Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 125–129*

Cyclic codes over A_k

Yasemin Cengellenmis ycengellenmis@yahoo.com
Trakya University
Steven T. Dougherty prof.steven.dougherty@gmail.com
University of Scranton

Abstract. In this paper, we give a characterization of cyclic codes over the ring A_k. We then examine when cyclic codes are self-dual and describe the binary images of these codes under a Gray map.

1 Introduction

We shall further investigate cyclic codes over the ring A_k building on the results of [2]. The ring A_k is defined to be $\mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i, v_i v_j = v_j v_i\rangle$. It is easy to see that A_k is a commutative principal ideal ring. We equip it with a distance preserving Gray map. Specifically, for $k = 1$ the map is defined as $\phi_{A_1}(a + bv_1) = (a, a + b)$. Then the Gray map for A_k is defined recursively as:

$$\phi_{A_k}(a + bu_k) = (\phi_{A_{k-1}}(a), \phi_{A_{k-1}}(a) + \phi_{A_{k-1}}(b))$$

where $a, b \in A_{k-1}$. A code of length n is a subset of A_k^n and it is said to be a linear code if it is a submodule of A_k^n. For a complete description of codes over this family of rings see [2].

A code is cyclic if it has the following property: if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(c_1, c_2, \ldots, c_{n-1}, c_0) \in C$. We call this the cyclic shift and denote this action by the map σ. Let $\mathbf{a} \in \mathbb{F}_2^{2^k n}$ with

$$\mathbf{a} = (a_0, \ldots, a_{2^k n-1}) = (a^{(0)}|a^{(1)}|\ldots|a^{(2^k-1)}), a^{(i)} \in \mathbb{F}_2^n$$

for $i = 0, 1, \ldots, 2^k - 1$. Let $\sigma^{\otimes 2^k}$ be the map from $\mathbb{F}_2^{2^k n}$ to $\mathbb{F}_2^{2^k n}$ given by $\sigma^{\otimes 2^k}(a) = (\sigma(a^{(0)})|\ldots|\sigma(a^{(2^k-1)}))$ where σ is the usual shift $(c_0, \ldots, c_{n-1}) \mapsto (c_{n-1}, c_0, \ldots, c_{n-2})$ on $\mathbb{F}_2^n$. A code C of length $2^k n$ over $\mathbb{F}_2$ is said to be quasi-cyclic of index 2^k if $\sigma^{\otimes 2^k}(C) = C$. The following is shown in [2].

Lemma 1. *[2] If C is a cyclic code over A_k then the image of C under the Gray map is a quasi-cyclic binary code of length $2^k n$ of index 2^k.*

In the usual correspondence, cyclic codes over A_k are in a bijective correspondence with the ideals of $A_k[x]/\langle x^n - 1\rangle$. That is, we associate the vector $(a_0, a_1, \ldots, a_{n-1})$ with the polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^n$. These ideals can be described in the following theorem proven in [2].

Theorem 1. *[2] Let n be odd and let $p(x)$ be a divisor of $x^n - 1$ in $\mathbb{F}_2[x]$. The ideals in $A_k[x]/\langle x^n - 1\rangle$ are of the form*

$$\langle p(x) + \sum_i \Big(\sum_{A \subset \{1,2,\ldots,k\}} \alpha_A v_A r_i(x) \Big), \sum_i \Big(\sum_{B \subset \{1,2,\ldots,k\}} \alpha_B v_B s_i(x) \Big), \ldots, \sum_i \Big(\sum_{C \subset \{1,2,\ldots,k\}} \alpha_C v_C q_i(x) \Big) \rangle.$$

Notice that even at length 1 there is an abundance of cyclic codes since each ideal of A_k is a cyclic code. Moreover, there is only one unit in A_k, so there are numerous non-trivial ideals in A_k.

2 Cyclic codes

We shall give an alternate description of cyclic codes than we gave in [2] as stated above. This approach is similar to the approach for codes over $\mathbb{F}_2 + v\mathbb{F}_2$ in [5] and for codes over $\mathbb{F}_3 + v\mathbb{F}_3$ in [3].

In [2], it is shown that $\langle w_1, w_2, \ldots, w_k\rangle$, with $w_i \in \{v_i, 1 + v_i\}$ is a maximal ideal of A_k and that there are 2^k distinct maximal ideals of this form. Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_{2^k}$, be these maximal ideals. Since the ring A_k is a principal ideal ring, we know that each is generated by a single element. Denote the single element that generates $\mathfrak{m}_i$ by m_i. In fact, in Theorem 2.6 in [2], it is shown that m_i is the sum of all non-empty products of $w_1, w_2, \ldots, w_k$.

Let C be a code over A_k. We then have

$$C = (m_1)C_1 \oplus (m_2)C_2 \oplus \cdots \oplus (m_{2^k})C_{2^k}, \tag{1}$$

where C_i is a binary code. It follows that

$$C^\perp = (m_1)C_1^\perp \oplus (m_2)C_2^\perp \oplus \cdots \oplus (m_{2^k})C_{2^k}^\perp. \tag{2}$$

Notice that this gives an isomorphism between $\mathbb{F}_2^{2^k n}$ and A_k^n.

Theorem 2. *Let C be a code over A_k and let C_i be the binary codes given in Equation 1. The code C is cyclic if and only if C_i is a cyclic code for all i.*

Proof. Let σ be the cyclic shift and let $\mathbf{v} \in C$ and $\mathbf{v}_i \in C_i$ with $\mathbf{v} = m_1\mathbf{v}_1 + m_2\mathbf{v}_2 + \cdots + m_{2^k}\mathbf{v}_{2^k}$. Then we have that

$$\sigma(\mathbf{v}) = \mathbf{v} = m_1\sigma(\mathbf{v}_1) + m_2\sigma(\mathbf{v}_2) + \cdots + m_{2^k}\sigma(\mathbf{v}_{2^k}). \tag{3}$$

If each C_i is cyclic then $\sigma(\mathbf{v}_i) \in C_i$ for all i then by Equation 3 we have $\sigma(\mathbf{v}) \in C$.

If C is cyclic then $\sigma(\mathbf{v}) \in C$ and so by Equation 3 we have that $\sigma(\mathbf{v}_i) \in C_i$ for all i. □

The following is immediate from this theorem using Equation 2, since the orthogonal of a binary cyclic code is cyclic.

Corollary 1. *If a code C over A_k is cyclic then $C^\perp$ is cyclic.*

The following theorem gives an alternate description of cyclic codes as opposed to Theorem 1.

Theorem 3. *Let C be a cyclic code over A_k, then there exists a polynomial $g(x)$ in $A_k[x]$ that divides $x^n - 1$ that generates the code.*

Proof. Let $C = (m_1)C_1 \oplus (m_2)C_2 \oplus \cdots \oplus (m_{2^k})C_{2^k}$ be a cyclic code and let $g_i(x)$ be the generator of C_i in its polynomial representation. Then the code C has the form

$$\langle m_1 g_1(x), m_2 g_2(x), \ldots, m_{2^k} g_{2^k}(x)\rangle. \tag{4}$$

Consider the code $D = \langle m_1 g_1(x) + m_2 g_2(x) + \cdots + m_{2^k} g_{2^k}(x)\rangle$. It is immediate that $D \subseteq C$. Notice that $m_i m_i = m_i$ and $m_i m_j = 0$ if $i \neq j$. Then $m_i(m_1 g_1(x), m_2 g_2(x), \ldots, m_{2^k} g_{2^k}(x)) = m_i g_i(x)$ which gives that $C \subseteq D$. Hence $C = D$ and C is generated by a single element.

Next, we know that $g_i(x)$ divides $x^n - 1$. Let $r_i(x)$ be the binary polynomial such that $g_i(x)r_i(x) = x^n - 1$. Then we have $x^n - 1 = (m_1 g_1(x) + m_2 g_2(x) + \cdots + m_{2^k} g_{2^k}(x))(m_1 r_1(x) + m_2 r_2(x) + \cdots + m_{2^k} r_{2^k}(x))$ recalling that $m_i m_i = m_i$ and $m_i m_j = 0$ for $i \neq j$. Then we have

$$x^n - 1 = g(x)(m_1 r_1(x) + m_2 r_2(x) + \cdots + m_{2^k} r_{2^k}(x)).$$

□

We can combine this result with the result in Theorem 1 and we have the following.

Corollary 2. *Any ideal of the form*

$$\langle p(x) + \sum_i (\sum_{A \subset \{1,2,\ldots,k\}} \alpha_A v_A r_i(x)), \sum_i (\sum_{B \subset \{1,2,\ldots,k\}} \alpha_B v_B s_i(x)), \ldots, \sum_i (\sum_{C \subset \{1,2,\ldots,k\}} \alpha_C v_C q_i(x)) \rangle$$

where $p(x)$ is a binary polynomial that divides $x^n - 1$ can be rewritten as $\langle g(x) \rangle$ where $g(x)$ divides $x^n - 1$ in $A_k[x]$.

For a polynomial, $p(x) = a_0 + a_1 x + \ldots, a_k x^k$ define $\overline{p(x)} = a_k + a_{k-1}x + \cdots + a_0 x^k$.

Lemma 2. *If C is a cyclic code over A_k generated by $g(x)$ then $C^\perp$ is a cyclic code generated by $\overline{(x^n - 1)/g(x)}$.*

Proof. Let C be a cyclic code over A_k generated by $g(x)$ where the code is of the form $\langle m_1 g_1(x), m_2 g_2(x), \ldots, m_{2^k} g_{2^k}(x) \rangle$ as given in Equation 4. This gives that, as in Equation 1,

$$C = (m_1)C_1 \oplus (m_2)C_2 \oplus \cdots \oplus (m_{2^k})C_{2^k},$$

where C_i is a binary code. It follows that

$$C^\perp = (m_1)C_1^\perp \oplus (m_2)C_2^\perp \oplus \cdots \oplus (m_{2^k})C_{2^k}^\perp.$$

We know that if $g_i(x)$ generates the binary cyclic code C_i then there exists a polynomial $\overline{h_i(x)}$ that generates $C^\perp$, where $h_i(x) = (x^n - 1)/g_i(x)$.

The result follows by applying the isomorphism to these polynomials. □

Theorem 4. *If $C = \langle g(x) \rangle$ is a cyclic self-orthogonal code over A_k then $g(x)\overline{g(x)} = x^n - 1$.*

Proof. As before let C be a cyclic code over A_k generated by $g(x)$ where the code is of the form $\langle m_1 g_1(x), m_2 g_2(x), \ldots, m_{2^k} g_{2^k}(x) \rangle$ as given in Equation 4. Then by the isomorphism each $g_i(x)$ generates a binary self-dual code. Then by [4], we have $g_i(x)\overline{g_i(x)} = x^n - 1$. □

Corollary 3. *The image of a cyclic self-dual code of length n over A_k is a length $2^k n$ self-dual quasi-cyclic code of index 2^k.*

Proof. From [2] we have that the image of a self-dual code under the Gray map is a self-dual code and by Lemma 1 we have that the image of a cyclic code is a quasi-cyclic code of index 2^k. □

We shall give an example of the importance of self-dual codes over these rings. Let $K = \mathbb{Q}(\sqrt{-7})$ be a quadratic number field with the ring of integers $\mathcal{O} = \mathbb{Z}[\alpha]$ with $\alpha^2 + \alpha + 2 = 0$. Then we can see $A_1 = \mathcal{O}/\langle 2 \rangle$. Then using Consruction A on a Hermitian self-dual code we have that the corresponding lattice is 7-modular.

References

[1] C. Bachoc, Application of Coding Theory to the Construction of Modular Lattices, *J. Combin. Theory Ser. A* **78**, 92–119, 1997.

[2] Y. Cengellenmis, A. Dertli, and S.T. Dougherty, Cyclic and Skew Cyclic Codes over an Infinite Family of Rings with a Gray Map, in submission.

[3] Y. Cengellenmis, On the Cyclic Codes over $\mathbb{F}_3 + v\mathbb{F}_3$, *International J. of Algebra*, **4**, No. 6, 253–259, 2010.

[4] N. J. A. Sloane and J. G. Thompson, Cyclic Self-Dual Codes, *IEEE Trans. Information Theory*, IT-29, 364–366, 1983.

[5] S. Zhu, Y. Wang, M. J. Shi, Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$, ISIT, Korea, 2009.