Finite Fields and Their Applications 40 (2016) 1–9

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Piecewise constructions of inverses of cyclotomic mapping permutation polynomials ☆

Yanbin Zheng [a,b], Yuyin Yu [b,c], Yuanping Zhang [a], Dingyi Pei [b,c,*]

[a] *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China*
[b] *School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China*
[c] *Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, Guangzhou 510006, China*

A R T I C L E   I N F O

Article history:
Received 13 October 2015
Received in revised form 7 February 2016
Accepted 8 February 2016
Available online 2 March 2016
Communicated by Rudolf Lidl

MSC:
11T06
11T71

Keywords:
Inverse of permutation polynomial
Piecewise interpolation formula
Cyclotomic mapping

A B S T R A C T

Given a permutation polynomial of a large finite field, finding its inverse is usually a hard problem. Based on a piecewise interpolation formula, we construct the inverses of cyclotomic mapping permutation polynomials of arbitrary finite fields.

☆ This work was supported by the NSF of China (Grant Nos. 11371106, 61502113, 61363069) and the Guangdong Provincial NSF (Grant No. 2015A030310174).

* Corresponding author at: School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China.

E-mail addresses: zhengyanbin@guet.edu.cn (Y. Zheng), yuyuyin@163.com (Y. Yu), ypzhang12@gmail.com (Y. Zhang), gztcdpei@scut.edu.cn (D. Pei).

http://dx.doi.org/10.1016/j.ffa.2016.02.005
1071-5797/

1. Introduction

For q a prime power, let $\mathbb{F}_q$ denote the finite field containing q elements, and $\mathbb{F}_q[x]$ the ring of polynomials over $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a bijection of $\mathbb{F}_q$. We define a polynomial $f^{-1}(x)$ as the inverse of $f(x)$ over $\mathbb{F}_q$ if $f^{-1}(f(c)) = c$ for all $c \in \mathbb{F}_q$, or equivalently $f^{-1}(f(x)) \equiv x \pmod{x^q - x}$. Given a PP $f(x)$ of $\mathbb{F}_q$, its inverse is unique in the sense of reduction modulo $x^q - x$. In theory one could use the Lagrange Interpolation Formula to compute the inverse, i.e.,

$$f^{-1}(x) = \sum_{c \in \mathbb{F}_q} c\big(1 - (x - f(c))^{q-1}\big).$$

It is a point-by-point interpolation formula and the computing is very inefficient for large q. In fact, finding the inverse of a PP of a large finite field is a hard problem except for the well-known classes such as the inverses of linear polynomials, monomials, and some Dickson polynomials. There are only several papers on the inverses of some special classes of PPs, see [10,17] for the inverse of PPs of the form $x^r h(x^{(q-1)/d})$, [19,20] for the inverse of linearized PPs, [4,21] for the inverses of two classes of bilinear PPs, [14] for the inverses of more general classes of PPs.

The basic idea of piecewise constructions of PPs is to partition a finite field into subsets and to study the permutation property through their behavior on the subsets. Although the idea is not new [3,11], it is still currently being used to find new PPs [2,5–8,18,22,23]. In our recent work [24], the piecewise idea is employed to construct the inverse of a large class of PPs. In Section 2, a piecewise interpolation formula for the inverses of arbitrary PPs of finite fields is presented, which generalizes the Lagrange Interpolation Formula and the result in [24]. In Section 3, using our piecewise interpolation formula, we construct the inverses of cyclotomic mapping PPs studied in [18]. Section 4 gives the explicit inverses of special cyclotomic mapping PPs.

2. Piecewise constructions of PPs and their inverses

The idea of piecewise constructions of PPs was summarized in [2] by Cao, Hu and Zha, which can also be applied to construct PPs over finite rings. For later convenience, the following lemma expresses it in terms of finite fields.

Lemma 2.1. *(See [2, Proposition 3].) Let $D_1, \ldots, D_m$ be a partition of $\mathbb{F}_q$, and $f_1(x), \ldots, f_m(x) \in \mathbb{F}_q[x]$. Define*

$$f(x) = \sum_{i=1}^{m} f_i(x) I_{D_i}(x), \tag{1}$$