

RESEARCH ARTICLE

More on Codes Over Finite Quotients of Polynomial Rings

EMAD KADHIM AL-LAMI¹, REZA SOBHANI¹, ALIREZA ABDOLLAHI²,
AND JAVAD BAGHERIAN²

¹Department of Applied Mathematics and Computer Science, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 8174673441, Iran

²Department of Pure Mathematics, Faculty of Mathematics and Statistics, University of Isfahan, Isfahan 8174673441, Iran

Corresponding author: Reza Sobhani (r.sobhani@sci.ui.ac.ir)

ABSTRACT Let $q = p^r$ be a prime power, $\mathbb{F}_q$ be the finite field of order q and $f(x)$ be a monic polynomial in $\mathbb{F}_q[x]$. Set $\mathbb{A} := \mathbb{F}_q[x]/\langle f(x) \rangle$. In this paper we continue the study (started by T. P. Berger and N. El Amrani) of $\mathbb{A}$ -codes of length l over $\mathbb{A}$, i.e. $\mathbb{A}$ -submodules of $\mathbb{A}^l$. We introduce two types of unique generating sets, called type I and type II basis of divisors, for an $\mathbb{A}$ -code. Using this, we present a building-up construction so that one can obtain all distinct $\mathbb{A}$ -codes of length l , with their basis of divisors. We complete the classification for the special case $l = 2$ and enumerate all the $\mathbb{A}$ -codes of length 2. As an example, we list all binary index-2 quasi-cyclic codes of lengths 16 and 32, and all ternary index-2 quasi-cyclic codes of lengths 6 and 18, which are best-known codes.

INDEX TERMS Polynomial ring, polynomial quotient ring, generator matrix, parity check matrix, basis of divisors.

I. INTRODUCTION

For a given length and dimension, designing linear codes over finite fields with higher minimum distance is one of the important coding theory problems. Researchers have tried to construct good codes with various approaches. From among these approaches, algebraic methods play an important role and among codes with algebraic structures, cyclic codes have been of much interest [1], [2], [3], [4]. Let $q = p^r$ be a prime power and $\mathbb{F}_q$ be the finite field of size q . A cyclic code of length n over $\mathbb{F}_q$ is in fact an ideal of the quotient ring $R := \mathbb{F}_q[x]/\langle x^n - 1 \rangle$. Cyclic codes have been generalized to constacyclic [5] and more generally to polycyclic codes [6, Page 241]. Polycyclic codes are in correspondence with ideals of the quotient ring $\mathbb{A} := \mathbb{F}_q[x]/\langle f(x) \rangle$, where $f(x)$ is a monic polynomial in $\mathbb{F}_q[x]$. Another generalization of cyclic codes are known as quasi-cyclic codes [7], [8], [9], [10]. Index- l quasi-cyclic codes of length nl are in correspondence with R -submodules of R^l . More recently in [11], as a generalization of quasi-cyclic codes, $\mathbb{A}$ -submodules of $\mathbb{A}^l$, called $\mathbb{A}$ -codes, have been studied. The method used in [11], is a generalization of the method used in [7] but with using simple algebra avoiding the concept of Gröbner basis.

The associate editor coordinating the review of this manuscript and approving it for publication was Yilun Shang.

More precisely, for an $\mathbb{A}$ -code of length l , a unique generating set, called basis of divisors, has been introduced there and the authors have tried to present a parity-check matrix for such a code, using the basis of divisors of the code. However, as we will see here, the parity-check matrix introduced there, only generates a subcode of the $\mathbb{A}$ -dual code and not the whole of the dual code. Also, no method presented there for finding all distinct $\mathbb{A}$ -codes of a given length l by finding all distinct basis of divisors.

In this paper, we present two types of unique generating sets for an $\mathbb{A}$ -code C of length l , called type I and type II basis of divisors. The type I basis of divisors is in fact that presented in [11] and the type II basis of divisors is new. Using both types of basis of divisors, we introduce a building-up construction for an $\mathbb{A}$ -code C which also gives us a parity-check matrix for C (the rows of this parity-check matrix are in fact the type II basis of divisors for the $\mathbb{A}$ -dual code $C^\perp$). We also complete the classification of the $\mathbb{A}$ -codes when the length l is 2. In the case where $l = 2$ and $f(x) = f_0(x)^{p^f}$ for some monic irreducible polynomial $f_0(x) \in \mathbb{F}_q[x]$, we enumerate all the $\mathbb{A}$ -codes and give a mass formula for the number of all $\mathbb{A}$ -codes.

The paper is organized as follows. In the next section, we present some basic definitions and necessary preliminaries. In Section III, Subsections III-A and III-B,

we introduce type I and type II basis of divisors for an $\mathbb{A}$ -code of length l , respectively. In Subsection III-C of this section, we present a building-up construction for $\mathbb{A}$ -codes of length l using those of length $l - 1$. In Section IV, we focus on the case $l = 2$ and give a complete classification for $\mathbb{A}$ -codes of length 2. We also give a mass formula for the number of $\mathbb{A}$ -codes of length 2, when the polynomial $f(x)$ is of the form $f_0(x)^{p^r}$, where $f_0(x)$ is a monic irreducible polynomial in $\mathbb{F}_q[x]$. As an example, we list all binary index-2 quasi-cyclic codes of lengths 16 and 32, and all ternary index-2 quasi-cyclic codes of lengths 6 and 18, which are best-known codes. Finally we close the paper with a conclusion section.

II. PRELIMINARIES

In all of this paper, we use notation p for a prime number, $q = p^r$ for a power of p , $\mathbb{F}_q$ for the finite field of size q and $\mathbb{A}$ for the polynomial quotient ring

$$\frac{\mathbb{F}_q[x]}{\langle f(x) \rangle},$$

where $f(x)$ is a monic polynomial of degree m over $\mathbb{F}_q$.

Definition 1: By a linear code of length l over $\mathbb{A}$, we mean an $\mathbb{A}$ -submodule of $\mathbb{A}^l$. We also call a linear code over $\mathbb{A}$, an $\mathbb{A}$ -code.

The ring $\mathbb{A}$ is a finite Frobenius ring and classical duality theorems for codes over finite fields, remains valid for codes over $\mathbb{A}$ [12].

Definition 2: Let C be an $\mathbb{A}$ -code of length l . The $\mathbb{A}$ -dual code $C^\perp$ is defined to be

$$C^\perp = \{v = (v_0, \dots, v_{l-1}) \in \mathbb{A}^l \mid v \cdot c = 0 \ \forall c \in C\},$$

where $v \cdot c = \sum_{i=0}^{l-1} v_i c_i$.

Proposition 1: For an $\mathbb{A}$ -code C of length l , we have

$$|C||C^\perp| = |\mathbb{A}|^l.$$

Proof: The proof follows from [11, Theorem 7.7] and the fact that $\mathbb{A}$ is a Frobenius ring. ■

III. BASIS OF DIVISORS

In this section we will introduce two types of unique generating sets called type I and type II basis of divisors. The type I basis of divisors is exactly that introduced in [11]. Type II basis of divisors is new and is introduced so that we can determine all distinct $\mathbb{A}$ -codes with their basis of divisors. In fact, using type II basis we obtain a parity-check matrix for a given $\mathbb{A}$ -code C . More precisely, we will find type II basis of the $\mathbb{A}$ -dual code $C^\perp$. Note that this is done in [11] but unfortunately, it is with an error and the matrix presented there generates a subcode of $C^\perp$ not the whole code. We will discuss this at the end of this section. Let us start the section with some definitions and notation. As we mentioned, the type I basis of divisors which we introduce here is exactly the one introduced in [11] with a bit difference.

A. TYPE I BASIS OF DIVISORS

Let C be an $\mathbb{A}$ -code of length l , i.e. an $\mathbb{A}$ -submodule of $\mathbb{A}^l$. Set $C_1 := C$ and for $2 \leq i \leq l$ define

$$C_i := \{v = (v_1(x), \dots, v_l(x)) \in C \mid v_1(x) = \dots = v_{i-1}(x) = 0\}.$$

Let π_i be the projection map on the i -th coordinate and set $T_i := \pi_i(C_i)$. Clearly, T_i is an ideal of the ring $\mathbb{F}_q[x]/\langle f(x) \rangle$. These codes are a generalization of cyclic codes and are known as polycyclic codes. Consequently, T_i is principally generated by a divisor $g_i(x)$ of $f(x)$, i.e. $T_i = \langle g_i(x) \rangle$. Also we know that $g_i(x)$ is the monic polynomial of minimal degree in T_i . We call T_i , the i -th type I torsion code of C . When $T_i = \{0\}$ we set $g_i(x) := f(x)$. Set

$$\bar{Z} := \{1 \leq i \leq l \mid g_i(x) \neq f(x)\},$$

and assume that $\bar{Z} = \{t_1, \dots, t_k\}$, where

$$1 \leq t_1 \leq \dots \leq t_k \leq l.$$

The integer k depends only on C which we call it the type I rank of C and denote it by $r_1(C)$. Also we set

$$Z := \{1, 2, \dots, l\} \setminus \bar{Z}.$$

We have the following lemma.

Lemma 1: Let C be an $\mathbb{A}$ -code of length l . Then there exist a set

$$W = \{w^{(i)} \mid i \in \bar{Z}\},$$

where

$$w^{(i)} = (\overbrace{0, \dots, 0}^{i-1 \text{ times}}, g_i(x), a_{i,1}(x), \dots, a_{i,l-i}(x)) \in C_i$$

is such that $T_i = \langle g_i(x) \rangle$, $g_i(x)$ is a monic divisor of $f(x)$ and for each $1 \leq j \leq l - i$ we have $\deg(a_{i,j}(x)) < \deg(g_{i+j}(x))$.

Proof: For each $i \in \bar{Z}$, by definition of C_i , there exists an element

$$v^{(i)} = (\overbrace{0, \dots, 0}^{i-1 \text{ times}}, g_i(x), b_{i,1}(x), \dots, b_{i,l-i}(x))$$

in C_i . Now set $V := \{v^{(i)} \mid i \in \bar{Z}\}$. For each $i \in \bar{Z}$ and $1 \leq j \leq l - i$, by division algorithm, there exist $q_{i,j}(x)$ and $r_{i,j}(x)$ such that

$$\deg(r_{i,j}(x)) < \deg(g_{i+j}(x))$$

and we have $b_{i,j}(x) = q_{i,j}(x)g_{i+j}(x) + r_{i,j}(x)$. Note that for those i 's for which $i + j \in Z$, i.e. $g_{i+j}(x) = f(x)$, we have $q_{i,j}(x) = 0$. For $i \in \bar{Z}$ set

$$w^{(i)} := v^{(i)} - \sum_{j=1}^{l-i} q_{i,j}(x)v^{(i+j)}.$$

The set $W = \{w^{(i)} \mid i \in \bar{Z}\}$ is now the desired set. ■

Theorem 1: The set W generates C and is unique.

Proof: Let $\bar{Z} = \{t_1, \dots, t_k\}$ and $v = (v_1(x), \dots, v_l(x))$ be an arbitrary element of C . Set $v^{(1)} := v$. According to the definition of the set $\bar{Z}$ we have

$$v_1(x) = \dots = v_{t_1-1}(x) = 0.$$

Since $v_{t_1}(x) \in T_{t_1}$, there exist $q_{t_1}(x)$ such that

$$v_{t_1}(x) = q_{t_1}(x)g_{t_1}(x).$$

Now set

$$v^{(2)} := v^{(1)} - q_{t_1}(x)w^{(t_1)}(x) = v - q_{t_1}(x)w^{(t_1)}(x).$$

Since $v_{t_1}^{(2)}(x) = 0$, again, according to the definition of the set $\bar{Z}$ we have

$$v_{t_1+1}^{(2)}(x) = \dots = v_{t_2-1}^{(2)}(x) = 0.$$

Since $v_{t_2}^{(2)}(x) \in C_{t_2}$, there exist $q_{t_2}(x)$ such that

$$v_{t_2}^{(2)}(x) = q_{t_2}(x)g_{t_2}(x).$$

Now set

$$\begin{aligned} v^{(3)} &:= v^{(2)} - q_{t_2}(x)w^{(t_2)}(x) \\ &= v - q_{t_1}(x)w^{(t_1)}(x) - q_{t_2}(x)w^{(t_2)}(x). \end{aligned}$$

Continuing this process we get that

$$v^{(k+1)} := v - \sum_{i=1}^k q_{t_i}(x)w^{(t_i)} = 0,$$

which shows that W generates C . For uniqueness, to contrary assume that there exists another set

$$\mathcal{W} = \{v^{(t_1)}, \dots, v^{(t_k)}\},$$

that generates C and

$$v^{(t_i)} = (\overbrace{0, \dots, 0}^{t_i-1 \text{ times}}, g_{t_i}(x), d_{t_i,1}(x), \dots, d_{t_i,l-t_i}(x)) \in C_{t_i},$$

$\deg(d_{t_i,j}(x)) < \deg(g_{t_i+j}(x))$. Set $\gamma^{(t_i)} := w^{(t_i)} - v^{(t_i)}$. We have

$$\gamma^{(t_i)} = (\overbrace{0, \dots, 0}^{t_i \text{ times}}, a_{t_i,1}(x) - d_{t_i,1}(x), \dots, a_{t_i,l-t_i}(x) - d_{t_i,l-t_i}(x)),$$

which is a vector in C_{t_i+1} . Now for each $1 \leq j \leq l - t_i$ we have $\deg(a_{t_i,j}(x) - d_{t_i,j}(x)) < \deg(g_{t_i+j}(x))$ and hence we have $a_{t_i,j}(x) - d_{t_i,j}(x) = 0$. The proof is now completed. ■

We call this basis, Type I basis of divisors. If we put the elements of this basis in the rows of a matrix G , then we call G , the type I standard generator matrix of C . The proof of the following proposition is similar to that for Proposition 1 of [11] and hence we omit the proof.

Proposition 2: Let W be the Type I basis of divisors for an $\mathbb{A}$ -code C and set $r_i := \deg(g_{t_i}(x))$. Then we have

$$|C| = q^{\sum_{i=1}^k (m-r_i)}.$$

□

Example 1: Let $\mathbb{F}_q = \mathbb{F}_2, f(x) = x^3 + 1, l = 2$ and C be the $\mathbb{A}$ -code

$$\{(0, 0), (x+1, x+1), (0, x^2+x+1), (x+1, x^2), (x^2+1, x^2+1), (x^2+1, x), (x^2+x, x^2+x), (x^2+x, 1)\}.$$

We have,

$$C_1 = C$$

$$C_2 = \{(0, 0), (0, x^2+x+1)\}$$

$$T_1 = \langle x+1 \rangle$$

$$T_2 = \langle x^2+x+1 \rangle$$

$$g_1(x) = x+1$$

$$g_2(x) = x^2+x+1$$

$$\bar{Z} = \{1, 2\}$$

$$t_1 = 1 \quad t_2 = 2$$

$$k = 2.$$

The type I basis of divisors of C is

$$\{(x+1, x+1), (0, x^2+x+1)\},$$

and the type I generator matrix for C is

$$G = \begin{pmatrix} x+1 & x+1 \\ 0 & x^2+x+1 \end{pmatrix}.$$

Also we have $|C| = 2^{(3-1)+(3-2)} = 8$.

Now, an important question is that how we can determine all $\mathbb{A}$ -codes of a given length l with the help of Theorem 1? Note that if we choose integers $1 \leq t_1 \leq \dots \leq t_k \leq l$, divisors $g_{t_1}(x), \dots, g_{t_k}(x)$ of $f(x)$ and polynomials $a_{t_i,j}(x)$ in $\mathbb{F}_q[x]$ with $\deg(a_{t_i,j}(x)) < \deg(g_{t_i+j}(x))$, it does not need to obtain different codes! See the following example.

Example 2: Let $\mathbb{F}_q = \mathbb{F}_2, f(x) = x^3 + 1, l = 2, t_1 = 1, t_2 = 2, C$ be the $\mathbb{A}$ -code generated by $\{(x+1, 1), (0, x+1)\}$ and D be the $\mathbb{A}$ -code generated by $\{(x+1, 0), (0, 1)\}$. Both sets are in the form introduced in Theorem 1 but the codes are not distinct. To see this note that we have

$$\begin{aligned} (x^2+x+1)(x+1, 1) &= (0, x^2+x+1) \in C \implies \\ x(0, x^2) &= (0, 1) \in C \implies \\ (x+1, 1) + (0, 1) &= (x+1, 0) \in C. \end{aligned}$$

Hence $D \subseteq C$. Clearly $C \subseteq D$ and consequently we have $C = D$.

In what follows we introduce another type of basis of divisors for an $\mathbb{A}$ -code, called type II basis of divisors, so that we can obtain a parity-check matrix for the code and also extra conditions for the elements in a type I basis of divisors to obtain all distinct $\mathbb{A}$ -codes. It is of worth mentioning that a parity-check matrix for an $\mathbb{A}$ -code with a given basis of divisors, has been presented in Theorem 3 of [11], but unfortunately, it is with an error. In fact the code generated by the matrix H introduced in that theorem, is a subcode of the $\mathbb{A}$ -dual code $C^\perp$ but not the whole code. To see this, we give the following counterexample which shows that the theorem is not true even when $f(x)$ is a simple-root polynomial over $\mathbb{F}_q$.

Example 3: Assume that $\mathbb{F}_q = \mathbb{F}_2$, $l = 2$ and $f(x) = x^3 - 1$. Let C be an $\mathbb{A}$ -code with generator matrix

$$G = \begin{pmatrix} x+1 & 0 \\ 0 & x+1 \end{pmatrix}$$

Easily one can see that this matrix is the type I standard generator matrix of C . Now, with notation as in [11], C' is the binary cyclic code of length 3 generated by $(x+1)$ and hence $H' = [x^2 + x + 1]$. According to Theorem 3 of [11], we have

$$H = \begin{pmatrix} x^2 + x + 1 & 0 \\ 0 & 0 \end{pmatrix}$$

is a parity-check matrix for C . It is clear that H generates a subcode of the $\mathbb{A}$ -dual code $C^\perp$ but not the whole code. For example $(0, x^2 + x + 1)$ is in $C^\perp$ but not in the code generated by H .

B. TYPE II BASIS OF DIVISORS

Again, let C be an $\mathbb{A}$ -code of length l , i.e. an $\mathbb{A}$ -submodule of $\mathbb{A}^l$. Set $C'_i := C$ and for $1 \leq i \leq l-1$ define

$$C'_i := \{v = (v_1(x), \dots, v_l(x)) \in C \mid v_{i+1}(x) = \dots = v_l(x) = 0\}.$$

Set $T'_i := \pi_i(C'_i)$. Assume that, T'_i is generated by a divisor $g'_i(x)$ of $f(x)$, i.e. $T'_i = \langle g'_i(x) \rangle$. Recall that $g'_i(x)$ is the monic polynomial of minimal degree in T'_i . Set

$$\overline{Z'} := \{1 \leq i \leq l \mid g'_i(x) \neq f(x)\},$$

and assume that $\overline{Z'} = \{t'_1, \dots, t'_{k'}\}$, where

$$1 \leq t'_1 \leq \dots \leq t'_{k'} \leq l.$$

The integer k' depends only on C which we call it the type II rank of C and denote it by $r_2(C)$. Also we set

$$Z' := \{1, 2, \dots, l\} \setminus \overline{Z'}.$$

We have the following lemma.

Lemma 2: Let C be an $\mathbb{A}$ -code of length l . Then there exist a set $W' = \{w^{(i)} \mid i \in \overline{Z'}\}$, where

$$w^{(i)} = (a'_{i,1}(x), \dots, a'_{i,i-1}(x), g'_i(x), \overbrace{0, \dots, 0}^{l-i \text{ times}}) \in C'_i$$

is such that $T'_i = \langle g'_i(x) \rangle$, $g'_i(x)$ is a monic divisor of $f(x)$ and for each $1 \leq j \leq i-1$ we have $\deg(a'_{i,j}(x)) < \deg(g'_i(x))$.

Proof: For each $i \in \overline{Z'}$, by definition of C'_i , there exists an element

$$v^{(i)} = (b'_{i,1}(x), \dots, b'_{i,i-1}(x), g'_i(x), \overbrace{0, \dots, 0}^{l-i \text{ times}})$$

in C'_i . Set $V' := \{v^{(i)} \mid i \in \overline{Z'}\}$. Now, for each $i \in \overline{Z'}$ and for each $1 \leq j \leq i-1$, by division algorithm, there exist $q'_{i,j}(x)$ and $r'_{i,j}(x)$ such that $\deg(r'_{i,j}(x)) < \deg(g'_i(x))$ and we have $b'_{i,j}(x) = q'_{i,j}(x)g'_i(x) + r'_{i,j}(x)$. Set

$$w^{(i)} := v^{(i)} - \sum_{j=1}^{i-1} q'_{i,j}(x)v^{(j)}.$$

Now, $W' = \{w^{(i)} \mid i \in \overline{Z'}\}$ is the desired set. ■

The proof of the following theorem is similar to that for Theorem 1 and hence we omit the proof.

Theorem 2: The set W' generates C and is unique. □

We call this basis, Type II basis of divisors. Also, if we put the elements of W' in the rows of a matrix G' then we call G' , the standard type II generator matrix of C . The standard type I (resp. type II) generator matrix for the $\mathbb{A}$ -dual code $C^\perp$ is called the standard type I (resp. type II) parity-check matrix for C . We also have the following proposition, similar to Proposition 2.

Proposition 3: Let W' be a Type II basis of divisors for an $\mathbb{A}$ -code C and for $1 \leq i \leq k'$, set $r'_i := \deg(g'_i(x))$. Then we have

$$|C| = q^{\sum_{i=1}^{k'} (m-r'_i)}.$$

□

Example 4: Let C be the $\mathbb{A}$ -code of Example 1. We have,

$$\begin{aligned} C'_1 &= \{(0, 0)\} \\ C'_2 &= C \\ T'_1 &= \langle 0 \rangle \\ T'_2 &= \langle 1 \rangle \\ g'_1(x) &= x^3 + 1 \\ g'_2(x) &= 1 \\ \overline{Z'} &= \{2\} \\ t'_1 &= 2 \\ k' &= 1. \end{aligned}$$

The type II basis of divisors of C is

$$\{(x^2 + x, 1)\},$$

and the type II generator matrix for C is

$$G' = \begin{pmatrix} x^2 + x & 1 \end{pmatrix}.$$

Also we have $|C| = 2^{(3-0)} = 8$.

C. A BUILDING UP CONSTRUCTION OF TYPE I BASIS OF DIVISORS

We start this section with the following definitions.

Definition 3: For a vector v in $\mathbb{A}^l$, we define v^* to be the vector v punctured at the first position.

Definition 4: Let C be an $\mathbb{A}$ -code of length l . Let $C(i, 0)$ be those vectors in C such that the i -th coordinate of them are 0. We define the code

$$C^* := \{c^* \mid c \in C(1, 0)\}.$$

In the rest of this section we provide a building up construction for the type I generator matrix of all $\mathbb{A}$ -codes. To do this, we start with an $\mathbb{A}$ -code $\tilde{C}$ of length $l-1$, the standard type I generator matrix $\tilde{G}$ of $\tilde{C}$, and the standard type II parity-check matrix $\tilde{H}$ of $\tilde{C}$. Then we construct the type I generator matrix of all $\mathbb{A}$ -codes C of length l for which $C^* = \tilde{C}$. In this way,

we also construct the standard type II parity-check matrix for such a code C .

Theorem 3: Let $\tilde{C}$ be an $\mathbb{A}$ -code of length $l - 1$ with standard type I generator matrix $\tilde{G}$ and standard type II parity-check matrix $\tilde{H}$. Let $\tilde{k}'$ be the type II rank of the $\mathbb{A}$ -dual code $\tilde{C}^\perp$ (the number of rows of $\tilde{H}$). Assume that $g(x)$ is a monic proper divisor of $f(x)$ and for $1 \leq j \leq l - 1$, $a_j(x)$ is a polynomial with $\deg(a_j(x)) < \deg(\tilde{g}_j(x))$, where $\tilde{g}_j(x)$ is the generator of the j -th type I torsion code of $\tilde{C}$. For $1 \leq i \leq \tilde{k}'$ set

$$\alpha_i(x) := \left(\sum_{j=1}^{l-1} a_j(x) \tilde{H}_{i,j} \right),$$

where $\tilde{H}_{i,j}$ is the (i, j) -th entry of the matrix $\tilde{H}$. Then

$$G = \begin{pmatrix} g(x) & a_1(x) & \cdots & a_{l-1}(x) \\ 0 & \tilde{G} & & \end{pmatrix}$$

is the standard type I generator matrix for an $\mathbb{A}$ -code C of length l , if and only if, for $1 \leq i \leq \tilde{k}'$ we have $g(x) \mid \alpha_i(x)$.

Proof: First assume that G is the standard type I generator matrix of an $\mathbb{A}$ -code C of length l . Now, if H is the standard type II parity-check matrix of C , then, according to the form of type II basis of divisors, H must be of the form

$$H = \begin{pmatrix} b(x) & 0 & \cdots & 0 \\ \delta_1(x) & & & \\ \vdots & & M & \\ \delta_k(x) & & & \end{pmatrix}.$$

Now since the first row of G and H are orthogonal, we must have $b(x) = f(x)/g(x)$. Also, since the matrix M generates $\tilde{C}^\perp$, we must have $M = \tilde{H}$ and $k = \tilde{k}'$. Moreover, since the first row of G is orthogonal to the $j + 1$ -th row of H , for $1 \leq j \leq \tilde{k}'$, we must have

$$g(x)\delta_j(x) + \alpha_j(x) = 0$$

which implies that $g(x) \mid \alpha_j(x)$ as desired. Now, conversely, assume that $g(x) \mid \alpha_j(x)$, for $1 \leq j \leq \tilde{k}'$. Assume that C is the $\mathbb{A}$ -code generated by G and set

$$H := \begin{pmatrix} f(x)/g(x) & 0 & \cdots & 0 \\ -\alpha_1(x)/g(x) & & & \\ \vdots & & \tilde{H} & \\ -\alpha_{\tilde{k}'}(x)/g(x) & & & \end{pmatrix}.$$

Let D be the $\mathbb{A}$ -code generated by H . Since $GH^t = 0$ we conclude that $D \subseteq C^\perp$. On the other hand, easily can be seen that $|C| \geq q^{m-\deg(g(x))}|\tilde{C}|$ and $|D| \geq q^{\deg(g(x))}|\tilde{C}^\perp|$. Hence, since $\mathbb{A}$ is a Frobenius ring, we have

$$\begin{aligned} |\mathbb{A}|^l &= |C||C^\perp| \\ &\geq |C||D| \\ &\geq q^m|\tilde{C}||\tilde{C}^\perp| \\ &= q^m|\mathbb{A}|^{l-1} \\ &= |\mathbb{A}|^l. \end{aligned}$$

Consequently, $D = C^\perp$, H is the standard type II parity-check matrix and G is the standard type I generator matrix for C , as desired. The proof is now completed. ■

IV. THE CASE $l = 2$

In this section we will focus on the $\mathbb{A}$ -codes of lengths 2 and present a complete classification for the codes of this length. Let $g_1(x)$ and $g_2(x)$ be monic divisors of $f(x)$. We denote by $\mathcal{C}(g_1(x), g_2(x))$, the set of $\mathbb{A}$ -codes C of length 2 for which $T_1(C) = \langle g_1(x) \rangle$ and $T_2(C) = \langle g_2(x) \rangle$. Also, let us denote by $A_{g_1, g_2}(x)$, the polynomial

$$A_{g_1, g_2}(x) := \gcd(g_2(x), \frac{f(x)}{g_1(x)}),$$

and d_{g_1, g_2} be the integer $d_{g_1, g_2} := \deg(A_{g_1, g_2}(x))$. We have the following theorem.

Theorem 4: For $g_1(x)$ and $g_2(x)$, monic divisors of $f(x)$, we have

$$|\mathcal{C}(g_1(x), g_2(x))| = q^{d_{g_1, g_2}}.$$

Proof: Choose a code C in $\mathcal{C}(g_1(x), g_2(x))$. First we assume that $g_1(x)$ is a proper divisor of $f(x)$. Set $\tilde{C} := C^*$. Clearly $\tilde{C}$ has $\tilde{G} = [g_2(x)]$ as its standard type I generator matrix and $\tilde{H} = [h_2(x)]$ as its type II parity-check matrix, where $h_2(x) := f(x)/g_2(x)$. Now, by Theorem 3,

$$G = \begin{bmatrix} g_1(x) & a(x) \\ 0 & g_2(x) \end{bmatrix}$$

is the standard type I generator matrix of C , if and only if

$$g_1(x) \mid a(x)h_2(x). \quad (1)$$

But easily can be verified that equation 1 is equivalent with

$$g_2(x) \mid a(x)h_1(x), \quad (2)$$

where $h_1(x) := f(x)/g_1(x)$. On the other have equation 2 holds if and only if

$$\frac{g_2(x)}{A_{g_1, g_2}(x)} \mid a(x).$$

Therefore we have

$$a(x) = \frac{g_2(x)}{A_{g_1, g_2}(x)} K(x),$$

where $K(x) \in \mathbb{F}_q[x]$ is such that

$$\deg(K(x)) < \deg(A_{g_1, g_2}(x)).$$

Now we conclude that $|\mathcal{C}(g_1(x), g_2(x))| = q^{d_{g_1, g_2}}$ as claimed. If $g_1(x) = f(x)$ then the standard type I generator matrix of C is $[0 \ g_2(x)]$ and hence $|\mathcal{C}(g_1(x), g_2(x))| = 1$ as desired ($d_{g_1, g_2} = 0$ in this case). ■

Theorem 5: Let $f(x) = f_0(x)^{p^t}$ such that $\text{char}(\mathbb{F}_q) = p$ and $f_0(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$ with $\deg(f_0(x)) = m_0$. Set $\alpha := q^{m_0}$. Then the total number of $\mathbb{A}$ -codes of length 2 is given by

$$\frac{(\alpha + 1)(\alpha^{p^t+1} - 1) - 2(\alpha - 1)(p^t + 1)}{(\alpha - 1)^2}.$$

Proof: In this case any divisor of $f(x)$ is of the form $f_0(x)^i$ for some $0 \leq i \leq p^t$. Let $M = (m_{ij})$ be the $(p^t + 1) \times (p^t + 1)$ matrix whose (i, j) -th entry is

$$m_{ij} = |\mathcal{C}(f_0(x)^i, f_0(x)^j)|,$$

for $0 \leq i, j \leq p^t$. According to Theorem 4, we have $m_{ij} = \alpha^{\min\{j, p^t - i\}}$. Hence M is of the form

$$M = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{p^t-1} & \alpha^{p^t} \\ \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{p^t-1} & \alpha^{p^t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha^0 & \alpha^1 & \alpha^1 & \cdots & \alpha^1 & \alpha^1 \\ \alpha^0 & \alpha^0 & \alpha^0 & \cdots & \alpha^0 & \alpha^0 \end{bmatrix}.$$

Adding entries of M on its all diagonals, the total number of codes is

$$\begin{aligned} & \left(\sum_{i=0}^{p^t} \alpha^i \right) + 2 \sum_{w=0}^{p^t-1} \left[\sum_{z=0}^w \alpha^z \right] \\ &= \frac{\alpha^{p^t+1} - 1}{\alpha - 1} + \left(2 \sum_{w=0}^{p^t-1} \alpha^{w+1} \right) - \frac{2p^t}{\alpha - 1} \\ &= \frac{\alpha^{p^t+1} - 1}{\alpha - 1} + \frac{2}{\alpha - 1} \left(\frac{\alpha^{p^t+1} - 1}{\alpha - 1} - 1 \right) - \frac{2p^t}{\alpha - 1} \\ &= \frac{(\alpha + 1)(\alpha^{p^t+1} - 1) - 2(\alpha - 1)(p^t + 1)}{(\alpha - 1)^2}, \end{aligned}$$

as desired. ■

Remark 1: Here we mention that, when $f(x) = x^n - 1$, the set of $\mathbb{A}$ -codes of length l , coincides with the set of so-called index- l quasi-cyclic codes of length ln over $\mathbb{F}_q$. Also, note that when $q = p^r$ and $n = p^t$, we have

$$f(x) = x^n - 1 = x^{p^t} - 1 = (x - 1)^{p^t}.$$

Hence we may consider $f_0(x) = x - 1$ and this case is an special case of the later case where $f(x) = f_0(x)^{p^t}$ and $f_0(x)$ is an irreducible polynomial over $\mathbb{F}_q$.

Example 5: In this example, we list all binary index-2 quasi-cyclic codes of lengths 16 and 32, and all ternary index-2 quasi-cyclic codes of lengths 6 and 18, which are best-known codes in the sense that they have minimum distances equal to that of the best-known code with the same length and dimension, in [13]. At each length, any code has an standard type I generator matrix of the form

$$G = \begin{bmatrix} (x - 1)^a & g(x) \\ 0 & (x - 1)^b \end{bmatrix}$$

and hence we can represent the code with a , b and $g(x)$ only. Recall that we denote a code of length n , dimension k and minimum distance d by $[n, k, d]$ -code.

Binary length-16:

[16,1,16]-code: $a = 7, b = 8, g(x) = (1 + x)^7$
 [16,3,8]-code: $a = 5, b = 8, g(x) = 1 + x + x^4 + x^5$
 [16,4,8]-code: $a = 4, b = 8, g(x) = 1 + x + x^2 + x^4 + x^5 + x^6$
 [16,5,8]-code: $a = 3, b = 8, g(x) = 1 + x^2 + x^3 + x^5$

[16,6,6]-code: $a = 2, b = 8, g(x) = 1 + x + x^2 + x^3$
 [16,7,6]-code: $a = 1, b = 8, g(x) = 1 + x + x^2 + x^3 + x^4$
 [16,8,5]-code: $a = 0, b = 8, g(x) = 1 + x^2 + x^3 + x^4$
 [16,9,4]-code: $a = 0, b = 7, g(x) = 1 + x + x^2$
 [16,10,4]-code: $a = 0, b = 6, g(x) = 1 + x + x^2$
 [16,11,4]-code: $a = 0, b = 5, g(x) = 1 + x + x^2$
 [16,12,2]-code: $a = 0, b = 4, g(x) = 1$
 [16,13,2]-code: $a = 0, b = 3, g(x) = 1$
 [16,14,2]-code: $a = 0, b = 2, g(x) = 1$
 [16,15,2]-code: $a = 0, b = 1, g(x) = 1$
 [16,16,1]-code: $a = 0, b = 0, g(x) = 0$

Binary length-32:

[32,1,32]-code: $a = 15, b = 16, g(x) = (1 + x)^{15}$
 [32,4,16]-code: $a = 12, b = 16, g(x) = 1 + x + x^2 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{10} + x^{12} + x^{14}$
 [32,5,16]-code: $a = 11, b = 16, g(x) = 1 + x^2 + x^3 + x^5 + x^8 + x^{10} + x^{11} + x^{13}$
 [32,14,8]-code: $a = 2, b = 16, g(x) = 1 + x + x^2 + x^4 + x^5 + x^6$
 [32,15,8]-code: $a = 1, b = 16, g(x) = 1 + x + x^2 + x^3 + x^5 + x^7$
 [32,16,8]-code: $a = 0, b = 16, g(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$
 [32,18,6]-code: $a = 0, b = 14, g(x) = 1 + x + x^2 + x^4 + x^5$
 [32,19,6]-code: $a = 0, b = 13, g(x) = 1 + x^2 + x^3 + x^4 + x^5$
 [32,23,4]-code: $a = 0, b = 9, g(x) = 1 + x + x^2$
 [32,27,2]-code: $a = 0, b = 5, g(x) = 1$
 [32,28,2]-code: $a = 0, b = 4, g(x) = 1$
 [32,29,2]-code: $a = 0, b = 3, g(x) = 1$
 [32,30,2]-code: $a = 0, b = 2, g(x) = 1$
 [32,31,2]-code: $a = 0, b = 1, g(x) = 1$
 [32,32,1]-code: $a = 0, b = 0, g(x) = 0$

Ternary length-6:

[6,1,6]-code: $a = 2, b = 3, g(x) = 1 + x + x^2$
 [6,2,4]-code: $a = 1, b = 3, g(x) = 2 + x$
 [6,3,3]-code: $a = 0, b = 3, g(x) = 2 + x$
 [6,4,2]-code: $a = 0, b = 2, g(x) = 1$
 [6,5,2]-code: $a = 0, b = 1, g(x) = 1$
 [6,6,1]-code: $a = 0, b = 0, g(x) = 0$

Ternary length-18:

[18,1,18]-code: $a = 8, b = 9, g(x) = (x^9 - 1)/(x - 1)$
 [18,7,8]-code: $a = 2, b = 9, g(x) = 1 + 2x + x^2 + x^3 + x^5$
 [18,8,7]-code: $a = 1, b = 9, g(x) = 1 + x^2 + 2x^3 + x^4 + x^5$
 [18,9,6]-code: $a = 0, b = 9, g(x) = 1 + x + x^2 + 2x^3 + x^4$
 [18,10,6]-code: $a = 0, b = 8, g(x) = 1 + x + 2x^2 + 2x^3 + x^4$
 [18,11,5]-code: $a = 0, b = 7, g(x) = 1 + x + 2x^2 + x^3$
 [18,14,3]-code: $a = 0, b = 4, g(x) = 1 + x$
 [18,15,2]-code: $a = 0, b = 3, g(x) = 1$
 [18,16,2]-code: $a = 0, b = 2, g(x) = 1$
 [18,17,2]-code: $a = 0, b = 1, g(x) = 1$
 [18,18,1]-code: $a = 0, b = 0, g(x) = 0$

V. CONCLUSION

We have completed the study of $\mathbb{A}$ -codes, i.e. $\mathbb{A}$ -submodules of $\mathbb{A}^l$. We introduced two types of unique generators, called type I and type II basis of divisors for such codes. A building-up construction was presented so that one can obtain all distinct $\mathbb{A}$ -codes of a given length l . In an special case

where $f(x) = f_0(x)^{p^l}$, the number of distinct $\mathbb{A}$ -codes of length 2 was enumerated.

It is natural to ask about the case $l \geq 3$. However, when $l \geq 3$, analyzing equations $g(x) \mid \alpha_i(x)$, given in Theorem 3, becomes more complicated and counting the number of $\mathbb{A}$ -codes is not as easy as that for the case $l = 2$ even if we have $f(x) = f_0(x)^{p^l}$. One may obtain partial results but a full description and enumeration is left as an open problem.

REFERENCES

- [1] E. Prange, "Cyclic error-correcting codes in two symbols," in *Air Force Cambridge Research Center*, USA, 1957.
- [2] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," in *Air Force Cambridge Research Center*, USA.
- [3] E. Prange, "The use of coset equivalence in the analysis and decoding of group codes," in *Air Force Cambridge Research Center*, USA.
- [4] E. Prange, *An Algorithm for Factoring x^{n-1} Over a Finite Field*, document TN-59-175, 1959.
- [5] B. Chen, Y. Fan, L. Lin, and H. Liu, "Constacyclic codes over finite fields," *Finite Fields Their Appl.*, vol. 18, no. 6, pp. 1217–1231, Nov. 2012.
- [6] T.-D. Chiueh, P.-Y. Tsai, and I.-W. Lai, "Error-correcting codes," in *Baseband Receiver Design for Wireless MIMO-OFDM Communications*. Cambridge, MA, USA: MIT Press, 2012, pp. 69–94.
- [7] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discrete Appl. Math.*, vol. 111, pp. 157–175, May 2001.
- [8] S. Ling and P. Sole, "On the algebraic structure of quasi-cyclic codes. I. finite fields," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2751–2760, Nov. 2001.
- [9] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes II: Chain rings," *Designs, Codes Cryptogr.*, vol. 30, pp. 113–130, Apr. 2014.
- [10] S. Ling and P. Sole, "On the algebraic structure of quasi-cyclic codes III: Generator theory," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2692–2700, Jul. 2005.
- [11] T. P. Berger and N. E. Amrani, "Codes over finite quotients of polynomial rings," *Finite Fields Their Appl.*, vol. 25, pp. 165–181, Oct. 2013.
- [12] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *Amer. J. Math.*, vol. 121, no. 3, pp. 555–575, Jun. 1999.
- [13] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Oct. 25, 2024. [Online]. Available: <http://www.codetables.de>
- [14] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, Sep. 1997.



EMAD KADHIM AL-LAMI received the master's degree from the College of Computer Science and Mathematics, University of Kufa, in 2013. He is currently pursuing the Ph.D. degree with the University of Isfahan, Iran. He is also with the Open Education College/Math Department, Maysan Center, Iraq.



REZA SOBHANI received the B.Sc. degree from Isfahan University of Technology, Iran, in 2003, the M.Sc. degree from the Sharif University of Technology, Iran, in 2005, and the Ph.D. degree in applied mathematics from Isfahan University of Technology, in 2010. Since 2010, he has been with the Department of Mathematics, University of Isfahan, as a Faculty Member. Since 2009, he has been an Associated Professor of mathematics with the University of Isfahan. He is the author of more than 30 articles. His research interests include algebraic coding theory, combinatorics, and graph theory with applications in communication theory.

ALIREZA ABDOLLAHI received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from the University of Isfahan, Iran, in 1996, 1997, and 2000, respectively, and the second Ph.D. degree in mathematics from the Université de Provence, CMI, France, in 2001. Since 2001, he has been with the Department of Mathematics, University of Isfahan, as a Faculty Member. Since 2009, he has been a Professor of mathematics with the University of Isfahan. He is the author of more than 120 articles. His research interests include group theory and combinatorics. He was a recipient of the Alkharazmi Young Prize, in 1999; and the Sheikh Bahaei Prize, in 1999. He also received "Institute for Studies in Theoretical Physics and Mathematics (IPM)" Young Mathematician Prize of 2005. He was the Head of Distinguished Center of Excellence in Basic Sciences selected by the Ministry of Science and Education of Iran, in 2010. He is the Editor-in-Chief of *Journal of the Iranian Mathematical Society*, the founder and the Editor-in-Chief of *International Journal of Group Theory and Transactions on Combinatorics*.

JAVAD BAGHERIAN received the B.S. degree in applied mathematics from the University of Kharazmi, Tehran, Iran, in 2002, and the M.S. degree in applied mathematics and the Ph.D. degree in pure mathematics from the Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, in 2004 and 2008, respectively. From 2008 to 2016, he was an Assistant Professor with the Mathematics and Computer Science Department, University of Isfahan, Iran. Since 2016, he has been an Associate Professor with the Mathematics and Computer Science Department, University of Isfahan. He has published more than 30 papers. His research interests include scheme theory, graph theory, and permutation codes.

...