Commun. Math. Res.
doi: 10.4208/cmr.2021-0029

Vol. **38**, No. 2, pp. 246-318
May 2022

Generalized Cyclotomic Mappings: Switching Between Polynomial, Cyclotomic, and Wreath Product Form

Alexander Bors and Qiang Wang*

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON K1S 5B6, Canada.

Received 1 March 2021; Accepted 9 July 2021

Abstract. This paper is concerned with so-called index d generalized cyclotomic mappings of a finite field $\mathbb{F}_q$, which are functions $\mathbb{F}_q \to \mathbb{F}_q$ that agree with a suitable monomial function $x \mapsto ax^r$ on each coset of the index d subgroup of $\mathbb{F}_q^*$. We discuss two important rewriting procedures in the context of generalized cyclotomic mappings and present applications thereof that concern index d generalized cyclotomic permutations of $\mathbb{F}_q$ and pertain to cycle structures, the classification of $(q-1)$-cycles and involutions, as well as inversion.

AMS subject classifications: Primary: 11T22. Secondary: 11A07, 11T06, 20E22

Key words: Finite fields, cyclotomy, cyclotomic mappings, permutation polynomials, wreath product, cycle structure, involution.

1 Introduction

1.1 Background and main results

Let q be a prime power, let ω be a primitive root of $\mathbb{F}_q$, let d be a positive integer with $d \mid q-1$, and let C be the (unique) index d subgroup of $\mathbb{F}_q^*$. Note that the cosets of C in $\mathbb{F}_q^*$ are of the form $C_i := \omega^i C$ for $i = 0,1,\dots,d-1$. Index d cyclotomic

*Corresponding author. *Email addresses:* `alexanderbors@cunet.carleton.ca` (A. Bors), `wang@math.carleton.ca` (Q. Wang)

and generalized cyclotomic mappings of $\mathbb{F}_q$ are an interesting yet still relatively well-controlled generalization of monomial mappings (functions $\mathbb{F}_q \to \mathbb{F}_q$ of the form $x \mapsto ax^r$ for a fixed $a \in \mathbb{F}_q$ and non-negative integer r). They are studied in varying degrees of generality. A generalized cyclotomic mapping of $\mathbb{F}_q$ of index d is a function $\mathbb{F}_q \to \mathbb{F}_q$ of the form

$$f_\omega(\vec{a},\vec{r}) : x \mapsto \begin{cases} 0, & \text{if} \quad x=0, \\ a_i x^{r_i}, & \text{if} \quad x \in C_i, \quad i \in \{0,1,\ldots,d-1\} \end{cases} \tag{1.1}$$

for fixed $\vec{a}=(a_0,a_1,\ldots,a_{d-1}) \in \mathbb{F}_q^d$ and $\vec{r}=(r_0,r_1,\ldots,r_{d-1}) \in \{1,\ldots,\frac{q-1}{d}\}^d$, and we call this representation of the function an ω-cyclotomic form of it. If $\vec{a'}=(a'_0,\ldots,a'_{d-1}) \in \mathbb{F}_q^d$ and $\vec{r'}=(r'_0,\ldots,r'_{d-1}) \in \{1,2\ldots,\frac{q-1}{d}\}^d$ are other choices of such tuples, then $f_\omega(\vec{a},\vec{r})=f_\omega(\vec{a'},\vec{r'})$ if and only if $\vec{a}=\vec{a'}$ and $r_i=r'_i$ for all $i \in \{0,\ldots,d-1\}$ such that $a_i=a'_i \neq 0$.

In case the entries of $\vec{r}$ are all equal, say to an integer r, the function $f_\omega(\vec{a},\vec{r})$ is called an r-th order cyclotomic mapping of $\mathbb{F}_q$ of index d. We note that the notions of a generalized cyclotomic mapping of $\mathbb{F}_q$ of index d and, for each fixed r, of an r-th order cyclotomic mapping of $\mathbb{F}_q$ of index d, are independent of the choice of ω. For more details, see [21].

In this paper, we are concerned with generalized cyclotomic mappings that are permutations of $\mathbb{F}_q$, or generalized cyclotomic permutations of $\mathbb{F}_q$ for short. Our two main results, given below as Theorems 1.1 and 1.2, provide ways to rewrite the cyclotomic form (1.1) of such a permutation into two other important forms.

For the first rewriting method, which is the subject of Theorem 1.1, we observe that the generalized cyclotomic permutations of $\mathbb{F}_q$ of index d form a permutation group on $\mathbb{F}_q$. As 0 is a fixed point of every generalized cyclotomic permutation of $\mathbb{F}_q$, only the behavior on $\mathbb{F}_q^*$ is of interest, and so we will consider the permutation group on $\mathbb{F}_q^*$ that consists of all restrictions to $\mathbb{F}_q^*$ of generalized cyclotomic permutations of $\mathbb{F}_q$ of index d – this permutation group will be denoted by $\mathrm{GCP}(d,q)$. The rewriting method of Theorem 1.1 is a permutation group isomorphism between $\mathrm{GCP}(d,q)$ and a certain imprimitive permutational wreath product, described below. Since wreath products are well-understood, this allows one to study certain aspects of generalized cyclotomic permutations, such as cycle structure and conjugacy classes, using well-known results (dating back to a 1937 paper of Pólya, [19]), and we discuss such applications in Subsections 6.1 to 6.3. In this context, we note that various authors have studied the cycle structures of elements of certain classes of permutation polynomials over finite fields, see for example [1,5,11,16].