Finite Fields and Their Applications 40 (2016) 138–149

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quasi-cyclic codes as cyclic codes over a family of local rings[☆]

Steven T. Dougherty[a], Cristina Fernández-Córdoba[b,*], Roger Ten-Valls[b]

[a] Department of Mathematics, University of Scranton, Scranton, PA 18510, USA
[b] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

ARTICLE INFO

Article history:
Received 3 December 2015
Accepted 3 April 2016
Available online 27 April 2016
Communicated by Gary L. Mullen

MSC:
94B60
94B25

Keywords:
Quasi-cyclic codes
Codes over rings

ABSTRACT

We give an algebraic structure for a large family of binary quasi-cyclic codes. We construct a family of commutative rings and a canonical Gray map such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space via the Gray map. We use the Gray map to produce optimal linear codes that are quasi-cyclic.

1. Introduction

Cyclic codes have been a primary area of study for coding theory since its inception. In many ways, they were a natural object of study since they have a natural algebraic

☆ This work has been partially supported by the Spanish MINECO grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-0691.
* Corresponding author.
E-mail addresses: prof.steven.dougherty@gmail.com (S.T. Dougherty), cristina.fernandez@uab.cat (C. Fernández-Córdoba), roger.ten@uab.cat (R. Ten-Valls).

http://dx.doi.org/10.1016/j.ffa.2016.04.002

description. Namely, cyclic codes can be described as ideals in a corresponding polynomial ring. A canonical algebraic description for quasi-cyclic codes has been more elusive. In this paper, we shall give an algebraic description of a large family of quasi-cyclic codes by viewing them as the image under a Gray map of cyclic codes over rings from a family which we describe. This allows for a construction of binary quasi-cyclic codes of arbitrary index.

In [6], cyclic codes were studied over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which gives rise to quasi-cyclic codes of index 2. In [1,2] and [3], a family of rings, $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0\rangle$, was introduced. Cyclic codes were studied over this family of rings. These codes were used to produce quasi-cyclic binary codes whose index was a power of 2. In this work, we shall describe a new family of rings which contains the family of rings R_k. With this new family, we can produce quasi-cyclic codes with arbitrary index as opposed to simply indices that are a power of 2.

A code of length n over a ring R is a subset of R^n. If the code is also a submodule then we say that the code is linear. Let π act on the elements of R^n by $\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. Then a code C is said to be cyclic if $\pi(C) = C$. If $\pi^s(C) = C$ then the code is said to be quasi-cyclic of index s.

2. A family of rings

In this section, we shall describe a family of rings which contains the family of rings described in [1,2] and [3].

Let $p_1, p_2, \ldots, p_t$ be prime numbers with $t \geq 1$ and $p_i \neq p_j$ if $i \neq j$, and let $\Delta = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Let $\{u_{p_i,j}\}_{(1\leq j\leq k_i)}$ be a set of indeterminants. Define the following ring

$$R_\Delta = R_{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}} = \mathbb{F}_2[u_{p_1,1}, \ldots, u_{p_1,k_1}, u_{p_2,1} \ldots, u_{p_2,k_2}, \ldots, u_{p_t,k_t}]/\langle u_{p_i,j}^{p_i} = 0\rangle,$$

where the indeterminants $\{u_{p_i,j}\}_{(1\leq i\leq t, 1\leq j\leq k_i)}$ commute. Note that for each Δ there is a ring in this family.

Any indeterminant $u_{p_i,j}$ may have an exponent in the set $J_i = \{0, 1, \ldots, p_i - 1\}$. For $\alpha_i \in J_i^{k_i}$ denote $u_{p_i,1}^{\alpha_{i,1}} \cdots u_{p_i,k_i}^{\alpha_{i,k_i}}$ by $u_i^{\alpha_i}$, and for a monomial $u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ in R_Δ we write u^α, where $\alpha = (\alpha_1, \ldots, \alpha_t) \in J_1^{k_1} \times \cdots \times J_t^{k_t}$. Let $J = J_1^{k_1} \times \cdots \times J_t^{k_t}$.

Any element c in R_Δ can be written as

$$c = \sum_{\alpha\in J} c_\alpha u^\alpha = \sum_{\alpha\in J} c_\alpha u_{p_1,1}^{\alpha_{1,1}} \cdots u_{p_1,k_1}^{\alpha_{1,k_1}} \cdots u_{p_t,1}^{\alpha_{t,1}} \cdots u_{p_t,k_t}^{\alpha_{t,k_t}}, \quad (1)$$

with $c_\alpha \in \mathbb{F}_2$.

Lemma 2.1. *The ring R_Δ is a commutative ring with $|R_\Delta| = 2^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}}$.*

Proof. The fact that the ring is commutative follows from the fact that the indeterminants commute.