Bases of the Galois Ring $GR(p^r, m)$
over the Integer Ring $\mathbb{Z}_{p^r}$

Virgilio Sison*
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
Email: vpsison@uplb.edu.ph

October 2, 2014

Abstract

The Galois ring $GR(p^r, m)$ of characteristic $p^r$ and cardinality $p^{rm}$, where $p$ is a prime and $r, m \geq 1$ are integers, is a Galois extension of the residue class ring $\mathbb{Z}_{p^r}$ by a root $\omega$ of a monic basic irreducible polynomial of degree $m$ over $\mathbb{Z}_{p^r}$. Every element of $GR(p^r, m)$ can be expressed uniquely as a polynomial in $\omega$ with coefficients in $\mathbb{Z}_{p^r}$ and degree less than or equal to $m - 1$, thus $GR(p^r, m)$ is a free module of rank $m$ over $\mathbb{Z}_{p^r}$ with basis $\{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$. The ring $\mathbb{Z}_{p^r}$ satisfies the invariant dimension property, hence any other basis of $GR(p^r, m)$, if it exists, will have cardinality $m$.

This paper was motivated by the code-theoretic problem of finding the homogeneous bound on the $p^r$-image of a linear block code over $GR(p^r, m)$ with respect to any basis. It would be interesting to consider the dual and normal bases of $GR(p^r, m)$.

By using a Vandermonde matrix over $GR(p^r, m)$ in terms of the generalized Frobenius automorphism, a constructive proof that every basis of $GR(p^r, m)$ has a unique dual basis is given. The notion of normal bases was also generalized from the classic case for Galois fields.

Keywords – Galois rings, trace function, Frobenius automorphism, Vandermonde matrix, dual basis, normal basis

1 Introduction

It was proved in [1] that every basis of the Galois ring $GR(4, m)$ has a dual basis, by treating each linear transformation from $GR(4, m)$ to $\mathbb{Z}_4$ as being uniquely determined in terms of the generalized trace function on $GR(4, m)$. In this paper this

*This author gratefully acknowledges financial grant from the UPLB Diamond Jubilee-Development Fund Professorial Chair Award.
result is generalized to the Galois ring $GR(p^r, m)$ following the alternate method of MacWilliams and Sloane [8] which constructs the dual basis using simple matrix algebra involving the generalized Frobenius automorphism. The material is organized as follows: Section [2] gives the preliminaries and basic definitions, while Section [3] gives the results.

## 2 Preliminaries and definitions

An overview of Galois fields and Galois rings, the Frobenius automorphism and the trace function, is presented in this section. For a thorough discussion of these topics, we refer the reader to [7], [8] and [11].

### 2.1 Galois fields and Galois rings

Let $p$ be a prime number and $r \geq 1$ an integer. Consider the ring $\mathbb{Z}_{p^r}$ of integers modulo $p^r$. When $r = 1$ the ring $\mathbb{Z}_p$ with $p$ elements is a field and is usually denoted by $\mathbb{F}_p$. Let $\mathbb{Z}_{p^r}[x]$ be the ring of polynomials in the indeterminate $x$ with coefficients in $\mathbb{Z}_{p^r}$.

The Galois field with $p^m$ elements, denoted $\mathbb{F}_{p^m}$, is a field extension $\mathbb{F}_p[\alpha]$ of $\mathbb{F}_p$ by a root $\alpha$ of an irreducible polynomial $\pi(x)$ of degree $m$ in $\mathbb{F}_p[x]$. Thus every element $z$ of $\mathbb{F}_{p^m}$ can be expressed uniquely as a polynomial in $\alpha$ of the form

$$z = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{m-1}\alpha^{m-1}$$

with degree at most $m - 1$ with the coefficients $a_i$ coming from $\mathbb{F}_p$, and hence can also be written as an $m$-tuple $(a_0, a_1, \ldots, a_{m-1})$ in $\mathbb{F}_p^m$. Elements of $\mathbb{F}_{p^m}$ may also be described as residue classes of the polynomials in $x$ with coefficients in $\mathbb{F}_p$ reduced modulo $\pi(x)$. When $m = 1$ we again have the field $\mathbb{F}_p$.

The canonical projection homomorphism $\mu : \mathbb{Z}_{p^r} \rightarrow \mathbb{F}_p$ is the mod-$p$ reduction map, and can be extended naturally as a map from $\mathbb{Z}_{p^r}[x]$ onto $\mathbb{F}_p[x]$. This extended map is a ring homomorphism with kernel $(p) = \mathbb{Z}_{p^r}[x]p = \{f(x)p \mid f(x) \in \mathbb{Z}_{p^r}[x]\}$.

Let $g(x)$ be a monic polynomial of degree $m \geq 1$ in $\mathbb{Z}_{p^r}[x]$. If $\mu(g(x))$ is irreducible in $\mathbb{F}_p[x]$, then $g(x)$ is said to be monic basic irreducible. If $\mu(g(x))$ is primitive in $\mathbb{F}_p[x]$, then $g(x)$ is said to be monic basic primitive. Clearly, monic basic primitive polynomials in $\mathbb{Z}_{p^r}[x]$ are monic basic irreducible.

In the general sense, a Galois ring is a finite commutative local ring with identity $1 \neq 0$ such that the set of zero divisors together with the zero element forms the unique maximal principal ideal $(p1)$ for some prime number $p$. The residue class ring $\mathbb{Z}_{p^r}[x]/(h(x))$, where $h(x)$ is a monic basic irreducible polynomial of degree $m$ in $\mathbb{Z}_{p^r}[x]$, is a Galois ring with characteristic $p^r$ and cardinality $p^m$. The elements of $\mathbb{Z}_{p^r}[x]/(h(x))$ are residue classes of the form

$$a_0 + a_1x + \ldots + a_{m-1}x^{m-1} + (h(x))$$

where $a_i \in \mathbb{Z}_{p^r}$. The identity is $1 + (h(x))$ and the zero element is $(h(x))$. The principal ideal $(p1 + (h(x))) = (p + (h(x)))$ consists of all the zero divisors and the zero element, and is the only maximal ideal.
If \( \deg h(x) = 1 \) then \( \mathbb{Z}_{p^r}[x]/(h(x)) \) is the ring \( \mathbb{Z}_{p^r} \). If \( r = 1 \), the canonical homomorphism \( \mu \) becomes the identity map and \( \mathbb{Z}_{p^r}[x]/(h(x)) = \mathbb{F}_p[x]/(h(x)) \cong \mathbb{F}_{p^m} \). Now let \( \omega = x + (h(x)) \), then \( h(\omega) = 0 \) and every element \( z \) of \( \mathbb{Z}_{p^r}[x]/(h(x)) \) can be expressed uniquely in the form
\[
z = a_0 + a_1 \omega + \ldots + a_{m-1} \omega^{m-1}
\] (3)
where \( a_i \in \mathbb{Z}_{p^r} \). We can thus think of \( \mathbb{Z}_{p^r}[x]/(h(x)) \) as a Galois extension \( \mathbb{Z}_{p^r}[\omega] \) of \( \mathbb{Z}_{p^r} \) by \( \omega \). The elements take the additive representation \( \mathbb{Z}_{p^r} \), a generalization of \( \mathbb{Z}_p \) for \( \mathbb{F}_{p^m} \). Since any two Galois rings of the same characteristic and the same cardinality are isomorphic, we simply use the notation \( GR(p^r, m) \) for any Galois ring with characteristic \( p^r \) and cardinality \( p^m \).

The Galois ring \( \mathcal{R} = GR(p^r, m) \) is a finite chain ring of length \( r \), its ideals \( p^i \mathcal{R} \) with \( p^{i-r} \) elements are linearly ordered by inclusion,
\[
\{0\} = p^r \mathcal{R} \subset p^{r-1} \mathcal{R} \subset \ldots \subset p \mathcal{R} \subset \mathcal{R}
\] (4)
The quotient ring \( \mathcal{R}/p \mathcal{R} \cong \mathbb{F}_{p^m} \) is the residue field of \( \mathcal{R} \). There exists a nonzero element \( \xi \) of order \( p^m - 1 \), which is a root of a unique monic basic primitive polynomial \( h(x) \) of degree \( m \) over \( \mathbb{Z}_{p^r} \) and dividing \( x^{p^m} - 1 \) in \( \mathbb{Z}_{p^r}[x] \). Consider the set
\[
\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}
\] (5)
of Téichmuller representatives. In this case, every element \( z \) of \( GR(p^r, m) \) has a unique multiplicative or \( p \)-adic representation as follows
\[
z = z_0 + pz_1 + p^2 z_2 + \ldots + p^{r-1} z_{r-1}
\] (6)
where \( z_i \in \mathcal{T} \). We have that \( z \) is a unit if and only if \( z_0 \neq 0 \), and \( z \) is a zero divisor or 0 if and only if \( z_0 = 0 \). The units form a multiplicative group of order \( (p^m - 1)p^{(r-1)m} \), which is a direct product \( \langle \omega \rangle \times \mathcal{E} \), where \( \langle \omega \rangle \) is the cyclic group of order \( p^m - 1 \) that is isomorphic to \( \mathbb{Z}_{p^m-1} \) and \( \mathcal{E} = \{1 + \pi \mid \pi \in (p)\} \) is a group of order \( p^{r-1}m \). Let \( \mu(\xi) = \alpha \). It can be shown that \( \alpha \) is a primitive element in \( \mathbb{F}_{p^m} \), and thus \( \mu(\mathcal{T}) = \mathbb{F}_{p^m} \). The \( p \)-adic representation in (6) is a generalization of the power representation of an element of \( \mathbb{F}_{p^m} \).

We realize that \( GR(p^r, m) \) is a free module of rank \( m \) over \( \mathbb{Z}_{p^r} \) with the set
\[
\mathcal{P}_m(\omega) = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}
\] (7)
as a free basis. The set \( \mathcal{P}_m(\omega) \) is called the standard or polynomial basis of \( GR(p^r, m) \). The ring \( \mathbb{Z}_{p^r} \) satisfies the invariant dimension property, hence any other basis of \( GR(p^r, m) \), if it exists, will have cardinality \( m \).

### 2.2 Generalized Frobenius automorphism and trace

The Generalized Frobenius map \( f \) on the Galois ring \( \mathcal{R} = GR(p^r, m) \) is defined by
\[
z^f := z_0^p + pz_1^p + p^2 z_2^p + \ldots + p^{r-1} z_{r-1}^p
\] (8)
where \( z \) has the \( p \)-adic representation given in (6). The map \( f \) satisfies the following properties.
(i) \( f \) is a ring automorphism of \( \mathcal{R} \).

(ii) \( f \) fixes every element of \( \mathbb{Z}_{p^r} \).

(iii) \( f \) is of order \( m \) and generates the cyclic Galois group of \( \mathcal{R} \) over \( \mathbb{Z}_{p^r} \).

When \( r = 1 \), the automorphism \( f \) reduces to the usual Frobenius automorphism \( \sigma \) of \( \mathbb{F}_{p^m} \) defined by \( \sigma(z) = z^p \).

The generalized trace map \( T \) from \( \mathcal{R} \) down to \( \mathbb{Z}_{p^r} \) is given by
\[
T(z) := z + zf + zf^2 + \ldots + zf^{m-1} \tag{9}
\]
and satisfies the following properties.

(i) \( T \) is surjective and \( \mathcal{R}/\text{ker} \ T \cong \mathbb{Z}_{p^r} \).

(ii) \( T \) takes on each value of \( \mathbb{Z}_{p^r} \) equally often \( p^{r(m-1)} \) times.

(iii) \( T(\alpha + \beta) = T(\alpha) + T(\beta) \) for all \( \alpha, \beta \in \mathcal{R} \).

(iv) \( T(\lambda \alpha) = \lambda T(\alpha) \) for all \( \lambda \in \mathbb{Z}_{p^r}, \alpha \in \mathcal{R} \).

(v) \( T(\alpha^f) = (T(\alpha))^f = T(\alpha) \) for all \( \alpha \in \mathcal{R} \).

Again when \( r = 1 \) the generalized trace map \( T \) reduces to the trace map \( t : \mathbb{F}_{p^m} \to \mathbb{F}_p \) defined by
\[
t(\beta) = \beta + \beta^p + \beta^{p^2} + \ldots + \beta^{p^{m-1}} \tag{10}
\]

2.3 Homogeneous weight on \( GR(p^r, m) \)

Let \( R \) be a finite ring with identity \( 1 \neq 0 \), and \( \mathbb{T} \) be the multiplicative group of unit complex numbers. The group \( \mathbb{T} \) is a one-dimensional torus. A character of \( R \) (considered as an additive abelian group) is a group homomorphism \( \chi : R \to \mathbb{T} \).

The set of all characters \( \hat{R} \) (called the character module of \( R \)) is a right (resp. left) \( R \)-module whose group operation is pointwise multiplication of characters and scalar multiplication is given by \( \chi^x = \chi(rx) \) (resp. \( r\chi = \chi xr \)). A character \( \chi \) of \( R \) is called a right (resp. left) generating character if the mapping \( \phi : R \to \hat{R} \) given by \( \phi(r) = \chi^r \) (resp. \( \phi(r) = r\chi \)) is an isomorphism of right (resp. left) \( R \)-modules.

The ring \( R \) is called Frobenius if and only if \( R \) admits a right or a left generating character, or alternatively, if and only if \( \hat{R} \cong R \) as right or left \( R \)-modules. It is known that for finite rings, a character \( \chi \) on \( R \) is a right generating character if and only if \( \ker \chi \) contains no non-zero right ideals.

Let \( \mathbb{R} \) be the set of real numbers. We define a homogeneous weight on an arbitrary finite ring \( R \) with identity in the sense of [4]. Let \( Rx \) denote the principal (left) ideal generated by \( x \in R \).

**Definition 2.1** A weight function \( w : R \to \mathbb{R} \) on a finite ring \( R \) is called (left) homogeneous if \( w(0) = 0 \) and the following is true.
(i) If $Rx = Ry$, then $w(x) = w(y)$ for all $x, y \in R$.

(ii) There exists a real number $\Gamma \geq 0$ such that
\[
\sum_{y \in Rx} w(y) = \Gamma \cdot \left| Rx \right|, \text{ for all } x \in R \setminus \{0\}.
\]

Right homogeneous weights are defined accordingly. If a weight is both left homogeneous and right homogeneous, we call it simply as a homogeneous weight. The constant $\Gamma$ in (11) is called the \textit{average value} of $w$. A homogeneous weight is said to be \textit{normalized} if its average value is 1. We can normalize the weight $w$ in Definition 2.1 by replacing it with $\tilde{w} = \Gamma^{-1}w$ [6].

The weight $w$ is extended naturally to $R^n$, the free module of rank $n$ consisting of $n$-tuples of elements from $R$, via $w(z) = \sum_{i=0}^{n-1} w(z_i)$ for $z = (z_0, z_1, \ldots, z_{n-1}) \in R^n$. The homogeneous distance metric $\delta : R^n \times R^n \rightarrow \mathbb{R}$ is defined by $\delta(x, y) = w(x - y)$, for $x, y \in R^n$.

It was proved in [5] that, if $R$ is Frobenius with generating character $\chi$, then every homogeneous weight $w$ on $R$ can be expressed in terms of $\chi$ as follows.
\[
w(x) = \Gamma \left[ 1 - \frac{1}{\left| R^x \right|} \sum_{u \in R^x} \chi(xu) \right]
\]
where $R^x$ is the group of units of $R$.

For the Galois ring $GR(p^r, m)$ we apply the following homogeneous weight given in [3] for finite chain rings.
\[
w_{\text{hom}}(x) = \begin{cases} 
0 & \text{if } x = 0 \\
p^{m(r-1)} & \text{if } x \in (p^r-1) \setminus \{0\} \\
(p^m - 1)p^{m(r-2)} & \text{otherwise}
\end{cases}
\]
where $(p^r-1)$ is the principal ideal generated by the element $p^r-1$ of $GR(p^r, m)$. Since the Galois ring $GR(p^r, m)$ is a commutative Frobenius ring with identity whose generating character is $\chi(z) = \xi^{b_mz}$, where $\xi = \exp(2\pi i/p^r)$ for $z = \sum_{i=0}^{m-1} b_i(\omega_i^m)$, the weight (13) can be derived from (12). The group of units of $GR(p^r, m)$ has cardinality $p^{m(r-1)}(p^m - 1)$ and it easy to compute from (11) that its average value is equal to
\[
\Gamma = (p^m - 1)p^{m(r-2)}
\]
which is its minimum non-zero value. When $r = 1$, we have $\Gamma = (p^m - 1)/p^m$ and $w_{\text{hom}}$ is just the usual Hamming weight $w_{\text{Ham}}$ on $\mathbb{F}_{p^m}$. When $m = 1$, the average value is $\Gamma = (p - 1)p^{r-2}$ for the integer ring $\mathbb{Z}_{p^r}$.

### 2.4 Codes over $GR(p^r, m)$

A block code $C$ of length $n$ over an arbitrary finite ring $R$ is a nonempty subset of $R^n$. The code $C$ is called right (resp. left) $R$-linear if $C$ is a right (resp. left) $R$-submodule of $R^n$. If $C$ is both left $R$-linear and right $R$-linear, we simply call $C$ a linear block code over $R$. A $k \times n$ matrix over $R$ is called a \textit{generator matrix} of a
linear block code $C$ if the rows span $C$ and no proper subset of the rows generates $C$.

Let the set $B_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be a basis of the Galois ring $\mathcal{R}$ over $\mathbb{Z}_{p^r}$, and $B$ be a linear block code of length $n$ over $\mathcal{R}$. We consider the map $\tau : \mathcal{R} \rightarrow \mathbb{Z}_{p^r}^m$ defined by

\[
\tau(z) = (a_0, a_1, \ldots, a_{m-1})
\]

for $z = a_0\beta_0 + a_1\beta_1 + \ldots + a_{m-1}\beta_{m-1} \in \mathcal{R}$, $a_i \in \mathbb{Z}_{p^r}$. This map is a bijection and can be extended coordinate-wise to $\mathcal{R}^n$. Thus, if $c \in B$ and $c = (c_0, c_1, \ldots, c_{n-1})$, $c_i = \sum_{j=0}^{m-1} a_{ij}\beta_j$, $a_{ij} \in \mathbb{Z}_{p^r}$, then

\[
\tau(c) = (a_{00}, \ldots, a_{0,m-1}, \ldots, a_{n-1,0}, \ldots a_{n-1,m-1})
\]

in $\mathbb{Z}_{p^r}^m$. The image $\tau(B)$ of $B$ under $\tau$ with respect to $B_m$ is called the $p^r$-ary image of $B$, and is obtained by simply substituting each element of $\mathcal{R}$ by the $m$-tuple of its coordinates over $B$. It is easy to prove that $\tau(B)$ is a linear block code of length $mn$ over $\mathbb{Z}_{p^r}$. For the degenerate case $m = 1$, the block code $B$ is a code over $\mathbb{Z}_{p^r}$ and the map $\tau$ is the identity map on $B$. We equip $\tau(B)$ with a homogeneous distance metric with respect to the weight $w_{\text{hom}}$ as given in (13).

The following lemma from [2] will be very useful in the succeeding discussion.

**Lemma 2.2 (Constantinescu, Heise and Honold, 1996)** For any linear block code $C \subseteq \mathbb{Z}_{p^r}^n$ we have

\[
\frac{w_{\text{hom}}(C)}{|C|} = \Gamma \cdot |\{i \mid \pi_i(C) \neq 0\}|
\]

where $w_{\text{hom}}(C)$ is the sum of the homogeneous weights of all codewords of $C$, and $\pi_i$ is the projection from $\mathbb{Z}_{p^r}^n$ onto the $i$-th coordinate.

**3 Major Results**

We denote by $w_{\text{hom}}(S)$ the sum of the homogeneous weights of the elements of set $S$, that is,

\[
w_{\text{hom}}(S) = \sum_{x \in S} w_{\text{hom}}(x).
\]

**Proposition 3.1** For any basis $B_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ we have

\[
\sum_{x \in GR(p^r, m)} w_{\text{hom}}(\tau(x)) = m(p - 1)p^{rm+m-2}.
\]

**Proof:** Let $S = \{x \mid x \in GR(p^r, m)\}$. Then $\tau(S)$ is a linear block code over $\mathbb{Z}_{p^r}$ of length $m$ and cardinality $p^{rm}$. Applying Lemma 2.2 to $\tau(S)$ gives us

\[
\frac{w_{\text{hom}}(\tau(S))}{|\tau(S)|} = \Gamma \cdot w_{\text{hom}}(\tau(S)).
\]
Therefore we have $w_{\text{hon}}(\tau(S)) = |\tau(S)| \cdot \Gamma \cdot w_s(S)$. The value of $\Gamma$ is given in (14), and the support size $w_s(\tau(S))$ of $\tau(S)$ is $m$. Using the notation in (17), the result now follows.

This proposition gives the simple corollary below which was used to prove the bound of Rabizzoni in [9, Theorem 1].

**Corollary 3.2** For any basis $B_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ of $\mathbb{F}_p^m$ over $\mathbb{F}_p$, we have

$$\sum_{x \in \mathbb{F}_p^m} w_{\text{han}}(\tau(x)) = m(p-1)p^{m-1}.$$  

**Proof:** The Galois ring $GR(p, m)$ is the Galois field $\mathbb{F}_p^m$, and the homogeneous weight $w_{\text{hon}}$ given in (13) is the Hamming weight $w_{\text{han}}$ on $\mathbb{F}_p$ with $\Gamma = (p-1)/p$.

The bound of Rabizzoni in [9, Theorem 1] was extended to linear block codes over Galois rings in [10].

Denote by $\text{Mat}_m(R)$ the ring of $m \times m$ matrices over the Galois ring $R = GR(p', m)$. It is known that a matrix $A$ in $\text{Mat}_m(R)$ is nonsingular (or invertible) if and only if $\det A$ is a unit in $R$. We will also use the usual notation $|A|$ for the determinant of $A$. The matrix $A$ is symmetric if and only if $A = A^t$, and is orthogonal if and only if $AA^t = A^tA = I$, where $A^t$ is the transpose of $A$ and $I$ is the identity matrix. We propose the following definition.

**Definition 3.3** Two bases $\{\alpha_i\} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\beta_j\} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ of $GR(p', m)$ over $\mathbb{Z}_{p'}$ are said to be dual if $T(\beta, \alpha) = \delta_{ij}$, where $\delta_{ij}$ is the Kronecker delta.

**Lemma 3.4** The matrix $\Omega \in \text{Mat}_m(R)$ given by

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \omega & \omega^f & \omega^{f^2} & \ldots & \omega^{f^{m-1}} \\ \omega^2 & (\omega^2)^f & (\omega^2)^{f^2} & \ldots & (\omega^2)^{f^{m-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{m-1} & (\omega^{m-1})^f & (\omega^{m-1})^{f^2} & \ldots & (\omega^{m-1})^{f^{m-1}} \end{pmatrix}$$

is nonsingular.

**Proof:** By the definition of the generalized Frobenius automorphism (8), it easy to show that $(\omega^i)^{f^j} = (\omega^{p^j})^i$ for $i, j = 0, 1, \ldots, m-1$. Hence,

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \omega & \omega^p & \omega^{p^2} & \ldots & \omega^{p^{m-1}} \\ \omega^2 & (\omega^2)^p & (\omega^2)^{p^2} & \ldots & (\omega^2)^{p^{m-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{m-1} & (\omega^{m-1})^p & (\omega^{m-1})^{p^2} & \ldots & (\omega^{m-1})^{p^{m-1}} \end{pmatrix}$$

which is a Vandermonde matrix whose determinant is

$$\det \Omega = \prod_{j=1}^{m-1} \prod_{i=j+1}^m (\omega^{p^{j-1}} - \omega^{p^{i-1}}).$$  

Each factor in this product is a unit of $R$ so that $\det \Omega$ is a unit in $R$. 


Lemma 3.5 Let \( \{ \beta_j \} = \{ \beta_1, \beta_2, \ldots, \beta_m \} \) be a basis. The matrix

\[
B = \begin{pmatrix}
\beta_1 & \beta_1^f & \beta_1^{f^2} & \cdots & \beta_1^{f^{m-1}} \\
\beta_2 & \beta_2^f & \beta_2^{f^2} & \cdots & \beta_2^{f^{m-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\beta_m & \beta_m^f & \beta_m^{f^2} & \cdots & \beta_m^{f^{m-1}} \\
\end{pmatrix}
\] (20)

is invertible.

Proof: Express the polynomial basis \( P_m(\omega) \) in (7) in terms of the basis \( \{ \beta_j \} \) as follows.

\[
\begin{pmatrix}
1 \\
\omega \\
\omega^2 \\
\vdots \\
\omega^{m-1}
\end{pmatrix} = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1m} \\
a_{21} & a_{22} & \cdots & a_{2m} \\
a_{31} & a_{32} & \cdots & a_{3m} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mm}
\end{pmatrix} \begin{pmatrix}
\beta_1 \\
\beta_2 \\
\beta_3 \\
\vdots \\
\beta_m
\end{pmatrix}
\]

where \( A = (a_{ij}) \) is a nonsingular matrix over \( \mathbb{Z}_{p^r} \). We compute the matrix product \( AB \). The fact that the Frobenius automorphism \( f \) fixes each \( a_{ij} \) implies that \( AB \) is the Vandermonde matrix \( \Omega \). Hence by Lemma 3.4, \( \det AB \) is a unit in \( \mathcal{R} \). Consequently, \( \det B \) is a unit in \( \mathcal{R} \).

We shall call the matrix \( B \) the automorphism matrix of \( \mathcal{R} \) relative to the basis \( \{ \beta_j \} \).

Corollary 3.6 \((\det B)^2\) is a unit in \( \mathbb{Z}_{p^r} \).

Proof: It can be shown that

\[
BB^t = \begin{pmatrix}
T(\beta_1^2) & T(\beta_1 \beta_2) & \cdots & T(\beta_1 \beta_m) \\
T(\beta_2 \beta_1) & T(\beta_2^2) & \cdots & T(\beta_2 \beta_m) \\
\vdots & \vdots & \ddots & \vdots \\
T(\beta_m \beta_1) & T(\beta_m \beta_2) & \cdots & T(\beta_m^2)
\end{pmatrix}
\] (21)

which is a matrix over \( \mathbb{Z}_{p^r} \). It follows that \((\det B)^2\) is an element of \( \mathbb{Z}_{p^r} \). By Lemma 3.5 we get the result.

Of course, \( \det B \) is not necessarily a unit in the base ring \( \mathbb{Z}_{p^r} \), although it is a unit in \( \mathcal{R} \) according to Lemma 3.5. Please see Example 3.8.

Theorem 3.7 Every basis has a unique dual basis.

Proof: We show the proof for \( m = 3 \) without loss of essential generality. Let \( \{ \beta_1, \beta_2, \beta_3 \} \) be a basis, and consider the automorphism matrix

\[
B = \begin{pmatrix}
\beta_1 & \beta_1^f & \beta_1^{f^2} \\
\beta_2 & \beta_2^f & \beta_2^{f^2} \\
\beta_3 & \beta_3^f & \beta_3^{f^2}
\end{pmatrix}
\]
which is nonsingular by Lemma 3.5. Let \( \text{adj} \, B = (b_{ij}) \) where \( b_{ij} = (-1)^{i+j}|B_{ji}| \). Then

\[
\text{adj} \, B = \begin{pmatrix}
\lambda_1 & \lambda_2 & \lambda_3 \\
\lambda_1^j & \lambda_2^j & \lambda_3^j \\
\lambda_1^j & \lambda_2^j & \lambda_3^j
\end{pmatrix}
\]

where \( \lambda_1 = \beta_1^j \beta_2^j - \beta_2^j \beta_3^j \), \( \lambda_2 = \beta_1^j \beta_3^j - \beta_1^j \beta_2^j \), and \( \lambda_3 = \beta_1^j \beta_2^j - \beta_1^j \beta_2^j \) so that \( B^{-1} = |B|^{-1} \text{adj} \, B \). Note that

\[
BB^{-1} = |B|^{-1} \begin{pmatrix}
T(\beta_1 \lambda_1) & T(\beta_1 \lambda_2) & T(\beta_1 \lambda_3) \\
T(\beta_2 \lambda_1) & T(\beta_2 \lambda_2) & T(\beta_2 \lambda_3) \\
T(\beta_3 \lambda_1) & T(\beta_3 \lambda_2) & T(\beta_3 \lambda_3)
\end{pmatrix}
\]

Following the argument of \([1]\) it can be shown by using the generalized trace that \( \{\lambda_1/|B|, \lambda_2/|B|, \lambda_3/|B|\} \) is a linearly independent set, and hence is the unique dual of \( \{\beta_j\} \).

**Example 3.8** The polynomial basis for \( GR(4, 2) \) is the set \( \{1, \omega\} \) where \( 1 + \omega + \omega^2 = 0 \). The automorphism matrix is

\[
B = \begin{pmatrix}
1 & 1 \\
\omega & 3 + 3\omega
\end{pmatrix}
\]

with determinant \( 3 + 2\omega \) which is a unit in \( GR(4, 2) \). Observe that \( (3 + 2\omega)^2 = 1 \) is a unit in \( \mathbb{Z}_4 \). The inverse

\[
B^{-1} = \begin{pmatrix}
3 + \omega & 1 + 2\omega \\
2 + 3\omega & 3 + 2\omega
\end{pmatrix}
\]

gives \( \{3 + \omega, 1 + 2\omega\} \) as the dual of the polynomial basis.

**Example 3.9** The polynomial basis for \( GR(4, 3) \) is the set \( \{1, \omega, \omega^2\} \) where \( \omega \) is the root of the basic primitive polynomial \( x^3 + 2x^2 + x - 1 \) over \( \mathbb{Z}_4 \). The automorphism matrix is given by

\[
B = \begin{pmatrix}
1 & 1 & 1 \\
\omega & \omega^2 & \omega^4 \\
\omega^2 & \omega^4 & \omega
\end{pmatrix}
\]

with determinant \( 3 \). The inverse is given by

\[
B^{-1} = \begin{pmatrix}
\omega + 3\omega^3 & w + 3\omega^4 & w^2 + 3\omega^4 \\
\omega^2 + 3\omega^6 & 3\omega + \omega^2 & 3\omega + \omega^4 \\
\omega^4 + 3\omega^5 & 3\omega^2 + \omega^4 & \omega + 3\omega^2
\end{pmatrix}
\]

so that \( \{3 + 2\omega + 2\omega^2, 2 + 2\omega + \omega^2, 2 + \omega + 2\omega^2\} \) is the dual basis. This corrects the mistake in \([1, \text{Example 1}]\).

**Example 3.10** The dual of the polynomial basis for \( \mathbb{Z}_8[\omega] \), where \( \omega \) is the root of the basic primitive polynomial \( 7 + 5x + 6x^2 + x^3 \) over \( \mathbb{Z}_8 \), is the set \( \{3 + 6\omega + 6\omega^2, 6 + 2\omega + 5\omega^2, 6 + 5\omega + 2\omega^2\} \).
We apply Definition 3.3 for the notion of self-dual basis.

**Definition 3.11** The basis \( \{ \beta_1, \beta_2, \ldots, \beta_m \} \) is self-dual if \( T(\beta_i \beta_j) = \delta_{ij} \).

**Definition 3.12** A normal basis of \( GR(p^r, m) \) is a basis of the form \( \{ \alpha, \alpha^f, \ldots, \alpha^{f^{m-1}} \} \) where \( \alpha \in GR(p^r, m) \) and \( f \) is the generalized Frobenius automorphism given in (8).

In this case we say that \( \alpha \) generates \( \beta_m \).

We have the following immediate results.

**Theorem 3.13** Let \( \{ \beta_j \} \) be a basis with automorphism matrix \( B \). Then \( B \) is or-thogonal if and only if \( \{ \beta_j \} \) is self-dual.

**Proof:** From (21) we get \( BB^t = I \iff T(\beta_i \beta_j) = \delta_{ij} \).

**Theorem 3.14** Let \( \{ \beta_j \} \) be a basis with automorphism matrix \( B \). Then the follow-ing statements are equivalent.

(i) The basis \( \{ \beta_j \} \) is a normal basis.

(ii) The automorphism matrix \( B \) is a symmetric matrix.

(iii) The Frobenius automorphism \( f \) is the \( m \)-cycle \( \beta_1 \mapsto \beta_2, \beta_2 \mapsto \beta_3, \ldots, \beta_m \mapsto \beta_1 \).

**Proof:** This equivalence is evident from the construction of the automorph ism matrix in (20). The basis \( \mathcal{B}_m = \{ \beta_j \} \) is normal \( \Leftrightarrow \beta_1 \) generates \( \mathcal{B}_m \), that is, \( \beta_2 = \beta_1^f, \beta_3 = \beta_2^f = \beta_1^{f^2}, \ldots, \beta_{m-2} = \beta_{m-1}^f = \beta_m, \beta_m = \beta_1^{f^{m-1}}, \beta_{m-1}^f = \beta_1^f, \ldots, \beta_3 \mapsto \beta_2, \beta_2 \mapsto \beta_3, \ldots, \beta_m \mapsto \beta_1 \).

**Example 3.15** The set \( \mathcal{B}_2 = \{ \omega, \omega^2 = 3 + 3\omega \} \) is a normal basis for \( \mathbb{Z}_4[x]/(x^2 + x + 1) \). The automorphism matrix relative to this basis is given by

\[
\begin{pmatrix}
\omega & 3 + 3\omega \\
3 + 3\omega & \omega
\end{pmatrix}
\]

which is not orthogonal, hence \( \mathcal{B}_2 \) is not self-dual. However \( B \) is symmetric.

**Example 3.16** The set \( \mathcal{B}_3 = \{ 1 + \omega, 1 + \omega^2, 3 + 3\omega + 3\omega^2 \} \) of \( GR(4, 3) = \mathbb{Z}_4[x]/(x^3 + 2x^2 + x + 3) \) is a self-dual normal basis as the automorphism matrix is both orthogonal and symmetric.

**References**


