SEMIFIELDS, RELATIVE DIFFERENCE SETS, AND BENT FUNCTIONS

ALEXANDER POTT, KAI-UWE SCHMIDT, AND YUE ZHOU

ABSTRACT. Recently, the interest in semifields has increased due to the discovery of several new families and progress in the classification problem. Commutative semifields play an important role since they are equivalent to certain planar functions (in the case of odd characteristic) and to modified planar functions in even characteristic. Similarly, commutative semifields are equivalent to relative difference sets. The goal of this survey is to describe the connection between these concepts. Moreover, we shall discuss power mappings that are planar and consider component functions of planar mappings, which may be also viewed as projections of relative difference sets. It turns out that the component functions in the even characteristic case are related to negabent functions as well as to $\mathbb{Z}_4$-valued bent functions.

1. INTRODUCTION

Semifields, also called distributive quasifields, have been investigated for almost a century. In this article, we do not want to give a survey about semifields in general, but rather concentrate on commutative semifields. Using the so called Knuth orbit, these are also equivalent to symplectic semifields. It is also not the intention of this article to survey commutative (or symplectic) semifields in general. We refer the reader to the excellent introduction by Lavrauw and Polverino [25]. The aim here is to discuss the equivalence between semifields, relative difference sets, and certain planar functions, which are mappings on finite fields. We hope that the investigation of relative difference sets may also stimulate the research on semifields. For instance, for the investigation of relative difference sets, tools from algebraic number theory are often used, which as far as we know have been only recently applied in the theory of semifields [33].

There is a difference between semifields in even and odd characteristic, which induces also differences between their corresponding relative difference sets and their planar functions. For example, on the level of the associated relative difference set, the ambient group is elementary abelian in the odd characteristic case, whereas it equals $\mathbb{Z}_4^n$ (for some n) in the even characteristic case. Using so called projections of relative difference sets, one obtains relative difference sets in subgroups. Such a projection may be viewed as a component function of the planar function associated with the relative difference set. In the case of odd characteristic, the components are p-ary bent functions, whereas in the even characteristic case they are (essentially) negabent functions.

This survey is organized as follows. In Section 2, we recall some results on semifields, including the connection to projective planes, and discuss the equivalence problem for semifields. In Section 3, we give some background on relative difference sets. In Section 4, we explain the connection between these concepts. In particular we give a partial

1

characterization of those relative difference sets that correspond to commutative semi-fields. In Sections 5 and 6, we look more closely at some examples of semifields, in particular at those that can be described by monomial planar functions. Section 5 deals with the odd characteristic case and Section 6 with the even characteristic case. In Section 7, we briefly investigate the component functions or, equivalently, the projections of the corresponding relative difference sets. We conclude with some open problems in Section 8.

2. Semifields

Roughly speaking, a semifield is a field without associativity for the multiplication. More precisely, a (finite) semifield is defined as follows.

Definition 2.1. Let $\mathbb{S}$ be a finite set containing at least two elements. Then $\mathbb{S}$ together with two binary operations $+$ and $\circ$ is a *semifield* $(\mathbb{S}, +, \circ)$ if the following hold:

(S1) $(\mathbb{S}, +)$ is an abelian group with identity element 0.
(S2) $x \circ (y + z) = x \circ y + x \circ z$ and $(x + y) \circ z = x \circ z + y \circ z$ for all $x, y, z \in \mathbb{S}$.
(S3) $x \circ y = 0$ implies $x = 0$ or $y = 0$.
(S4) There is an element $1 \neq 0$ such that $1 \circ x = x \circ 1 = x$ for all $x \in \mathbb{S}$.

If (S4) is missing, then $\mathbb{S}$ is a *pre-semifield*. If the operation $\circ$ is commutative, then $\mathbb{S}$ is a *commutative* semifield.

Notice that, since $\mathbb{S}$ is finite, each of the equations

$$a \circ x = b$$
$$x \circ a = b$$

has a unique solution x (this would not be true if $\mathbb{S}$ were infinite, in which case the existence of a solution of the above equations has to be added to the axioms for a semifield).

The distributive laws together with (S3) simply say that multiplication from the left and multiplication from the right act as automorphisms of the additive group of the semifield. Let a and b be two nonzero elements in $\mathbb{S}$. Then we find an automorphism x of $(\mathbb{S}, +)$ such that $x \circ a = b$. Hence a and b have the same order and $\mathbb{S}$ must be an elementary abelian p-group. This prime number p is also called the *characteristic* of the semifield.

Of course, finite fields are semifields. For a current list of known semifields (including some infinite families and some sporadic examples), we refer to [25]. We shall see several examples in later sections, which we describe in terms of planar functions. We note that semifields of order p or p^2 are necessarily finite fields [10]. Moreover, there are only two classes of semifields of order p^3 [28]. The situation is getting much more involved for semifields of order p^4.

The fascination of semifields comes from the fact that the elements in $\mathbb{S}$ have two different meanings: Multiplication from the left is a bijective linear mapping on $\mathbb{S}$, viewed as a vector space, but the elements on the right hand side of $\circ$ are just considered to be vectors. This may help to motivate the following definition of isotopy of semifields.

Definition 2.2. Two semifields $(\mathbb{S}, +, \circ_s)$ and $(\mathbb{T}, +, \circ_t)$ are *isotopic* if there are bijective linear mappings F, G, and H from $\mathbb{T}$ to $\mathbb{S}$ such that

$$F(x) \circ_s G(y) = H(x \circ_t y) \quad \text{for all } x, y \in \mathbb{T}.$$

There are essentially two reasons why isotopism is defined in this unusual way, involving different mappings F and G on the two sides of a product $x \circ y$. One reason is that, as mentioned above, semifield elements on the left are associated with linear mappings, whereas on the right they are interpreted as vectors. Another reason is that every semifield can be used to construct a projective plane and, as we shall see in Proposition 2.10, isotopy just means that the planes are isomorphic. (We do not recall the definition of an isomorphism of an incidence structure here, since we hope it is clear. Otherwise we refer to [4, Section I.4].) It is known that every pre-semifield is isotopic to a semifield [25], which is the reason why we restrict ourselves to semifields.

Definition 2.3. A *projective plane* is a point-line incidence structure with the following three properties:

(P1) Every two different points are contained in a unique line.
(P2) Every two different lines intersect in exactly one point.
(P3) There are four points with the property that no three of them are contained in a single line.

For background on projective planes, we refer the reader to [20]. If the number of points and lines in a projective plane is finite, then there is a number n (called the *order* of the plane) such that each line contains exactly $n + 1$ points and through each point there are exactly $n + 1$ lines.

The following are perhaps the two most famous open problems concerning projective planes.

Question 2.4 (Prime power conjecture)**.** Is the order of a finite projective plane necessarily a prime power?

Question 2.5. Is a projective plane of prime order unique (up to isomorphism)?

Most researchers believe that Question 2.5 has a positive answer.
We shall now describe how a projective plane can be constructed from a semifield.

Construction 2.6. Let $(\mathbb{S}, +, \circ)$ be a semifield and let $m, b \in \mathbb{S}$. We define a point $(x, y) \in \mathbb{S} \times \mathbb{S}$ to be on the line $[m, b]$ if $m \circ x + b = y$. This defines a point-line incidence structure with $|\mathbb{S}|^2$ points and $|\mathbb{S}|^2$ lines.

The incidence structure in Construction 2.6 is not quite a projective plane. It is a divisible design, whose definition is recalled below. We shall see in Construction 2.9 how a divisible design gives rise to a projective plane. For background and a substantial collection of results on divisible designs and projective planes, we refer the reader to the two books [4].

Definition 2.7. A *divisible design* with parameters (m, n, k, λ) is a point-line incidence structure with mn points and mn lines that satisfies the following properties:

(D1) The point set can be partitioned into m point classes, each of size n.
(D2) The line set can be partitioned into m line classes, each of size n.
(D3) Every two different points not in a common point class are joined by exactly λ lines.
(D4) Every two different lines not in a common line class intersect in exactly λ points.
(D5) Every line contains exactly k points, and through every point there are exactly k lines.

Note that the definition of a divisible design (as the definition of a projective plane) is symmetric in points and lines. Hence the incidence structure obtained by interchanging points and lines (the so called *dual incidence structure*) is again a divisible design (a projective plane).

The following result is readily verified using the defining properties of a semifield.

Proposition 2.8. *If $\mathbb{S}$ is a semifield of order n, then Construction 2.6 gives a divisible $(n, n, n, 1)$ design.*

We now show how to extend such a divisible design uniquely to a projective plane by adding $n + 1$ points and $n + 1$ lines.

Construction 2.9. Let $\mathcal{D}$ be a divisible $(n, n, n, 1)$ design. Add a new point ∞. For each point class $\mathcal{P}$ of $\mathcal{D}$, add a new line joining the points in $\mathcal{P}$ and ∞. For each line class $\mathcal{L}$ of $\mathcal{D}$, add a new point $\infty_{\mathcal{L}}$ to each line in $\mathcal{L}$. Finally, add a new line joining all new points. It is not difficult to see that this incidence structure is a projective plane of order n.

We note that two isomorphic divisible designs give rise to isomorphic projective planes, but the converse is not necessarily true: One projective plane may be obtained from different (non-isomorphic) divisible designs. This can occur if the automorphism group of the plane is not transitive on lines.

A *semifield plane* of order n is the projective plane constructed from a semifield of order n via Constructions 2.6 and 2.9. The next result shows why semifield isotopy is a natural concept.

Proposition 2.10 ([1])**.** *Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.*

Given a semifield with multiplication $\circ$, another semifield with multiplication $\star$ can be obtained by changing the order of the multiplication, viz $x \star y := y \circ x$. There is a more subtle possibility to obtain more semifields from just one semifield via the Knuth orbit. We refer the reader to [24] for details.

We conclude this section by showing how a spread can be obtained from a semifield. Let $(\mathbb{S}, +, \circ)$ be a semifield of characteristic p. Let $e_1, \ldots, e_n$ be a basis of $\mathbb{S}$, viewed as a vector space over the field with p elements. The mappings $e_i : \mathbb{S} \to \mathbb{S}$ defined by $e_i(v) := e_i \circ v$ are linear and bijective. Moreover, the vector space W of linear mappings on $\mathbb{S}$ spanned by $e_1, \ldots, e_n$ has dimension n and consists of $p^n - 1$ bijective linear mappings and the zero mapping. As F ranges over W, the sets $\{(x, F(x)) : x \in \mathbb{S}\}$ form a set of p^n subspaces of $\mathbb{S} \times \mathbb{S}$, each of dimension n. These subspaces together with $\{(0, x) : x \in \mathbb{S}\}$ form a spread, namely a set of $p^n + 1$ n-dimensional subspaces of the $2n$-dimensional space $\mathbb{S} \times \mathbb{S}$ intersecting pairwise trivially. A spread corresponding to a semifield is called *semifield spread*.

3. Relative difference sets

We now describe a concept, which seems at a first glance unrelated to semifields.

Definition 3.1. Let G be a group of order mn containing a subgroup N of order n. A k-subset R of G is called a *relative (m, n, k, λ) difference set* (relative to N) if the list of nonzero differences $r - r'$ with $r, r' \in R$ contains all elements in $G \setminus N$ exactly λ times and no element in N. The subgroup N is called the *forbidden subgroup*.

Sometimes we simply say that R is a difference set relative to N. In case that $N = \{0\}$, the definition of a relative difference set coincides with the definition of a difference set in the usual sense. We refer the reader to [4], [31], [32] for background.

Example 3.2. (a) The set $\{1, 2, 4\} \subseteq \mathbb{Z}_8$ is a relative $(4, 2, 3, 1)$ difference set. The forbidden subgroup is the unique subgroup $4\mathbb{Z}_8 = \{0, 4\}$ of order 2 in $\mathbb{Z}_8$.

(b) The set $\{(0,0), (0,1), (1,3), (3,0)\}$ is a relative $(4, 4, 4, 1)$ difference set in $\mathbb{Z}_4 \times \mathbb{Z}_4$ with forbidden subgroup $2\mathbb{Z}_4 \times 2\mathbb{Z}_4$.

(c) The set $\{(0,0), (1,1), (2,1)\}$ is a relative difference set in $\mathbb{Z}_3 \times \mathbb{Z}_3$ with forbidden subgroup $\{0\} \times \mathbb{Z}_3$.

We now show how to construct a divisible design from a relative difference set.

Construction 3.3. Let R be a relative (m, n, k, λ) difference set in a group G with forbidden subgroup N. We construct a divisible (m, n, k, λ) design as follows. The points are the elements of G and the lines are the translates $R + g$ with $g \in G$. The point classes are the (right) cosets of N. Similarly, the line classes are induced by the (right) cosets of N. The group G itself acts via right translation $\tau_g : x \mapsto x + g$ regularly (=sharply transitively) on the points as well as on the lines.

Conversely, a divisible designs that admits an automorphism group acting regularly on points and lines can be described by a relative difference set. This is a well known fact in design theory [4, Section VI.10].

Note that translation τ_x by elements $x \in N$ fixes the point class N, but not necessarily the right cosets of N. The right cosets of N are fixed if and only if N is a normal subgroup. Sometimes normality of N is part of the definition of a relative difference set.

In view of Constructions 2.9 and 3.3, a relative difference set with parameters $(n, n, n, 1)$ gives rise to a projective plane of order n. It is remarkable that the prime power conjecture (see Question 2.4) has been solved in the special case that the plane can be described by such a relative difference set in an abelian group. This was proved by Ganley [12] for even n (see also [22]) and by Blokhuis, Jungnickel, and Schmidt [6] for odd n.

Theorem 3.4 ([12], [6]). *Let R be a relative $(n, n, n, 1)$ difference set in an abelian group G. If n is even, then $n = 2^m$ (for some m) and G is isomorphic to $\mathbb{Z}_4^m$ and the forbidden subgroup is isomorphic to $\mathbb{Z}_2^m$. If n is odd, then $n = p^m$ where p is a prime and G contains an elementary abelian subgroup of order p^{m+1}.*

The following problem remains unsolved.

Question 3.5. Let q be an odd prime power and let R be a relative $(q, q, q, 1)$ difference set in an abelian group G. Is it true that G must be elementary abelian?

Another question is which planes can be obtained from relative $(n, n, n, 1)$ difference sets. We shall see in the next section that with the exception of a single family, all known relative $(n, n, n, 1)$ difference sets give rise to semifield planes. Moreover, all known examples of relative difference sets with parameters $(p^2, p^2, p^2, 1)$ or $(p, p, p, 1)$ describe Desarguesian planes (namely semifield planes constructed from finite fields). This is not a surprise in the latter case since, as mentioned in connection with Question 2.5, it is conjectured that there is only one plane of prime order (which is necessarily Desarguesian). For planes coming from relative difference sets, this has been proved independently in [16], [17], [34].

Theorem 3.6. *A projective plane described by a relative $(p, p, p, 1)$ difference set with p prime is Desarguesian. Moreover, the relative difference set is unique up to equivalence.*

It is an open question as to whether all projective planes described by relative $(p^2, p^2, p^2, 1)$ difference sets (with p prime) are Desarguesian. Since a semifield of order p^2 is necessarily a finite field, a putative counterexample cannot be a semifield plane.

In connection with relative difference sets, there are two concepts of equivalence. We call two relative difference sets R and R' in a group G *equivalent* if there is a group automorphism φ of G and a group element $g \in G$ such that $R' = \varphi(R) + g$. It is readily verified that equivalent relative difference sets describe isomorphic divisible designs. The converse is in general not true. We call two relative difference sets *isomorphic* if their corresponding divisible designs are isomorphic. Of course, two isomorphic relative difference sets are equivalent. In general, determining whether two relative difference sets are isomorphic is much more difficult than determining whether they are equivalent.

Relative difference sets have the following nice property.

Proposition 3.7. *Let R be an (m, n, k, λ) difference set in an abelian group G relative to N. Let U be a subgroup of N of order u and let φ denote the canonical epimorphism $G \to G/U$. Then $\varphi(R)$ is a difference set with parameters $(m, n/u, k, \lambda u)$ relative to N/U.*

With the notation as in Proposition 3.7, suppose that N can be written as a direct product of abelian groups $N_1, \ldots, N_s$. Then we may take a set of coset representatives $g_1, \ldots, g_m$ of N in G and describe the new relative difference set using a mapping $g_i \mapsto n_i$ from the set of coset representatives into the group N. The element n_i can be written as a product $\prod_{j=1}^{s} n_i^{(j)}$ with $n_i^{(j)} \in N_j$. We may view the mappings $g_i \mapsto n_i^{(j)}$ as the component functions of the relative difference set. Note that there is much freedom in this construction since we may change the set of coset representatives arbitrarily. Hence it is not the mapping that is important here but the mapping together with the choice of coset representatives. In case that the relative difference set is splitting, there is a canonical set of coset representatives, namely the elements in a group theoretic complement of N.

4. Relative difference sets and semifields

We have already seen that a projective plane of order n can be constructed from a relative $(n, n, n, 1)$ difference set and also from a semifield of order n. The following fundamental theorem shows that a semifield of order n also gives rise to a relative $(n, n, n, 1)$ difference set (see [21] and [13], for example).

Theorem 4.1. *Let $(\mathbb{S}, +, \circ)$ be a semifield of order n. Then the set $R = \{(x, x \circ x) : x \in \mathbb{S}\}$ is a relative $(n, n, n, 1)$ difference set in $G = \{(x, y) : x, y \in \mathbb{S}\}$, where the group operation on G is given by*

$$(x, y) \star (x', y') = (x + x', y + y' + x \circ x').$$

The forbidden subgroup is $N = \{(0, y) : y \in \mathbb{S}\}$.

Proof. It is straightforward to check that G is a group. The inverse element of $(x, y) \in G$ is

$$(x, y)^{-1} = (-x, -y + x \circ x).$$

The differences that we can form with elements from R are

$$
\begin{aligned}
(a, a \circ a) \star (b, b \circ b)^{-1} &= (a, a \circ a) \star (-b, 0) \\
&= (a - b, a \circ a - a \circ b) \\
&= (a - b, a \circ (a - b)),
\end{aligned}
$$

whose nonzero values cover all elements in $G \setminus N$ exactly once. □

Remark 4.2. The group G in Theorem 4.1 is commutative if and only if the semifield is commutative. The order of the elements in $G \setminus N$ equals p if p is odd and equals 4 if $p = 2$. In both cases, the forbidden subgroup N is elementary abelian.

We may also ask whether the converse of Theorem 4.1 is true, namely is it possible to construct a semifield starting from a relative difference set with parameters $(n, n, n, 1)$? A partial answer to this question can be given in the case that the ambient group G is either $\mathbb{Z}_4^m$ or $\mathbb{Z}_p^m$ for an odd prime p.

We first consider the case that G is an abelian p-group and p is odd. We represent G as the additive group of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. It is not hard to verify that every relative $(p^m, p^m, p^m, 1)$ difference set in G can be written as

$$
R = \{(x, f(x)) : x \in \mathbb{F}_{p^m}\}
$$

for some function $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$, in which case the forbidden subgroup is $\{0\} \times \mathbb{F}_{p^m}$. The set R is a relative difference set if and only if the equation $f(x + a) - f(x) = b$ has a unique solution x for all $a, b \in \mathbb{F}_{p^m}$ with $a \neq 0$. Functions with this property are called *planar*. Here we give a definition, which is valid for all groups.

Definition 4.3. Let H and N be two groups. A function $f : H \to N$ is *planar* if the mapping $\delta_a : H \to N$ defined by $\delta_a(x) = f(x + a) - f(x)$ is bijective for all nonzero $a \in H$.

The following result is readily verified.

Proposition 4.4. *Let H and N be two groups of order n and let R be a subset of $H \times N$. Then R is an $(n, n, n, 1)$ difference set in $H \times N$ relative to $\{0\} \times N$ if and only if there is a planar function $f : H \to N$ such that*

$$
R = \{(x, f(x)) : x \in H\}.
$$

In view of Proposition 4.4 and Constructions 2.9 and 3.3, every planar function corresponds to a unique projective plane. A partial answer to the question of which relative difference sets describe semifield planes can be given in terms of planar functions, for which we need one more definition. Note that every mapping $f : \mathbb{F}_q \to \mathbb{F}_q$ is a polynomial mapping $f(x) = \sum_{i=0}^{q-1} a_i x^i$ for some uniquely determined $a_0, \ldots, a_{q-1} \in \mathbb{F}_q$.

Definition 4.5. Let p be a prime. A polynomial $f \in \mathbb{F}_{p^m}[x]$ (and also the corresponding mapping) is called *Dembowski-Ostrom* if, for some $a_{i,j} \in \mathbb{F}_{p^m}$,

$$
f(x) = \sum_{0 \leq i \leq j < m} a_{i,j} x^{p^i + p^j}
$$

for odd p or

$$
f(x) = \sum_{0 \leq i < j < m} a_{i,j} x^{p^i + p^j}
$$

for $p = 2$. The polynomial f is *affine* if $f(x) = \sum_{i=0}^{m-1} c_i x^{p^i} + d$ for some $c_i, d \in \mathbb{F}_{p^m}$. An *affine Dembowski-Ostrom polynomial* is a sum of a Dembowski-Ostrom polynomial and an affine polynomial.

Our next result, which is essentially [7, Theorem 3.3], gives the promised partial answer to the question of which relative difference sets describe semifield planes.

Theorem 4.6. *Let q be an odd prime power and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a mapping. If f is an affine Dembowski-Ostrom planar function, then the corresponding projective plane is a semifield plane, where the semifield is isotopic to the (commutative) pre-semifield $(\mathbb{F}_q, +, \circ)$ whose multiplication is given by $x \circ y = f(x + y) - f(x) - f(y) + f(0)$. Conversely, if a projective plane is a semifield plane corresponding to a commutative semifield $(\mathbb{S}, +, \star)$, then $f(x) = x \star x$ is a Dembowski-Ostrom planar function.*

Now suppose that $f : \mathbb{F}_q \to \mathbb{F}_q$ is a planar function, but not an affine Dembowski-Ostrom polynomial. Is it possible that the corresponding projective plane is a semifield plane (where the semifield multiplication is possibly not related in an obvious way to the function f)? As far as we know, this problem remains open.

Only one family of planar functions not of Dembowski-Ostrom type is known. It is also known that the corresponding projective planes are not semifield planes.

Theorem 4.7 ([8]). *Let $f : \mathbb{F}_{3^m} \to \mathbb{F}_{3^m}$ be a mapping defined by $f(x) = x^{(3^k+1)/2}$. Then f is planar if $\gcd(k, 2m) = 1$. If $3 \leq k < m - 1$, the corresponding projective plane is not a semifield plane.*

The following nice observation is contained in [39].

Proposition 4.8 ([39, Theorem 2.3]). *Let q be an odd prime power and let $f \in \mathbb{F}_q[x]$ be a Dembowski-Ostrom polynomial. Then f is planar if and only if f is a 2-to-1 mapping, namely $f(x) = a$ has 0 or 2 solutions in x for all nonzero $a \in \mathbb{F}_q$.*

Example 4.9. The mapping $x \mapsto x^{10} \pm x^6 - x^2$ on $\mathbb{F}_{3^m}$ is planar for odd m (and also Dembowski-Ostrom). These functions have been found [8] and [11]. The planarity is easily verified using Proposition 4.8. First observe that the polynomial $y^5 \pm y^3 - y$ is a Dickson polynomial, which is a permutation polynomial in $\mathbb{F}_{3^m}[y]$ if and only if m is odd [27, Theorem 6.17]. Hence, after replacing y by x^2, we obtain a 2-1 Dembowski-Ostrom mapping on $\mathbb{F}_{3^m}$ for odd m.

Next we consider the case that the ambient group G is $\mathbb{Z}_4^m$. Unlike in the case that G is elementary abelian, there is no canonical way to represent G by the additive group of a finite field. One may use the Galois ring $\mathrm{GR}(4, m)$ as in [37], which has the advantage that the Galois ring multiplication can be used, but we prefer a different (equivalent) approach.

We represent the group $\mathbb{Z}_4^m$ as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with the group operation

$$(1) \qquad\qquad (x, y) \star (x', y') = (x + x', y + y' + x \cdot x').$$

Since this group is not a direct product of two groups of order 2^m, we cannot use Proposition 4.4 to construct relative $(2^m, 2^m, 2^m, 1)$ difference sets in this group. However, observe that every relative $(2^m, 2^m, 2^m, 1)$ difference set in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ can still be written as

$$R = \{(x, f(x)) : x \in \mathbb{F}_{2^m}\}$$

for some function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, in which case the forbidden subgroup is $\{0\} \times \mathbb{F}_{2^m}$. It is then readily verified that R is a relative difference set if and only if the equation

$$f(x + a) - f(x) + a \cdot x = b$$

has a unique solution x for all $a, b \in \mathbb{F}_{2^m}$ with $a \neq 0$. We therefore modify the definition of a planar function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$, which reflects the structure of the ambient group.

Definition 4.10. A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is *planar* if $x \mapsto f(x + a) + f(x) + ax$ is a permutation on $\mathbb{F}_{2^m}$ for all nonzero $a \in \mathbb{F}_{2^m}$.

There will be no confusion of this definition with Definition 4.3 since every function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ satisfies

$$f(x + a) - f(x) = f((x + a) + a) - f(x + a) \quad \text{for all } x, a \in \mathbb{F}_{2^m},$$

and hence planar functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ according to Definition 4.3 cannot exist. A trivial example of a planar function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is $f(x) = 0$. More generally, every affine polynomial $f \in \mathbb{F}_{2^m}[x]$ induces a planar function on $\mathbb{F}_{2^m}$.

We have now established the following result, which is essentially contained in [41].

Theorem 4.11 ([41])**.** *Let R be a subset of the group $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ whose operation is given in (1). Then R is a $(2^m, 2^m, 2^m, 1)$ difference set relative to $\{0\} \times \mathbb{F}_{2^m}$ if and only if there is a planar function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ such that*

$$R = \{(x, f(x)) : x \in \mathbb{F}_{2^m}\}.$$

Theorem 4.11 should be compared with Proposition 4.4. Again, by Constructions 2.9 and 3.3, every planar function according to Definition 4.10 corresponds to a unique projective plane. We also have the following counterpart of Theorem 4.6.

Theorem 4.12. *Let q be a power of 2 and let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a mapping. If f is an affine Dembowski-Ostrom planar function, then the corresponding projective plane is a semifield plane, where the semifield is isotopic to the (commutative) pre-semifield $(\mathbb{F}_q, +, \circ)$ whose multiplication is given by $x \circ y = f(x + y) + f(x) + f(y) + f(0) + xy$. Conversely, if a projective plane is a semifield plane corresponding to a commutative semifield $(\mathbb{S}, +, \star)$, then $f(x) = x \star x$ is a Dembowski-Ostrom planar function.*

All known planar functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ are induced by affine Dembowski-Ostrom polynomials. Hence, in view of Theorem 4.12, all known planar functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ produce semifield planes. This is contrary to the case of planar functions from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ for p an odd prime, where we have the exceptional example given in Theorem 4.7.

5. Planar functions in odd characteristic

We have seen in the previous section that every commutative semifield can be described by a planar function. We do not claim that such a description is natural and indeed the planar function of a commutative semifield can look quite cumbersome. However, interesting examples of commutative semifields have been found using Dembowski-Ostrom planar functions (see [40] and [42], for example). We have already seen examples of such planar functions in Example 4.9.

In what follows, we let p be an odd prime and consider the simplest polynomial mappings on $\mathbb{F}_{p^m}$, namely monomial mappings $x \mapsto cx^d$. It is readily verified that in order to study planar monomials cx^d in $\mathbb{F}_{p^m}[x]$, we can without loss of generality restrict

TABLE 1. Known planar monomial mappings x^d on $\mathbb{F}_{p^m}$

d	p	condition	reference
2	odd	none	folklore, Desarguesian plane
$p^k + 1$	odd	$\dfrac{m}{\gcd(k, m)}$ is odd	commutative Albert semifields [2]
$\dfrac{p^k + 1}{2}$	3	$\gcd(k, 2m) = 1$	Coulter-Matthews [8]

ourselves to the case $c = 1$ and $d < p^m$ and $p \nmid d$. The only known examples of planar monomial mappings $x \mapsto x^d$ on $\mathbb{F}_{p^m}$ with $d < p^m$ and $p \nmid d$ are given in Table 1.

It is sometimes conjectured that the list of examples given Table 1 is exhaustive. We believe that this is difficult to prove. It is however possible to get a slightly weaker result, for which we need the following definition.

Definition 5.1. Let p be a prime. A monomial x^d in $\mathbb{F}_p[x]$ is *exceptional planar* if x^d induces a planar function on infinitely many extensions of $\mathbb{F}_p$.

Notice that the mappings in Table 1 are all exceptional. Indeed, it has been proved in [26] and [43] that there are no further examples (the case that $p \mid d - 1$ is handled in [26] and the remaining cases are settled in [43]).

Theorem 5.2 ([26], [43]). *The only exceptional planar monomials x^d in $\mathbb{F}_p[x]$ with $p \nmid d$ are those given in Table 1.*

6. PLANAR FUNCTIONS IN CHARACTERISTIC 2

In this section, we give some examples of planar functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ according to Definition 4.10. We have already seen that every affine polynomial in $\mathbb{F}_{2^m}[x]$ induces a planar function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. These are trivial examples. A large family of nontrivial examples were given in [41], which is based on a construction for commutative semifields due to Kantor [23].

Theorem 6.1 ([41, Example 2.2]). *Assume that we have a chain of finite fields $\mathbb{K} = \mathbb{K}_0 \supset \mathbb{K}_1 \supset \cdots \supset \mathbb{K}_n$ of characteristic 2 with $[\mathbb{K} : \mathbb{K}_n]$ odd. Let tr_i be the relative trace from $\mathbb{K}$ to $\mathbb{K}_i$. Then, for all nonzero $\zeta_1, \ldots, \zeta_n \in \mathbb{K}$, the mapping $f : \mathbb{K} \to \mathbb{K}$ given by*

$$f(x) = \left(x \sum_{i=1}^{n} \mathrm{tr}_i(\zeta_i x) \right)^2$$

is planar.

Kantor [23] also gives a lower bound on the number of non-isomorphic projective planes constructed by the planar functions in Theorem 6.1.

In what follows, we consider planar monomial mappings $x \mapsto cx^d$ on $\mathbb{F}_{2^m}$. Unlike in the case of odd characteristic, the planarity of this function can depend on the choice of the coefficient c. We can however assume without loss of generality that $d < 2^m$. We are interested in those exponents $d < 2^m$ such that $x \mapsto cx^d$ is planar on $\mathbb{F}_{2^m}$ for some nonzero $c \in \mathbb{F}_{2^m}$. The only known such exponents are listed in Table 2. A full characterization of those $c \in \mathbb{F}_{2^m}$ for which these monomials are planar on $\mathbb{F}_{2^m}$ is also

TABLE 2. Known exponents d such that cx^d is planar on $\mathbb{F}_{2^m}$ for some $c \in \mathbb{F}_{2^m}$

d	condition	reference
2^k	none	trivial
$2^k + 1$	$m = 2k$	[37]
$4^k(4^k + 1)$	$m = 6k$	[35]

given in [35]. It can be shown that the planes corresponding to the planar functions identified in Table 2 are all Desarguesian.

It has been conjectured in [37] that the list provided in Table 2 is exhaustive. As in the case of odd characteristic, we believe that this is difficult to prove. We are therefore interested in classifying *exceptional planar exponents*, namely positive integers d such that $x \mapsto cx^d$ is planar on $\mathbb{F}_{2^m}$ for some nonzero $c \in \mathbb{F}_{2^m}$ and infinitely many m. It was shown in [37] that, if d is an odd exceptional planar exponent, then $d = 1$. The even exceptional planar exponents have been classified in [29]. In fact, the following sharper result was proved in [29].

Theorem 6.2 ([29, Theorem 1.1]). *Let d be a positive integer such that $d^4 \leq 2^m$ and let $c \in \mathbb{F}_{2^m}$ be nonzero. Then the function $x \mapsto cx^d$ is planar on $\mathbb{F}_{2^m}$ if and only if d is a power of 2.*

7. COMPONENT FUNCTIONS OF PLANAR FUNCTIONS

In this section we study the component functions corresponding to a planar function. When p is an odd prime, the component functions of a planar function on $\mathbb{F}_{p^m}$ are p-ary bent functions. These are well-studied objects. We therefore study the component functions corresponding to a planar function on $\mathbb{F}_{2^m}$, according to Definition 4.10. Identifying such a planar function with a $(2^m, 2^m, 2^m, 1)$ difference set in $\mathbb{Z}_4^m$ relative to $2\mathbb{Z}_4^m$, the component functions are obtained by a projection with respect to a subgroup of $2\mathbb{Z}_4^m \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ of order 2^{m-1} (see Proposition 3.7). Thus the component functions correspond to relative $(2^m, 2, 2^m, 2^{m-1})$ difference sets in $\mathbb{Z}_4 \times \mathbb{Z}_2^{m-1}$. We represent this group as follows. Let B be a symmetric bilinear form on $\mathbb{F}_2^m$, write

$$G = \{(x, y) : x \in \mathbb{F}_2^m, y \in \mathbb{F}_2\},$$

and define an operation on G via

$$(2) \qquad\qquad (x, y) * (x', y') = (x + x', y + y' + B(x, x')).$$

Proposition 7.1. *With the notation as above, $(G, *)$ is an abelian group isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2^{m-1}$ if B is nonalternating and isomorphic to $\mathbb{Z}_2^{m+1}$ if B is alternating.*

Proof. It is immediate that $(G, *)$ is abelian. We have $(x, y) * (x, y) = (0, B(x, x))$. Hence, the nonzero elements in G have order 2 or 4. If B is alternating, then every element in G has order 2 and G is isomorphic to $\mathbb{Z}_2^{m+1}$. If B is nonalternating, then $B(x, x)$ is a nontrivial linear form, from which we see that exactly half of the elements in G have order 2 and therefore G is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2^{m-1}$. $\square$

The following result characterizes the relative $(2^m, 2, 2^m, 2^{m-1})$ difference sets in G.

Theorem 7.2. *Let R be a subset of G whose operation is given in* (2). *Then R is a* $(2^m, 2, 2^m, 2^{m-1})$ *difference set in G relative to* $N = \{(0, y) : y \in \mathbb{F}_2\}$ *if and only if there is a function* $f : \mathbb{F}_2^m \to \mathbb{F}_2$ *such that*

$$f(x + a) + f(x) + B(a, x) = b$$

has 2^{m-1} solutions for all $b \in \mathbb{F}_2$ and all nonzero $a \in \mathbb{F}_2^m$ and

$$(3) \qquad\qquad R = \{(x, f(x)) \ : \ x \in \mathbb{F}_2^m\}.$$

Proof. Note that the inverse of $(x, y) \in G$ is given by

$$(x, y)^{-1} = (x, y + B(x, x)).$$

We therefore obtain, for all $x, a \in \mathbb{F}_2^m$,

$$(4) \qquad (x + a, f(x + a)) * (x, f(x))^{-1} = (a, f(x + a) + f(x) + B(a, x)).$$

We now readily verify that, if f has the properties stated in the theorem, then R is a $(2^m, 2, 2^m, 2^{m-1})$ difference set relative to N. Conversely, if R is such a relative difference set, then there is some function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ such that (3) holds. From (4) we then verify that f must have the properties stated in the theorem. $\qquad\square$

Let f be a function from $\mathbb{F}_2^m$ to $\mathbb{F}_2$ and write $R = \{(x, f(x)) \ : \ x \in \mathbb{F}_2^m\}$. It is well known that relative difference sets are subsets of a group with certain character values. In particular, R is a $(2^m, 2, 2^m, 2^{m-1})$ difference set in G relative to $N = \{(0, y) : y \in \mathbb{F}_2\}$ if and only if

$$\left| \sum_{z \in R} \chi(z) \right|^2 = 2^m$$

for every character χ of G that is nontrivial on N. The characters of G depend on the choice of the bilinear form B. Take the standard bilinear form defined via the scalar product

$$B(x, y) = \langle x, y \rangle.$$

Then the characters of G are as follows. For $a \in \mathbb{F}_2^m$, the functions $\chi_a : G \to \mathbb{C}$ defined by

$$\chi_a(x, y) = (-1)^{\langle a, x \rangle}$$

are the 2^m characters of G that are trivial on N. Define $\gamma : G \to \mathbb{C}$ by

$$\gamma(x, y) = i^{w(x)} (-1)^y,$$

where $w(x)$ denotes the (Hamming) weight of the vector $x \in \mathbb{F}_2^m$ and $i = \sqrt{-1}$. It is readily verified that γ is indeed a homomorphism. Therefore, the 2^m characters of G that are nontrivial on N are $\chi_a \cdot \gamma$ for $a \in \mathbb{F}_2^m$.

Since

$$\sum_{z \in R} (\chi_a \cdot \gamma)(z) = \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle x, a \rangle + f(x)} i^{w(x)},$$

we find that R is a $(2^m, 2, 2^m, 2^{m-1})$ difference set in G relative to N if and only if

$$\left| \sum_{x \in \mathbb{F}_2^m} (-1)^{\langle x, a \rangle + f(x)} i^{w(x)} \right|^2 = 2^m$$

for all $a \in \mathbb{F}_2^m$. Functions f with this property have been called *negabent* in the literature [30]. One can also show that $\mathbb{Z}_4$-valued bent functions [36] are equivalent to such relative difference sets, hence also equivalent to negabent functions.

We remark that, while the notions of negabent functions and $\mathbb{Z}_4$-valued bent functions have been introduced only fairly recently, the underlying relative difference sets have been studied before, as the following construction from [3] shows.

Theorem 7.3. *Let G be a group and let D and E be two difference sets (in the usual sense) in G. Then the set*

$$\{0\} \times D \ \cup \ \{1\} \times E \ \cup \ \{2\} \times (G \setminus D) \ \cup \ \{3\} \times (G \setminus E)$$

is a relative $(2|G|, 2, 2|G|, |G|)$ difference set in $\mathbb{Z}_4 \times G$ relative to $2\mathbb{Z}_4 \times \{0\}$.

Note that every bent function on $\mathbb{F}_2^m$ gives rise to a difference set in $\mathbb{Z}_2^m$. Hence we can use Theorem 7.3 to construct from every bent function a relative difference set in $\mathbb{Z}_4 \times \mathbb{Z}_2^m$ that corresponds to a negabent function on $\mathbb{F}_2^{m+1}$. Since, for a bent function on $\mathbb{F}_2^m$, m is necessarily even, we obtain negabent functions on $\mathbb{F}_2^m$ with m odd.

8. Concluding remarks and open problems

We summarize some open problems related to the content of this paper. We note that there are many problems related to semifields and bent functions, which we do not want to recall here; we just want to restrict ourselves to problems which arise from the difference set point of view.

Problem 8.1. Improve the bound on the rank of an abelian group in Theorem 3.4 containing a relative $(p^m, p^m, p^m, 1)$ difference set if p is an odd prime.

Related to this problem one may ask whether a result similar to Theorem 3.4 holds for nonabelian groups. One may also ask whether it is possible to relax the condition that $\lambda = 1$ to a small value of λ. The case $\lambda = 2$ is discussed in [18].

In case of odd characteristic, we know one example of a planar function that is not Dembowski-Ostrom (see Table 1). In the even characteristic case, such an example is not known.

Problem 8.2. Is it possible to find planar functions in characteristic 2 that are not of Dembowski-Ostrom type?

As we have seen, difference sets are natural descriptions of projective planes. Some (but not all) interesting substructures of planes have nice interpretations when the plane is described using a difference set (unitals, subplanes, ovals, arcs, blocking sets [9], [5], [14], [15], [19], for example). Typically, the classical difference set representation of a plane (namely a Singer cycle [38]) or planar functions in odd characteristic have been used. We believe that more interpretations can be found using the planar functions in even characteristic described here.

Problem 8.3. Is it possible to describe substructures of the Desarguesian projective plane easily in terms of planar functions or in terms of the corresponding relative difference set in $\mathbb{Z}_4^m$?

References

[1] A. A. Albert, *Finite division algebras and finite planes*, Proc. Sympos. Appl. Math., Vol. 10, American Mathematical Society, Providence, R.I., 1960, pp. 53–70.

[2] A. A. Albert, *Generalized twisted fields*, Pacific J. Math. **11** (1961), 1–8.

[3] K. T. Arasu, D. Jungnickel, and A. Pott, *Divisible difference sets with multiplier* -1, Journal of Algebra **133** (1990), no. 1, 35–62.

[4] T. Beth, D. Jungnickel, and H. Lenz, *Design theory i, ii*, 2nd ed., Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 1999.

[5] M. Biliotti and G. Korchmáros, *Transitive blocking sets in cyclic projective planes*, Proceedings of the First International Conference on Blocking Sets (Giessen, 1989), no. 201, 1991, pp. 35–38.

[6] A. Blokhuis, D. Jungnickel, and B. Schmidt, *Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2*, Proc. Amer. Math. Soc. **130** (2002), no. 5, 1473–1476.

[7] R. S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), no. 1, 282–304.

[8] R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), no. 2, 167–184.

[9] M. J. de Resmini, D. Ghinelli, and D. Jungnickel, *Arcs and ovals from abelian groups*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 213–228.

[10] L. E. Dickson, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc. **7** (1906), no. 4, 514–522.

[11] C. Ding and J. Yuan, *A new family of skew Paley-Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.

[12] M. J. Ganley, *On a paper of P. Dembowski and T. G. Ostrom: "Planes of order n with collineation groups of order n^2" (Math. Z. **103** (1968), 239–258)*, Arch. Math. (Basel) **27** (1976), no. 1, 93–98.

[13] D. Ghinelli and D. Jungnickel, *Finite projective planes with a large abelian group*, Surveys in combinatorics, 2003 (Bangor) (Cambridge), London Math. Soc. Lecture Note Ser., vol. 307, Cambridge Univ. Press, 2003, pp. 175–237.

[14] _____, *On finite projective planes in Lenz-Barlotti class at least I.3*, Adv. Geom. (2003), no. suppl., S28–S48, Special issue dedicated to Adriano Barlotti.

[15] _____, *Some geometric aspects of finite abelian group*, Rend. Mat. Appl. (7) **26** (2006), no. 1, 29–68.

[16] D. Gluck, *Affine planes and permutation polynomials*, Coding theory and design theory, Part II, Springer, New York, 1990, pp. 99–100.

[17] Y. Hiramine, *On planar functions*, J. Algebra **133** (1990), no. 1, 103–110.

[18] _____, *On abelian $(2n, n, 2n, 2)$-difference sets*, J. Combin. Theory Ser. A **117** (2010), no. 7, 996–1003.

[19] C. Y. Ho, *Arc subgroups of planar Singer groups*, Mostly finite geometries (Iowa City, IA, 1996), Lecture Notes in Pure and Appl. Math., vol. 190, Dekker, New York, 1997, pp. 227–233.

[20] D. R. Hughes and F. C. Piper, *Projective planes*, Graduate Texts in Mathematics, vol. 6, Springer-Verlag, New York, 1973.

[21] D. Jungnickel, *On automorphism groups of divisible designs*, Canad. J. Math. **34** (1982), no. 2, 257–297.

[22] _____, *On a theorem of Ganley*, Graphs Combin. **3** (1987), no. 2, 141–143.

[23] W. M. Kantor, *Commutative semifields and symplectic spreads*, J. Algebra **270** (2003), no. 1, 96–114.

[24] D. E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.

[25] M. Lavrauw and O. Polverino, *Finite semifields*, Current Research Topics in Galois Geometry (L. Storme and J. De Beule, eds.), Nova Science Publishers, New York, 2012, pp. 131–159.

[26] E. Leducq, *Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd*, 2012, arXiv:1006.2610v2 [math.NT] (to appear in Des. Codes Cryptogr.).

[27] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.

[28] C. Menichetti, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra **47** (1977), no. 2, 400–410.

[29] P. Müller and M. E. Zieve, *Low-degree planar monomials in characteristic two*, 2013, arXiv:1305.6597v1 [math.NT].

[30] M. G. Parker and A. Pott, *On Boolean functions which are bent and negabent*, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 9–23.

[31] A. Pott, *Finite geometry and character theory*, Lecture Notes in Mathematics, vol. 1601, Springer-Verlag, Berlin, Heidelberg, 1995.

[32] _____ , *A survey on relative difference sets*, Groups, Difference Sets, and the Monster. Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993 (Berlin) (K. T. Arasu, J.F. Dillon, K. Harada, S. Sehgal, and R. Solomon, eds.), Walter de Gruyter, 1996, pp. 195–232.

[33] A. Pott and Y. Zhou, *A character theoretic approach to planar functions*, Cryptogr. Commun. **3** (2011), no. 4, 293–300.

[34] L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), no. 3, 315–320.

[35] Z. Scherr and M. E. Zieve, *Planar monomials in characteristic* 2, 2013, arXiv:1302.1244v1 [math.CO].

[36] K.-U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA*, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1824–1832.

[37] K.-U. Schmidt and Y. Zhou, *Planar functions over fields of characteristic two*, 2013, arXiv:1301.6999v1 [math.CO] (to appear in J. Algebraic Combin.).

[38] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385.

[39] G. Weng and X. Zeng, *Further results on planar DO functions and commutative semifields*, Des. Codes Cryptogr. **63** (2012), no. 3, 413–423.

[40] Z. Zha, G. M. Kyureghyan, and X. Wang, *Perfect nonlinear binomials and their semifields*, Finite Fields Appl. **15** (2009), no. 2, 125–133.

[41] Y. Zhou, $(2^n, 2^n, 2^n, 1)$*-relative difference sets and their representations*, J. Combin. Des. **21** (2013), no. 12.

[42] Y. Zhou and A. Pott, *A new family of semifields with 2 parameters*, Adv. Math. **234** (2013), 43–60.

[43] M. E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, 2013, arXiv:1301.5004v1 [math.CO] (to appear in Des. Codes Cryptogr.).

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

E-mail address: `alexander.pott@ovgu.de`

Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

E-mail address: `kaiuwe.schmidt@ovgu.de`

Department of Mathematics and System Sciences, College of Science, National University of Defense Technology, Changsha, China

E-mail address: `yue.zhou.ovgu@gmail.com`