Mediterr. J. Math. (2022) 19:94
https://doi.org/10.1007/s00009-022-01980-0

Mediterranean Journal of Mathematics

Constructing Functions with Low Differential Uniformity

Emily Bergman and Robert S. Coulter

Abstract. The lower the differential uniformity of a function, the more resilient it is to differential cryptanalysis if used in a substitution box. APN functions and planar functions are specifically those functions which have optimal differential uniformity in even and odd characteristic, respectively. In this article, we provide two methods for constructing functions with low, but not necessarily optimal, differential uniformity. Our first method involves altering the coordinate functions of any known planar function and relies upon the relation between planar functions and orthogonal systems identified by Coulter and Matthews in 1997. As planar functions exist only over fields of odd order, the method works for odd characteristic only. The approach also leads us to a generalization of Dillon's Switching Technique for constructing APN functions. Our second construction method is motivated by a result of Coulter and Henderson, who showed in 2008 how commutative presemifields of odd order were in one-to-one correspondence with planar Dembowski–Ostrom polynomials via the multiplication of the presemifield. Using this connection as a starting point, we examine the functions arising from the multiplication of other well-structured algebraic objects such as non-commutative presemifields and planar nearfields. In particular, we construct a number of infinite classes of functions which have low, though not optimal, differential uniformity. This class of functions originally stems from the presemifields of Kantor and Williams of characteristic 2. Thus, regardless of the characteristic, between our two methods we are able to construct infinitely many functions which have low, though not optimal, differential uniformity over fields of arbitrarily large order.

Mathematics Subject Classification. 11T71, 11T06, 12K10, 12K05.

Keywords. Differential uniformity, differential cryptanalysis, semifields, planar nearfields.

Published online: 19 March 2022

Birkhäuser

1. Motivation and Outline

Throughout this work, we let p be a prime, n be a natural number, and $q = p^n$. The finite field with q elements will be denoted as $\mathbb{F}_q$ and $\mathbb{F}_q^n$ denotes the n dimensional vector space over $\mathbb{F}_q$. In general, if we have a set $\mathcal{S}$ with a binary operation and an identity element e corresponding to the binary relation, we will denote the set $S\backslash\{e\}$ as $\mathcal{S}^\star$. For example, the set of non-zero elements of $\mathbb{F}_q$ is $\mathbb{F}_q^\star$. Since the multiplicative group of a finite field is cyclic, it can be generated by a primitive element $\mathfrak{z}$, so that $\mathbb{F}_q^\star = \langle \mathfrak{z} \rangle$.

Let $\mathbb{F}_q[X]$ denote the polynomial ring over $\mathbb{F}_q$ in indeterminate X. Any function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ can be represented by infinitely many polynomials in $\mathbb{F}_q[X]$, and represented uniquely by a polynomial of degree less than q which we call the *reduced form*. While this paper is concerned with a property of functions, we will at times find it more useful to refer to a polynomial form of the function, and shall use the terms function and polynomial somewhat interchangeably to suit our discussion. We use $\mathrm{Im}(f)$ to denote the image set of the function f; that is, $\mathrm{Im}(f) = \{f(a) : a \in \mathbb{F}_q\}$. The *differential operator* of a function f is defined to be the function given by $\Delta_f(x, a) = f(x + a) - f(x) - f(a)$.

In this article, the central property of functions we shall be interested in is *differential uniformity*.

Definition 1. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is said to be *differentially δ-uniform (δ-DU)* if for all non-zero $a \in \mathbb{F}_{p^n}$ and for all $b \in \mathbb{F}_{p^m}$ $\Delta_f(x, a) = b$ has at most δ solutions in x.

Note that differential uniformity is invariant under the addition of an affine transformation or under composition with non-singular affine transformations. This leads naturally to the concept of *affine* equivalence (more commonly referred to as EA-equivalence in the literature).

Differential uniformity has practical applications in cryptography; the lower the differential uniformity of a function used in the design of an S-box, the more resistant that S-box is to differential cryptanalysis; see Nyberg and Knudsen [24] for example. Optimal examples exist in both odd and even characteristic, though the change of parity in the characteristic does alter the essential behavior of optimal differentially uniform functions. This is most easily described when $n = m$. For p odd, it is possible to construct functions which are 1-DU. These are more commonly known as planar functions, and were first introduced by Dembowski and Ostrom [13] in connection to the study of projective planes allowing collineation groups with certain specific, but natural, properties. For $p = 2$, it is impossible to construct functions which are 1-DU. This is because whenever $x \in \mathbb{F}_q$ satisfies $\Delta_f(x, a) = b$, we must also have $\Delta_f(x + a, a) = b$. Consequently, all solutions come in pairs, and optimal differential uniformity is thus 2 in characteristic 2. Such functions are known as *almost perfect non-linear (APN)*.

Most desirable of all would be bijective examples of either optimal scenario. For p odd, it can be shown that bijective examples do not exist. Indeed, Coulter and Senger [12] have given a non-trivial upper bound for $\#\mathrm{Im}(f)$ with

f planar: $\#\mathrm{Im}(f) \leq q - \frac{2(q-1)}{1+\sqrt{4q+3}}$. For $p = 2$, a major problem in the study of APN functions is the determination of bijective examples. The APN monomials X^{2^i+1}, with $\gcd(i, n) = 1$, provide examples of APN bijections over $\mathbb{F}_{2^n}$ for any odd n. For even n, only one example is known, the APN function over $\mathbb{F}_{2^6}$ of Browning, Dillon, McQuistan, and Wolfe from [4].

Almost all previous work in this area has concentrated on the construction or classification of optimal differentially uniform functions. Our aim in this paper is to construct functions with low, though not necessarily optimal, differential uniformity. Perhaps the most significant work in this direction can be found in the work of Helleseth and Sandberg [19], where many examples were found via computational means and infinite classes of low differentially uniform functions then established theoretically. We present two methods for constructing functions with low differential uniformity. We first show that a connection between orthogonal systems and planar functions first identified by Coulter and Matthews [10] leads naturally to a simple way of constructing functions with low differential uniformity relative to the field size. The method involves altering coordinate functions of a function when represented as a vectorial function. This approach also leads us to re-examine Dillon's Switching Technique and consequently generalize the technique. Our second, and perhaps more significant approach, is based on a 2008 result of Coulter and Henderson [9] that connects the largest known general class of planar functions with commutative presemifields of odd order, via the multiplication of the presemifield. Motivated by that connection, we look to use the multiplication of other well-structured algebraic objects to construct low differentially uniform functions. In this article, we first produce a class of low differentially uniform functions which include the function arising from the multiplication of the non-commutative presemifields of even order found by Kantor and Williams [21]. We also consider the differential uniformity of those functions arising from the multiplication of the planar nearfields. We find several infinite classes of functions with low differential uniformity, though these, too, are not bijective.

The paper is structured as follows. In the next section, we introduce coordinate functions and orthogonal systems and show how a result of [10] can be adapted to construct p-DU functions over fields of order p^n for odd p and arbitrarily large n. In Sect. 3, we recount the result of Coulter and Henderson that connects differential uniformity with commutative presemifields of odd order. This also allows us to explain our general approach. In Sect. 4, we introduce and generalize Dillon's switching technique, which is used for proving if certain functions are APN or not. In the subsequent sections, we proceed to examine the differential uniformity and bijectivity of functions arising from Kantor and Williams' characteristic 2 presemifields, and the regular and irregular planar nearfields, respectively, before ending with a summary.

2. Bases, Coordinate Functions, Orthogonal Systems and Implications

Given a fixed basis, $\{b_i\}_{i=1}^n$, for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ we can view $x \in \mathbb{F}_{q^n}$ as the element $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ where $x = x_1 b_1 + \ldots x_n b_n$. This is an isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$ (when viewed as vector spaces over $\mathbb{F}_q$); therefore, we may use these interchangeably depending on what is more useful.

This isomorphism can have an impact on the representation of functions also. Let $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. We can view f as a function in n variables, called F, where

$$F(x_1, \ldots, x_n) = f(x_1 b_1 + \ldots + x_n b_n).$$

We may also view f as a *vectorial function* $f = (f_1(x), \ldots, f_n(x))$, where each $f_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is defined as $f_i(x) = c_i$ where $f(x) = c_1 b_1 + \ldots + c_n b_n$. We call the f_i's *coordinate functions*. We can also view the coordinate functions as multivariate functions given as $(F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots x_n))$ with $F_i : \mathbb{F}_q^n \to \mathbb{F}_q$. We call the F_i's *multivariate coordinate functions*. The version of the function we use can depend on how we want to examine the function, with different representations lending themselves to different problems. For example, in [10], Coulter and Matthews showed a relationship between maximal orthogonal systems and planar functions through coordinate functions.

Definition 2. A system of functions $f_1, \ldots, f_m$ in n variables over $\mathbb{F}_q$ with $1 \leq m \leq n$ is *orthogonal* over $\mathbb{F}_q$ if the system

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= y_1 \\ f_2(x_1, \ldots, x_n) &= y_2 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= y_m \end{aligned}$$

has exactly q^{n-m} solutions in $\mathbb{F}_q^n$ for each $(y_1, \ldots, y_m) \in \mathbb{F}_q^m$. If $m = n$, then an orthogonal system is said to be maximal.

Orthogonal systems were introduced implicitly by Carlitz in [6,7], and again by Nöbauer in [23]. It was Carlitz who first showed that every orthogonal system can be extended to a maximal orthogonal system. The following result is a weaker form of Theorem 3.2 of [10].

Theorem 3. *Let $f \in \mathbb{F}_{q^n}[X]$ be planar, $\{b_1, \ldots, b_n\}$ a fixed basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $f_1, \ldots, f_n \in \mathbb{F}_{q^n}[X]$ be the corresponding coordinate functions for f as polynomials. Then, the system of polynomials $\{\Delta_{f_i}(X, a) : i = 1, \ldots, n\}$ forms a maximal orthogonal system in $\mathbb{F}_q$ for each non-zero $a \in \mathbb{F}_{q^n}$.*

This result gives an immediate way to construct functions for which we have some control on the differential uniformity.

Lemma 1. *Changing any k coordinate functions of a planar function $f(x)$ over $\mathbb{F}_{p^n}$ produces a function that is at most p^k-DU.*

Proof. Consider $f(x) = (f_1(x), \ldots, f_n(x))$ as a planar function over $\mathbb{F}_{p^n}$ in coordinate function form. Without loss of generality, suppose we replace the last k coordinate functions arbitrarily to produce the function

$$g(x) = (f_1(x), \ldots, f_{n-k}(x), g_{n-k+1}(x), \ldots, g_n(x)).$$

Then, the difference polynomial of g is

$$\Delta_g(x, a) = (\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a), \Delta_{g_{n-k+1}}(x, a), \ldots, \Delta_{g_n}(x, a)).$$

The set $\{\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a)\}$ still forms a mutually orthogonal system, but it is no longer maximal. This means that for $\alpha_1, \ldots \alpha_{n-k} \in \mathbb{F}_p$ there exists p^k solutions to

$$\Delta_{f_1}(x, s) = \alpha_1, \ldots, \Delta_{f_{n-k}}(x, a) = \alpha_{n-k}.$$

Therefore, when $(\alpha_1, \ldots \alpha_n) \in \mathbb{F}_{p^n}$, the maximum number of solutions to

$$(\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a), \Delta_{g_{n-k+1}}(x, a), \ldots, \Delta_{g_n}(x, a)) = (\alpha_1, \ldots, \alpha_n)$$

is p^k. Specifically the elements satisfying

$$(\Delta_{f_1}(x, a), \ldots, \Delta_{f_{n-k}}(x, a)) = (\alpha_1, \ldots, \alpha_{n-k})$$

all might also satisfy $\Delta_{g_{n-k+1}}(x, a) = \alpha_{n-k+1}, \ldots, \Delta_{g_n}(x, a) = \alpha_n$. Hence, the new function g is at most p^k-DU. □

One can push this further to produce functions which are precisely p-DU.

Corollary 1. *Let $f \in \mathbb{F}_{q^n}[X]$ be a planar polynomial, $\{b_1, \ldots, b_n\}$ a fixed basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $f_1, \ldots, f_n \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the corresponding multivariate coordinate functions for f as polynomials. Fix i, j with $1 \leq i, j, \leq n$ and let $F_j \in \mathbb{F}_q[X_1, \ldots, X_n]$ be the polynomial we obtain from removing all the terms involving X_i from the multivariate coordinate function f_j. Then, the function $F \in \mathbb{F}_{q^n}[X]$ defined by $F = (f_1, \ldots, f_{j-1}, F_j, f_{j+1}, \ldots f_n)$ is p-DU.*

Proof. From Lemma 1, we know that this new function is at most p-DU. Without loss of generality, suppose we remove all terms involving X_n from f_n. Then, when we consider $a = (0, \ldots, 0, 1)$, the difference polynomials of the coordinate polynomials f_i, with $1 \leq i \leq n-1$, are $f_i(X_1, \ldots, X_{n-1}, X_n + 1) - f_i(X_1, \ldots, X_n) - f_i(0, \ldots, 0, 1)$, and for f_n the difference polynomial is 0. We know by properties of orthogonal systems that for any $(\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_p^n$ there are p elements of $\mathbb{F}_p^n$ satisfying

$$\begin{aligned} f_1(x_1, \ldots, x_{n-1}, x_n + 1) - f_1(x_1, \ldots, x_n) &= b_1, \\ &\vdots \\ f_{n-1}(x_1, \ldots, x_{n-1}, x_n + 1) - f_{n-1}(x_1, \ldots x_n) &= b_{n-1}. \end{aligned}$$

Therefore, the new function is necessarily p-DU. □

3. Algebraic Structures and Differential Uniformity

A finite set $\mathcal{S}$ with a binary operation $*$ is a *quasigroup* if for every $a, b \in \mathcal{S}$ there exists unique $x, y \in \mathcal{S}$ such that $a * x = b$ and $y * a = b$.

Definition 4. A finite set $\mathcal{S}$ with two operations, $+$ (addition) and $*$ (multiplication), is called a *presemifield* if

- $(\mathcal{S}, +)$ is an abelian group with identity 0,
- $(\mathcal{S}^\star, *)$ is a quasigroup,
- there are no zero divisors, and
- both left and right distributive properties hold.

If a presemifield has a multiplicative identity, then we call it a *semifield*.

Since finite fields are semifields, we call a semifield which is not a finite field a *proper semifield*. Note that presemifields and semifields do not have to be associative nor commutative with respect to multiplication. It is an open, and seemingly extremely difficult, problem to classify finite semifields. This should be compared with finite fields, arguably the closest algebraic objects, the classification of which was completed in 1893 when E.H. Moore proved uniqueness in [22].

The additive structure of a presemifield is necessarily elementary abelian so presemifields can be viewed as $\mathcal{S} = (\mathbb{F}_q, +, *)$, where $(\mathbb{F}_q, +)$ is the additive group of $\mathbb{F}_q$ and $x * y = \phi(x, y)$ for some function $\phi : \mathbb{F}_q^2 \to \mathbb{F}_q$. Moreover, the polynomial representation of $\phi \in \mathbb{F}_q[X, Y]$ must satisfy

$$\phi(X, Y) = \sum_{ij} a_{ij} X^{p^i} Y^{p^j},$$

so that ϕ is additive in both variables (this follows from having both distributive laws). Any polynomial of the form

$$\sum_{ij} a_{ij} X^{p^i + p^j}$$

is called a *Dembowski–Ostrom (DO)* polynomial, so it is immediate from the above that $X * X = \phi(X, X)$ is a DO polynomial with additional properties when $*$ is a presemifield multiplication. This observation led to the following result, which is central to our approach to constructing functions with low differential uniformity.

Theorem 5. (Coulter and Henderson, [9], Theorem 3.3) *Let q be an odd prime power. If $f \in \mathbb{F}_q[X]$ is a planar DO polynomial, then $(\mathbb{F}_q, +, *)$ is a commutative presemifield, where $x * y = f(x + y) - f(x) - f(y)$. Conversely, if $(\mathbb{F}_q, +, *)$ is a commutative presemifield, then $f(X) = \frac{1}{2}(X * X)$ is a planar DO polynomial.*

The result shows that there is a strong connection between the multiplication of commutative presemifields of odd order and functions with optimal differential uniformity. We use this as a starting point for our search for other functions with low differential uniformity by considering functions $x \mapsto x * x$, where $*$ is the multiplication of other well-structured algebraic objects, such

as non-commutative presemifields in both odd and even characteristic, or planar nearfields. What we shall find is that if we use algebraic structures that do not fit the criteria of Theorem 5, then we can still obtain functions with very low differential uniformity relative to the field size.

The first step is to identify which algebraic objects we should use instead of commutative presemifields of odd order. In this article, we choose to use non-commutative presemifields of even order and a second class of structures known as the planar nearfields.

Definition 6. A finite set $\mathcal{S}$ with two operations, $+$ (addition) and $*$ (multiplication), is called a *planar nearfield* if

- $(\mathcal{S}, +)$ is an abelian group with identity 0,
- $(\mathcal{S}^\star, *)$ is a group, and
- one of the distributive properties hold.

As with presemifields, the additive structure of a planar nearfield is necessarily elementary abelian. Dickson [15,16] introduced the concept of a nearfield in 1905 and constructed two types of planar nearfields, now known as the regular and irregular nearfields. These were shown to be the only ones in 1935 by Zassenhaus [25]. We will describe the regular nearfields in Sect. 6, and the irregular planar nearfields in an Appendix.

4. The Extended Switching Technique

A function f that maps into $\mathbb{F}_2$ is called a *Boolean function*. Given an APN function F and $u \in \mathbb{F}_{2^n}^\star$, Edel and Pott [17] gave the following conditions on a Boolean function f so that $F(x) + uf(x)$ is APN. They called this the *Dillon Switching Technique*.

Theorem 7. (Edel and Pott, [17]) *Assume that $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an APN function. Let $u \in \mathbb{F}_{2^n}^\star$ and let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. Then, $F(x) + uf(x)$ is an APN function if and only if for all $x, y, a \in \mathbb{F}_{2^n}$ such that $F(x) + F(x + a) + F(y) + F(y + a) = u$, we also have*

$$f(x) + f(x + a) + f(y) + f(y + a) = 0.$$

This result of Edel and Pott stemmed from a more general switching technique they described in [17], though they only analyzed the Boolean function case.

It is worth considering further just what is happening in the alteration of F to $F+uf$ in the Dillon Switching Technique. Fix a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ that includes u, call it $\{u = b_1, b_2, \ldots, b_n\}$. Using this basis, we can represent the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ by the coordinate functions $(f_1, \ldots, f_n)$. Now, given any Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, the coordinate function representation of $F(X)+uf(X)$ is simply $(f_1+f, f_2, \ldots, f_n)$. Therefore, we can think of the Dillon Switching Technique as a condition on how to change one coordinate of an APN function and obtain an APN function. In these terms, there is a natural generalization of this theorem, which we will call the Extended Switching Technique.

Theorem 8. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function and $f : \mathbb{F}_{2^n} \to B$, where B is a k dimensional subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then, $F(X) + f(X)$ is an APN function if and only if for all $x, y, a \in \mathbb{F}_{2^n}$, with $a \neq 0$, such that $f(x) + f(x + a) + f(y) + f(y + a) = b \in B$, we also have*

$$F(x) + F(x + a) + F(y) + F(y + a) \neq b.$$

Proof. As was noted in the Introduction, if x is a solution to $\Delta_f(x, a) = b$ in characteristic 2, then $x + a$ is also a solution. If $F + f$ is not APN, then for some $z \in \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}^\star$ there are (at least) four solutions to $F(x) + F(x + a) + f(x) + f(x + a) = z$. Call our solutions $x, x + a, y, y + a$. We have the following system of equations:

$$F(x) + F(x + a) + f(x) + f(x + a) = z,$$
$$F(y) + F(y + a) + f(y) + f(y + a) = z.$$

Then, we have

$$F(x) + F(x + a) + F(y) + F(y + a) + f(x) + f(x + a) + f(y) + f(y + a)=0,$$

or equivalently,

$$F(x) + F(x + a) + F(y) + F(y + a) = f(x) + f(x + a) + f(y) + f(y + a).$$

These can only be equal when $F(x) + F(x + a) + F(y) + F(y + a) = b$ for some $b \in B$. Therefore, $F(x) + f(x)$ is APN if and only if for all x, y, a in $\mathbb{F}_{2^n}$ with $a \neq 0$ such that $f(x) + f(x + a) + f(y) + f(y + a) = b \in B$, $F(x) + F(x + a) + F(y) + F(y + a) \neq b$. □

Let $\{u_1, u_2, \ldots, u_k\}$ be a basis for B over $\mathbb{F}_2$ and extend this to a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $\{u_1 = b_1, \ldots, u_k = b_k, b_{k+1}, \ldots, b_n\}$. If we represent $F(x)$ and $f(x)$ in their coordinate function form with respect to this basis as $F(x) = (f_1(x), \ldots, f_n(x))$ and $f(x) = (g_1(x), \ldots g_k(x))$, then the coordinate function form of $F(x) + f(x)$ is

$$(f_1(x) + g_1(x), f_2(x) + g_2(x), \ldots, f_k(x) + g_k(x), f_{k+1}(x), \ldots, f_n(x)).$$

Thus, the Extended Switching Technique can be seen to be a generalization of the Dillon Switching Technique. Our result also extends a result of Budaghyan, Carlet and Leander [5] concerning APN DO polynomials. Indeed, one can prove the following extension of the result from [5].

Theorem 9. *Let $F \in \mathbb{F}_{2^n}[X]$ be an APN DO polynomial and $f \in \mathbb{F}_{2^n}[X]$ be a DO polynomial which, under evaluation, satisfies $f(\mathbb{F}_{2^n}) \subseteq B$, where B is a k dimensional subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. The polynomial $F + f$ is APN if for every $a \in \mathbb{F}_{2^n}^\star$ there exists a linear function $l_a : \mathbb{F}_{2^n} \to B$ satisfying*

(i) $\Delta_{f,a} = l_a(\Delta_{F,a})$, *and*
(ii) *if there exists $x \in \mathbb{F}_{2^n}$ such that $\Delta_{F,a}(x) = y \in B$ with $y \neq 0$, then $l_a(y) \neq y$.*

Proof. Since $F(x) + f(x)$ is a DO polynomial, its difference operator is necessarily a linear transformation (see Coulter and Matthews [11], Theorem 3.2). Consequently, we only need to determine the roots of $\Delta_{F+f}(x, a)$ for

all non-zero $a \in \mathbb{F}_{2^n}^\star$. If there are at most two solutions, then the function is APN. By (i), we have

$$\begin{aligned} 0 &= \Delta_{F+f}(x,a) \\ &= \Delta_F(x,a) + \Delta_f(x,a) \\ &= \Delta_F(x,a) + l_a(\Delta_F(x,a)). \end{aligned}$$

By (ii), this only occurs when $\Delta_F(x,a) = 0$. Since $F(x)$ is APN we know there are only 2 solutions, namely $x = 0$ and $x = a$. Hence, $F(x) + f(x)$ is APN. □

Though the results in this section concern APN functions, the techniques used to derive them can also be applied when considering functions without non-optimal differential uniformity, and it is in this way we shall apply them in the following sections.

5. Functions Motivated by the Presemifields of Kantor and Williams

We now move to consider the differential uniformity of functions coming from some other algebraic objects that do not quite meet the criteria of Theorem 5. To begin, we consider semifields and presemifields in characteristic 2. We shall be specifically interested in the semifields of Kantor and Williams [21], but before doing so, we make some observations.

Suppose q is a power of two and that we have a semifield of the form $\mathcal{S} = (\mathbb{F}_q, +, *)$ with multiplicative identity 1 (note: if there is a multiplicative identity in $\mathcal{S}$, then it can always be made to coincide with the 1 of $\mathbb{F}_q$; see Coulter [8]). Set $f(x) = x * x$ over $\mathbb{F}_q$. The difference function of f is $\Delta_f(x,a) = x * a + a * x$. If $a = 1$, then $\Delta_f(x,1) = 0$, so that f is q-DU. More generally, define $\mathcal{Z}(\mathcal{S}) = \{z \in \mathcal{S} : xz = zx \text{ for all } x \in \mathcal{S}\}$. For any element $a \in \mathcal{Z}(\mathcal{S})$, we have $\Delta_f(x,a) = 0$. In particular, this shows that using a commutative presemifield in characteristic 2 to construct a function $f(x) = x * x$ will always yield a function with the worst possible differential uniformity. For non-commutative semifields with unity 1, if we choose any $a \in \mathbb{F}_q \backslash \{0,1\}$, the number of solutions to $\Delta_f(x,a) = 0$ is bounded below by 4, because $\Delta_f(1,a) = 1 * a + a * 1 = a + a = 0$, and so $0, 1, a, a+1$ are all solutions. For the above reasons we choose to focus on non-commutative presemifields that are strictly not semifields.

Kantor and Williams gave the following presemifield construction in [21] which is particularly suitable for our needs. Consider the field $\mathbb{F}_{q^n}$ with q a power of 2 and n odd. Given a chain of fields

$$\mathbb{K} = \mathbb{F}_q \subseteq \mathbb{F}_1 \subsetneq \ldots \subsetneq \mathbb{F}_k \subsetneq \mathbb{F} = \mathbb{F}_{q^n},$$

with corresponding trace functions $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$, and a sequence of elements $a_1, \ldots a_k$ where $a_i \in \mathbb{F}^\star$, we define a multiplication by

$$x * y = xy^2 + \sum_{i=1}^{k} (\mathrm{Tr}_i(a_i x)y + a_i \,\mathrm{Tr}_i(xy)).$$

Then, $\mathcal{KW} = (\mathbb{F}_{q^n}, +, *)$ is a presemifield, see [21].

5.1. A Class of 4-DU Functions that Include Those from the Kantor–Williams Presemifields

We now wish to examine the differential uniformity of functions $x \mapsto x * x$, arising from the multiplication of $\mathcal{KW}$. We first deal with a minor case.

Lemma 2. *Consider the presemifield $\mathcal{KW} = (\mathbb{F}_{2^3}, +, *)$ defined with $\mathbb{F}_0 = \mathbb{F}_2$, $\mathbb{F}_1 = \mathbb{F}_{2^3}$, and $a_1 = 1$. The polynomial $f(X) = X * X$ is APN and linearly equivalent to X^5.*

Proof. We have

$$\begin{aligned} f(X) = X^3 + \mathrm{Tr}(X)X + \mathrm{Tr}(X) &= X^3 + X^2 + X^3 + X^5 + \mathrm{Tr}(X) \\ &= X^5 + X^2 + \mathrm{Tr}(X). \end{aligned}$$

Thus, $f(X)$ is affine equivalent to X^5, which is known to be APN. □

For the general Kantor–Williams presemifield, $\mathcal{KW}$, we have the polynomial $f(X) = X * X = X^3 + X\sum_{i=1}^{k} \mathrm{Tr}_i(a_i X) + a_i \mathrm{Tr}_k(X^2)$, which is affine equivalent to $g(X) = X^3 + X\sum_{i=1}^{k} \mathrm{Tr}_i(a_i X)$. We now prove the following result, which includes this entire class of polynomials as a subclass.

Theorem 10. *Fix $n > 3$ and integer i satisfying $\gcd(i, n) = 1$. Set*

$$f(X) = X^{2^i+1} + X\sum_j \mathrm{Tr}_j(a_j X),$$

where $a_j \in \mathbb{F}_{2^n}^\star$. Let k be the dimension of the image set of the linear operator $\sum_j \mathrm{Tr}_j(a_j X)$. Then, f is at most 2^{k+1}-DU. In particular, if $k = 1$, then f is 4-DU.

Proof. We have

$$\Delta_f(X, a) = X^{2^i}a + a^{2^i}X + a\sum_j \mathrm{Tr}(a_j X) + X\sum_j \mathrm{Tr}(a_j a).$$

This results in the system of equations

$$\sum_j \mathrm{Tr}_j(a_j x) = b$$

$$x^{2^i}a + a^{2^i}x + x\,\mathrm{Tr}(a_1 a) = ab.$$

From the second part of this system, we have the additive polynomial $X^{2^i}a + a^{2^i}X + X\,\mathrm{Tr}(a_1 a)$, which is a linear operator of the form $L(X) = aX^{2^i} + cX$ with $\gcd(i, n) = 1$. It is shown in Corollary 1 of Bracken et al. [2] that such polynomials have at most 2 zeros in $\mathbb{F}_q$. Consequently, there can be at most 2^{k+1} solutions to the system above, which establishes the claim. The case where $k = 1$ is clear. □

The authors gratefully acknowledge the anonymous referee, who provided this generalization of our original result. The following corollary, which covers all of the functions arising from the Kantor–Williams presemifields, is immediate.

Corollary 2. *Fix $n > 3$ odd. Consider the presemifield $\mathcal{KW} = (\mathbb{F}_{2^n}, +, *)$ defined by the chain of*

$$\mathbb{K} = \mathbb{F}_q \subseteq \mathbb{F}_1 \subsetneq \ldots \subsetneq \mathbb{F}_k \subsetneq \mathbb{F} = \mathbb{F}_{q^n}.$$

If $\mathbb{F}_k = \mathbb{F}_{2^m}$, then the polynomial $f(X) = X * X$ is at most 2^{m+1}-DU.

In particular, we can now easily obtain 4-DU functions.

Corollary 3. *Fix $n > 3$ odd. Consider the presemifield $\mathcal{KW} = (\mathbb{F}_{2^n}, +, *)$ defined by the chain of fields $\mathbb{F}_0 = \mathbb{F}_2$, $\mathbb{F}_1 = \mathbb{F}_{2^n}$, and $a_1 \in \mathbb{F}_{2^n}^\star$. Then, $f(X) = X * X$ is 4-DU.*

Proof. We need only show that f cannot be APN, since it follows immediately from the above corollary that f is at most 4-DU. As noted above f is affine equivalent to the DO polynomial $g(X) = X^3 + X\,\mathrm{Tr}(a_1 X) = XL(X)$, for some linear operator L. Since $a_1 \neq 0$, the linear operator has more than 1 term. Berger et al. showed that a polynomial like g cannot be APN; see [1], Proposition 7. This now forces g, and hence f, to be 4-DU. □

Theorem 10 means that we can create relatively low differentially uniform functions with respect to the field size using this approach. Fixing m, and setting $n = jm$ for some arbitrarily large integer j results in a function which is at most 2^{m+1}-DU, with with arbitrary choice of the elements $a_1, \ldots, a_k \in \mathbb{F}_{2^n}^\star$ in a field of order much larger than 2^{m+1}. It should be mentioned that the bound is not always tight. Computational results over $\mathbb{F}_{2^9}$ using the Kantor–Williams presemifield construction with the chain of fields $\mathbb{K} = \mathbb{F}_2 \subseteq \mathbb{F}_{2^3} \subseteq \mathbb{F}_{2^9} = \mathbb{F}$, yields 15,974 4-DU functions, 241,233 8-DU functions, and 4,014 16-DU functions.

5.2. The Non-bijectivity of Functions Coming from Kantor–Williams Presemifields

We will now prove that the 4-DU polynomials identified in Corollary 3 are not permutation polynomials. We shall need the following historical result.

Theorem 11. (Hermite, [20]; Dickson, [14]) *Let $q = p^n$. A polynomial $f \in \mathbb{F}_q[X]$ is a permutation polynomial over $\mathbb{F}_q$ if and only if*

(i) *f has exactly one root in $\mathbb{F}_q$, and*
(ii) *the reduction of f^t mod $(X^q - X)$, with $0 < t < q - 1$ and $t \not\equiv 0 \bmod p$, has degree less than $q - 1$.*

As was noted, the polynomials being considered were affine equivalent to $g(X) = X^3 + X\,\mathrm{Tr}(a_1 X)$. We will show that neither f nor g are permutation polynomials.

Theorem 12. *The polynomial $g(X) = X^3 + X\,\mathrm{Tr}(\alpha X)$, with $n > 3$ odd and $\alpha \in \mathbb{F}_{2^n}^\star$, is not a permutation polynomial.*

Proof. First, when $\mathrm{Tr}(\alpha) = 1$, we have $g(1) = 0 = g(0)$, so g is not a permutation if $\mathrm{Tr}(\alpha) = 1$.

For the remainder, assume $\mathrm{Tr}(\alpha) = 0$. We will use Hermite's criterion to prove g is not a permutation polynomial. Specifically, letting $t = 2 + \sum_{i=0}^{\frac{n-3}{2}} 2^{2i}$,

we will show that $g^t(X) \bmod X^q - X$ has degree $q-1$ with leading coefficient $\alpha^{2^{n-1}}$.

First, we note that the absolute trace in characteristic 2 has the property that $\mathrm{Tr}(x)^k = \mathrm{Tr}(x)$ for any integer k. We also note that $g^t(X)$ has the form

$$\begin{aligned} g^t(X) &= (X^{2+1} + X\,\mathrm{Tr}(\alpha X))^t \\ &\equiv (X^{2+1} + X\,\mathrm{Tr}(\alpha X))(X^{4+2} + X^2\,\mathrm{Tr}(\alpha X)) \\ &\quad \times \prod_{i=2}^{\frac{n-3}{2}} (X^{2^{2i-1}+2^{2i-2}} + X^{2^{2i-2}}\,\mathrm{Tr}(\alpha X)) \bmod X^q - X. \end{aligned}$$

Each term in the expanded form of $g^t(X)$ is constructed by choosing one of the two terms in each part of the product. We will let $A_0 = X^{2+1} + X\,\mathrm{Tr}(\alpha X)$, $A_1 = X^{4+2} + X^2\,\mathrm{Tr}(\alpha X)$, and $A_i = X^{2^{2i-1}+2^{2i-2}} + X^{2^{2i-2}}\,\mathrm{Tr}(\alpha X)$ for $i = 2, \ldots, \frac{n-3}{2}$.

We consider the coefficient of X^{q-1} in the reduced form of $g^t(X)$. Now, $q - 1 = 2^n - 1 = \sum_{i=0}^{n-1} 2^i$. The choices of terms from the A_i's are powers of two which will yield an exponent that is a sum of powers of two. This restricts our choices.

Before taking into account the terms involving the trace, the largest power of X you can choose to include in a particular term is $2^{n-2} + 2^{n-3}$ which is less than 2^{n-1}. Therefore, the 2^{n-1} power must be obtained from the trace. When we construct the terms for the expanded version of $g^t(X)$, the X^{2^n-1} term will be the result of a term that includes the absolute trace. We also notice that each term in the absolute trace will only add one power of two to the exponent. Therefore, we will only choose the term with the power 2^{n-1} from the trace.

The A_1 term will always add at least 2 to the exponent of a particular term. Since the A_1 and A_0 terms offer the only way to choose a term that adds a 2 to the exponent, if we choose 2 in both of them, then we will get a 4 instead, and so cannot construct the X^{2^n-1} term. This forces us to choose $X\,\mathrm{Tr}(\alpha X)$ from A_0. Similarly, we are also forced to choose $X^2\,\mathrm{Tr}(\alpha X)$ from A_1 as A_2 adds at least 4 to the power. Specifically, we must choose the $\alpha^{2^{n-2}} X^{2^{n-2}+1}$ term from A_0 and the $\alpha^{2^{n-2}} X^{2^{n-2}+2}$ term from A_1. When $i = 2, \ldots, \frac{n-3}{2}$ we are forced to choose $X^{2^{2i-1}+2^{2i-2}}$, as otherwise we will miss an odd power of two for our exponent. Therefore, the coefficient of the X^{2^n-1} term in this polynomial is $\alpha^{2^{n-2}} \times \alpha^{2^{n-2}} = \alpha^{2^{n-1}}$, which is clearly not zero; hence, $g(x)$ is not a permutation. □

We note that the function of Theorem 12 is not a permutation when n is even either, unless $n = 2$ and $\alpha = 1$. It is easily checked that when $n = 2$, $g(x)$ is a permutation only when $\alpha = 1$, when $g(x) = x^2$. Now, suppose $n > 2$ is even, so that 3 divides $q - 1$. Let $\{1, \zeta, \zeta^{-1}\}$ be the three roots of unity in $\mathbb{F}_q$. We now define the sets U and V by

$$\begin{aligned} U &= \{x \in \mathbb{F}_q : \mathrm{Tr}(\alpha x) = 0\}, \\ V &= \{x \in \mathbb{F}_q : \mathrm{Tr}(\alpha \zeta x) = 0\}. \end{aligned}$$

Now, U and V are both $n-1$ dimensional subspaces of $\mathbb{F}_q$, viewed as a vector space over $\mathbb{F}_2$. Consequently, using the classical dimension of the intersection of subspaces identity, we see that U and V must have non-trivial intersection as $n > 2$. Let u be any non-zero element of $U \cap V$. Then, $\mathrm{Tr}(\alpha u) = \mathrm{Tr}(\alpha\zeta u) = 0$ and $g(u) = g(\zeta u) = u^3$. Hence, g is not a permutation.

Now, we shall show that the original polynomial of Corollary 3 is not a permutation polynomial.

Theorem 13. *The polynomial* $f(X) = X^3 + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X)$ *over* $\mathbb{F}_{2^n}$, *with* $n > 3$ *odd and* $\alpha \in \mathbb{F}_{2^n}^\star$, *is not a permutation polynomial over* $\mathbb{F}_{2^n}$.

Proof. We will again use Hermite's criterion, but here we must split the proof into two cases: $\alpha = 1$ and $\alpha \neq 1$.

Case 1: Let $\alpha \neq 1$ and $t = 1 + 4 + \sum_{i=0}^{\frac{n-5}{2}} 2^{2i+1}$. Then, $f^t(X) \bmod X^q - X$ is

$$(X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))(X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^4 \times \prod_{i=0}^{\frac{n-5}{2}} (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^{2^{2i+1}}.$$

Let $A_0 = (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))$, $A_1 = (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^4$ and

$$\begin{aligned} A_i &= (X^{2+1} + X\,\mathrm{Tr}(\alpha X) + \alpha\,\mathrm{Tr}(X))^{2^{2(i-2)+1}} \\ &= (X^{2^{2(i-1)}+2^{2(i-2)+1}} + X^{2^{2(i-2)+1}}\,\mathrm{Tr}(\alpha X) + \alpha^{2^{2(i-2)+1}}\,\mathrm{Tr}(X)), \end{aligned}$$

for $i = 2 \cdots \frac{n-1}{2}$. We want to determine the coefficient of the X^{2^n-1} term.

Before we consider the terms involving the trace, the largest power of X that we can choose from any part of the product is $X^{2^{2(n-5/2+1)}} = X^{2^{n-3}}$. Therefore, we will be forced to choose $X^{2^{n-2}}$ and $X^{2^{n-1}}$ from $\mathrm{Tr}(\alpha X)$ and $\mathrm{Tr}(X)$. To get terms of the form $X^{2^{2k}}$ for $k \geq 2$, we need to choose the term $X^{2^{2k}+2^{2(k-1)+1}}$ from A_{k+1}.

Consequently, we have to make choices for A_0, A_1, and A_2 to get the X^{2^n-1} term. We are forced to choose either X^{2+1} or $X\,\mathrm{Tr}(\alpha X)$ from A_0 to get the 1 in the representation of $2^n - 1$ as a sum of powers of 2. From A_1 we are forced to choose $X^4\,\mathrm{Tr}(\alpha X)$ or $\alpha^4\,\mathrm{Tr}(X)$ to avoid getting $2(8)$ in the sum of powers of 2. The choice of A_2 is completely determined by the choices we make in A_0 and A_1.

Subcase 1: Suppose we choose the terms X^{2+1} and $X^4\,\mathrm{Tr}(\alpha x)$. Then, we will choose $\alpha^2\,\mathrm{Tr}(X)$ from A_2. Then, the coefficient of X^{2^n-1} is

$$\alpha^{2^{n-1}}\alpha^2 + \alpha^{2^{n-2}}\alpha^2 = \alpha^{2^{n-2}}\alpha^2(1+\alpha^2).$$

Subcase 2: Suppose we choose $X\,\mathrm{Tr}(\alpha X)$ and $\alpha^4\,\mathrm{Tr}(X)$ then we will choose X^{4+2} from A_2. Therefore, the coefficient of X^{2^n-1} is $\alpha^{2^{n-1}}\alpha^4 + \alpha^{2^{n-2}}\alpha^4 = \alpha^4\alpha^{2^{n-2}}(1+\alpha^2)$.

Overall, then, the coefficient of X^{2^n-1} is

$$\alpha^{2^{n-2}}\alpha^2(1+\alpha^2) + \alpha^{2^{n-2}}\alpha^4(1+\alpha^2) = \alpha^{2^{n-2}}\alpha^2(1+\alpha^2)^2.$$

This is only zero if $\alpha = 0$ or $\alpha = 1$. Since, α is neither 0 nor 1 then the coefficient is non-zero. Therefore, the degree of $f^t(X)$ is $2^n - 1$ and $f(X)$ is not a permutation.

Case 2: Let $\alpha = 1$. When $n = 5$, then $t = 11$ and when $n > 5$, then $t = 11 + \sum_{i=2}^{\frac{n-3}{2}} 2^{2i}$.

Subcase 1: When $n = 5$ then $f^t(X) \bmod X^q - X$ is

$$(X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X))(X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)) \times (X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)).$$

We let

$$A_0 = (X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_1 = (X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)), \text{ and}$$
$$A_2 = (X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)).$$

There are 5 ways to choose terms to multiply to a term with exponent X^{2^n-1}; they are given in Table 1.

Summing, we find the coefficient is 1. Hence, the degree of $f^t(X)$ is $2^n - 1$ and therefore, $f(X)$ is not a permutation.

Subcase 2: Let $n > 5$ and $t = 11 + \sum_{i=2}^{\frac{n-3}{2}} 2^{2i}$. Then, $f^t(X) \bmod X^q - X$ is

$$\left(X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X)\right)\ \left(X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)\right) \times \left(X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)\right) \prod_{i=2}^{\frac{n-3}{2}} \left(X^{2^{2i+1}+2^{2i}} + X^{2^{2i}}\,\mathrm{Tr}(X) + \mathrm{Tr}(X)\right).$$

We let

$$A_0 = (X^{2+1} + X\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_1 = (X^{4+2} + X^2\,\mathrm{Tr}(X) + \mathrm{Tr}(X)),$$
$$A_2 = (X^{8+16} + X^8\,\mathrm{Tr}(X) + \mathrm{Tr}(X)), \text{ and}$$
$$A_i = (X^{2^{2(i-1)+1}+2^{2(i-1)}} + X^{2^{2(i-1)}}\,\mathrm{Tr}(X) + \mathrm{Tr}(X)) \text{ for } i \geq 3.$$

The largest exponent on X that we can choose from one of these terms before taking into account $\mathrm{Tr}(X)$ is $2(\frac{n-3}{2}) + 1 = n - 2$. We need a 2^{n-1} exponent on X. Therefore, we must choose the $X^{2^{n-1}}$ term from the trace function.

To obtain the odd powers of 2 (the terms of the form $2^{2(i-1)+1}$) we must choose the $X^{2^{2(i-1)+1}+2^{2(i-1)}}$ term from A_i for $1 \leq i \leq \frac{n-1}{2}$. This will give us the term $X^{2+4+\ldots+2^{n-2}}$. This forces us to choose $X\,\mathrm{Tr}(X)$ from A_0. Therefore, there is only one way to choose terms to get the term X^{2^n-1} and the coefficient on the term is 1. Hence, $f(X)$ is not a permutation. □

One can also show that the functions of this last theorem are not permutations when n is even unless $n = 2$ and $\alpha = 1$. The argument is similar, though slightly more involved, than the work needed to eliminate the even case of Theorem 12. For $n = 2$, it is easily checked that only the case $\alpha = 1$

Table 1. Choosing terms from A_0, A_1, and A_2 to obtain a X^{2^n-1} term

Term from A_0	Term from A_1	Term from A_2	Choice from $\mathrm{Tr}(X)$	Coefficient
X^{2+1}	$X^2\,\mathrm{Tr}(X)$	X^{16+8}	X^2	1
X^{2+1}	$\mathrm{Tr}(X)$	X^{16+8}	X^4	1
$X\,\mathrm{Tr}(X)$	X^{4+2}	X^8	X^{16}	1
$X\,\mathrm{Tr}(X)$	$X^2\,\mathrm{Tr}(X)$	X^{16+8}	X^4	1
$\mathrm{Tr}(X)$	X^{4+2}	X^{16+8}	X	1

leads to a permutation, so suppose $n > 2$ is even and again let $\{1, \zeta, \zeta^{-1}\}$ be the three roots of unity in $\mathbb{F}_q$. Note that $\mathbb{F}_4$ consists of these three elements and 0. Using the transitivity of trace identity, we have

$$\mathrm{Tr}(x) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(x)) = \begin{cases} 0 & \text{if } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(x) \in \{0,1\}, \\ 1 & \text{if } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(x) \in \{\zeta, \zeta^{-1}\}. \end{cases}$$

Note also that $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\zeta) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\zeta^{-1}) = 1$. Consequently, whenever $\mathrm{Tr}(x) = 0$, we also have

$$\mathrm{Tr}(\zeta x) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\zeta\,\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(x)) = 0,$$

and similarly $\mathrm{Tr}(\zeta^{-1}x) = 0$. We now define the sets U and V by

$$U = \{x \in \mathbb{F}_q \,:\, \mathrm{Tr}(x) = 0\},$$
$$V = \{x \in \mathbb{F}_q \,:\, \mathrm{Tr}(\alpha x) = 0\}.$$

As before, U and V are both $n-1$ dimensional subspaces of $\mathbb{F}_q$, viewed as a vector space over $\mathbb{F}_2$, and we can again conclude that U and V must have non-trivial intersection as $n > 2$. Let u be any non-zero element of $U \cap V$. Then,

$$0 = \mathrm{Tr}(u) = \mathrm{Tr}(\alpha u) = \mathrm{Tr}(\zeta u) = \mathrm{Tr}(\zeta^{-1}u) = \mathrm{Tr}(\alpha\zeta u) = \mathrm{Tr}(\alpha\zeta^{-1}u),$$

and so $f(u) = f(\zeta u) = f(\zeta^{-1}u) = u^3$. Hence, f is not a permutation.

6. Functions from Planar Nearfields

A second class of well-structured algebraic objects are the planar nearfields. In this section, we shall consider the differential uniformity of functions generated by the multiplication of these structures. As mentioned earlier, there are both regular and irregular planar nearfields.

6.1. The Regular Planar Nearfields

Let q be a prime power and n a natural number such that the prime divisors of n also divide $q-1$. In addition, if $q \equiv 3 \pmod 4$, then $n \not\equiv 0 \bmod 4$. Let $\mathfrak{z}$ be a primitive element of $\mathbb{F}_{q^n}$ and let $\mathcal{C}$ be the group generated by $\mathfrak{z}^n$. The coset representatives of $\mathcal{C}$ are $\mathfrak{z}_i = \mathfrak{z}^{q^i-1/q-1}$ with $i = 0, \ldots, n-1$. Let $\mathcal{F}$ be the Frobenius group of automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. That is $\mathcal{F} = \langle\phi\rangle$

where $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ satisfies $\phi(x) = x^q$. We define the function $\alpha : \mathbb{F}_q^\star \mapsto \mathcal{F}$ by $\alpha : y \mapsto (x \mapsto x^{q^i})$ if and only if $y \in \mathfrak{z}_i\mathcal{C}$. Define a new multiplication on $\mathbb{F}_{q^n}$ by

$$x * y = \begin{cases} x^{\alpha(y)}y & \text{if } y \in \mathbb{F}_{q^n}^\star, \\ 0 & \text{if } y = 0. \end{cases}$$

Set $\mathbb{N}(n, q) = (\mathbb{F}_{q^n}, +, *)$, where $+$ is the field addition. Then, Dickson showed $\mathbb{N}(n, q)$ is a *regular* planar nearfield.

We shall consider the function $f(x) = x * x$ where we use the multiplication from the regular nearfields $\mathbb{N}(2s, q)$, where $q = p^{2t}$ for some odd prime p and integers $t, s \geq 1$. Note that the function f is a function over $\mathbb{F}_{q^{2s}}$. We make the following conjecture based on computational evidence.

Conjecture 14. The function $f(x)$ as just defined is $\frac{q+1}{2}$-DU.

In support of our conjecture, we prove that the differential uniformity of f can be no less than $\frac{q+1}{2}$ when $s = 1$.

Theorem 15. *If $s = 1$, then $f(x)$ as defined above is at least $\frac{q+1}{2}$-DU.*

The proof will require the following obvious lemma and corollary.

Lemma 3. *For q odd, $4k \not\equiv 4j + r \pmod{q^2 - 1}$ for any integers k, j and $0 < r < 4$.*

We immediately get the following corollary which is a necessary condition for Conjecture 14.

Corollary 4. *If $\mathbb{F}_{q^2}^\star = \langle \mathfrak{z} \rangle$, then $\mathfrak{z}^{4k} \neq \mathfrak{z}^{4j+2}$ for all integers j, k.*

The following three lemmas were developed in collaboration with B. Fain during the first author's dissertation studies.

Lemma 4. *Let q be an odd prime power.*

(i) *If $q \equiv 1 \bmod 4$, then the set of zeros of the trace function $\mathrm{Tr}_{q^2/q}$ is given by a set of $q - 1$ non-square elements in $\mathbb{F}_{q^2}$ and 0.*
(ii) *If $q \equiv 3 \bmod 4$, then the set of zeros of the trace function $\mathrm{Tr}_{q^2/q}(X)$ is a set of $q - 1$ square elements in $\mathbb{F}_{q^2}$ and 0.*

Proof. Suppose $\mathrm{Tr}_{q^2/q}(\beta) = 0$. Then, $\beta^q + \beta = \beta(\beta^{q-1} + 1) = 0$. If $\beta \neq 0$, then $\beta^{q-1} = -1$. Therefore,

$$\beta^{(q^2-1)/2} = (\beta^{q-1})^{(q+1)/2} = (-1)^{(q+1)/2}.$$

Thus, β is a square if $q \equiv 3 \bmod 4$ and a non-square if $q \equiv 1 \bmod 4$. □

As a generalization, we have the following lemma.

Lemma 5. *Let q be an odd prime power and fix $a \in \mathbb{F}_{q^2}^\star$. Denote the quadratic character over $\mathbb{F}_{q^2}$ by η, and the quadratic character of $\mathbb{F}_q$ by ψ. Set $L(X) = \mathrm{Tr}_{q^2/q}(a^q X) = aX^q + a^q X$. If $L(\beta) = 0$, then either $\beta = 0$ or $\eta(\beta) = -\psi(-1)\eta(a)$.*

Proof. Suppose $L(\beta) = 0$. Then, $a\beta^q + a^q\beta = a\beta(\beta^{q-1} + a^{q-1}) = 0$. If $\beta \neq 0$, then $\beta^{q-1} = -a^{q-1}$. Therefore,

$$\eta(\beta) = (\beta^{q-1})^{(q+1)/2} = (-a^{q-1})^{(q+1)/2} = (-1)^{(q+1)/2}\eta(a).$$

Thus, $\eta(\beta) = \eta(a)$ if $q \equiv 3 \bmod 4$ and $\eta(\beta) = -\eta(a)$ if $q \equiv 1 \bmod 4$. □

Lemma 6. *Let q be an odd prime power. If $\mathrm{Tr}_{q^2/q}(\beta) = 0$, then $\eta(\beta + 1) = \eta(\beta - 1)$.*

Proof. Consider the following relationship:

$$\begin{aligned}(x+1)^{q+1} - (x-1)^{q+1} &= (x^q + 1)(x + 1) - (x^q - 1)(x - 1)\\ &= x^{q+1} + x^q + x + 1 - x^{q+1} + x^q + x - 1\\ &= 2(x^q + x)\\ &= 2\,\mathrm{Tr}_{q^2/q}(x).\end{aligned}$$

Therefore, if $\mathrm{Tr}_{q^2/q}(\beta) = 0$, then $(\beta + 1)^{q+1} - (\beta - 1)^{q+1} = 0$. Thus, $(\beta + 1)^{q+1} = (\beta - 1)^{q+1}$. Raising both sides to the $\frac{q-1}{2}$ proves the statement. □

Lemma 7. *The equation $\mathrm{Tr}_{q^2/q}(x) = 0$ has q solutions. When $q \equiv 1 \bmod 4$, the $q - 1$ non-zero solutions, α, are non-squares and $(q - 1)/2$ are such that $\alpha + 1$ is a square and $(q - 1)/2$ are such that $\alpha + 1$ is a non-square. When $q \equiv 3 \bmod 4$, the $q - 1$ non-zero solutions, α, are squares and $(q - 1)/2$ are such that $\alpha + 1$ is a square and $(q - 1)/2$ are such that $\alpha + 1$ is a non-square.*

Proof. Since $q \equiv 1 \bmod 4$, we know that the non-zero elements of the kernel of $\mathrm{Tr}_{q^2/q}$ are non-squares from Lemma 4. The kernel of $\mathrm{Tr}_{q^2/q}$ is a one dimensional subspace of $\mathbb{F}_q$ and we can denote it as $\overline{\beta}$ where β is any non-zero element in the kernel. We want to investigate the quadratic character on $\alpha + 1 = k\beta + 1$. We can divide $\mathbb{F}_{q^2} \backslash \mathbb{F}_q$ into q one dimensional subspaces, $\overline{\beta + \lambda}$ for $\lambda \in \mathbb{F}_q^\star$. The members of the same subspace will have the same quadratic character; thus, $(q - 1)/2$ of them are sets of squares and $(q + 1)/2$ are sets of non-squares. The set $\{k\beta + 1 : k \in \mathbb{F}_q^\star\}$ intersects each of these subspaces, other than the space $\overline{\beta}$, exactly once. Since $\overline{\beta}$ is a set of non-squares, the number of non-zero solutions to $\mathrm{Tr}_{q^2/q}(\alpha) = 0$ divides evenly into $\frac{q-1}{2}$ elements such that $\alpha + 1$ is a non-square and $\frac{q-1}{2}$ elements such that $\alpha + 1$ is a square.

The proof for $q \equiv 3 \bmod 4$ is similar to the above except the kernel of the elements of $\mathrm{Tr}_{q^2/q}$ are squares from Lemma 4. □

We can now prove Theorem 15.

Proof. We consider the derivative $D_f(x, a) = f(x + a) - f(x)$ in place of the difference function $\Delta_f(x, a)$.

Fix $a \in \mathbb{F}_{p^{4t}}^\star$. We have four cases, based on if x and $x + a$ are each squares or not. We outline the cases as follows.

(1) If x and $x + a$ are squares, then, $D_f(x, a) = (x + a)^2 - x^2 = 2ax + a^2$.
(2) If x is a square and $x + a$ is not a square, then, $D_f(x, a) = (x + a)^{q+1} - x^2 = x^{q+1} + x^q a + a^q x + a^{q+1} - x^2$.

(3) If $x+a$ is a square and x is not a square, then, $D_f(x,a) = (x+a)^2 - x^{q+1} = x^2 + 2xa + a^2 - x^{q+1}$.
(4) If x and $x+a$ is not squares, then, $D_f(x,a) = (x+a)^{q+1} - x^{q+1} = x^q a + a^q x + a^{q+1}$.

In Case 1, after we fix a $c \in \mathbb{F}_{q^2}$ we are solving $2xa + a^2 = c$. Solving this we obtain $x = 2^{-1}a^{-1}c - 2^{-1}a$. Case 1 only adds a solution if $2^{-1}a^{-1}c - 2^{-1}a$ and $2^{-1}a^{-1}c - 2^{-1}a + a$ are squares.

Similarly, Case 4 provides at most q solutions. In Case 4, $D_f(x,a) = a^q x + x^q a = D_{x^{q+1}}(x,a)$. This linear transformation has degree q, so has at most q solutions. However, we need to determine how many of these solutions satisfy the conditions that x and $x+a$ must both be non-squares.

To prove the lower bound of $\frac{q+1}{2}$ for the differential uniformity, we need only produce a choice of a, b for which the number of solutions is at least $\frac{q+1}{2}$. To this end, fix $a = 1$ and $b = 0$. First, we have in Case 1 that $x = -2^{-1}$ and $x + 1 = 1 - 2^{-1}$; since both x and $x+1$ are in $\mathbb{F}_q$, they are necessarily squares in $\mathbb{F}_{q^2}$. Therefore, this will yield a solution.

Next, we claim that Case 2 and Case 3 yield no solutions. In Case 2, we get $0 = (x+1)^{q+1} - x^2$, or equivalently, $x^2 = (x+1)^{q+1}$. Since x is a square $x+1$ is a non-square, $x = \mathfrak{z}^{2s}$ and $x+1 = \mathfrak{z}^{2t+1}$ for integers s, t. Therefore, we find $\mathfrak{z}^{4s} = \mathfrak{z}^{4(2st+s+t)+2}$, which has no solution by Lemma 4 as $q \equiv 1 \bmod 4$. Therefore, there are no solutions in this case. A similar argument shows there are no solutions in Case 3.

Finally, for Case 4, from Lemma 7, there are $\frac{q-1}{2}$ solutions since $q \equiv 1 \bmod 4$.

Therefore, there are a total of $\frac{q+1}{2}$ solutions to $D_f(x,1) = 0$. Hence, the differential uniformity of f is at least $\frac{q+1}{2}$. □

6.2. The Irregular Planar Nearfields

The majority of Zassenhaus' classification of planar nearfields involves tying down the sporadic examples of planar nearfields that do not fall into Dickson's infinite class. He showed that the 7 sporadic examples identified by Dickson were, in fact, the only ones. These are now called the *irregular* planar nearfields. There are several standard descriptions of them, but none of them could be called succinct. For each of the 7 examples, the largest of which has order 59^2, we compute the differential uniformity of the corresponding multiplication function $x \mapsto x * x$ using the Magma algebra package [3], which has built-in versions of each. Even though we have only computational results regarding them, for completeness, we outline a description of the irregular planar nearfields in an appendix.

With regards to the differential uniformity, using Magma we set up a correspondence between the elements of a given exceptional nearfield $\mathbb{N}_i$ of order p^2 and the finite field $\mathbb{F}_{p^2}$: this was done via the command `Element`($\mathbb{N}_i$,`a`), where $a \in \mathbb{F}_{p^2}$. This then allowed us to generate, through interpolation, a polynomial f_i that satisfies $f_i(x) = x * x$. The differential uniformity of that function was then computed.

Magma #	Order	$du(f)$
1	$25 = 5^2$	6
2	$121 = 11^2$	6
3	$49 = 7^2$	9
4	$529 = 23^2$	19
5	$121 = 11^2$	17
6	$841 = 29^2$	21
7	$3481 = 59^2$	25

In particular, we see that, for $i = 2$ and $i = 7$, we obtain functions with low differential uniformity compared to the characteristic. Indeed, for those two cases, we obtain functions with differential uniformity less than or equal to $\frac{p+1}{2}$ on fields of order p^2. This was something we were unable to do through the more direct approach given in Sect. 2.

7. Final Comments

In this article, our aim has been to construct functions which have low, but not optimal, differential uniformity relative to their field of definition. Two methods were provided which allowed us to successfully meet this aim. In characteristic 2, we were able to construct 4-DU functions in any field $\mathbb{F}_{2^n}$ with n odd using the multiplication stemming from the remarkable class of presemifields of Kantor and Williams and then expanding to a more general class thanks to results of [2]. In odd characteristic p, using a known connection between planar functions and orthogonal systems, we gave a general method which would allow one to construct p-DU functions in any field $\mathbb{F}_{p^n}$ without restriction on n. In addition, the functions produced from the multiplications of two of the irregular nearfields were also found to be at most $(\frac{p+1}{2})$-DU in fields of order p^2, with $p = 11$ or $p = 59$. Ideally, we would like to construct bijective functions with low differentially uniformity relative to their field of definition. However, the examples constructed in this article are not bijective, and so the major problem remains, just as it remains for APN functions, namely to construct bijective examples.

Funding This research was partially funded by the National Science Foundation, award #1855723.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Appendix: The Irregular Planar Nearfields

In this appendix, we wish to give a description of the irregular planar nearfields. We follow the outline given by S.D. Groves [18]. To describe them, we need to give a description of both the addition and multiplication of each. For the addition, we have the following theorem which holds for all nearfields.

Theorem 16. *Let $\mathbb{N}$ be a nearfield of finite dimension n over its prime field $\mathbb{F}_p$. Then, $\mathrm{GL}(n,p)$ has a fixed point free subgroup $\mathcal{S}^\star$ such that if $\mathcal{S} = \mathcal{S}^\star \cup \{\mathbf{0}\}$, where $\mathbf{0}$ denotes the $n \times n$ zero matrix, then an addition can be defined on $\mathcal{S}$ in such a way that, under this addition and matrix multiplication, $\mathcal{S}$ is a nearfield isomorphic to $\mathbb{N}$.*

Though this does not give an explicit description of the addition, it does allow for a description of the irregular nearfields in terms of just the generators of the subgroup $\mathcal{S}^\star$ of the theorem. This is given in the following classification statement due to Zassenhaus [25].

Theorem 17. *Let $\mathbb{N}$ be a finite irregular nearfield. Then, $\mathbb{N}$ has order p^2 and is isomorphic to one of the following nearfields $\mathcal{S}_i$, where $\mathcal{S}_i^\star$ is the subgroup of $\mathrm{GL}(2,p)$ generated by the matrices given below and where addition is defined as in Theorem 16.*

I. $|\mathcal{S}_1| = 5^2$ *and* $\mathcal{S}_1^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}.$$

II. $|\mathcal{S}_2| = 11^2$ *and* $\mathcal{S}_2^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

III. $|\mathcal{S}_3| = 7^2$ *and* $\mathcal{S}_3^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & 4 \\ -1 & -2 \end{pmatrix}.$$

IV. $|\mathcal{S}_4| = 23^2$ *and* $\mathcal{S}_4^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

V. $|\mathcal{S}_5| = 11^2$ *and* $\mathcal{S}_5^\star = \langle \mathbf{a}, \mathbf{b} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}.$$

VI. $|\mathcal{S}_6| = 29^2$ *and* $\mathcal{S}_6^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}.$$

VII. $|\mathcal{S}_7| = 59^2$ *and* $\mathcal{S}_7^\star = \langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle$, *where*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

References

[1] Berger, T.P., Canteaut, A., Charpin, P., Laigle-Chapuy, Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inform. Theory **52**, 4160–4170 (2006)

[2] Bracken, C., Byrne, E., Markin, N., McGuire, G.: Determining the nonlinearity of a new family of APN functions. In: Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 4851, pp. 72–79. Spring, Berlin, (2007)

[3] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: The user language. J. Symbolic Comput. **24**, 235–265 (1997)

[4] Browning, K., Dillon, J., McQuistan, M., Wolfe, A.: An APN permutation in dimension six. In: Finite fields: theory and applications, Contemp. Math., vol. 518, pp. 33–42. Amer. Math. Soc., Providence, RI (2010)

[5] Budaghyan, L., Carlet, C., Leander, G.: On a construction of quadratic APN functions. IEEE Trans. Inform. Theory **54**, 374–378 (2009)

[6] Carlitz, L.: Invariantive theory of equations in a finite field. Trans. Am. Math. Soc. **75**, 405–427 (1953)

[7] Carlitz, L.: Invariant theory of systems of equations in a finite field. J. Anal. Math. **3**, 382–413 (1954)

[8] Coulter, R.: On coordinatising planes of prime power order using finite fields. J. Austral. Math. Soc. **106**, 184–199 (2019)

[9] Coulter, R., Henderson, M.: Commutative presemifields and semifields. Adv. Math. **217**, 282–304 (2008)

[10] Coulter, R., Matthews, R.: Bent polynomials over finite fields. Bull. Austral. Math. Soc. **56**, 429–437 (1997)

[11] Coulter, R., Matthews, R.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes Cryptogr. **10**, 167–184 (1997)

[12] Coulter, R., Senger, S.: On the number of distinct values of a class of functions with finite domain. Ann. Comb. **18**, 233–243 (2014)

[13] Dembowski, P., Ostrom, T.: Planes of order n with collineation groups of order n^2. Math. Z. **103**, 239–258 (1968)

[14] Dickson, L.: The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. Ann. Math. **11**(65–120), 161–183 (1897)

[15] Dickson, L.: Definitions of a group and a field by independent postulates. Trans. Am. Math. Soc. **6**, 198–204 (1905)

[16] Dickson, L.: On finite algebras. Nachr. Kgl. Ges. Wiss. Göttingen, Math.-phy. Klasse pp. 358–393 (1905)

[17] Edel, Y., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**, 59–81 (2009)

[18] Groves, S.: Locally finite near-fields. Ph.D. thesis, Australian National University, Canberra, ACT, Australia (1974)

[19] Helleseth, T., Sandberg, D.: Some power mappings with low differential uniformity. Appl. Algebra Engrg. Comm. Comput. **8**, 363–370 (1997)

[20] Hermite, C.: Sur les fonctions de sept lettres. CR Acad. Sci. Paris **57**, 750–757 (1863)

[21] Kantor, W., Willianm, M.: Symplectic semifields and $\mathbb{Z}_4$-linear codes. Trans. Am. Math. Soc. **356**, 895–938 (2004)

[22] Moore, E.: A doubly-infinite system of simple groups. Bull. N. Y. Math. Soc. **3**, 69–82 (1893)

[23] Nöbauer, W.: Zur Theorie der Polynomtransformationen und Permutationspolynome. Math. Ann. **157**, 332–342 (1964)

[24] Nyberg, K., Knudsen, L.: Provable security against differential cryptanalysis. In: E. Brickell (ed.) Advances in Cryptology—Crypto '92, Lecture Notes in Computer Science, vol. 740, pp. 566–574 (1992)

[25] Zassenhaus, H.: Uber endlicke Fastoper. Abh. Math. Sem. Univ. Hamburg **11**, 187–220 (1935)

Emily Bergman and Robert S. Coulter
Department of Mathematical Sciences
University of Delaware
Newark
DE 19716
USA
e-mail: coulter@udel.edu

Received: March 9, 2021.

Revised: July 6, 2021.

Accepted: January 28, 2022.