon x \mapsto (G'(x), f(x))$.

Note that Step 2 and 3 of the above procedure were already suggested in [8]. However, starting from a 4-uniform permutation with trivial nonlinearity allows more freedom to obtain a 4-uniform 2-1 function. For $n \in \{6, 7, 8\}$ we checked all the constructions of Proposition 2 whether they can be extended to an APN permutation by Step 3 of the above algorithm. The answer is negative in all cases. We used an exhaustive tree search for constructing the last coordinate function.

Acknowledgements

This work was funded by *Deutsche Forschungsgemeinschaft (DFG)*; project number 411879806, and by DFG under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] Y. Alsalami. Constructions with high algebraic degree of differentially 4-uniform (n, n - 1)-functions and differentially 8-uniform (n, n - 2)-functions. *Cryptography and Communications*, 10(4):611–628, 2018.

[2] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Trans. Information Theory*, 52(3):1141–1152, 2006.

[3] C. Carlet. Vectorial boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[4] C. Carlet, P. Charpin, and V. A. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[5] L. Carlitz and S. Uchiyama. Bounds for exponential sums. *Duke mathematical journal*, 24(1):37–41, 1957.

[6] C. Ding, L. Qu, Q. Wang, J. Yuan, and P. Yuan. Permutation trinomials over finite fields with even characteristic. *SIAM Journal on Discrete Mathematics*, 29(1):79–92, 2015.

[7] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE transactions on Information Theory*, 14(1):154–156, 1968.

[8] V. Idrisova. On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". *Cryptography and Communications*, 11(1):21–39, 2019.

[9] K. Nyberg. Differentially uniform mappings for cryptography. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[10] X. Zhu, X. Zeng, and Y. Chen. Some binomial and trinomial differentially 4-uniform permutation polynomials. *International Journal of Foundations of Computer Science*, 26(4):487–497, 2015.