Finite Fields and Their Applications 45 (2017) 170–182

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Groups of permutations generated by function–linear translator pairs

K. Kim, J. Namgoong, I. Yie *

Department of Mathematics, Inha University, 100 Inharo, Nam-gu, Incheon 22212, South Korea

ARTICLE INFO

Article history:
Received 27 April 2016
Received in revised form 5 October 2016
Accepted 8 December 2016
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
11T55
20B99
20E99

Keywords:
Permutation polynomial
Linear translator
Permutation group

ABSTRACT

In [8], G. Kyureghyan showed that the function $F(x) = x + \gamma f(x)$ is a permutation of $\mathbb{F}_{q^m}$ when $f : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is a function, $\gamma \in \mathbb{F}_{q^m}$ is a b-linear translator for f for some $b(\neq -1) \in \mathbb{F}_q$. His idea has been extended in [19] by Qin et al. and in [9] by M. Kyureghyan and Abrahamyan to finitely many function–linear translator pairs. In this paper, we study the permutations generated by function–linear translator pairs along G. Kyureghyan's idea and prove that these permutations form groups whose group structures are well understood.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. If a function f is bijective from $\mathbb{F}_q$ onto itself then f is called a permutation of $\mathbb{F}_q$. In particular, if f is given by a polynomial over $\mathbb{F}_q$, i.e., $f \in \mathbb{F}_q[x]$, we call f a permutation polynomial of $\mathbb{F}_q$. By means of interpolation

* Corresponding author.
E-mail addresses: ktkim@inha.ac.kr (K. Kim), anaeggum@inha.edu (J. Namgoong), ikyie@inha.ac.kr (I. Yie).

http://dx.doi.org/10.1016/j.ffa.2016.12.003
1071-5797/

due to Lagrange or Carlitz, every permutation of $\mathbb{F}_q$ can be represented by a polynomial in $\mathbb{F}_q[x]$ of degree less than q. Accordingly, we may use the terms permutation function and permutation polynomial interchangeably.

Permutation polynomials over finite fields have attracted a lot of attention due to their various applications as well as theoretical interests ([10–12,17,20,21] etc.). Many of the recent works concerning permutations have focused on finding classes of permutations of simple forms or certain algebraic properties ([1,4,7,8,14,18,19]). On the other hand, less effort is devoted to disclose structures of newly found permutations. Therefore, it seems natural to investigate such classes of permutations in order to figure out their precise structures.

Recall that the set of permutations of $\mathbb{F}_q$ becomes a group of order $q!$ under function composition. In the one-page paper [2], Carlitz proved that, when $q > 2$, the group is generated by the linear polynomials over $\mathbb{F}_q$ and the power map $x \mapsto x^{q-2}$. Motivated by Carlitz's result, several researches have been conducted to clarify either group structure or cycle structure of certain classes of permutation functions ([3,5,13,16,15,20,22–24]).

In the papers [4,8,14], new methods to construct permutation polynomials were introduced by exploiting effectively the additive structure of finite fields, not only the multiplicative one. Some of the results were slightly extended in [18,19]. In particular, Kyureghyan [8] utilized the so-called linear translator, also known as the linear structure, for finding permutations. For a given function $f : \mathbb{F}_{q^m} \to \mathbb{F}_q$ and an element $a \in \mathbb{F}_q$, a *nonzero* element $\alpha \in \mathbb{F}_{q^m}$ is called an a-linear translator if $f(x + u\alpha) - f(x) = ua$ for all $x \in \mathbb{F}_{q^m}$ and $u \in \mathbb{F}_q$. Kyureghyan showed that the map (†) $x \mapsto x + \gamma f(x)$ gives a permutation of $\mathbb{F}_{q^m}$ if γ is a b-linear translator for f for some $b(\neq -1) \in \mathbb{F}_q$ and went ahead to determine the cycle structure of such permutations. Qin et al. showed exactly when the map (‡) $x \mapsto x + \gamma_1 f_1(x) + \cdots + \gamma_n f_n(x)$ is a permutation of $\mathbb{F}_{q^m}$, where each $\gamma_1, \ldots, \gamma_n$ are linear translators for each of $f_1, \ldots, f_n$. In [6], Evoyan et al. tried to handle the maps of the form (‡) systematically using the concept of k-switching but they did not consider any group structure.

In this paper, we show that there are three groups naturally arising from permutations constructed by Kyureghyan and by Qin et al. and determine the structure of these groups. In Section 2 we prepare the background by studying vector spaces related with the concept of linear translators. In Section 3 we introduce three sets P^f, P_α, and P_V of functions of the form (†) or (‡), and we show these sets are closed under function composition. Then we note that in each case the functions with an inverse form a group. Finally in Section 4 we determine the structures of these groups.

2. Linear translators and related subspaces

In this section, we briefly summarize basic properties related to the concept of linear translators. We denote the field of q elements by $\mathbb{F}_q$. Throughout this paper we consider the extension $\mathbb{F}_{q^m}$ of degree m over $\mathbb{F}_q$. We start with the definition of linear translators.