Discrete Mathematics 338 (2015) 922–937

Contents lists available at ScienceDirect

Discrete Mathematics

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

Enumeration and construction of additive cyclic codes over Galois rings

Yonglin Cao [a,*], Jian Gao [b], Fang-Wei Fu [b], Yuan Cao [c]

[a] School of Sciences, Shandong University of Technology, Zibo, Shandong 255091, China

[b] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China

[c] College of Electrical and Information Engineering, Hunan University, Changsha 410082, China

ARTICLE INFO

Article history:
Received 28 October 2014
Received in revised form 6 January 2015
Accepted 15 January 2015
Available online 11 February 2015

Keywords:
Additive cyclic code
Galois ring
Linear code
Dual code
Trace inner product
Self-dual code
Quasi-cyclic code

ABSTRACT

Let $R = \mathrm{GR}(p^\epsilon, l)$ be a Galois ring of characteristic p^ϵ and cardinality $p^{\epsilon l}$, where p and l are prime integers. First, we give a canonical form decomposition for additive cyclic codes over R. This decomposition is used to construct additive cyclic codes and count the number of such codes, respectively. Then we give the trace dual code for each additive cyclic code over R from its canonical form decomposition and linear codes of length l over some extension Galois rings of $\mathbb{Z}_{p^\epsilon}$.

1. Introduction

Algebraic coding theory deals with the design of error-correcting and error-detecting codes for the reliable transmission of information across noisy channel. It in general makes use of many algebra systems such as finite fields, groups, Galois rings, polynomial algebra, module theory and matrix theory over finite chain rings and areas of discrete mathematics.

Let $R = \mathrm{GR}(p^\epsilon, l)$ be a Galois ring of characteristic p^ϵ and cardinality $p^{\epsilon l}$ where p is a prime integer and ϵ, l are positive integers. We can regard $\mathbb{Z}_{p^\epsilon}$ as a subring of R in the usual sense. Let n be a positive integer. A nonempty subset $\mathcal{C}$ of the R-module R^n is called an *additive code* over R of length n if $\mathcal{C}$ is a subgroup of R^n under addition. Then the minimal distance of an additive code $\mathcal{C}$ is equal to $d = \min\{\mathrm{wt}_H(c) \mid c \neq 0,\ c \in \mathcal{C}\}$, where $\mathrm{wt}_H(c) = |\{i \mid c_i \neq 0,\ 0 \leq i \leq n-1\}|$ is the Hamming weight of $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ with $c_i \in R$. By the Singleton Bound, we have $|\mathcal{C}| \leq |R|^{n-d+1}$. If $|\mathcal{C}| = |R|^{n-d+1}$, $\mathcal{C}$ is said to be MDS (maximal distance separable). It is clear that $\mathcal{C}$ is an additive code over R if and only if $\mathcal{C}$ is a $\mathbb{Z}_{p^\epsilon}$-submodule of R^n. Furthermore, an additive code $\mathcal{C}$ is said to be *cyclic* if $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$ for all $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$.

When $\epsilon = 1$, $R = \mathrm{GR}(p, l) = \mathbb{F}_{p^l}$ which is a finite field of characteristic p and cardinality p^l. For the special case of $p = l = 2$, additive codes over the finite field $\mathbb{F}_4$ were first introduced in the year 1998 in [3] connecting these codes to binary quantum codes. One year later, for the special case of $l = 2$ additive codes over the finite field $\mathbb{F}_{p^2}$ were connected

* Corresponding author.
E-mail addresses: ylcao@sdut.edu.cn (Yonglin Cao), jiangao@mail.nankai.edu.cn (J. Gao), fwfu@nankai.edu.cn (F.-W. Fu), yuan_cao@hnu.edu.cn (Yuan Cao).

http://dx.doi.org/10.1016/j.disc.2015.01.012
0012-365X/

in [14] to nonbinary quantum codes. Additive codes over finite fields were also generalized and studied in many papers, for example [1,2,4,5].

Let $l = rm$ and denote $q = p^r$. Then $\mathbb{F}_{p^l}$ has a unique subfield of cardinality q, say $\mathbb{F}_q$, and $\mathbb{F}_{p^l} = \mathbb{F}_{q^m}$ which is an extension field of $\mathbb{F}_q$ with degree m. As a generalization of additive codes over $\mathbb{F}_{q^m}$, a nonempty subset $\mathcal{C}$ of the $\mathbb{F}_{q^m}$-linear space $\mathbb{F}_{q^m}^n$ is called an $\mathbb{F}_q$-*linear code* over $\mathbb{F}_{q^m}$ of length n if $\mathcal{C}$ is closed under addition and multiplication with elements from $\mathbb{F}_q$ (cf. [6,8–10]). Huffman presented a theory for constructing and counting additive cyclic codes and additive cyclic self-orthogonal codes over $\mathbb{F}_4$ of odd length in [11]. And later, the author extended this work to even length in [12], and developed a general theory to $\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_{q^m}$ in [8].

In the rest of this paper, let $R = \mathrm{GR}(p^\epsilon, l)$ where $\epsilon \geq 2$ and l is a prime number, and n is a positive integer satisfying $\gcd(p, n) = 1$. We plan to consider the following questions for additive cyclic codes over R of length n:

- How many distinct additive cyclic codes over R of length n are there?
- How can we construct all additive cyclic code over R of length n?
- For each additive cyclic code $\mathcal{C}$ over R of length n constructed above, how can we give an encoder (for example, a generator matrix) and obtain the dual code of $\mathcal{C}$?

Now, let $\mathcal{R}_n$ denote the group ring $R[X]/(X^n - 1)$ where $(X^n - 1)$ is the ideal in $R[X]$ generated by $X^n - 1$, and $\mathcal{R}_n^{(p)}$ the group ring $\mathbb{Z}_{p^\epsilon}[X]/(X^n - 1)$ where $(X^n - 1)$ is the ideal in $\mathbb{Z}_{p^\epsilon}[X]$ generated by $X^n - 1$. From now on, we regard $\mathcal{R}_n^{(p)}$ as a subring of $\mathcal{R}_n$ in the natural way, and identify $a(X) + (X^n - 1) \in \mathcal{R}_n$ with $a(X) \pmod{X^n - 1}$ for any $a(X) \in R[X]$. Then $\mathcal{R}_n$ is a $\mathcal{R}_n^{(p)}$-module. Now, for any $a(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in \mathcal{R}_n$ we define $\Upsilon : a(X) \mapsto a = (a_0, a_1, \ldots, a_{n-1})$. Then Υ is an R-module isomorphism from $\mathcal{R}_n$ onto R^n. It is clear that $\mathcal{C}$ is an additive cyclic code over R of length n if and only if there is a unique $\mathcal{R}_n^{(p)}$-submodule $\mathcal{D}$ of $\mathcal{R}_n$ such that $\Upsilon(\mathcal{D}) = \mathcal{C}$. In this paper, we will identify $\mathcal{C}$ with $\mathcal{D}$ for convenience.

The present paper is organized as follows. In Section 2, we investigate the structural properties of the ring $\mathcal{R}_n$ and $\mathcal{R}_n^{(p)}$ first, and then consider the relationship between the decompositions of $\mathcal{R}_n$ and $\mathcal{R}_n^{(p)}$. In Section 3, we present a canonical form decomposition of additive cyclic codes over R of length n, and consider how to enumerate, construct and encode these codes respectively. In Section 4, we give the trace dual code of an additive cyclic code over R from its canonical form decomposition, and investigate the quasi-cyclic code over $\mathbb{Z}_{p^\epsilon}$ of length nl and index l corresponding to each additive cyclic code over R of length n. Then we consider the construction of additive cyclic codes over the Galois ring $\mathrm{GR}(3^2, 2)$ of length 10 in Section 5.

2. Preliminaries

In this section, we consider decompositions for the rings $\mathcal{R}_n$ and $\mathcal{R}_n^{(p)}$ first. Let $C_i^{(b)} = \{i, ib, ib^2, \ldots\} \pmod n$ be the b-cyclotomic coset containing i modulo n and denote the size of $C_i^{(b)}$ by $|C_i^{(b)}|$, where b is either p or p^l. Since l is a prime integer, from [8] Lemma 1 we deduce the following.

Lemma 2.1. (i) *If* $\gcd(|C_i^{(p)}|, l) = 1$, *then* $C_i^{(p)} = C_i^{(p^l)}$.

(ii) *If* $l \| C_i^{(p)}|$, *then* $|C_i^{(p)}| = l|C_i^{(p^l)}|$ *and* $C_i^{(p)} = C_i^{(p^l)} \cup C_{ip}^{(p^l)} \cup \cdots \cup C_{ip^{l-1}}^{(p^l)}$ *where the union is disjoint.*

Assume $\upsilon = \min\{k \in \mathbb{Z}^+ \mid (p^l)^k \equiv 1 \pmod n\}$. By the theory of Galois rings (cf. Wan [15]), there is an extension Galois ring $\widehat{R}$ of R with degree υ and an invertible element $\zeta \in \widehat{R}$ of multiplicative order $p^{\upsilon l} - 1$. Denote $\widehat{\mathcal{T}} = \{0, 1, \zeta, \ldots, \zeta^{p^{\upsilon l}-2}\}$, which is a *Teichmüller* set of $\widehat{R}$. Then each element $a \in \widehat{R}$ can be uniquely expressed as $a_0 + a_1p + \cdots + a_{\epsilon-1}p^{\epsilon-1}$, $a_0, a_1, \ldots, a_{\epsilon-1} \in \widehat{\mathcal{T}}$. Define

$$\widehat{\phi}(a) = a_0^p + a_1^p p + \cdots + a_{\epsilon-1}^p p^{\epsilon-1}$$

and let $\phi = \widehat{\phi}|_R$ be the restriction of $\widehat{\phi}$ to R. Then $\widehat{\phi}$ is a ring automorphism of $\widehat{R}$ satisfying $\widehat{\phi}(b) = b$ for any $b \in \mathbb{Z}_{p^\epsilon}$ (cf. [15] Theorem 14.30). $\widehat{\phi}$ is called the *generalized Frobenius automorphism* of $\widehat{R}$ over $\mathbb{Z}_{p^\epsilon}$. Let X be an indeterminate over $\widehat{R}$ and extend $\widehat{\phi}$ to a ring automorphism of $\widehat{R}[X]$ by $\widehat{\phi}(\sum \alpha_i X^i) = \sum \widehat{\phi}(\alpha_i)X^i$ $(\forall \alpha_i \in \widehat{R})$. In the rest of this paper, let $\omega = \zeta^{\frac{p^{\upsilon l}-1}{p^l-1}}$ and denote $\mathcal{T} = \{0, 1, \omega, \ldots, \omega^{p^l-2}\}$. Then from Galois ring theory (cf. [15] Theorem 14.27 and Corollary 14.28) we deduce the following.

- $\mathrm{ord}(\omega) = p^l - 1$.
- $R = \mathbb{Z}_{p^\epsilon}[\omega] = \{\sum_{i=0}^{l-1} c_i\omega^i \mid c_0, c_1, \ldots, c_{l-1} \in \mathbb{Z}_{p^\epsilon}\}$, and each element $a \in R$ can be uniquely expressed as $a = \sum_{i=0}^{\epsilon-1} a_i p^i$ with $a_i \in \mathcal{T}$.
- $\phi = \widehat{\phi}|_R : R \to R$, given by $\phi(a) = \sum_{i=0}^{\epsilon-1} a_i^p p^i$ for all $a_0, a_1, \ldots, a_{\epsilon-1} \in \mathcal{T}$, is a ring automorphism of R satisfying $\phi(b) = b$ for any $b \in \mathbb{Z}_{p^\epsilon}$. In fact, ϕ is the *generalized Frobenius automorphism* of R over $\mathbb{Z}_{p^\epsilon}$. Furthermore, by [15] Theorem 14.30 we have

$$\phi(a) = \sum_{i=0}^{l-1} c_i\omega^{ip}, \quad \forall a = \sum_{i=0}^{l-1} c_i\omega^i,\ c_0, c_1, \ldots, c_{l-1} \in \mathbb{Z}_{p^\epsilon}.$$