A Unique Representation of Cyclic Codes over $GR(p^n, r)$

Sami Alabiad * and Yousef Alkhamees

Department of Mathematics, King Saud University, Riyadh 11451, Saudi Arabia
* Correspondence: ssai1@ksu.edu.sa or alabiad2012@gmail.com

Abstract: Let $R$ be a Galois ring, $GR(p^n, r)$, of characteristic $p^n$ and of order $p^{mr}$. In this article, we study cyclic codes of arbitrary length, $N$, over $R$. We use discrete Fourier transform (DFT) to determine a unique representation of cyclic codes of length $N$, in terms of that of length, $p^n$, where $s = v_p(N)$ and $v_p$ are the $p$-adic valuation. As a result, Hamming distance and dual codes are obtained. In addition, we compute the exact number of distinct cyclic codes over $R$ when $n = 2$.

Keywords: Galois rings; cyclic codes; linear codes; polynomials; coding theory

1. Introduction

Cyclic codes are a special class in coding theory and have been a primary field of study since its inception, for instance see [1–8]. These codes have been traditionally described over finite fields; however, many important nonlinear codes over finite fields relate, via the Gray map, to linear codes over finite chain rings. Let $R$ be a finite chain ring. Theoretically, cyclic codes which have arbitrary length, $N$, over $R$ correspond with ideals of $R[x]/ < x^N − 1 >$. Let $p$ be the characteristic of the residue field of $R$. When $p \nmid N$, $x^N − 1$ has unique factorization into irreducible polynomials; this is the key to examining the ideals of $R[x]/ < x^N − 1 >$ and then constructing cyclic codes over $R$. However, $x^N − 1$ does not factor uniquely if $p \mid N$, and such cases produce what are called repeated-root cyclic codes over $R$. Such codes were first described by Berman [9] in 1967. In the literature, there is not much research on the study of repeated-root cyclic codes over finite rings, see [10–15]. The basic purpose of this manuscript is to find unique representation for all repeated-root cyclic codes of length, $N$, over a Galois ring—$GR(p^n, r)$ of characteristic $p^n$ and residue degree $r$.

In [11], Abualrub et al. introduced minimal degree polynomials to describe cyclic codes over $\mathbb{Z}_q$ with length $2^s$. Doughtry et al. [12] expanded the results to cyclic codes over $\mathbb{Z}_{p^n} = GR(p^n, 1)$ of length, $N$. They utilized discrete Fourier transform (DFT) in proving that $\mathbb{Z}_{p^n}[x]/(x^N − 1)$ is mapped isomorphically to a direct product of rings with the form $GR(p^n, r)[x]/ < x^p^{s} − 1 >$, where $s = v_p(N)$ and $v_p$ is the $p$-adic valuation. Kiah et al. [13] considered cyclic codes over $GR(p^n, r)$ which have length $p^n$. Finally, by a different method from that of [12], Jasbir et al. [14] obtained minimal degree polynomials generating cyclic over $GR(p^n, r)$ based on the concept of Gröbner basis.

In the present article, we generalize the approach of Doughtry et al. [12], and determine a unique representation of cyclic codes of any finite length, $N$, over $GR(p^n, r)$ in terms of polynomials with minimal degrees. The generating polynomials are constructed by a different method (i.e., DFT) and have more explicit structural forms than those given in [14]. This explicit construction for generators polynomial allows us to describe dual codes, and establish Hamming distance. The article is sectioned as follows. In Section 3, we make use of the (unique) $p$-adic expression of elements of $GR(p^n, r)$ to construct a unique description of cyclic codes of length $p^n$. The obtained structure allows us to compute their dual codes and Hamming distance. In Section 4, we employ DFT to express cyclic codes of length $N = m p^n$ in terms of that of length $p^n$ over Galois extensions of $GR(p^n, r)$. This means, it suffices to investigate cyclic codes of length $p^n$ over Galois rings. Consequently, dual codes...
Axioms 2022, 11, 519

and Hamming distance are completely determined. Moreover, we obtain the enumeration of cyclic codes with length, \( N \), and we give the precise number of cyclic codes when \( n = 2 \).

2. Preliminaries

This section presents some facts and mentions the background used in the subsequent sections.

2.1. Galois Ring

Suppose that \( p \) is prime, and suppose \( R = GR(p^n,r) \) is Galois extension of degree \( r \) over \( \mathbb{Z}_p^r \). This ring extension, \( GR(p^n,r) \), is called a Galois ring with \( p^n \) elements \([16]\), and \( GR(p^n,r) \cong \mathbb{Z}_{p^n}[x] / < f > \), where \( f \) is a basic polynomial of degree \( r \) in the \( \mathbb{Z}_{p^n} \) irreducible modulo \( p \). The maximal ideal in \( GR(p^n,r) \) is principal and of the form \( pGR(p^n,r) = < p > \). Indeed, every ideal is principal to \( < p^i > pGR(p^n,r) \), where \( 0 \leq i \leq n \).

There is a of order \( p^r - 1 \) such that \( GR(p^n,r) = \mathbb{Z}_{p^n}[a] \). The set \( \Gamma(r) = \{0,1,a,\ldots,a^{p^r-2}\} \) is called the Teichmuller set which is a set of closet representatives modulo \( p \). Suppose \( c \) is an element of \( GR(p^n,r) \); then, \( c \) can be uniquely written (p-adic expression) as:

\[
c = c_0 + c_1p + \cdots + c_{n-1}p^{n-1},
\]

where \( c_0, c_1, \ldots, c_{n-1} \) are elements in \( \Gamma(r) \). Moreover, \( c \) is a unit if and only if \( c_0 \neq 0 \). The set \( \Gamma(r) \) is mapped onto \( F_{p^r} \) under the canonical map \( \mu \) between \( GR(p^n,r) \) and \( F_{p^r} \). The group of automorphisms \( Aut(R) \) of \( R \) is a cyclic group with order \( r \). Furthermore, \( Aut(R) = < \rho > \), where \( \rho \) is the Frobenius correspondence. For more details, see \([17,18]\).

Proposition 1 \([18]\). Let \( r' \) be any positive integer; then, there is a basic polynomial in \( GR(p^n,r)[x] \) of degree \( r' \) which divides as \( x^{p^{r'}-1} - 1 \).

Proposition 2 \([18]\). Let \( h(x) \) be a basic irreducible polynomial over \( GR(p^n,r) \) of degree \( r' \); then, \( GR(p^n,r)[x] / < h(x) > \) is a Galois ring which contains \( GR(p^n,r) \) as sub-ring and denoted by \( GR(p^n,r') \).

2.2. Cyclic Codes

Let \( R \) be a finite ring. A cyclic code is a linear code over \( R \) which is invariant under cyclic shifts. Each codeword of length, \( N \), written as a vector, \( c = (c_0, c_1, \ldots, c_{N-1}) \), traditionally corresponds to a polynomial form \( c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1} \); thus, we can identify a code, \( C \), as a set, with polynomial forms for its codewords. This means, in \( R[x] / < x^N - 1 > \), \( xc(x) \) represents the cyclic shift of \( c(x) \).

Proposition 3 \([19,20]\). A linear code \( C \) is cyclic over \( R \) with length, \( N \), if and only if \( C \) is an ideal of the ring \( R[x] / < x^N - 1 > \).

Assume \( R(r) \) is the finite ring \( GR(p^n,r)[x] / < x^p^r - 1 > \), \( \overline{R}(r) \) is the ring \( F_{p^r}[x] / < x^p^r - 1 > \), and \( \mu \) is usual map (modulo \( p \)) between \( R(r) \) and \( \overline{R}(r) \). We define the following codes for any cyclic code, \( C \), over \( R = GR(p^n,r) \).

Definition 1. As \( 0 \leq i \leq n - 1 \), let

\[
Tor_i(C) = \mu\{c \in R \mid p^ic \in C\}.
\]

We call \( Tor_i(C) \) the \( i \)th torsional code for \( C \); particularly, \( \mu(C) = Res(C) = Tor_0(C) \) is called the residue code for \( C \).
Proposition 4 ([12]). Suppose that $C$ is a cyclic code with length $p^s$ over $R$, and $0 \leq i \leq n - 1$. Thus, $\text{Tor}_i(C)$ is a cyclic code over $F_{p^s}$ of length $p^s$ and 

$$\text{Tor}_i(C) = \langle (x - 1)^{T_i} \rangle,$$

where $0 \leq T_i \leq p^s$. Furthermore,

(i) $|\text{Tor}_i(C)| = (p^s)^{p^s - T_i}$,

(ii) If $g(x) \in R(r)$ and $p^i ((x - 1)^{t_i} + pg(x)) \in C$, then $T_i \leq t_i$.

(iii) $p^s 1 \geq T_0 \geq T_1 \geq \cdots \geq T_{n-1} \geq 0$.

(iv) $|C| = (p^s)^{np^s - (T_0 + T_1 + \cdots + T_{n-1})}$.

Definition 2. If $C$ is a cyclic code over $R$, as $0 \leq i \leq n - 1$, then we call $T_i = T_i(C)$ the $i$th torsional degree for $C$.

The above notations shall keep their meanings through the paper, and $N = n_1 p^s$, $(n_1, p) = 1$.

3. Cyclic Codes of Length $p^s$

Throughout this section, we aim to uniquely represent any cyclic code over $R = GR(p^n, r)$, with length $p^s$. Using this representation, we were able to obtain Hamming distances and describe dual codes. Moreover, we determine the number of these codes, i.e., the ideals of $R(r)$.

3.1. The Representation of Cyclic Codes

Next, the subsequent theorem gives us a unique representation for $C$.

Theorem 1. Suppose that $C$ is a cyclic code over $R$ of length $p^s$. Therefore, $C$ can be expressed uniquely as:

$$C = \langle p_1(x), \cdots, p_{n-1}(x) \rangle,$$

$$p_i(x) = \begin{cases} 
  p^i(x - 1)^{T_i} + \sum_{j=1}^{n-1} p^{i+j}(x - 1)^{t_{ij}} h_{ij}(x), & \text{if } T_i(C) < p^s, \\
  0, & \text{if } T_i(C) = p^s,
\end{cases}$$

where $h_{ij}(x)$ is a unit or zero, and $t_{ij} + \deg h_{ij} < T_{i+j}$.

Proof. As $C$ is an ideal in $R(r)$, from [12], $C = \langle r_0(x), \cdots, r_{n-1}(x) \rangle$, where $r_i(x) = p^i(x - 1)^{T_i} + g_i(x)$ when $T_i < p^s$ for some $g_i(x) \in R(r)$ and $r_i(x) = 0$ otherwise. By the $p$-adic expression (1) of elements of $R$, $g_i(x)$ is expressed by:

$$g_i(x) = \sum_{j=1}^{n-1} (p^s)^j \sum_{l=0}^{p^s-1} c_{ij,l}(x-1)^l,$$

where $c_{ij,l} \in \Gamma(r)$. Moreover, the inner sum in (3) can be rewritten as:

$$\sum_{l=0}^{p^s-1} c_{ij,l}(x-1)^l = (x-1)^{t_{ij} h_{ij}(x)},$$

where $h_{ij}(x)$ is a unit or zero, and $t_{ij} + \deg h_{ij} < T_{i+j}$. Let

$$p_i(x) = p^i(x - 1)^{T_i} + \sum_{j=1}^{n-1} p^{i+j}(x - 1)^{t_{ij}} h_{ij}(x);$$

then, we obtain the results. The uniqueness of the polynomials $p_i(x)$ is direct from Equation (1). □
Axioms 2022, 11, 519

Theorem 2. Let $C$ be a cyclic code over $R$ with length $p^n$. Assume that $T_i < p^s$ and $p_i(x)$ is the polynomial described in Theorem 1. Thus, $deg p_i(x) = T_i$ and its leading coefficient is $p^i$.

Remark 1. To simplify the representation of $C$, let $h_i(x) = \sum_{j=1}^{n-i} (x-1)^{i-j} h_{ij}(x)$. Then, $C = < e_0(x), p e_1(x), \ldots, p^{n-1} e_{n-1}(x) >$, where $e_i(x) = (x-1)^{T_i} + ph_i(x)$.

Example 1. Let $e_0(x) = (x-1)^3$, $e_1(x) = (x-1)^2$ and $e_2(x) = (x-1) + 2$ and $e_3(x) = (x-1)$. Suppose $C$ is a cyclic code with length 8 over $GR(8,2)$ spanned by $e_0(x), e_1(x)$ and $e_2(x)$. One can easily check $e_0(x), e_1(x)$ and $e_2(x)$ verify the hypothesis in Theorem 1. Thus, $< e_0(x), 2e_1(x), 4e_2(x) >$ is the representation of $C$.

Example 2. If $R = GR(4,2)$ and $C$ is a cyclic code over $R$ with length 4 spanned by $e_0(x) = (x-1) + 2$ and $e_1(x) = (x-1)$, then, by Theorem 1, $< e_0(x), 2e_1(x) >$ is the representation of $C$.

3.2. Hamming Distance

For $c = (c_0, c_1, \ldots, c_{N-1}) \in R^N$, the Hamming weight, $wt(c)$, of $c$ is the number of nonzero components of $c$. The Hamming distance, $d(c, c')$, between $c$ and $c'$ is defined as $d(c, c') = wt(c - c')$.

Theorem 2. If $C$ is a cyclic code over $R$ with length $p^s$, then

$$d(C) = d(\text{Tor}_{n-1}(C)).$$
Proof. As \( c(x) \in C \), we have \( \text{wt}(p^{n-1}c(x)) \leq \text{wt}(c(x)) \). So, it is sufficient to give the Hamming distance of \( p^{n-1}c(x) \) in order to determine the Hamming distance for \( C \). Now, since \( p^{n-1}c(x) \) and \( \overline{c}(x) \) have equal number of nonzero components, so \( \text{wt}(p^{n-1}c(x)) = \text{wt}(\overline{c}(x)) \). Therefore,

\[
\text{d}(C) = \text{d}(\text{Tor}_{n-1}(C)).
\]

The Hamming distance, \( \text{d}(\text{Tor}_{n-1}(C)) \), is fully characterized in \([3,21]\). \( \square \)

3.3. Dual Codes

Let \( x = (x_0, x_1, \cdots, x_{N-1}) \) and \( y = (y_0, y_1, \cdots, y_{N-1}) \) in \( \mathbb{R}^N \); then, \( x \cdot y = x_0y_0 + x_1y_1 + \cdots + x_{N-1}y_{N-1} \) (usual dot product). Furthermore, \( x \) and \( y \) are said orthogonal when \( x \cdot y = 0 \). Now, suppose that \( C \) is a linear code over \( R \), the dual code of \( C \) is defined as:

\[
C^\perp = \{ x \mid x \cdot y = 0, \forall y \in C \}.
\]

Next, we mention the following already known results in \([2,19,20,22]\).

Proposition 6. Suppose that \( R \) is a finite chain ring of order \( p^r \). Then,

\[
| C | = p^r,
\]

where \( e \in \{0, 1, \cdots, zN\} \). In addition, \( C^\perp \) has order \( p^r \), where \( e + e' = zN \); that is,

\[
|C| \cdot |C^\perp| = |\mathbb{R}|^N.
\]

Proposition 7. The dual code of a cyclic code is cyclic.

Theorem 3. If \( C \) is a cyclic code over \( R \) of length \( p^s \), then \( C^\perp \) has a unique representation,

\[
C^\perp = \langle e'_0(x), pe'_1(x), \cdots, p^{n-1}e'_{n-1}(x) \rangle,
\]

where \( e'_i(x) = (x - 1)^{T'_i} + ph'_i(x) \) if \( T'_i < p^s \) and \( e'(x) = 0 \) otherwise. Furthermore, \( T'_i = p^s - T_{n-1-i}, 0 \leq i \leq n-1 \).

Proof. As \( C \) is a cyclic code over \( R \) with length \( p^s \), then, by Proposition 7, \( C^\perp \) is also cyclic with the same length; so, by Theorem 1 and Remark 1, \( C^\perp \) has a representation

\[
C^\perp = \langle e'_0(x), pe'_1(x), \cdots, p^{n-1}e'_{n-1}(x) \rangle,
\]

where \( e'_i(x) = (x - 1)^{T'_i} + ph'_i(x) \) and \( T'_i \) is the \( i \)-th torsion degree of \( C^\perp \). Based on definition of \( C^\perp \), \( p^{n-1-i}(x - 1)^{p^n-T_{n-i}} \in C^\perp, T'_{n-1-i} \leq p^s - T_{n-i}, 0 \leq i \leq m-1 \). Now, since \( |C| \cdot |C^\perp| = |\mathbb{R}|^{p^s} \) (Proposition 6), from Proposition 4,

\[
\sum_{i=0}^{n-1} T_i + \sum_{i=0}^{n-1} T'_i = np^s.
\]

This implies \( T'_i = p^s - T_{n-1-i} \). \( \square \)

4. Cyclic Codes of Length \( N \)

Throughout this section, we denote \( R_N = GR[p^n, r][x]/ < x^N - 1 > \) and \( R(r) = GR(p^n, r)[u]/ < u^{p^N} - 1 > \). Define \( \phi : R(r)^{n_1} \rightarrow R_N \) by:

\[
\phi(\sum_{i=0}^{p^{n_1}-1} c_{0,i}u^i, \cdots, \sum_{i=0}^{p^{n_1}-1} c_{n_1-1,i}u^i) = (c_{0,0}, \cdots, c_{n_1-1,0}, \cdots, c_{0,p^{n_1}-1}, c_{1,p^{n_1}-1} \cdots, c_{n_1-1,p^{n_1}-1}).
\]
Axioms 2022, 11, 519

Proposition 8 (Hensel’s shifting [20]). Assume $f$ is a monic polynomial in $\text{GR}(p^n, r)[x]$ and $\overline{f} = \overline{g_1}\overline{g_2}$ in $F_p[x]$, where $g_1, g_2$ are co-prime polynomials over $F_p$, so there are $f_1, f_2$ in $\text{GR}(p^n, r)[x]$ with $f = f_1f_2$ and $\overline{f_1} = g_1, f_2 = g_2$.

Remark 2. Hensel’s Lemma is a critical tool in the study of finite commutative chain rings, which ensures that factorization over $F_p$ lifts to that over $\text{GR}(p^n, r)$. We assume $(n_1, p) = 1$ so that $p$ has an inverse modulo $n_1$, i.e., $p^{n_1} \equiv 1 \pmod{n}$ for some positive integer, $r'$. It follows that $\text{GR}(p^n, r')$ contains a primitive $n_1$th root in unity and so does $\text{GR}(p^n, r_p)$. Then, Hensel’s Lemma implies that $\text{GR}(p^n, r')$ contains a primitive $n_1$th root $\alpha$; thus, $x^{n_1} - 1 = f_1(x) f_2(x) \cdots f_{s_1}(x)$ over $\text{GR}(p^n, r)$. For every $j, 0 \leq j \leq n_1 - 1$, there is only one $i, 0 \leq i \leq l$ with $f_i(\alpha^j) = 0$. The polynomial $f_i(x)$ is said to be minimal polynomial for $\alpha^j$ in $\text{GR}(p^n, r)[x]$.

Suppose that $r'$ is the order of $p$ modulo $n_1$, and $l$ is a set of all $p'$-cyclotomic closet representatives modulo $n_1$. Suppose also $\text{cl}_{r'}(b, n_1)$ is $p'$-cyclotomic closet modulo $n_1$ of $b$, and $r_{b} = |\text{cl}_{r'}(b, n_1)|$. Assume $\alpha$ is a $n_1$th primitive root in $\text{GR}(p^n, r)$.

4.1. Discrete Fourier Transform (DFT)

Discrete Fourier transform (DFT) is used when the codes length, $N$, is an arbitrary number not necessarily a power of primes; in our case, $N = n_1p^n$ and $(n_1, p) = 1$. This method has been widely utilized to investigate linear codes over finite rings, for instance see [1,4,5,12,23,24]. Next, we use DFT as an important key to describe the structure for cyclic codes over $\text{GR}(p^n, r)$.

Definition 4 (DFT). Assume $c \in \text{GR}(N)$ and $c(x) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{p-1} c_{ij}x^{i+jn_1}$ the corresponding polynomial. The DFT of $c(x)$ is

$$\hat{c}_0, \hat{c}_1, \cdots, \hat{c}_{n_1-1} \in \text{GR}(r')^{n_1},$$

where

$$\hat{c}_b = c(u^b\alpha^j) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{p-1} c_{ij}u^{i+jn_1} \alpha^bj,$$

$b \in I$ and $n_1n'(1) \equiv 1 \pmod{p^{s+n-1}}$. Moreover, the Mattson–Solomon of $c$ to be the polynomial:

$$\hat{c}(z) = \sum_{b=0}^{n_1-1} \hat{c}_b z^b.$$

Note that $\hat{c}_{n_1} = \hat{c}_0$.

We then illustrate that $c$ can be obtained from the Mattson–Solomon polynomial of $c$.

Lemma 1. Let $c \in \text{GR}(N)$, and let $\hat{c}(z)$ be its Mattson–Solomon polynomial. Thus,

$$c = \phi[(1, u^{-n'}, u^{-2n'}, \cdots, u^{-(n_1-1)n'}) * \frac{1}{n_1} (\hat{c}(1), \hat{c}(\alpha^1), \cdots, \hat{c}(\alpha^{n_1-1}))],$$

where $*$ means component-wise multiplication.

Proof. Suppose $0 \leq l' \leq n_1 - 1$. So,

$$\hat{c}(\alpha^{l'}) = \sum_{b=0}^{n_1-1} \hat{c}_b \alpha^{-bt'} = \sum_{b=0}^{n_1-1} (\sum_{i=0}^{n_1-1} \sum_{j=0}^{p-1} c_{ij} u^{i+jn_1} \alpha^bj) \alpha^{-bt'}$$

$$= \sum_{i=0}^{n_1-1} \sum_{j=0}^{p-1} c_{ij} u^{i+jn_1} \sum_{b=0}^{n_1-1} \alpha^b(i-t') = (n_1 u^{l'}) \sum_{j=0}^{p-1} c_{ij} u^{j}.$$
Axioms 2022, 11, 519

Note that $\sum_{i=0}^{n_1-1} a^i = 0$, when $j \neq 0$ (mod $n_1$). From the definition of $\phi$,

$$c = \phi[(1, u^{-n'}, u^{-2n'}, \cdots, u^{-(n_1-1)n'}) \ast \frac{1}{n_1}(\ell(1), \ell(a^1), \cdots, \ell(a^{n_1-1}))].$$

\[\square\]

4.2. The Representation of Cyclic Codes over R

Since $R(rr_b) = GR(p^n, rr_b)[u]/<u^{p^s} - 1>$, then $a^b$ and $c_{i,j}$ are elements of $R(rr_b)$, and thus by Equation (8), $\hat{c}_b = c(u^{n'} a^b) \in R(rr_b)$. Now,

$$\hat{c}_{p^rb} = \sum_{i=0}^{n_1-1} \sum_{j=0}^{p^s-1} c_{i,j}u^{n'i+j}a^{rb_i}$$

$$= \sum_{i=0}^{n_1-1} \sum_{j=0}^{p^s-1} \sigma(c_{i,j}u^{n'i+j}a^{rb_i})$$

$$= \sigma\left(\sum_{i=0}^{n_1-1} \sum_{j=0}^{p^s-1} c_{i,j}u^{n'i+j}a^{rb_i}\right)$$

$$= \sigma(c_b),$$

where $\sigma$ is the extension of the Frobenius automorphism $\rho$ from $GR(p^n, rr_b)$ onto $R(rr_b)$ by setting $\sigma(u) = u$ and the subscript are calculated modulo $n_1$. Now, let

$$A = \{(\hat{c}_0, \hat{c}_2, \cdots, \hat{c}_{n_1-1}) \in R(rr_b)^{n_1} \mid \hat{c}_b \in R(rr_b), \hat{c}_{p^rb} = \sigma(\hat{c}_b)\}. \quad (11)$$

By component-wise addition and multiplication, $A$ admits the structure of a ring. Moreover, one can see that $A \cong \bigoplus_{b \in I} R(rr_b)$.

**Theorem 4.** Suppose that $\gamma$ is a map $\gamma : R_N \rightarrow \bigoplus_{b \in I} R(rr_b)$ such that $\gamma(c(x)) = (\hat{c}_b)_{b \in I}$. Thus, $\gamma$ is an isomorphism. In addition, suppose $C$ is a cyclic code over $R$ of length, $N$,

$$C \cong \bigoplus_{b \in I} C_b, \quad (12)$$

where $C_b = \{c(u^{n'} a^b) \mid c(x) \in C\}$ which is a cyclic code over $GR(p^n, rr_b)$ with length $p^s$.

**Proof.** Let $\gamma : R_N \rightarrow A$, defined by $\gamma(c(x)) = (\hat{c}_0, \hat{c}_2, \cdots, \hat{c}_{n_1-1})$. Suppose $a(x)$ and $b(x)$ are in $R[x]$ such that their degrees are less than $N$. It follows that

$$\gamma(a(x) + b(x)) = \gamma(a(x)) + \gamma(b(x))$$

and

$$\gamma(a(x)b(x)) = \gamma(a(x)) \ast \gamma(b(x)).$$

Now, if $\gamma(c(x)) = 0$, we have by Lemma 1, $\Sigma_{j=0}^{p^s-1} c_{i,j}u^j = 0$, where $0 \leq t' \leq n_1 - 1$. This implies that $c(x) = 0$, and thus $\gamma$ is one-to-one. Note that

$$|A| = \prod_{b \in I} p^{rn_b p^s} = p^{rn_N}.$$ 

Therefore, $\gamma$ is a bijection, and hence $\gamma$ is an isomorphism. As $\gamma$ is a ring isomorphism, the second part is direct. \[\square\]

**Lemma 2.** For every $b \in I$, assume $f_b(x)$ is the minimal polynomial of $a^b$ and $n'$ satisfies $n_1 n' \equiv 1$ (mod $p^{s+n-1}$). Then,

(i) $f_b(u^{n'} a^i)$ is invertible when $i \notin \Omega(b, n_1)$. 

Axioms 2022, 11, 519

(ii) $f_b(u^n a^b) \in < u - 1 >$ but $f_b(u^n a^b) \not\in (u - 1)^2 >$.

**Proof.** (i) Assuming $f_b(x) = \prod_{l \in cl_R(b, n_1)} (x - a^l)$, then

$$f_b(u^n a^l) = \prod_{l \in cl_R(b, n_1)} (u^n a^l - a^l) = \prod_{l \in cl_R(b, n_1)} [(u^n - 1) a^l + (a^i - a^l)].$$

However, we have $a^i - a^l \neq 0$ if $i$ is not in $cl_R(b, n_1)$, and hence $(u^n - 1) a^l$ is not unit. Thus, $f_b(u^n a^l)$ is a unit if $i \notin cl_R(b, n_1)$. (ii) Because $x^{n_1} - 1 = \prod_{i \in I} f_i(x)$,

$$\prod_{i \in I} f_i(u^n a^k) = (u^n a^k)^{n_1} - 1 = u - 1.$$  

However, from (i) we have that $f_i(u^n a^k)$ is invertible if $i \neq b$. So, $f_b(u^n a^b) = a(u)(u - 1)$, when $a(u)$ is a unit of $R(rr_b)$. It follows that $f_b(u^n a^b) \in (u - 1)$. Suppose that $f_b(u^n a^b) \in < (u - 1)^2 >$. Hence, there is $q(u) \in GR(p^n, rr_b)[u]$ with $f_b(u^n a^b) = q(u)(u - 1)^2$, and thus $a(u)(u - 1) \in < (u - 1)^2 >$, i.e., $< u - 1 > \subseteq < (u - 1)^2 >$ but this is impossible, and the proof is finished. 

Suppose that $C$ is a cyclic code over $R$ with length, $N$. Theorem 4 claims that $C \cong \bigoplus_{b \in I} C_b$, $C_b$ is a cyclic code over $R(rr_b)$ of length $p^n$. Then, by Remark 1,

$$C_b = < e_{0,b}(u), p e_{1,b}(u), \ldots, p^{n-1} e_{n-1,b}(u) >,$$

where $e_{i,b}(u) = (u - 1)^{T_{i,b}} + p h_{i,b}(u)$. Let $i$ be fixed and $0 \leq j \leq p^s$, we denote $F_j(x)$ the multiplication of all minimal polynomials for $a^l$ with $Tor_i(C_b) = < (u - 1)^j >$. Note that Lemma 2 indicates

$$\prod_{j=0}^{p^s} [F_j(u^n a^b)]^j = a_b(u)(u - 1)^j,$$

where $a_b(u) \in R(rr_b)$ is invertible. Set

$$g_i(x) = \prod_{j=0}^{p^s} [F_j(x)]^j + p b_i(x),$$

where $b_i(x) = \gamma^{-1}((a_b(u) h_{i,b}(u))_{b \in I}).$

**Theorem 5.** If $C$ is a cyclic code over $R$ of length, $N$, then

$$C = < g_0(x), p g_1(x), \ldots, p^{n-1} g_{n-1}(x) >.$$  

Moreover, this representation is unique.

**Proof.** If $b \in I$, then $g_i(u^n a^b) \in < e_{i,b}(u) >$; hence, $p^i g_i(u^n a^b) \in C_b$. Moreover, for every $i$, $0 \leq i \leq n - 1$, $p^i g_i(x) \in C$. By Equations (13) and (14), $< g_i(u^n a^b) >=< e_{i,b}(u) >$. Thus, $g_0(x), p g_1(x), \ldots, p^{n-1} g_{n-1}(x)$ generate $C$ (Theorem 4). The last part is direct from the uniqueness of $h_{i,b}(u)$’s (Remark 1). 

**Corollary 3.** If $C = < g_0(x), p g_1(x), \ldots, p^{n-1} g_{n-1}(x) >$, then $|C| = p^{t'},$ where $t' = Nn - \Sigma_{j=0}^{p^n} \deg F_j$.

**Proof.** From Theorem 4, $|C| = \prod_{b \in I} |C_b|$, and $|C_b| = p^{t_b}(p^n - (T_{0,b} + T_{1,b} + \cdots + T_{n-1,b}))$. The result is concluded by computing the multiplication of $|C_b|$. 

From Theorem 5, we have the proof of the following.
Corollary 4. The enumeration of cyclic codes over \( R \) of length, \( N \), is
\[
\prod_{b \in I} N_b,
\]
where \( N_b \) is the enumeration of distinct cyclic codes over \( GR(p^n, r, r_b) \) with length \( p^i \).

Theorem 6. Let \( n = 2 \); then, the enumeration of cyclic codes over \( R \) of length, \( N \), is
\[
\prod_{b \in I} \left( \frac{p^{r(2z_b+1)} - 1}{p^r - 1} \right),
\]
where \( z_b = \min\{\left\lfloor \frac{d_b}{r} \right\rfloor, p^r - 1 \} \), such that \( T_0(C_b) + T_1(C_b) = d_b \leq p^r \).

Proof. From Corollary 4, we only need to determine \( N_b, b \in I \). Moreover, by (Corollary 3.9, [13]),
\[
N_b = \frac{p^{r(2z_b+1)} - 1}{p^r - 1},
\]
where \( z_b = \min\{\left\lfloor \frac{d_b}{r} \right\rfloor, p^r - 1 \} \), \( T_0(C_b) + T_1(C_b) = d_b \leq p^r \). Thus, the result follows. \( \Box \)

4.3. Torsion Codes and Hamming Distance

This subsection deals with torsion codes for cyclic codes over \( R \), and their Hamming distances.

Lemma 3. Suppose \( C = < g_0(x), pg_1(x), \ldots, p^{n-1}g_{n-1}(x) > \) and \( p^i(h(x)) \in C \) with \( h(x) \in Tor_i(C) \). Thus, \( \deg g_i \leq \deg h \).

Proof. If \( p^i(h(x)) \in C \), then \( p^i(h(u^n a^b)) \in C \), \( b \in I \), \( n_1 n' \equiv 1 \) \( (mod \ p^{s+n-1}) \). Since \( h(x) \in Tor_i(C) \), \( h(u^n a^b) \in Tor_i(C_p) \). It follows that, \( h(u^n a^b) = c(u)(u-1)^T_i \), where \( c(u) \in R(rr_b) \) is unit. Moreover, if \( g(x) = p(x) \prod_{j=0}^{p^i} [F_j(x)]^l \), (see Theorem 5), and if \( p(x) = \gamma^{-1}(c_p(u)a_b^{-1}(u))x(1) \), then—for \( b \in I \)—\( g(u^n a^b) = c(u)(u-1)^T_i \) by Equation (13); thus, \( \gamma(h(x)) = \gamma(g(x)) \), which leads to \( h(x) = g(x) \), i.e., \( \deg h = \deg g \). Hence, \( \deg g \geq \deg \prod_{j=0}^{p^i} [F_j(x)]^l = \deg g_i \) from Equation (14). \( \Box \)

Theorem 7. Assume \( C = < g_0(x), pg_1(x), \ldots, p^{n-1}g_{n-1}(x) > \), \( Tor_i(C) = < \overline{g_i}(x) > \).

Proof. Since \( p^i g_i \in C \), \( \overline{g_i}(x) \subseteq Tor_i(C) \). On the other hand, assume \( h(x) \in Tor_i(C) \), then \( p^i h(x) \in C \) from the definition of \( Tor_i(C) \). In light of Lemma 3, \( \deg h \geq \deg g_i \). Now, there exist \( r(x) \) and \( q(x) \) in \( R_N \) satisfying \( h(x) - g_i(x)q(x) = r(x) \), where \( r(x) = 0 \) or \( \deg r < \deg g_i \) (division algorithm). Because \( p^i r(x) \in C \), so \( r(x) = 0 \) from the minimality of \( \deg g_i \). This means that \( h(x) \in < g_i(x) > \), and hence \( h(x) \in < \overline{g_i}(x) > \). Thus, \( Tor_i(C) \subseteq < \overline{g_i}(x) > \). \( \Box \)

Theorem 8. If \( C \) is a cyclic code over \( R \) of length, \( N \), then
\[
d(C) = d(Tor_{n-1}(C)).
\]

Proof. A similar argument to that of Theorem 2, where leads to \( d(C) = d(Tor_{n-1}(C)) \), is present, where \( Tor_{n-1}(C) = < \overline{g_{n-1}}(x) > = < \prod_{j=0}^{p^{n-1}} F_j(x) > \) (Theorem 7). \( \Box \)
4.4. Dual Codes

Let \( F_i(x) \) maintain the same definition as in Theorem 5. Assume also \( a_j \) is the constant term of \( F_i(x) \), where \( 0 \leq j < p^t \). Because \( \prod_{j=0}^{p^t} F_i(x) = x^{n_1} - 1 \), \( \prod_{j=0}^{p^t} a_j = -1 \). Thus, \( a_j \)'s are invertible and leading coefficients for \( F_i(x) = x^{\deg F_i} F_i(x^{-1}) \). Suppose

\[
m_j(x) = a_j^{-1} F_i(x).
\]  

(18)

Note that \( m_j(x) \) is monic polynomial with \( \prod_{j=0}^{p^t} a_j^{-1} = -1 \). So,

\[
\prod_{j=0}^{p^t} m_j(x) = \left( \prod_{j=0}^{p^t} a_j^{-1} \right) \prod_{j=0}^{p^t} F_i(x) = -x^{\sum_{j=0}^{\deg F_i} F_i(x)} \prod_{j=0}^{p^t} F_j(x^{-1}) = -x^{n_1}(x^{-n_1} - 1) = x^{n_1} - 1.
\]

In other words, the polynomials \( m_j(x) \) are monic co-prime divisors of \( x^{n_1} - 1 \) over \( R \). As \( \text{Tor}_i(C_b) = < (u - 1)^l >, F_j(x^b) = 0 \), which gives \( F_i(x^{a_n} - b) = 0 \). Hence, \( m_j(x^{a_n} - b) = 0 \). Therefore, \( m_j(x) \) is the multiplication of all minimal polynomials for \( a^{n_1} - b \), satisfying

\[
\text{Tor}_i(C_b^\perp) = < (u - 1)^{p^t} >.
\]

By Lemma 2,

\[
\prod_{j=0}^{p^t} \left[ F_j^\ast(u^{a_n} - b)^{p^t - j} \right] = a_b(u)(u - 1)^{p^t - j},
\]

(19)

where \( a_b(u) \in R(\mathfrak{r}_b) \) is a unit. Set

\[
G_i(x) = \prod_{j=0}^{p^t} \left[ F_j^\ast(x) \right]^{p^t - j} + pc_i(x),
\]

(20)

where \( c_i(x) = \gamma^{-1}((a_b(u)h_{i,b}(u))_{b \in I}) \) and let \( h_{i,b}(u) \) as in Theorem 3.

**Theorem 9.** If \( C \) is a cyclic code over \( R \) with length, \( N \), then

\[
C^\perp = < G_0(x), pG_1(x), \ldots, p^{n-1}G_{n-1}(x) >.
\]

In addition, \( |C^\perp| = p^{tl'}, \) where \( t' = \sum_{j=0}^{\deg F_i} \).

**Proof.** Note that \( C = \oplus_{b \in I} C_{b, b} \) is a cyclic code over \( GR(p^n, \mathfrak{r}_b) \) of length \( p^s \). Suppose that \( D = \oplus_{b \in I} C_{b}^\perp \). Then, \( D \subseteq C^\perp \). Moreover, we have \( |C_b| : |C_b^\perp| = p^{r\delta} \). So, \( |C| : |D| = p^{rnN} \), and then

\[
C^\perp = D = \oplus_{b \in I} C_{b}^\perp.
\]

Thus, by an argument similar to that of Theorem 5, we have

\[
C^\perp = < G_0(x), pG_1(x), \ldots, p^{n-1}G_{n-1}(x) >,
\]

where \( G_i(x) \) is known in (20) and \( 0 \leq i \leq n - 1 \). From Corollary 3 and from the formula \( |C^\perp| : |C| = p^{rnN} \), we obtain \( |C^\perp| = p^{tl'}, \) where \( t' = \sum_{j=0}^{\deg F_i} \). \( \Box \)
To sum up, the section presents an algorithm for creating a structure for cyclic codes with length $n_1p^s$ using those of length $p^s$. The following steps might be helpful in this regard.

1. Obtain $a$, $I$ and $r_b$, $b \in I$.
2. For every $0 \leq j \leq p^s$, find $F_j(x)$ if $i$ is fixed.
3. Use Equation (13) to compute $a_b(x)$, $b \in I$.
4. By using $b_j(x) = \gamma^{-1}((a_b(u)h_i(u))_{b \in I})$, determine $b_j(x)$, where $0 \leq i \leq n - 1$.
5. Finally, obtain $g_j(x)$ by the formula (14).

We next give some examples clarifying the above steps.

**Example 3.** Suppose $R = \mathbb{Z}_4$ and $N = 6$. Then, $n_1 = 3$, $I = \{0, 1\}$, $r_0 = 1$ and $r_1 = 2$. Let $C_0 = \langle (u - 1), 2(u - 1) \rangle$ and $C_1 = \langle (u - 1), 2 \rangle$ be cyclic codes over $\mathbb{Z}_4$ and $GR(4, 2)$ with length 2, respectively. First, find $F_j(x)$ for $i = 0$. Because $T_0(C_0) = 1 = T_0(C_1)$,

$$
\begin{cases}
F_0(x) = 1, \\
F_2(x) = 1, \\
F_1(x) = f_0(x)f_1(x) = (x - 1)(x - \alpha)(x - \alpha^2) = x^3 - 1,
\end{cases}
$$

where $\alpha$ is satisfying $\alpha^2 + \alpha + 1 = 0$ (primitive root). Since $h_{0,0}(x) = h_{0,1}(x) = 0$, so $b_0(x) = 0$, and hence

$$g_0(x) = \prod_{j=0}^{2} F_j(x)^j = x^3 - 1.
$$

Second, determine $F_j(x)$ with $i = 1$. As $T_1(C_0) = 1$ and $T_1(C_1) = 0$, it follows that

$$
\begin{cases}
F_0(x) = (x - \alpha)(x - \alpha^2) = x^2 + x + 1, \\
F_1(x) = (f_0(x)) = (x - 1), \\
F_2(x) = 1.
\end{cases}
$$

As $b_1(x) = 0$ since $h_{1,0}(x) = 0 = h_{1,1}(x)$,

$$g_1(x) = \prod_{j=0}^{2} F_j(x)^j = x - 1.
$$

**Theorem 5** implies that

$$C = \langle x^3 - 1, 2(x - 1) \rangle.
$$

**Example 4.** Let $C_0 = \langle (u - 1) + 2, 2(u - 1) \rangle$ and $C_1 = \langle (u - 1)^2, 2(u - 1) \rangle$ be cyclic codes of length 2 over $\mathbb{Z}_4$ and $GR(4, 2)$, respectively. We will construct a cyclic code $C$ over $\mathbb{Z}_4$ with length 6 by $C_0$ and $C_1$. First, note that $T_0(C_0) = 1$ and $T_0(C_1) = 2$, then

$$
\begin{cases}
F_0(x) = 1, \\
F_1(x) = x - 1, \\
F_2(x) = (x - \alpha)(x - \alpha^2) = x^2 + x + 1.
\end{cases}
$$

Simple calculation yields,

$$\prod_{j=0}^{2} F_j(x)^j = x^5 + x^4 + x^3 - x^2 - x - 1.
$$

Furthermore, $b_0(x) = x^2 + x + 1$. Hence,

$$g_0(x) = x^5 + x^4 + x^3 + x^2 + x + 1.
$$
Next, we construct \( g_1(x) \). Observe that \( T_1(C_0) = 1 \) and \( T_1(C_1) = 1 \), so
\[
\begin{align*}
F_0(x) &= 1, \\
F_1(x) &= (x - 1)(x - a)(x - a^2) = (x - 1)(x^2 + x + 1) = x^3 - 1, \\
F_2(x) &= 1.
\end{align*}
\]

Moreover,
\[
g_1(x) = \prod_{j=0}^{2} F_j(x)^j = x^4 - x^3 - x + 1,
\]
and thus,
\[
C = \langle x^5 + x^4 + x^3 + x^2 + x + 1, 2(x^3 - 1) \rangle.
\]
(22)

**Remark 3.** Similar processes can be used to describe the generators of dual codes—that is, replace \( C_b \) with \( C_b^\perp \), \( b \in \mathbb{F} \).

**Example 5.** Consider \( R, N, C_0 \) and \( C_1 \) as in Example 3. We want to construct \( C_1^\perp \) for \( C \) given in Equation (21). First note that
\[
\begin{align*}
C_0^\perp &= \langle u - 2, 2(u - 1) \rangle, \\
C_1^\perp &= \langle 2(u - 1) \rangle.
\end{align*}
\]
Let \( i \) be fixed, then consider \( T_{n-i-1}(C_b) \) instead of \( T_i(C_b) \) and \( b \in \mathbb{I} \). If \( i = 0 \), by the definition of \( F_i(x) \), then
\[
\begin{align*}
T_0(C_0) &= 1, T_1(C_1) = 0, \\
F_0(x) &= x^2 + x + 1, & F_0^*(x) &= x^2 + x + 1, \\
F_1(x) &= x - 1, & F_1^*(x) &= 1 - x, \\
F_2(x) &= 1, & F_2^*(x) &= 1.
\end{align*}
\]
Since \( G_0(x) = \prod_{j=0}^{n-1} [F_j^*(x)]^{2-j} + 2b_0(x) \), then
\[
G_0(x) = (x^2 + x + 1)(1 - x^3),
\]
where \( b_0(x) = x^2 + x + 1 \). On the other hand, suppose that \( i = 1 \),
\[
\begin{align*}
T_0(C_0) &= 1, T_0(C_1) = 1, \\
F_0(x) &= 1, & F_0^*(x) &= 1, \\
F_1(x) &= (x - 1)(x^2 + x + 1) = x^3 - 1, & F_1^*(x) &= 1 - x^3, \\
F_2(x) &= 1, & F_2^*(x) &= 1.
\end{align*}
\]
Hence,
\[
G_1(x) = \prod_{j=0}^{2} [F_j^*(x)]^{2-j} = 1 - x^3.
\]
Therefore,
\[
C_1^\perp = \langle G_0(x), pG_1(x) \rangle = \langle (x^2 + x + 1)(1 - x^3), 2(1 - x^3) \rangle.
\]
(23)

Note that one can easily verify that \( (x^2 + x + 1)(1 - x^3)C = 0 \) and \( 2(1 - x^3)C = 0 \).
Example 6. Suppose we have the same $R,N,C_0,C_1$ as in Example 4. The aim is to find $C^\perp$ of $C$ presented in Equation (22). Observe that

$$
\begin{align*}
C_0^\perp &= \langle (u - 1), 2(u - 1) \rangle, \\
C_1^\perp &= \langle (u - 1) \rangle.
\end{align*}
$$

Assume that $i = 0$, then for $F_j(x)$ we have

$$
\begin{align*}
T_1(C_0) &= 1, T_1(C_1) = 1, \\
F_0(x) &= 1, \\
F_1(x) &= (x - 1)(x^2 + x + 1), \\
F_2(x) &= 1.
\end{align*}
$$

Since $G_0(x) = \prod_{j=0}^{2} [F_j^*(x)]^{2^{-j}} + 2c_0(x)$, then

$$
G_0(x) = (1 - x)(x^2 + x + 1),
$$

where $c_0(x) = 0$. Next, let $i = 1$,

$$
\begin{align*}
T_0(C_0) &= 1, T_0(C_1) = 2, \\
F_0(x) &= 1, \\
F_1(x) &= (x - 1), \\
F_2(x) &= x^2 + x + 1.
\end{align*}
$$

Thus,

$$
G_1(x) = \prod_{j=0}^{2} [F_j^*(x)]^{2^{-j}} = (1 - x)(x^2 + x + 1),
$$

and so

$$
C^\perp = \langle (1 - x)(x^2 + x + 1), 2(1 - x)(x^2 + x + 1) \rangle. \quad (24)
$$

5. Conclusions

In the present paper, we utilized the discrete Fourier transform (DFT) approach to uniquely express a representation for cyclic codes over $GR(p^n,r)$. By using this representation, we were able to find dual codes and Hamming distances. In addition, we gave the enumeration of cyclic codes of length, $N$, in terms of that of length $p^s$, $v_p(N) = s$. When $n = 2$, the exact number of such codes is provided.

Author Contributions: Conceptualization, S.A. and Y.A.; methodology, S.A. and Y.A; investigation, S.A. and Y.A; writing—original draft preparation, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank the Deanship of scientific research in King Saud University for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References