Finite Fields and Their Applications 53 (2018) 175–188

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the isotopism classes of the Budaghyan–Helleseth commutative semifields

Tao Feng, Weicong Li [*]

School of Mathematical Sciences, Zhejiang University, 38 Zheda Road, Hangzhou 310027, Zhejiang, PR China

ARTICLE INFO

Article history:
Received 7 December 2017
Received in revised form 4 May 2018
Accepted 1 June 2018
Available online xxxx
Communicated by Olga Polverino

MSC:
05B25
12K10
13M05

Keywords:
Commutative semifield
Budaghyan–Helleseth family
Isotopism
Strong isotopism

ABSTRACT

In this paper, we completely determine the isotopism classes of the Budaghyan–Helleseth commutative semifields constructed in Budaghyan and Helleseth (2011) [4].

1. Introduction

A finite *presemifield* $\mathbb{S}$ is a finite ring with no zero-divisors such that both the left and right distributive laws hold. If it further contains a multiplicative identity, then

[*] Corresponding author.
E-mail addresses: tfeng@zju.edu.cn (T. Feng), conglw@zju.edu.cn (W. Li).

https://doi.org/10.1016/j.ffa.2018.06.001

we call $\mathbb{S}$ a *semifield*. A semifield is not necessarily commutative or associative, but by Wedderburn's Theorem [11], associativity necessarily implies commutativity in the finite case. The study of semifields was initiated by Dickson [7] in the study of division algebras. Knuth [8] showed that the additive group of a semifield $\mathbb{S}$ is an elementary abelian group. Hence, any finite presemifield can be represented by $(\mathbb{F}_{p^n}, +, *)$, where $(\mathbb{F}_{p^n}, +)$ is the additive group of the finite field $\mathbb{F}_{p^n}$ with p^n elements and $x * y = \varphi(x, y)$ with φ a bilinear function from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. For a recent survey on finite semifields, please refer to [9]. In this paper, we are concerned with commutative presemifields with odd characteristic. Such presemifields can be equivalently described by planar polynomials of Dembowski–Ostrom type, cf. [5,6].

Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, *)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, *')$ be two presemifields. They are *isotopic* if there exist three linear permutations L, M, N over $\mathbb{F}_{p^n}$ such that $L(x*y) = M(x)*'N(y)$ for all $x, y \in \mathbb{F}_{p^n}$, and we say that (M, N, L) is an *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$. If there is an isotopism (N, N, L) between the presemifields $\mathbb{S}_1$ and $\mathbb{S}_2$, then it is a *strong isotopism* and $\mathbb{S}_1$ and $\mathbb{S}_2$ are *strongly isotopic*. In the particular case $\mathbb{S}_1 = \mathbb{S}_2$, a (strong) isotopism is called a (strong) *autotopism*. Both isotopism and strong isotopism define an equivalence relation on the finite presemifields, and the equivalence classes are called isotopism classes and strong isotopism classes respectively. Two isotopic presemifields are called *isotopes* of each other. For a presemifield $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ and its nonzero element e, we define a new multiplication $\star$ by $(x * e) \star (e * y) = x * y$. Then $\mathbb{S}' = (\mathbb{F}_{p^n}, +, \star)$ is a semifield with an identity $e * e$, which is strongly isotopic to $\mathbb{S}$.

In [3,4], Budaghyan and Helleseth constructed two families of commutative presemifields of order p^{2k} from certain planar functions of Dembowski–Ostrom type over $\mathbb{F}_{p^{2k}}$, where p is an odd prime. They established that the first family is non-isotopic to previously known semifields for $p \neq 3$ and k odd, and determined the middle nuclei in some special cases. Later on, Bierbrauer [1] observed that the two families are in fact the same and have been also independently discovered in [14]. This family of semifields is now commonly called the Budaghyan–Helleseth family in the literature. In the same paper, Bierbrauer gave a generalization of the Budaghyan–Helleseth family which also contains the LMPT-construction [10]. The new semifields sometimes are called the LMPTB family, and it is not isotopic to any previously known commutative semifields with the possible exception of the Budaghyan–Helleseth family as shown in [1]. However, Marino and Polverino proved that the LMPTB family is contained in the Budaghyan–Helleseth family in [13], and they determined the nuclei and middle nuclei of the Budaghyan–Helleseth semifields in [13].

In this paper, we completely determine the isotopism classes of the Budaghyan–Helleseth presemifields. In Section 2, we introduce some background and preliminary results. We determine the strong isotopism classes of the Budaghyan–Helleseth presemifields in Section 3, and completely determine the isotopism classes in Section 4. For odd q, with the center size q and semifield order q^{2l} fixed, the number of isotopism classes in the Budaghyan–Helleseth family is equal to