Finite Fields and Their Applications 45 (2017) 422–427

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# A note on inverses of cyclotomic mapping permutation polynomials over finite fields [☆]

Qiang Wang

*School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada*

ARTICLE INFO

*Article history:*
Received 16 December 2016
Accepted 21 January 2017
Available online xxxx
Communicated by Gary L. Mullen

*MSC:*
11T06

*Keywords:*
Finite fields
Permutation polynomials
Inverse polynomials
Cyclotomic mappings
Involutions

ABSTRACT

In this note, we give a shorter proof of the result of Zheng, Yu, and Pei on the explicit formula of inverses of generalized cyclotomic permutation polynomials over finite fields. Moreover, we characterize all these cyclotomic permutation polynomials that are involutions. Our results provide a fast algorithm (only modular operations are involved) to generate many classes of generalized cyclotomic permutation polynomials, their inverses, and involutions.

Let $q = p^m$ be the power of a prime number $p$, $\mathbb{F}_q$ be a finite field with $q$ elements, and $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$. We denote the composition of two polynomials $P(x), Q(x) \in \mathbb{F}[x]$ by $(P \circ Q)(x) := P(Q(x))$. We call $P(x) \in \mathbb{F}_q[x]$ a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$. Note that since $x^q = x$ for all $x \in \mathbb{F}_q$, one only needs to consider polynomials of degree less than $q$. It is clear that permutation polynomials form a group under composition and reduction modulo

[☆] Qiang Wang's research is partially supported by NSERC of Canada.

*E-mail address:* wang@math.carleton.ca.

http://dx.doi.org/10.1016/j.ffa.2017.01.006
1071-5797/© 2017 Elsevier Inc. All rights reserved.

$x^q - x$ that is isomorphic to the symmetric group on $q$ letters. Thus for any permutation polynomial $P(x) \in \mathbb{F}_q[x]$, there exists a unique $P^{-1}(x) \in \mathbb{F}_q[x]$ such that $P^{-1}(P(x)) \equiv P(P^{-1}(x)) \equiv x \pmod{x^q - x}$. Here $P^{-1}(x)$ is defined as the *compositional inverse* of $P(x)$, although we may simply call it sometimes the *inverse* of $P(x)$ on $\mathbb{F}_q$.

In [7], Mullen posed the problem of computing the coefficients of the inverse polynomial of a permutation polynomial efficiently (Problem 10). In fact, there are very few known permutation polynomials whose explicit compositional inverses have been obtained, and the resulting expressions are usually of a complicated nature except for the classes of the permutation linear polynomials, monomials, Dickson polynomials. Among them, see [15,16] for the inverses of linearized PPs and see [5,15] for inverses of some classes of bilinear PPs. A generalization of these results can be found in [10]. We note that each polynomial can be written uniquely in the form $x^r f(x^{(q-1)/\ell})$ where $\ell \mid (q-1)$ is the so-called index of the polynomial [1]. Although the explicit characterization of the inverses of PPs of the form $x^r f(x^{(q-1)/\ell})$ over $\mathbb{F}_q$ can be found in [8] and [12], computing these inverses of PPs in general is still not efficient if the index $\ell$ is large.

Let $\gamma$ be a fixed primitive element of $\mathbb{F}_q$ throughout the paper, $\ell \mid q-1$, and the set of all nonzero $\ell$-th powers be $C_0$. Then $C_0$ is a subgroup of $\mathbb{F}_q^*$ of index $\ell$. The elements of the factor group $\mathbb{F}_q^*/C_0$ are the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i = 0, 1, \cdots, \ell - 1.$$

For any $A_0, A_1, \cdots, A_{\ell-1} \in \mathbb{F}_q$ and a positive integer $r$, the *$r$-th order cyclotomic mapping $f^r_{A_0,A_1,\cdots,A_{\ell-1}}$ of index $\ell$* from $\mathbb{F}_q$ to itself is defined by

$$f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x) = \begin{cases} 0, & \text{if } x = 0; \\ A_i x^r, & \text{if } x \in C_i,\ 0 \le i \le \ell - 1. \end{cases}$$

Essentially $r$-th order cyclotomic mappings of index $\ell$ produce polynomials of the form $x^r f(x^{(q-1)/\ell})$. Earlier, Niederreiter and Winterhof [9] and Wang [11] have studied these cyclotomic mapping permutations. We note that a polynomial could be written in the form of cyclotomic mappings with different indices $\ell$'s, however, only the least index among them is defined as the index of the polynomial [1]. Normally it is harder to generate permutation polynomials with large indices. However, in [13], the author extended the idea of piecewise construction to obtain more classes of PPs with large indices. More specifically, different branch functions on these cyclotomic cosets were introduced.

For any $A_0, A_1, \cdots, A_{\ell-1} \in \mathbb{F}_q$ and monic polynomials $R_0(x), \ldots, R_{\ell-1}(x) \in \mathbb{F}_q[x]$ we define a *generalized cyclotomic mapping $f^{R_0(x),R_1(x),\ldots,R_{\ell-1}(x)}_{A_0,A_1,\cdots,A_{\ell-1}}$ of index $\ell$* from $\mathbb{F}_q$ to itself by

$$f^{R_0(x),R_1(x),\ldots,R_{\ell-1}(x)}_{A_0,A_1,\cdots,A_{\ell-1}}(x) = \begin{cases} 0, & \text{if } x = 0; \\ A_i R_i(x), & \text{if } x \in C_i,\ 0 \le i \le \ell - 1. \end{cases} \tag{1}$$