

Duals over Artinian Rings and the MacWilliams Identity

6 AUG, 1999

Thomas Mittelholzer
IBM Zurich Research Laboratory
Säumerstrasse 4
CH-8803 Rueschlikon, Switzerland
Email: tmi@zurich.ibm.com

Abstract Linear codes over commutative artinian rings R are considered. For a linear functional based definition of duality, it is shown that the class of length- n linear block codes over R should consist of projective submodules of the free module R^n . For this class, the familiar duality properties from the field case can be generalized to the ring case. In particular, the MacWilliams Identity is derived for linear codes over any finite commutative ring. For commutative artinian rings, the duality concept of linear block codes is extended to convolutional codes.

1 Introduction

Recently duality of modules over a finite ring R has been studied in [1], where it was shown that if R is a quasi-Frobenius ring (i.e., R is injective as an R -module) then the duality concept based on Pontryagin duality via characters is equivalent to the duality concept based on linear functionals. In that study, the underlying category of codes consisted of all finitely generated R -modules. In this paper, we will restrict the category of codes to projective modules that are submodules of R^n . As a consequence of this reduction, one can extend the class of rings for which the usual duality properties hold.

The linear functional-based *dual (or orthogonal)* of an R -submodule $M \subset R^n$ is defined via orthogonality in R^n , i.e., $M^\perp = \{f \in \text{Hom}(R^n, R) : f(\mathbf{c}) = 0 \text{ all } \mathbf{c} \in C\}$, which is equivalent to

$$M^\perp = \{\mathbf{x} \in R^n : \mathbf{x} \cdot \mathbf{m}^T = 0, \text{ all } \mathbf{m} \in M\}.$$
 ¹ (1)

The motivation for this paper arose from the following example of a code over a non quasi-Frobenius ring, where character-based duality and the duality concept based on linear functionals do not agree.

Example 1 *The commutative ring $R = GF(2)[x, y]/(x^2, y^2, xy)$ is artinian but not quasi-Frobenius (i.e., R is not injective as an R -module). Let $C \subset R^2$ be the free rank-1 module generated by the systematic encoding matrix*

$$G = [1 \quad 1 + x + y],$$

i.e., the code C equals

$$\{[0 \ 0], [1 \ 1 + x + y], [1 + x + y \ 1], [x \ x], [y \ y], [1 + x \ 1 + x], [1 + y \ 1 + y], [x + y \ x + y]\}.$$

The parity check matrix for this code is equal to the generator matrix, $H = G$; that is, the code is self-dual, $C^\perp = C$, when using the linear functional duality concept.

Pontryagin duality is based on the notion of a continuous character, that is of a continuous group-homomorphism from the additive group of R to the multiplicative group of the complex number field \mathbf{C} . Let \hat{R} denote the set of all such homomorphisms. As an additive group, R is isomorphic to \mathbf{Z}_2^3 , viz.,

$$\phi : \mathbf{Z}_2 \cdot 1 \oplus \mathbf{Z}_2 \cdot x \oplus \mathbf{Z}_2 \cdot y \rightarrow R$$

where $\phi(r_1, r_x, r_y) = r_1 + r_x x + r_y y$. The set of all characters \hat{R} is an abelian group. One can show that there is an isomorphism $\alpha : R \rightarrow \hat{R}$ such that every $a = a_1 + a_x x + a_y y$ defines a character $\alpha(a) = \chi_a$, which operates on an element $r = r_1 + r_x x + r_y y$ by

$$\chi_a(r) = (-1)^{a_1 \cdot r_1 + a_x \cdot r_x + a_y \cdot r_y}.$$

The character-based dual of the code C is defined by orthogonality:

$$C^\perp = \{[\chi^{(1)}, \chi^{(2)}] \in \hat{R}^2 : \chi^{(1)}(c_1) \cdot \chi^{(2)}(c_2) = 1, \text{ all } [c_1 \ c_2] \in C\}.$$
 (2)

When viewed as subgroup of R^2 , the Pontryagin dual $\alpha^{-1}(C^\perp)$ equals

$$\{[0 \ 0], [1 \ 1], [x \ 1 + x], [y \ 1 + y], [1 + x \ x], [1 + y \ y], [1 + x + y \ 1 + x + y], [x + y \ x + y]\}.$$

¹ \mathbf{m} is considered as a row vector and \mathbf{m}^T denotes the transpose.

Note that $\alpha^{-1}(C^\perp)$ is not an R -module and $C^\perp \neq \alpha^{-1}(C^\perp)$. The complete weight enumerator for the code C and the dual $\alpha^{-1}(C^\perp)$ are polynomials in the 8 indeterminates $Z_0, Z_1, Z_x, Z_y, Z_{1+x}, Z_{1+y}, Z_{x+y}, Z_{1+x+y}$ given by

$$\begin{aligned} A(\mathbf{Z}) &= Z_0^2 + 2Z_1Z_{1+x+y} + Z_x^2 + Z_y^2 + 2Z_{1+x}Z_{1+y} + Z_{x+y}^2 \\ B(\mathbf{Z}) &= Z_0^2 + Z_1^2 + 2Z_xZ_{1+x} + 2Z_yZ_{1+y} + Z_{1+x+y}^2 + Z_{x+y}^2 \end{aligned}$$

respectively. Note that $A(\mathbf{Z}) \neq B(\mathbf{Z})$. However, when specializing to weight enumerators for Hamming weight (i.e., setting $Z_0 = 1$ and the 7 other indeterminates to Z), the resulting polynomials are equal $A_H(Z) = 1 + 7Z^2 = B_H(Z)$.

The MacWilliams identities always hold for the character-based definition of duals for ‘linear’ codes defined over finite abelian groups [2]; in particular, they hold for the polynomials $A(\mathbf{Z})$ and $B(\mathbf{Z})$ as well as for $A_H(Z)$ and $B_H(Z)$, when considering the dual pair C and C^\perp . For the dual pair C and C^\perp of codes based on linear functionals the generalized MacWilliams identities do not hold because $C = C^\perp \neq \alpha^{-1}(C^\perp)$ but $A(\mathbf{Z}) \neq B(\mathbf{Z})$. However, in the special case of the weight enumerator polynomials $A_H(Z)$, $B_H(Z)$ with respect to Hamming weight, the identity (6) as given below holds.

After setting a suitable framework for duals over commutative artinian rings in the next Section, a generalization of the MacWilliams Identities from the field to the ring case will be formulated and proved in Section 3 for weight enumerators with respect to Hamming distance. In Section 4, the duality results are extended from linear block codes to convolutional codes.

2 Duality Properties of Codes over Artinian Rings

Let R be a commutative artinian ring. According to the structure theorem for such rings [3], R can be written as a finite direct sum of local rings R_i , i.e.,

$$R = R_1 \oplus R_2 \oplus \dots \oplus R_e. \quad (3)$$

Proposition 1 *Let R be a commutative artinian ring with a decomposition (3). Then,*

(i) *R has e maximal ideals, which are of the form*

$$m_i = R_1 \oplus \dots \oplus R_{i-1} \oplus m'_i \oplus R_{i+1} \oplus \dots \oplus R_e$$

where m'_i denotes the maximal ideal of R_i ;

(ii) *the localization of R at the maximal ideal m_i is isomorphic to R_i , i.e., $R_i \cong R_{m_i}$.*

Proof: (i) is clear because m'_i is maximal in R_i .

To proof (ii), we consider the homomorphism $i : R_i \rightarrow R_{m_i}$ given by sending an element $r^{(i)} \in R_i$ to $r^{(i)}/1$ in $R_{m_i} \triangleq \{r/s : r \in R, s \in R \setminus m_i\}$ and show that it is an isomorphism. The homomorphism i is injective because the annihilator of an element $r^{(i)} \neq 0$ is an ideal that is contained in the maximal ideal m_i and, hence, there is no $s \in R \setminus m_i$ such that $s \cdot r^{(i)} = 0$. To show surjectivity, consider an arbitrary element $r/s \in R_{m_i}$. Using (3), one has $r = (r_1, \dots, r_i, \dots, r_e)$ and $s = (s_1, \dots, s_i, \dots, s_e)$, where $s_i \in R_i \setminus m'_i$. Since m'_i is a maximal ideal, s_i is invertible in R_i with inverse s'_i . The element $s'_i r_i$ is mapped onto r/s , i.e., there is an element $t \in R \setminus m_i$ such that $t(r - ss'_i r_i) = 0$, viz., $t = (0, \dots, 1, \dots, 0)$ with a single component 1 at position i . \square

Using (3), every R -module M can be decomposed as

$$M = R \otimes_R M = M_1 \oplus M_2 \oplus \dots \oplus M_e$$

where $M_i = R_i \otimes_R M$ is the tensor product of the R -modules R_i and M . The following proposition is a special case of a well-known local-global result in commutative algebra (see [4] Chap. I.3, Corollary 3.4), applied to the special case of artinian rings where $R_i \cong R_{m_i}$ (cf. Proposition 1 (ii)).

Proposition 2 *Let M be a finitely generated module over R . Then, M is R -projective if and only if M_i is R_i -projective for all i .*

Remark: The R_i -modules M_i are actually free since the rings R_i are local.

The following property of projective modules over commutative artinian rings is crucial for duality based on linear functionals.

Lemma 1 *Suppose $M \subset R^n$ is projective. Then there exists a projective submodule Q of R^n such that*

$$R^n = M \oplus Q. \quad (4)$$

Proof: Using the results above, one can assume without loss of essential generality that R is local artinian and, hence, consider M to be free over R . For this case, (4) was proved in Appendix II of [5]. \square

It is well-known in commutative algebra that when localizing a finitely generated projective module U at a prime ideal \wp , one obtains an R_\wp -module U_\wp that is free (see e.g. Chap. 7.7 in [3]). This allows one to define the \wp -rank $rk_\wp(U)$ of a finitely generated projective module U , which is given by the cardinality of a basis of the localization U_\wp .

Proposition 3 *Let R be commutative artinian and suppose that U and V are submodules of R^n , which are projective. Then*

(i) U^\perp is projective and $(U^\perp)^\perp = U$; moreover, $rk_\wp(U^\perp) = n - rk_\wp(U)$ for any prime ideal \wp .

(ii) $(U + V)^\perp = U^\perp \cap V^\perp$.

(iii) $U + V$ and $U \cap V$ are projective and for any prime ideal \wp , the following rank formula holds

$$rk_\wp(U \cap V) + rk_\wp(U + V) = rk_\wp(U) + rk_\wp(V).$$

Remark: If R is artinian but not local then even if U and V are free the intersection $U \cap V$ need not be free. A simple example for this fact is obtained by letting R be the ring \mathbf{Z}_6 of integers modulo 6 and by considering the \mathbf{Z}_6 -submodules U and V of R^2 generated by $[2 \ 3]$ and $[1 \ 0]$, respectively. Then, $U \cap V = \{[0 \ 0], [2 \ 0], [4 \ 0]\}$ is projective but not free. Thus, when R is commutative artinian, the class of free modules need not be closed under the intersection operation, but the class of projective modules is.

Proof: Using Proposition 2, one can assume that R is local and, hence, that the projective modules U and V are free.

Proof of (i): Let $rk(U) = k$ and choose a basis $\mathbf{g}_1, \dots, \mathbf{g}_k$ for U . Let G be the corresponding generator matrix. By the above Lemma, there is a complementary free module U' such that

$$R^n = U \oplus U'. \quad (5)$$

In other words, the basis of U can be extended by $n - k$ n -tuples $\mathbf{q}_{k+1}, \dots, \mathbf{q}_n$ to form a basis of R^n . Let Q be the $(n - k) \times n$ -matrix with $\mathbf{q}_{k+1}, \dots, \mathbf{q}_n$ as rows. The $n \times n$ -matrix consisting of the submatrices G and Q is invertible, i.e.,

$$\begin{bmatrix} G \\ Q \end{bmatrix} \cdot \begin{bmatrix} K^T & H^T \end{bmatrix} = \begin{bmatrix} I_k & 0 \\ 0 & I_{n-k} \end{bmatrix} = \begin{bmatrix} K^T \\ H^T \end{bmatrix} \cdot \begin{bmatrix} G^T & Q^T \end{bmatrix}$$

where I_k denotes the $k \times k$ identity matrix and H and K are $(n - k) \times n$ and $k \times n$ matrices, respectively. It follows that the rows of H form a basis for U^\perp , hence, U^\perp is free of rank $n - k$ and, therefore, $rk_\varphi(U^\perp) = n - rk_\varphi(U)$. Similarly, the rows of G form a basis for $(U^\perp)^\perp$ and, therefore, $(U^\perp)^\perp = U$.

Proof of (ii):

$$\begin{aligned} (U + V)^\perp &= \{ \mathbf{x} \in R^n : \mathbf{x} \cdot \mathbf{y}^T = 0, \text{ for all } \mathbf{y} \in U \text{ or } \mathbf{y} \in V \} \\ &= \{ \mathbf{x} : \mathbf{x} \cdot \mathbf{u}^T = 0, \text{ for all } \mathbf{u} \in U \} \cap \{ \mathbf{x} : \mathbf{x} \cdot \mathbf{v}^T = 0, \text{ for all } \mathbf{v} \in V \} \\ &= U^\perp \cap V^\perp \end{aligned}$$

Proof of (iii): (5) implies $V \cap U \oplus V \cap U' = V$. Thus, $V \cap U$ is a direct summand in the free module V and, hence, projective. Using (i), it follows similarly that $V^\perp \cap U^\perp$ is projective. Now (ii) and (i) imply that $U + V$ is projective.

We now show the rank formula. The above Lemma implies that there is a free R -module V' such that $R^n = V \oplus V'$. One has $U + V = U \cap V + U \cap V' + V \cap U'$ and the right side is actually a direct sum. Thus,

$$(U \cap V) \oplus (U + V) \cong U \cap V \oplus U \cap V' \oplus U \cap V \oplus V \cap U' \cong U \oplus V$$

and this implies the rank formula

$$rk(U \cap V) + rk(U + V) = rk(U \oplus V) = rk(U) + rk(V).$$

which also holds after further localization at a prime ideal φ . □

In terms of category theory [3], the result of Proposition 3 can be expressed by saying that $^\perp$ is a (contravariant) duality functor from the category of projective submodules $U \subset R^n$ onto itself. Here, the considered morphisms must be defined for the entire space R^n . Duality means that the functor that results from applying $^\perp$ twice is naturally equivalent to the identity functor.

Example 2 *The commutative ring $R = GF(2)[x, y]/(x^2, y^2, xy)$ is artinian but not quasi-Frobenius. The non-projective R -module $U = \{0, x\}$ has the dual $U^\perp = \{0, x, y, x + y\}$. But $U \neq (U^\perp)^\perp = U^\perp$ and, therefore, $^\perp$ is not a duality functor on the category of finitely generated R -modules. This shows that the restriction to projective modules is essential.*

The two notions of duality (1) and (2), which are based on linear functionals and on characters, coincide for finite commutative quasi-Frobenius rings [1]. In the case of other rings, the two duality notions can be viewed to be complementary. E.g., the ring of integers \mathbf{Z} is not quasi-Frobenius (not injective) and not artinian. The linear functional based functor does not give the desired duality properties but Pontryagin duality does.

A complementary example is given by the field of rational numbers \mathbf{Q} . The rationals are not locally compact and, hence, Pontryagin duality does not provide the duality property but duality based on linear functionals does.

3 The MacWilliams Identities

In the sequel it is assumed that the ring R is finite and commutative; in particular, R is artinian and the results of the preceding section apply. The considered class of codes are projective modules $U \subset R^n$. The spectrum of a code U and its dual U^\perp is given by

$$A_i = |\{\mathbf{u} \in U : w_H(\mathbf{u}) = i\}|$$

$$B_i = |\{\mathbf{v} \in U^\perp : w_H(\mathbf{v}) = i\}|$$

where $w_H(\mathbf{u})$ denotes the Hamming weight of a codeword \mathbf{u} and $|V|$ denotes the cardinality of a set V .

The MacWilliams Identities give a relation between the weight coefficients A_i and B_i .

Theorem 1 (*MacWilliams Identity*) *Let R be a finite commutative ring and let A_i and B_i be the weight coefficients of an R -linear code U and its dual U^\perp , resp. Then, the following polynomial identity holds*

$$\sum_{i=1}^n B_i X^i = \frac{1}{|U|} \sum_{i=1}^n A_j (1-X)^j \{1 + (|R| - 1)X\}^{n-j}. \quad (6)$$

Remark: From Example 1 it is clear that the generalized MacWilliams Identity does not hold for generalized distance measures.

Proof: The proof goes along the lines of the original proof No. 1 in [6]. Setting $X = 1/(1+Y)$ in (6), one obtains

$$\sum_{i=1}^n B_i (1+Y)^{n-i} = \frac{1}{|U|} \sum_{j=1}^n A_j Y^j (Y + |R|)^{n-j}.$$

Expanding and comparing coefficients of Y^ℓ yields

$$\sum_{i=1}^{n-\ell} B_i \binom{n-i}{\ell} = \frac{|R|^{n-\ell}}{|U|} \sum_{j=1}^{\ell} A_j \binom{n-j}{n-\ell}. \quad (7)$$

It is enough to show (7) for all $\ell = 0, 1, \dots, n$.

For each subset $s = \{s_1, \dots, s_\ell\} \subset \{1, \dots, n\}$ of cardinality ℓ , we define a free rank- ℓ submodule $F_s \subset R^n$ with support in s :

$$F_s = \{\mathbf{x} \in R^n : \text{supp}(\mathbf{x}) \subseteq s\} = R\mathbf{e}_{s_1} \oplus \dots \oplus R\mathbf{e}_{s_\ell}$$

where $\mathbf{e}_1, \dots, \mathbf{e}_n$ is the standard basis for R^n and $\text{supp}(\mathbf{x})$ denotes the support, i.e., the indices with non-zero components, of \mathbf{x} . Let $t = \{1, \dots, n\} \setminus s$ be the complementary set of s . Then, clearly $F_s^\perp = F_t$. Using Proposition 3, one obtains

$$\begin{aligned} (U + F_s)^\perp &= U^\perp \cap F_t \\ rk_m(U + F_s) &= rk_m(U^\perp \cap F_t)^\perp = n - rk_m(U^\perp \cap F_t) \\ rk_m(U) + rk_m(F_s) &= rk_m(U \cap F_s) + rk_m(U + F_s), \end{aligned}$$

where m is one of the e maximal ideals of R . Since $rk_m(F_s) = \ell$, the last two equations imply

$$n - \ell + rk_m(U \cap F_s) - rk_m(U) = rk_m(U^\perp \cap F_t) \quad (8)$$

or, equivalently,

$$|R_m|^{n-\ell+rk_m(U \cap F_s)-rk_m(U)} = |R_m|^{rk_m(U^\perp \cap F_t)} \quad (9)$$

where R_m denotes the localization at the maximal ideal m .

For fixed cardinality ℓ , consider pairs (s, \mathbf{u}) , where $\mathbf{u} \in U \cap F_s$. For each choice of s , there are $|U \cap F_s| = \prod_m |R_m|^{rk_m(U \cap F_s)}$ such pairs, where the product is over all the e maximal ideals m of R . Considering all possible choices for s , the total number of such pairs is

$$\sum_{\substack{s \subset \{1, \dots, n\} \\ |s| = \ell}} \prod_m |R_m|^{rk_m(U \cap F_s)}.$$

A second way of counting these pairs is as follows. For each $\mathbf{u} \in U$ of weight j , there are $n - j$ zero components. Thus, any subset $t = \{t_1, \dots, t_{n-\ell}\} \subset \{1, \dots, n\} \setminus \text{supp}(\mathbf{u})$ of cardinality $n - \ell$ defines a complementary set s , which can be paired with \mathbf{u} . There are $\binom{n-j}{n-\ell}$ choices for t or s , respectively. There are A_j codewords of weight j in U , hence

$$\sum_{\substack{s \subset \{1, \dots, n\} \\ |s| = \ell}} \prod_m |R_m|^{rk_m(U \cap F_s)} = \sum_{j=0}^{\ell} A_j \binom{n-j}{n-\ell}.$$

Applying the same argument to U^\perp , one obtains

$$\sum_{\substack{t \subset \{1, \dots, n\} \\ |t| = n-\ell}} \prod_m |R_m|^{rk_m(U^\perp \cap F_t)} = \sum_{i=0}^{n-\ell} B_i \binom{n-i}{\ell}.$$

Using (9) and the fact that the complementary sets s and t are in one-to-one correspondence yields

$$\sum_{i=0}^{n-\ell} B_i \binom{n-i}{\ell} = \sum_{\substack{t \subset \{1, \dots, n\} \\ |t| = n-\ell}} \prod_m |R_m|^{rk_m(U^\perp \cap F_t)}$$

$$\begin{aligned}
&= \sum_{\substack{t \subset \{1, \dots, n\} \\ |t| = n - \ell}} \prod_m |R_m|^{n - \ell + rk_m(U \cap F_s) - rk_m(U)} \\
&= \prod_m |R_m|^{n - \ell - rk_m(U)} \sum_{j=0}^{\ell} A_j \binom{n - j}{n - \ell} \\
&= \frac{|R|^{n - \ell}}{|U|} \sum_{j=0}^{\ell} A_j \binom{n - j}{n - \ell}.
\end{aligned}$$

□

Example 3 [2 2] generates a \mathbf{Z}_6 -module $U = \{[0\ 0], [2\ 2], [4\ 4]\}$, which is projective but not free. The dual code is

$$U^\perp = \{[0\ 0], [3\ 0], [0\ 3], [3\ 3], [2\ 4], [4\ 2], [1\ 5], [5\ 1], [1\ 2], [2\ 1], [4\ 5], [5\ 4]\}.$$

The weight enumerator polynomials of U and U^\perp are $A(X) = 1 + 2X^2$ and $B(X) = 1 + 2X + 9X^2$, respectively. The MacWilliams identities are readily verified:

$$B(X) = \frac{1}{3} \sum_{j=0}^2 A_j (1 - X)^j (1 + 5X)^{n-j}.$$

4 Duality of Convolutional Codes over Rings

An (n, k) convolutional code over a field F can be viewed as a block code over the field of rational functions $F(D)$ [7]. For a commutative ring R , we can define the ring of rational functions similarly as in the field case by

$$R(D) = \left\{ \frac{f(D)}{D^m s(D)} : f(D), s(D) \in R[D], s(0) = 1, m \in \mathbf{Z} \right\}.$$

An *convolutional code over R* is an $R(D)$ -submodule of $R(D)^n$. The following proposition is crucial to extend the duality results from linear block codes to convolutional codes.

Proposition 4 *If R is commutative artinian, then so is $R(D)$.*

Proof: Due to the structure theorem for commutative artinian rings (cf. 3), the ring of rational functions decomposes as

$$R(D) = R_1(D) \oplus R_2(D) \oplus \dots \oplus R_e(D).$$

Thus, one can assume that R is local, artinian with a nilpotent maximal ideal \wp , say $\wp^t = 0$ but $\wp^{(t-1)} \neq 0$.

We will show that $R(D)$ is local and has the nilpotent maximal ideal $\wp R(D)$. By the mentioned structure theorem, this implies that $R(D)$ is artinian.

Since \wp is nilpotent, it is clear that also $\wp R(D)$ is nilpotent. Thus, it remains to show that $R(D)$ is local, which will be proven by showing that $R(D) \setminus \wp R(D)$ consists of invertible elements.

Let $r(D) = \frac{f(D)}{s(D)} \in R(D) \setminus \wp R(D)$. Since $s(D)$ is invertible it is enough to show that also $f(D) \in R[D] \setminus \wp R[D]$ is invertible. Write

$$f(D) = a(D) + b(D)$$

where $a(D) \in (R \setminus \wp)R[D]$ and $b(D) \in \wp R[D]$. By successive multiplication of $a(D) + b(D)$ by complementary binomial-like terms, one obtains

$$\begin{aligned} f(D) \cdot (a(D) - b(D)) &= a^2(D) - b^2(D) \\ f(D) \cdot (a(D) - b(D))(a^2(D) + b^2(D)) &= a^4(D) - b^4(D) \\ &\text{etc.} \end{aligned}$$

Continuing in this way, one finds a polynomial $h(D)$ such that $f(D) \cdot h(D) = a^{2^\ell}(D) - b^{2^\ell}(D)$ for some ℓ , such that $t \leq 2^\ell$. Since $\wp^t = 0$, it follows that $b^{2^\ell}(D)$ vanishes and, therefore, $f(D) \cdot h(D) = a^{2^\ell}(D)$. By construction, the trailing coefficient a_T of $a(D)$, i.e., the first non-zero coefficient of lowest order, is a unit of R because it lies in $R \setminus \wp$. Therefore, also the trailing coefficient of $a^{2^\ell}(D)$, which equals $a_T^{2^\ell}$, is a unit. Thus, $f(D) \cdot h(D) = a^{2^\ell}(D)$ and, a fortiori, also $f(D)$ is invertible in $R(D)$. \square

The *dual (or orthogonal)* of a convolutional code $C \subset R(D)^n$ is defined as in the block code case:

$$C^\perp = \{\mathbf{x}(D) \in R^n(D) : \mathbf{x}(D) \cdot \mathbf{c}(D)^T = 0, \text{ all } \mathbf{c}(D) \in C\}.$$

Corollary 1 *Let R be a commutative, artinian ring. Then, every convolutional code C over R has a dual C^\perp , which satisfies $(C^\perp)^\perp = C$. Moreover, if $C \subset R(D)^n$ is free of rank k , then C^\perp has rank $n - k$.*

References

- [1] J.A. Wood, "Duality for Modules over Finite Rings and Applications to Coding Theory," *American J. of Math.*, Vol. 121.3, June 1999, pp. 555 – 575.
- [2] T. Ericson, V. Zinoviev, "On Fourier-invariant partitions of finite abelian groups and the MacWilliams identity for group codes," *Prob. Peredachi Informatsii*, vol. 32, pp. 137-143, 1996.
- [3] N. Jacobson, *Basic Algebra II*, Freeman, San Francisco, 1980 .
- [4] T.Y. Lam, *Serre's Conjecture*, LNM 635, Springer, 1978.
- [5] H.-A. Loeliger, T. Mittelholzer, "Convolutional Codes over Groups, *IEEE Trans. Information Th.*, Vol. 42, No. 6, Nov 1996, pp. 1660 – 1686.
- [6] J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," *Bell Syst. Tech. J.*, vol. 42, pp. 79 – 94, 1963.
- [7] James L. Massey, *Coding Theory*, in *Handbook of Applicable Mathematics* (Ed. W. Ledermann), Vol. V, Part B, *Combinatorics and Geometry* (Ed. W. Ledermann, S. Vajda). Chichester & New York: Wiley, 1985.