Journal der mathematischen Ablehnungen
Paper No.29 (2013)

On a conjecture on planar polynomials of the form $X(\mathsf{Tr}_n(X) - uX)$

Robert S. Coulter[1] and Marie Henderson[2]

[1]Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA
[2]9/84a Boulcott Street, Wellington, New Zealand

AMS Subject class: 11T06, 12E10
Keywords: Planar functions

Note: This is a personal preprint; for correct page numbering and references please see the original paper, the proper citation for which is:

R.S. Coulter and M. Henderson, *On a conjecture on planar polynomials of the form $X(Tr_n(X) - uX)$*, Finite Fields Appl. **21** (2013), 30–34.

Abstract

In a recent paper, Kyureghyan and Özbudak proved that $u \in \{1, 2\}$ was a sufficient condition for the polynomial $X(X^{q^2} + X^q + (1-u)X)$ to be planar over $\mathbb{F}_{q^3}$, and conjectured the condition was also necessary. This conjecture is established in this note.

§ 1. Introduction

Let q be an odd prime power. We use $\mathbb{F}_q$ to denote the finite field of q elements, $\mathbb{F}_q^*$ it's nonzero elements, and $\mathbb{F}_q[X]$ the ring of polynomials in indeterminate X with coefficients from $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[X]$. Then f is a *permutation polynomial* on $\mathbb{F}_q$ if it induces a bijection on $\mathbb{F}_q$ under evaluation. If $f(X+a) - f(X)$ is a permutation polynomial for all $a \in \mathbb{F}_q^*$, then f is called *planar* over $\mathbb{F}_q$. The motivation for studying permutation polynomials or planar polynomials has been presented many times, with connections ranging from projective geometry to cryptology.

In this note we are interested in a specific conjecture concerning planar polynomials. Let $n \geq 2$ be a natural number. Set $\mathsf{Tr}_n(X) = \sum_{i=0}^{n-1} X^{q^i}$. The polynomial $\mathsf{Tr}_n \in \mathbb{F}_{q^n}[X]$ induces the trace map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$. In a recent paper [3], Kyureghyan and Özbudak considered the planarity of $f_u(X) = X(\mathsf{Tr}_n(X) - uX)$ with $u \in \mathbb{F}_{q^n}$. Their main results can be summarised as follows.

Theorem 1.1 (Kyureghyan & Özbudak, [3])**.**

(i) If $n \geq 5$, then f_u cannot be planar over $\mathbb{F}_{q^n}$ for any $u \in \mathbb{F}_{q^n}$.

(ii) If $n = 3$ and $u \in \{1, 2\}$, then f_u is planar over $\mathbb{F}_{q^3}$.

Kyureghyan and Özbudak conjectured that f_u cannot be planar for any u when $n = 4$, and that when $n = 3$, the condition on u given above was necessary. Their latter conjecture is indeed true, for in this note we prove

Theorem 1.2. *The polynomial $f_u(X) = X(Tr_3(X) - uX)$ is planar over $\mathbb{F}_{q^3}$ if and only if $u \in \{1, 2\}$.*

Our method of proof is quite indirect; we never consider the planarity of f_u directly. Instead, we use certain classification results on planar Dembowski-Ostrom polynomials given in our paper [1].

§ 2. Approach

A polynomial $L \in \mathbb{F}_{q^n}[X]$ is a *q-polynomial* if it has the form $\sum_i a_i X^{q^i}$. Such polynomials represent all linear transformations of $\mathbb{F}_{q^n}$ when viewed as a vector space over $\mathbb{F}_q$. They are non-singular (permutation polynomials) over $\mathbb{F}_{q^n}$ if and only if $L(x) = 0$ implies $x = 0$.

A polynomial $f \in \mathbb{F}_{q^n}[X]$ is a *q-Dembowski Ostrom (q-DO) polynomial* if it has the form $\sum_{ij} a_{ij} X^{q^i+q^j}$. When planar, such a polynomial yields a commutative presemifield of order q^n which can be represented as a vector space over $\mathbb{F}_q$.

In [1], we consider the isotopy problem for commutative presemifields, deriving results based on the size of the nuclei. In particular, an unstated but useful fact inherent in all of the results of [1], Section 2, is that when dealing with commutative presemifields of order q^n with nuclei of order q, the non-singular linear transformations involved are, in fact, non-singular linear transformations of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and can thus be represented by non-singular q-polynomials. Furthermore, again when dealing with commutative presemifields of order q^n with nuclei of order q, one can strengthen the statement of [1], Theorem 3.3 to deal with planar q-DO polynomials (the proof is the same as that given). Theorems 2.6 and 3.5 can thus be stated in terms of planar q-DO polynomials and non-singular q-polynomials, provided the size of the nucleus is specified as being of order at least q. This observation is critical, as by combining Theorems 2.6 and 3.5 with Menichetti's classification [5] of commutative presemifields of dimension 3 over their nucleus – he proved there are only two inequivalent commutative presemifields, the finite field and Albert's twisted field – we get the following useful lemma, which can be viewed as the q-DO polynomial equivalent of [1], Corollary 3.11.

Lemma 2.1. *If $D \in \mathbb{F}_{q^3}[X]$ is a planar q-DO polynomial, then there exists non-singular q-polynomials $L, M \in \mathbb{F}_{q^3}[X]$ and $i \in \{0, 1\}$ satisfying*

$$L(X^{q^i+1}) \equiv D(M(X)) \pmod{X^{q^3} - X}. \tag{1}$$

The cases $i = 0$ and $i = 1$ correspond to when D yields a commutative presemifield equivalent to the finite field or Albert's twisted field, respectively, and we say D is equivalent to X^2 or X^{q+1}, depending upon the case.

Lemma 2.1 is the key to our proof. We shall show firstly that if $f_u \in \mathbb{F}_{q^3}[X]$ is planar, then it cannot be equivalent to X^2. Then, we prove that if f_u is equivalent to X^{q+1}, then necessarily $u \in \{1, 2\}$. Since the planarity of f_u has been established in those cases in [3], Theorem 1.2 then follows at once.

Before moving on to these cases, we observe if $u = 0$, then $f_u(X)$ cannot be planar as then $f_u(X)$ must have non-zero roots, which contradicts results given in any of [2, 4, 6]. Consequently, we assume $u \neq 0$ in all that follows.

§ 3. Inequivalence of $f_u(X)$ and X^2

Suppose $f_u \in \mathbb{F}_{q^3}[X]$ is planar, $u \in \mathbb{F}_{q^3}^*$, and equivalent to X^2. By Lemma 2.1, there exists two q-polynomials L and M which satisfy (1). Set

$$L(X) = \alpha X^{q^2} + \beta X^q + \gamma X,$$
$$M(X) = a X^{q^2} + b X^q + c X.$$

(There are conditions on the coefficients for L and M to be permutation polynomials, but surprisingly we will not need them.) Direct calculation shows

$$L(X^2) \pmod{X^{q^3} - X} = \alpha X^{2q^2} + \beta X^{2q} + \gamma X^2,$$

and

$$\begin{aligned} f_u(M(X)) \pmod{X^{q^3} - X} = (t^{q^2}a - ua^2)X^{2q^2} &+ (t^q b - ub^2)X^{2q} + (tc - uc^2)X^2 \\ &+ (t^{q^2}b + t^q a - 2uab)X^{q^2+q} \\ &+ (t^{q^2}c + ta - 2uac)X^{q^2+1} \\ &+ (t^q c + tb - 2ubc)X^{q+1}, \end{aligned}$$

where $t = c + a^q + b^{q^2}$. By (1), we may equate coefficients. In particular, we get

$$t^{q^2}b + t^q a - 2uab = 0, \tag{2}$$
$$t^{q^2}c + ta - 2uac = 0, \tag{3}$$
$$t^q c + tb - 2ubc = 0. \tag{4}$$

First, suppose $abc = 0$. Suppose $a = 0$, say. Then (2) and (3) imply $b = c = 0$ or $t = 0$. In the former case, we find $M(X) = 0$, contrary to M being a permutation polynomial. In the latter case, we must have $c = -b^{q^2}$ and now (4) implies $2ub^{q^2+1} = 0$, so that $b = 0 = c$ and again $M(X) = 0$. A similar argument shows $b \neq 0$ and $c \neq 0$.

Thus $abc \neq 0$. We can thus solve for $2u$ in each of the three equations (2), (3) and (4); we obtain

$$\begin{aligned} 2u &= \frac{t^{q^2}b + t^q a}{ab} \\ &= \frac{t^{q^2}c + ta}{ac} \\ &= \frac{t^q c + tb}{bc}. \end{aligned}$$

Via some more simple arithmetic we find

$$u = \frac{t}{c} = \frac{t^q}{b} = \frac{t^{q^2}}{a}. \tag{5}$$

Returning to (1), we also have

$$\begin{aligned} \alpha &= t^{q^2}a - ua^2, \\ \beta &= t^q b - ub^2, \\ \gamma &= tc - uc^2. \end{aligned}$$

Substituting the appropriate part of (5) where necessary, we now find $\alpha = \beta = \gamma = 0$, and so $L(X) = 0$, a final contradiction.

There being no more possibilities, we have thus shown $f_u(X)$ can never be equivalent to X^2 over $\mathbb{F}_{q^3}$. We note that practically the same argument can be applied to show that if $f_u(X)$ is planar over $\mathbb{F}_{q^n}$ for $n = 4$, then it cannot be equivalent to X^2.

§ 4. Equivalence of $f_u(X)$ and X^{q+1}

Now suppose $f_u \in \mathbb{F}_{q^3}[X]$ is planar, $u \in \mathbb{F}_{q^3}^*$, and equivalent to X^{q+1}. As above, we appeal to Lemma 2.1 for the existence of two q-polynomials L and M, whose coefficients we will denote as above, which satisfy (1). The calculation for $f_u(M(X)) \pmod{X^{q^3} - X}$ is as before, while

$$L(X^{q+1}) \pmod{X^{q^3} - X} = \alpha X^{q^2+1} + \beta X^{q^2+q} + \gamma X^{q+1}.$$

The two cases are again $abc = 0$ or $abc \neq 0$.

This time, let us deal with the case $abc \neq 0$ first, which is practically the direct reverse argument of the corresponding case in our last proof. Equating coefficients for the X^{2q^j} terms, $j \in \{0, 1, 2\}$, we find

$$\begin{aligned} 0 &= t^{q^2} a - ua^2, && (6) \\ &= t^q b - ub^2, && (7) \\ &= tc - uc^2. && (8) \end{aligned}$$

Solving for u in each of these equations, we obtain the identities

$$u = \frac{t}{c} = \frac{t^q}{b} = \frac{t^{q^2}}{a}.$$

Now equating the coefficients in (1) for the remaining terms, we have

$$\begin{aligned} \beta &= t^{q^2} b + t^q a - 2uab, \\ \alpha &= t^{q^2} c + ta - 2uac, \\ \gamma &= t^q c + tb - 2ubc. \end{aligned}$$

Now substituting leads to $\alpha = \beta = \gamma = 0$, so that $L(X) = 0$, a contradiction.

Hence $abc = 0$ must hold. If any two of a, b and c are zero, then the remaining non-zero equation from (6), (7), and (8), along with $t = c + a^q + b^{q^2}$, forces $u = 1$, a case we know to be planar.

Now suppose only $a = 0$. Then we still have

$$u = \frac{t}{c} = \frac{t^q}{b}.$$

Solving for c and b, we can substitute into the formula for t to find

$$\begin{aligned} t &= c + b^{q^2} \\ &= \frac{t}{u} + \frac{t}{u^{q^2}}. \end{aligned}$$

Since $u \neq 0$, we know $t \neq 0$, and so we can multiply through by u^{q^2}/t to obtain the equation

$$0 = u^{q^2} - u^{q^2-1} - 1. \tag{9}$$

Now multiplying by u, we can factor to obtain

$$\begin{aligned} 1 &= (u-1)(u^{q^2} - 1) \\ &= (u^q - 1)(u - 1) \\ &= (u^{q^2} - 1)(u^q - 1), \end{aligned}$$

where the last two identities are obtained by successively raising the previous identity to the qth power. Clearly $u \neq 1$, and so we find $u \in \mathbb{F}_q$. Now (9) simplifies to $u = 2$, another case which we know to be planar. The cases $b = 0$ and $c = 0$ lead to the same conclusion.

Hence $u \in \{1, 2\}$ is forced, and since we already know both are planar, Theorem 1.2 has been established. We also have the following corollary.

Corollary 4.1. *If $u \in \{1, 2\}$, then the planar DO polynomial $f_u \in \mathbb{F}_{q^3}[X]$ necessarily yields a commutative presemifield equivalent to Albert's twisted field.*

§ 5. Final comments

While we have resolved one of the two conjectures of Kyureghyan and Özbudak, there remains the problem of showing $f_u(X)$ is never planar over $\mathbb{F}_{q^n}$ with $n = 4$. One might be tempted to approach the $n = 4$ case in a similar way; certainly, one can show $f_u(X)$ is never equivalent to X^2 in almost identical fashion to our Section 3. However, additional problems arise. Firstly, the classification of planar DO polynomials representing commutative presemifields of dimension 4 over $\mathbb{F}_q$ is incomplete. Secondly, and perhaps more importantly, even if we had such a classification, the strict strong isotopy results from [1] no longer hold in general (though they do in some cases, in particular the case X^2), and so there is no four dimensional version of Lemma 2.1. So we suspect that a different approach will be needed to resolve the $n = 4$ conjecture from [3].

References

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

[2] R.S. Coulter and R.W. Matthews, *On the number of distinct values of a class of functions over a finite field*, Finite Fields Appl. **17** (2011), 220–224.

[3] G. Kyureghyan and F. Özbudak, *Planar products of two linearized polynomials*, submitted.

[4] G.M. Kyureghyan and A. Pott, *Some theorems on planar mappings*, Arithmetic of Finite Fields: Proceedings of the 2nd International Workshop, WAIFI 2008 (J. von zur Gathen, J.L. Imanã, and C.K. Koç, eds.), Lecture Notes in Computer Science, vol. 5130, 2008, pp. 117–122.

[5] G. Menichetti, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra **47** (1977), 400–410.

[6] W. Qiu, Z. Wang, G. Weng, and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), 49–62.