arXiv:1609.07833v2 [math.CO] 10 Jun 2017

FINITE FLAG-TRANSITIVE AFFINE PLANES WITH A SOLVABLE AUTOMORPHISM GROUP

TAO FENG

Abstract. In this paper, we consider finite flag-transitive affine planes with a solvable automorphism group. Under a mild number-theoretic condition involving the order and dimension of the plane, the translation complement must contain a linear cyclic subgroup that either is transitive or has two equal-sized orbits on the line at infinity. We develop a new approach to the study of such planes by associating them with planar functions and permutation polynomials in the odd order and even order case respectively. In the odd order case, we characterize the Kantor-Suetake family by using Menichetti's classification of generalized twisted fields and Blokhuis, Lavrauw and Ball's classifcation of rank two commutative semifields. In the even order case, we develop a technique to study permutation polynomials of DO type by quadratic forms and characterize such planes that have dimensions up to four over their kernels.

1. Introduction

Let V be a $2n$-dimensional vector space over the finite field $\mathbb{F}_q$. A *spread* $\mathcal{S}$ of V is a collection of n-dimensional subspaces that partitions the nonzero vectors in V. The members of $\mathcal{S}$ are the *components*, and V is the *ambient space*. The *kernel* is the subring of $\Gamma L(V)$ that fixes each component, and it is a finite field containing $\mathbb{F}_q$. The *dimension* of $\mathcal{S}$ is the common value of the dimensions of its components over the kernel. The *automorphism group* $\mathrm{Aut}(\mathcal{S})$ is the subgroup of $\Gamma L(V)$ that maps components to components. The incidence structure $\Pi(\mathcal{S})$ with point set V and line set $\{W + v : W \in \mathcal{S}, v \in V\}$ and incidence being inclusion is a translation plane. The kernel or dimension of $\Pi(\mathcal{S})$ is that of $\mathcal{S}$ respectively. Andre [4] has shown that $\mathrm{Aut}(\mathcal{S})$ is the translation complement of the plane $\Pi(\mathcal{S})$ and each finite translation plane can be obtained from a spread in this way. Two spreads $\mathcal{S}$ and $\mathcal{S}'$ of V are *isomorphic* if $\mathcal{S}' = \{g(W) : W \in \mathcal{S}\}$ for some $g \in \Gamma L(V)$, and isomorphic spreads correspond to isomorphic planes.

An affine plane is called *flag-transitive* if it admits a collineation group which acts transitively on the flags, namely, the incident point-line pairs. Throughout this paper, we will only consider finite planes. Wagner [47] has shown that finite flag-transitive planes are necessarily translation planes, so the plane must have prime power order and can be constructed from a spread $\mathcal{S}$ with ambient space V of dimension $2n$ over $\mathbb{F}_q$ for some n and q. The affine plane $\Pi(\mathcal{S})$ constructed from a spread $\mathcal{S}$ is flag-transitive if and only if $\mathrm{Aut}(\mathcal{S})$ is transitive on the components. Foulser has determined all flag-transitive groups of finite affine planes in [24, 25]. The only non-Desarguesian flag-transitive affine planes with nonsolvable collineation groups are the nearfield planes of order 9, the Hering plane of order 27 [23], and the Lüneburg planes of even order [36], cf. [13, 30]. In the solvable case, Foulser has shown that with a finite number of exceptions, which are explicitly described, a solvable flag transitive group of a finite affine plane is a subgroup of a one-dimensional Desarguesian affine plane.

Kantor and Suetake have constructed non-Desuarguesian flag-transitive affine planes of odd order in [29, 31, 43, 44], and we will refer to these planes as the Kantor-Suetake family. The dimension two case is also due to Baker and Ebert [8]. Kantor and Williams have constructed large numbers of flag-transitive affine planes of even order arising from symplectic spreads in [27, 32]. The dimensions of these planes over their kernels are odd. It remains open whether

Key words and phrases. spread, affine plane, planar function, commutative semifield, quadratic form, permutation polynomial.

there is a non-Desarguesian flag-transitive affine plane of even order whose dimension over its kernel is even and greater than 2. Prince has completed the determination of all the flag-transitive affine planes of order at most 125 in [42], and there are only the known ones.

Except for the Lüneburg planes and the Hering plane of order 27, all the known finite non-Desarguesian flag-transitive affine planes have a translation complement which contains a linear cyclic subgroup that either is transitive or has two equal-sized orbits on the line at infinity. Under a mild number-theoretic condition involving the order and dimension of the plane (see Lemma 3.1 below), it can be shown that one of these actions must occur. We call flag-transitive planes of the first kind *$\mathcal{C}$-planes* and those of the second kind *$\mathcal{H}$-planes*, and call the corresponding spreads of *type* $\mathcal{C}$ and *type* $\mathcal{H}$ respectively. There has been extensive study on these two types of planes in the literature. In the case the plane has odd order and dimension two or three over its kernel, it has been shown that the known examples are the only possibilities for either of these two types, see [5, 6, 7, 9, 10, 22]. The classification takes a geometric approach by making use of the intersection of the corresponding spread with the orbits of a certain Singer subgroup and considering relevant Baer subgeometry partitions.

In the study of finite flag-transitive projective planes, deep results from finite group theory are invoked and considerable progress has been made towards a complete classification, cf. [28, 45, 46]. In contrast, the affine case is more of a combinatorial flavor, and a complete classification seems far out of reach. In this paper, we show that there is a broader connection between flag-transitive affine planes and other combinatorial objects than that is previously known. This will lead us to new characterization results on such planes by making use of the deep results already obtained in other circumstances. To be specific, in Section 3 we develop a new approach to the study of such planes by associating them with planar functions and permutation polynomials in the odd order and even order case respectively. In the odd order case, this new approach allows us to characterize the Kantor-Suetake family by making use of Menichetti's classification of generalized twisted fields in [37, 38]. In particular, the cases of dimension two and three over their kernels follow as a consequence. In Section 4 we will consider the nuclei of the associated commutative semifields and study planar functions that correspond to rank two commutative semifields by the classification results of such semifields by Blokhuis, Lavrauw and Ball in [14, 33]. In the even order case, we will develop a technique to study permutation polynomials of DO type by quadratic forms and characterize such planes that have dimensions up to four over their kernels in Section 5. This is the first characterization result in the even order case to our knowledge.

2. Preliminaries

A finite *presemifield* S is a finite ring with no zero-divisors such that both the left and right distributive laws hold. If further it contains a multiplicative identity, then we call S a *semifield*. The additive group of a finite presemifield is necessarily an elementary abelian p-group for some prime p, so it is conventional to identify $(S,+)$ as the additive group of the finite field $\mathbb{F}_q$ with $q=|S|$ elements. Two presemifields $S_1=(\mathbb{F}_q,+,\star)$ and $S_2=(\mathbb{F}_q,+,*)$ are *isotopic* if there exist three linear bijections L, M, N from $(\mathbb{F}_q,+)$ to itself such that $M(x)*N(y)=L(x\star y)$ for all $x,y\in\mathbb{F}_q$. In this case, we call S_1 an *isotope* of S_2 and vice versa. For a presemifield $S=(\mathbb{F}_q,+,*)$, fix any $e\neq 0$ and define a new multiplication $\circ$ by $(x*e)\circ(e*y)=x*y$. Then $S'=(\mathbb{F}_q,+,\circ)$ is a semifield with multiplicative identity $e*e$ that is isotopic to S.

Let $S=(\mathbb{F}_q,+,*)$ be a commutative semifield. Its *middle nucleus* $\mathcal{N}_m(S)$ and *nucleus* $\mathcal{N}(S)$ are defined respectively as follows:

$$\mathcal{N}_m(S)=\{\alpha\in\mathbb{F}_q:\,(x*\alpha)*y=x*(\alpha*y)\text{ for all }x,y\},$$
$$\mathcal{N}(S)=\{\alpha\in\mathbb{F}_q:\,(\alpha*x)*y=\alpha*(x*y)\text{ for all }x,y\}.$$

Both $\mathcal{N}_m(S)$ and $\mathcal{N}(S)$ are finite fields, and we can regard S as a vector space over $\mathcal{N}_m(S)$. For more details, please refer to [26] or the surveys in [40, Chapter 9] and [34].

A *rank two commutative semifield* (RTCS for short) is a commutative semifield that is of rank at most two over its middle nucleus. A finite field is a RTCS by definition, and other known examples include: Dickson semifields [21], Cohen-Ganley semifields [15] and the Penttila-Williams semifield [41]. They have close connections with many central objects in finite geometry, cf. [11, 34]. The following approach to RTCS is due to Cohen and Ganley [15].

Theorem 2.1. *Let q be odd, and fix $t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let f, $g : \mathbb{F}_q \mapsto \mathbb{F}_q$ be two functions. The algebraic system $S(g, f) := (\mathbb{F}_{q^2}, +, \circ)$ with multiplication*

$$(xt + y) \circ (ut + v) = (xv + yu + g(xu))t + yv + f(xu) \tag{2.1}$$

is a RTCS if and only if f, g are linear and $g(x)^2 + 4xf(x)$ is a nonsquare for $x \neq 0$.

In this manner, the Dickson semifield can be described as $S(g, f)$ with $g(z) = 0$ and $f(z) = mz^\sigma$, where q is odd, σ is an automorphism of $\mathbb{F}_q$, and m is a nonsquare. It is clear that a different choice of t in the theorem lead to an isotopic semifield. In the following theorem we collect some characterization results of Dickson semifields among all RTCSs.

Theorem 2.2 ([14, 33])**.** *Let S be a RTCS of order p^{2n}, p an odd prime. If the nucleus $\mathcal{N}(S) = \mathbb{F}_q$, and $p^n = q^s$, then S is isotopic to either a finite field or a Dickson semifield if $p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, $q \geq 4s^2 - 8s + 2$ or $s = 3$.*

A polynomial $f(X) \in \mathbb{F}_q[X]$ is *reduced* if $\deg(f) \leq q - 1$. It is well known that any function $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ is uniquely representable by a reduced polynomial in $\mathbb{F}_q[X]$, i.e., there exists a unique reduced polynomial $g(X) \in \mathbb{F}_q[X]$ such that $f(x) = g(x)$ for all $x \in \mathbb{F}_q$. We will write $f(X)$ and $f(x)$ when we regard f as a polynomial and a function respectively. A polynomial of the form $L(X) = \sum_{i=0}^{m} a_i X^{q^i}$ with coefficients a_i's in $\mathbb{F}_{q^n}$ is called a *q-polynomial* over $\mathbb{F}_{q^n}$. If q is not specified in the context, then it is also called a *linearized polynomial.* If $L(X)$ is a reduced linearized polynomial over $\mathbb{F}_{q^n}$, then the map $x \mapsto L(x)$ is $\mathbb{F}_q$-linear if and only $L(X)$ is a q-polynomial. If a subspace U is in the kernel of L, then $L_U(X) = \prod_{a \in U}(X - a)$ is a linearized polynomial, and there is a linearized polynomial R such that $L(X) = R(L_U(X))$, cf. [35, Theorem 3.52, Theorem 3.62]. For a q-polynomial $L(X) = \sum_{i=0}^{n-1} d_i X^{q^i}$, define its *adjoint* polynomial as $\tilde{L}(X) = \sum_{i=0}^{n-1} d_i^{q^{n-i}} X^{q^{n-i}}$, and its associated matrix as

$$M := \begin{pmatrix} d_0 & d_1 & \cdots & d_{n-1} \\ d_{n-1}^q & d_0^q & \cdots & d_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ d_1^{q^{n-1}} & d_2^{q^{n-1}} & \cdots & d_0^{q^{n-1}} \end{pmatrix}. \tag{2.2}$$

The following lemma is well-known, and we sketch a proof.

Lemma 2.3. *If $L(X) = \sum_{i=0}^{n-1} d_i X^{q^i} \in \mathbb{F}_{q^n}[X]$, then the kernel of the $\mathbb{F}_q$-linear map $x \mapsto L(x)$ from $\mathbb{F}_{q^n}$ to itself has dimension $n - \mathrm{rank}(M)$, where M is as defined in (2.2).*

Proof. Take $\{t_0, t_1, \cdots, t_{n-1}\}$ to be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let T be the $n \times n$ matrix whose (i, j)-th entry is $t_j^{q^i}$ for $0 \leq i, j \leq n - 1$. By [35, Lemma 3.51], T is invertible. It is routine to check that $(T^t MT)_{i,j} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(t_i L(t_j))$ and $(MT\mathbf{x}^t)_i = L(x)^{q^i}$, where $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_q^n$ and $x = x_0 t_0 + x_1 t_1 + \cdots + x_{n-1} t_{n-1} \in \mathbb{F}_{q^n}$. It follows that $L(x) = 0$ if and only if $\mathbf{x}^t$ is in the null space of $T^t MT$. The matrix $T^t MT$ has all its entries in $\mathbb{F}_q$, so its rank over $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ are the same. The conclusion now follows. □

A function $f : \mathbb{F}_q \mapsto \mathbb{F}_q$ is a *planar function* if $x \mapsto f(x + a) - f(x) - f(a)$ is a permutation of $\mathbb{F}_q$ for any $a \neq 0$. It is known that there are no planar functions in even characteristic. A

Dembowski-Ostrom (or DO) polynomial over a field of characteristic p is a polynomial of the shape $\sum_{i,j} a_{ij}X^{p^i+p^j}$. If a function $f:\mathbb{F}_q\mapsto\mathbb{F}_q$ is representable by a DO polynomial, we call f a function of DO type. Two planar functions f,g of DO type are *equivalent* if there exist linearized polynomials L_1, L_2 such that $f(x)=L_1(g(L_2(x)))$ for all $x\in\mathbb{F}_q$. It is shown in [16] that there is a close connection between commutative presemifield and planar functions of DO type: if $(\mathbb{F}_q,+,*)$ is a commutative presemifield, then $x\mapsto x*x$ is a planar function of DO type over $\mathbb{F}_q$; conversely, if f is a planar function of DO type, then $S_f=(\mathbb{F}_q,+,*)$ is a commutative presemifield, where the multiplication is $x*y=f(x+y)-f(x)-f(y)$. Weng and Hu have given a characterization of planar functions in terms of the images of f in [48, Theorem 2.3].

Lemma 2.4. *Let $f:\mathbb{F}_q\mapsto\mathbb{F}_q$ be a DO polynomial. Then f is a planar function if and only if f is 2-to-1, namely, every nonzero element has 0 or 2 preimages.*

We shall need the following simple lemma.

Lemma 2.5. *Let q be an odd prime power and w be a nonsquare of $\mathbb{F}_q$. If $L_1(X)$ and $L_2(X)$ are linearized polynomials such that $Q(x)=L_1(x)^2-wL_2(x)^2$ is a planar function over $\mathbb{F}_q$, then at least one of L_1 and L_2 is a permutation polynomial.*

Proof. If neither L_1 nor L_2 is a permutation, then there exists nonzero elements u_1,u_2 such that $L_1(u_1)=L_2(u_2)=0$. However, this leads to that $Q(u_1+u_2)-Q(u_1)-Q(u_2)=0$, which contradicts the planarity property. □

A *quadratic space* is a pair $(Q,\,V)$ where V is a finite dimensional vector space over $\mathbb{F}_q$ and $Q:\,V\mapsto\mathbb{F}_q$ satisfies that: (1) $Q(\lambda v)=\lambda^2Q(v)$ for all $\lambda\in\mathbb{F}_q$ and $v\in V$; (2) $B_Q(x,y):=Q(x+y)-Q(x)-Q(y)$ is a bilinear form. If we fix a basis $\{e_1,\cdots,e_n\}$ of V over $\mathbb{F}_q$, then $f(x_1,\cdots,x_n)=Q(\sum_{i=1}^n x_ie_i)$ is a *quadratic form* in n indeterminants over $\mathbb{F}_q$. A different choice of basis yields an equivalent form, and the *rank* of Q is the minimum number of variables in a quadratic form induced from Q in this way. The *radical* of a quadratic space $(Q,\,V)$ is

$$\mathrm{rad}(Q):=\{v\in V:\,B_Q(v,x)=0\text{ for all }x\in V\}.$$

In the following theorem we collect the facts about quadratic forms with q even that we shall need, cf. [40, Theorem 7.2.9] and Section 6.2 of [35].

Theorem 2.6. *Let q be even and (Q,V) be a quadratic space over $\mathbb{F}_q$. Fix an element $d\in\mathbb{F}_q$ such that X^2+X+d is irreducible over $\mathbb{F}_q$. Write $n:=\dim(V)$, $r=\dim(\mathrm{rad}(Q))$, and denote by N_0 the number of $v\in V$ such that $Q(v)=0$. Then $n-r=2s$ is even and there is a basis of V such that the resulting quadratic form is one of the following:*

(i) $x_1x_2+x_3x_4+\cdots+x_{2s-1}x_{2s}$ *(hyperbolic),*
(ii) $x_1^2+x_1x_2+dx_2^2+x_3x_4+\cdots+x_{2s-1}x_{2s}$ *(elliptic),*
(iii) $x_0^2+x_1x_2+\cdots+x_{2s-1}x_{2s}$ *(parabolic),*

and $N_0=q^{n-1}+(q-1)q^{r+s-1}\epsilon$, where $\epsilon=1,\,-1,\,0$ in (i), (ii) and (iii) respectively. Moreover, (iii) occurs if and only if $Q(\mathrm{rad}(Q))\neq\{0\}$.

Corollary 2.7. *Let q be even and (Q,V) be a quadratic space over $\mathbb{F}_q$ with $\dim_{\mathbb{F}_q}V=n$. Then the number of $v\in V$ such that $Q(v)=0$ is q^{n-1} if and only if Q has odd rank.*

Proof. In Theorem 2.6, Q has even rank in case (i) and (ii), and has odd rank in case (iii). □

For $n\geq 1$, we define the trace function $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}:\mathbb{F}_{q^n}\mapsto\mathbb{F}_q$ by $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)=x+x^q+\cdots+x^{q^{n-1}}$. If a function $f:\mathbb{F}_{q^n}\mapsto\mathbb{F}_{q^n}$ satisfies that $f(\lambda x)=\lambda^d f(x)$ for some positive integer d and all $\lambda\in\mathbb{F}_q$ and $x\in\mathbb{F}_{q^n}$, then we call $f(X)$ a *homogeneous* polynomial of *degree* d over the subfield $\mathbb{F}_q$. Such a polynomial f naturally induces a map $\bar{f}:\mathbb{F}_{q^n}^*/\mathbb{F}_q^*\mapsto\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ such that $\bar{f}(\bar{x}):=\overline{f(x)}$ for each $\bar{x}=x\mathbb{F}_q^*$. In the case $\bar{f}$ is a bijection, we say that f induces a permutation of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ or simply say that f permutes $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$.

Lemma 2.8. *Let $Q(X)=\sum_{i,j}a_{ij}X^{q^i+q^j}\in\mathbb{F}_{q^n}[X]$ with q even. Then $Q(X)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $Q_y(x)=\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yQ(x))$ has odd rank for $y\neq 0$.*

Proof. If $Q(X)$ is a permutation polynomial of $\mathbb{F}_{q^n}$, then the size of $\{x:\ Q_y(x)=0\}$ is equal to that of $\{z:\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yz)=0\}$, which is q^{n-1} for $y\neq 0$. By Corollary 2.7, the quadratic form Q_y has odd rank for each $y\neq 0$. This proves the necessary part.

Now assume that Q_y has odd rank for each $y\neq 0$. Since q is even and $Q(X)$ is homogeneous of degree 2 over $\mathbb{F}_q$, it is easy to show that $Q(X)$ is a permutation polynomial if and only if it induces a permutation of the quotient group $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. We regard $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$, and identify the elements of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ with the projective points of $\mathrm{PG}(n-1,q)$ in the natural way. Each hyperplane of $\mathrm{PG}(n-1,q)$ is of the form $\{x\mathbb{F}_q^*:\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yx)=0\}$ for some $y\neq 0$, and $Q(x)\mathbb{F}_q^*$ lies on the hyperplane if and only if $Q_y(x)=0$. For each element $g\in\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$, we define $n(g):=\{x\in\mathbb{F}_{q^n}^*/\mathbb{F}_q^*:\ Q(x)\mathbb{F}_q^*=g\}$. For a set U of projective points, write $n(U):=\sum_{g\in U}n(g)$. If H is a hyperplane, then $n(H)=\frac{q^{n-1}-1}{q-1}$ by Corollary 2.7. For a fixed point $g\in\mathrm{PG}(n-1,q)$, let $H_1,\cdots,H_{\frac{q^{n-1}-1}{q-1}}$ be the set of hyperplanes containing it. As a multiset, $\bigcup_i H_i$ covers the point g exactly $\frac{q^{n-1}-1}{q-1}$ times and each other point $\frac{q^{n-2}-1}{q-1}$ times. We thus have

$$q^{n-2}\cdot n(g)+\frac{q^{n-2}-1}{q-1}\cdot\sum_{h\in\mathrm{PG}(n-1,q)}n(h)=\sum_i n(H_i)=\left(\frac{q^{n-1}-1}{q-1}\right)^2.$$

On the other hand, $\sum_{h\in\mathrm{PG}(n-1,q)}n(h)=\frac{q^n-1}{q-1}$. It follows that $n(g)=1$ for each g. Hence $Q(X)$ induces a permutation of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$, and so it permutes $\mathbb{F}_{q^n}$. This proves the sufficiency part. $\square$

The above lemma describes how to study the permutation behavior of a polynomial of DO type via quadratic forms. This is the technique that we will apply in Section 5.

3. A function approach to $\mathcal{C}$-planes and $\mathcal{H}$-planes

Let q be a prime power, $n\geq 2$ be an integer, and regard the finite field $\mathbb{F}_{q^{2n}}$ as a $2n$-dimensional vector space over $\mathbb{F}_q$. Let γ be a primitive element of $\mathbb{F}_{q^{2n}}$ and let $\sigma:\ x\mapsto x^p$ be the Frobenius automorphism. For each $a\in\mathbb{F}_{q^{2n}}^*$, we use $\Theta(a)$ for the linear map from $\mathbb{F}_{q^{2n}}$ to itself that maps x to ax. The group $\langle\Theta(\gamma)\rangle$ is a Singer group, and $\Gamma L(1,q^{2n})=\langle\Theta(\gamma)\rangle\rtimes\mathrm{Aut}(\mathbb{F}_{q^{2n}})$. Let $\mathcal{S}$ be a spread with ambient space $(\mathbb{F}_{q^{2n}},+)$ and kernel $\mathbb{F}_q$. The associated affine plane $\Pi(\mathcal{S})$ is flag-transitive if and only if $\mathrm{Aut}(\mathcal{S})$ is transitive on the components. If further $\mathrm{Aut}(\mathcal{S})$ is solvable, then it is isomorphic to a subgroup of $\Gamma L(1,q^{2n})$. After taking an isomorphic spread if necessary, we assume that $\mathrm{Aut}(\mathcal{S})$ is a subgroup of $\langle\Theta(\gamma)\rangle\rtimes\mathrm{Aut}(\mathbb{F}_{q^{2n}})$. If the Singer subgroup $\mathrm{Aut}(\mathcal{S})\cap\langle\Theta(\gamma)\rangle$ has order $\frac{q^n+1}{2}$ or q^n+1 respectively, then we call $\mathcal{S}$ a spread of *type* $\mathcal{H}$ or *type* $\mathcal{C}$ and the corresponding plane $\Pi(\mathcal{S})$ a $\mathcal{H}$-*plane* or a $\mathcal{C}$-plane respectively. All the known flag-transitive affine planes with a solvable full collineation group are either $\mathcal{C}$-planes or $\mathcal{H}$-planes, and there are no other such planes of order at most 125. The following result summarizes Lemma 1 and the subsequent comments in [22], restricting to the solvable case.

Lemma 3.1. *Let $q=p^e$ with p prime and $n\geq 2$ be an integer. If $\mathcal{S}$ is a spread of $(\mathbb{F}_{q^{2n}},+)$ with kernel $\mathbb{F}_q$ such that $\mathrm{Aut}(\mathcal{S})$ is solvable and transitive on the components, then $\mathcal{S}$ is either of type $\mathcal{H}$ or of type $\mathcal{C}$ provided that $\gcd(\frac{q^n+1}{2},ne)=1$ in the case p is odd and $\gcd(q^n+1,ne)=1$ in the case $p=2$.*

The above lemma indicates that $\mathcal{C}$-planes and $\mathcal{H}$-planes are the only possibilities under a mild number theoretical condition in the solvable case, and it is an open problem whether the gcd condition can be dropped. In this paper, we will focus on $\mathcal{C}$-planes and $\mathcal{H}$-planes. *Throughout the paper, we fix the following notation.* Take β to be an element of order $(q^n+1)(q-1)$. Let $\mathcal{S}$ be a spread of type $\mathcal{H}$ or type $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{S})\cap\langle\Theta(\gamma)\rangle=\langle\Theta(\beta^2)\rangle$ or $\langle\Theta(\beta)\rangle$ respectively.

Let W be a component of $\mathcal{S}$, so that $\mathcal{S} = \{g(W) : g \in \mathrm{Aut}(\mathcal{S})\}$. Since the number of $\mathbb{F}_{q^n}$-subspaces of $\mathbb{F}_{q^{2n}}$ is $q^n + 1$, there exists $\delta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that $W \cap \mathbb{F}_{q^n} \cdot \delta = \{0\}$. From the decomposition $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^n} \cdot \delta$, we can write the $\mathbb{F}_q$-subspace W as follows:

$$W = \{x + \delta \cdot L(x) : x \in \mathbb{F}_{q^n}\}, \tag{3.1}$$

where $L(X) \in \mathbb{F}_{q^n}[X]$ is a reduced q-polynomial. We also define

$$Q(X) := (X + \delta L(X)) \cdot (X + \delta^{q^n} L(X)), \tag{3.2}$$

which is a DO polynomial over $\mathbb{F}_{q^n}$. The following is our key lemma.

Lemma 3.2. *Take notation as above, and let W be the $\mathbb{F}_q$-subspace in* (3.1).

(1) *If q is odd, then the orbit of W under the group $\langle\Theta(\beta^2)\rangle$ forms a partial spread if and only if $Q(x)$ is a planar function over $\mathbb{F}_{q^n}$.*
(2) *If q is odd, then the orbit of W under the group $\langle\Theta(\beta)\rangle$ forms a spread if and only if $x \mapsto Q(x)$ induces a permutation of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$.*
(3) *If q is even, then the orbit of W under the group $\langle\Theta(\beta)\rangle$ forms a spread if and only if $x \mapsto Q(x)$ is a permutation of $\mathbb{F}_{q^n}$.*

Proof. We first prove (1). The orbit of W under $\langle\Theta(\beta^2)\rangle$ forms a partial spread if and only if the following holds: $y + \delta L(y) = \beta^{2i}(x + \delta L(x)) \neq 0$ occurs only in the case $\beta^{2i} \in \mathbb{F}_q^*$ and $y = \beta^{2i}x$. First assume that we get a partial spread from W as described. If $Q(x) = Q(y)$ for $xy \neq 0$, then $s_1^{q^n+1} = 1$, where $s_1 = \frac{y+\delta L(y)}{x+\delta L(x)}$. Since $s_1 \in \langle\beta^2\rangle$, it follows from our assumption that $s_1 \in \mathbb{F}_q^*$ and $y = s_1 x$. Since $\gcd(q^n + 1, q - 1) = 2$, we get $s_1^2 = 1$, i.e., $s_1 = \pm 1$. We thus have shown that $x \mapsto Q(x)$ is 2-to-1, and it follows that $Q(x)$ is planar by Lemma 2.4. Conversely, assume that $Q(x)$ is a planar function. If $y + \delta L(y) = \beta^{2i}(x + \delta L(x)) \neq 0$, then taking norm we get $Q(y) = \beta^{2(q^n+1)i}Q(x) = Q(\beta^{(q^n+1)i}x)$. It follows from Lemma 2.4 that $y = \pm\beta^{(q^n+1)i}x$. Plugging this into $y + \delta L(y)$, we get $\pm\beta^{(q^n+1)i} = \beta^{2i}$. This gives that $\beta^{2i(q^n-1)} = 1$, i.e., $\beta^{2i} \in \mathbb{F}_{q^n}^*$. It is easy to show that $\langle\beta^2\rangle \cap \mathbb{F}_{q^n}^* = \mathbb{F}_q^*$, so $\beta^{2i} \in \mathbb{F}_q^*$. The conclusion now follows.

We next prove (2). Since $Q(\lambda x) = \lambda^2 Q(x)$ for $\lambda \in \mathbb{F}_q$, the map $x \mapsto Q(x)$ induces a function from $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ to itself. Observe that $\langle\beta\rangle$ is the set of elements in $\mathbb{F}_{q^{2n}}^*$ whose relative norm to $\mathbb{F}_{q^n}$ is in $\mathbb{F}_q^*$. The orbit of W under $\langle\Theta(\beta)\rangle$ forms a spread if and only if the following holds: $y+\delta L(y) = \beta^i(x+\delta L(x)) \neq 0$ occurs only in the case $\beta^i \in \mathbb{F}_q^*$ and $y = \beta^i x$. First assume that we get a spread from W as described. If $Q(x)/Q(y) \in \mathbb{F}_q^*$ for $xy \neq 0$, then $y+\delta L(y) = s_1(x+\delta L(x))$ for some $s_1 \in \langle\beta\rangle$. It follows that $s_1 \in \mathbb{F}_q^*$ and $y = s_1 x$. Hence $Q(x)$ permutes $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. Conversely, assume that $Q(x)$ permutes $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. If $y + \delta L(y) = \beta^i(x + \delta L(x)) \neq 0$, then taking norm we get $Q(y)/Q(x) = \beta^{i(1+q^n)} \in \mathbb{F}_q^*$. It follows that $y/x \in \mathbb{F}_q^*$, and the conclusion follows.

The claim (3) can be proved similarly, and we omit the details. □

Corollary 3.3. *Let W be the $\mathbb{F}_q$-subspace in* (3.1), *and assume that q and n are odd. If the orbit of W under $\langle\Theta(\beta^2)\rangle$ forms a partial spread, then its orbit under $\langle\Theta(\beta)\rangle$ forms a spread of type $\mathcal{C}$.*

Proof. By the previous lemma, we see that $Q(x)$ is a planar function, and so $x \mapsto Q(x)$ is 2-to-1 by Lemma 2.4. Denote by D the image set $\{Q(x) : x \neq 0\}$, and write E for its complement in $\mathbb{F}_{q^n}^*$. For a nonsquare $\lambda \in \mathbb{F}_q^*$, we have $E = \lambda \cdot D$ by [48, Proposition 3.6]. In particular, $Q(y)/Q(x) \in \mathbb{F}_q^*$ implies that $Q(y)/Q(x) = u^2$ for some $u \in \mathbb{F}_q^*$. The 2-to-1 property of Q then gives that $y/x = \pm u \in \mathbb{F}_q^*$. This shows that $Q(x)$ permutes $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. The claim then follows from claim (2) in Lemma 3.2. □

Theorem 3.4. *There is no type $\mathcal{C}$ spread with ambient space $(\mathbb{F}_{q^{2n}}, +)$ and kernel $\mathbb{F}_q$ when n is even and q is odd.*

Proof. We take notation introduced preceding Lemma 3.2 and prove by contradiction. By claim (2) in Lemma 3.2, $x \mapsto Q(x)$ induces a permutation of $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. By [48, Lemma 3.3], $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Q(x))$ is a nondegenerate quadratic form over $\mathbb{F}_q$. By [35, Theorem 6.26], the number $N_0 = \#\{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Q(x)) = 0\}$ is equal to $q^{n-1} \pm (q-1)q^{n/2-1}$. On the other hand, $N_0 = \#\{y \in \mathbb{F}_{q^n} : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(y) = 0\} = q^{n-1}$ by the fact that $Q(x)$ permutes $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. This contradiction completes the proof. □

In the case q is odd, we may further restrict the form of W.

Lemma 3.5. *Let $\mathcal{S}$ be a spread such that* $\mathrm{Aut}(\mathcal{S}) \cap \langle \Theta(\gamma)\rangle$ *contains* $\langle\Theta(\beta^2)\rangle$*, and let W be a component. If q is odd and $\delta^{q^n-1} = -1$, then W intersects $\mathbb{F}_{q^n}$ or $\mathbb{F}_{q^n} \cdot \delta$ trivially.*

Proof. From the decomposition $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^n} \cdot \delta$, we can write $W = \{L_1(x) + \delta L_2(x) : x \in \mathbb{F}_{q^n}\}$ for some q^n-polynomials $L_1(X)$, $L_2(X)$. The argument in Lemma 3.2 shows that $Q(x) = L_1(x)^2 - \delta^2 L_2(x)^2$ is planar. By Lemma 2.5, at least one of L_1, L_2 is a permutation, and correspondingly W intersects one of $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^n} \cdot \delta$ trivially. □

Remark 3.6. *In Lemma 3.5, if* $\mathrm{Aut}(\mathcal{S})$ *is transitive, then* $\mathcal{S}' = \{g(\delta \cdot W) : g \in \Theta(\delta) \cdot \mathrm{Aut}(\mathcal{S}) \cdot \Theta(\delta)^{-1}\}$ *is a spread isomorphic to $\mathcal{S}$ and* $\mathrm{Aut}(\mathcal{S}')$ *contains* $\langle\Theta(\beta^2)\rangle$*. So after replacing W by $\delta \cdot W$ if necessary, we always assume that $\delta^{q^n-1} = -1$ in* (3.1) *in the case q is odd.*

The Kantor-Suetake family constitutes a major part of the known non-Desarguesian flag-transitive affine planes of odd order. As a first application of our new approach, we give a characterization of this important family based on the following result of Menichetti. Please refer to [1, 26] for details on generalized twisted fields.

Theorem 3.7. [37, 38] *Let S be a finite semifield of prime dimension n over the nucleus $\mathbb{F}_q$. Then there is an integer $\nu(n)$ such that if $q \ge \nu(n)$ then S is isotopic to a finite field or a generalized twisted field. Moreover, we have $\nu(3) = 0$.*

By [26, Proposition 11.31], which is essentially due to Albert [2, 3], a generalized twisted field that has a commutative isotope must be isotopic to the commutative presemifield defined by a planar function x^{1+p^α} over $\mathbb{F}_{p^e}$, where $1 \le \alpha \le n-1$ and $e/\gcd(e,\alpha)$ is odd. The following result characterizes planar functions whose associated presemifield is isotopic to a commutative twisted field or a finite field, see [16, Corollaries 3.9, 3.10].

Lemma 3.8. *Let p be an odd prime and $q = p^e$. Let f be a planar function of DO type over $\mathbb{F}_q$ and $S_f = (\mathbb{F}_q, +, *)$ be the associated presemifield with $x * y = f(x+y) - f(x) - f(y)$. There exist linearized permutation polynomials M_1 and M_2 such that*

1. *if S_f is isotopic to a finite field, then $f(M_2(x)) \equiv M_1(x^2)$ for $x \in \mathbb{F}_q$;*
2. *if S_f is isotopic to a commutative twisted field, then $f(M_2(x)) = M_1(x^{p^\alpha+1})$ for $x \in \mathbb{F}_q$, where α is an integer such that $1 \le \alpha \le e-1$ and $e/\gcd(e,\alpha)$ is odd.*

Lemma 3.9. *Let n be an odd prime, $\nu(n)$ be as in Theorem 3.7, and let q be an odd prime power such that $q \ge \nu(n)$. Suppose that the orbit of $W = \{x + \delta \cdot L(x) : x \in \mathbb{F}_{q^n}\}$ under $\langle\Theta(\beta^2)\rangle$ forms a partial spread, where $\delta^{q^n-1} = -1$ and $L(X)$ is a q-polynomial over $\mathbb{F}_{q^n}$. Then $W = \{\alpha \cdot (x + u\delta x^{q^i}) : x \in \mathbb{F}_{q^n}\}$ for some $\alpha \in \mathbb{F}_{q^{2n}}^*$, $u \in \mathbb{F}_{q^n}$ and $0 \le i \le n-1$.*

Proof. By Lemma 3.2, $Q(x) = x^2 - \delta^2 L(x)^2$ is a planar function. By Theorem 3.7, the associated presemifield S_Q is isotopic to a finite field or a commutative twisted field under the conditions in the lemma. By Lemma 3.8, there are reduced linearized permutation polynomials M_1, M_2 such that

$$M_1(X^2) \equiv M_2(X)^2 - \delta^2 L(M_2(X))^2 \pmod{X^{q^n} - X}, \tag{3.3}$$

or

$$M_1(X^{1+p^\alpha}) \equiv M_2(X)^2 - \delta^2 L(M_2(X))^2 \pmod{X^{q^n} - X}, \tag{3.4}$$

where $q=p^e$ with p prime, $1\le\alpha\le ne-1$ and $\frac{ne}{\gcd(ne,\alpha)}$ is odd. Write $M_2(X)=\sum_{i=0}^{ne-1}a_iX^{p^i}$, $L(M_2(X))\equiv\sum_{i=0}^{ne-1}b_iX^{p^i} \pmod{X^{q^n}-X}$, and set $I=\{i:\,a_i\neq 0\}$, $J=\{i:\,b_i\neq 0\}$.

Comparing coefficients of x^{2p^i} in (3.4), we see that $0=a_i^2-\delta^2b_i^2$ for $0\le i\le ne-1$. Since δ^2 is a nonsquare in $\mathbb{F}_{q^n}^*$, all the a_i's and b_j's are zero. This contradicts the assumption that M_2 is a permutation polynomial, so (3.4) can not occur. It remains to check (3.3). We look at the coefficients of $x^{p^i+p^j}$, $0\le i<j\le ne-1$, on both sides and get $a_ia_j=\delta^2b_ib_j$. If $|I|\ge 2$ or $|J|\ge 2$, then it is easy to deduce that $I=J$. If both I and J have size at most 1, then L is a monomial and W takes the desired form with $\alpha=1$. We assume that $I=J$ and they have size at least two below. In this case, for any distinct $i,j\in I$, exactly one of $\{a_ib_i^{-1},\,a_jb_j^{-1}\}$ is a square and the other is a nonsquare, since δ^2 is a nonsquare in $\mathbb{F}_{q^n}^*$. This is only possible when $|I|=2$. Therefore, $M_2(X)=aX^{p^k}+bX^{p^\ell}$, $L(M_2(X))=cX^{p^k}+dX^{p^\ell}$ for some $0\le k<\ell\le ne-1$ and $a,b,c,d\in\mathbb{F}_{q^n}^*$ such that $ab=\delta^2cd$. Since $x\mapsto M_2(x)$ is a permutation, the elements of W can be written as

$$M_2(x)+\delta\cdot L(M_2(x))=(a+\delta c)\cdot(y+\delta da^{-1}y^{p^{\ell-k}}),\ y=x^{p^k}.$$

Since W is a $\mathbb{F}_q$-linear subspace, $p^{\ell-k}$ is a power of q. This completes the proof. $\square$

Remark 3.10. *Let q be an odd prime power, w be a nonsquare of $\mathbb{F}_q$, and $N>1$ be an integer. Let $\mathbf{a}=(a_0,a_1\cdots,a_{N-1})$ and $\mathbf{b}=(b_0,b_1,\cdots,b_{N-1})$ be two sequences consisting of elements in $\mathbb{F}_q$, and define their supports as $I_1=\{i:\,a_i\neq 0\}$, $I_2=\{i:\,b_i\neq 0\}$ respectively. As in the proof of Lemma 3.9, we can show that: if $a_ia_j=wb_ib_j$ for any distinct i, j, then either both $|I_1|$ and $|I_2|$ have size at most one or $I_1=I_2$ and both have size 2.*

Theorem 3.11. *Let n be an odd prime, $\nu(n)$ be as in Theorem 3.7, and let q be an odd prime power such that $q\ge\nu(n)$. A type $\mathcal{C}$ spread $\mathcal{S}$ of $(\mathbb{F}_{q^{2n}},+)$ with kernel $\mathbb{F}_q$ is isomorphic to the orbit of $W=\{x+\delta\cdot x^{q^i}\,:\,x\in\mathbb{F}_{q^n}\}$ under $\langle\Theta(\beta)\rangle$ for some δ and i such that $\delta^{q^n-1}=-1$, $1\le i\le n-1$ and $\gcd(i,n)=1$.*

Proof. Let W be a component of $\mathcal{S}$ such that $\mathcal{S}$ is the orbit of W under the Singer subgroup $\langle\Theta(\beta)\rangle$. By the remark following Lemma 3.5, up to isomorphism $W=\{x+\delta' L(x):\,x\in\mathbb{F}_{q^n}\}$ for some q-polynomial $L(X)$ and δ' such that $\delta'^{q^n-1}=-1$. By Lemma 3.9, $W=\{\alpha\cdot(x+u\delta' x^{q^i}):\,x\in\mathbb{F}_{q^n}\}$ for some $\alpha\in\mathbb{F}_{q^{2n}}^*$ and $u\in\mathbb{F}_{q^n}^*$. Its orbit under $\langle\Theta(\beta)\rangle$ is a spread isomorphic to the one described in the theorem with $\delta=u\delta'$. The kernel contains the fixed subfield of $x\mapsto x^{q^i}$, so we have $\gcd(i,n)=1$. $\square$

Theorem 3.12. *Let n be an odd prime, $\nu(n)$ be as in Theorem 3.7, and let q be an odd prime power such that $q\ge\nu(n)$. A type $\mathcal{H}$ spread $\mathcal{S}$ of $(\mathbb{F}_{q^{2n}},+)$ with kernel $\mathbb{F}_q$ is isomorphic to the orbit of $\{x+\delta x^{q^k}\,:\,x\in\mathbb{F}_{q^n}\}$ under the group A generated by $\langle\Theta(\beta^2)\rangle$ and $\psi:\,z\mapsto\eta z^{q^n}$, where $1\le k\le n-1$, $\gcd(k,n)=1$, $\delta^{q^n-1}=-1$, $\eta^{(1+q^n)(q^k-1)}=1$ and η is a nonsquare.*

Proof. Write $q=p^e$ with p prime. By Lemma 3.9, under the conditions in the theorem a spread $\mathcal{S}$ of type $\mathcal{H}$ is isomorphic to the orbit of $W=\{x+\delta\cdot x^\tau\,:\,x\in\mathbb{F}_{q^n}\}$ under $\mathrm{Aut}(\mathcal{S})$, where $\delta^{q^n-1}=-1$, $\tau=q^k$ with $1\le k\le n-1$ and $\gcd(k,n)=1$, and $\mathrm{Aut}(\mathcal{S})\cap\langle\Theta(\gamma)\rangle=\langle\Theta(\beta^2)\rangle$. There exists $\psi\in\mathrm{Aut}(\mathcal{S})$ that permutes the two $\langle\Theta(\beta^2)\rangle$-orbits by the transitivity of $\mathrm{Aut}(\mathcal{S})$ on the components, so the spread $\mathcal{S}$ consists of the orbit of W under the subgroup $A:=\langle\Theta(\beta^2),\,\psi\rangle$. By elementary group theory,

$$\mathrm{Aut}(\mathcal{S})/\langle\Theta(\beta^2)\rangle\cong\mathrm{Aut}(\mathcal{S})\cdot\langle\Theta(\gamma)\rangle/\langle\Theta(\gamma)\rangle\le\langle\Theta(\gamma)\rangle\rtimes\mathrm{Aut}(\mathbb{F}_{q^{2n}})/\langle\Theta(\gamma)\rangle\cong\mathrm{Aut}(\mathbb{F}_{q^{2n}}).$$

Since any odd power of ψ also permutes the two $\langle\Theta(\beta^2)\rangle$-orbits, we can assume that the order of $\overline{\psi}\in\mathrm{Aut}(\mathcal{S})/\langle\Theta(\beta^2)$ is a power of 2. Write $\psi(z)=\eta z^\sigma$, where $\sigma=p^\ell$ $(1\le\ell\le 2ne-1)$ and $\eta\in\mathbb{F}_{q^{2n}}^*$. We now derive conditions on ψ to guarantee that the orbit of W under the subgroup A forms a spread. To be specific, we need to make sure the following hold:

(1) $\psi^2(W)=\beta^{2i}\cdot W$ for some i, since ψ^2 stabilizes the $\langle\Theta(\beta^2)\rangle$-orbits;
(2) $\psi(W)$ intersects each of $\beta^{2i}\cdot W$, $0\le i\le\frac{q^n-1}{2}$, trivially.

We fist consider the condition (1). Assume that $\psi^2(W)=\beta^{2i}\cdot W$ for some i. This means that for each $x\in\mathbb{F}_{q^n}$, there exists $y\in\mathbb{F}_{q^n}$ such that $\eta^{1+\sigma}\left(x+\delta x^\tau\right)^{\sigma^2}=\beta^{2i}(y+\delta y^\tau)$. Write $\eta^{1+\sigma}\beta^{-2i}=u+v\delta$ for some $u,v\in\mathbb{F}_{q^n}$. Expanding and comparing the coefficients of the basis $\{1,\delta\}$, we get $y=ux^{\sigma^2}+v\delta^{\sigma^2+1}x^{\tau\sigma^2}$, $y^\tau=u\delta^{\sigma^2-1}x^{\tau\sigma^2}+vx^{\sigma^2}$. Canceling out y, we see that $(u^\tau-u\delta^{\sigma^2-1})x^{\tau\sigma^2}+v^\tau\delta^{\tau(\sigma^2+1)}x^{\tau^2\sigma^2}-vx^{\sigma^2}=0$ for all x. Hence, the reduced polynomial $(u^\tau-u\delta^{\sigma^2-1})X^{\tau\sigma^2}+v^\tau\delta^{\tau(\sigma^2+1)}X^{\tau^2\sigma^2}-vX^{\sigma^2} \pmod{X^{q^n}-X}$ is the zero polynomial. Since $\tau\ne 1$ and n is odd, the reduced monomial $X^{\sigma^2} \pmod{X^{q^n}-X}$ occurs only once. This gives $v=0$, and the remaining coefficient gives $u^{\tau-1}=\delta^{\sigma^2-1}$. Raising both sides of $\eta^{1+\sigma}\beta^{-2i}=u$ to the $\frac{1}{2}(q^n+1)(\tau-1)$-st power, we get $\eta^{(q^n+1)(\tau-1)(1+\sigma)/2}=u^{\tau-1}$, so it must hold that

$$\eta^{(1+q^n)(\tau-1)(1+\sigma)/2}=\delta^{\sigma^2-1}. \tag{3.5}$$

Conversely, if (3.5) is true, then (1) holds with $\beta^{2i}=\eta^{(1-q^n)(1+\sigma)/2}$ by direct check. To summarize, we have shown that (1) holds if and only if (3.5) holds.

We claim that $\gcd(e,\ell)=r$, $\delta_0^{(p^r-1)/2}=-1$ and $\eta^{(1+q^n)(\tau-1)}=\delta^{2(\sigma-1)}$, where $r=\gcd(e,2\ell)$, and $\delta_0=\delta^{2(q^n-1)/(q-1)}$. By raising both sides of (3.5) to the $\left(\frac{q^n-1}{q-1}\right)$-th power we get $\delta_0^{(p^{2\ell}-1)/2}=1$. It follows from $\gcd(p^{2\ell}-1,p^e-1)=p^r-1$ that $\delta_0^{p^r-1}=1$. On the other hand, δ^2 is a nonsquare in $\mathbb{F}_{q^n}^*$, so $\delta_0^{(p^e-1)/2}=-1$. Now, we see that δ_0 has order dividing $\gcd(\frac{p^{2\ell}-1}{2},p^r-1)$ which is equal to either p^r-1 or $(p^r-1)/2$. The latter case will not occur, since it would lead to the contradiction $\delta_0^{(p^e-1)/2}=1$. Hence p^r-1 divides $\frac{p^{2\ell}-1}{2}$, which is the case only if $2\ell/r$ is even, i.e., $r|\ell$. This shows that $r=\gcd(e,\ell)$ and $\delta_0^{(p^r-1)/2}=-1$. It is clear that $g:=\gcd\left(\frac{q^n-1}{q-1},\frac{\sigma+1}{2}\right)$ divides $\gcd(p^{ne}-1,p^{2\ell n}-1)=p^{\gcd(ne,2\ell n)}-1=p^{nr}-1$, so it also divides $\gcd(p^{n\ell}-1,p^\ell+1)=2$. On the other hand, $\frac{q^n-1}{q-1}$ is odd, so $g=1$. It follows from (3.5) that $\eta^{(1+q^n)(\tau-1)}=\delta^{2(\sigma-1)}$.

We now consider the condition (2). Recall that $\langle\beta\rangle$ is the set of elements of $\mathbb{F}_{q^{2n}}^*$ whose relative norm to $\mathbb{F}_{q^n}$ is in $\mathbb{F}_q^*$. The condition amounts to that $\eta^{1+q^n}Q(x)^\sigma=\lambda^2Q(y)$ does not hold for any $x,y\in\mathbb{F}_{q^n}^*$ and $\lambda\in\mathbb{F}_q^*$, where Q is as defined in (3.2). By expanding $\eta^{1+q^n}Q(x)^\sigma=\lambda^2Q(y)$ and rearranging terms, we get $Y=\delta^2Y^\tau$ with $Y=\eta^{1+q^n}x^{2\sigma}-\lambda^2y^2\in\mathbb{F}_{q^n}$. Here we have made use of the fact that $\eta^{(1+q^n)(\tau-1)}=\delta^{2(\sigma-1)}$. If $Y\ne 0$, then $Y^{1-\tau}$ is a square while δ^2 is not, which is impossible. We thus must have $Y=0$. It is clear that $Y=0$ has a solution $(x,y,\lambda)\in\mathbb{F}_{q^n}^*\times\mathbb{F}_{q^n}^*\times\mathbb{F}_q^*$ if and only if η^{1+q^n} is a square in $\mathbb{F}_{q^n}^*$. To summarize, (2) holds only if η^{1+q^n} is a nonsquare in $\mathbb{F}_{q^n}^*$.

Let e' be the highest power of 2 that divides e. It follows from $r=\gcd(e,\ell)=\gcd(e,2\ell)$ that e/r is odd, i.e., $e'|r$. Hence ℓ is a multiple of e'. Recall that the order of $\overline{\psi}$ is a power of 2, so ℓ is a multiple of ne. On the other hand, $0<\ell<2ne$ implies that $\ell=ne$. In this case, $r=e$, and the conditions reduce to the same as stated in the theorem.

The sufficiency part of the theorem is shown in [29, 31]. □

The spreads described in Theorem 3.11 and Theorem 3.12 are due to Kantor and Suetake [29, 31]. The case $n=3$ has been characterized by Baker and Ebert et al in a series of papers [5, 6, 7, 10] by a geometric approach. It is well-known that a two-dimensional finite semifield is a finite field [20], so the same arguments in this section can be applied to characterize the case $n=2$ which has been dealt with in [9].

4. Planar functions of the form $L(x)^2-wx^2$

In Section 3, we have shown that $\mathcal{C}$-planes and $\mathcal{H}$-planes of odd order have close connections with planar functions of the form $X^2-\delta^2L(X)^2$ over $\mathbb{F}_{q^n}$, where $\delta^{q^n-1}=-1$. In this section, we study the properties of the commutative semifields associated with such planar functions and determine the planarity of functions of particular forms. Throughout this section, we shall fix the following notation. For convenience, we write alternatively $Q(X) = L(X)^2 - wX^2$, where $w(=\delta^{-2})$ is a nonsquare in $\mathbb{F}_{q^n}$ and $L(X)$ is a reduced q-polynomial such that

$$\{\lambda \in \mathbb{F}_{q^n} : L(\lambda x) = \lambda L(x) \text{ for all } x \in \mathbb{F}_{q^n}\} = \mathbb{F}_q, \tag{4.1}$$

Assume that $Q(X)$ is a planar function over $\mathbb{F}_{q^n}$. Then

$$x \mapsto \frac{1}{2}\left(Q(x+1) - Q(x) - Q(1)\right) = L(1)L(x) - wx$$

is a $\mathbb{F}_q$-linear bijection of $\mathbb{F}_{q^n}$ by definition. Let L_1 be its inverse under composition, which is also $\mathbb{F}_q$-linear. Denote by $S_Q = (\mathbb{F}_{q^n}, +, \circ)$ the associated semifield with multiplication

$$x \circ y = L(L_1(x))L(L_1(y)) - wL_1(x)L_1(y), \tag{4.2}$$

The multiplicative identity is $e_Q = L(1)^2 - w$, and $\mathcal{N}(S_Q)$ contains $\mathbb{F}_q \cdot e_Q$. We have $(ae_Q) \circ z = az$ for $a \in \mathbb{F}_q$ and $z \in \mathbb{F}_{q^n}$. Let q^m and q^r be the sizes of $\mathcal{N}_m(S_Q)$ and $\mathcal{N}(S_Q)$ respectively.

We now explicitly construct a commutative isotope of S_Q that has $\mathbb{F}_{q^m}$ as the middle nucleus. For each $x \in S_Q$, let R_x be the $\mathbb{F}_q$-linear map over $(\mathbb{F}_{q^n}, +)$ such that $R_x(z) = z \circ x$. For $u \in \mathcal{N}_m(S_Q)$ and $i \geq 1$, we use $u^{\circ i}$ for the product of i copies of u under the multiplication $\circ$, and set $u^{\circ 0} := e_Q$. Let z' be a fixed primitive element of $\mathbb{F}_{q^m}$ with minimal polynomial $X^m + \sum_{i=0}^{m-1} c_i X^i$ over $\mathbb{F}_q$. The map $a \mapsto ae_Q$ is a field isomorphism between $(\mathbb{F}_q, +, \cdot)$ and $(\mathbb{F}_q \cdot e_Q, +, \circ)$, and it naturally extends to a ring isomorphism between their polynomial rings. Therefore, there exists a primitive element $z \in \mathcal{N}_m(S_Q)$ such that $z^{\circ m} + \sum_{i=0}^{m-1}(c_i e_Q) \circ z^{\circ i} = 0$. Let $\{f_1 = e_Q, f_2 \cdots, f_{n/m}\}$ and $\{f_1' = 1, f_2' \cdots, f_{n/m}'\}$ be a basis of $(\mathbb{F}_{q^n}, +)$ over $\mathcal{N}_m(S_Q)$ and $\mathbb{F}_{q^m}$ respectively. Now define a $\mathbb{F}_q$-linear map $\psi : (\mathbb{F}_{q^n}, +) \mapsto (\mathbb{F}_{q^n}, +)$ such that

$$\psi(z'^i f_j') = z^{\circ i} \circ f_j, \quad 0 \leq i \leq m-1,\ 1 \leq j \leq n/m.$$

Here, $\mathbb{F}_q$-linearity means that $\psi(\lambda x) = \lambda\psi(x)$ for $\lambda \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$. The map ψ is a bijection and has the properties: (1) The restriction $\psi|_{\mathbb{F}_{q^m}}$ is a field isomorphism between $\mathbb{F}_{q^m}$ and $\mathcal{N}_m(S_Q)$; (2) $\psi(ax) = \psi(a) \circ \psi(x)$, i.e., $\psi^{-1}R_{\psi(a)}\psi(x) = ax$, for $a \in \mathbb{F}_{q^m}$ and $x \in \mathbb{F}_{q^n}$. By the definition of the nucleus, $R_{\psi(y)}R_{\psi(a)} = R_{\psi(a)}R_{\psi(y)}$ for $a \in \mathbb{F}_{q^r}$ and $y \in \mathbb{F}_{q^n}$, so $\psi^{-1}R_{\psi(y)}\psi$ is $\mathbb{F}_{q^r}$-linear for each y by (2). On the other hand, $\psi^{-1}(\psi(y) \circ \psi(x)) = \psi^{-1}R_{\psi(y)}\psi(x)$ is symmetric in x, y, so it is $\mathbb{F}_{q^r}$-linear in both x and y. Therefore, $\psi^{-1}(\psi(y) \circ \psi(x)) = x *_K y$, where $x *_K y = \sum_{i,j} c_{ij} x^{q^{ri}} y^{q^{rj}}$ for some constants c_{ij}'s such that $c_{ij} = c_{ji}$. It follows that $\psi(x) \circ \psi(y) = \psi(x *_K y)$ and also $a *_K x = ax$ for $a \in \mathbb{F}_{q^m}$ by (2). The algebraic system $S_K := (\mathbb{F}_{q^n}, +, *_K)$ is a semifield isotopic to S_Q, and its middle nucleus is $\mathbb{F}_{q^m}$.

We write $K(X) = \sum_{i,j=0}^{n/r-1} c_{ij} X^{q^{ri}+q^{rj}}$, so that $K(x) = x *_K x$ for $x \in \mathbb{F}_{q^n}$. Let $M_1(X), M_2(X)$ be the reduced q-polynomials s.t. $M_1(x) = L(L_1(\psi(x)))$ and $M_2(x) = L_1(\psi(x))$ for $x \in \mathbb{F}_{q^n}$ respectively. Applying the map $x \mapsto L(1)L(x) - wx$ to both sides of $M_2(x) = L_1(\psi(x))$, we get $\psi(x) = L(1)M_1(x) - wM_2(x)$. Now $\psi(x) \circ \psi(x) = \psi(x *_K x)$ takes the form

$$M_1(X)^2 - wM_2(X)^2 \equiv L(1)M_1(K(X)) - wM_2(K(X)) \pmod{X^{q^n} - X}. \tag{4.3}$$

Lemma 4.1. *Let q be an odd prime power, $n \geq 2$ be an integer, and w be a nonsquare in $\mathbb{F}_{q^n}$. Suppose that $L(X)$ is a reduced q-polynomial over $\mathbb{F}_{q^n}$ such that* (4.1) *holds. If $Q(x) = L(x)^2 - wx^2$ is planar over $\mathbb{F}_{q^n}$, then the semifield $S_Q = (\mathbb{F}_{q^n}, +, \circ)$ with multiplication as defined in* (4.2) *is either isotopic to a finite field or has nucleus equal to $\mathbb{F}_q$.*

Proof. We use the notation introduced preceding the lemma, and write $s = n/r$. The semifield S_Q is isotopic to a finite field if and only $r = n$, so we assume that $1 < r < n$ and try to derive a contradiction. First we introduce some notation for the proof. For a reduced q-polynomial $f(X) \in \mathbb{F}_{q^n}[X]$, we have a unique decomposition

$$f(X) = f_0(X) + f_1(X^q) + \cdots + f_{r-1}(X^{q^{r-1}}),$$

where the f_i's are reduced q^r-polynomials. We call it the *q^r-decomposition* of f, and call f_i the *i-th component*. For $t \in \{1, 2\}$, write $M_t(X) = \sum_{i=0}^{n-1} a_{i,t} X^{q^i}$, and define

$$I_t := \{0 \le i \le r-1 : \text{ one of } a_{i,t},\, a_{i+r,t}, \cdots, a_{i+(s-1)r,t} \text{ is nonzero}\}.$$

We comment that $i \in I_t$ if and only if M_t has a nonzero i-th component in its q^r-decomposition. Since M_2 is a permutation and L is not the zero polynomial, both I_1 and I_2 are nonempty. Observe that for $i \not\equiv j \pmod r$, the coefficient of $X^{q^i+q^j}$ is zero on the right hand side of (4.3), so we have $a_{i1}a_{j1} = w a_{i2}a_{j2}$ from the left hand side. We can pick two subsequences of length r whose supports are I_1 and I_2 from the coefficients of $M_1(X)$ and $M_2(X)$ respectively, satisfying the conditions in Remark 3.10. It follows that each of I_1 and I_2 has size at most 2 and $I_1 = I_2$ when one of them has size 2.

We first consider the case $|I_1| = |I_2| = 1$. In this case, we have $M_t(X) = U_t(X^{q^{r_t}})$ for $t \in \{1, 2\}$, where U_1 and U_2 are q^r-polynomials, and $0 \le r_1, r_2 \le r-1$. Set $r_3 := r_1 - r_2 \pmod r$. Since $M_1(X) \equiv L(M_2(X)) \pmod{X^{q^n} - X}$, the q^r-decomposition of $L(X)$ has exactly one nonzero component, namely the r_3-rd. We have $r_3 \neq 0$: otherwise $L(X)$ is q^r-polynomial, contradicting (4.1). By comparing exponents of the monomials in (4.3), we get $M_1(x)^2 = L(1)M_1(K(x))$ and $M_2(x)^2 = M_2(K(x))$ for $x \in \mathbb{F}_{q^n}$. Applying L to both sides of the second equation, we get $L(M_2(x)^2) = M_1(K(x))$. Recall that $x \mapsto M_2(x) = L_1(\psi(x))$ is a permutation. By setting $z := M_2(x)$ and combining $L(M_2(x)^2) = M_1(K(x))$ with the first equation, we get $L(z)^2 = L(1)L(z^2)$. It follows that $L(X)$ is a monomial and S_Q is isotopic to a finite field, contradicting our assumption.

We next consider the case $I_1 = I_2 = \{r_1, r_2\}$, where $0 \le r_1 < r_2 \le r-1$. In this case, we have the q^r-decomposition $M_1(X) = A(X^{q^{r_1}}) + B(X^{q^{r_2}})$, $M_2(X) = C(X^{q^{r_1}}) + D(X^{q^{r_2}})$, where A, B, C, D are reduced q^r-polynomials neither of which is the zero polynomial. Plugging them into (4.3) and again by comparing exponents of monomials, we get

$$A(X^{q^{r_1}})B(X^{q^{r_2}}) = wC(X^{q^{r_1}})D(X^{q^{r_2}}), \tag{4.4}$$

$$A(X^{q^{r_1}})^2 - wC(X^{q^{r_1}})^2 \equiv L(1)A(K(X)^{q^{r_1}}) - wC(K(X)^{q^{r_1}}) \pmod{X^{q^n} - X}, \tag{4.5}$$

$$B(X^{q^{r_2}})^2 - wD(X^{q^{r_2}})^2 \equiv L(1)B(K(X))^{q^{r_2}} - wD(K(X)^{q^{r_2}}) \pmod{X^{q^n} - X}. \tag{4.6}$$

The equation (4.4) holds without modulo $X^{q^n} - X$ since both sides have degree at most $2q^{n-1} \le q^n - 1$. If the coefficient of $X^{q^{r\ell}}$ in $B(X)$ is nonzero, then by considering the coefficients of the monomials $\{X^{q^{r_2+r\ell}+q^{r_1+ri}} : 0 \le i \le s-1\}$ on both sides of (4.4), we see that A and C differs by a constant. That is, $A(X) = \lambda C(X)$, $B(X) = \lambda^{-1}wD(X)$ for some $\lambda \neq 0$. Canceling A and B from (4.5) and (4.6) by substitution, we get

$$(\lambda L(1) - w) \cdot C(K(x)^{q^{r_1}}) = (\lambda^2 - w) \cdot C(x^{q^{r_1}})^2, \tag{4.7}$$

$$(\lambda^2 - \lambda L(1)) \cdot D(K(x)^{q^{r_2}}) = (\lambda^2 - w) \cdot D(x^{q^{r_2}})^2. \tag{4.8}$$

Since w is a nonsquare, $\lambda^2 - w \neq 0$. It follows that $\lambda L(1) - w$ and $\lambda^2 - \lambda L(1)$ are both nonzero. By expansion using the q^m-decomposition of M_1, M_2, we have

$$M_1(x)^2 - wM_2(x)^2 = (\lambda^2 - w) \cdot (C(x^{q^{r_1}})^2 - \lambda^{-2}wD(x^{q^{r_2}})^2).$$

The map $x \mapsto Q(M_2(x)) = M_1(x)^2 - wM_2(x)^2$ is a planar function of DO type equivalent to Q, so at least one of C, D is a permutation polynomial by Lemma 2.5. If C is a permutation polynomial, then we substitute $x + y$, x, y into (4.7) and take their linear combination to get $c_1 C((x *_K y)^{q^{r_1}}) = \big(c_1 C(x^{q^{r_1}})\big) \cdot \big(c_1 C(y^{q^{r_1}})\big)$, where $c_1 = \frac{\lambda^2 - w}{\lambda L(1) - w}$. Here, we have used the fact that $K(x + y) - K(x) - K(y) = 2(x *_K y)$. This shows that S_K is isotopic to a finite field, contradicting our assumption. The case D is a permutation polynomial leads to the same contradiction. This completes the proof. $\square$

The size of the nucleus is an invariant under isotopism and provides a measure for the non-associativity of a commutative semifield. Lemma 4.1 suggests that the associated semifield S_Q of a planar function $Q(x)$ of the form described in the lemma behaves in two extremes: the size of its nucleus is either the maximum possible or the minimum possible. The planar functions that have associated semifields isotopic to a finite field have been characterized in [16], and those of the prescribed form is implicitly described in Lemma 3.9. This provides some evidence to the conjecture that the planar functions of this form are all known. There is not much that we can say about the middle nucleus. In [18], the authors have studied the equivalent forms of planar functions whose corresponding commutative semifields have specified nuclei. We deal with the planar functions of our special form in the following lemma.

Lemma 4.2. *Let q be odd, $n \geq 2$ be an integer, and w be a nonsquare in $\mathbb{F}_{q^n}$. Let $L(X)$ be a reduced q-polynomial over $\mathbb{F}_{q^n}$ such that (4.1) holds. Assume that $Q(X) = L(X)^2 - wX^2$ is planar over $\mathbb{F}_{q^n}$ and the semifield $S_Q = (\mathbb{F}_{q^n}, +, \circ)$ with multiplication as in (4.2) has a middle nucleus of size q^m with $1 \leq m < n$. Then $Q(X)$ is equivalent to either*

(i) $A(X)^2 - w'X^{2q^k}$, *with* $\gcd(k, m) = 1$, w' *a nonsquare and* $A(x)$ *a* q^m*-polynomial, or*
(ii) $(L(1)X + T_1(\Delta) + R(\Delta))^2 - w\left(X + T_0(\Delta) + L(1)w^{-1}R(\Delta)\right)^2$, *where* $\Delta = X^{q^m} - X$, T_0, T_1 *are* q^m*-polynomial and* R *is a nonzero* q*-polynomial.*

Proof. Take the same notation as in the proof of Lemma 4.1, and write $s = n/m$. Let $M_1(X) = \sum_{i=0}^{s-1} f_i(X^{q^i})$ and $M_2(X) = \sum_{i=0}^{s-1} g_i(X^{q^i})$ be their q^m-decompositions respectively, where the f_i's and g_i's are reduced q^m-polynomials. Set $I_1 = \{i : f_i \neq 0\}$ and $I_2 = \{i : g_i \neq 0\}$. Both I_1 and I_2 are non-empty subsets of $\{0, 1, \cdots, s-1\}$.

For $a \in \mathbb{F}_{q^m}$, we have $K(a) = a *_K a = a^2$, so (4.3) gives that $M_1(a)^2 - wM_2(a)^2 = L(1)M_1(a^2) - wM_2(a^2)$. In other words,

$$M_1(X)^2 - wM_2(X)^2 \equiv L(1)M_1(X^2) - wM_2(X^2) \pmod{X^{q^m} - X}. \tag{4.9}$$

It is similar to (3.3) and the same argument using Remark 3.10 show that either

(1) $M_1(X) \equiv c_1X^{q^k} + c_2X^{q^l}$ and $M_2(X) \equiv c_3X^{q^k} + c_4X^{q^l} \pmod{X^{q^m} - X}$, or
(2) $M_1(X) \equiv c_1'X^{q^u}$ and $M_2(X) \equiv c_2'X^{q^v} \pmod{X^{q^m} - X}$,

where $0 \leq k, l, u, v \leq m-1$, $k < l$, the c_i's and c_i''s are constants with $c_1c_2 = wc_3c_4 \neq 0$. Notice that $c_2' \neq 0$, since $M_2(X)$ is a permutation polynomial over $\mathbb{F}_{q^n}$. If $c_1' = 0$, then we set $u = v$ for uniform treatment. The monomials in $M_t(X) \pmod{X^{q^m} - X}$ correspond to the components of $M_t(X)$ in its q^m-decomposition for $t \in \{1, 2\}$, so $k, l \in I_1 \cap I_2$ in the case (1), $v \in I_2$ in the case (2), and $u \in I_1$ in the case (2) if $c_1' \neq 0$.

In the case (2), after plugging them back into (4.9) and comparing coefficients we get $c_1' = L(1)$ and $c_2' = 1$ if $u \neq v$ and $c_1'^2 - wc_2'^2 = L(1)c_1' - wc_2'$ if $u = v$. Now consider the special case $c_1' = 0$. We deduce that $c_2' = 1$, $M_2(a) = a^{q^u}$ for $a \in \mathbb{F}_{q^m}$, so M_2 maps $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$ bijectively. On the other hand, $L(M_2(a)) = M_1(a) = c_1'a^{q^u} = 0$ for all $a \in \mathbb{F}_{q^m}$. This shows that $\mathbb{F}_{q^m}$ lies in the kernel of L. Therefore, there exists a q-polynomial R such that $L(X) = R(X^{q^m} - X)$, so $Q(X)$ is of the second form in the lemma. We thus assume that $c_1' \neq 0$ in the case (2).

For $a \in \mathbb{F}_{q^m}$ and $x \in \mathbb{F}_{q^n}$, we plug $x + a$, x and a into (4.3) and take their linear combination to get $M_1(a)M_1(x) - wM_2(a)M_2(x) = L(1)M_1(ax) - wM_2(ax)$. Here, we have used the fact $K(x) = x *_K x$ and $a *_K x = ax$ for $a \in \mathbb{F}_{q^m}$. Since both $M_1(X)$ and $M_2(X)$ are reduced, we have $M_1(a)M_1(X) - wM_2(a)M_2(X) = L(1)M_1(aX) - wM_2(aX)$. By expanding it using the q^m-decompositions and comparing exponents of monomials, we get

$$(M_1(a) - L(1)a^{q^i})f_i(X^{q^i}) = w(M_2(a) - a^{q^i})g_i(X^{q^i}), \quad 0 \leq i \leq s-1. \tag{4.10}$$

If i is an integer such that $0 \leq i \leq s-1$ and neither $M_1(X) - L(1)X^{q^i}$ nor $M_2(X) - X^{q^i}$ is zero modulo $X^{q^m} - X$, then we claim that i is either in both of I_1 and I_2 or in neither of them. There exists $a \in \mathbb{F}_{q^m}$ such that $M_1(a) - L(1)a^{q^i} \neq 0$ by the assumption, so it follows from

(4.10) that f_i is equal to g_i multiplied by a constant. Similarly, g_i is equal to f_i multiplied by a constant, so the claim follows.

After these preparations, we are now ready to handle each case separately. In the case (1), we claim that $I_1 = I_2 = \{k, l\}$, $M_2(X) = g_k(X^{q^k}) + g_l(X^{q^l})$ and $M_1(X) = c_1c_3^{-1}g_k(X^{q^k}) + c_2c_4^{-1}g_l(X^{q^l})$. For each $0 \le i \le s-1$, neither $M_1(X) - L(1)X^{q^i}$ nor $M_2(X) - X^{q^i}$ is zero modulo $X^{q^m} - X$, so $I_1 = I_2$ by the preceding claim. For $i \in I_1 = I_2$, there is a nonzero constant d_i such that $g_i = d_if_i$ and plugging it in (4.10) we get

$$(L(1) - wd_i)a^{q^i} = M_1(a) - wd_iM_2(a) = (c_1 - wd_ic_3)a^{q^k} + (c_2 - wd_ic_4)a^{q^l}. \tag{4.11}$$

It is straightforward to check that the right hand side has at least one nonzero coefficient, so $L(1) - wd_i \neq 0$. It follows that $i = k$ or $i = l$. Comparing the coefficients of a^{q^l} in (4.11) in the case $i = k$ gives $d_k = w^{-1}c_4^{-1}c_2 = c_3c_1^{-1}$. Similarly, we get $d_l = c_4c_2^{-1}$ in the case $i = l$. This proves the claim. We then compute that

$$Q(M_2(x)) = M_1(x)^2 - wM_2(x)^2 = (1 - wd_k^2)g_k(x^{q^k})^2 + (1 - wd_l^2)g_l(x^{q^l})^2.$$

Since $Q(M_2(x))$ is a planar function equivalent to $Q(x)$, one of g_k and g_l must be a permutation polynomial by Lemma 2.5. Consider the case g_k is a permutation polynomial. With $y = g_k(x^{q^k})^{q^{l-k}}$ we have $x^{q^k} = h_k(y^{q^{k-l}})$ for some q^m-polynomial h_k, and so $g_l(x^{q^l}) = g_l(h_k(y^{q^{k-l}})^{q^{l-k}}) = A(y)$ for some q^m-polynomial A. We now have $Q(M_2(x)) = (1-wd_k^2)y^{2q^{k-l}} + (1 - wd_l^2)A(y)^2$ with A a q^m-polynomial, and so $Q(x)$ is equivalent to one of the first form in the lemma. Since the nucleus of S_Q is $\mathbb{F}_q$ by Lemma 4.1, we have $\gcd(k - l, m) = 1$. The case g_l is a permutation polynomial is dealt with similarly.

In the case (2) with $u \neq v$, we claim that $I_1 = \{u\}$ and $I_2 = \{v\}$. Recall that $c_1' = L(1) \neq 0$, $c_2' = 1$, $u \in I_1$ and $v \in I_2$ in this case. For each $i \in \{0, 1, \cdots, s-1\} \setminus \{u, v\}$, neither $M_1(X) - L(1)X^{q^i}$ nor $M_2(X) - X^{q^i}$ is zero modulo $X^{q^m} - X$ in this case, so $I_1 \setminus \{u, v\} = I_2 \setminus \{u, v\}$. If $i \in I_1 \setminus \{u, v\} = I_2 \setminus \{u, v\}$, then there exists a nonzero constant d_i such that $g_i = d_if_i$, and (4.10) reduces to $(L(1) - wd_i)a^{q^i} = c_1'a^{q^u} - wd_ic_2'a^{q^v}$. This is impossible since $c_1' \neq 0$ and $wd_ic_2' \neq 0$. Hence I_1, I_2 are both subsets of $\{u, v\}$. By setting $i = v$ in (4.10), we get $f_v = 0$. Similarly, $g_u = 0$. This proves the claim. By the same argument in the previous case, $Q(x)$ is equivalent to one of the first form in the lemma.

Finally, consider the case (2) with $u = v$ and $c_1' \neq 0$. In this case, u is in both I_1 and I_2. As before we have $I_1 \setminus \{u\} = I_2 \setminus \{u\}$. If $I_1 = I_2 = \{u\}$, then from the fact $M_2(X)$ is a permutation polynomial and $M_1(X) = L(M_2(X)) \pmod{X^{q^n} - X}$ we deduce that L is a q^m-polynomial, contradicting (4.1). Hence $I_1 \setminus \{u\} = I_2 \setminus \{u\} \neq \emptyset$. For $t \in I_1 \setminus \{u\}$, there exists a constant $d_t \neq 0$ such that $g_t = d_tf_t$ and (4.10) reduces to $c_1'a^{q^u} - L(1)a^{q^t} = wd_t(c_2'a^{q^u} - a^{q^t})$ for $a \in \mathbb{F}_{q^m}$. By comparing coefficients we get $L(1) = wd_t$ and $c_1' = wd_tc_2'$. Together with $c_1'^2 - wc_2'^2 = L(1)c_1' - wc_2'$, we deduce that $c_2' = 1$, $c_1' = L(1)$ and $d_t = L(1)w^{-1}$. To sum up, we have $M_2(X) - g_u(X^{q^u}) = L(1)w^{-1}(M_1(X) - f_u(X^{q^u}))$, $M_1(X) \equiv L(1)X^{q^u}$ and $M_2(X) \equiv X^{q^u} \pmod{X^{q^m} - X}$. The $\mathbb{F}_{q^m}$-linear maps $x \mapsto f_u(x) - L(1)x$ and $x \mapsto g_u(x) - x$ both have $\mathbb{F}_{q^m}$ in their kernels, so there exist q^m-polynomials T_1, T_0 such that $T_1(X^{q^m} - X) = f_u(X) - L(1)X$ and $T_0(X^{q^m} - X) = g_u(X) - X$. Meanwhile, $M_1(X) - f_u(X^{q^u})$ has $\mathbb{F}_{q^m}$ in the kernel, so there exists a q-polynomial R such that it is equal to $R(X^{q^{m+u}} - X^{q^u})$. We thus have $M_1(X) = L(1)X^{q^u} + T_1(X^{q^m} - X) + R(X^{q^{m+u}} - X^{q^u})$, $M_2(X) = X^{q^u} + T_0(X^{q^m} - X) + L(1)w^{-1}R(X^{q^{m+u}} - X^{q^u})$, and $Q(X)$ is equivalent to the second form in this case. $\square$

For the rest of this section, we will only consider the simplest cases as a demonstration of techniques, where the associated semifields are rank two commutative semifields. They correspond to Case (i) in Lemma 4.2 with $n = 2m$. We start with a technical lemma.

Lemma 4.3. *Let q be an odd prime power, m be a positive integer, and take $\zeta \in \mathbb{F}_{q^{2m}}$ such that $\zeta^{q^m-1} = -1$. Let $\Psi : \mathbb{F}_{q^{2m}}^2 \mapsto \mathbb{F}_{q^m}^3$ be the map defined by*

$$\Psi(x_0\zeta + x_1, y_0\zeta + y_1) := (x_1y_1,\ x_0y_0,\ x_0y_1 + x_1y_0), \quad \forall\, x_0, x_1, y_0, y_1 \in \mathbb{F}_{q^m}. \tag{4.12}$$

Then its image set is equal to $\{(A, B, C) \in \mathbb{F}_{q^m}^3 : C^2 - 4AB$ is a square in $\mathbb{F}_{q^m}\}$, and $\Psi(x, y) = (0, 0, 0)$ if and only if $x = 0$ or $y = 0$.

Proof. If $(A, B, C) = \Psi(x, y)$ with $x = x_0\zeta + x_1$, $y = y_0\zeta + y_1$ $(x_i, y_i \in \mathbb{F}_{q^m})$, then $A = x_1y_1$, $B = x_0y_0$, $C = x_0y_1 + x_1y_0$, and $C^2 - 4AB = (x_0y_1 - x_1y_0)^2$ is a square in $\mathbb{F}_{q^m}$. If further $A = B = C = 0$, then it is straightforward to show that at least one of x and y is 0.

Conversely, suppose that $(A, B, C) \in \mathbb{F}_{q^m}^3$ satisfies that $C^2 - 4AB$ is a square. We can directly check that $\Psi(\zeta, B\zeta + C) = (A, B, C)$ if $A = 0$ and $\Psi(1, C\zeta + A) = (A, B, C)$ if $B = 0$. Now assume that $AB \neq 0$, and let t be a solution to $BX^2 - CX + A = 0$. It is now routine to check that $t \in \mathbb{F}_q^*$ and $\Psi(\zeta + t, B\zeta + At^{-1}) = (A, B, C)$. □

Lemma 4.4. *Suppose that $m \geq 3$, $1 \leq k \leq m - 1$ and $\gcd(k, m) = 1$. Let q be odd and w be a nonsquare in $\mathbb{F}_{q^{2m}}$. Then $Q(X) = (X^{q^m} - X)^2 - wX^{2q^k}$ is not planar over $\mathbb{F}_{q^{2m}}$.*

Proof. Take $\zeta \in \mathbb{F}_{q^{2m}}$ such that $\zeta^{q^m-1} = -1$, and let Ψ be as defined in (4.12). Write $x = x_0\zeta + x_1$, $y = y_0\zeta + y_1$ with x_i, $y_i \in \mathbb{F}_{q^m}$, and set $(A, B, C) = \Psi(x, y)$. Then $Q(x + y) = Q(x) + Q(y)$ if and only if

$$-\, wA^{q^k} + (4\zeta^2 B - w\zeta^{2q^k} B^{q^k}) - w\zeta^{q^k} C^{q^k} = 0. \tag{4.13}$$

The left hand side is equal to $\frac{1}{2}(Q(x+y) - Q(x) - Q(y))$. By Lemma 4.3, $Q(x)$ is planar if and only if there is no triple $(A, B, C) \in \mathbb{F}_{q^m}^3 \setminus \{(0, 0, 0)\}$ such that $C^2 - 4AB$ is a square and (4.13) holds. To show that $Q(x)$ is not planar, we need to establish the existence of such a triple.

By raising both sides of (4.13) to the q^m-th power we get another equation, and together with (4.13) we deduce that

$$A^{q^k} = 2(w^{-q^m} + w^{-1})\zeta^2 B - \zeta^{2q^k} B^{q^k},\ C^{q^k} = 2\zeta^{2-q^k}(w^{-1} - w^{-q^m})B, \tag{4.14}$$

We then compute that

$$\begin{aligned}
(C^2 - 4AB)^{q^k} &= 4\zeta^{4-2q^k}(w^{-1} - w^{-q^m})^2 B^2 - 4B^{q^k}\left(2(w^{-q^m} + w^{-1})\zeta^2 B - \zeta^{2q^k} B^{q^k}\right) \\
&= 4\zeta^{4-2q^k} B^2 \left((w^{-1} - w^{-q^m})^2 - 2(w^{-q^m} + w^{-1})\zeta^{2(q^k-1)} B^{q^k-1} + \zeta^{4(q^k-1)} B^{2(q^k-1)}\right) \\
&= 4\zeta^{4-2q^k} B^2 \left((w^{-1} + w^{-q^m} - \zeta^{2(q^k-1)} B^{q^k-1})^2 - 4w^{-1-q^m}\right).
\end{aligned}$$

Since ζ^2 is a nonsquare in $\mathbb{F}_{q^m}^*$ and $\gcd(q^k - 1, q^m - 1) = q - 1$, we need to find $z \in \mathbb{F}_{q^m}^*$ such that $H(z) := (w^{-1} + w^{-q^m} - \zeta^{2(q^k-1)} z^{q-1})^2 - 4w^{-1-q^m}$ is a nonsquare. Then by taking $B \in \mathbb{F}_{q^m}$ such that $B^{q^k-1} = z^{q-1}$ and setting A, C as in (4.14), we get the desired triple. It remains to establish the existence of such an element.

Let ρ be the multiplicative character of order two of $\mathbb{F}_{q^m}^*$, i.e., $\rho(x) = 1$ if x is a nonzero square and $\rho(x) = -1$ otherwise. We extend it to $\mathbb{F}_{q^m}$ by setting $\rho(0) = 0$. Let $\overline{\mathbb{F}}_{q^m}$ be the algebraic closure of $\mathbb{F}_{q^m}$. If $H(X) = h(X)^2$ for some polynomial $h(X) \in \overline{\mathbb{F}}_{q^m}[X]$, then

$$(w^{-1} + w^{-q^m} - \zeta^{2(q^k-1)} X^{q-1} + h(X))(w^{-1} + w^{-q^m} - \zeta^{2(q^k-1)} X^{q-1} - h(X)) = 4w^{-1-q^m}.$$

It implies that the two factors on the left hand side both have degree 0, which is impossible. We can now apply [40, Theorem 6.2.2] to see that $|\sum_{z \in \mathbb{F}_{q^m}} \rho(H(z))| \leq (2(q-1) - 1)q^{m/2}$. It is straightforward to check that $(2(q-1) - 1)q^{m/2} < q^m - 1$ holds for all q odd and $m \geq 3$, so there exists $z \in \mathbb{F}_{q^m}^*$ such that $H(z)$ is a nonsquare. This completes the proof. □

Theorem 4.5. *Let k, m be positive integers with $m \geq 3$, $\gcd(k,m) = 1$, and let $q = p^e$ with p an odd prime. Suppose that either of the following holds: (1) $q \geq 4n^2 - 8n + 2$, (2) $p > 2(em)^2 - (4-2\sqrt{3})em + (3-2\sqrt{3})$, (3) $m = 3$. Then $Q(X) = (aX + bX^{q^m})^2 - wX^{2q^k}$ is planar over $\mathbb{F}_{q^{2m}}$ if and only if $ab = 0$, where $a, b \in \mathbb{F}_{q^{2m}}$ and w is a nonsquare in $\mathbb{F}_{q^{2m}}^*$.*

Proof. Take $\zeta \in \mathbb{F}_{q^{2m}}$ such that $\zeta^{q^m-1} = -1$, and let Ψ be as defined in (4.12). Set $s := a+b$, $\beta := (a-b)\zeta$. The case $s = 0$ has been handled in Lemma 4.4, so assume that $s \neq 0$. By multiplying $Q(x)$ by a nonzero constant if necessary, we set $s = 1$ without loss of generality. If β is in $\mathbb{F}_{q^m}$, then $a = \frac{1+\beta\zeta^{-1}}{2}$, $b = \frac{1-\beta\zeta^{-1}}{2}$, $-ab^{-1} = \frac{\beta+\zeta}{\beta-\zeta} = (\beta-\zeta)^{q^m-1}$, and $a^{-2}(\beta-\zeta)^{-2}Q\left((\beta-\zeta)X\right)$ is of the form in Lemma 4.4. Therefore, we only need to consider the case $s = 1$ and $\beta \notin \mathbb{F}_{q^m}$. As in the case of Lemma 4.4, $Q(x)$ is planar if and only if there is no triple $(A, B, C) \in \mathbb{F}_{q^m}^3 \setminus \{(0,0,0)\}$ such that $C^2 - 4AB$ is a square and

$$A - wA^{q^k} + \beta^2 B - w\zeta^{2q^k} B^{q^k} + \beta C - w\zeta^{q^k} C^{q^k} = 0. \tag{4.15}$$

The left hand side equals $\frac{1}{2}(Q(x+y) - Q(x) - Q(y))$ in the case $(A, B, C) = \Psi(x, y)$.

Assume that $Q(x)$ is planar. We claim that the $\mathbb{F}_q$-linear map

$$\Upsilon : \mathbb{F}_{q^m}^2 \mapsto \mathbb{F}_{q^{2m}},\ (A, C) \to A - wA^{q^k} + \beta C - w\zeta^{q^k} C^{q^k}$$

is a bijection. Otherwise, there exists a pair $(A, C) \neq (0, 0)$ such that (4.15) holds with $B = 0$. Since $C^2 - 4 \cdot A \cdot 0 = C^2$ is trivially a square, this is impossible by our assumption. Therefore, for each $B = u \in \mathbb{F}_{q^m}$, there is a unique pair $(A, C) = (f(u), g(u))$ such that $\Upsilon(f(u), g(u)) = -\beta^2 u + w\zeta^{2q^k} u^{q^k}$, where $f(X), g(X) \in \mathbb{F}_{q^m}[X]$. It is clear that both f and g are $\mathbb{F}_q$-linear. By the definition of f and g we have

$$f(u) - wf(u)^{q^k} + \beta^2 u - w\zeta^{2q^k} u^{q^k} + \beta g(u) - w\zeta^{q^k} g(u)^{q^k} = 0, \quad \forall\, u \in \mathbb{F}_{q^m}. \tag{4.16}$$

If $f(u) = 0$ for some $u \neq 0$, then $(A, B, C) = (0, u, g(u))$ satisfies (4.15) and $C^2 - 4AB = g(u)^2$ is a square. This contradicts our assumption, so the map $u \mapsto f(u)$ is a bijection.

By the planarity of $Q(x)$, $g(u)^2 - 4uf(u)$ is a nonsquare for all $u \in \mathbb{F}_{q^m}^*$, so $S(-g, -f) = (\mathbb{F}_{q^{2m}}, +, \circ)$ as defined in Theorem 2.1 with $t = \zeta$ is a RTCS. Recall that for $x, y \in \mathbb{F}_{q^{2m}}$ and $(A, B, C) = \Psi(x, y)$, we have

$$x \circ y = (-g(B) + C)\zeta - f(B) + A.$$

Let M be the the $\mathbb{F}_q$-linear map such that $M(z_0\zeta + z_1) := \Upsilon(z_1, z_0)$ for $z_0, z_1 \in \mathbb{F}_{q^m}$. It is nondegenerate, and with $(A, B, C) = \Psi(x, y)$ we have

$$\begin{aligned} M(x \circ y) &= \Upsilon(-f(B) + A, -g(B) + C) = -\Upsilon(f(B), g(B)) + \Upsilon(A, C) \\ &= \beta^2 B - w\zeta^{2q^k} B^{q^k} + \Upsilon(A, C) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)). \end{aligned}$$

Therefore, the semifield S_Q defined by Q is isotopic to $S(-g, -f)$.

Under the conditions in the theorem, $S(-g, -f)$ is isotopic to either a finite field or a Dickson semifield by Theorem 2.2. By [15, Example 2], $S(-g, -f)$ is isotopic to a finite field if and only if $g(u) = cu$ and $f(u) = du$, where $c^2 - 4d$ is a nonsquare. In this case, (4.16) becomes $(d + \beta c + \beta^2)u = w(d + \zeta c + \zeta^2)^{q^k} u^{q^k}$. It holds for all u, so $d + \zeta c + \zeta^2 = 0$ and $d + \beta c + \beta^2 = 0$. Since $\zeta^2 \in \mathbb{F}_{q^m}$, we deduce that $c = 0$, $d = -\zeta^2$ and $\beta = \pm\zeta$. It follows from $a + b = 1$ and $a - b = \beta\zeta^{-1}$ that $(a, b) = (1, 0)$ or $(0, 1)$.

From now on, assume that $S(-g, -f)$ is not isotopic to a finite field but is isotopic to a Dickson semifield $S(0, \lambda x^\theta) = (\mathbb{F}_{q^{2m}}, +, \circ')$ as defined in Theorem 2.1 with $t = \zeta$, where λ is a nonsquare in $\mathbb{F}_{q^m}$ and $\theta \in \mathrm{Aut}(\mathbb{F}_{q^{2m}})$. By Lemma 4.1, the semifield S_Q and so $S(-g, -f)$ has nucleus $\mathbb{F}_q$. It follows that $x^\theta = x^{q^\ell}$ for some $1 \leq \ell \leq m-1$ such that $\gcd(\ell, m) = 1$, cf. [26, Theorem 10.16]. By [16, Theorem 2.6], there exist nondegenerate linear maps $L, N : \mathbb{F}_{q^{2m}} \mapsto \mathbb{F}_{q^{2m}}$ and $\alpha \in \mathbb{F}_{q^m}^*$ such that

$$L(x \circ y) = N(x) \circ' (\alpha N(y)). \tag{4.17}$$

There exist linear maps $L_i : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m}$, $1 \le i \le 4$, such that $N(x) = (L_1(x_0) + L_2(x_1))\zeta + L_3(x_0) + L_4(x_1)$ for $x = x_0\zeta + x_1$. Write $L_1(X) = \sum_{i=0}^{em-1} a_i X^{p^i}$ and $L_3(X) = \sum_{i=0}^{em-1} b_i X^{p^i}$, with $a_i, b_i \in \mathbb{F}_{q^m}$. We consider (4.17) in three cases.

(1) In the case $x_1 = y_1 = 0$, it shows that $L(-g(x_0y_0)\zeta - f(x_0y_0))$ is equal to

$$\lambda\alpha^{q^\ell} L_1(x_0)^{q^\ell} L_1(y_0)^{q^\ell} + \alpha L_3(x_0)L_3(y_0) + \alpha(L_1(x_0)L_3(y_0) + L_3(x_0)L_1(y_0))\zeta.$$

The coordinates with respect to the basis $\{1, \zeta\}$ in the above expression are polynomials in x_0y_0. By comparing coefficients we get $\lambda\alpha^{q^\ell} a_i^{q^\ell} a_j^{q^\ell} + \alpha b_{i+el} b_{j+el} = 0$, and $a_{i+el}b_{j+el} + a_{j+el}b_{i+el} = 0$ for $i \ne j$. The subscripts are read modulo em here. We observe that $-a_ia_jb_{i+el}b_{j+el}$ is a nonsquare and $-a_{i+el}a_{j+el}b_{i+el}b_{j+el}$ is a square, yielding that $a_ia_{i+el}a_ja_{j+el}$ is a nonsquare in the case $i \ne j$ and the terms involved are nonzero. Assume that $a_ua_v \ne 0$ for $0 \le u < v \le em - 1$. We claim that none of the elements in $\{a_{u+rel}, b_{v+sel} : 0 \le r, s \le m-1\}$ is zero. It follows from the first equation with $(i,j) = (u,v)$ that $b_{u+el}b_{v+el} \ne 0$, and follows from the second equation with $(i,j) = (u - e\ell, u)$ and $(i,j) = (v - e\ell, v)$ that none of $a_{u+el}, a_{v+el}, b_u, b_v$ is zero. The claim then follows by induction. For $0 \le i < j \le m-1$, exactly one of $a_{u+iel}a_{u+(i+1)el}$ and $a_{u+jel}a_{u+(j+1)el}$ is a square and the other is a nonsquare by our previous observation. This is impossible when $m \ge 3$. We conclude that L_1 is a monomial, and similarly L_3 is a monomial. Write $L_1(x_0) = c_1x_0^{p^i}$ and $L_3(x_0) = c_3x_0^{p^i}$ for some i and constants c_1, c_3. Since N is nondegenerate, $(c_1, c_3) \ne (0,0)$. In this case, (4.17) reduces to

$$-L(g(u)\zeta + f(u)) = 2\alpha c_1c_3u^{p^i}\zeta + \alpha c_3^2u^{p^i} + \lambda\alpha^{q^\ell}c_1^{2q^\ell}u^{q^\ell p^i},\ \forall\, u \in \mathbb{F}_{q^m}. \tag{4.18}$$

(2) In the case $x_1 = y_0 = 0$, (4.17) gives that $L(x_0y_1\zeta)$ is equal to

$$\alpha x_0^{p^i}(c_1L_4(y_1) + c_3L_2(y_1))\zeta + \alpha c_3x_0^{p^i}L_4(y_1) + \lambda\alpha^{q^\ell}c_1^{q^\ell}x_0^{p^iq^\ell}L_2(y_1)^{q^\ell}.$$

As in the previous case, we know that $\alpha c_3x_0^{p^i}L_4(y_1) + \lambda\alpha^{q^\ell}c_1^{q^\ell}x_0^{p^iq^\ell}L_2(y_1)^{q^\ell}$ is a polynomial in x_0y_1. This is possible if and only if there exists constants c_2, c_4 such that $L_2(x) = c_2x^{p^i}$ and $L_4(x) = c_4x^{p^i}$ for the same i. The nondegeneracy of N requires that $c_1c_4 - c_2c_3 \ne 0$. In this case, (4.17) takes the form

$$L(u\zeta) = \alpha(c_1c_4 + c_2c_3)u^{p^i}\zeta + \alpha c_3c_4u^{p^i} + \lambda\alpha^{q^\ell}c_1^{q^\ell}c_2^{q^\ell}u^{q^\ell p^i},\ \forall\, u \in \mathbb{F}_{q^m}. \tag{4.19}$$

(3) In the case $x_0 = y_0 = 0$, (4.17) gives that

$$L(u) = 2\alpha c_2c_4u^{p^i}\zeta + \alpha c_4^2u^{p^i} + \lambda\alpha^{q^\ell}c_2^{2q^\ell}u^{p^iq^\ell},\ \forall\, u \in \mathbb{F}_{q^m}. \tag{4.20}$$

We compute $L(g(u)\zeta) + L(f(u))$ using (4.19) and (4.20) and add it to (4.18) to cancel out the left hand side. The coordinate of ζ on the right hand side gives that

$$2c_2c_4f(u)^{p^i} + (c_1c_4 + c_2c_3)g(u)^{p^i} + 2c_1c_3u^{p^i} = 0. \tag{4.21}$$

We claim that none of c_1, c_2, c_3, c_4 is zero. If $c_2c_4 = 0$, then $c_1c_4 + c_2c_3 \ne 0$ and (4.21) gives that $g(u) = c_5u$ for some constant c_5. The equation (4.16) now takes the form

$$f(u) - wf(u)^{q^k} = -(\beta^2 + \beta c_5)u + (w\zeta^{2q^k} + w\zeta^{q^k}c_5^{q^k})u^{q^k}.$$

We obtain another equation by raising both sides to the q^m-th power, and then deduce that both $f(u)$ and $f(u)^{q^k}$ are linear combinations of u and u^{q^k}. Since $\gcd(m,k) = 1$, this is possible only if f has degree 1. However, $S(-g,-f)$ is then isotopic to a finite field: a contradiction. Hence $c_2c_4 \ne 0$. If $c_1c_3 = 0$, then with the role of $z = f(u)$ and u interchanged and g considered as a function of z, we derive the same contradiction. This proves the claim.

From (4.21), we see that $f(u) = d_1 g(u) + d_2 u$ for some constants $d_1, d_2 \in \mathbb{F}_{q^m}$ with $d_2 \neq 0$. Canceling f from (4.16) by substitution, we get

$$(\beta + d_1)g(u) - w(d_1+\zeta)^{q^k} g(u)^{q^k} = -(d_2+\beta^2)u + w(d_2+\zeta^2)^{q^k} u^{q^k}. \tag{4.22}$$

We claim that $\frac{w(d_1+\zeta)^{q^k}}{\beta+d_1} \in \mathbb{F}_{q^m}^*$. Otherwise, raising both sides of (4.22) to the q^m-th power, we get another equation that is linear independent with (4.22). We then deduce that both $g(u)$ and $g(u)^{q^k}$ are linear combinations of u, u^{q^k}. This is possible only if $g(u) = c_6 u$ for a constant c_6, but then $f(u)$ has degree 1: a contradiction. This proves the claim.

After dividing both sides of (4.22) by $\beta + d_1$, the left hand side is in $\mathbb{F}_{q^m}[u]$, so should be the right hand side. This gives that both $\frac{d_2+\beta^2}{d_1+\beta}$ and $\frac{d_2+\zeta^2}{d_1+\zeta}$ are in $\mathbb{F}_{q^m}$. Since $d_2 + \zeta^2$ is in $\mathbb{F}_{q^m}$ but $d_1 + \zeta$ is not, we must have $d_2 = -\zeta^2$. We have $d_2 + \beta^2 \neq 0$, since otherwise $\beta^2 = \zeta^2$ and S_Q is isotopic to a finite field as we have shown. Now set $z := g(u)$. The equation (4.22) gives that $u = h_1 z + h_2 z^{q^k}$ for some constants $h_1, h_2 \in \mathbb{F}_{q^m}^*$. In particular, this shows that $u \mapsto z = g(u)$ is a bijection. It follows that $f(u) = h_3 z - \zeta^2 h_2 z^{q^k}$ with $h_3 = d_1 - \zeta^2 h_1$, and we have

$$\begin{aligned} g(u)^2 - 4uf(u) &= z^2 - (h_1 z + h_2 z^{q^k})(h_3 z - \zeta^2 h_2 z^{q^k}) \\ &= z^2 (h_5 + h_6 z^{q^k-1} + \zeta^2 h_2^2 z^{2(q^k-1)}), \end{aligned}$$

where $h_5 = 1 - h_1 h_3$, $h_6 = \zeta^2 h_1 h_2 - h_2 h_3$.

Set $H(X) := h_5 + h_6 X^{q-1} + \zeta^2 h_2^2 X^{2(q-1)}$. We have $H(X) = \left(\zeta h_2 X^{q-1} + \frac{h_6}{2\zeta h_2}\right)^2 + \frac{4\zeta^2 h_2^2 h_5 - h_6^2}{4\zeta^2 h_2^2}$. We directly compute that $4\zeta^2 h_2^2 h_5 - h_6^2 = (4\zeta^2 - d_1^2) h_2^2 \neq 0$, so $H(X)$ is not a square in $\overline{\mathbb{F}}_{q^m}[X]$ by the same argument in the proof of Lemma 4.4, where $\overline{\mathbb{F}}_{q^m}$ is the algebraic closure of $\mathbb{F}_{q^m}$. The same exponential sum bound there establishes the existence of z such that $h_5 + h_6 z^{q^k-1} + \zeta^2 h_2^2 z^{2(q^k-1)}$ is a square. If we take u such that $z = g(u)$, then $g(u)^2 - 4uf(u)$ is a nonsquare. This contradiction completes the proof. $\square$

In the proof of Theorem 4.5, we do not directly consider the planarity of Q. Instead, we show that the semifield S_Q is a RTCS and make use of the classification results of such semifields obtained in [14, 33]. This is in the same spirit as in Section 3, where we make use of Menichetti's classification of generalized twisted fields. Coulter and Henderson have used this approach to characterize planar functions of certain form over $\mathbb{F}_{q^3}$, cf. [17]. The list of known commutative semifields is short [12, 34, 49], and Minami and Nakagawa [39] have determined the polynomial forms of certain commutative semifields. It may be of some interest to examine the known commutative semifields one by one to check whether their isotopes will yield planar functions of the form $L(X)^2 - wX^2$, but the answer is most probably negative. We need new techniques to prove or disprove the planarity of the functions of interest.

5. Low-dimensional $\mathcal{C}$-planes of even order

In this section, we consider type $\mathcal{C}$ spreads of even order. Let q be even. Recall that β is an element of order $(q^n+1)(q-1)$ in $\mathbb{F}_{q^{2n}}$, and $\Theta(\beta) \in \Gamma L(1, q^{2n})$ is defined by $\Theta(\beta)(x) = \beta x$. A type $\mathcal{C}$ spread $\mathcal{S}$ of order q^n with kernel $\mathbb{F}_q$ is isomorphic to the orbit of $W = \{L(x) + \delta x : x \in \mathbb{F}_{q^n}\}$ under the group $\langle \Theta(\beta) \rangle$, where $L(X)$ is a monic reduced q-polynomial and $\delta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$. By Lemma 3.2, $Q(X) = (L(X) + \delta X)(L(X) + \delta^{q^n} X) \in \mathbb{F}_{q^n}[X]$ is a permutation polynomial of $\mathbb{F}_{q^n}$. For each $y \in \mathbb{F}_{q^n}$, we define the quadratic form $Q_y(x) := \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left((\delta + \delta^{q^n})^{-1} y Q(x)\right)$, i.e.,

$$Q_y(x) := \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left((\delta + \delta^{q^n})^{-1} y L(x)^2 + (\delta^{-1} + \delta^{-q^n})^{-1} y x^2 + yxL(x)\right). \tag{5.1}$$

By Lemma 2.8, Q_y has odd rank for any $y \neq 0$. Its associated bilinear form is

$$B_y(u, v) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yuL(v) + yvL(u)) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left((\tilde{L}(yu) + yL(u))v\right),$$

where $\tilde{L}$ is the adjoint polynomial of L. The radical $\mathrm{rad}(Q_y) = \{u \in \mathbb{F}_{q^n} : \tilde{L}(yu) + yL(u) = 0\}$. By Theorem 2.6, $Q_y(\mathrm{rad}(Q_y)) \neq \{0\}$ for each $y \neq 0$. We will fix these notation throughout this section. We first examine two special cases in the following examples.

Example 5.1. *Assume that n is even, and $L(x) = x^{q^k}$ with $\gcd(n,k) = 1$. In this case, the adjoint polynomial $\tilde{L}(X) = X^{q^{n-k}}$. Take y to be a primitive element. Since $\gcd(q^{n-k} - q^k, q^n - 1) = q^2 - 1$ and $\gcd(1 - q^{n-k}, q^n - 1) = q - 1$, we have $\mathrm{rad}(Q_y) = \{u \in \mathbb{F}_{q^n} : u^{q^{n-k}-q^k} = y^{1-q^{n-k}}\} = \{0\}$. Hence, Q_y has rank n and $Q(X)$ is not a permutation polynomial of $\mathbb{F}_{q^n}$.*

Example 5.2. *Assume that n is even, and $L(x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$. In this case, $\tilde{L}(X) = L(X)$. Set $\Delta := (\delta^{-1} + \delta^{-q^n})^{-1}$. Take $y \in \mathbb{F}_{q^2}$ such that $y + y^q = \Delta$ if $\Delta \in \mathbb{F}_q^*$, and take $y = \Delta^{-1}$ otherwise. Then $y \notin \mathbb{F}_q$ and $\mathrm{rad}(Q_y) = \{u : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(yu) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(u) = 0\}$. For $u \in \mathrm{rad}(Q_y)$, we have $Q_y(u) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\Delta y \cdot u^2)$. It is clear that $\Delta y \in \mathbb{F}_q + \mathbb{F}_q \cdot y^2$ for the chosen y, so Q_y is constantly zero on $\mathrm{rad}(Q_y)$. It follows that $Q(X)$ is not a permutation polynomial of $\mathbb{F}_{q^n}$.*

The main objective of this section is to characterize the case $n = 3$ and $n = 4$ completely. The case $n = 2$ can be reduced to either of the above examples with a proper choice of δ. In the case $n = 3$, there is the construction by Kantor in [27]. We start with the case $n = 4$. The strategy is to show that there is a trivial $\mathrm{rad}(Q_y)$ except the cases where it can be reduced to the second example above.

Theorem 5.3. *If q is even, then there is no type $\mathcal{C}$ spread with ambient space $(\mathbb{F}_{q^8}, +)$ and kernel $\mathbb{F}_q$.*

Proof. We continue with the arguments in the beginning of this section. We only deal with the case $\deg(L) = q^3$ and the other cases can be handled similarly. If $L(X) = X^{q^3} + ax^{q^2} + bx^q + cx$, then by replacing δ with $\delta + c$ we assume that $c = 0$. In this case, $\tilde{L}(X) = b^{q^3}X^{q^3} + a^{q^2}X^{q^2} + X^q$ and $\tilde{L}(yu) + L(u)y = (b^{q^3}y^{q^3} + y)u^{q^3} + (a^{q^2}y^{q^2} + ay)u^{q^2} + (y^q + by)u^q$. The associated matrix of this q-polynomial as in (2.2) has determinant $f(y)^2$, where

$$f(y) = y^{1+q}c_1 + y^{1+q^2}c_2 + y^{q+q^2}c_1^q + y^{q^3+1}c_1^{q^3} + y^{q+q^3}c_2^q + y^{q^2+q^3}c_1^{q^2},$$

with $c_1 = b^q + a^{1+q}$, $c_2 = 1 + b^{1+q^2}$.

(1) If at least one of c_1, c_2 is not zero, then $f(Y)$ is a nonzero polynomial with degree less than q^4. For $y \in \mathbb{F}_{q^4}$ such that $f(y) \neq 0$, $\mathrm{rad}(Q_y) = \{0\}$ and Q_y has rank 4.

(2) If $c_1 = c_2 = 0$, then $b^{1+q^2} = 1$ and $b^q = a^{1+q}$. It follows that $a^{(1+q)(1+q^2)} = 1$, i.e., a is a $(q-1)$-st power in $\mathbb{F}_{q^4}^*$. Since $\gcd(q^3 - 1, q^4 - 1) = q - 1$, there exists $u \in \mathbb{F}_{q^4}^*$ such that $a = u^{q^3-1}$. Then $b = a^{(1+q)q^2} = u^{q^2-1}$, and so $L(x) = u^{-1}\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(u^q x) + u^{q-1}x$. With $x' = u^q x$ and $\delta' = 1 + \delta u^{1-q}$, we have

$$L(x) + \delta x = u^{-1}(\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(x') + \delta' x')$$

This reduces to the case in Example 5.2.

In either case, $Q(X)$ is not a permutation polynomial of $\mathbb{F}_{q^4}$. This completes the proof. ∎

The rest of this section is devoted to the classification of the case $n = 3$.

Lemma 5.4. *For $\delta \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^3}$, the map $x \mapsto Q(x) = (\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x) + \delta x)^{1+q^3}$ is a permutation of $\mathbb{F}_{q^3}$ if and only if $\delta^{-1} + \delta^{-q^3} \in \mathbb{F}_q^*$.*

Proof. Set $r := 1 + \delta^{-1}$, $h := (\delta^{-1} + \delta^{-q^3})^{-1}$, and set $\mathrm{Tr} := \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}$ throughout this proof. By Lemma 2.8 and Theorem 2.6, $Q(X)$ is a permutation polynomial of $\mathbb{F}_{q^3}$ if and only if Q_y is not constantly zero on $\mathrm{rad}(Q_y)$ for each $y \neq 0$, where Q_y is as defined in (5.1). In this case,

$$Q_y(x) = \mathrm{Tr}((\delta + \delta^{q^3})^{-1}y) \cdot \mathrm{Tr}(x^2) + \mathrm{Tr}(hyx^2) + \mathrm{Tr}(yx) \cdot \mathrm{Tr}(x).$$

If $y \in \mathbb{F}_q^*$, then $\mathrm{rad}(Q_y) = \mathbb{F}_{q^3}$ and $Q_y(x) = y\mathrm{Tr}(cx^2)$, with $c = h+1+\mathrm{Tr}((\delta+\delta^{q^3})^{-1})$. If $y \notin \mathbb{F}_q$, then $\mathrm{rad}(Q_y) = \{u : \mathrm{Tr}(u) = \mathrm{Tr}(yu) = 0\} = \mathbb{F}_q \cdot (y^q + y^{q^2})$, and

$$Q_y(y^q + y^{q^2}) = y^{1+q+q^2} \cdot \mathrm{Tr}\left(h(y^{q-q^2} + y^{q^2-q})\right).$$

If $h \notin \mathbb{F}_q^*$, then $Q_h(h^q + h^{q^2}) = 0$ and $Q_h(\mathrm{rad}(Q_h)) = \{0\}$. Hence we must have $h \in \mathbb{F}_q^*$ in order for Q to be a permutation polynomial, and this proves the necessity part.

Now assume that $h \in \mathbb{F}_q^*$. In this case, it is straightforward to show that $c = \mathrm{Tr}(r^{1+q^3})h$ and the minimal polynomial of rh over $\mathbb{F}_{q^3}$ is $X^2 + X + r^{1+q^3}h^2 = 0$. By [35, Theorem 2.25], $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}(h^2r^{1+q^3}) = 1$, which in particular implies that $\mathrm{Tr}(h^2r^{1+q^3}) = hc \neq 0$. Hence $Q_y(x) = y\mathrm{Tr}(cx^2)$ is not constantly zero on $\mathrm{rad}(Q_y) = \mathbb{F}_{q^3}$ if $y \in \mathbb{F}_q^*$. For each $y \notin \mathbb{F}_q$, the $\mathbb{F}_q$-linear subspace $\{x \in \mathbb{F}_{q^3} : \mathrm{Tr}((y^{q-q^2} + y^{q^2-q})x) = 0\}$ is spanned by y and y^{-1}. It can not contain $\mathbb{F}_q$, since otherwise y would lie in a degree two extension of $\mathbb{F}_q$. It follows that $\mathrm{Tr}(y^{q-q^2} + y^{q^2-q}) \neq 0$, so $Q_y(\mathrm{rad}(Q_y)) \neq \{0\}$ for all $y \notin \mathbb{F}_q$. This proves the sufficiency part. □

Remark 5.5. *Take $\delta \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^3}$ such that $\delta^{-1} + \delta^{-q^3} \in \mathbb{F}_q^*$, and take the decomposition $\mathbb{F}_{q^3} = T_0 \oplus \mathbb{F}_q$ as in [32], where $T_0 = \{x \in \mathbb{F}_{q^3} : \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x) = 0\}$. Let W be the image of $\mathbb{F}_{q^3}$ under the map $x \mapsto \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x)+\delta x$. Then $W = T_0\cdot\delta\oplus\mathbb{F}_q\cdot(1+\delta)$, and $\{\beta^i\cdot W : 0 \le i \le q^3\}$ forms a spread $\mathcal{S}$ of type $\mathcal{C}$, where β is an element of order $(q^3+1)(q-1)$. Moreover, the spread $\mathcal{S}$ is symplectic with respect to the nondegenerate alternating form $A(x,y) = \mathrm{Tr}_{q^6/q}\big((\delta+\delta^{q^3})^{-1}xy^{q^3}\big)$.*

Lemma 5.6. *Let $L(X) \in \mathbb{F}_{q^3}[X]$ be a monic reduced q-polynomial and $\delta \in \mathbb{F}_{q^6} \setminus \mathbb{F}_{q^3}$. The map $x \mapsto Q(x) = (L(x)+\delta x)^{1+q^3}$ is a permutation of $\mathbb{F}_{q^3}$ if and only if $L(x)+\delta x = u^{-1}\mathrm{Tr}_{q^3/\mathbb{F}_q}(u^qx)+\delta' x$ for some $\delta' \notin \mathbb{F}_{q^3}$ and $u \in \mathbb{F}_{q^3}^*$ such that $\delta'^{-1} + \delta'^{-q^3} \in u^{1-q} \cdot \mathbb{F}_q^*$.*

Proof. If $L(x) + \delta x = u^{-1}\mathrm{Tr}_{q^3/\mathbb{F}_q}(u^qx) + \delta' x$, then with $y = u^qx$ we have $L(x) + \delta x = u^{-1}\left(\mathrm{Tr}_{q^3/\mathbb{F}_q}(y) + \delta' u^{1-q}y\right)$, and the sufficient part of the theorem follows from Lemma 5.4. Therefore, we only need to prove the necessary part.

Assume that $x \mapsto Q(x)$ is a a permutation, and we need to prove that $L(x) + \delta x$ is of the desired form. If $L(x) = x^{q^2} + ax^q + bx$, then by replacing δ with $\delta + b$ we assume that $b = 0$. If a is a nonzero $(q-1)$-st power, then $a = u^{q^2-1}$ for some $u \in \mathbb{F}_{q^3}^*$ and $L(x) + \delta x = u^{-1}\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(u^qx) + (u^{q-1} + \delta)x$. Similar to the first paragraph of this proof, we can deduce that $L(x) + \delta x$ is of the desired form by Lemma 5.4. There are two remaining cases.

(1) In the case a is not a nonzero $(q-1)$-st power, $y \mapsto u = y^{q^2} + a^qy^q$ is a permutation of $\mathbb{F}_{q^3}$ and $L(u) + u\delta = (1 + a^q\delta)^{1+q^3}(y^{q^2} + \delta' y^q)^{1+q^3}$, where $\delta' = \frac{\delta+a^{1+q^2}}{\delta a^q+1}$. Therefore, $x \mapsto Q(x)$ is a permutation if and only if the map $x \mapsto (x^q + \delta' x)^{1+q^3}$ is.
(2) In the case $a = 0$, $x^{q^2} + \delta x = \delta \cdot (y^q + \delta^{-1}y)$ for $y = x^{q^2}$. Therefore, $x \mapsto Q(x)$ is a permutation if and only if the map $x \mapsto (x^q + \delta^{-1}x)^{1+q^3}$ is.

We now show that $x \mapsto Q(x) = (x^q + \delta x)^{1+q^3}$ is not a permutation of $\mathbb{F}_{q^6}$ for any $\delta \notin \mathbb{F}_{q^3}$, which will exclude these two cases and conclude the proof. In this case, we have $Q(X) = (X^q + \delta X)(X^q + \delta^{q^3}X)$. By Hermite's criterion for permutation polynomials (cf. [35, Theorem 7.4]), $Q(X)^{q^2-1} \pmod{X^{q^3} - X}$ has degree at most $q^3 - 2$. The polynomial $Q(X)^{q^2-1}$ has degree at most $2q(q^2-1) < 2(q^3-1)$, so its coefficient of X^{q^3-1} should be zero. Since $q^2 - 1 = (q-1)q + (q-1)$, we can rewrite $Q(X)^{q^2-1}$ as

$$X^{2q^2-2} \cdot \left(X^{2(q^2-q)} + s^qX^{q^2-q} + t^q\right)^{q-1} \cdot \left(X^{2(q-1)} + sX^{q-1} + t\right)^{q-1},$$

where $s = \delta + \delta^{q^3}$ and $t = \delta^{1+q^3}$. The second term in the product contributes monomials that are powers of $X^{q(q-1)}$ and the third term contributes monomials that are powers of X^{q-1}. If

$q^3-1=2(q^2-1)+q(q-1)i+(q-1)j$ with $0\le i,j\le 2(q-1)$, then we necessarily have $j=q-1$ and $i=q-2$. Thus the coefficient of X^{q^3-1} in $Q(X)^{q^2-1}$ is the product of the coefficient of X^{q-1} in $(X^2+sX+t)^{q-1}$ and that of X^{q-2} in $(X^2+s^qX+t^q)^{q-1}$, i.e.,

$$\sum_{i=0}^{q/2}\binom{q-1}{i,q-1-2i,i}s^{q-1-2i}t^i\cdot\sum_{j=0}^{q/2-1}\binom{q-1}{j,q-2-2j,j+1}s^{q(q-2-2j)}t^{q(j+1)}. \tag{5.2}$$

Here, the numbers $\binom{q-1}{i,j,k}$'s are trinomial coefficients. A straightforward analysis using Lucas' theorem shows that: $\binom{q-1}{i}$ is odd for all $0\le i\le q-2$; $\binom{2i}{i}$ is odd if and only if $i=0$; $\binom{2j+1}{j}$ is odd if and only if $j=2^\ell-1$ for some nonnegative integer ℓ. Since $\binom{q-1}{i,q-1-2i,i}=\binom{2i}{i}\binom{q-1}{2i}$ and $\binom{q-1}{j,q-2-2j,j+1}=\binom{2j+1}{j}\binom{q-1}{2j+1}$, the quantity in (5.2) is equal to

$$s^{q-1}\cdot\sum_{\ell=0}^{e-1}s^{q(q-2^{\ell+1})}t^{2^\ell q}=s^{q^2+q-1}\cdot\sum_{\ell=0}^{e-1}(ts^{-2})^{2^\ell q},$$

where e is such that $q=2^e$. Recall that this quantity is zero. Since $s\ne 0$, we have $\sum_{\ell=0}^{e-1}(ts^{-2})^{2^\ell}=0$ and thus $\mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_2}(ts^{-2})=0$. By [35, Theorem 2.25], there exists $u\in\mathbb{F}_{q^3}$ such that $ts^{-2}=u^2+u$. Set $z=\delta^{q^3-1}$. We have $z\notin\mathbb{F}_{q^3}$ and $ts^{-2}=(z+z^{-1})^{-1}$ by direct check. The minimal polynomial of z over $\mathbb{F}_{q^3}$ is $(X-z)(X-z^{-1})=X^2+(u^2+u)^{-1}X+1$, but the latter has $\frac{u}{u+1}\in\mathbb{F}_{q^3}$ as a root: a contradiction. This completes the proof. $\square$

As an immediate corollary, we get the following characterization result.

Theorem 5.7. *Let q be even. The type $\mathcal{C}$ spreads with ambient space $(\mathbb{F}_{q^6},+)$ and kernel $\mathbb{F}_q$ are isomorphic to those described in Remark 5.5.*

We end this section with some remarks on the higher dimensional case. Theorem 5.3 supports the conjecture that there is no $\mathcal{C}$-plane of even order and even dimension. The simple nature of the proof in the case $n=4$ suggests that the method may be applicable to larger values of even n, and of course new ingredients are needed to prove the conjecture. In the case where n is odd, there are the constructions in [32], making a characterization in this case a challenging problem. It may be more practical to classify the $\mathcal{C}$-planes of order 2^p with p an odd prime, where no such non-Desargeusian planes are known. The approach in this section provides the first step towards a complete characterization of $\mathcal{C}$-planes of even order.

Acknowledgement. This research was supported by the National Natural Science Foundation of China under Grant 11422112 and Fundamental Research Fund for the Central Universities of China. The author thanks the referees for detailed comments and suggestions that helped to improve the presentation of the paper. The author is indebted to Professor William M. Kantor for numerous helpful comments and suggestions during this project, and he also thanks Professor Gary L. Ebert who brought the problem to his attention in 2011.

References

[1] A.A. Albert, On nonassociative division algebra, Trans. Amer. Math. Soc. 72 (1952), 296-309.
[2] A.A. Albert, Generalized twisted fields, Pacific J. Math. 11(1961), 1-8.
[3] A.A. Albert, Isotopy for generalized twisted fields, An. Acad. Brasil. Ci. 33 (1961), 265-275.
[4] J. Andre, Uber nicht-Desarguesche Ebenen mit transitiver Translationsgruppe, Math. Z. 60 (1954), 156-186.
[5] R.D. Baker, C. Culbert, G.L. Ebert, K.E. Mellinger, Odd order flag-transitive affine planes of dimension three over their kernel, Adv. Geometry (2003), 215-223.
[6] R.D. Baker, J.M. Dover, G.L. Ebert, K.L. Wantz, Perfect Baer subplane partitions and three-dimensional flag-transitive planes, Des. Codes Cryptogr. 21 (2000), 19-39.
[7] R.D. Baker, J.M. Dover, G.L. Ebert, K. L. Wantz, Baer subgeometry partitions, J. Geom. 67 (2000), 23-34.

[8] R.D. Baker, G.L. Ebert, Constructions of two-dimensional flag-transitive planes, Geom. Dedicata 27 (1988), 9-14.

[9] R.D. Baker, G.L. Ebert, Two-dimensional flag-transitive planes revisited, Geom. Dedicata 63 (1996), 1-15.

[10] R.D. Baker, G.L. Ebert, K.H. Leung, Q. Xiang, A trace conjecture and flag-transitive affine planes, J. Combin. Theory Ser. A 95 (2001), 158-168.

[11] S. Ball, M. Lavrauw, Commutative semifields of rank 2 over their middle nucleus, in: G.L. Mullen et al. (eds), *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin-Heidelberg, 2002.

[12] L. Budaghyan, T. Helleseth, Planar functions and commutative semifields, Tatra Mt. Math. Publ. 45 (2010), 15-25.

[13] F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M. Liebeck, J. Saxl, Linear spaces with flag-transitive automorphism groups, Geom. Dedicata 36 (1990), 89-94.

[14] A. Blokhuis, M. Lavrauw, S. Ball, On the classification of semifield flocks, Adv. Math. 180 (2003), 104-111.

[15] S.D. Cohen, M.J. Ganley, Commutative semifields, two dimensional over their middle nucleus, J. Algebra 75 (1982), 373-385.

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

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

[18] R.S. Coulter, M. Henderson, P. Kosick, Planar polynomials for commutative semifields with specified nuclei, Des. Codes Cryptogr. 44 (2007), 275-286.

[19] P. Dembowski, *Finite geometries*, Springer, Berlin-Heidelberger-New York, 1968.

[20] L.E. Dickson, On commutative linear algebras in which division is always uniquely possible, Trans. Amer. math. Soc. 7 (1906), 514-522.

[21] L.E. Dickson, Linear algebra with associativity not assumed, Duke Math. J. 1 (1935), 113-125.

[22] G.L. Ebert, Partitioning problems and flag-transitive planes, Rend. Circ. Mat. Palermo Ser. II Suppl. 53 (1998), 27-44.

[23] C. Hering, Eine nicht-desarguesche zweifach transitive affine Ebene der Ordnung 27, Abh. Math. Sem. Univ. Hamburg 34 (1969), 203-208.

[24] D.A. Foulser, Solvable flag transitive affine groups, Math. Z. 86 (1964), 191-204.

[25] D.A. Foulser, The flag-transitive collineation groups of the finite Desarguesian affine planes, Canad. J. Math. 16 (1964), 443-472.

[26] N.L. Johnson, V. Jha, M. Biliotti, *Handbook of Finite Translation Planes*, Pure Appl. Math. (Boca Raton), vol. 289, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[27] W.M. Kantor, Spreads, translation planes and Kerdock sets, I, SIAM J. Alg. Disc. Methods 3 (1982), 151-165.

[28] W. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes, J. Algebra 106 (1987), 15-45.

[29] W.M. Kantor, Two families of flag-transitive affine planes, Geom. Dedicata 41 (1992), 191-200.

[30] W.M. Kantor, 2-transitive and flag-transitive designs, in: D. Jungnickel, S.A. Vanstone (Eds), *Coding Theory, Design Theory, Group Theory*, Wiley, New York, 1993, pp. 13-30.

[31] W. M. Kantor, C. Suetake, A note on some flag-transitive affine planes, J. Combin. Theory Ser. A 65 (1994), 307-310.

[32] W.M. Kantor, M.E. Williams, New Flag-Transitive Affine Planes of Even Order, J. Combin. Theory Ser. A 74 (1996), 1-13.

[33] M. Lavrauw, Sublines of prime order contained in the set of internal points of a conic, Des. Codes Cryptogr. 38 (2006), 113-123.

[34] M. Lavrauw, O. Polverino, Finite Semifields, in: L. Storme, J.D. Beule (Eds), *Current Research Topics in Galois Geometry*, 2011, pp. 127-155.

[35] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, Cambridge, 1997.

[36] H. Luneburg, *Ü*ber projektive Ebenen in denen jede Fahne von einer nicht-trivialen Elation invariant gelassen wird, Abh. Math. Sem. Univ. Hamburg 29 (1965), 37-76.

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

[38] G. Menichetti, n-Dimensional algebras over a field with a cyclic extension of degree n, Geom. Dedicata 63 (1996) 69-94.

[39] K. Minami, N. Nakagawa, On planar functions of elementary abelian p-group type, Hokkaido Math. J. 37 (2008), 531-544.

[40] G.L. Mullen, D. Panario, *Handbook of finite fields*, CRC Press, 2013.

[41] T. Penttila, B. Williams, Ovoids of parabolic spaces, Geom. Dedicata 82 (2000), 1-19.

[42] A.R. Prince, Flag-transitive affine planes of order at most 125, J. Geom. 67 (2000), 208-216.
[43] C. Suetake, Flag transitive planes of order q^n with a long cycle ℓ_∞ as a collineation, Graphs Combin. 7 (1991), 183-195.
[44] C. Suetake, On flag-transitive affine planes of order q^3, Geom. Dedicata 51 (1994), 123-131.
[45] K. Thas, Finite flag-transitive projective planes: a survey and some remarks, Discrete Math. 266 (2003), 417-429.
[46] K. Thas, D. Zagier, Finite projective planes, Fermat curves, and Gaussian periods, J. Eur. Math. Soc. 10 (2008), 173-190.
[47] A. Wagner, On finite affine line transitive planes, Math. Z. 87 (1965), 1-11.
[48] G. Weng, X. Zeng, Further results on planar DO functions and commutative semifields, Des. Codes Cryptogr. 63 (2012), 413-423.
[49] Y. Zhou, A. Pott, A new family of semifields with 2 parameters, Adv. Math. 234 (2011), 43-60.

School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China
E-mail address: `tfeng@zju.edu.cn`