Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia pp. 41–45

A family of semifields of order 729

Daniele Bartoli, Giorgio Faina, Stefano Marcugini, Fernanda Pambianco
{daniele.bartoli,faina,gino,fernanda}@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy
Jürgen Bierbrauer
Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

Abstract. Semifields (or: non-associative division algebras) are the algebraic structures which coordinatize an important class of geometric objects, projective planes which are translation planes and also the duals of translation planes. The construction from [2] uses projective polynomials (see [3]). It produces semifields for each square order in odd characteristic and contains the Budaghyan-Helleseth family of commutative semifields (see [4]). We study the special case of order 729. Up to isotopy exactly two semifields arise. One belongs to the Budaghyan-Helleseth family and has 1248 autotopisms, the other is not isotopic to commutative nor to a generalized twisted field. Its autotopism group has order 624. Similar features are valid in order 3^8.

1 A family of semifields in odd characteristic

A family of presemifields of odd order is constructed in [2] as follows. Let p be an odd prime, $q = p^m, L = \mathbb{F}_q \subset F = \mathbb{F}_{q^2}$. Let $\overline{x} = x^q$ and $T : F \longrightarrow L$ the trace. Let $0 < s < 2m, \sigma = p^s, l \in L^*$ such that $-l \notin (L^*)^{\sigma-1}$. Further let $C_1, C_2 \in F$ such that the following polynomial condition is satisfied:

$$P_{C_1,C_2,s}(X) = C_2X^{\sigma+1} + \overline{C_1}X^{\sigma} + C_1X + \overline{C_2} \in F[X]$$
$$\text{has no root } z \text{ such that } z^{q+1} = 1.$$

Then presemifields $B(p, m, s, l, C_1, C_2)$ of order p^{2m} are defined such that the addition coincides with the addition in the field F and the multiplication is given by

$$x * y = (1/2)T((C_1y^{\sigma} + C_2\overline{y}^{\sigma})x) + (l/2)T((\overline{C_1}y + C_2\overline{y})x^{\sigma}) + (xy - \overline{xy})/2 \quad (1)$$

The semifield associated to $B(p, m, s, l, C_1, C_2)$ is defined as $(F, +, \circ)$ where

$$x \circ y := \beta\big(\gamma(x) * y\big). \quad (2)$$

and $\beta, \gamma \colon F \to F$ are invertible linear mappings defined by

$$1 * \beta(x) = x \quad \text{and} \quad \gamma(x) * 1 = 1 * x \tag{3}$$

2 The commutative case

Two families of commutative semifields were constructed by L. Budaghyan and T. Helleseth in [4]. It is easy to see that this family is contained in our family, more precisely in the special cases when $\{C_1, C_2\} \subset L$ and $C_1 = 0$, respectively. It remains an open question if our family contains examples which are commutative and not isotopic to members of the Budaghyan-Helleseth family. $B(3,3,1,1,0,C_2)$ is isotopic to commutative if and only if $(C_2/\overline{C_2})^7 = 1$.

3 A standard situation in odd characteristic

In odd characteristic, let

$$L = \mathbb{F}_{p^m} \subset F = \mathbb{F}_{p^{2m}}$$

and $T : F \longrightarrow L$ the trace $T(x) = x + x^q$ where $q = p^m$. Use a basis $1, \omega$ for $F|L$ where $T(\omega) = 0$. In particular we have a direct sum decomposition $F = L \oplus L\omega$ where $L\omega = \{x \mid x \in F, T(x) = 0\}$. Then $\mu = \omega^2$ is a non-square in L. Observe that this comes down to describe the quadratic extension F of L by the irreducible polynomial $X^2 - \mu$ where μ is a non-square in L. Let $x = a + b\omega$. We also write

$$x = (\underbrace{a}_{Re}, \underbrace{b}_{Im})$$

and refer to $a = Re(x)$ and $b = Im(x)$ as the real and imaginary part of x, respectively. The field multiplication in F is then

$$(a,b)(c,d) = (ac + \mu bd, ad + bc).$$

4 Isotopism relations

Presemifields $(F, +, *)$ and $(F, +, \circ)$ are **isotopic** if there exist invertible $\mathbb{F}_p$-linear mappings $\alpha_1, \alpha_2, \beta$ such that

$$x \circ y = \beta(\alpha_1(x) * \alpha_2(y)) \text{ for all } x, y \in F.$$

This definition is motivated by the fact that presemifields are isotopic if and only if the projective planes they coordinatize are isomorphic. We specialize to the case $B(3,3,s,l,C_1,C_2)$ of order 3^6. Let $L = \mathbb{F}_{27} \subset F = \mathbb{F}_{729}$. Choose $\mu = -1$

and $\omega = i \in F$ where $i^2 = -1$ (see Section 3). Some isotopism relations between the $B(3,3,s,l,C_1,C_2)$ are easy to see. In fact, $B(3,3,s,l,C_1,C_2)$ is isotopic to $B(3,3,3+s,l,C_2,C_1)$ and to $B(3,3,3-s,1/l,C_2,\overline{C_1})$. This shows that we may assume $s=1$. The parameter $l \in L$ is determined only up to its coset $lL^{*(\sigma-1)}$. This shows that up to isotopy we may choose $l=1$. It follows from the theory of projective polynomials that the number of pairs $(C_1,C_2) \in F \times F$ satisfying the polynomial condition from Section 1 equals $27 \times 26 \times 13 \times 21$. Some more relations of isotopy between the corresponding presemifields $B(3,3,1,1,C_1,C_2)$ are obvious:

- **Scalar isotopy:** The pair (C_1,C_2) may be replaced by $(\lambda C_1, \lambda C_2)$ for $0 \neq \lambda \in L$.
- **Galois isotopy:** $B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,C_1^3,C_2^3)$.

Here are some more important types of isotopy:

Theorem 4. *$B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,\alpha^{82}C_1,\alpha^4C_2)$ for all $0 \neq \alpha \in F$.*

Theorem 5. *Let $A,B \in F^*$ such that $A\overline{A} \neq B\overline{B}$. Then $B(3,3,1,1,0,C_2)$ is isotopic to $B(3,3,1,1,C_1',C_2')$ where*

$$C_1' = C_2AB^3 + \overline{C_2A^3B}, C_2' = C_2A^4 + \overline{C_2B^4}.$$

Theorem 6 (diagonal isotopy). *Let $C_i = (v_i,h_i)$ in the terminology of Section 3 and work with parameters*

$$v_+ = v_1 + v_2, v_- = v_1 - v_2, h_+ = h_1 + h_2, h_- = h_1 - h_2.$$

Then the following substitutions can be performed without affecting isotopy:

$$v_+ \mapsto k_1^4 v_+, v_- \mapsto k_2^4 v_-,$$

$$h_+ \mapsto k_1^3 k_2 h_+, h_- \mapsto k_1 k_2^3 h_-$$

for arbitrary nonzero $k_1,k_2 \in L$.
Explicitly this means that $B(3,3,1,1,C_1,C_2)$ is isotopic to $B(3,3,1,1,C_1',C_2')$, where

$$C_1' = -((k_1^4+k_2^4)v_1 + (k_1^4-k_2^4)v_2, (k_1^3k_2+k_1k_2^3)h_1 + (k_1^3k_2 - k_1k_2^3)h_2),$$

$$C_2' = -((k_1^4-k_2^4)v_1 + (k_1^4+k_2^4)v_2, (k_1^3k_2-k_1k_2^3)h_1 + (k_1^3k_2 + k_1k_2^3)h_2).$$

5 The census

Consider at first the subcase $C_1 = 0$. By Theorem 4 the parameter C_2 may be multiplied by an arbitrary fourth power, so we may choose C_2 in $\{1, i, 1+i, 1-i\}$. The existence condition of Section 1 says that $-\overline{C_2}/C_2$ is not in the group of order 7. This excludes $C_2 = i$. As $1+i, 1-i$ are conjugates, those lead to isotopic semifields by Galois isotopy. This shows that we obtain precisely two isotopy classes of semifields in case $C_1 = 0$, with representatives $B(3,3,s,l,0,1)$ (denoted by $\mathcal{C}$) and $B(3,3,1,1,0,1-i)$ (which we denote by $\mathcal{B}$). In fact, $\mathcal{C}$ is commutative while Section 2 shows that $\mathcal{B}$ is not isotopic to commutative. Here the field $L = \mathbb{F}_{27}$ has been constructed as $L = \mathbb{F}_3(\epsilon)$, where $\epsilon^3 = \epsilon^2 - 1$. The associated semifields have right and left nucleus $\mathbb{F}_3$ and middle nucleus of order 9.

Consider the generic case $C_1 \neq 0$. Theorem 4 shows that C_1 may be chosen as 1 or $1-i$. Using also diagonal isotopy it is easy to see that we can choose $C_1 = 1$. Using Galois isotopy, diagonal isotopy and Theorem 4 it is easy to show that the $B(3,3,1,1,1,C_2)$ come in two isotopy classes. Theorem 5 can be used to show that those are isotopic to $\mathcal{C}$ and $\mathcal{B}$, respectively.

5.1 Description of $\mathcal{C}$

This (pre)semifield is commutative and belongs to the Budaghyan-Helleseth family. Its autotopism group has order 1248. It is in fact easy to see that the autotopism group has order at least 1248 : start from Equation (1) which takes on the form

$$x * y = -T(x\overline{y}^3 + x^3\overline{y}) + \overline{xy} - xy.$$

When will $\alpha_1(x) = Ax, \alpha_2(y) = By$ define an autotopism? The imaginary part shows $AB \in L$, equivalently $B = c\overline{A}$ for $c \in L$. The real part yields the condition $c^3A^4 = cA^4 \in L$. This shows $c = \pm 1$ and there are 4×26 choices for A. Together with the field automorphisms (generated by $\alpha_1(x) = x^3, \alpha_2(y) = y^3, \beta(z) = z^{3^5}$) this yields an autotopism group of order $26 \times 4 \times 2 \times 6 = 1248$.

5.2 Description of $\mathcal{B}$

This (pre)semifield is not isotopic to commutative. Its autotopism group has order 624.

The semifields $\mathcal{C}, \mathcal{B}$ are not isotopic to generalized twisted fields, see Albert [1]. In fact, consider a generalized twisted field of order 3^6 with left and right nucleus of order 3. Such a twisted field is isotopic to a presemifield

$$x * y = xy + lx^\sigma y^\tau$$

where $l \in F$ has to satisfy the obvious conditions. Let $\sigma = 3^s, \tau = 3^t$. The nuclei show that s, t are coprime to 6. Consider autotopisms of the form $\alpha_1(x) =$

$Ax, \alpha_2(y) = By, \beta(z) = z/(AB)$. Such a pair of nonzero constants $A, B \in F$ defines an autotopism if and only if $A^{\sigma-1}B^{\tau-1} = 1$. We can choose B arbitrarily and have then two choices for A. This shows that the twisted field has at least $2 \times (3^6 - 1) = 1456$ autotopisms and is therefore more symmetric than our semifields.

6 A generalization

The isotopisms described in Section 4 are in fact special cases of isotopism relations which are valid for the family $B(p, m, s, l, C_1, C_2)$ (see Section 1) in general. Consider $B(3, 4, s, l, C_1, C_2)$ (of order 3^8). Case $s = 2$ is not interesting as it yields isotopes of Dickson semifields. When $s = 1$ it can be assumed that $l = -\mu$ where $\mu = \epsilon^5 \in L$ is an element of order 16 and ϵ is a primitive element of $L = \mathbb{F}_{81}$. We carried out a search analogous to the procedure described in Section 5 for presemifields $B(3, 4, 1, -\mu, C_1, C_2)$. The result is that again there are precisely two isotopism types, with representatives $B(3, 4, 1, -\mu, 0, 1)$ and $B(3, 4, 1, -\mu, 1+\epsilon/\mu^2, 1-\epsilon/\mu^2)$. Here the former is commutative and the unique isotopy class of Budaghyan-Helleseth semifields of order 3^8, the second is not isotopic to commutative.

References

[1] A. A. Albert: *Generalized twisted fields, Pacific Journal of Mathematics* **11** (1961), 1-8.

[2] J. Bierbrauer: *Projective polynomials, a projection construction and a family of semifields,* manuscript.

[3] A.W. Bluher: *On $x^{q+1} + ax + b$, Finite Fields and Their Applications* **10** (2004), 285-305.

[4] L. Budaghyan and T. Helleseth: *New commutative semifields defined by new PN multinomials, Cryptogr. Commun.* **3** (2011), 1-16.