Finite Fields and Their Applications 52 (2018) 214–242

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A mass formula for cyclic codes over Galois rings of characteristic p^3

Boran Kim [a], Yoonjin Lee [b,*,1]

[a] *Institute of Mathematical Sciences, Ewha Womans University, 52 Ewhayeodae-gil, Seodaemun-gu, Seoul, 03760, South Korea*
[b] *Department of Mathematics, Ewha Womans University, 52 Ewhayeodae-gil, Seodaemun-gu, Seoul, 03760, South Korea*

A R T I C L E   I N F O

Article history:
Received 10 September 2017
Received in revised form 5 March 2018
Accepted 11 April 2018
Available online xxxx
Communicated by W. Cary Huffman

MSC:
primary 94B15

Keywords:
Cyclic code
Galois ring
Mass formula
Ideal
Generator

A B S T R A C T

We completely determine the explicit generators of cyclic codes of length p^k ($k \geq 1$) over a Galois ring of characteristic p^3 by their *residue degree*, and their two *torsional degrees*; there are exactly three types of cyclic codes, that is, one-generator, two-generator and three-generator cyclic codes. Using this classification result, we explicitly obtain a mass formula for cyclic codes of length p^k over a Galois ring of characteristic p^3.

* Corresponding author.
E-mail addresses: borank@ewha.ac.kr (B. Kim), yoonjinl@ewha.ac.kr (Y. Lee).

1 Supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (NRF-2017R1A2B2004574). The authors are also supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827).

https://doi.org/10.1016/j.ffa.2018.04.005
1071-5797/

1. Introduction

Cyclic codes over finite fields or finite rings have been actively developed. For instance, Jia et al. investigated the existence of cyclic self-dual codes over finite fields [3]. Pless et al. studied cyclic self-dual codes over $\mathbb{Z}_4$ of odd lengths and found a list of cyclic self-dual codes of lengths up to 39 [9]. In [1], they completely determined the explicit generators of cyclic codes over $\mathbb{Z}_4$ of length 2^k ($k \geq 1$), and in [2], they found the generators for cyclic codes over $\mathbb{Z}_4$ of length $2n$ with an odd n.

A ring $GR(p^e, m) = \mathbb{Z}_{p^e}[x]/\langle g(x)\rangle$ is called a *Galois ring* of characteristic p^e with $(p^e)^m$ elements, where p is a prime number and $g(x)$ is a *monic basic irreducible polynomial* of degree m in $\mathbb{Z}_{p^e}[x]$ with $e \geq 1$. A notion of Galois rings is a broader concept in a sense that Galois rings contain both finite rings $\mathbb{Z}_{p^e} \cong GR(p^e, 1)$ and finite fields $\mathbb{F}_{p^m} \cong GR(p, m)$. Kiah et al. found the classification of all cyclic codes over $GR(p^2, m)$ of length p^k ($k \geq 1$) [5]. Kiah et al. and Sobhani et al. investigated the cyclic self-dual codes over $GR(p^2, m)$ of length p^k and their mass formula [6,10]. X. Kai and S. Zhu found the minimum Hamming weights of cyclic codes over $\mathbb{Z}_4$ of length 2^k and some partial results on minimum Lee weights of cyclic codes over $\mathbb{Z}_4$ of length 2^k [4]. In [8], the authors completely determined the minimum Lee weights of cyclic self-dual codes of length p^k over a Galois ring $GR(p^2, m)$ of characteristic p^2.

We completely determine the explicit generators of cyclic codes of length p^k ($k \geq 1$) over a Galois ring $GR(p^3, m)$ of characteristic p^3 by their *residue degree*, and their two *torsional degrees*; there are exactly three types of cyclic codes, that is, one-generator, two-generator and three-generator cyclic codes. Using this classification result, we explicitly obtain a mass formula for cyclic codes over a Galois ring $GR(p^3, m)$ of length p^k.

This paper is organized as follows. In Section 2, we introduce some basic facts and notations. In Section 3, we completely determine the first torsional degree and the second torsional degree of every cyclic code of length p^k ($k \geq 1$) over a Galois ring $GR(p^3, m)$ of characteristic p^3 (Lemmas 3.2, 3.3 and 3.4). We then explicitly classify the generators of cyclic codes of length p^k over a Galois ring $GR(p^3, m)$ of characteristic p^3 by their residue degree, and their two torsional degrees (Theorem 3.5). We present a mass formula for cyclic codes of length p^k over $GR(p^3, m)$ (Theorem 4.1).

2. Preliminaries

We use the following notation throughout this paper.

Notation 1.

p	a prime number
$m,\ k$	positive integers
$\mathbb{F}_{p^m}$	a finite field with p^m elements
$\mathcal{R} = GR(p^3, m)$	a Galois ring of characteristic p^3 with $(p^3)^m$ elements