axioms

MDPI

Article

MacWilliams Identities and Generator Matrices for Linear Codes over $\mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$

Sami Alabiad [1,*], Alhanouf Ali Alhomaidhi [1] and Nawal A. Alsarori [2]

[1] Department of Mathematics, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia; aalhomaidhi@ksu.edu.sa
[2] Department of Mathematics, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad 431004, India; n_alsarori@yahoo.com
* Correspondence: ssaif1@ksu.edu.sa

Abstract: Suppose that $R = \mathbb{Z}_{p^4}[u]$ with $u^2 = p^3\beta$ and $pu = 0$, where p is a prime and β is a unit in R. Then, R is a local non-chain ring of order p^5 with a unique maximal ideal $J = (p, u)$ and a residue field of order p. A linear code C of length N over R is an R-submodule of R^N. The purpose of this article is to examine MacWilliams identities and generator matrices for linear codes of length N over R. We first prove that when $p \neq 2$, there are precisely two distinct rings with these properties up to isomorphism. However, for $p = 2$, only a single such ring is found. Furthermore, we fully describe the lattice of ideals of R and their orders. We then calculate the generator matrices and MacWilliams relations for the linear codes C over R, illustrated with numerical examples. It is important to address that there are challenges associated with working with linear codes over non-chain rings, as such rings are not principal ideal rings.

Keywords: MacWilliams identities; coding over rings; local rings; generator matrices

MSC: 16L30; 94B05; 16P20; 94B60

check for updates

Citation: Alabiad, S.; Alhomaidhi, A.A.; Alsarori, N.A. MacWilliams Identities and Generator Matrices for Linear Codes over $\mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$. *Axioms* **2024**, *13*, 552. https://doi.org/10.3390/axioms13080552

Academic Editor: Hashem Bordbar

Received: 21 July 2024
Revised: 7 August 2024
Accepted: 8 August 2024
Published: 14 August 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Linear codes of length N over a finite ring R are R-submodules of R^N. These codes have been traditionally studied over finite fields; however, many significant codes over fields have been related to those over finite rings by Gray maps [1–4]. In this article, all of the alphabet rings involved are finite, commutative, and have an identity. A ring R is called local if it has a unique maximal ideal, denoted by J (Jacobson radical). When all ideals of R are principal, R is then called the principal ideal ring (PIR). A chain ring is a principal local ring, and thus many conclusions obtained for coding over chain rings also hold over PIRs. One of the main reasons that Frobenius rings, defined later, are considered the appropriate class to describe codes is because they satisfy both MacWilliams theorems. Furthermore, Frobenius local rings can be decomposed into their component parts and this enables us to find their generating characters. To fully understand codes over Frobenius rings, it is therefore necessary, despite the challenges, to consider local non-chain rings [5–7]. For more information on the subject, please refer to [5,8–11] and the references therein.

In this work, the main purpose is to obtain significant coding results over Frobenius local rings. In particular, linear codes of length N over the ring $\mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$, are the focus of this paper. Prior work on these rings was presented in [12], emphasizing their applicability to coding theory, and their close connection to $\mathbb{Z}_{p^n}$ and linear binary codes [3]. Our attention is also on exploring the roles of generator matrices and MacWilliams relations in error-correction theory, particularly in their role to weight enumerators of a code and its dual code. The authors of [6] considered these approaches for Frobenius local rings of order 16. While in [7], generator matrices and the MacWilliams relations were described for codes

over rings of order 32. This work makes an effort to build on the previous findings and provides access to more general rings with higher orders. Let $R = \mathbb{Z}_{p^4}[u]$, with $u^2 = \beta p^3$ and $pu = 0$ as conditions, where $\beta \in U(R)$, the unite group of R. Initially, we provide a formula for a generating character χ associated with R, through which we can calculate the MacWilliams relations as matrices of specific sizes for a code C over R. For codes over non-chains, it is more challenging to build a generator matrix G than for codes over chains. Although a simple set of generators can still be found, this type of generator matrix may not provide straightforward information about the code size. In this research, we introduce multiple numerical examples that show the code size might not always determined directly from such a generator matrix. Additionally, the generator matrix G of a code C is completely determined through the algorithm described in Theorem 8.

In Section 3, the classification of rings of the form $\mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu)$, with invariants $p, n, 1, 1, n-1$ is described, after the initial definitions and results in Section 2. Particular attention is given to providing all the details necessary to characterize rings of order p^5 and to outline the lattice of their ideals. Section 4 provides the general procedure for generating characters for $\mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$. Additionally, the symmetrized weight enumerator's corresponding to the matrix is acquired, and MacWilliams relations are derived. In Section 5, the findings regarding matrices that produce linear codes over such rings are presented.

2. Preliminaries

The notations and basic information that will be used later in our discussion are introduced in this section. Let R be a local ring of identity, and let J be its maximal ideal. For the results mentioned in this section, we refer readers to [4,12–16].

The order of J is $p^{(m-1)r}$ provided $J^m = 0$, and the size of R, is $|R| = p^{mr}$ with $R/J \cong GF(p^r) = F$. In R, the characteristic takes the form p^n, and $1 \leq n \leq m$. Additionally, R has a subring R_0, of the form $GR(p^n, r)$, called a Galois ring with p, n, r. Moreover, there is $u \in J$, and

$$\begin{aligned} R &= R_0 + uR_0, \\ J &= pR_0 + uR_0. \end{aligned} \tag{1}$$

If J is principal, then R is chain, and particularly when $J = (p)$, we have $n = m$ and

$$R = \mathbb{Z}_{p^n}[\alpha] \cong \mathbb{Z}_{p^n}[x]/(g(x)),$$

where α is a root of a specific polynomial $g(x) \in \mathbb{Z}_{p^n}[x]$. Let

$$\begin{aligned} \Gamma(r) &= (\alpha) \cup \{0\} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^r-2}\}; \\ \Gamma^*(r) &= (\alpha) = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^r-2}\}. \end{aligned}$$

Suppose $\gamma \in R$, so

$$\gamma = \alpha_1 + p\alpha_1 + p^2\alpha_2 + \cdots + p^{n-1}\alpha_{n-2} \quad \text{(p-adic expression)}. \tag{2}$$

where $\alpha_i \in \Gamma(r)$. Furthermore, assume that t is the smallest number with condition of $p^t u = 0$. We label p, n, r and t as the parameter (invariants) of R.

In our later discussion, we use $r = 1$ and $t = 1$. This implies that $R_0 = \mathbb{Z}_{p^n}$ and $pu = 0$. In addition, we consider $g(x)$ as

$$g(x) = x^2 - p^{(n-1)}\beta, \tag{3}$$

where $\beta \in \Gamma^*(1)$. From [12],

$$R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{(n-1)}\beta, pu),$$

where $(p, n, r, t, d) = (p, n, 1, 1, n-1)$.

The total sum of all minimal ideals in R is what we define as the socle of R, also known as $\mathrm{soc}(R)$. As R is commutative, thus

$$soc(R) = \{v \in R : v \in \ \mathrm{ann}(J)\},$$
$$\mathrm{ann}(J) = \{a \in R : ay = 0, \text{ for all } y \in J\}.$$

We will highlight the definition of Frobenius rings that is most pertinent to our analysis. In [14], R is called Frobenius if

$$R/J \cong soc(R).$$

Let $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^*)$ denote the character group of $(R, +)$, then elements of $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^*)$ are called characters χ of $(R, +)$. If $\ker\chi$ has no non-trivial ideals of R, then χ is named a generating character.

Theorem 1 (Honold [14]). *Let R be a finite ring. Then, $soc(R)$ is cyclic, if and only if R is a Frobenius ring.*

A code C of length N over R is a subset of R^N; it is called a linear code if C is a submodule [4]. Furthermore, by including the inner-product $(\cdot)$ in R^N, we can define the dual code $C^{\perp}$ of C as follows

$$C^{\perp} = \{\mathbf{u} : \mathbf{c} \cdot \mathbf{u} = 0, \mathbf{c} \in C\}. \tag{4}$$

3. On the Ring $\mathbb{Z}_{p^n}[u]/(u^2 - p^{(n-1)}\beta, pu)$

In this section, we prove some results on the ring $R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{(n-1)}\beta, pu)$ which is a finite ring of order p^{n+1} and with residue field $F = \mathbb{Z}_p$. These results help us in the subsequent discussion.

Theorem 2. *The ring $R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu)$ is a Frobenius local ring.*

Proof. As each element of R is uniquely written $a + bu$, where $a \in \mathbb{Z}_{p^n}$ and $b \in \Gamma(1)$. Also, as $J = (p, u)$, then R is a local ring of order p^{n+1} and $J^n = 0$. In fact, R is a local ring with a singleton basis and $p, n, 1, 1$. We now prove that R is Frobenius. Because elements of $\mathrm{soc}(R)$ annihilates $J = (p, u)$, particularly $pu = 0$, $p^{n-1}p = 0$, then $p^{n-1}J = 0$. Thus, $p^{n-1} \in \mathrm{soc}(R)$. Suppose $x \in \mathrm{soc}(R)$ and $x \neq 0$. Then, $xJ = 0$; in particular, $xu = 0$. This implies that $x \in (p)$, but as $xp = 0$ will also lead to $x \in (p^{n-1})$. Hence,

$$soc(R) = (p^{n-1}).$$

Using Theorem 1, R is Frobenius. □

Corollary 1. *As $J = (p, u)$, then R is a non-chain singleton ring.*

Remark 1. *For any Frobenius local ring R with invariants p, n, r and $t = 1$, then*

$$soc(R) = (p^{n-1}).$$

3.1. Determination of Rings of Order p^{n+1} with $p, n, 1, 1, n-1$

An exhaustive characterization of all rings with $p, n, 1, 1, n-1$ is given by Theorem 3, which is essential for our upcoming discussion.

Theorem 3. *Assume that R is a ring and that $(p, n, r, t, d) = (p, n, 1, 1, n-1)$ is its invariant. Then, among the rings given in Table 1, R is isomorphic to one particular ring.*

Table 1. Rings of order p^{n+1} with $p, n, 1, 1, n-1$.

$p \neq 2$	$p = 2$
$R_1 = \mathbb{Z}_{p^4 n}[u]/(u^2 - p^{n-1}\beta, pu)$	
$R_2 = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}, pu)$	$R_3 = \mathbb{Z}_{2^n}[u]/(u^2 - 2^{n-1}, 2u)$

Proof. Every element of R is uniquely expressed as $a + bu$, where $a \in \mathbb{Z}_{p^n}$ and $b \in \Gamma(1)$. As $pu = 0$, then the associated polynomial is of the form $g(x) = x^2 - p^{n-1}\beta$, where $\beta \in \Gamma^*(1)$. Suppose that $p = 2$. As $\Gamma^*(1) = \{1\}$, hence there exists precisely one class represented by

$$R_3 = \mathbb{Z}_{2^n}[u]/(u^2 - 2^{n-1}, 2u).$$

From now, we assume that $p \neq 2$. Consider the usual partition on $\Gamma^*(1)$.

$$A = \{\beta \in \Gamma^*(1) : \beta \notin \Gamma^*(1)^2\};$$
$$B = \{\beta \in \Gamma^*(1) : \beta \in \Gamma^*(1)^2\}.$$

It is worth noting that $| A | = \frac{p-1}{2} = | B |$. We next proceed the proof with two cases.
Case a. We show that R_1 and R_2 are not isomorphic, that is, they are not in the same class when $\beta \in A$. In contrast, suppose that $R_1 \cong R_2$, and define the isomorphism as ϕ. Assuming $J(R_2) = (p, v)$, for some $\beta' \in \Gamma^*(1)$, $\phi(u) = \beta' v$. Consequently, we note

$$\begin{aligned}
(\phi(u))^2 &= \phi(u^2) \\
(\beta' v)^2 &= \phi(p^{n-1}\beta) \\
\beta'^2 v^2 &= p^{n-1}\phi(\beta) \\
\beta'^2 (p^{n-1}) &= p^{n-1}\phi(\beta) \\
p^{n-1}\beta'^2 &= p^{n-1}\phi(\beta) \\
\beta'^2 &= \phi(\beta).
\end{aligned}$$

We have $\phi(\beta) = \beta$, because ϕ restricted to $\Gamma(1)$ is a fixed isomorphism. Furthermore, because $p \neq 2$, this contradicts the assumption about β, and thus $\beta \neq \beta'^2$. Therefore, $R_1 \ncong R_2$.
Case b. When $\beta \in B$. In such a case, there exists $\beta_1 \in \Gamma^*(1)$ such that $\beta = \beta_1^2$. Note that

$$\begin{aligned}
g(x) &= x^2 - p^{n-1}\beta \\
&= x^2 - p^{n-1}\beta_1^2 \\
&= \beta_1^2[(\beta_1^2)^{-1}x^2 - p^{n-1}] \\
&= \beta_1^2[(\beta_1^{-1}x)^2 - p^{n-1}].
\end{aligned}$$

As u is a root of $g(x)$, then $g(u) = 0$, and hence $u^2 - p^{n-1}\beta = 0$. This implies that, from the above argument, $\beta_1^2[(\beta_1^{-1}u)^2 - p^{n-1}] = 0$. Thus, $(\beta_1^{-1}u)^2 - p^{n-1} = 0$. This suggests that $g(x)$ for R_1 can be taken as $g(x) = x^2 - p^{n-1}$, which is identical to that of R_2. As a result, $R_1 \cong R_2$. To sum up, we have two classes of such rings that are not isomorphic

$$\Omega_1 : \text{ All rings with associated polynomials } g(x) = x^2 - p^{n-1}\beta, \text{ where } \beta \in A;$$
$$\Omega_2 : \text{ All rings with associated polynomials } g(x) = x^2 - p^{n-1}\beta, \text{ where } \beta \in B.$$

The first class is represented by

$$R_1 = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu),$$

where β is any element in A. While the second class is represented by

$$R_2 = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}, pu).$$

□

Corollary 2. *Let $N(p,4,1,1,3)$ be the number rings with $(p,4,1,1,3)$. Then,*

$$N(p,4,1,1,3) = \begin{cases} 1, & \text{if } p = 2; \\ 2, & \text{if } p \neq 2. \end{cases}$$

Proof. The proof is direct from the proof of Theorem 3 with $n = 4$ and $d = n - 1$. □

3.2. Lattice of Ideals of R

Theorem 4. *The ideals of R is given by the following lattice (see Figure 1).*

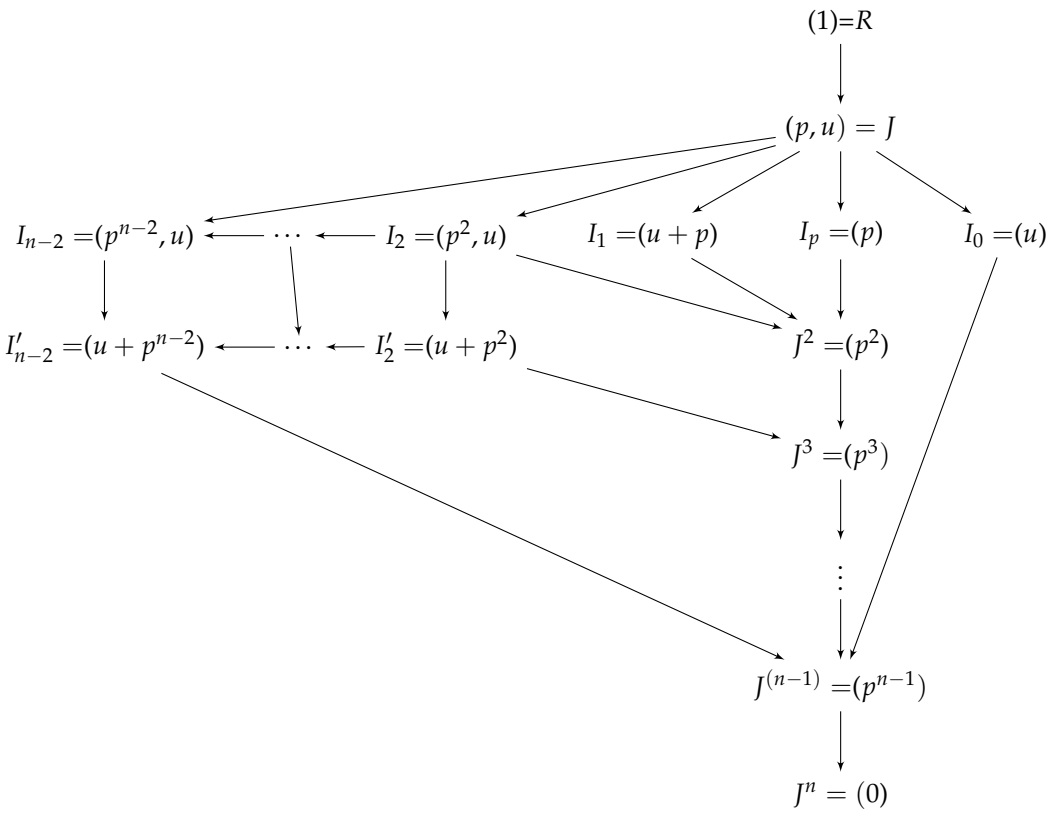


Figure 1. Lattice of ideals of $R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu)$.

Proof. Consider a proper ideal of R, I. As R is local, J represents the only maximal ideal of R; hence, $I \subseteq J$. This indicates that I is generated by a combination of p and u and their powers. Given that $pu = 0$ and $u^2 = \beta p^{n-1}$, we have $(p^i + u^2) = (p^i, u^2) = (p^j)$, where $j = \min\{i, n-1\}$. Thus, we only consider ideals generated by p^i and u and their combinations. In other words, without raising J to a power, there are only n choices for I, namely

$$(1), (p^i), (vp^i + u), (p^i, u),$$

where $v \in U(R)$ and $i = 1, 2, \ldots, n$. First, note that $(vp^i + u) = (p^i + w)$, where $w = v^{-1}u$. It is clear that $(p^i + u) \subset (p^i, u)$ and $(p^i, u) \subset (p^j, u)$, and, moreover, $(p^i + u) \subset (p^j + u)$, where $i > j$. Thus, if $I_i = (p^i, u)$ and $I_i' = (p^i + u)$,

$$\begin{aligned} &I_{n-2} \subset I_{n-3} \subset \cdots \subset I_2 \subset I_1; \\ &I_{n-2}' \subset I_{n-3}' \subset \cdots \subset I_2' \subset I_1'; \\ &I_i' \subset I_i. \end{aligned}$$

As $u^2 = \beta p^{n-1}$, thus $I_{n-1} = (p^{n-1}, u) = (p^{n-1} + u) = (u) = I_0$. Finally, we justify that $J^i = (p^i)$, where $i > 1$. As $pu = 0$, then $J^i = (p^i, u^i)$. If $i = 2$, then $J^2 = p^2(1, p^{n-3}\beta) = (p^2.)$ Now, if $i > 2$, then $u^i = 0$, and hence $J^i = (p^i)$. Therefore, the results follow. □

Corollary 3. *Suppose R as in Theorem 4. Then, for* $i = 1, 2, \ldots, n$,

$$| I | = \begin{cases} p^{n+1}, & \text{if } I = R; \\ p^n, & \text{if } I = J; \\ p^{n-1}, & \text{if } I = I_p; \\ p^2, & \text{if } I = I_0; \\ (p-1)p^{n-i}, & \text{if } I = I_i; \\ p^{n-i-1} & \text{if } I = I_i'; \\ p^{n-i} & \text{if } I = J^i. \end{cases}$$

Remark 2. *Two non-isomorphic rings can have the same ideal lattice.*

Remark 3. *Theorem 4 states that every ideal of R contains soc*(R).

Example 1. *The ring* $\mathbb{Z}_{3^4}[u]/(3^2 - 27, 3u)$ *is a Frobenius local non-chain ring. Because* $d = 3$, $t = 1$, *the assumption of Theorem 2. Note that soc*$(R) = (3^3)$ *and* $| \, soc(R) \, | = | \, F \, |$.

3.3. Units of $R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu)$

The form of the units of R will be established in this subsection, which will be useful in the following section. The elements in $R \setminus J$ are the units of R, as R is local. Furthermore, because $J = (p, u)$, if $\alpha \in R \setminus J$,

$$\alpha = a + bu, \tag{5}$$

where $a \in \mathbb{Z}_{p^n}$, $(a, p) = 1$ and $b \in R$. The elements of $\mathbb{Z}_{p^n}$ can be written as

$$a = \alpha_1 + p\alpha_2 + p^2\alpha_3 + \cdots + p^{n-1}\alpha_n,$$

where $\alpha_1 \in \Gamma(1)^*$ and $\alpha_i \in \Gamma(1)$, for $i = 2, 3, \ldots, n$. Thus, $\alpha \in U(R)$ can be expressed as

$$\alpha = \beta + wx, \tag{6}$$

where $\beta \in \Gamma(1)^*$, $w \in R$ and $x \in J$. In other words,

$$\alpha = \beta h, \tag{7}$$

where $h = 1 + w\beta^{-1}x \in H = 1 + J$. Moreover, observe that $\Gamma(1)^* \cap H = 1$, as $(p - 1, p^n) = 1$. Consequently, the following theorem is established.

Theorem 5. *Every element v of* $U(R)$ *is of the form* $v = x$ *or* $v = x + \alpha u$, *where* $(x, p) = 1$ *and* $\alpha \in \Gamma(1)^*$. *Moreover,* $U(R)$ *is of order* $(p - 1)p^n$ *and*

$$U(R) = (\alpha) \times H. \tag{8}$$

Example 2. *If* $R = \mathbb{Z}_{2^4}[u]/(u^2 - 2^3\beta, 2u)$, *then the units of* R *are of the form*

$$U(R) = \{1,3,5,7,9,11,13,15,1+u,3+u,5+u,7+u,9+u,11+u,13+u,15+u\}.$$

4. MacWilliams Identities

With $p, n, 1, 1$ as invariants and $g(x) = x^2 - p^{n-1}\beta$, let R be a Frobenius local ring. Theorem 6 outlines a method to produce a generating character χ for any such ring. Suppose γ_i is a p^{n_i}-root of unity and $a_i \leq mr$ for each i.

Theorem 6 ([7]). *Let* R *be a ring with* p, n, r, t, d. *There is* $q \in \mathbb{Z}$, *such that* $q \geq 1$, *and*

$$\chi(\omega) = \gamma_1^{a_1}\gamma_2^{a_2}\dots\gamma_q^{a_q}, \tag{9}$$

is a generating character of R, $1 \leq i \leq q$.

The formulas of χ for R are shown in the following Table 2, where γ, δ, and ζ are the p^nth, pth, and 2^nth roots of unity, respectively.

Table 2. χ for the ring R.

Ring	$(R,+)$	χ
$\mathbb{Z}_{2^n}[u]/(u^2 - 2^{n-1}, 2u)$	$\mathbb{Z}_{2^4} \times \mathbb{Z}_2$	$\chi(a+bu) = \zeta^a(-1)^b$
$\mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}, pu)$	$\mathbb{Z}_{p^n} \times \mathbb{Z}_p$	$\chi(a+bu) = \gamma^a\delta^b$

The MacWilliams identities for various version of R are now computed. Actually, the class of all Frobenius rings is a broader class of finite rings to which these relationships can be extended. These identities are fundamental to the study of coding theory because they introduce a crucial link between a code's dual and weight enumerator. Assume the following: The elements in $R = \{a_1, a_2, a_3, \dots a_{p^{(n+1)}}\}$ are in that order. Suppose C is a linear code over R with length N. Let us assume that $n_i(\mathbf{c})$ is the number of instances of a_i in $\mathbf{c} \in C$. The complete weight enumerator is then denoted as

$$CWE(C) = \sum_{c\in}\prod_i a_i^{n_i(\mathbf{c})}. \tag{10}$$

$$CWE_C(x_{a_1}, \dots, x_{a_{p^{(n+1)}}}) = \frac{1}{\mid C^\perp \mid} CWE_{C^\perp}(A \cdot x_{a_1}, \dots, x_{a_{p^{(n+1)}}}), \tag{11}$$

where $A = (a_{ij})$, and $a_{ij} = \chi(a_i a_j)$. We define $wt(\mathbf{c}) = \mid \{i : c_i \neq 0\} \mid$. The Hamming weight (HW) enumerator and its MacWilliams identity are given by

$$HW_C(a,b) = \sum_{c\in C} a^{N-wt(\mathbf{c})}b^{wt(\mathbf{c})}, \tag{12}$$

$$HW_C(a,b) = \frac{1}{\mid C^\perp \mid} HW_{C^\perp}(a + (p^{(n+1)} - 1)b, a - b). \tag{13}$$

Suppose that $\sim$ is defined on R by $x \sim y$ when there is $\omega \in U(R)$, such that $x = \omega y$. It is evident that this relation is equivalent. Let $\hat{b}_1, \dots, \hat{b}_q$ be the equivalence classes and let $n_i'(\mathbf{c})$ calculate the number of elements of $\hat{b}_i$ that occurred in the codeword $\mathbf{c}$. Hence, SWE is defined as follows

$$SWE_C(x_{\hat{b}_1}, \dots, x_{\hat{b}_q}) = \sum_{\mathbf{c}\in C}\prod_i x_{\hat{b}_i}^{n_i'(\mathbf{c})}. \text{ (symmetrized weight enumerator)} \tag{14}$$

We introduce the MacWilliams equation for SWE as

$$SWE_C(x_{\hat{b}_1}, \dots, x_{\hat{b}_q}) = \frac{1}{\mid C^\perp \mid} SWE_{C^\perp}(S \cdot (x_{\hat{b}_1}, \dots, x_{\hat{b}_q})), \tag{15}$$

where $S = (b_{ij})$ and

$$b_{ij} = \sum_{a \in \hat{b}_j} \chi(a_i a).$$

As we can notice, once χ is obtained, it is straightforward to obtain the matrix A in Equation (11). Nonetheless, S in Equation (15) necessitates the determination of the classes $\hat{b}_i$. While it takes more work, this procedure is essential for building S. If we look at the broader case for n, that is, $\mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}\beta, pu)$. Note that $J = (p, u)$ in this ring, of order $(p-1)p^4$, with $l = 4$, as its index of nilpotency, and $soc(R) = (p^3)$. Then, one can obtain the set of $\hat{b}_i$ as follows.

$$\begin{cases} \hat{b}_1 = \{0\}, \\ \hat{b}_2 = U(R) = \{i, i + ju : \ \ (i,p) = 1, j = 1, 2, \ldots, p-1\}, \\ \hat{b}_3 = (p) \setminus (p^2), \\ \hat{b}_4 = (u) \setminus soc(R), \\ \hat{b}_5 = (u + p) \setminus (p^2), \\ \hat{b}_6 = (u + p^2) \setminus (p^3), \\ \hat{b}_7 = (p^2) \setminus (p^3), \\ \hat{b}_8 = (u + p^3) \setminus (p^4), \\ \hat{b}_9 = (p^3) \setminus (p^4), \\ \vdots \\ \hat{b_j} = (u + p^i) \setminus (p^{i+1}), \\ \hat{b_{j'}} = (p^i) \setminus (p^{i+1}), \\ \vdots \\ \hat{b}_{n-1} = soc(R) \setminus \{0\} = J^{n-1} \setminus \{0\} = (p^{n-1}). \end{cases}$$

For a more general case, we have a detailed scheme for finding b_{ij} in the following lemma.

Lemma 1. *Let $R = \mathbb{Z}_{p^n}[u]/(u^2 - p^{n-1}, pu)$. Then,*

$$b_{ij} = \begin{cases} \mid \hat{b_j} \mid, & \text{if } a_i \hat{b_j} = \{0\}; \\ 0, & \text{if } p^{n-1} \notin a_i \hat{b_j}; \\ (-1)^{\frac{1}{p-1}} \mid \hat{b_j} \mid, & \text{if } p^{n-1} \in a_i \hat{b_j}. \end{cases}$$

Proof. Suppose that $a_i \hat{b_j} = \{0\}$, then $b_{ij} = \sum_{b \in \hat{b_j}} \chi a_i b = \sum_{b \in \hat{b_j}} 0 = \mid \hat{b_j} \mid$. For the other cases, assume that $a_i \hat{b_j} \neq \{0\}$. First, let $p^{n-1} \in a_i \hat{b_j}$. As $\mathrm{soc}(R) = (p^{n-1})$, then $p^{n-1} = \alpha y$, where $\alpha \in \Gamma^*(1)$ and $y \in \hat{b_j}$ are a representative of $\hat{b_j}$. Now, also suppose that $x \in a_i \hat{b_j}$, then $x = a_i y'$ for some y' in $\hat{b_j}$. It follows that $x = \gamma p^{n-1}$, where $\gamma \in \Gamma^*(1)$. This means that all elements of $a_i \hat{b_j}$ are of the form αp^{n-1}, which can be interpreted as the set $a_i \hat{b_j}$ is just copies of $\mathrm{soc}(R)$. Thus,

$$b_{ij} = N_0 \sum_{\alpha \in \Gamma^*(1)} e^{\frac{(2\pi i)\alpha}{p}}.$$

However, we have the following formula for complex numbers,

$$1 + \sum_{j=1}^{p-1} e^{\frac{(2\pi i)j}{p}} = 0. \tag{16}$$

The positive N_0 reflects the number of copies of $\mathrm{soc}(R)$, which is precisely $N_0 = \frac{1}{p-1} \mid \hat{b_j} \mid$ Therefore,

$$b_{ij} = (-1)\frac{1}{p-1} \mid \hat{b_j} \mid .$$

The last case of the proof can be achieved similarly by noting that every element of $a_i\hat{b_j}$ can be expressed as $x + \alpha p^{n-1}$, where $\alpha \in \Gamma(1)$. In such a case,

$$b_{ij} = \sum_x \chi(x) \sum_{\alpha \in \Gamma(1)} \chi(\alpha p^{n-1}).$$

Hence, by Equation (16), we conclude the results. □

Theorem 7. *The S matrix for* $R = \mathbb{Z}_{p^4}[u]/(u^2 - p^3, pu)$ *is given as*

$$S(p,4,1,1,3) = \begin{pmatrix} 1 & (p-1)p^4 & (p-1)p^2 & (p-1)p & (p-1)p^2 & (p-1)p & (p-1)p & (p-1) \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & (p-1)p & 0 & -p & -p & (p-1) \\ 1 & 0 & (p-1)p^2 & -p & -p^2 & -p & p(p-1) & (p-1) \\ 1 & 0 & 0 & -p & 0 & -p & -p & (p-1) \\ 1 & 0 & -p^2 & p(p-1) & -p^2 & p & p(p-1) & (p-1) \\ 1 & 0 & -p^2 & (p-1)p & -p^2 & (p-1)p & (p-1)p & (p-1) \\ 1 & -p^4 & (p-1)p^2 & (p-1)p & (p-1)p^2 & (p-1)p & (p-1)p & (p-1) \end{pmatrix}.$$

Proof. Let us assume that the elements of R are ordered as follows: if $i, j \in \mathbb{Z}_{p^4}$, then i comes before j if $i < j$ as an integer, and $i + u$ comes before $j + u$ if i precedes j. The equivalency classes are therefore

$$\begin{cases} \hat{b_1} = \{0\}, \\ \hat{b_2} = U(R) = \{i, i + ju : \ \ (i,p) = 1\}, \\ \hat{b_3} = (p) \setminus (p^2), \\ \hat{b_4} = (u) \setminus soc(R), \\ \hat{b_5} = (u + p) \setminus (p^2), \\ \hat{b_6} = (u + p^2) \setminus soc(R), \\ \hat{b_7} = (p^2) \setminus soc(R), \\ \hat{b_8} = soc(R) \setminus \{0\} = J^3 \setminus \{0\} = (p^3). \end{cases}$$

Thus, by using Lemma 16 and after making the necessary computations, the results are obtained. □

Remark 4. *The matrix S can be obtained for R when* $n > 4$*, but the computations will be tedious.*

We then move on to a numerical demonstration of these computations and their steps for examples of rings with 3^5. We will first concentrate on comprehending $\hat{b_i}$ under $\sim$ before building S.

Example 3. *Suppose that* $R = \mathbb{Z}_{3^4}[u]/(u^2 - 3^3, 3u)$*. Assuming the order for the elements of R as:*

$$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = u, a_5 = u + 3, a_6 = u + 9, a_7 = 9, a_8 = 27.$$

We then compute S, which requires a large number of calculations. The $\hat{b}_i$ *for R that we must obtain are listed as*

$$\begin{cases} \hat{b_1} = \{0\}, \\ \hat{b}_2 = U(R) = \{i, i+ju: \ \ (i,3) = 1, j = 1,2\}, \\ \hat{b_3} = (3) \setminus (9), \\ \hat{b_4} = (u) \setminus soc(R), \\ \hat{b_5} = (u+3) \setminus (9), \\ \hat{b_6} = (u+9) \setminus soc(R), \\ \hat{b_7} = (9) \setminus soc(R), \\ \hat{b_8} = soc(R) \setminus \{0\} = J^3 \setminus \{0\} = (27). \end{cases}$$

Therefore, by Theorem 7, we obtain

$$S(3,4,1,1,3) = \begin{pmatrix} 1 & 162 & 18 & 6 & 18 & 6 & 6 & 2 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 6 & 0 & -3 & -3 & 2 \\ 1 & 0 & 18 & -3 & -9 & -3 & 6 & 2 \\ 1 & 0 & 0 & -3 & 0 & -3 & -3 & 2 \\ 1 & 0 & -9 & 6 & -9 & 3 & 6 & 2 \\ 1 & 0 & -9 & 6 & -9 & 6 & 6 & 2 \\ 1 & -81 & 18 & 6 & 18 & 6 & 6 & 2 \end{pmatrix}$$

As a summary, we introduce Table 3 to present S and $\hat{b}_i$.

Table 3. S and $\hat{b}_i$ for $\mathbb{Z}_{p^4}[u]/(u^2 - p^3, pu)$.

Ring	S	$\hat{b}_i$
$\mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$	$S(p,4,1,1,3)$	$\{0\}, U(R), (p) \setminus (p^2), (u) \setminus soc(R), (u+p) \setminus (p^2), (u+p^2) \setminus (p^3), (p^2) \setminus (p^3), (p^3) \setminus \{0\}$
$\mathbb{Z}_{p^4}[u]/(u^2 - p^3, pu)$	$S(p,4,1,1,3)$	
$\mathbb{Z}_{2^4}[u]/(u^2 - 2^3, 2u)$	$S(2,4,1,1,3)$	$\{0\}, U(R), (2) \setminus (4), (u) \setminus soc(R), (u+2) \setminus (4), (u+4) \setminus (8), (4) \setminus (8), (8) \setminus \{0\}$

Remark 5. *From the above discussion, S is an equivalent matrix for every ring that is examined in this article.*

5. Generator Matrices

The remaining content of the article is devoted to Frobenius local rings of order p^5,

$$R = \mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu). \tag{17}$$

Definition 1. *If the vectors with coefficients from J cannot be combined linearly in a nontrivial way to equal the zero vector, we refer to the vectors* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_e$ *as modularly independent. When the rows of G independently produce the code C, then G is a generator matrix over the ring R.*

Remark 6. *Every linear code C over R has a generator matrix G and this matrix is unique up to raw equivalency.*

This section finds matrices G that produce linear codes over R. Building a generator matrix G for codes over non-chains is more difficult than for those over chains. This kind of generator matrix might not provide straightforward information about the code size or number of codewords, even though one can still locate a basic set of generators.

Figure 2 above illustrates ideals of R. As $| J |= p^4$, $| (p) |=| (u) |=| (u+p) |=| (p^2, u) |= p^3$, $| (u+p^2) |=| (p^2) |= p^2$ and $| (p^3) = soc(R) |= p$. Therefore, the goal of this section is to produce a collection of independent modular elements that function as a code's generator matrix's rows. A complete description of the structure of G is given by the following theorem.

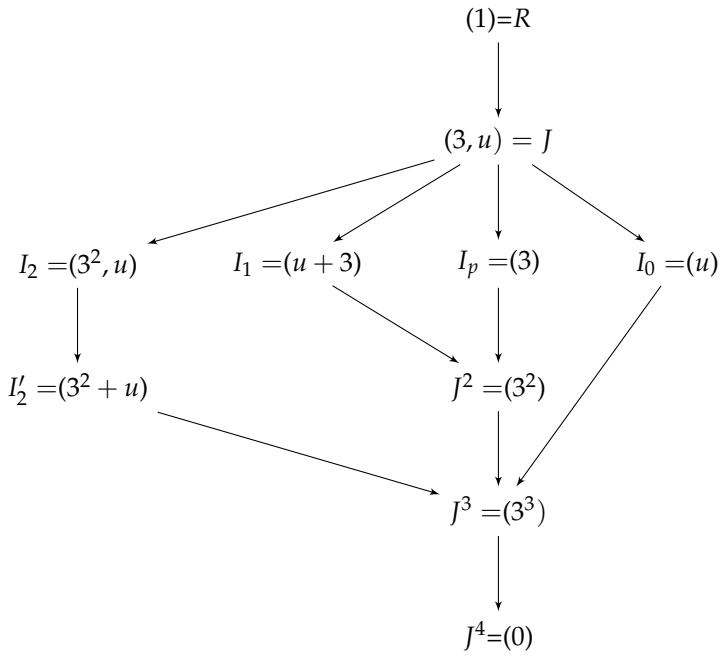


Figure 2. Lattice of ideals of $R = \mathbb{Z}_{3^4}[u]/(u^2 - 3^3\beta, 3u)$.

Theorem 8. *Assume C is a linear code with N over $R = \mathbb{Z}_{p^4}[u]/(u^2 - p^3\beta, pu)$. Thus, for any C, any G is raw equivalent to*

$$G = \left(\begin{array}{c|c|c|c|c|c|c|c|c} I_{e_0} & A_{12} & A_{13} & A_{14} & A_{15} & A_{16} & A_{17} & A_{18} & A_{19} \\ ine\ 0 & pI_{e_1} & A_{23} & A_{24} & A_{25} & A_{26} & A_{27} & A_{28} & A_{29} \\ \hline 0 & uI_{e_1} & & & & & & & \\ ine\ 0 & 0 & uI_{e_2} & 0 & 0 & 0 & A_{37} & & \\ \hline 0 & 0 & 0 & (u+p^2)I_{e_3} & 0 & 0 & & & \\ \hline 0 & 0 & 0 & 0 & pI_{e_4} & 0 & 0 & A_{48} & A_{49} \\ \hline 0 & 0 & 0 & 0 & 0 & (p+u)I_{e_5} & 0 & & \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & p^2I_{e_6} & & \\ ine\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p^3I_{e_7} & A_{99} \end{array}\right)$$

where A_{ij} are matrices of various sizes.

Proof. Let G be a matrix such that the rows r_i's of the matrix produce C as an R-module. Every column containing a unit is moved to the left of G. We obtain a matrix of the form by row reduction on those columns,

$$G = \begin{pmatrix} I_{e_0} & * \\ 0 & A \end{pmatrix}$$

Now, not every element in A is a unit. To transform the matrix into the next form, we shift all columns containing elements of $J = (2, \pi)$ to the left once more and apply the primary row operations.

$$G = \begin{pmatrix} I_{e_0} & * & * \\ 0 & p & * \\ 0 & u & * \\ 0 & 0 & A_1 \end{pmatrix}$$

We continue with this algorithm, making sure that the matrix A_1 is created by putting elements in columns such that they form a pair (p, u). We keep doing this until the matrix takes on the form that we want.

$$\left(\begin{array}{c|c|c} I_{e_0} & * & * \\ \text{ine } 0 & pI_{e_1} & * \\ \hline 0 & uI_{e_1} & \\ \text{ine } 0 & 0 & A_2 \end{array}\right)$$

where only one of (p), (u), $(p+u)$, and (p^2+u) is represented by the elements of the matrix A_2's columns. We will now move over to the matrix A_2. The four ideals are (u), (p^2+u), (p), and $(p+u)$. We choose a particular ordering for each ideal for the sake of producing a one expression of the matrix. The matrix will be constructed using this selected order consistently. Assuming v is a unit of R, we proceed as follows: columns with entries of the form uv, columns with elements of the form $(u+p^2)v$, and finally columns with elements of the form $(p)v$. Lastly, we address columns that take the form $(u+p)v$. We carry out row reduction in the standard way in each step. Observe that both (p) and $(u+p)$ contain the ideal (p^2). Consequently, we redo similar a process with (p^2) as the remaining column entries will come from (p^2).

$$\left(\begin{array}{c|c|c|c|c|c} uI_{e_2} & 0 & 0 & 0 & * & \\ \hline 0 & (u+p^2)I_{e_3} & 0 & 0 & & \\ \hline 0 & 0 & pI_{e_4} & 0 & 0 & * \\ \hline 0 & 0 & 0 & (p+u)I_{e_5} & 0 & \\ \hline 0 & 0 & 0 & 0 & p^2I_{e_6} & \\ \text{ine } 0 & 0 & 0 & 0 & 0 & A_3 \end{array}\right).$$

Finally, every component of A_3 originates from the ideal that p^3 generates. We obtain a matrix that precisely corresponds to the desired form by removing any rows that contain only zeros and completing one last row reduction round. □

Proposition 1. *If $\boldsymbol{v} \in R^N$, and $M = (\boldsymbol{v})$ is a R-submodule. Then, $\mid M \mid \in \{p^5, p^4, p^3, p^2, p, 0\}$.*

Proof. Let I be an ideal created by the vector **v**'s coordinates. Also, let $T = \text{annl}(I)$. Then,

$$\mid M \mid = \frac{\mid R \mid}{\mid T \mid} = \mid I \mid .$$

By Figure 2, $\mid I \mid \in \{p^5, p^4, p^3, p^2, p, 0\}$. □

Theorem 9. *Let $M = (\boldsymbol{w}, \boldsymbol{v})$ be R-submodule, where the coordinates of $\boldsymbol{w}$,$\boldsymbol{v}$ are not units of R. Thus,*

$$\mid M \mid \in \{p^8, p^7, p^6, p^5, p^4, p^3, p^2\}.$$

Proof. From Proposition 1, we have $\mid M \mid \leq p^8$. As $\mid (p^3) \mid = p$, then $p^2 \leq \mid M \mid$. □

Example 4. *To have a code C over $R = \mathbb{Z}_{p^4}[u]/(u^2 - p^3, pu)$ of order p^4, set $N = 1$ with $C = (p, u)$. Then, $\mid C \mid = p^4$. Meanwhile, to construct C with size p^5, suppose $C = (\boldsymbol{w}, \boldsymbol{v})$ with $N = 2$, $\boldsymbol{w} = (p, u)$ and $\boldsymbol{v} = (u, p)$. This implies $\mid C \mid = p^5$. Take $N = 4$, $\boldsymbol{w} = (p, 0, u, p)$ and $\boldsymbol{v} = (u, p, 0, 0)$. Hence, $\mid C \mid = p^8$. Therefore,*

$$C \cong (\boldsymbol{w}) \oplus (\boldsymbol{v}).$$

Example 5 shows a minimal set of generators may not exist for C over a (non-chain) Frobenius local, which makes the code more complex. Stated differently, it highlights the differences in coding over chain rings and that over non-chain rings.

Example 5. *Let G be a generator matrix of the code C over $\mathbb{Z}_{p^4}[u]/(u^2 - p^3, 2u)$ of the form*

$$\begin{pmatrix} p & u \\ u & 0 \\ 0 & p \end{pmatrix}.$$

Assuming that M_1 represents the R-submodule produced by r_1 and r_2 of G, and M_2 the R-submodule produced by r_3 G,

$$M_1 \cap M_2 \neq \phi.$$

This indicates that the module C cannot be reduced.

6. Conclusions

We conclude that, up to isomorphism, all rings of the form $R = \mathbb{Z}_{p^n}[u]$ with $u^2 = p^{n-1}\beta$ and $pu = 0$ have been successfully classified in terms of $p, n, 1, 1, n - 1$. Furthermore, generator matrices and MacWilliams relations for linear codes over such rings have been discovered. These are popular and effective tools for encoding data over chain rings; codes over local non-chain rings may not be able to achieve such a case. The challenge is in identifying a smallest number of generators and counting the code size because non-chain local rings are not PIRs. This restriction suggests that in order to effectively handle such an issue, different approaches or strategies are needed.

Author Contributions: Conceptualization, S.A. and A.A.A.; methodology, S.A. and A.A.A.; formal analysis, S.A., A.A.A. and N.A.A.; investigation, S.A. and A.A.A.; writing—original draft, S.A. and N.A.A.; writing—review & editing, S.A., A.A.A. and N.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Researchers Supporting Project number (RSPD2024R871), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: No new data were created or analyzed in this study.

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

References

1. Norton, G.; Salagean, A. On the structure of linear cyclic codes over finite chain rings. *Appl. Algebra Eng. Commun. Comput.* **2000**, *10*, 489–506. [CrossRef]
2. Greferath, M. Cyclic codes over finite rings. *Discrete Math.* **1997**, *177*, 273–277. [CrossRef]
3. Dougherty, S.T.; SaltÃ¼rk, E.; Szabo, S. Codes over local rings of order 16 and binary codes. *Adv. Math. Commun.* **2016**, *10*, 379–391. [CrossRef]

4. Alabiad, S.; Alkhamees, Y. Constacyclic codes over finite chain rings of characteristic p. *Axioms* **2021**, *10*, 303. [CrossRef]
5. Yildiz, B.; Karadeniz, S. Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes. *Finite Fields Their Appl.* **2014**, *27*, 24–40. [CrossRef]
6. Dougherty, S.T.; SaltÃ¼rk, E.; Szabo, S. On codes over Frobenius rings: Generating characters, MacWilliams identities and generator matrices. *Appl. Algebra Eng. Commun. Comput.* **2019**, *30*, 193–206. [CrossRef]
7. Alabiad, S.; Alhomaidhi, A.A.; Alsarori, N.A. On Linear Codes over Finite Singleton Local Rings. *Mathematics* **2024**, *12*, 1099. [CrossRef]
8. MartÃnez-Moro, E.; Szabo, S.; Yildiz, B. Linear codes over $\mathbb{Z}_4[x]/(x^2 + 2x)$. *Int. Inf. Coding Theory* **2015**, *3*, 78–96.
9. Sriwirach, W.; Klin-Eam, C. Repeated-root constacyclic codes of length $2p^s$ over $F_{p^m} + uFpm + u^2F_{p^m}$. *Cryptogr. Comm.* **2021**, *13*, 27–52. [CrossRef]
10. Laaouine, J.; Charkani, M.E.; Wang, L. Complete classification of repeated-root-constacyclic codes of prime power length over $F_{p^m}[u]/(u^3)$. *Discrete Math.* **2021**, *344*, 112325. [CrossRef]
11. Shi, M.; Zhu, S.; Yang, S. A class of optimal p-ary codes from one-weight codes over $F_p[u]/ < u^m >$. *J. Frankl. Inst.* **2013**, *350*, 929–937. [CrossRef]
12. Alkhamees, Y.; Alabiad, S. The structure of local rings with singleton basis and their enumeration. *Mathematics* **2022**, *10*, 4040. [CrossRef]
13. Raghavendran, R. Finite associative rings. *Compos. Math.* **1969**, *21*, 195–229.
14. Honold, T. Characterization of finite Frobenius rings. *Arch. Math.* **2001**, *76*, 406–415. [CrossRef]
15. MartÃnez-Moro, E.; Szabo, S. On codes over local Frobenius non-chain rings of order 16. In *Noncommutative Rings and Their Applications*; Contemporary Mathematics; Dougherty, S., Facchini, A., Leroy, A., Puczylowski, E., SolÃ©, P., Eds.; American Mathematical Society: Providence, RI, USA, 2015; Volume 634, pp. 227–241.
16. Wood J.A. Duality for modules over finite rings and applications to coding theory. *Am. J. Math.* **1999**, *121*, 555–575. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.