Discrete Applied Mathematics 184 (2015) 213–222

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On constructing complete permutation polynomials over finite fields of even characteristic

Baofeng Wu [*], Dongdai Lin

State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 13 February 2014
Received in revised form 3 November 2014
Accepted 8 November 2014
Available online 4 December 2014

Keywords:
Complete permutation polynomial
Recursive
Compositional inverse
Monomial

ABSTRACT

In this paper, a construction of complete permutation polynomials over finite fields of even characteristic proposed by Tu et al. recently is generalized in a recursive manner. Besides, several classes of complete permutation polynomials are derived by computing compositional inverses of known ones.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements where q is a prime or a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial over $\mathbb{F}_q$ if it can induce a bijective map from $\mathbb{F}_q$ to itself, and the polynomial $f^{-1}(x) \in \mathbb{F}_q[x]$ satisfying

$$f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x},$$

is called the compositional inverse of $f(x)$. Permutation polynomials have important applications in combinatorics, coding and cryptography, thus constructions of them have been extensively studied (see e.g. [1,2,4,16,17]). On the other hand, for known classes of permutation polynomials, explicitly determining their compositional inverses also attracts a lot of attention. However, it is generally quite difficult to obtain explicit representations of known permutation polynomials. See [14,13,11] for some recent progresses on this topic.

A permutation polynomial $f(x) \in \mathbb{F}_q[x]$ is known as a complete permutation polynomial (CPP) over $\mathbb{F}_q$ if $f(x) + x$ can permute $\mathbb{F}_q$ as well. Such polynomials were initially studied by Niederreiter and Robinson in [10] motivated by their work on complete mappings of groups [9]. In fact, complete permutation polynomials can be related to such important combinatorial objects as orthogonal latin squares. However, to construct large classes of them is a big challenge, and there are rare classes of complete permutation polynomials known. We refer to [8,5,15,1,12], for example, for some results on this topic.

Generally speaking, it seems easier to construct complete permutation polynomials over finite fields of even characteristic, since it is implied by a result of Cohen that complete permutation polynomials over $\mathbb{F}_p$ of degree ≥ 2 do not exist for a sufficiently large prime p [3]. Very recently, several new classes of complete permutation polynomials over finite fields of even characteristic were constructed by Tu et al. in [12]. More precisely, they proposed three classes of complete permutation monomials and a class of complete permutation trinomials. Denote by $\mathrm{tr}_s^r(\cdot)$ the relative trace function from $\mathbb{F}_{2^r}$ to $\mathbb{F}_{2^s}$ for any positive integers r and s with $s \mid r$. Their results can be summarized in the following two theorems.

[*] Corresponding author. Fax: +86 13426076355.
E-mail address: wubaofeng@iie.ac.cn (B. Wu).

http://dx.doi.org/10.1016/j.dam.2014.11.008

Theorem 1.1 (*See [12, Theorem 1, Theorem 2, Theorem 3]*). *For two positive integers m, n, and an element $\upsilon \in \mathbb{F}_{2^n}^*$, the monomial $\upsilon^{-1}x^d$ is a complete permutation polynomial over $\mathbb{F}_{2^n}$ in either of the following three cases:*

(1) *$m \geq 2$, $n = 3m$, $(3, m) = 1$, $\mathrm{tr}_m^n(\upsilon) = 0$, and $d = 2^{2m} + 2^m + 2$;*

(2) *$m \geq 3$ is odd, $n = 2m$, $\mathrm{tr}_m^n(\beta\upsilon) = 0$ or $\mathrm{tr}_m^n(\beta^2\upsilon) = 0$ where β is a primitive 3rd root of unity in $\mathbb{F}_{2^n}^*$, and $d = 2^{m+1} + 3$;*

(3) *$m \geq 3$ is odd, $n = 2m$, υ is a non-cubic with $\upsilon^{2^m+1} = 1$, and $d = 2^{m-2}(2^m + 3)$.*

Theorem 1.2 (*See [12, Theorem 4]*). *For a positive integer m and an element $\upsilon \in \mathbb{F}_{2^m}\backslash\{0, 1\}$, the trinomial*

$$F(x) = x^{2^{2m}+1} + x^{2^m+1} + \upsilon x$$

is a complete permutation polynomial over $\mathbb{F}_{2^{3m}}$.

In this paper, we mainly focus on the class of complete permutation polynomials in Theorem 1.2. After noticing that the polynomial $F(x)$ in Theorem 1.2 is just $F(x) = x\left(\mathrm{tr}_m^{3m}(x) + x\right) + \upsilon x$, we find it can be easily derived that the polynomial

$$\bar{F}(x) = x\left(\mathrm{tr}_m^{nm}(x) + x\right) + \upsilon x$$

is a complete permutation polynomial over $\mathbb{F}_{2^{nm}}$ for any $\upsilon \in \mathbb{F}_{2^m} \setminus \{0, 1\}$ if n is an odd positive integer. Motivated by this fact, we generally consider polynomials of the form $xL(x) + \upsilon x$, where $L(x)$ is a linearized polynomial [7]. Our main observation is that complete permutation polynomials of this form over finite fields of characteristic 2 can be constructed recursively. More precisely, we find a complete permutation polynomial of this form over a finite field of characteristic 2 can be obtained from a complete permutation polynomial of the same form over certain subfield by virtue of the relative trace function.

On the other hand, it can be easily proved that the compositional inverse of a complete permutation polynomial also plays as a complete one; thus new classes of complete permutation polynomials can be derived from known ones, say, the classes of complete permutation monomials presented in Theorem 1.1, by computing their compositional inverses. For the class of complete permutation polynomials constructed recursively in this paper, we can also explicitly determine the compositional inverse class thanks to a technique given by the first author and Liu in [14], obtaining another recursive class of complete permutation polynomials over finite fields of even characteristic.

The rest of the paper is organized as follows. In Section 2, we construct a class of complete permutation polynomials recursively to generalize Theorem 1.2. In Section 3, we derive several new classes of complete permutation polynomials by computing compositional inverses of known ones. Concluding remarks are given in Section 4.

2. A construction of CPP's generalizing Theorem 1.2

Let m and n be two positive integers and $q = 2^m$. For simplicity, we denote by "tr" the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ in the remainder of the paper. Now we give a construction of complete permutation polynomials over $\mathbb{F}_{q^n}$ based on complete permutation polynomials over $\mathbb{F}_q$.

Theorem 2.1. *Let m and n be two positive integers where n is odd, and $q = 2^m$. Assume $L(x)$ is a linearized polynomial over $\mathbb{F}_q$ (i.e., $L(x)$ is of the form $\sum_{i=0}^{m-1} a_i x^{2^i}$ with $a_i \in \mathbb{F}_q$, $0 \leq i \leq m - 1$) such that $xL(x) + \upsilon x$ is a complete permutation polynomial over $\mathbb{F}_q$ for some $\upsilon \in \mathbb{F}_q \setminus \{0, 1\}$. Then*

$$F(x) = x\left(L(\mathrm{tr}(x)) + u\,\mathrm{tr}(x) + ux\right) + \upsilon x$$

is a complete permutation polynomial over $\mathbb{F}_{q^n}$ for any $u \in \mathbb{F}_q$.

Proof. We need only to prove that $F(x)$ can permute $\mathbb{F}_{q^n}$ for any $u \in \mathbb{F}_q$ if $xL(x) + \upsilon x$ can permute $\mathbb{F}_q$, for some $\upsilon \in \mathbb{F}_q \setminus \{0, 1\}$. Assume $F(x) = F(y)$ for two distinct elements x and y in $\mathbb{F}_{q^n}$. Since

$$\begin{aligned}\mathrm{tr}(F(x)) &= \mathrm{tr}(x)L(\mathrm{tr}(x)) + u\,\mathrm{tr}(x)^2 + u\,\mathrm{tr}(x^2) + \upsilon\mathrm{tr}(x)\\ &= \mathrm{tr}(x)L(\mathrm{tr}(x)) + \upsilon\mathrm{tr}(x)\end{aligned}$$

due to the relation $\mathrm{tr}(x)^2 = \mathrm{tr}(x^2)$, we have

$$\mathrm{tr}(x)L(\mathrm{tr}(x)) + \upsilon\mathrm{tr}(x) = \mathrm{tr}(y)L(\mathrm{tr}(y)) + \upsilon\mathrm{tr}(y),$$

which implies $\mathrm{tr}(x) = \mathrm{tr}(y)$ because $xL(x) + \upsilon x$ is a permutation polynomial of $\mathbb{F}_q$. Then from $F(x) = F(y)$ we can get

$$(x + y)\left(L(\mathrm{tr}(x)) + u\,\mathrm{tr}(x)\right) + u(x + y)^2 = \upsilon(x + y),$$

and thus

$$L(\mathrm{tr}(x)) + u\,\mathrm{tr}(x) + \upsilon = u(x + y)$$