Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

A note over constructions of cyclic codes over certain semigroups

Antonio Aparecido de Andrade
Department of Mathematics, São Paulo State University
15054-000, São José do Rio Preto, SP
E-mail: andrade@ibilce.unesp.br

Tariq Shah
Department of Mathematics, Quaid-i-Azam University
Islamabad, Pakistan
E-mail: stariqshah@gmail.com

Abstract: *Let B be any finite commutative ring with identity. In this case, $\cdots \subset B[X;\frac{1}{p^k}\mathbb{Z}_0]\cdots \subset B[X;\frac{1}{p^2}\mathbb{Z}_0] \subset B[X;\frac{1}{p}\mathbb{Z}_0]$, where p is a prime number and $k \geq 1$, is the descending chain of commutative semigroup rings. All these semigroup rings are containing the polynomial ring $B[X;\mathbb{Z}_0]$. In this paper, we introduced a construction technique of cyclic codes through the semigroup ring $B[X;\frac{1}{p^k}\mathbb{Z}_0]$ instead of a polynomial ring.*

Key-words: *Semigroup ring, monoid ring, cyclic codes*

1 Introduction

In algebra the finite commutative rings are of most interest as they have many applications. The ideals in these structures are playing very essential role for their applications and it is often important to know when the ideals in a ring are singly generated. The most useful class of rings in this perspective is the polynomial rings in one indeterminate with coefficients from a finite field, that is an Euclidean domain. The coding for error control has vital role in the design of modern communication systems and high speed digital computers. Most of the classical error-correcting codes are ideals in finite commutative rings, especially in quotient rings of Euclidean domains of polynomials and group rings, that is cyclic codes are principal ideals in the quotient ring $\mathbb{F}_q[X]/(X^n-1)$, where q is a power of a prime.

This paper is organized as follows. In Section 2, we present the exposition of the problem. In Section 3, we give some basic results of semigroups and semigroup rings necessary for the construction of the linear codes. In Section 4, we present the construction of cyclic codes through the semigroup ring $B[X;\frac{1}{p^k}\mathbb{Z}_0]$, where p is a prime number and $k \geq 1$. Finally, in Section 5, the concluding remarks are drawn.

2 Exposition of the problem

Cazaran and Kelarev [1] established necessary and sufficient conditions for an ideal to be the principal; further they described all finite quotient rings $\mathbb{Z}_m[X_1,\cdots,X_n]/I$, where I is an ideal generated by an univariate polynomial, which are commutative principal ideal rings. In another

DOI: 10.5540/03.2015.003.01.0223

paper, Cazaran and Kelarev [2] characterize the certain finite commutative rings as a principal ideal rings. Though, the extension of a BCH code C embedded in a semigroup ring $F[S]$, where S is a finite semigroup, was considered in 2006 by Cazaran et. all [3], where an algorithm was established for computing the weights of extensions for these codes embedded in semigroup rings as ideals. The information relating various ring constructions and about polynomial codes are given by Kelarev [4], where in Sections 9.1 and 9.2 are devoted for error-correcting codes in ring constructions very closely related to semigroup rings. Specially Section 9.1 is dealing error-correcting cyclic codes of length n which are ideals in group ring $\mathbb{F}[G]$, where $\mathbb{F}$ is a field and G is a finite torsion group of size n. Another work concerning extensions of BCH codes in various ring constructions has been given by Kelarev in [5] and [6], where the results can also be considered as the special cases of semigroup rings of particular type. In [7], the authors discussed cyclic codes through the polynomial ring $B[X;\mathbb{Z}_0]$, where B is any finite commutative ring with identity. In this paper, we introduce a construction technique of cyclic codes through a monoid ring $B[X;\frac{1}{p^k}\mathbb{Z}_0]$, where p is any prime integer and $k \geq 0$, instead of a polynomial ring $B[X;\mathbb{Z}_0]$.

3 Basic results from monoid ring

Let $(S,*)$ be a commutative semigroup and $(R,+,\cdot)$ a commutative associative ring. The set J of all finitely nonzero functions f from S into R is a ring with respect to binary operations addition and multiplication defined as $(f+g)(s) = f(s)+g(s)$ and $(fg)(s) = \sum_{t*u=s} f(t)g(u)$, where the symbol $\sum_{t*u=s}$ indicates that the sum is taken over all pairs (t,u) of elements of S such that $t*u=s$ and if s is not expressible in the form $t*u$ for any $t,u \in S$, then $(fg)(s)=0$. The set J is known as *semigroup ring* of S over R. If S is a monoid, then J is called monoid ring. This ring J is represented as $B[S]$, where S is a multiplicative semigroup, and the elements of J are written either as $\sum_{s\in S} f(s)s$ or as $\sum_{i=1}^{n} f(s_i)s_i$. The representation of J will be $R[X;S]$ whenever S is an additive semigroup. As there is an isomorphism between additive semigroup S and multiplicative semigroup $\{X^s : s \in S\}$, it follows that a nonzero element f of $R[X;S]$ is uniquely represented in the canonical form $\sum_{i=1}^{n} f(s_i)X^{s_i} = \sum_{i=1}^{n} f_i X^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for all $i \neq j$. Degree is not generally defined in commutative semigroup rings but if the semigroup S is a totally ordered semigroup, we can define the degree of a generalized polynomial of the semigroup ring $R[X;S]$. If $f = \sum_{i=1}^{n} f_i X^{s_i}$ is the canonical form of the nonzero element $f \in R[X;S]$, where $s_1 < s_2 < \cdots < s_n$, then s_n is called the degree of f and we write $deg(f) = s_n$ [8].

If S is $\mathbb{Z}_0$, the additive monoid of non negative integers and B is an associative commutative ring, then the semigroup ring is simply the polynomial ring $B[X]$. It can be observed that $B[X] = B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{p^k}\mathbb{Z}_0]$. Furthermore, as $\frac{1}{p^k}\mathbb{Z}_0$ is an ordered monoid, it follows that we can define the degree of elements in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$.

4 Construction of cyclic codes

Let $f(X^{\frac{1}{p^k}}) \in B[X;\frac{1}{p^k}\mathbb{Z}_0]$ be a monic generalized polynomial of degree n. Thus, $\frac{B[X;\frac{1}{p^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{p^k}}))}$ is the set of residue classes of generalized polynomials in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$ module the ideal $(f(X^{\frac{1}{p^k}}))$ and a class can be represented as $\overline{a}(X^{\frac{1}{p^k}}) = \overline{a_0} + \overline{a_{\frac{1}{p^k}}}X^{\frac{1}{p^k}} + \cdots + \overline{a_{\frac{p^k n-1}{p^k}}}X^{\frac{p^k n-1}{p^k}}$. A principal ideal, which consists of all multiples of a fixed generalized polynomial $g(X^{\frac{1}{p^k}})$ by elements of

$\frac{B[X;\frac{1}{p^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{p^k}}))}$, called generator generalized polynomial of the ideal. Now, we shall prove some results which show a method of getting the generator generalized polynomial of a principal ideal. This method shall provide a base for the construction of a principal ideal in the ring $\frac{B[X;\frac{1}{p^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{p^k}}))}$. In what follows $\Re_{p^k}$ shall represent the factor ring $\frac{B[X;\frac{1}{p^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{p^k}}))}$.

Definition 1. *A linear code C of length $p^k n$ over B is a B-submodule of the B-module of all $p^k n$-tuples of $B^{p^k n}$, and a linear code C over B is cyclic, if when $v = (v_0, v_{\frac{1}{p^k}}, v_{\frac{2}{p^k}}, v_1, \cdots, v_{\frac{p^k n-1}{p^k}}) \in C$, every cyclic shift $v^{(1)} = (v_{\frac{p^k n-1}{p^k}}, v_0, v_{\frac{1}{p^k}}, \cdots, v_{\frac{p^k n-2}{p^k}}) \in C$, with $v_i \in B$ for $0 \leq i \leq \frac{p^k n-1}{p^k}$.*

Theorem 1. *A subset C of $\Re_{p^k}$, where p is any prime integer and $k \geq 0$, is a cyclic code if and only if C is an ideal of $\Re_{p^k}$.*
Proof. Assume C is an ideal in $\Re_{p^k}$, and hence a B-module. It is also closed under multiplication by any ring element, in particular under multiplication by $X^{\frac{1}{p^k}}$. Hence, C is a cyclic code. Conversely, let the subset C is a cyclic code. Thus, C is closed under addition and multiplication by $X^{\frac{1}{p^k}}$. Therefore, it is closed under multiplication by powers of $X^{\frac{1}{p^k}}$ and linear combinations of powers of $X^{\frac{1}{p^k}}$. This means, C is closed under multiplication by an arbitrary generalized polynomial. Hence, C is an ideal.

Corollary 1. *[7, Theorem 2.1] A subset C of $\Re_{p^k}$ is a cyclic code if and only if C is an ideal of $\Re_{p^k}$.*

Lemma 1. *Let I be an ideal in the ring $\Re_{p^k}$, where p is any prime integer and $k \geq 0$. If the leading coefficient of some generalized polynomial of lowest degree in I is a unit in B, then there exists a unique monic generalized polynomial of minimal degree in I.*
Proof. Let $\overline{f}(X^{\frac{1}{p^k}}) \in I$ with lowest degree r in I. If the leading coefficient $\overline{a}_r$ of $\overline{f}(X^{\frac{1}{p^k}})$ is a unit in B, then it is always possible to get a monic generalized polynomial $\overline{f}_1(X^{\frac{1}{p^k}}) = \overline{a_r} f(X^{\frac{1}{p^k}})$ with the same degree in I. Now, if both $\overline{g}(X^{\frac{1}{p^k}})$ and $\overline{f}(X^{\frac{1}{p^k}})$ are monic generalized polynomials of minimal degree r in I, then the generalized polynomial $\overline{k}(X^{\frac{1}{p^k}}) = \overline{f}(X^{\frac{1}{p^k}}) - \overline{g}(X^{\frac{1}{p^k}})$ is in I and has degree fewer than r. Therefore, by the choice of $\overline{f}(X^{\frac{1}{p^k}})$ follows that $\overline{k}(X^{\frac{1}{p^k}}) = 0$, and hence, $\overline{f}(X^{\frac{1}{p^k}}) = \overline{g}(X^{\frac{1}{p^k}})$.

Corollary 2. *[7, Lemma 2.2] Let I be an ideal in the ring $\Re_{p^k}$. If the leading coefficient of some polynomial of lowest degree in I is a unit in B, then there exists a unique monic polynomial of minimal degree in I.*

Theorem 2. *Let J be an ideal in the ring $\Re_{p^k}$, where p is any prime integer and $k \geq 0$. If the leading coefficient of some generalized polynomial $\overline{g}(X^{\frac{1}{p^k}})$ of lowest degree in ideal J is a unit in B, then I is generated by $\overline{g}(X^{\frac{1}{p^k}})$.*
Proof. Let $\overline{a}(X^{\frac{1}{p^k}})$ be a generalized polynomial in J. By Euclidean algorithm, it follows that there are unique generalized polynomials $\overline{q}(X^{\frac{1}{p^k}})$ and $\overline{r}(X^{\frac{1}{p^k}})$ with $\overline{a}(X^{\frac{1}{p^k}}) = \overline{q}(X^{\frac{1}{p^k}})\overline{g}(X^{\frac{1}{p^k}}) + \overline{r}(X^{\frac{1}{p^k}})$, where $\overline{r}(X^{\frac{1}{p^k}}) = 0$ or $\deg(r(X^{\frac{1}{p^k}})) < \deg(g(X^{\frac{1}{p^k}}))$. So, clearly $\overline{r}(X^{\frac{1}{p^k}}) \in J$. Hence, by the choice of $\overline{g}(X^{\frac{1}{p^k}})$, it follows that $\overline{r}(X^{\frac{1}{p^k}}) = 0$, and therefore, $\overline{a}(X^{\frac{1}{p^k}}) = \overline{q}(X^{\frac{1}{p^k}})\overline{g}(X^{\frac{1}{p^k}})$. Therefore, J is generated by $\overline{g}(X^{\frac{1}{p^k}})$.

DOI: 10.5540/03.2015.003.01.0223

Corollary 3. *[7, Theorem 2.2] Let J be an ideal in the ring $\Re_{p^k}$. If the leading coefficient of some polynomial $\overline{g}(X)$ of lowest degree in ideal J is a unit in B, then J is generated by $\overline{g}(X)$.*

Lemma 2. *Let $r(X^{\frac{1}{p^k}})$ be a generalized polynomial in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$. If $\deg(r(X^{\frac{1}{p^k}})) < \deg(f(X^{\frac{1}{p^k}}))$ and $r(X^{\frac{1}{p^k}}) \neq 0$, then $\overline{r}(X^{\frac{1}{p^k}})$ is nonzero in $\Re_{p^k}$.*

Proof. If $\overline{r}(X^{\frac{1}{p^k}}) = \overline{0}$, then there is $q(X^{\frac{1}{p^k}}) \neq 0$ in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$ such that $r(X^{\frac{1}{p^k}}) = f(X^{\frac{1}{p^k}})q(X^{\frac{1}{p^k}})$. Since $f(X^{\frac{1}{p^k}})$ is regular and $r(X^{\frac{1}{p^k}}) \neq 0$, it follows that $\deg(r(X^{\frac{1}{p^k}})) = \deg(f(X^{\frac{1}{p^k}}))+\deg(q(X^{\frac{1}{p^k}}))$ $\geq \deg(f(X^{\frac{1}{p^k}}))$, which is a contradiction. Hence, $\overline{r}(X^{\frac{1}{p^k}}) \neq 0$.

Corollary 4. *[7, Lemma 2.2] Let $r(X)$ be a generalized polynomial in $B[X;\mathbb{Z}_0]$. If $\deg(r(X)) < \deg(f(X))$ and $r(X) \neq 0$, then $\overline{r}(X)$ is nonzero in $\Re_{p^k}$.*

Lemma 3. *Let I be an ideal in the ring $\Re_{p^k}$, where p is any prime integer, $k \geq 0$ and $g(X^{\frac{1}{p^k}})$ $\in B[X;\frac{1}{p^k}\mathbb{Z}_0]$ with leading coefficient unit in B such that $\deg(g(X^{\frac{1}{p^k}})) < \deg(f(X^{\frac{1}{p^k}}))$. If $\overline{g}(X^{\frac{1}{p^k}}) \in I$ and has lowest degree in I, then $g(X^{\frac{1}{p^k}})$ divides $f(X^{\frac{1}{p^k}})$ in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$.*

Proof. According to Euclidean algorithm for commutative rings, it follows that there are unique polynomials $\overline{q}(X^{\frac{1}{p^k}})$ and $\overline{r}(X^{\frac{1}{p^k}})$ such that $\overline{0} = \overline{g}(X^{\frac{1}{p^k}})\overline{q}(X^{\frac{1}{p^k}}) + \overline{r}(X^{\frac{1}{p^k}})$, where $\overline{r}(X^{\frac{1}{p^k}}) = \overline{0}$ or $\deg(\overline{r}(X^{\frac{1}{p^k}})) < \deg(\overline{g}(X^{\frac{1}{p^k}}))$. Thus, $\overline{r}(X^{\frac{1}{p^k}}) = -\overline{g}(X^{\frac{1}{p^k}})\overline{q}(X^{\frac{1}{p^k}})$, i.e., $\overline{r}(X^{\frac{1}{p^k}})$ is in I. So, it follows by the choice of $\overline{g}(X^{\frac{1}{p^k}})$, that $\overline{r}(X^{\frac{1}{p^k}}) = \overline{0}$. Again, by Euclidean algorithm for commutative rings, it follows that there are unique generalized polynomials $q_1(X^{\frac{1}{p^k}})$ and $r_1(X^{\frac{1}{p^k}})$ such that $f(X^{\frac{1}{p^k}}) = g(X^{\frac{1}{p^k}})q_1(X^{\frac{1}{p^k}})+r_1(X^{\frac{1}{p^k}})$, where $r_1(X^{\frac{1}{p^k}}) = 0$ or $\deg(r_1(X^{\frac{1}{p^k}})) < \deg(g(X^{\frac{1}{p^k}}))$. So, $\overline{0} = \overline{g}(X^{\frac{1}{p^k}})\overline{q_1}(X^{\frac{1}{p^k}}) + \overline{r_1}(X^{\frac{1}{p^k}}) = \overline{g}(X^{\frac{1}{p^k}})\overline{q}(X^{\frac{1}{p^k}}) + \overline{r}(X^{\frac{1}{p^k}})$. Thus, $\overline{q_1}(X^{\frac{1}{p^k}}) = \overline{q}(X^{\frac{1}{p^k}})$ and $\overline{r_1}(X^{\frac{1}{p^k}}) = \overline{r}(X^{\frac{1}{p^k}}) = \overline{0}$. By Lemma 2, it follows that $r_1(X^{\frac{1}{p^k}}) = 0$, and therefore, $g(X^{\frac{1}{p^k}})$ divides $f(X^{\frac{1}{p^k}})$.

Corollary 5. *[7, Lemma 2.2] Let I be an ideal in the ring $\Re$ and $g(X) \in B[X;\mathbb{Z}_0]$ with leading coefficient unit in B such that $\deg(g(X)) < \deg(f(X))$. If $\overline{g}(X) \in I$ and has lowest degree in I, then $g(X)$ divides $f(X)$ in $B[X;\mathbb{Z}_0]$.*

Theorem 3. *Let I be an ideal in the ring $\Re_{p^k}$, where p is any prime integer and $k \geq 0$. If $g(X^{\frac{1}{p^k}})$ divides $f(X^{\frac{1}{p^k}})$ and $\overline{g}(X^{\frac{1}{p^k}}) \in I$, then $\overline{g}(X^{\frac{1}{p^k}})$ has lowest degree in $(\overline{g}(X^{\frac{1}{p^k}}))$.*

Proof. Suppose that there is $\overline{b}(X^{\frac{1}{p^k}})$ in $(\overline{g}(X^{\frac{1}{p^k}}))$ such that $\deg(\overline{b}(X^{\frac{1}{p^k}})) < \deg(\overline{g}(X^{\frac{1}{p^k}}))$. Since $\overline{b}(X^{\frac{1}{p^k}}) \in (\overline{g}(X^{\frac{1}{p^k}}))$, it follows that $\overline{b}(X^{\frac{1}{p^k}}) = \overline{g}(X^{\frac{1}{p^k}})\overline{h}(X^{\frac{1}{p^k}})$ for some $\overline{h}(X^{\frac{1}{p^k}}) \in R$. Thus, $b(X^{\frac{1}{p^k}}) - g(X^{\frac{1}{p^k}})h(X^{\frac{1}{p^k}}) \in (f(X^{\frac{1}{p^k}}))$, i.e., $b(X^{\frac{1}{p^k}}) - g(X^{\frac{1}{p^k}})h(X^{\frac{1}{p^k}}) = f(X^{\frac{1}{p^k}})a(X^{\frac{1}{p^k}})$ for some $a(X^{\frac{1}{p^k}})$ in $B[X;\frac{1}{p^k}\mathbb{Z}_0]$. This gives $b(X^{\frac{1}{p^k}}) = g(X^{\frac{1}{p^k}})h(X^{\frac{1}{p^k}}) + f(X^{\frac{1}{p^k}})a(X^{\frac{1}{p^k}})$. Since $g(X^{\frac{1}{p^k}})$ divides $f(X^{\frac{1}{p^k}})$, and so, $g(X^{\frac{1}{p^k}})$ divides $g(X^{\frac{1}{p^k}})h(X^{\frac{1}{p^k}}) + f(X^{\frac{1}{p^k}})a(X^{\frac{1}{p^k}})$, which implies that $g(X^{\frac{1}{p^k}})$ divides $b(X^{\frac{1}{p^k}})$, which is a contradiction. Hence, $\overline{g}(X^{\frac{1}{p^k}})$ has lowest degree in $(\overline{g}(X^{\frac{1}{p^k}}))$.

Corollary 6. *[7, Theorem 2.4] Let I be an ideal in the ring $\Re_{p^k}$. If $g(X)$ divides $f(X)$ and $\overline{g}(X) \in I$, then $\overline{g}(X)$ has lowest degree in $(\overline{g}(X))$.*

5 Conclusion

In [7], cyclic codes over finite rings with length $n = q^{mt} - 1$, where m, t are positive integers and q is any prime integer, are defined. Though in this paper, we obtained cyclic codes over

finite rings with length $n \leq q^{p^k mt} - 1$ where p is a prime integer and $k = 0, 1, 2, \cdots$. Also, we used the monoid ring $B[X; \frac{1}{p^k}\mathbb{Z}_0]$ instead of a polynomial ring $B[X; \mathbb{Z}_0]$, where B is any finite commutative ring with identity. Linear codes obtained through the technique of a monoid ring is better than the linear codes based on polynomial rings [9].

References

[1] J. Cazaran, A.V. Kelarev, *Generators and weights of polynomial codes*, Archiv. Math., **69** (1997), 479-486.

[2] J. Cazaran, A.V. Kelarev, *On finite principal ideal rings*, Acta Math. Univ. Comenianae, **68**(1) (1999), 77-84.

[3] J. Cazaran, A.V. Kelarev, S.J. Quinn, D. Vertigan, *An algorithm for computing the minimum distances of extensions of BCH codes embedded in semigroup rings*, Simgroup Forum, **73**(2006), 317-329.

[4] A.V. Kelarev, *Ring constructions and applications*, World Scientific, River Edge, New York (2002).

[5] A.V. Kelarev, *An algorithm for BCH codes extended with finite state automata*, Fundamenta Informaticae, **84**(1) (2008), 51-60.

[6] A.V. Kelarev, *Algorithms for computing parameters of graph-based extensions of BCH codes*, Journal of Discrete Algorithms, **5** (2007), 553-563.

[7] A. A. de Andrade, R. Palazzo Jr., *Linear codes over finite rings*, Tend. Mat. Apl. Comput., **6**(2) (2005), 207-217.

[8] R. Gilmer, *Commutative semigroup rings*, University Chicago Press Chicago and London (1984).

[9] T. Shah, A. Khan, A. A. Andrade, *Encoding through generalized polynomial codes*, Comput. Appl. Math., **30**(2) (2011), 349-366.

DOI: 10.5540/03.2015.003.01.0223