COMMUTATIVE SEMIFIELDS OF ORDER 243 AND 3125

ROBERT S. COULTER AND PAMELA KOSICK

Abstract. This note summarises a recent search for commutative semifields of order 243 and 3125. For each of these two orders, we use the correspondence between commutative semifields of odd order and planar Dembowski-Ostrom polynomials to classify those commutative semifields which can be represented by a planar DO polynomial with coefficients in the base field. The classification yields a new commutative semifield of each order. Furthermore, the new commutative semifield of order 243 describes a skew Hadamard difference set which is also new.

1. Introduction

Let q be an arbitrary power of an odd prime p. We denote the field of order q by $\mathbb{F}_q$ and its nonzero elements by $\mathbb{F}_q^*$. A *finite semifield* $\mathcal{R}$ is a not necessarily associative ring with no zero divisors and a multiplicative identity. If we do not insist on the existence of a multiplicative identity, then we talk of a *presemifield*. Existence is clear, as any finite field satisfies these requirements. We refer to a semifield in which associativity fails as a *proper* semifield. It is straightforward to show the additive group of a presemifield is elementary abelian, see Knuth [11]. Further, if the presemifield has order q, then it can be represented by field addition and a bivariate polynomial over $\mathbb{F}_q$ representing the multiplication with some obvious restrictions. Consequently, throughout this paper we denote a semifield of order q by $\mathcal{R} = (\mathbb{F}_q, +, \star)$.

There are two important subfields of a commutative semifield $\mathcal{R}$: the middle nucleus $\mathcal{N}_m$ and the nucleus $\mathcal{N}$, defined as follows:

$$\mathcal{N}_m = \{x \in \mathcal{R} \mid a \star (x \star b) = (a \star x) \star b \text{ for all } a, b \in \mathcal{R}\},$$
$$\mathcal{N} = \{x \in \mathcal{R} \mid x \star (a \star b) = (x \star a) \star b \text{ for all } a, b \in \mathcal{R}\}.$$

It is easy to show these sets are finite fields and that $\mathcal{N}$ is a subfield of $\mathcal{N}_m$. Additionally, every commutative semifield can be described as a vector space over either field. Essentially, the two nuclei describe how much associativity fails in the semifield $\mathcal{R}$.

There is a one-to-one correspondence between presemifields and translation planes of Lenz-Barlotti type V, see Dembowski [7] for details. Within this correspondence, a result of Albert [2] shows isomorphic planes are equivalent to isotopic presemifields. Here, by isotopy we mean to say two presemifields $\mathcal{R}_1 = (\mathbb{F}_q, +, \star)$ and $\mathcal{R}_2 = (\mathbb{F}_q, +, \times)$ are *isotopic* if there exists three non-singular linear transformations $(N, L; M)$ such that

$$M(a \times b) = N(a) \star L(b)$$

for all $a, b \in \mathbb{F}_q$. If $N = L$, we call this a *strong* isotopism. Any presemifield can be converted to a semifield via a strong isotopy. Thus, when talking of isotopy classes

of presemifields, we can restrict ourselves to discussing semifields only. Further, when talking of isotopic commutative semifields, results of Coulter and Henderson [5] guarantee the existence of very specific isotopes between them. In particular, isotopic commutative semifields of odd order with $[\mathcal{N}_m : \mathcal{N}]$ odd must be strongly isotopic by [5, Theorem 2.6].

In this note we present a partial classification of commutative semifields of order 243 and 3125. Our approach, which we describe below, exploits the connection between commutative presemifields of odd order and planar Dembowski-Ostrom polynomials. We detail the method implemented to perform this search, including the description of an efficient test to determine if two semifields are isotopic. The results of our searches are presented in Theorems 1 and 2; they include a new commutative semifield of each order. Finally, a result of Giu *et al*, [10], shows that any commutative semifield of order $q \equiv 3 \pmod 4$ yields a special type of difference set called a skew Hadamard difference set. Here we show the new commutative semifield of order 243 defines a skew Hadamard difference set inequivalent to those previously known.

2. Dembowski-Ostrom polynomials and commutative semifields

We denote the ring of polynomials in indeterminate X over $\mathbb{F}_q$ by $\mathbb{F}_q[X]$. Any function on $\mathbb{F}_q$ can be uniquely represented by a polynomial of degree at most $q-1$ and this polynomial of smallest degree is referred to as *reduced*. Two polynomials $f, h \in \mathbb{F}_q[X]$ representing the same function must satisfy $f(X) \equiv h(X) \pmod{X^q - X}$.

A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation* polynomial over $\mathbb{F}_q$ if it induces a bijection of $\mathbb{F}_q$ under evaluation. A *planar* polynomial over $\mathbb{F}_q$ is any polynomial $f \in \mathbb{F}_q[X]$ for which every difference polynomial $f(X+a) - f(X) - f(a)$ with $a \in \mathbb{F}_q^*$ is a permutation polynomial over $\mathbb{F}_q$. It is straightforward to verify that any quadratic polynomial is planar over any field of odd characteristic.

A *linearised* polynomial $L \in \mathbb{F}_q[X]$ is any polynomial of the shape

$$L(X) = \sum_i a_i X^{p^i}.$$

The reduction of a linearised polynomial modulo $X^q - X$ is linearised and any linearised polynomial is additive: $L(a+b) = L(a) + L(b)$ for all $a, b \in \mathbb{F}_q$. The set of all reduced linearised permutation polynomials represents the set of all non-singular linear transformations over $\mathbb{F}_q$. In particular, this set forms a group under composition modulo $X^q - X$ isomorphic to the general linear group $GL(e,p)$ (where $q = p^e$), see Lidl and Niederreiter [12].

A *Dembowski-Ostrom (DO)* polynomial $D \in \mathbb{F}_q[X]$ is any polynomial of the shape

$$D(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}.$$

In odd characteristic, DO polynomials are closed under composition with linearised polynomials, and the reduction of a DO polynomial modulo $X^q - X$ is a DO polynomial. There is a one-to-one correspondence between commutative presemifields of odd order and planar DO polynomials. If $f \in \mathbb{F}_q[X]$ is a planar DO polynomial, then $\mathcal{R} = (\mathbb{F}_q, +, \star)$ is a commutative presemifield with multiplication defined by

$$a \star b = f(a+b) - f(a) - f(b).$$

Conversely, given a commutative presemifield $\mathcal{R} = (\mathbb{F}_q, +, \star)$, the polynomial given by $f(X) = \frac{1}{2}(X \star X)$ is a planar DO polynomial.

For the remainder of this paper we restrict ourselves to discussing commutative semifields with the following parameters:

- The order of the nucleus is $|\mathcal{N}| = s = p^k$ with p an odd prime and $k \in \mathbb{N}$.
- The order of the middle nucleus is $|\mathcal{N}_m| = r = s^n$ with n odd.
- The order of the commutative semifield is $|\mathcal{R}| = q = r^d$.

By [5, Theorem 2.6], isotopic commutative semifields with these parameters are necessarily strongly isotopic.

Let $\mathcal{R}$ be a commutative semifield with the above parameters. A combination of recent work in [5, 6] shows that within the isotopy class of $\mathcal{R}$ there must exist a commutative semifield $\mathcal{R}_f$ where the corresponding (reduced) planar DO polynomial $f \in \mathbb{F}_q[X]$ has the shape

$$f(X) = L(t^2(X)) + D(t(X)) + \frac{1}{2}X^2, \tag{1}$$

where $L, D \in \mathbb{F}_q[X]$ are a linearised and DO polynomial, respectively, and $t(X) = X^r - X$. Moreover, D contains no term of the form X^{2p^i}.

Now let $h \in \mathbb{F}_q[X]$ be a planar DO polynomial with $\mathcal{R}_h$ a commutative semifield isotopic to $\mathcal{R}_f$. A strong isotopism between $\mathcal{R}_f$ and $\mathcal{R}_h$ corresponds to the existence of two linearised permutation polynomials $M, N \in \mathbb{F}_q[X]$ (the same two non-singular linear transformations from the strong isotopy) satisfying

$$M(f(X)) \equiv h(N(X)) \pmod{X^q - X}.$$

We shall call two planar DO polynomials *equivalent* if their corresponding commutative semifields are isotopic. By [6, Theorem 5.1], if f and h both have the shape (1), then

$$N(X) = \left(\sum_{i=0}^{d-1} \alpha_i X^{r^i} \right)^{p^j}$$

for some integer $0 \leq j < d$ and $M(X) \equiv N(1) \star N(X) \pmod{X^q - X}$ where $\star$ is the multiplication of $\mathcal{R}_h$. (We conjecture one can limit the shape of N further by insisting $p^j = s^l$ for some integer l.) Thus, if one has two planar DO polynomials over $\mathbb{F}_q$ of the shape (1), to prove the corresponding semifields are not isotopic, it is sufficient to exhaust the possibilities for N.

The above theory offers a two-step approach to finding commutative semifields with the parameters outlined above. Firstly, find all planar DO polynomials over $\mathbb{F}_q$ of the shape (1). Secondly, use the type of isotopes (M, N) above to determine the distinct classes.

The smallest interesting case with parameters as described is where $q = p^5$. Even when $p = 3$, an exhaustive search over the polynomials with shape (1) seems infeasible. The upside is that one can easily restrict coefficients to some subset of $\mathbb{F}_q$ to do "selective" searches for commutative semifields. Secondly, with $q = p^5$, the above restriction on the shape of N is no restriction at all, so that one is really looking at all reduced linearised permutation polynomials over $\mathbb{F}_q$. Since the number of linearised permutation polynomials over $\mathbb{F}_{p^5}$ is $O(p^{25})$ (order of general linear group), a direct approach to the exhaustive search for isotopes also appears infeasible. It is possible, however, to rectify this with a little theory.

Suppose we have two planar DO polynomials f, h of the shape (1) and we wish to determine whether or not they are equivalent. We know from above that if they are, then there exist linearised permutation polynomials M, N with N as described, and M completely determined by N and one of f or h. As isotopes, we know

$$M(x \times y) = N(x) \star N(y)$$

for all $x, y \in \mathbb{F}_q$, with $\times$ and $\star$ the multiplications of $\mathcal{R}_f$ and $\mathcal{R}_h$, respectively.

Being a linear transformation, every linearised polynomial is determined by the image of a basis over $\mathbb{F}_p$. When $k = n = 1$ and d is odd, we select a very special type of basis: $\{1, \alpha_1, \alpha_1^{-1}, \ldots, \alpha_m, \alpha_m^{-1}\}$ where $m = (d-1)/2$. Here $\alpha_i \times \alpha_i^{-1} = 1$; i.e. we are taking inverses in the commutative semifield $\mathcal{R}_f$. The existence of such a basis for any commutative semifield of the form under consideration is an open problem, but for those of order 3^5 and 5^5 there is always one. The exhaustive search now proceeds as follows:

(1) Guess $N(1)$. This, in turn, determines $M(1) = N(1) \star N(1) = z$.
(2) Now guess $N(\alpha_1)$, which must be linearly independent of $N(1)$. By our relation, we know
$$M(\alpha_i \times \alpha_i^{-1}) = M(1) = z = N(\alpha_i) \star N(\alpha_i^{-1}),$$
so that guessing $N(\alpha_i)$ determines $N(\alpha_i^{-1})$. If $\{N(1), N(\alpha_1), N(\alpha_1^{-1})\}$ are linearly dependent, then repeat Step 2.
(3) Repeat Step 2 for α_i. If, at any stage, a linearly independent set of values for N over the basis is generated, determine M and test if $M(f(X)) \equiv h(N(X)) \pmod{X^q - X}$. Otherwise continue until all possibilities have been exhausted.

Basically, by using this special type of basis we obtain roughly a square root reduction in the size of the search space. Since multiplying a solution by any constant from $\mathbb{F}_p^*$ also yields a solution, one can limit the search space by an additional factor of $p-1$ at the time of guessing $N(1)$. Consequently, the worst case for this algorithm over $\mathbb{F}_{p^5}$ is

$$\frac{(p^5-1)(p^5-p^2)(p^5-p^4)}{p-1} < p^{14}$$

guesses, though in practice it is far less than this as many guesses for α_1 result in a linearly dependent value for α_1^{-1}.

The fact that the size of the isotopy problem can be significantly reduced means a search for planar DO polynomials with restricted coefficients is a worthwhile endeavour. Consequently, we decided to implement the algorithm to classify all commutative semifields of order p^5 with $p \in \{3, 5\}$ described by planar DO polynomials with coefficients in $\mathbb{F}_p$. A slightly more detailed outline of our approach to finding commutative semifields of order p^5 is as follows:

(1) Find all planar polynomials of the shape (1) with coefficients in $\mathbb{F}_p$. The planarity of these polynomials can be tested in groups using their relation with $\mathbb{F}_r$-complete mappings, see [6, Theorem 3.2].
(2) Remove those planar polynomials describing commutative semifields isotopic to the finite field. To do so, for each planar DO polynomial f, select any element $g \notin \mathbb{F}_p$. If $g \in \mathcal{N}_m(\mathcal{R}_f)$, then the commutative semifield is isotopic to the finite field.

(3) Of those planar DO polynomials remaining, group them into isotopy classes by calculating $M(f(N)) \pmod{X^q - X}$ for all linearised permutation polynomials M, N with coefficients in $\mathbb{F}_p$. This is a short test, but will determine which of the planar DO polynomials are equivalent via an "isotopy" involving only linearised polynomials from the coefficient field.
(4) Finally, taking one example from each of the isotopy classes just determined, exhaustively check for isotopes over the general field. This last step is by far the most computationally demanding.

We implemented the above approach using the Magma algebra package, [4]. The algorithm mainly relies on the efficiency of implementations of testing for linear independence and polynomial evaluation; we made no attempt to improve the efficiency of these components of Magma for our specific situation.

It should be mentioned that it is particularly easy to construct, from any planar DO polynomial, a planar DO polynomial of the shape (1) which describes an isotopic commutative semifield and without changing the coefficient field of the polynomial. This is important as practically all of the known planar DO polynomials are not of this shape, and the final step of this approach is specifically designed to take advantage of it.

3. Commutative semifields of order 243 and 3125

For commutative semifields of order 243, 448 planar DO polynomials were found with coefficients restricted to $\mathbb{F}_3$. Of these, 64 were found to be equivalent to the finite field. The remaining 384 split into 6 distinct isotopy classes, each of size 64. Since the isotopy test is exhaustive, we thus have

Theorem 1. *There are exactly seven non-isotopic commutative semifields of order 243 which can be described by a planar DO polynomial with coefficients in $\mathbb{F}_3$:*

(i) *The finite field (known).*
representative: X^2.
(ii) *Albert's twisted field #1 (known).*
representative: X^4.
(iii) *Albert's twisted field #2 (known).*
representative: X^{10}.
(iv) *TST$^+$ (Ten-Six-Two +) (known).*
representative: $X^{10} + X^6 - X^2$.
(v) *TST$^-$ (Ten-Six-Two -) (known).*
representative: $X^{10} - X^6 - X^2$.
(vi) *The example of Weng (known, unpublished).*
representative: $X^{90} + X^2$.
(vii) *(unknown).*
representative: $L(X) = -X^3, D(X) = -X^{36} + X^{30} + X^{28} + X^4$.
representative: $L(X) = -X, D(X) = -X^{36} + X^{28} + X^{12} + X^4$.

Albert's twisted fields were introduced in [1]. Examples (iv) and (v) are dealt with in full generality in [5]. The example of Guobiao Weng was previously known to us via personal correspondence.

For commutative semifields of order 3125, 2000 planar DO polynomials were found with coefficients restricted to $\mathbb{F}_5$. Of these, 500 were found to be equivalent

to the finite field. The remaining 1500 split into 3 distinct isotopy classes, each of size 500. Again, since the isotopy test is exhaustive, we thus have

Theorem 2. *There are exactly four non-isotopic commutative semifields of order* 3125 *which can be described by a planar DO polynomial with coefficients in* $\mathbb{F}_5$*:*

(i) *The finite field (known).*
representative: X^2.
(ii) *Albert's twisted field #1 (known).*
representative: X^6.
(iii) *Albert's twisted field #2 (known).*
representative: X^{26}.
(iv) *(unknown).*
representative: $L(X) = X^{125} + X^{25} + 2X^5 + 3X$, $D(X) = 0$.
representative: $L(X) = 2X^{25} + X^5, D(X) = 2X^{130} + 2X^{26}$.

The representatives given for the unknown class for each order are simply a couple selected from the search list with a small number of terms for L and D; there was no other reason for selecting these as a representative over any other examples for the new classes.

4. Skew Hadamard difference sets in groups of order 243

Let G be a finite group of order v, written additively, and D a k-element subset of G. If the multiset $\{* \ d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2 \ *\}$ contains each non-identity element of G exactly λ times, then D is called a (v, k, λ)-*difference set*. Two difference sets D_1 and D_2 are *equivalent* if there is an automorphism of the group, ϕ, and an element $a \in G$, such that $\phi(D_1) + a = D_2$. When a difference set D possesses the additional property that G is the disjoint union of D, $-D$ and $\{0\}$ it is called a *skew Hadamard difference set (SHDS)*. The classical example of a SHDS is the Paley difference set; take $q \equiv 3 \pmod 4$ and let $\mathbb{F}_q$ be the finite field of q elements. Then $\mathcal{P} = \{x^2 : x \in \mathbb{F}_q, x \neq 0\}$ is a $(q-1, \frac{q-1}{2}, \frac{q-3}{4})$-difference set in $(\mathbb{F}_q, +)$.

If f is a planar DO polynomial over $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$, then $D_f = f(\mathbb{F}_q^*)$ is a skew Hadamard difference set in $(\mathbb{F}_q, +)$, see [10, Theorem 2.2]. Moreover, isotopic commutative semifields describe equivalent difference sets. The converse, however, is not necessarily true. Each of the semifields in Theorem 1 give rise to a skew Hadamard difference set. It is known that classes (i), (ii) and (iii) of Theorem 1 are equivalent to the Paley difference set. Ding and Yuan [9] show classes (iv) and (v) yield two additional distinct skew Hadamard difference sets. Classes (vi) and (vii) of Theorem 1 have not previously been dealt with. We shall show the difference set generated from class (vii) is new, while that generated by (vi) is equivalent to Paley. That (vi) is equivalent to Paley is easily seen: construct $\mathbb{F}_{243}$ using a root g of the irreducible polynomial $X^5 - X + 1$. It is easily verified $g^{-1}X^2$ and $X^{90} + X^2$ have the same image set. Hence class (vi) yields a difference set equivalent to Paley.

It remains to consider class (vii). To complete the description of known skew Hadamard difference sets of order 243, we need to introduce two further examples. Ding *et al* [8] showed the difference sets arising from the Rees-Tits slice symplectic spread are also skew Hadamard difference sets inequivalent to Paley; we refer to

these as $RT(+)$ and $RT(-)$. The description of these sets is as follows:

$$RT(+) = \{x^{114} + x^{54} - x^2 \mid x \in \mathbb{F}_{3^5}^*\},$$
$$RT(-) = \{x^{114} - x^{54} - x^2 \mid x \in \mathbb{F}_{3^5}^*\}.$$

Hence, the known distinct skew Hadamard difference sets in an elementary abelian group of order 243 are class (i) (Paley skew Hadamard difference set), class (iv), class(v), $RT(+)$, and $RT(-)$. To show class (vii) is inequivalent to all of the examples listed, we need another invariant. For nonzero $a, b \in \mathbb{F}_q^*$ with $a \neq b$, define $T_{a,b} = |D \cap (D + a) \cap (D + b)|$ to be the *triple intersection numbers*. The multiset of triple intersection numbers is an invariant of a skew Hadamard difference set, see Baumert [3]. Below we calculate the triple intersection numbers for the known skew Hadamard difference sets of order 243. In the second column the triple intersection numbers are listed as y^m where y is the size of the intersection and m is the multiplicity.

Class	Triple intersection numbers
(i)	$26^{1815}, 27^{3630}, 28^{1815}, 29^{7260}, 30^{5566}, 31^{1815}, 32^{5445}, 33^{1815}$
(iv)	$24^{75}, 25^{435}, 26^{1155}, 27^{2385}, 28^{4155}, 29^{5460}, 30^{6001},$ $31^{4650}, 32^{2700}, 33^{1470}, 34^{555}, 35^{120}$
(v)	$23^{15}, 24^{30}, 25^{285}, 26^{1245}, 27^{2760}, 28^{3945}, 29^{5520},$ $30^{5911}, 31^{4365}, 32^{2880}, 33^{1530}, 34^{615}, 35^{45}, 36^{15}$
(vii)	$24^{45}, 25^{315}, 26^{975}, 27^{2790}, 28^{4800}, 29^{5115}, 30^{5056},$ $31^{5085}, 32^{2955}, 33^{1335}, 34^{540}, 35^{120}, 36^{30}$
RT(+)	$24^{75}, 25^{330}, 26^{1155}, 27^{2535}, 28^{4530}, 29^{5235}, 30^{5461},$ $31^{4665}, 32^{3165}, 33^{1410}, 34^{495}, 35^{105}$
RT(-)	$24^{90}, 25^{330}, 26^{1095}, 27^{2655}, 28^{4335}, 29^{5310}, 30^{5611},$ $31^{4590}, 32^{3135}, 33^{1395}, 34^{495}, 35^{1320}$

From this table it is clear class (vii) yields a difference set inequivalent to those previously known.

References

[1] A.A. Albert, *On nonassociative division algebras*, Trans. Amer. Math. Soc. **72** (1952), 296–309.

[2] ———, *Finite division algebras and finite planes*, Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics (Providence), Symposia in Applied Mathematics, vol. 10, American Mathematical Society, 1960, pp. 53–70.

[3] L.D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, vol. 182, Springer-Verlag, 1971.

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

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

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

[7] P. Dembowski, *Finite Geometries*, Springer-Verlag, New York, Heidelberg, Berlin, 1968, reprinted 1997.
[8] C. Ding, Z. Wang, and Q. Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in* $PG(3, 3^{2h+1})$, J. Combin. Theory Ser. A **114** (2007), 867–887.
[9] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.
[10] W. Giu, Z. Wang, G. Weng, and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr. **44** (2007), 49–62.
[11] D.E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.
[12] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

520 Ewing Hall, Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, USA
E-mail address: coulter@math.udel.edu

Natural Sciences and Mathematics, The Richard Stockton College of New Jersey, PO Box 195, Pomona, NJ, 08240, USA
E-mail address: pamela.kosick@stockton.edu

Finite Fields: Theory and Applications -- Proceedings of the 9th International Conference on Finite Fields and Applications (G. McGuire, G.L. Mullen, D. Panario and I.E. Shparlinski, eds.) Contemporary Mathematics, vol.518, 2010, pp.129-136