Bull. Korean Math. Soc. **50** (2013), No. 5, pp. 1513–1521
http://dx.doi.org/10.4134/BKMS.2013.50.5.1513

CYCLIC CODES OVER SOME SPECIAL RINGS

Cristina Flaut

Abstract. In this paper we will study cyclic codes over some special rings: $\mathbb{F}_q[u]/(u^i)$, $\mathbb{F}_q[u_1,\ldots,u_i]/(u_1^2,u_2^2,\ldots,u_i^2,u_1u_2-u_2u_1,\ldots,u_ku_j-u_ju_k,\ldots)$, and $\mathbb{F}_q[u,v]/\left(u^i,v^j,uv-vu\right)$, where $\mathbb{F}_q$ is a field with q elements $q=p^r$ for some prime number p and $r\in\mathbb{N}-\{0\}$.

0. Introduction

Codes over finite rings have been intensively studied in the last time, some of the earliest results of them are in [5], [18]. Ones of the most important finite rings in the coding theory are: the finite field $\mathbb{F}_q$ and the ring $\mathbb{Z}_q$, where $q=p^r$ for some prime number p and $r\in\mathbb{N}-\{0\}$. For example, in the paper [10] some codes over $\mathbb{Z}_4$ are investigated. The class of cyclic codes is an important class of linear codes with a big interest in coding theory. Described as ideals in certain polynomial rings, they have a good algebraic structure and the cyclic codes over some special finite rings were recently described (see [2], [3], [6], [9], [14], [15], [19]). Two classes of these main rings are: Galois rings and rings of the form $\mathbb{F}_q[u]/(u^i)$ or generalization of these, where $q=p^r$ for some prime number p and $r\in\mathbb{N}-\{0\}$.

In this paper, we will investigate the structure of cyclic codes of arbitrary length over the rings:

$$\mathbb{F}_q[u]/(u^i),$$
$$\mathbb{F}_q[u_1,\ldots,u_i]/(u_1^2,u_2^2,\ldots,u_i^2,u_1u_2-u_2u_1,\ldots,u_ku_j-u_ju_k,\ldots),$$
$$\mathbb{F}_q[u,v]/\left(u^i,v^j,uv-vu\right).$$

1. Preliminaries

The *Galois ring* $GR(q,n)$ is the residue class ring $\mathbb{Z}/p^r\mathbb{Z}[x]\ /\ (f(x))$, where $f(x)$ is a monic irreducible polynomial of degree n in $\mathbb{Z}_{p^r}[x]$ such that $f(x)$ *mod* p is a monic irreducible polynomial in $\mathbb{Z}_p[x]$. The existence of the polynomial $f(x)$ is given by the Hensel lifting, which allows us to "lift" a root ρ of a

Received April 17, 2012; Revised November 15, 2012.
2010 *Mathematics Subject Classification.* 94B15, 94B05.
Key words and phrases. cyclic codes, codes over rings, Hamming distance.

polynomial $f \ mod \ p^t$ to a new root σ for the polynomial $f \ mod \ p^{t+1}$, $t \in \mathbb{N}-\{0\}$ (see [8], [13]). From here, it results that we can choose the polynomial f, monic and irreducible over $\mathbb{Z}_p$, as in the standard construction of the Galois field $\mathbb{F}_{p^r}$ from $\mathbb{Z}_p$, and we lift it to a polynomial over $\mathbb{Z}/p^r\mathbb{Z}$. We remark that $|GR(q,n)| = p^{rm}$. For example, $GR(q,1) = \mathbb{Z}_q$ and $GR(p,r) = \mathbb{F}_q$. Let θ be a root of the polynomial $f(x)$. Since we can think at $GR(q,n)$ as a Galois extension $\mathbb{Z}_{p^r}[\theta]$ of $\mathbb{Z}_{p^r}$ by a root θ of $f(x)$, each element $v \in GR(q,n)$ has the form

$$v = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1},$$

where $a_i \in \mathbb{Z}_{p^r}$, $i \in \{0,1,\ldots,n-1\}$ (see [16] and [17]).

The Galois ring $GR(q,n)$ is a free module of rank n over $\mathbb{Z}_q$ and the set

$$\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$$

is a free basis for $GR(q,n)$. Since the ring $\mathbb{Z}_{p^r}$ satisfies the invariant dimension property, it results that all bases in $GR(q,n)$ have n elements.

Let R be a commutative ring and I be an ideal of the ring R. The ideal I is called *principal* if it is generated by one element. The ring R is called *principal* if all its ideals are principal. The ring R is called a *local ring* if it has a unique maximal ideal. A ring R is called a *chain ring* if the set of all ideals of R is ordered by inclusion (is a chain under set inclusion). For a chain ring its unique maximal ideal contains the nilpotent elements.

All ideals in a finite chain ring R are principal. Indeed, if I is not a principal ideal, since R is finite, we have that I is finite generated and $I = \langle a_1, \ldots, a_t\rangle$, where $\{a_1, \ldots, a_t\}$ is a minimal set of generators. It results $\langle a_i\rangle \subsetneq \langle a_j\rangle$, $i \neq j, i, j \in \{1,2\}$, which is a contradiction, since R is a chain ring. We obtain that all ideals in a finite chain ring are principal and there is a unique maximal ideal. It results that a chain ring is a local ring. For details about the chain rings, the reader is referred to [12].

Let $\boldsymbol{m}$ be the maximal ideal in a finite chain ring and let u be its generator, i.e., $\boldsymbol{m} = \langle u\rangle = Ru$. Since R is finite, the chain $R = \langle u^0\rangle \supseteq \langle u^1\rangle \supseteq \langle u^2\rangle \supseteq \cdots \langle u^j\rangle \supseteq \cdots$ is a finite chain. It results that there is an element j with the property $\langle u^j\rangle = 0$. The smallest number t such that $\langle u^t\rangle = 0$ is called *the nilpotency index* of u. The residue field $\mathbb{F} = R/\boldsymbol{m}$ has $q = p^t$ elements with p a prime number, $\text{char}\mathbb{F} = p$ and $|\mathbb{F}^*| = p^t - 1$.

For details about the finite chain rings, the reader is referred to [12].

Galois rings or the rings of the form $\mathbb{F}_q[u]/(u^i)$ are principal ideal rings.

Galois ring $GR(p^r,n)$ is a finite chain ring (of length r).

Finite chain rings allow us to find good description for cyclic codes over these rings.

Let R be a unitary finite commutative ring. A *code* C of length n over R is a nonempty subset of $R^n = \underbrace{R \times R \times \cdots \times R}_{n\text{-times}}$. The elements of C are called *codewords*. A *linear code* C of length n over R is a R-submodule of R^n. We remark that such a submodule is not necessary a free module. A linear code

C of length n is a *cyclic code* if for each codeword $c = (c_0, \ldots, c_{n-1}) \in C$, the codeword $(c_{n-1}, c_0, \ldots, c_{n-2})$ belongs to C.

For the cyclic codes, we will write the codewords as polynomials. Let C be a cyclic code. For each $c = (c_0, \ldots, c_{n-1}) \in C$ we associate the polynomial $c(x)$ of degree less than n, $c(x) = c_0 + c_1 x + \cdots + c_i x^i + \cdots + c_{n-1} x^{n-1} \in R[x]$, called *the associated polynomial*. The codeword $\overline{c} = (c_{n-1}, c_0, \ldots, c_{n-2})$ has the associated polynomial $\overline{c}(x) = c_{n-1} + c_0 x + \cdots + c_i x^{i+1} + \cdots + c_{n-2} x^{n-1}$ and we have $\overline{c}(x) = c(x)x - c_{n-1}(x^n - 1)$, therefore $\overline{c}(x) = c(x)x \ mod\ (x^n - 1)$. We remark that $c(x) \in C \ mod\ (x^n - 1)$ if and only if $c(x)x \in C \ mod\ (x^n - 1)$. Using induction steps, $c(x)x \in C \ mod\ (x^n - 1)$ if and only if $c(x)x^2 \in C mod\ (x^n - 1)$. Therefore we have $c(x)\, x^i \in C \ mod\ (x^n - 1)$ for all $i \in \mathbb{N} - \{0\}$. From here, it results that C is a cyclic code of length n over R if and only if C is an ideal in the ring $R[x]/(x^n - 1)$.

2. The rings

With the above notations, we consider the rings

$$R_i \simeq \mathbb{F}_q[u]/(u^i),$$

$$S_i \simeq \mathbb{F}_q[u_1, \ldots, u_i]/(u_1^2, u_2^2, \ldots, u_i^2, u_1u_2 - u_2u_1, \ldots, u_ku_j - u_ju_k, \ldots), k \neq j,$$

$$T_{(i,j)} = \mathbb{F}_q[u, v]/\left(u^i, v^j, uv - vu\right),\ i, j \in \mathbb{N} - \{0\}.$$

For example, the ring R_i is a commutative chain ring and $\langle u \rangle$ is a maximal ideal (see [7]).

For $R \in \{R_i, S_i, T_{(i,j)}\}$, $i, j, n \in \mathbb{N} - \{0\}$, we denote

$$R_{i,n} = R_i[x]/(x^n - 1),$$

$$S_{i,n} = S_i[x]/(x^n - 1),$$

$$T_{(i,j),n} = T_{(i,j)}[x]/(x^n - 1).$$

Remark 2.1. Since the rings R_i, S_i, $T_{(i,j)}$ are finite rings, the rings $R_{i,n}$, $S_{i,n}, T_{(i,j),n}$ are isomorphic with the group ring RG,where $G = (g \ / \ g^n - 1 = 0)$ is the cyclic group of order n and $R \in \{R_{i,n}, S_{i,n}, T_{(i,j),n}\}$.

Remark 2.2. If the characteristic of the ring is not prime with the length n of the code, then the polynomial $x^n - 1$ factors uniquely over $\mathbb{F}_q$, but does not factor uniquely over the rings $R_i, S_i, T_{(i,j)}$. Indeed, for example, for $p = 2, r = 2, i = 3, j = 2, n = 2$, we have $x^2 - 1 = (x - 1)^2 = (x - (1 - u^2))^2$ over R_3, $x^2 - 1 = (x - 1)^2 = (x - (1 + u_1^2 + u_2^2 + u_3^2))^2$ over S_3, $x^2 - 1 = (x - 1)^2 = \left(x - \left(1 + u^2 + v\right)\right)^2$ over $T_{(3,2)}$.

In [15], if $\gcd(n, p) = 1$, the authors proved that $R_{i,n}$ is a principal ideal ring. In the case of the rings $S_{i,n}$ and $T_{(i,j),n}$ situation is not the same.

Proposition 2.3. *The rings $S_{i,n}$ and $T_{(i,j),n}$ are not principal ideal rings.*

Proof. In the following, we will use some ideas given in [19], Lemma 2.4, when the authors proved the above result for $S_{i,n}$ in the case when $i = 2, p = 2, r = 1$.

Let $R \in \{S_i, T_{(i,j)}\}$. From Remark 2.1, we define the ring morphism $\varphi : RG \to R, \varphi\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) = c_0 + c_1 + \cdots + c_{n-1}$, which is a surjective map, called the *augmentation morphism*. Let $I_i = (u_1, \ldots, u_i)$ be the ideal in S_i generated by the elements $\{u_1, \ldots, u_i\}$ and $I_{u,v}$ be the ideal in $T_{(i,j)}$ generated by the elements $\{u, v\}$. These ideals are not principal ideals. Let $I \in \{I_i, I_{u,v}\}$. We have that $\varphi^{-1}(I) = J$ is an ideal in RG. Since φ is surjective, therefore $\varphi(J)$ is an ideal in R and $\varphi(J) = \varphi\left(\varphi^{-1}(I)\right) = I$. From here, if J is a principal ideal, it results that I is a principal ideal, false. □

Proposition 2.4. *With the above notations, for $n = p^l k$, with $k > 1$, $\gcd(p, k) = 1$, the rings $R_{i,n}$, $S_{i,n}$ and $T_{(i,j),n}$ are not local rings.*

Proof. From [11], we know that a ring is local if and only if the non-units form a maximal ideal in the ring. Let $R \in \{R_{i,n}, S_{i,n}, T_{(i,j),n}\}$.

Case 1. $\gcd(p, k-1) \neq 1$. From the hypothesis, in R, we have

$$0 = x^{p^l k} - 1 = (x^{p^l} - 1)\left(x^{p^l(k-1)} + x^{p^l(k-2)} + \cdots + 1\right).$$

It results that $f(x) = x^{p^l(k-1)} + x^{p^l(k-2)} + \cdots + 1$ is a zero divisor, so that it is not invertible in R. We obtain

$$\varphi\left(x^{p^l(k-2)} + x^{p^l(k-2)} + \cdots + 1\right) = \underbrace{1 + 1 + \cdots + 1}_{(k-1)\text{-times}} = 0.$$

Then $g(x) = x^{p^l(k-2)} + x^{p^l(k-2)} + \cdots + 1$ is a non-unit in R. Since $x^{p^l(k-1)}x^{p^l} = 1$, we have that $f(x) - g(x) = x^{p^l(k-1)}$ is a unit in R. Therefore non-invertible elements in R do not form an ideal, hence R is not a local ring.

Case 2. $\gcd(p, k-1) = 1$. Let $g_1 = ug$, g_1 be a non-unit element. Such an element is a nilpotent element. Denoting $h(x) = f(x) + g_1(x)$, we have $\varphi(h(x)) = k + (k-1)u$. Since $\gcd(p, k-1) = 1$, it results that $(k-1)u$ is a nonzero nilpotent element. From here, we obtain that $k + (k-1)u$ is a sum between an invertible element, k, and a nilpotent element, therefore it is an invertible element. It results that $\varphi(h(x))$ is a unit and $h(x)$ is also a unit, hence non-invertible elements do not form an ideal. We just proved that R is not a local ring. □

Proposition 2.5. *With the above notations, for $n = p^l$ the rings $R_{i,n}$, $S_{i,n}$, $T_{(i,j),n}$ are local rings.*

Proof. Let $R_n \in \{R_{i,n}, S_{i,n}, T_{(i,j),n}\}$, $R \in \{R_i, S_i, T_{(i,j)}\}$. We will prove that the non-units form an ideal in the ring R_n. First of all, we remark that a non-unit element in R_n different from zero is a zero divisor. Indeed, if $\alpha \in R_n, \alpha \neq 0$, is a non-invertible element, then the ideal generated by α is different from R_n. Hence we can find the elements $\alpha_1 \neq \alpha_2$ such that $\alpha_1\alpha = \alpha_2\alpha$. Therefore $(\alpha_1 - \alpha_2)\alpha = 0$ and α is a zero divisor. We remark that an element θ in R

has the form $\theta = \theta_1 + \theta_2$, where $\theta_1 \in \mathbb{F}_q$ and $\theta_2 \in R - \mathbb{F}_q$. If θ is a unit in R, then $\theta_1 \in \mathbb{F}_q^*$. Let $s = s_0 + s_1 x + \cdots + s_{n-1}x^{n-1} \in R_n$ and $s_k = (s_k)_1 + (s_k)_2$, where $(s_k)_1 \in \mathbb{F}_q$ and $(s_k)_2 \in R - \mathbb{F}_q, j \in \{1, \ldots, n-1\}$. Since $x^{p^j} = 1$, it results that $s^{p^j} = s_0^{p^j} + s_1^{p^j} + \cdots + s_{n-1}^{p^j}$ and s^{p^j} is a unit or a zero divisor. If s^{p^j} is a zero divisor, then s is a zero divisor, hence a non-unit. If s^{p^j} is a unit, it results that s is a unit, since $s \cdot s^{p^j-1} = s^{p^j}$. If s^{p^j} is a zero divisor, then $\sum_{k=1}^{n-1}(s_k^{p^j})_1 = 0$ and this characterize a zero-divisor, hence a non-unit in the ring R_n. Let $t = t_0 + t_1 x + \cdots + t_{n-1}x^{n-1} \in R_n$, with $\sum_{k=1}^{n-1}(t_k^{p^j})_1 = 0$, be another non-unit. The element $r = s + t$ is also a non-unit. For prove this, we compute $\sum_{k=1}^{n-1}(r_k^{p^j})_1$. It results $\sum_{k=1}^{n-1}(r_k^{p^j})_1 = \sum_{k=1}^{n-1}(s_k + t_k)_1^{p^j} = \sum_{k=1}^{n-1}(s_k^{p^j})_1 + \sum_{k=1}^{n-1}(t_k^{p^j})_1 = 0 + 0 = 0$, therefore r is a non-unit and non-units form an ideal. Hence R is a local ring. □

Propositions 2.5 and 2.6 were proved for the ring $S_{i,n}$ in [19] in the particular case $i = 2$ (see Theorem 2.5 and Theorem 2.7).

3. Ranks for the cyclic codes over the rings $R_i, S_i, T_{(i,j)}$

In [4], Proposition 1, the authors described cyclic codes of length n over the Galois ring $GR(q, l) = \mathbb{Z}_{p^m}[x]/(f)$, $\deg f = l$, $q = p^m$, $(n, q) = 1$. Using some ideas given in this proof, we can describe cyclic codes over the rings $R_i, S_i, T_{(i,j)}$ in the general case.

Proposition 3.1. *Let $R \in \{R_i, S_i, T_{(i,j)}\}$. A non-zero cyclic code C of length n over R is a free module over R if it is generated by a monic polynomial $h(x)$, where $h(x) \mid (x^n - 1)$ over R. In this case,* rank $C = n - r$, $\deg h(x) = r$, *and $\{h(x), xh(x), \ldots, x^{n-r-1}h(x)\}$ is a basis in C.*

Proof. Let C be a non-zero cyclic code C of length n over R generated by the polynomial $h(x)$, where $h(x) \mid (x^n - 1)$. Since $h(x) \mid (x^n - 1)$, we can consider $h(x)$ a monic polynomial. Then there is a monic polynomial $q(x) \in R$ such that $h(x)q(x) = x^n - 1$. From here, it results that $\deg q(x) = n - r$ and q has the form $q(x) = q_0 + q_1 x + \cdots + x^{n-r}$. Let $R_n \in \{R_{i,n}, S_{i,n}, T_{(i,j),n}\}$. In R_n we have $h(x)q(x) = h(x)(q_0 + q_1 x + \cdots + x^{n-r}) = 0$. Therefore $x^i h(x)$, for $i \geq n - r$, can be written as a linear combination of the elements $\{h(x), xh(x), \ldots, x^{n-r}h(x)\}$, hence each element in C of the form $p(x)h(x)$, $p(x) \in R_n$ is a linear combination of $\{h(x), xh(x), \ldots, x^{n-r-1}h(x)\}$. It results that the system $\{h(x), xh(x), \ldots, x^{n-r-1}h(x)\}$ spans C. For linearly independence over R, let $\alpha_0, \ldots, \alpha_{n-r-1} \in R$ such that $\alpha_0 h(x) + \alpha_1 xh(x) + \cdots + \alpha_{n-r-1}x^{n-r-1}h(x) = 0$. We obtain $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-r-1}x^{n-r-1})h(x) = 0$ in R_n, hence $(x^n - 1) \mid (\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-r-1}x^{n-r-1})h(x)$ in $R[x]$, with

$$\deg(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-r-1}x^{n-r-1})h(x) = n - 1 < n.$$

From here, we have $(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-r-1}x^{n-r-1})h(x) = 0$ in $R[x]$. Since $h(x)$ is monic, it results $\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-r-1}x^{n-r-1} = 0$, hence $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-r-1} = 0$. □

We remark that another proof of the above results can be obtained using the main result from [9].

Corollary 3.2. *With the notations used in Proposition 3.1, if C is a nonzero-cyclic code of length n over R generated by a monic polynomial $h(x)$, where $h(x) \mid (x^n - 1)$ over R, then $|C| = |R|^{n-r}$.*

Proposition 3.3. *Let C be a non-zero cyclic code of length n over $R \in \{R_i, S_i, T_{(i,j)}\}$ generated by the polynomials $\{h_1, \ldots, h_t\}$. Therefore C is a vector space over $\mathbb{F}_q$ and $|C| \leq |q|^{sn}$, where $s = \dim_{\mathbb{F}_q} R$.*

Proof. We know that R is a vector space over $\mathbb{F}_q$. Let $s = \dim_{\mathbb{F}_q} R$ and $\{1, v_1, \ldots, v_{s-1}\}$ be a basis in R. We will prove that $B = \{1, x, \ldots, x^{n-1}, v_1, v_1x, \ldots, v_1x^{n-1}, \ldots, v_{s-1}, v_{s-1}x, \ldots, v_{s-1}x^{n-1}\}$ is a basis in the $\mathbb{F}_q$-vector space $R_n, R_n \in \{R_{i,n}, S_{i,n}, T_{(i,j),n}\}$.

First, we will show the linearly independence of the elements from B. If there are the elements $\alpha_{1,i_1}, \alpha_{2i_2}, \ldots, \alpha_{si_s} \in \mathbb{F}_q$, $i_j \in \{0, 1, 2, \ldots, n-1\}$, $j \in \{1, 2, \ldots, s\}$ such that $\alpha_{1,0} \cdot 1 + \cdots + \alpha_{1,n-1}x^{n-1} + \cdots + \alpha_{s,0}v_{s-1} + \cdots + \alpha_{s,n-1}v_{s-1}x^{n-1} = 0$, comparing the coefficients in this equation, we get

$$\alpha_{1,0} \cdot 1 + \alpha_{2,0}v_{s-1} + \cdots + \alpha_{s,0}v_{s-1} = 0. \tag{3.1.}$$

Since $v_1, \ldots, v_{s-1}$ are nilpotent elements in R, if $\alpha_{1,0} \neq 0$, from relation (3.1), we obtain that a unit is equal with a nilpotent element, false. Hence $\alpha_{1,0} = 0$ and $\alpha_{2,0}v_{s-1} + \cdots + \alpha_{s,0}v_{s-1} = 0$, therefore $\alpha_{2,0} = \cdots = \alpha_{s,0} = 0$. In the same way, comparing coefficients of $x, x^2, \ldots, x^{n-1}$ with zero, we have $\alpha_{1,i_1} = \alpha_{2,i_2} = \cdots = \alpha_{s,i_s} = 0$ for all $i_j \in \{0, 1, 2, \ldots, n-1\}$, $j \in \{1, 2, \ldots, s\}$.

We will prove that B generates R_n. Let $f(x) \in R_n$. By straightforward calculations, we obtain that $f(x)$ is a linear combination of elements in B with coefficients in $\mathbb{F}_q$. It results $|R_n| = |q|^{sn}$.

Now, let C be a nonzero cyclic code. Then C is a vector subspace of the $\mathbb{F}_q$-vector space R_n, therefore $|C| \leq |q|^{sn}$. □

In [2], Theorem 3, and in [3], Theorem 4.2, the authors gave a basis or a minimal spanning set for the codes of even length over $\mathbb{Z}_2 + u\mathbb{Z}_2$, respectively $\mathbb{Z}_2 + u\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$. The same description could be done, in general case, over the ring R_i. If we have supplementary relations between polynomials $h_1, \ldots, h_t$, we can compute $|C|$, as we can see in the following examples.

Example 3.4. Over R_i, for $i = 2$, using Theorem 3 from [2], if C is a nonzero cyclic code of length $n, (n, p) \neq 1$, and $C = (g(x) + up(x), ua(x))$, $a(x) \mid g(x) \mid (x^n - 1)$, with $\deg g(x) = r$, $\deg a(x) = t$, $r \geq t$, $\deg a(x) > \deg p(x)$, then $|C| = (q)^{2n-r-t}$. Indeed, C is a vector space over $\mathbb{F}_q$ and let

$B = \{g(x)+up(x), x(g(x)+up(x)), \ldots, x^{n-r-1}(g(x)+up(x)), ua(x), xua(x), \ldots, x^{n-t-1}ua(x)\}$. We will prove that B is a basis in the $\mathbb{F}_q$-vector space C.

First, we will show that B spans C. Let $c(x) \in C$. Then

$$c(x) = q_1(x)\,(g(x) + up\,(x)) + q_2(x)ua(x), q_i\,(x) \in R[x],\ i \in \{1, 2\}.$$

If $\deg q_1(x) < n - r$ and $\deg q_2(x) < n - t$, we have B spans C. If $\deg q_1(x) \geq n - r$ or $\deg q_2(x) \geq n - t$, it suffices to show that $x^{n-r}\,(g(x) + up(x))$, $u\,(g(x) + up(x))$ and $x^{n-t}ua\,(x)$ are generated by B over $\mathbb{F}_q$.

We have $x^{n-r}\,(g(x) + up(x)) = x^n - 1 + q(x)$, $\deg q(x) \leq n-1$. But $q\,(x) \in C$ and, by the division algorithm, we have $q(x) = (g(x) + up(x))\,h_1(x) + s_1(x)$, $\deg s_1(x) < r$, $\deg h_1\,(x) \leq n - 1$, $s_1(x) = ua(x)h_2\,(x) + s_2(x)$, $\deg s_2(x) < \deg ua\,(x)$, $\deg h_2(x) \leq r - t$. Since $\deg ua(x) = \deg a(x)$ and in C any polynomial must have degree greater or equal with $\deg a(x)$, it results $s_2(x) = 0$. Since $a(x) \mid g(x)$, hence $g(x) = a\,(x)\,h(x)$ and we have $ug(x) = u\,(g\,(x) + up(x)) = ua(x)h(x)$, with $\deg h(x) \leq r - t < n - t - 1$. It results that $u\,(g(x) + up(x))$ is generated by B over $\mathbb{F}_q$. To finish the proof, it is enough to show that the element $ux^{r-t}a(x)$ is generated by B over $\mathbb{F}_q$. We have $ux^{r-t}a(x) = u\,(g(x) + up(x)) + uh_3(x)$, where uh_3 belongs to C and $t \leq \deg h_3(x) < r$. Therefore $uh_3(x) = \alpha_0 ua(x) + \alpha_1 xua(x) + \cdots + \alpha_{r-t-1}x^{r-t-1}ua(x), \alpha_i \in \mathbb{F}_q, i \in \{0, \ldots, r - t - 1\}$.

We will prove that B is a linearly independent system. Indeed, if there are the elements $\alpha_{1,i_1}, \alpha_{2,i_2} \in \mathbb{F}_q$, $i_j \in \{0, 1, 2, \ldots, n - 1\}$, $j \in \{1, 2\}$ such that $\alpha_{1,0}\,(g(x) + up(x)) + \cdots + \alpha_{1,n-1}x^{n-r-1}\,(g(x) + up(x)) + \alpha_{2,0}ua(x) + \cdots + \alpha_{2,n-1}x^{n-t-1}ua\,(x) = 0$, comparing the coefficients in this equation, we get $\alpha_{1,0}g\,(0) + \alpha_{1,0}up\,(0) + \alpha_{2,0}ua\,(0) = 0$. If $\alpha_{1,0} \neq 0$, since $g\,(0)$ is a unit and u a nilpotent element, it results that a unit is equal with a nilpotent, false. Therefore $\alpha_{1,0} = 0$. We obtain $\alpha_{2,0}ua\,(0) = 0$. If $\alpha_{2,0} \neq 0$, it results $ua\,(0) = 0$, false, since $a\,(0)$ is a unit. We repeat this procedure and we get $\alpha_{1,i_1} = \alpha_{2,i_2} = 0$ for all $i_j \in \{0, 1, 2, \ldots, n - 1\}$, $j \in \{1, 2\}$, hence B is a linearly independent system. It results that B is a basis in the $\mathbb{F}_q$-vector space C and $|C| = |q|^{2n-r-t}$.

4. Minimum Hamming distance for the cyclic codes over the rings $R_i, S_i, T_{(i,j)}$

Let C be a linear code over the ring R. The *Hamming distance* between two codewords c_1 and c_2, denoted by $H\,(c_1, c_2)$, is the number of coordinates in which the codewords c_1 and c_2 differ. The number of nonzero entries of a codeword c, denoted $w(c)$, is called the *Hamming weight* of the codeword c. The *Hamming distance* of a linear code C is

$$d\,(C) = \min\{w(c) \mid c \in C, c \neq 0\}.$$

In [1], the authors studied the Hamming distance of cyclic codes of even length, especially codes of length $2^e, e \in \mathbb{N} - \{0\}$ (Lemmas 16, 17, and 18). In the following, using some ideas from the mentioned lemmas, we will investigate the

Hamming distance for cyclic codes of length $n = p^r, r \in \mathbb{N} - \{0\}$, over the rings $R_i, S_i, T_{(i,j)}$.

Definition 4.1. Let $n = a_{s-1}p^{s-1} + a_{s-2}p^{s-2} + \cdots + a_1p^1 + a_0p^0$, $\alpha_i \in \{0, 1, \ldots, p-1\}$, $i \in \{0, 1, \ldots, s-1\}$, be the p-adic expansion of n.

1) If $a_{s-1} = \cdots = a_{s-t} \neq 0$, $s - t > 0$ and $a_{s-i} = 0$ for all $i \in \{t+2, t+3, \ldots, s-1\}$, then n has a p-adic length t zero expansion.

2) If $a_{s-1} = \cdots = a_{s-t} \neq 0$, $s - t > 0$ and $a_{s-i} \neq 0$ for some elements $i \in \{t+2, t+3, \ldots, s-1\}$, then n has a p-adic length t non-zero expansion.

3) If $s = t$, then n has a p-adic full expansion.

Proposition 4.2. *Let $C = (g(x))$ be a cyclic code over $R \in \{R_i, S_i, T_{(i,j)}\}$ of length $p^r, r \in \mathbb{N} - \{0\}$, where $g(x) = (x^{ap^{r-1}} - 1)g_1(x)$. If $g_1(x)$ generates a cyclic code of length p^{r-1} and Hamming distance d, then $d(C) = 2d$.*

Proof. For $c \in C$ we have $c = (x^{ap^{r-1}} - 1)g_1(x)g_2(x)$, $g_2(x) \in \mathbb{F}_q[x]/(x^n - 1)$ and $g_1(x)\, g_2(x) \in (g_1(x))$. It results $w(c) = w((x^{ap^{r-1}} - 1)g_1(x)g_2(x)) = w(x^{ap^{r-1}} g_1(x)g_2(x)) + w(g_1(x)g_2(x))$. Then $d(C) = d + d = 2d$. □

Conclusion. In this paper we investigate the structure of cyclic codes of arbitrary length over the rings $R_i, S_i, T_{(i,j)}$. Moreover the ranks and minimum Hamming distance of these codes were studied. Since the rings with Hamming weight cannot produce always better codes, a more relevant weight as, for example, the homogeneous weight on the above mentioned rings can be studied. The remark above can constitute the starting point for further research.

Acknowledgements. I would like to thank the referee for his/her many suggestions which helped me improve this paper.

References

[1] T. Abualrub and I. Siap, *On the construction of cyclic codes over the ring $\mathbb{Z}_2 + u\mathbb{Z}_2$*, WSEAS Trans. Math. **5** (2006), no. 6, 750–755.

[2] ———, *Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$*, Des Codes Cryptogr. **42** (2007), no. 3, 273–287.

[3] M. M. Al-Ashker and M. Hamoudeh, *Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$*, Turk J. Math. **34** (2010), 1–13.

[4] M. Bhaintwal and S. K. Wasan, *On quasi-cyclic codes over $\mathbb{Z}_q$*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5-6, 459–480.

[5] I. F. Blake, *Codes over certain rings*, Inf. Control **20** (1972), 396–404.

[6] S. T. Dougherty, S. Karadeniz, and B. Yildiz, *Cyclic codes over R_k*, Des. Codes Cryptogr. **63** (2012), no. 1, 113–126.

[7] S. T. Dougherty, H. Liu, and Y. H. Park, *Lifted codes over finite chain rings*, Math. J. Okayama Univ. **53** (2011), 39–53.

[8] D. Eisenbud, *Commutative Algebra*, Graduate Texts in Mathematics, **150**, Springer-Verlag, Berlin, New York, 1995.

[9] M. Greferath, *Cyclic codes over finite rings*, Discrete Math. **177** (1997), no. 1-3, 273–277.

[10] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4 liniarity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.
[11] T. W. Hungerford, *Algebra*, Springer Verlag, New York, 1974.
[12] B. R. McDonald, *Finite Rings with Identity*, New York, Marcel Dekker Inc., 1974.
[13] J. G. Milne, *Étale cohomology*, Princeton University Press, 1980.
[14] A. A. Nechaev and T. Honold, *Fully weighted modules and representations of codes*, (Russian) Problemy Peredachi Informatsii **35** (1999), no. 3, 18–39; translation in Problems Inform.Transmission **35** (1999), no. 3, 205–223.
[15] J.-F. Qian, L.-N. Zhang, and A.-X. Zhu, *Cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$*, IEICE Trans. Fundamentals Vol. **E88-A** (2005), no. 3, 795–797.
[16] P. Solé and V. Sison, *Bounds on the minimum homogeneous distance of the p^r-ary image of linear block codes over the Galois ring $GR(p^r, m)$*, IEEE Trans. Inform. Theory **53** (2007), no. 6, 2270–2273.
[17] ———, *Quaternary convolutional codes from linear block codes over Galois rings*, IEEE Trans. Inform. Theory **53** (2007), no. 6, 2267–2270.
[18] E. Spiegel, *Codes over Z_m revisited*, Inform. and Control **37** (1978), no. 1, 100–104.
[19] B. Yildiz and S. Karadeniz, *Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$*, Des. Codes Cryptogr. **58** (2011), no. 3, 221–234.

Faculty of Mathematics and Computer Science
Ovidius University
Bd. Mamaia 124, 900527, Constanta, Romania
E-mail address: cflaut@univ-ovidius.ro; cristina_flaut@yahoo.com