ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

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

Primitive idempotents of irreducible cyclic codes and self-dual cyclic codes over Galois rings

Yansheng Wu [a,b,c], Qin Yue [a,b,c,*], Fengwei Li [d]

[a] Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 211100, PR China
[b] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, PR China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, PR China
[d] School of Mathematics and Statistics, Zaozhuang University, Zaozhuang, 277160, PR China

ARTICLE INFO

Article history:
Received 6 June 2017
Received in revised form 5 October 2017
Accepted 24 October 2017
Available online xxxx

Keywords:
Primitive idempotents
Irreducible cyclic codes
Weight distribution
Self-dual cyclic codes

ABSTRACT

Let R be the Galois ring $GR(p^k, s)$ of characteristic p^k and cardinality p^{sk}. Firstly, we give all primitive idempotent generators of irreducible cyclic codes of length n over R, and a p-adic integer ring with $\gcd(p, n) = 1$. Secondly, we obtain all primitive idempotents of all irreducible cyclic codes of length rl^m over R, where r, l, and t are three primes with $2 \nmid l$, $r|(q^t-1)$, $l^v \parallel (q^t-1)$ and $\gcd(rl, q(q-1)) = 1$. Finally, as applications, weight distributions of all irreducible cyclic codes for $t = 2$ and generator polynomials of self-dual cyclic codes of length l^m and rl^m over R are given.

1. Introduction

At the beginning of the 1990s, codes over rings drew the attention of scholars due to the work of Nechaev [26] and Hammons et al. [19]. They showed that several prominent families of good nonlinear binary codes can be identified as images of $\mathbb{Z}_4$-linear codes under the fundamental Gray isometry between $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$, the former equipped with the Lee metric, the latter with the Hamming metric. Since then, codes and sequences over rings have been widely investigated (see [5–7,12–14]).

Let R be a commutative ring with identity. A linear code $\mathcal{C}$ of length n over R is an R-submodule of R^n. In particular, if R is a finite field of order q, a linear $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q$. Note that cyclic codes of length n over the ring R are described by the ideals of the ring $R[x]/\langle x^n - 1\rangle$ or as an ideal in the group algebra RC_n, where C_n denotes the cyclic group of order n. Irreducible cyclic codes of length n are the ideals generated by primitive idempotents. A lot of papers investigate the primitive idempotents of cyclic codes over finite rings, especially for finite fields. For instance, in 1997, Kanwar et al. [20] obtained all primitive idempotents of irreducible cyclic codes over the ring of integers modulo p^m. For more details about primitive idempotents of cyclic codes, the reader is referred to [1–4,10,18,20,22–24,29].

For a code $\mathcal{C}$ of length n over R, the dual code of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{u \in R^n | u \cdot v = 0, \textit{for all } v \in \mathcal{C}\}$, where $u \cdot v$ denotes the standard Euclidean inner product of u and v in R^n. The code $\mathcal{C}$ is said to be self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and self-dual if $\mathcal{C} = \mathcal{C}^\perp$. Qian et al. [28] presented enumeration formulas for self-dual cyclic codes of odd length over $\mathbb{Z}_{2m}$. Later, Chen et al. [9] got some new necessary and sufficient conditions for the existence of nontrivial self-dual cyclic codes of length n over finite commutative chain rings. More papers related to self-dual codes over rings or fields are following: [5,8,11,15,16,28].

* Corresponding author at: Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 211100, PR China.
E-mail address: yueqin@nuaa.edu.cn (Q. Yue).

https://doi.org/10.1016/j.disc.2017.10.027
0012-365X/

Let A_i be the number of codewords with Hamming weight i in the code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by $A(z) = 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$. The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code $\mathcal{C}$. In coding theory it is often desirable to know the weight distributions of the codes because they can be used to estimate the error correcting capability and the error probability of error detection and correction with respect to some algorithms.

The remainder of this paper is organized as follows. In Section 2, there are some preliminaries. In Section 3, we investigate primitive idempotents of $R[x]/\langle x^n - 1\rangle$ for a Galois ring R; in particular, we also obtain all irreducible cyclic codes of length n over the p-adic integer ring with $\gcd(p, n) = 1$. In Section 4, primitive idempotents of all irreducible cyclic codes of length rl^m over a Galois ring R are obtained. This work, see Theorems 4.1 and 4.2, is an extension of the results of [22, Theorem 3.3, Theorem 3.7]. Finally, as applications, weight distributions of irreducible cyclic codes of length rl^m in case of $t = 2$ and all generator polynomials of self-dual cyclic codes of length l^m and rl^m over a Galois ring are given in Section 5.

For convenience, we introduce the following notations in this paper:

q	A power of prime p, $q = p^s$,
$\mathbb{Z}_{p^k}$	A residue class ring modulo p^k,
$R = GR(p^k, s)$	Galois ring of characteristic p^k and cardinality p^{ks},
$R' = GR(p^k, st)$	Galois ring of characteristic p^k and cardinality p^{kst},
$\mathbb{F}_q$	Finite field $GF(q)$,
Tr	Trace function from R' to R,
tr	Trace function from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$,
μ	The map of reduction modulo p,
$\widehat{f(x)}$	$\widehat{f(x)} = (x^n - 1)/f(x)$ if the polynomial $f(x)$ divides $x^n - 1$,
$f^*(x)$	The reciprocal polynomial of $f(x)$.

2. Review of Galois rings and p-adic integer rings

Some preliminaries on Galois rings and p-adic integer rings are given below. For more details, the reader is referred to [19,17,21,25,30].

For positive integers k and m such that $k, m \geq 1$, let $\mathbb{Z}_{p^k}$ be the ring of integers modulo p^k and f a monic basic irreducible polynomial of degree m in $\mathbb{Z}_{p^k}[x]$. The ring $\mathbb{Z}_{p^k}[x]/(f)$ is called the Galois ring denoted by $GR(p^k, s)$, which is a Galois extension of the ring $\mathbb{Z}_{p^k}$. In particular, $GR(p^k, 1) = \mathbb{Z}_{p^k}$ and $GR(p, s) = \mathbb{F}_{p^s}$. In this paper, assume that $R = GR(p^k, s)$. Then R is a finite chain ring of length $k + 1$ and its unique maximal ideal is pR, i.e.

$$\{0\} = p^k R < p^{k-1} R < \cdots < pR < R.$$

The group of units of the Galois ring contains a unique cyclic multiplicative group $\mathcal{T}_s^*$ of order $p^s - 1$. If ξ_s is a generator of this group, then $\mathcal{T}_s^* = \langle \xi_s \rangle$ and the set

$$\mathcal{T} = \mathcal{T}_s^* \cup \{0\} = \{0, 1, \xi_s, \ldots, \xi_s^{p^s - 2}\}$$

is called the Teichmuller representative set of R. Let $\mathbb{F}_{p^s}$ denote the Galois field $GF(p^s)$, then there is a ring isomorphism $R/pR \cong \mathbb{F}_{p^s}$ and there is a multiplicative group isomorphism $\mathcal{T}_s^* \cong \mathbb{F}_{p^s}^*$. For $a \in R$,

$$a = \sum_{i=0}^{k-1} p^i a_i = a_0 + a_1 p^1 + \cdots + a_{k-1} p^{k-1}, a_i \in \mathcal{T}.$$

We need more knowledges of algebraic number theory. Let $\mathbb{Q}_p$ be the p-adic field and E an un-ramified extension over $\mathbb{Q}_p$ with $[E : \mathbb{Q}_p] = s$. Let $v_p(\cdot)$ be the canonical exponential valuation of E, $O = \{a \in E | v_p(a) \geq 0\}$ is called the integral ring of E, i.e. for $a \in O$,

$$a = \sum_{i=0}^{\infty} a_i p^i = a_0 + a_1 p^1 + \cdots + a_n p^n + \cdots, a_i \in T.$$

In fact, $O/p^k O \cong R = GR(p^k, s)$, $O/pO \cong R/pR \cong \mathbb{F}_{p^s}$. Let E' be an unramified extension of the p-adic field E with $[E' : E] = t$ and O' the integral ring of E'. Then $O'/p^k O' \cong R' = GR(p^k, st)$ and $O'/pO' \cong \mathbb{F}_{p^{st}}$.

Let $Tr' : E' \to E$, $Tr : R' \to R$, and $tr : \mathbb{F}_{p^{st}} \to \mathbb{F}_{p^s}$ be trace maps. Then there is a commutative diagram:

$$\begin{array}{ccccc} O' & \longrightarrow & R' & \longrightarrow & \mathbb{F}_{p^{st}} \\ \downarrow & & \downarrow Tr & & \downarrow tr \\ O & \longrightarrow & R & \longrightarrow & \mathbb{F}_{p^s} \end{array}$$

where for $a' = \sum_{i=0}^{k-1} a_i' p^i \in R'$, $Tr(a') = \sum_{i=0}^{k-1} tr(a_i') p^i \in R$.

Please cite this article in press as: Y. Wu, et al., Primitive idempotents of irreducible cyclic codes and self-dual cyclic codes over Galois rings, Discrete Mathematics (2017), https://doi.org/10.1016/j.disc.2017.10.027.