International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:8, 2011

Pontrjagin Duality and Codes over Finite Commutative Rings

Khalid Abdelmoumen, Mustapha Najmeddine, Hussain Ben-Azza

Abstract—We present linear codes over finite commutative rings which are not necessarily Frobenius. We treat the notion of syndrome decoding by using Pontrjagin duality. We also give a version of Delsarte's theorem over rings relating trace codes and subring subcodes.

Keywords—Codes, Finite Rings, Pontrjagin Duality, Trace Codes.

I. Introduction

We recall some notions of algebra useful for the following discussion (see [3] for more background). The reader may skip to the next sections.

Here, we consider an unitary ring A, which is not necessarily commutative. An $A-$module I is said injective if for any injection $i : M \to N$ of $A-$modules and for every linear application $f : M \to I$, there exists a linear application $g : N \to I$ such that $f = g \circ i$. A submodule N of an $A-$module M is said essential if for every submodule $L \neq 0$, we have $N \cap L \neq 0$. We denote by $Soc(M)$ the socle of an $A-$module M which is the intersection of all essential submodules, and $J(A)$ is the Jacobson radical (it is the intersection of all non-trivial maximal ideals of A). For a left ideal I, resp. a right ideal K, of A the annihilators are $l(I) = \{a \in A : aI = 0\}$ and $r(I) = \{a \in A : Ia = 0\}$. An Artinian ring A is said quasi-Frobenius if for any left ideal I and right ideal K, we have

$$l(r(I)) = I, r(l(K)) = K. \quad (1)$$

Furthermore, if $Soc(A) \simeq A/J(A)$, then A is said Frobenius. If the ring is commutative, then the two notions coincide, and the relation (1) becomes $l^2(I) = I$.

Wood [1] has shown the fundamental result that The MacWilliams relation holds for a code if and only if the ring is quasi-Frobenius, in the framework of linear functional-based duality. This result singles out the class of codes over quasi-Frobenius rings. But we make emphasis here on finite commutative rings, not necessarily Frobenius, and on Pontrjagin duality.

In the sequel of this paper, we consider a finite commutative ring A of cardinality q. Paragraph II introduces the concept of linear codes over a ring. Paragraph III recalls Pontrjagin duality and basic facts (such as a module over A is isomorphic to its bidual) . Paragraph IV presents syndrome decoding. In Paragraph V the control matrix is introduced for a $A-$code with a free dual, and we also show how a code is decomposed in terms of its local codes (that is codes over local rings). In paragraph VI, we present an example. Paragraph VII gives a version of Delsarte's theorem for the ring extension $A \subseteq B$, requiring the existence of a nondegenerate bilinear 'form' with values in the Pontrjagin dual of A and that the subring A is Frobenius. The last section is a conclusion for further investigations.

K.Abdelmoumen is with the Department of Mathematics Faculty of sciences and thechnology Sidi Mohammed ben Abdellah Fès Morocco e-mail: abkhalid9@gmail.com

M.Najmeddine is with the Department of Mathematics ENSAM My Ismaïl University Meknès Morocco e-mail: najmeddine.mustapha@gmail.com

H.Ben-Azza is with the Department of Mathematics ENSAM My Ismaïl University Meknès Morocco e-mail: hbenazza@yahoo.com

II. Definitions

Definition 1:
1) A linear code C over A of length n is a submodule of A^n. (we also say that C is a linear $A-$code.)
2) A linear code of length n free over A of rank k is said an $[n, k]-$code over A.

Definition 2:
1) The Hamming distance between x and y in A^n is $d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$.
2) The Hamming weight of $x \in A^n$ is $w(x) = d(x, 0)$.
3) The minimal distance of a code C is $d(C) = \min\{d(x, y) : x \neq y \in C\} = \min\{w(c) : c \in C \setminus \{0\}\}$.

Definition 3: Let C be an $[n, k]-$code linear over A with basis $(e_1, \dots, e_k)$.
1) The matrix $G \in \mathscr{M}_{k,n}(A)$ with lines $e_i, 1 \leq i \leq k$ is said the generator matrix of C.
2) The message $m \in A^k$ is encoded by the codeword $c = mG \in C$.

III. Pontrjagin Duality

A general background reference for Pontrjagin duality is [7]. Let M be an $A-$module and $\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq \{z \in \mathbb{C} :| z |= 1\}$ the one dimensional torus.

Definition 4: A charater of M is a group homomorphism from $(M, +)$ to $\mathbb{T}$.

A character χ is trivial over a subset N of M if $\forall x \in N, \chi(x) = 1$. We define a addition on characters by : for χ and χ' and all $x \in M$,

$$(\chi + \chi')(x) = \chi(x)\chi'(x).$$

The set of characters $\widehat{M}$. is an abelian group. We define for a character $\chi \in \widehat{M}$, a scalar $a \in A$ and an element $x \in M$

$$(a \cdot \chi)(x) = \chi(ax).$$

Thus $\widehat{M}$ is an $A-$module.

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:5, No:8, 2011

Definition 5: 1) The orthogonal of a submodule N of M is the submodule of $\widehat{M}$:

$$N^{\perp} = \{\chi \in \widehat{M} : \chi = 1 \text{ over } N\}$$

2) The dual of $\widehat{M}$, denoted $\widehat{\widehat{M}}$, is called the bidual of M.
3) The orthogonal of a submodule H de $\widehat{M}$ is the submodule of M :

$$H^{\perp} = \{x \in M : (\forall \chi \in H), \chi(x) = 1\}.$$

4) The bi-orthogonal of N is the orthogonal $N^{\perp\perp} \subset M$ of $N^{\perp}$.

Theorem 1 (Extension): If N is a submodule of M, then the modules $\widehat{M/_N}$ and $N^{\perp}$ are isomorphic .

Theorem 2 (Separation): Suppose that M is a module of finite cardinality. Let N be a submodule and $x \in M$.

1) A necessary and sufficient condition for $x = 0$ is that for all $\chi \in \widehat{M}, \chi(x) = 1$.
2) $x \in N$ if and only if every character of M trivial on N is also trivial at x.
3) The module M is rflexive (i.e., isomorphic to its bidual).
4) The modules N and $N^{\perp\perp}$ are isomorphic.

IV. Syndrome Decoding

Let C be a linear $A-$code of length n, of minimal distance d and $t = \left[\dfrac{d-1}{2}\right]$.

Definition 6: The syndrome of $x \in A^n$ is $s(x) = (\chi(x))_{\chi \in C^{\perp}}$.

Proposition 1: Let $x \in A^n$. Then $x \in C$ iff $s(x) = 1 = (1_{\chi})_{\chi \in C^{\perp}}$ where $1_{\chi} = 1 \in \mathbb{T}$.

Proof

That the condition is necessary is a consequence of the orthogonal of C. Conversely, suppose that $s(x) = 1$. then for all $\chi \in C^{\perp}$, $\chi(x) = 1$. So, $x \in C^{\perp\perp} = C$. □

Proposition 2: Two elements x and y of A^n have the same class in $A^n/_C$ iff they have the same syndrome.

Proof

Note that every character $\chi : A^n \to \mathbb{T}$ is a group morphism to the multiplicative group $\mathbb{T}$. The group $\mathbb{T}^{|C^{\perp}|}$ is equiped with pointwise multiplication. We have:

$$\begin{array}{rcl} \bar{x} = \bar{y} & \Longleftrightarrow & x - y \in C \\ & \Longleftrightarrow & s(x-y) = 1 \\ & \Longleftrightarrow & \chi(x-y) = 1, \forall \chi \in C^{\perp} \\ & \Longleftrightarrow & \chi(x)\chi(y)^{-1} = 1, \forall \chi \in C^{\perp} \\ & \Longleftrightarrow & \chi(x) = \chi(y), \forall \chi \in C^{\perp} \\ & \Longleftrightarrow & s(x) = s(y) \end{array}$$

□

Remark 1: Let y be the received word and e the associated error vector . Then $c = y - e \in C$ and $s(y) = s(e)$.

Proposition 3: Let e be the error vector of weight $\leq t$ and syndrome s. Then e is the unique vector of weight $\leq t$ and with syndrome s.

Proof

Let $e' \in A^n$ of weight $\leq t$ and $s(e) = s(e')$. Then, by the proposition 2, we have $e - e' \in C$.

$$\begin{array}{rcl} w(e-e') & = & d(e-e') \\ & = & d(e,e') \\ & \leq & d(e,0) + d(0,e') \\ & \leq & w(e) + w(e') \\ & \leq & 2t < d \end{array}$$

So $e - e' = 0$ and $e = e'$. □

Based on these results, we describe a syndrome decoding algorithm which computes the error vector:
Input : received noisy word $y \in A^n$.
Output : codeword c nearest to y.

1) Compute the syndrome $s(y)$ of y.
2) Determine the class $\bar{y}$ of y modulo C.
3) Determine the vector $e \in \bar{y}$ of weight $\leq t$ with $s(y) = s(e)$.
4) Return $c = y - e \in C$.

V. Control Matrix

Let C be an $[n,k]-$code linear over A such that $C^{\perp}$ is free over A.

Proposition 4: All the bases of $C^{\perp}$ have the same cardinality and $C^{\perp}$ is an $[n, n-k]-$code linear over A.

Proof

Let h be the cardinal of a basis of $C^{\perp}$. By theorem 1, $C^{\perp}$ and $\widehat{A^n/_C}$ are isomorphic, and

$$\left|C^{\perp}\right| = \left|\widehat{A^n/_C}\right| = \left|A^n/_C\right| = \left[A^n : C\right] = \frac{|A^n|}{|C|}.$$

Therefore, $q^n = q^k q^h$ and $h = n - k$. Thus, $C^{\perp}$ is an $[n, n-k]-$code. □

A linear $A-$code is said local when the underlying ring is local. We will indicate how a general linear $A-$code C is the product of local codes and will give a condition for $C^{\perp}$ to be free when C is free. We are indebted to and inspired by the work of [5] for the next proposition. Let $M_1, ..., M_l$ be the set of maximal ideals of A. For each ideal I denote by $i(I) = min\{j : I^j = I^{j+1}\}$ the nilpotency of I. Let $A_i = A/M_i^{i(M_i)}$ the local ring with maximal ideal $M_i/M_i^{i(M_i)}$. Then

$$A = \prod_{i=1}^{l} A_i \tag{2}$$

By using the Chinese remainder theorem we get

$$C = \prod_{i=1}^{l} C_i \tag{3}$$

Thus the decomposition of a ring as (2) induces a decomposition of a code (3) as a product of its 'local codes.' Also we have $d(C) \leq min\{d(C_i) : 1 \leq i \leq l\}$. Using the property that the character of a product is the product of characters, and from (3), we get a decomposition of the dual

$$C^{\perp} = \prod_{i=1}^{l} C_i^{\perp} \tag{4}$$

We recall that an $A-$module is said *projective* if it is a direct summand of a free $A-$module[9], and since a projective module over a local ring is free, we have

Proposition 5: Suppose C is free. Then $C^{\perp}$ is free iff each of its local codes $C_i^{\perp}$ is projective.

Remark 2: Since a linear $A-$code C is trivially Noetherian and Artinian, it admits a composition series (or a Jordan-Hölder series), and we may study the concept of its length (as an $A-$module), even if the code is not free.

Definition 7: The matrix $H \in \mathscr{M}_{n-k,n}(A)$ formed by the lines of a basis vectors of the code $C^{\perp}$ is called the control matrix of C.

Proposition 6: Suppose that $A = \mathbb{Z}/_{m\mathbb{Z}}$ and that H is the control matrix of C. Then, for all $x, y \in A^n$:

1) $s(x) = 1$ iff $Hx^t = 1$.
2) $s(x) = s(y)$ iff $Hx^t = Hy^t$.

Proof

1) That the condition is necessary is trivial .
Conversely, Suppose that $Hx^t = 1$. Let

$$H = \begin{pmatrix} \chi_{11} & \cdots & \chi_{1n} \\ \vdots & \ddots & \vdots \\ \chi_{n-k,1} & \cdots & \chi_{n-k,n} \end{pmatrix}$$

Then for all $i = 1 \ldots n-k,\ e_i = (\chi_{i1}, \ldots, \chi_{in}) \in C^{\perp}$. Let $\chi \in C^{\perp}$, then there exists $a_1, \ldots, a_{n-k}$ in A such that $\chi = \sum_{i=1}^{n-k} a_i e_i$. We have

$$\begin{aligned} \chi(x) &= \prod_{i=1}^{n-k} (a_i e_i)(x) \\ &= \prod_{i=1}^{n-k} e_i(a_i x) \\ &= \prod_{i=1}^{n-k} (e_i(x))^{a_i} = 1 \end{aligned}$$

Therefore, $s(x) = 1$.

2) uses 1). ☐

Proposition 7: Let H be the control matrix of a code C. Then the minimal distance of C is the minimal number of dependent columns of H.

Proof

Let d be the minimal distance of C, $v_1, \ldots, v_n$ column vectors of H, $c = (c_1, \ldots, c_n) \in C$ of weight $w(c) = d$ and $I = \{i \in \{1, \ldots, n\} : c_i \neq 0\}$. Then $|I| = d$ and $\sum_{i \in I} c_i v_i = 0$. So, $(v_i)_{i \in I}$ is a dependent family.
Conversely, let $(v_i)_{i \in J}$ be a dependent family. Then there exists $(\alpha_i)_{i \in J} \subset A$ such that $\sum_{i \in J} \alpha_i v_i = 0$. Let $c = (\alpha_1, \ldots, \alpha_n) \in A^n$ such that for all $i \notin J,\ \alpha_i = 0$. Then $Hc^t = 1$ and $c \in C$. So, $|J| \geq d$. ☐

VI. An Example

We give a simple example illustrating the concepts studied above.

Let $A = \mathbb{Z}/_{4\mathbb{Z}}$ and C the linear code over A of length 5 and generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 3 & 0 \\ 0 & 1 & 1 & 0 & 3 \end{pmatrix}$$

Let $v_1 = (1,0,1,3,0)$ and $v_2 = (0,1,1,0,3)$ be the lines of G. We have $\widehat{A} = \left\{1, \psi, \psi^2, \psi^3\right\}$, such that $\psi(1) = \omega$ and $1(1) = 1 \in \mathbb{T}$ where ω is a primitive root of order four of unity . The Pontrjagin dual of A^5 is $\widehat{A}^5$. We will determine a control matrix H of C. Let $\chi = (\chi_1, \chi_2, \chi_3, \chi_4, \chi_5) \in \widehat{A^5}$ such that $\chi_1(1) = \omega_1,\ \chi_2(1) = \omega_2, \chi_3(1) = \omega_3,\ \chi_4(1) = \omega_4$ and $\chi_5(1) = \omega_5$. We have

$$\begin{aligned} \chi \in C^{\perp} &\iff \begin{cases} \chi(v_1) = 1 \\ \chi(v_2) = 1 \end{cases} \\ &\iff \begin{cases} \omega_1 \omega_3 \omega_4^3 = 1 \\ \omega_2 \omega_3 \omega_5^3 = 1 \end{cases} \\ &\iff \begin{cases} \omega_4 = \omega_1 \omega_3 \\ \omega_5 = \omega_2 \omega_3 \end{cases} \end{aligned}$$

Then $\chi(1) = \left(\omega_1, \omega_2, \omega_3, \omega_2, \omega_1 \omega_3^2\right)$. There exists $\alpha_1, \alpha_2, \alpha_3$ and α_3 in A such that for all $i = 1..3,\ \omega_i = \omega^{\alpha_i}$. Then $\chi = \alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \alpha_3 \varphi_3$ where $\varphi_1(1) = (\omega, 1, 1, \omega, 1)$, $\varphi_2(1) = (1, \omega, 1, 1, \omega)$ et $\varphi_3(1) = (1, 1, \omega, \omega, \omega)$. Therefore, $C^{\perp}$ is free and the following matrix

$$H = \begin{pmatrix} \omega & 1 & 1 & \omega & 1 \\ 1 & \omega & 1 & 1 & \omega \\ 1 & 1 & \omega & \omega & \omega \end{pmatrix}$$

is the control matrix of C. By proposition 7, the minimal distance of C is $d = 3$ and this permits to detect 2 errors and to correct one error, $t = \left[\frac{d-1}{2}\right] = 1$. Let $c = 11233 \in C$ the transmitted message and $y = 11213$ the received noisy word. In order to detect an error, we compute the syndrome of y :

$$Hy^t = \begin{pmatrix} \omega^2 \\ 1 \\ \omega^2 \end{pmatrix} \neq 1$$

Thus the message is erroneous. The class of y modulo C is $\overline{y} = \{x = (x_1, x_2, x_3, x_4, x_5) : s(x) = s(y)\}$.

$$\begin{aligned} s(x) = s(y) &\iff Hx^t = Hy^t \\ &\iff \begin{cases} x_1 + x_4 = 2 \\ x_2 + x_5 = 0 \\ x_3 + x_4 + x_5 = 2 \end{cases} \\ &\iff \begin{cases} x_4 = 2 + 3x_1 \\ x_5 = 3x_2 \\ x_3 = x_1 + x_2 \end{cases} \end{aligned}$$

By theorem 2, C is defined by the equations

$$\begin{cases} x_4 = 3x_1 \\ x_5 = 3x_2 \\ x_3 = x_1 + x_2 \end{cases}$$

and $\overline{y} = \overline{e}$, with $e = 00020$. Since $d = 3$ and $w(e) = 1 \leq t$, e is the convenient error. Thus the transmitted codeword is $y - e = 11233 = c$.

VII. Trace Codes

A. Generalities

Let $k = \mathbb{F}_q \subset K = \mathbb{F}_{q^m}$ be a finite Galois field extension. For a K-linear code C, we denote by $C^\perp$ the dual code with respect to the usual inner product, $Res(C) = C_{|k} = C \cap k^n$ the code restricted to k, and $Tr(C) = \{Tr(c) : c \in C\}$ the trace code.

Theorem 3 (Delsarte): For a K-linear code C, we have

$$Res(C)^\perp = Tr(C^\perp)$$

Our aim is to give a version of this theorem over finite commutative rings, following the proof given in [4].

In the following A, B designate finite commutative rings with identities and n is a nonnegative integer. We recall the

Definition 1: We say that $C \subseteq B^n$ is a linear $B-$code if C is a submodule of B^n.

Suppose that $A \subseteq B$ is a ring extension such that B is an $A-$algebra with dimension $dim_A B = m$ and basis $(w_i)_{1\le i\le m}$. Then we define the trace function

$$Tr_{B/A} = Tr : B \to A$$

$$b \mapsto Tr_{B/A}(b) = Tr_{B/A}(bw_i)_{1\le i\le m} = Tr((\alpha_{ij})_{1\le j\le m})$$

where $bw_i = \sum_{i=1}^m \alpha_{ij} w_j$, extended to

$$Tr : B^n \to A^n, (b_i)_i \mapsto (Tr(b_i))_i.$$

It is easy to see that for every $a \in A$, we have $Tr_{B/A}(a) = ma$. Recall that the characteristic of a ring A denoted $charA$ is the least positive integer p such that for all $x \in A$, $px = 0$.

Lemma 1: If $charA$ does not divide m, then the trace function is nonzero.

For an extension $A \subseteq B$ and a linear $B-$code C, we define the trace code and the restricted code, respectively:

$$Tr(C) = \{Tr(c) : c \in C\}$$

$$Res(C) = C_{|A} = C \cap A^n$$

We recall the following fundamental and well-known

Lemma 2: [3] If A is a ring, then $\hat{A}$ is in injective as an $A-$module.

B. A form of Delsarte's theorem

We make the following hypothesis : there exists a nondegenerate bilinear form $\beta_A = \beta : A \times A \to \hat{A}$ extended to

$$\beta_A : A^n \times A^n \to \hat{A}, (x, y) \mapsto \sum_{i=1}^n \beta_A(x_i, y_i).$$

For C a linear $A-$code, we define its $\beta-$dual as

$$l_{\beta_A}(C) = \{a \in A^n : \beta_A(a, b) = 0, \forall b \in C\} \subseteq A^n$$

We need the following result which is called the double annihilator property, which is well documented in [1], [2]

Lemma 3: let $C \subseteq C'$ be a linear codes over a *Frobenius* ring A. Then

$$l^2_{\beta_A}(C) = C \text{ and } l_{\beta_A}(C') \subseteq l_{\beta_A}(C).$$

Suppose $A \subseteq B$ is a ring extension such that A is equipped with the form $\beta_A = \beta$. Then, by lemma 2, there exists $\beta' : B^n \times B^n \to \hat{A}$ such that $\beta'_{|A^2} = \beta$ (extension). Furthermore, we will use the existence of an isomorphism $\rho : \hat{A} \to A$ and that $\beta : A^n \times A^n \to \hat{A} \simeq A$ is given by the matrix $M = (m_{ij})_{n\times n}$ with values in A :

$$\beta(x, y) = \sum_{i,j=1}^n m_{ij} x_i y_j.$$

Note that the group isomorphism $\rho : \hat{A} \to A$ is obtained by a standard use of the main theorem of the decomposition of a finite abelian group in terms of cyclic groups. In the following, we will identify $\rho\beta$ with β and make use of the matrix representation M of β.

Lemma 4: Let $f : B \to A$ be a linear map, extended to B^n by $f(b_1, ..., b_n) = (f(b_1), ..., f(b_n))$. Then for every $a, b \in B^n$, we have $\beta'(f(b), a) = f(\beta'(b, a))$.

Proof

We have

$$\beta'(f(b), a) = \sum_{i,j} m_{i,j} f(b_i) a_j = \sum_i f(b_i) \sum_j m_{i,j} a_j$$

$$= \sum_i f(b_i \sum_j m_{i,j} a_j) = f(\sum_i b_i \sum_j m_{i,j} a_j)$$

$$= f(\beta'(b, a))$$

□

In particular, for the trace function, $\beta'(Tr(b), a) = Tr(\beta'(b, a))$.

Theorem 4: For any linear $B-$code C, and for A Frobenius, if $charA$ does not divide m, then

$$Tr(l_{\beta'}(C)) = l_\beta(C_{|A})$$

Proof

We show that $Tr(l_{\beta'}(C)) \subseteq l_\beta(C_{|A})$. Let $a = Tr(b) = (Tr(b_i)_{1\le i\le n})$, where $b \in l_{\beta'}(C)$. Then

$$\forall c \in C, \beta'(b, c) = 0. \tag{5}$$

Let $a' \in Res(C)$. We have

$$\beta(a, a') = \beta(Tr(b), a) = \sum_{i=1}^n \beta(Tr(b_i), a'_i).$$

Then, by lemma 4 we have $\beta(a, a') = \sum_{i=1}^n Tr(\beta(b, a'))$. It follows from (5) that $\beta(a, a') = 0$.

Conversely, we show the inverse inclusion. By lemma 3, this is equivalent to showing $l_\beta(Tr(l_{\beta'}(C))) \subseteq C_{|A}$. Suppose that this is not the case. Let $u \in l_\beta(Tr(l_{\beta'}(C))) \setminus C_{|A}$. Then $\exists v \in l_\beta(C_{|A})$ such that $\beta(u, v) \neq 0$. note that we are using the identification $\rho : \hat{A} \simeq A$; thus $\beta(u, v)$ is identified with $\rho(\beta(u, v))$. By lemma 1, $\exists \gamma \in B$ such that $Tr(\gamma{\cdot}\beta(u, v)) \neq 0$. Using lemma 4, we have

$$\beta(u, Tr(\gamma v)) = Tr(\gamma\beta(u, v)) \neq 0.$$

But $\forall x \in Tr(l_{\beta'}C)), \beta(u, x) = 0$ and $\gamma v \in l_{\beta'}(C)$. So, $\beta(u, Tr(\gamma v)) = 0$. A contradiction. □

Remark 3: We may also give a version of this theorem by considering $\beta_B : B^2 \to \hat{B}$ and its restriction $\beta_{B\downarrow A}$ to A. Then we may have the following version

$$Tr(l_{\beta_B}(C)) = l_{\beta_{B\downarrow A}}(C_{|A})$$

VIII. Conclusion

In this paper, we have studied block codes over finite commutative rings A, giving a concept of syndrome in the framework of Pontrjagin duality. Also, an analogue of Delsarte's theorem is proved. We note that a comparison between linear functional-based duality and Pontrjagin duality has been treated for 'projective codes'[5]. It is well known [6] that the ring A has a unique decomposition

$$A = A_1 \bigoplus ... \bigoplus A_m,$$

where each A_i is a local ring. This in turn gives a decomposition of the code in terms of 'local codes', which suggests further investigation of codes over local rings (both for encoding and decoding). With the notation of section VII, if we suppose that the extension $A \subseteq B$ of local rings is Galois [9], with Galois group G, then it is easy to see that if a $B-$code is $G-$invariant then $Res(C) = Tr(C)$. This result and its converse are proved in the case of finite fields in [8].

As a general conclusion, more examination of particular codes over rings (such as cyclic codes) is possible, with use of Pontrjagin duality.

Acknowledgment

The third author would like to thank the two institutions, Académie Hassan II and Moulay Ismail University, for their support. Thanks also to the colleagues attending the seminar on 'codes and cryptography' in Fes, specially M. Boulagouaz.

References

[1] J. Wood J. Duality for modules over finite rings and applications to coding theory. Amer. J. Math. 121, pp. 555-575 (1999).
[2] J. Wood J. Foundations of Linear Codes defined over Finite Modules : The extension Theorem and the MacWilliams Identities. In ' Codes over Rings, Proceedings of the CIMPA Summer School, Ankara, Turkey, 18–29 August 2008, Patrick Sol, editor', Series on Coding Theory and Crytology, Vol. 6, World Scientific, Singapore, 2009, pp. 124–190.
[3] C. W. Curtis and I. Reiner. Representation Theory of Finite Groups and Associative Algebras. Interscience Publishers, 1962.
[4] H. Stichtenoth. Algebraic Function Fields and Codes. Springer, 1993.
[5] S. T. Dougherty and H. Liu, Independence of vectors in codes over rings, Designs, Codes and Cryptography, Volume 51, Number 1, 55-68, 2009.
[6] M. F. Atiyah and I. G. Macdonald. Introduction to commutative Algebra. Addison-Wesley, 1969.
[7] W. Rudin. Fourier Analysis on Groups, Wiley-Interscience, 1990.
[8] M. Giorgetti and A. Previtali. Galois invariance, traces codes and subfield subcodes. Finite Fields and Their Applications 16(2): 96-99 (2010).
[9] B. A. McDonald. Finite Rings with Identity. Marcel Dekker, 1974.