Georgian Mathematical Journal
Volume 8 (2001), Number 3, 553–570

CONVOLUTIONAL CODES AND FREQUENCY RESPONSES

V. LOMADZE

Abstract. Frequency responses are introduced as objects that are much finer than transfer functions, and their investigation is carried out via convolutional codes. In particular, a canonical one-to-one correspondence is established between frequency responses and equivalence classes of AR-models. These new objects are important because the study of linear dynamical systems can to a great extent be reduced to the study of them.

2000 Mathematics Subject Classification: 93B05, 95B25, 93B27, 94B10.
Key words and phrases: Transfer function, convolutional encoder, AR-model, convolutional code, frequency response, exact sequence, controllable.

1. Introduction

Throughout the paper k will be an arbitrary field, s an indeterminate, O the ring of proper rational functions over k. We adopt Willems' [7] point of view that makes no distinction between inputs and outputs, and q will stand for the signal number.

By a transfer function we understand a $k(s)$-linear subspace in $k(s)^q$ (i.e., exactly what Forney [1] calls a convolutional code.) Frequency responses are defined as k-linear subspaces in $k(s)^q$ satisfying certain natural conditions. One condition is a finiteness condition according to which a frequency response must contain a transfer function and have finite dimension relative to it; other conditions require a frequency response to be invariant under taking the polynomial and strictly proper parts, and the forward and backward shift operators. There is a canonical nondegenerate symmetric k-bilinear form on $k(s)^q$, which is obtained by composing the standard $k(s)$-bilinear form with the residue map at infinity. It is easily seen that transfer functions are self-dual with respect to this form. Based on this simple fact, we show (see Theorem 1 and Theorem 2) that frequency responses are connected via a duality relation with convolutional codes. It is almost obvious that convolutional codes are in a bijective correspondence with equivalence classes of convolutional encoders. We therefore obtain that frequency responses correspond bijectively to equivalence classes of AR-models, which represents the main result of the paper.

The system-theoretic significance of the concept of a frequency response will become clear in [5]. It will be shown in that follow-up paper that knowledge of frequency responses is equivalent to that of linear dynamical systems. It

ISSN 1072-947X / $8.00 / © Heldermann Verlag *www.heldermann.de*

does not matter that linear dynamical systems are discrete-time or continuous-time. This emphasizes once more that the theory of linear dynamical systems is essentially algebraic in nature.

It should be noted that we treat here the general singular case; the classical regular case is derived easily from it. If the reader is interested in this latter case only, he should start with the bilinear form $k[s]^q \times s^{-1}O^q \to k$. An advantage in considering general frequency responses rather than "classical" frequency responses (as we call them) lies in the fact that the just mentioned bilinear form is not so easy to treat. Next, general frequency responses are related with general linear dynamical systems. And we know that linear dynamical systems having singularity also deserve to be studied.

The reader is referred to Willems [7] for linear systems, Forney [1] for convolutional codes, and Rosenthal *et al.* [6] for both of them.

2. Some Preliminaries

There are two important functions on $k(s)$: ord_∞ and Res_∞. Given a rational function f, $\mathrm{ord}_\infty(f)$ is the least integer n such that $s^n f \in O$, and $\mathrm{Res}_\infty(f)$ is the coefficient at s^{-1} in the representation of f as a power series in s^{-1}.

For each $r \geq 1$, one has a canonical k-bilinear form

$$< -, - >: k(s)^r \times k(s)^r \to k, \tag{1}$$

which is defined by the formula

$$< f, g >= \mathrm{Res}_\infty(f^{tr} g).$$

(Here and below "*tr*" stands for "transpose".) Clearly, this form is symmetric, and one can easily check that it is nondegenerate.

Lemma 1. *We have*

$$(k[s]^r)^\perp = k[s]^r \quad and \quad (s^{-1}O^r)^\perp = s^{-1}O^r.$$

Proof. Obvious. □

For each rational function f, set

$$\pi_-(f) = \text{polynomial part of } f \quad \text{and} \quad \pi_+(f) = \text{strictly proper part of } f.$$

Lemma 2. *For all $f, g \in k(s)^r$,*

$$< \pi_- f, g >=< f, \pi_+(g) > .$$

Proof. Obvious. □

Lemma 3. *Let X_1 and X_2 be k-linear subspaces in $k(s)^r$. Then*

$$(X_1 + X_2)^\perp = X_1^\perp \cap X_2^\perp.$$

Proof. Obvious. □

Remark. The equality $(X_1 \cap X_2)^\perp = X_1^\perp + X_2^\perp$ is not always true (and this causes some problems). In general, we have only "$\supseteq$".

Lemma 4. *Let X and Y be k-linear subspaces in $k(s)^r$ such that $X \subseteq Y$. If $X^{\perp\perp} = X$, then the canonical bilinear form*

$$Y/X \times X^{\perp}/Y^{\perp} \to k$$

is nondegenerate.

Proof. This is obviously nondegenerate from the right. The hypothesis implies that this is nondegenerate from the left as well. □

Lemma 5. *Let $l, m \geq 1$ and let A be a rational matrix of size $l \times m$. If X is a k-linear subspace in $k(s)^l$, then*

$$(A^{tr}X)^{\perp} = A^{-1}(X^{\perp}).$$

Proof. For all $f \in k(s)^l$ and $g \in k(s)^m$,

$$< A^{tr}f, g > = < f, Ag >,$$

and the lemma follows. □

Lemma 6. *If L is a $k[s]$-submodule in $k(s)^r$, then so is $L^{\perp}$. Likewise, if M is an O-submodule in $k(s)^r$, then so is $L^{\perp}$.*

Proof. Left to the reader. (When L, M are finitely generated, the proof is immediate by the previous lemma and Lemma 1.) □

The following simple lemma will be very helpful in the sequel.

Lemma 7. *If V is a $k(s)$-linear subspace in $k(s)^r$, then so is $V^{\perp}$ and $V^{\perp\perp} = V$.*

Proof. One can check easily that

$$V^{\perp} = \{g \mid f^{tr}g = 0 \text{ for all } f \in V\};$$

whence follows the lemma. □

Given k-linear spaces X and Y such that $X \subseteq Y$, we write $[Y : X]$ to denote the dimension of the quotient space Y/X.

Lemma 8. *Let X be a k-linear subspace in $k(s)^r$.*

a) *There exists at most one $k(s)$-linear subspace V in $k(s)^r$ such that $X \subseteq V$ and $[X : V] < +\infty$.*

b) *There exists at most one $k(s)$-linear subspace V in $k(s)^r$ such that $V \subseteq X$ and $[V : X] < +\infty$.*

Proof. Assume that V_1 and V_2 are two $k(s)$-linear subspaces satisfying the desired property. Then $V_1 + V_2$ also has the same property, and clearly

$$[(V_1 + V_2) : V_1] < +\infty \quad \text{and} \quad [(V_1 + V_2) : V_2] < +\infty.$$

It follows that $V_1 = V_1 + V_2$ and $V_2 = V_1 + V_2$; whence $V_1 = V_2$. □

Given a polynomial (resp. a proper) matrix A, we say that A is left unimodular (resp. left biproper) if $BA = I$ for some polynomial (resp. proper) matrix B.

Lemma 9.

a) *Let L be a submodule in $k[s]^r$. Then the following are equivalent:* 1) $k[s]^r/L$ *is torsion free;* 2) $L = E \cap k[s]^r$ *for some $k(s)$-linear subspace $E \subseteq k(s)^r$;* 3) $L = Pk[s]^m$ *for some $m \geq 0$ and left unimodular $r \times m$ matrix P.*

b) *Let M be a submodule in O^r. Then the following are equivalent:* 1) O^r/M *is torsion free;* 2) $M = E \cap O^r$ *for some $k(s)$-linear subspace $E \subseteq k(s)^r$;* 3) $M = QO^m$ *for some $m \geq 0$ and left biproper $r \times m$ matrix Q.*

Proof. The assertion a) is fairly well-known. We give a sketch proof for the assertion b).

Let E denote the $k(s)$-submodule of $k(s)^r$ generated by M (that is, $k(s)M$). Then, $k(s)^r/E$ is the fraction space of O^r/M, and hence the latter is torsion free if and only if the canonical map $O^r/M \to k(s)^r/E$ is injective. Since the kernel of this map is equal to $(O^r \cap E)/M$, we obtain $b1) \iff b2)$. Further, both $b1)$ and $b3)$ are equivalent to saying that $O^r \simeq M \oplus O^r/M$, and hence we have $b1) \iff b3)$. $\square$

Concluding the section, define k-linear operators $\tau : k[s] \to k[s]$ and $\sigma : O \to O$, the forward and backward shifts, respectively by

$$\tau(a_0 s^n + \cdots + a_n) = a_0 s^{n-1} + \cdots + a_{n-1} \text{ and } \sigma(b_0 + b_1 s^{-1} + \dots) = b_1 + b_2 s^{-1} + \cdots .$$

3. Convolutional Encoders and AR-Models

We begin by recalling some basic definitions and facts concerning nonsingular (square) rational matrices as given in [3].

The cohomology spaces of a nonsingular rational matrix D are defined by

$$H^0(D) = k[s]^r \cap DO^r \quad \text{and} \quad H^1(D) = k(s)^r/(k[s]^r + DO^r),$$

where r denotes the size of D. The Chern number is defined by the formula $\mathrm{ch}(D) = -\mathrm{ord}_\infty(\det D)$, and the dual is defined to be $D^* = (D^{-1})^{tr}$. Two nonsingular rational matrices D_1 and D_2 are called equivalent if there exists a unimodular matrix U such that $D_2^{-1}UD_1$ is biproper. According to the Wiener–Hopf theorem (which is the most significant fact about rational matrices), if D is a nonsingular rational matrix of size r, then there exist integers $n_1, \dots, n_r$ such that D is equivalent to the diagonal matrix with $s^{n_1}, \dots, s^{n_r}$ on the diagonal. The integers $n_1, \dots, n_r$ are uniquely determined up to permutation; they are called the Wiener–Hopf indices.

Lemma 10 (Serre's formulas). *Let n be an integer.*

a) *If $n \geq 0$, then the canonical linear map $k^{n+1} \to H^0(s^n)$ given by*

$$(a_0, \dots, a_n) \mapsto a_0 s^n + \cdots + a_n$$

is bijective; if $n < 0$, then $H^0(s^n) = 0$.

b) *If $n \geq 0$, then the canonical linear map $k^{n+1} \to H^1(s^{-n-2})$ given by*

$$(b_0, \dots, b_n) \to (b_0 s^{-1} + \cdots + b_n s^{-n-1}) \,\mathrm{mod}(k[s] + s^{-n-2}O)$$

is bijective; if $n < 0$, then $H^1(s^{-n-2}) = 0$.

Lemma 11 (Finiteness theorem). *Cohomology spaces have finite dimension.*

Lemma 12 (Riemann–Roch theorem). *If D is a nonsingular rational matrix, then*

$$\dim H^0(s^{-1}D) - \dim H^1(s^{-1}D) = \mathrm{ch}(D).$$

Lemma 13 (Serre's duality theorem). *If D is a nonsingular rational matrix of size r, then the canonical pairing* (1) *induces a nondegenerate pairing*

$$H^0(s^{-1}D) \times H^1(s^{-1}D^*) \to k.$$

Lemma 14.

a) *If A is a nonsingular rational matrix, then its Wiener–Hopf indices are nonpositive if and only if there exists a full column rank rational matrix F such that FA is proper.*

b) *If B is a nonsingular rational matrix, then its Wiener–Hopf indices are nonnegative if and only if there exists a full row rank rational matrix G such that $B^{-1}G$ is proper.*

Two nonsingular rational matrices are said to be congruent if they are connected via right multiplication by a biproper matrix. We define a linear bundle as a congruence class of nonsingular rational matrices. The rank of a linear bundle is the size of any its representative. The cohomology spaces, the Chern number, the Wiener–Hopf indices, and the dual of a linear bundle are defined obviously.

As noted in Introduction, by a transfer function we mean any $k(s)$-linear subspace in $k(s)^q$.

A convolutional encoder is a pair (α, F), where α is a linear bundle and F a full column rank polynomial matrix, with q rows, such that FA is proper for any representative A of α. The rank of α is called the input number, the number $-\mathrm{ch}(\alpha)$ the complexity, the space $H^1(s^{-1}\alpha)$ the state space. The space $\operatorname{Im} F = Fk(s)^m$, where m is the input number, is called the transfer function. By Lemma 14a), the Wiener–Hopf indices of α must be nonpositive. These indices, taken with minus, are called the constraint lengths. By Serre's formulas and the Riemann–Roch theorem, their sum is equal to the complexity. Two convolutional encoders (α_1, F_1) and (α_2, F_2) are said to be equivalent if there exists a unimodular matrix U such that $A_1^{-1}UA_2$, where $A_1 \in \alpha_1$ and $A_2 \in \alpha_2$, is biproper and $F_2 = F_1U$.

An AR-model is a pair (β, G), where β is a linear bundle and G a full row rank polynomial matrix, with q columns, such that $B^{-1}G$ is proper for any representative B of β. The rank of β is called the output number, the number $\mathrm{ch}(\beta)$ the McMillan degree, the space $H^0(s^{-1}\beta)$ the state space. The space $\operatorname{Ker} G = G^{-1}\{0\}$ is called the transfer function. The Wiener–Hopf indices, which are nonnegative by Lemma 14b), are called the lag indices. By Serre's formulas and the Riemann–Roch theorem, their sum is equal to the McMillan degree. Two AR-models (β_1, G_1) and (β_2, G_2) are said to be equivalent if there exists a unimodular matrix U such that $B_2^{-1}UB_1$, where $B_1 \in \beta_1$ and $B_2 \in \beta_2$, is biproper and $G_2 = UG_1$.

There is an evident one-to-one correspondence between convolutional encoders and AR-models, which is given by

$$(\alpha, F) \mapsto (\alpha^*, F^{tr}).$$

A convolutional encoder (α, F) is said to be controllable if F is left unimodular and FA, where A is any representative of α, is left biproper. An AR-model (β, G) is said to be controllable if G is right unimodular and $B^{-1}G$, where B is any representative of β, is right biproper. Certainly, controllable convolutional encoders and controllable AR-models correspond to each other.

Let (α, F) be a controllable convolutional encoder with input number m, and (β, G) a controllable AR-model with output number p. Let $A \in \alpha$ and $B \in \beta$. We say that (α, F) and (β, G) form an exact pair if the sequences

$$0 \to k[s]^m \xrightarrow{F} k[s]^q \xrightarrow{G} k[s]^p \to 0 \quad \text{and} \quad 0 \to O^m \xrightarrow{FA} O^q \xrightarrow{B^{-1}G} O^p \to 0 \tag{2}$$

are exact. We then say also that (α, F) is a kernel description of (β, G) and (β, G) a cokernel description of (α, F).

Lemma 15. *Let (α, F) be an controllable convolutional encoder and (β, G) a controllable AR-model, and suppose that they form an exact pair. Then, for each integer n, there is a "long" cohomological exact sequence*

$$\begin{aligned} 0 \to H^0(s^n\alpha) \to H^0(s^n I_q) \to H^0(s^n\beta) \to H^1(s^n\alpha) \\ \to H^1(s^n I_q) \to H^1(s^n\beta) \to 0. \end{aligned}$$

Proof. Left to the reader. □

Corollary 1. *There is a canonical isomorphism*

$$H^1(s^{-1}\alpha) \simeq H^0(s^{-1}\beta),$$

and hence the complexity of (α, F) and the McMillan degree of (β, G) are equal to each other.

Lemma 16.

a) *Every controllable convolutional encoder possesses a cokernel description, and the latter is determined uniquely up to equivalence.*

b) *Every controllable AR-model possesses a kernel description, and the latter is determined uniquely up to equivalence.*

Proof. Left to the reader. □

Proposition 1. *Let (α, F) be a convolutional encoder with complexity d, and let $n \geq \max\{d-1, 0\}$. Then (α, F) is controllable if and only if the linear map*

$$H^1(s^{-n-2}\alpha) \to H^1(s^{-n-2}I_q)$$

is injective.

Proof.

Proof. Follows from the following proposition by Serre's duality theorem. □

Proposition 2. *Let (β, G) be an AR-model with McMillan degree d, and let $n \geq \max\{d-1, 0\}$. Then (β, G) is controllable if and only if the linear map*

$$H^0(s^n I_q) \to H^0(s^n \beta)$$

is surjective.

Proof. *"If".* Note that if $l \geq 0$, then $H^0(s^{l+1}) = H^0(s^l) + sH^0(s^l)$. From this, using the Wiener–Hopf theorem, we obtain that

$$\forall i \geq 0, \quad H^0(s^{l+1}\beta) = H^0(s^l\beta) + sH^0(s^l\beta).$$

It follows by induction that

$$H^0(s^i I_q) \to H^0(s^i \beta)$$

is surjective for each $i \geq n$. Using now Lemma 4 in [3], we see that the homomorphisms

$$k[s]^q \to k[s]^p \quad \text{and} \quad O^q \to BO^p$$

are surjective.

"Only if". Let (α, F) be a kernel description. By Lemma 15, we have an exact sequence

$$H^0(s^n I_q) \to H^0(s^n \beta) \to H^1(s^n \alpha).$$

We know (see Lemma 14(a)) that the Wiener–Hopf indices of α are nonpositive. On the other hand, their sum is equal to $\mathrm{ch}(\alpha) = -\mathrm{ch}(\beta)$. Hence these indices are greater than or equal to $-d$. We see that every index of $s^n\alpha$ is greater than or equal to -1, and therefore its one-dimensional cohomologies are trivial. □

4. Convolutional Codes

A convolutional code is a k-linear subspace C in $k(s)^q$ satisfying the following conditions:

(CC1) There is a transfer function E such that $C \subseteq E$ and $[E : C] < +\infty$.

(CC2) C is invariant with respect to π_- and π_+;

(CC3) $C \cap k[s]^q$ and $sC \cap O^q$ are submodules in $k[s]^q$ and O^q, respectively.

By Lemma 8(a) , the "E" is uniquely determined, and we call it the transfer function of C. The number $[E : C]$ is called the complexity. By the property (CC2), we have

$$C = (C \cap k[s]^q) + (C \cap s^{-1}O^q).$$

Remarks. 1) As remarked in Introduction, Forney [1] defines a convolutional code as a $k(s)$-linear subspace of $k(s)^q$. In Rosenthal *et al.* [6] a convolutional code is defined as a $k[s]$-submodule of $k[s]^q$. The relationships of these definitions with the definition above are explained respectively in Proposition 6 and Lemma 22.

2) Our definition has been motivated by the purpose to make obvious the connection with the definition of a frequency response given below, and it is equivalent to that provided in [4]. In the cited paper a convolutional code is

defined as a pair (L, M), where L and M are submodules in $k[s]^q$ and O^q, respectively, such that $k(s)L = k(s)M$. That the two definitions are equivalent follows from the next lemma. The relation is established as follows. If (L, M) is a convolutional code in the sense of [4], then $L + s^{-1}M$ is a convolutional code in the sense of the present paper. Conversely, if C is a convolutional code in the sense of this paper, then $(C \cap k[s]^q, sC \cap O^q)$ is a convolutional code in the sense of [4].

Lemma 17. *If L and M are submodules in $k[s]^q$ and O^q, respectively, then $k(s)L = k(s)M$ if and only if there exists a transfer function E such that*

$$L, M \subseteq E \quad \textit{and} \quad [E : (L + s^{-1}M)] < +\infty.$$

Proof. *"If".* The hypothesis implies that the modules L and M have the same rank, say, m. There exist a polynomial matrix F and a proper rational matrix Q, both of size $q \times m$, such that

$$L = Fk[s]^m \quad \text{and} \quad M = QO^m.$$

Then $Fk(s)^m = Qk(s)^m$, and consequently $Q = A^{-1}F$ for some nonsingular rational matrix A. Putting $E = k(s)M$, we have a bijective linear map $F : k(s)^m \to E$. This induces an isomorphism

$$H^0(s^{-1}A) \simeq E/(L + s^{-1}M).$$

It remains now to apply the Finiteness theorem.

"Only if". It is clear that $k(s)L,\ k(s)M \subseteq E$. We claim that in fact we have equalities. Indeed, assume that, say, $k(s)L \neq E$. We then have an exact sequence

$$0 \to (M + k(s)L)/k(s)L \to E/k(s)L \to E/(k(s)L + M) \to 0.$$

Clearly, $(M + k(s)L)/k(s)L$ is a finitely generated O-submodule in $E/k(s)L$ and therefore has infinite codimension (as a k-linear subspace). On the other hand, the hypothesis implies that $E/(k(s)L + M)$ has finite dimension. A contradiction. $\square$

Let (α, F) be a convolutional encoder, with input number m, and let A be a representative of α. We define the convolutional code of (α, F) by the formula

$$CC(\alpha, F) = Fk[s]^m + s^{-1}FAO^m.$$

It is easily seen that this indeed is a convolutional code. Its transfer function certanly is equal to $Fk(s)^m$.

Notice that two equivalent convolutional encoders generate the same convolutional code.

Proposition 3. *The mapping $(\alpha, F) \mapsto CC(\alpha, F)$ induces a one-to-one correspondence between the equivalence classes of convolutional encoders and the convolutional codes.*

Proof. Suppose that (α_1, F_1) and (α_2, F_2) generate the same code, i.e.,

$$F_1k[s]^m + s^{-1}F_1A_1O^m = F_2k[s]^m + s^{-1}F_2A_2O^m.$$

We clearly have

$$F_1k[s]^m = F_2k[s]^m \quad \text{and} \quad F_1A_1O^m = F_2A_2O^m.$$

It follows that

$$F_2 = F_1U \quad \text{and} \quad F_2A_2 = F_1A_1V$$

for some unimodular matrix U and biproper matrix V. It is easily seen that $V = A_1^{-1}UA_2$, and so the encoders are equivalent.

The rest follows from the proof of the "if" part of Lemma 17. Indeed, suppose that C is a convolutional code. Put $L = C \cap k[s]^q$ and $M = sC \cap O^q$, and let A and F be as in that proof. Then (α, F), where α is the congruence class of A, generates C. □

Lemma 18. *Let C be a convolutional code with transfer function E. Then*

$$[C^\perp : E^\perp] = [E : C].$$

Proof. Let m be the input number and (α, F) a convolutional encoder generating C.

Choose any representative A of α, and put $G = F^{tr}$. Applying Lemmas 3 and 5, we obtain

$$\begin{aligned} C^\perp &= (Fk[s]^m + s^{-1}FAO^p)^\perp = (Fk[s]^m)^\perp \cap (s^{-1}FAO^m)^\perp \\ &= G^{-1}k[s]^m \cap G^{-1}(s^{-1}A^*O^m) = G^{-1}H^0(s^{-1}A^*). \end{aligned}$$

Using again Lemma 5, we have

$$E^\perp = (Fk(s)^m)^\perp = G^{-1}\{0\}.$$

Since G has a full row rank, it induces a surjective linear map of $G^{-1}H^0(s^{-1}A^*)$ onto $H^0(s^{-1}A^*)$. The kernel is equal to $G^{-1}\{0\}$, and consequently we have a canonical isomorphism

$$C^\perp/E^\perp \simeq H^0(s^{-1}A^*).$$

There is also a canonical isomorphism

$$H^1(s^{-1}A) \simeq E/C,$$

which is determined by the bijective linear map $k(s)^m \to E$. It remains now to apply Serre's duality theorem. □

5. Frequency Responses

A frequency response is a linear subspace R in $k(s)^q$ satisfying the following conditions:

(FR1) There is a transfer function T such that $T \subseteq R$ and $[R : T] < +\infty$;

(FR2) R is invariant with respect to π_- and π_+;

(FR3) $R \cap k[s]^q$ and $sR \cap O^q$ are invariant with respect to τ and σ, respectively.

By Lemma 8(b), the "T" is determined uniquely, and we call it the transfer function of R. The number $[R : T]$ is called the McMillan degree. By the property (FR2), we have

$$R = (R \cap k[s]^q) + (R \cap s^{-1}O^q).$$

Proposition 4. *Let (β, G) be an AR-model with state space X. Then $G^{-1}(X)$ is a frequency response.*

Proof. Put $R = G^{-1}X$, and let p be the output number and B a representative of β.

The space R satisfies (FR1). Indeed, if $T = G^{-1}\{0\}$ is the transfer function of our AR-model, then we have a short exact sequence

$$0 \to T \to R \to X \to 0,$$

and this implies that $[R : T] < +\infty$.

Take $f \in k[s]^q$ and $g \in s^{-1}O^q$. We have $Gf \in k[s]^p$ and $Gg \in s^{-1}BO^p$. Therefore $G(f + g) \in X$ if and only if $Gf \in X$ and $Gg \in X$. Hence R satisfies (FR2).

Let $f \in R \cap k[s]^q$, and let a be the free coefficient of f. We then have $\tau f = s^{-1}f - as^{-1}$. Since $Gf \in s^{-1}BO^p$ and $Ga \in BO^p$, it follows that $G(\tau f) \in s^{-1}BO^p$. On the other hand, $G(\tau f) \in k[s]^p$ because $\tau f \in k[s]^q$. Consequently $G(\tau f) \in X$; whence $\tau f \in R \cap k[s]^q$. Let now $g \in sR \cap O^q$, and let b be the free coefficient of g. We then have $\sigma g = sg - sb$. Since $Gg \in sk[s]^p$ and $Gb \in k[s]^p$, it follows that $G(\sigma g) \in sk[s]^p$. On the other hand, $G(\sigma g) \in BO^p$ because $\sigma g \in O^q$. Consequently $G(\sigma g) \in sX$; whence $\sigma g \in sR \cap O^q$. We see that R satisfies (FR3). $\square$

We shall write $FR(\beta, G)$ to denote the frequency response associated to an AR-model (β, G).

Proposition 5. *If (β, G) is an AR-model, then*

$$FR(\beta, G) = CC(\beta^*, G^{tr})^{\perp}.$$

Proof. Let p be the output number of (β, G) and B a representative of β. Applying Lemmas 1, 3 and 5, we have

$$\begin{aligned} FR(\beta, G) &= G^{-1}(k[s]^p \cap s^{-1}BO^p) = G^{-1}k[s]^p \cap s^{-1}(B^{-1}G)^{-1}O^p \\ &= (G^{tr}k[s]^p)^{\perp} \cap (s^{-1}(B^{-1}G)^{tr}O^p)^{\perp} = (G^{tr}k[s]^p + s^{-1}(B^{-1}G)^{tr}O^p)^{\perp} \\ &= CC(\beta^*, G^{tr})^{\perp}. \quad \square \end{aligned}$$

Theorem 1.
a) *If C is a convolutional code, then $C^{\perp}$ is a frequency response.*
b) *If R is a frequency response, then $R^{\perp}$ is a convolutional code.*

Proof. a) Follows from the previous two propositions and the fact that C is representable as the convolutional code of some convolutional encoder.

b) By Lemmas 7 and 4, we have a nondegenerate bilinear form

$$R/T \times T^{\perp}/R^{\perp} \to k. \tag{3}$$

This implies that $[T^{\perp} : R^{\perp}] < +\infty$, and thus $R^{\perp}$ satisfies (CC1).

Using Lemmas 1 and 3, we can easily see that $R^{\perp}$ satisfies the property (CC2).

Let us show that $R + k[s]^q$ and $s^{-1}R + s^{-2}O^q$ are modules over $k[s]$ and O, respectively. Suppose first $w \in R + k[s]^q$. By (FR2), $w = f + s^{-1}g$, where $f \in k[s]^q$ and $g \in sR \cap O^q$. Let $g = b_0 + b_1 s^{-1} + \dots$. Then, for each $i \geq 0$, we have

$$s^i w = s^i f + s^{i-1} g = (s^i f + b_0 s^{i-1} + \cdots + b_{i-1}) + \sigma^i g \in R + k[s]^q.$$

It follows that $R + k[s]^q$ is a $k[s]$-submodule. Now, suppose that $w \in s^{-1}R + s^{-2}O^q$. By (FR2), $w = s^{-1}f + s^{-2}g$, where $f \in R \cap k[s]^q$ and $g \in O^q$. Let $f = a_0 s^n + \cdots + a_n$. Then, for each $n \geq i \geq 0$, we have

$$\begin{aligned} s^{-i} w &= s^{-i-1} f + s^{-i-2} g \\ &= s^{-1}(\tau^i f + a_{n-i+1} s^{-1} + \cdots + a_n s^{-i}) + s^{-i-2} g \in s^{-1}R + s^{-2}O^q. \end{aligned}$$

Further, $hw \in s^{-2}O^q$ for each $h \in s^{-n-1}O^q$. It follows that $s^{-1}R + s^{-2}O^q$ is an O-module. Using Lemmas 1 and 3, we see that

$$R^{\perp} \cap k[s]^q = (R + k[s]^q)^{\perp} \quad \text{and} \quad sR^{\perp} \cap O^q = (s^{-1}R + s^{-2}O^q)^{\perp}$$

are submodules in $k[s]^q$ and O^q, respectively. Thus $R^{\perp}$ has the property (CC3). $\square$

Theorem 2.
a) *If C is a convolutional code, then $C^{\perp\perp} = C$.*
b) *If R is a frequency response, then $R^{\perp\perp} = R$.*

Proof. The proofs for both statements are similar, and we restrict ourselves to showing, say, b).

Let T be the transfer function of R. Put $C = R^{\perp}$ and $E = T^{\perp}$. From (3) and Lemma 18 (and Lemma 7) we obtain

$$[R : T] = [E : C] = [C^{\perp} : T].$$

Further, it is obvious that $R \subseteq C^{\perp}$. Hence there is a canonical exact sequence

$$0 \to R/T \to C^{\perp}/T \to C^{\perp}/R \to 0.$$

By the dimension argument, the second linear map in this sequence is bijective. So $C^{\perp}/R = 0$, and the theorem follows. $\square$

We can now state and prove our main result.

Theorem 3. *The mapping* $(\beta, G) \mapsto FR(\beta, G)$ *induces a one-to-one correspondence between the equivalence classes of AR-models and the frequency responses.*

Proof. Follows immediately from Proposition 3, and Theorems 1 and 2. $\square$

6. Controllability

A convolutional code C with transfer function E is called controllable if

$$E \cap k[s]^q \subseteq C \quad \text{and} \quad E \cap s^{-1}O^q \subseteq C.$$

Remark. In [4] we called the property above the observability property (we have done this following [7]). In view of Proposition 8, we feel that the term "controllable" is more appropriate.

Proposition 6. *If* E *is a transfer function, then* $(E \cap k[s]^q) + (E \cap s^{-1}O^q)$ *is a controllable convolutional code. The map*

$$E \mapsto (E \cap k[s]^q) + (E \cap s^{-1}O^q)$$

establishes a one-to-one correspondence between transfer functions and controllable convolutional codes.

Proof. Let E be a transfer function. It is clear that $E \cap k[s]^q$ and $sE \cap O^q$ are submodules in $k[s]^q$ and O^q, respectively. The fraction spaces of these modules clearly coincide with E. So $(E \cap k[s]^q) + (E \cap s^{-1}O^q)$ is a convolutional code whose transfer function is E. It immediately follows from the definition that this code is controllable.

Let now C be a controllable convolutional code with transfer function E. By definition,

$$C \cap k[s]^q = E \cap k[s]^q \quad \text{and} \quad C \cap s^{-1}O^q = E \cap s^{-1}O^q.$$

Therefore $C = (E \cap k[s]^q) + (E \cap s^{-1}O^q)$. $\square$

Proposition 7. *Let* (α, F) *be a convolutional encoder and* C *its code. Then* C *is controllable if and only if so is* (α, F).

Proof. Follows from Lemma 9. $\square$

A frequency response R with transfer function T is called controllable if

$$R \subseteq T + k[s]^q \quad \text{and} \quad R \subseteq T + s^{-1}O^q.$$

Lemma 19. *Let* E *be a transfer function. Then*

$$(E \cap k[s]^q)^\perp = E^\perp + k[s]^q \quad \textit{and} \quad (E \cap s^{-1}O^q)^\perp = E^\perp + s^{-1}O^q.$$

Proof. Let m denote the dimension of E.

There exist a right unimodular polynomial matrix P such that $E \cap k[s]^q = P^{tr} k[s]^m$ and a right biproper matrix Q such that $E \cap O^q = Q^{tr} O^m$. We clearly have $Pk[s]^q = k[s]^m$ and $QO^q = O^m$. Consequently,

$$P^{-1}(k[s]^m) = P^{-1}\{0\} + k[s]^q \quad \text{and} \quad Q^{-1}(s^{-1}O^m) = Q^{-1}\{0\} + s^{-1}O^q.$$

Lemma 5 completes the proof. □

Proposition 8. *Let R be a frequency response, and let C be the corresponding convolutional code. Then R is controllable if and only if C is controllable.*

Proof. The "if" part follows from the previous lemma. The "only if" part is obvious by Lemma 3. □

Proposition 9. *If T is a transfer function, then $(T + k[s]^q) \cap (T + s^{-1}O^q)$ is a controllable frequency response. The map*

$$T \mapsto (T + k[s]^q) \cap (T + s^{-1}O^q)$$

establishes a one-to-one correspondence between transfer functions and controllable frequency responses.

Proof. Follows from Lemma 3 and the previous two propositions. □

Remark. Transfer functions and controllable frequency responses are not the same objects. The equality $T = (T + k[s]^q) \cap (T + s^{-1}O^q)$ holds if and only if T is generated by a scalar matrix.

Proposition 10. *Let (β, G) be an AR-model and R its frequency response. Then R is controllable if and only if so is (β, G).*

Proof. Follows from Propositions 7 and 8. □

We need the following

Lemma 20. *Let D be a nonsingular rational $r \times r$ matrix having nonpositive Wiener–Hopf indices. Let d be the Chern number of D^{-1}, and let $n \geq d$. Then, for all $f, g \in k(s)^r$, there exists $h \in k(s)^r$ such that*

$$s^n h \equiv f \bmod k[s]^m \quad \textit{and} \quad h \equiv g \bmod s^{-1}DO^m.$$

Proof. If the assertion is true for D, then it is true for UD as well, where U is a unimodular matrix. Therefore, by the Wiener–Hopf factorization theorem, there will be no loss of generality if we assume that $D = \operatorname{diag}(s^{-d_1}, \dots, s^{-d_r})$. The proof can be obviously reduced to the case where $r = 1$, which is easy. Indeed, let

$$f = (a_1 s^{-1} + a_2 s^{-2} + \cdots) \bmod k[s] \text{ and } g = (b_0 s^{-d} + b_1 s^{-d+1} + \cdots) \bmod s^{-d-1}O,$$

where a_i and b_i are constants. Clearly,

$$h = s^{-n}(a_1 s^{-1} + a_2 s^{-2} + \cdots) + (b_0 s^{-d} + b_1 s^{-d+1} + \cdots)$$

has the required property. □

We now present an interpretation of controllability that is analogous to that of Willems [7].

Theorem 4. *Let R be a frequency response with transfer function T and McMillan degree d, and let $n \geq d$. Then R is controllable if and only if, for all $w_- \in R \cap k[s]^q$ and $w_+ \in R \cap s^{-1}O^q$, there exists $w \in T$ such that*

$$\pi_-(w) = w_- \quad \textit{and} \quad \pi_+(s^n w) = w_+.$$

Proof. The "if" part is obvious.

To prove the "only if" part consider an AR-model (β, G) generating R. Let (α, F) be its kernel description. We remark that the complexity of (α, F) is equal to the McMillan degree of (β, G) (see Corollary 1). Take $w_- \in R \cap k[s]^q$ and $w_+ \in R \cap s^{-1}O^q$. The exact sequences (2) imply that there exist $f_+ \in s^{-1}O^q$ and $f_- \in k[s]^q$ such that $Gf_+ = Gw_-$ and $Gf_- = Gw_+$. We have $w_- - f_+ \in T$ and $w_+ - f_- \in T$. Therefore we can choose $u_1,\ u_2 \in k(s)^m$ such that $Fu_1 = w_- - f_+,\ Fu_2 = w_+ - f_-$. By the previous lemma, there exists $u \in k(s)^m$ satisfying the condition

$$u \equiv u_1 \bmod s^{-1}AO^m \quad \text{and} \quad s^n u \equiv u_2 \bmod k[s]^m.$$

(Here A is a representative of α.) Set $w = Fu$. Using again (2), we have

$$w \equiv (w_- - f_+) \bmod s^{-1}O^q \quad \text{and} \quad s^n w \equiv (w_+ - f_-) \bmod k[s]^q.$$

It follows that w does the job. $\square$

7. "Classical" Case

A convolutional encoder (α, F) is regular if FA, where A is any representative of α, is left biproper.

Lemma 21. *There is a canonical one-to-one correspondence between regular convolutional encoders and full column rank polynomial matrices which is given by*

$$(\alpha, F) \to F.$$

Proof. Let F be a full column rank polynomial matrix of size $m \times q$. The set

$$F^{-1}O^q = \{u \in k(s)^m |\ Fu \in O^q\}$$

obviously is an O-submodule of $k(s)^m$. There is a canonical embedding $F^{-1}O^q \to O^q$, and therefore this module must be finitely generated. We obtain that $F^{-1}O^q = AO^m$ for some nonsingular rational matrix A. Clearly, FA is proper because $FAO^m \subseteq O^q$. By construction, $FAO^m = Fk(s)^m \cap O^q$, and therefore FA must be left biproper (see Lemma 9b)). We conclude that our mapping is surjective.

To show that our mapping is injective, assume that A' is another nonsingular rational matrix such that FA' is left biproper. Using again Lemma 9b), we have $FA'O^m = Fk(s)^m \cap O^q$. This implies that $FA'O^m = F^{-1}O^q$, and consequently $FA'O^m = FAO^m$. It follows that $A'O^m = AO^m$, and thus $A^{-1}A'$ is biproper. $\square$

A convolutional code C with transfer function E is said to be regular if

$$E \cap s^{-1}O^q \subseteq C.$$

We refer to convolutional codes as defined in Rosenthal *et al.* [6] as "classical" convolutional codes. These are submodules in $k[s]^q$.

Lemma 22. *There is a canonical one-to-one correspondence between regular convolutional codes and "classical" ones; this is given by*

$$C \mapsto C \cap k[s]^q.$$

Proof. We have a canonical mapping in the opposite direction. Indeed, if $C \subseteq k[s]^q$ is a "classical" convolutional code, then

$$C + s^{-1}(E \cap O^q),$$

where $E = k(s)C$, is a regular convolutional code. It is easily seen that the two mappings are inverse to each other. □

Given a full column rank polynomial matrix (i.e., a "classical" convolutional encoder) F, one defines its code by the formula

$$CC(F) = Fk[s]^m,$$

where m is the column number of F. Clearly, if (α, F) is a regular convolutional encoder, then

$$CC(F) = CC(\alpha, F) \cap k[s]^q.$$

Proposition 3′. *The mapping $F \mapsto CC(F)$ induces a one-to-one correspondence between equivalence classes of full column rank polynomial matrices and "classical" convolutional codes.*

Proof. Follows from Proposition 3 and the previous two lemmas. □

Remark. Of course the proposition above can be proved directly, and of course the direct proof is obvious.

An AR-model (β, G) is regular if $B^{-1}G$, where B is any representative of β, is right biproper.

Lemma 23. *There is a canonical one-to-one correspondence between regular AR-models and full row rank polynomial matrices which is given by*

$$(\beta, G) \to G.$$

Proof. Follows from Lemma 21 by transposition. □

A frequency response R with transfer function T is said to be regular if

$$R \subseteq T + s^{-1}O^q.$$

We call any k-linear subspace $R \subseteq s^{-1}O^q$ such that

$$[sR : M] < +\infty \text{ for some "classical" transfer function } M \quad\text{and}\quad \sigma(sR) \subseteq sR$$

a "classical" frequency response. By a "classical" transfer function we mean any submodule $M \subseteq O^q$ that satisfies the conditions of Lemma 9b).

Lemma 24. *There is a canonical one-to-one correspondence between regular frequency responses and "classical" ones which is given by*

$$R \mapsto R \cap s^{-1}O^q.$$

Proof. Let R be a regular frequency response, and let T be its transfer function. The canonical linear map

$$R \cap s^{-1}O^q \to R/T$$

is surjective. Indeed, if $w \in R$, then $w = w_0 + g$, where $w_0 \in T$ and $g \in s^{-1}O^q$, and we clearly have $g \in R \cap s^{-1}O^q$ and $g \bmod T = w \bmod T$. Further, the kernel of this map is equal to $T \cap s^{-1}O^q$, and therefore there is a canonical isomorphism

$$(R \cap s^{-1}O^q)/(T \cap s^{-1}O^q) \simeq R/T.$$

It immediately follows from this that $R \cap s^{-1}O^q$ is a "classical" frequency response.

Let now R be a "classical" frequency response, and let M be the "classical" transfer function that exists by definition. Put $T = k(s)M$. We claim that $T + R$ is a regular frequency response.

Consider the canonical linear map

$$R \to (T + R)/T, \quad w \mapsto w \bmod T.$$

It is easily seen that this map is surjective and its kernel is equal to $T \cap R$. We have

$$s^{-1}M \subseteq T \cap R \subseteq T \cap s^{-1}O^q = s^{-1}M,$$

and consequently $T \cap R = s^{-1}M$. It follows that $[(T + R) : T] = [R : s^{-1}M]$.

Let $n \geq 1$ and $g \in M$. If $g = b_0 + b_1 s^{-1} + b_2 s^{-2} + \dots$, then

$$s^{n-1}g = (b_0 s^{n-1} + \dots + b_{n-1}) + s^{-1}(b_n + b_{n+1}s^{-1} + \dots).$$

Consequently,

$$\pi_-(s^{n-1}g) = s^{n-1}g - s^{-1}\sigma^n(g) \in T + R.$$

Now the point is that modulo $s^{-1}O^q$ any element of T is equal to a linear combination of elements of the form $s^{n-1}g$, with $n \geq 1$ and $g \in M$. (Indeed, because $T = k(s)M$, every element in T is a sum of elements of the form ag, with $a \in k(s)$ and $g \in M$. Therefore modulo $s^{-1}O^q$ every element in T is a sum of elements of the form ag, with $a \in k[s]$ and $g \in M$.) It follows that the polynomial parts of elements in T belong to $T + R$. Automatically, the same is true for the strictly proper parts. We conclude that $T + R$ satisfies (FR2).

Notice that $(T + R) \cap k[s]^q$ consists just of the polynomial parts of elements in T. Take an arbitrary $f \in (T + R) \cap k[s]^q$, and suppose that $f = \pi_-(w)$, where $w \in T$. Then

$$\tau(f) = \pi_-(s^{-1}w) \in (T + R) \cap k[s]^q.$$

Hence $(T + R) \cap k[s]^q$ is invariant under τ. Further, it is easily seen that $(T + R) \cap s^{-1}O^q = R$, and we conclude that $T + R$ satisfies (FR3).

Obviously, $T + R \subseteq T + s^{-1}O^q$, and the proof is completed. $\square$

Given a full row rank polynomial matrix (i.e., a "classical" AR-model) G, we define its frequency response by the formula

$$FR(G) = \{w \in s^{-1}O^q \mid Gw \in k[s]^p\}.$$

This is exactly what Kuijper [2] calls the *rational behavioral space*. It is clear that if (β, G) is a regular AR-model, then

$$FR(G) = FR(\beta, G) \cap s^{-1}O^q.$$

Theorem 3′. *The mapping $G \mapsto FR(G)$ induces a one-to-one correspondence between equivalence classes of full row rank polynomial matrices and "classical" frequency responses.*

Proof. Follows from Theorem 3 and the previous two lemmas. $\square$

Remark. One may want to deduce the above theorem directly from Proposition 3′. For this one should consider the bilinear form $k[s]^q \times s^{-1}O^q \to k$. But this consideration is not so easy.

Acknowledgement

The author wishes to express his gratitude to the referee for a very careful reading of the manuscript and indicating several errors.

References

1. G. D. Forney, Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory* **19**(1970), 720–738.
2. M. Kuijper, First order representations of linear systems. *Birkhäuser, Boston,* 1994.
3. V. Lomadze, Singular linear behaviors and their AR-representations. *Math. Control Signals Systems* **14**(2001), 194–211.
4. V. Lomadze, Convolutional codes and coherent sheaves. *Appl. Algebra Engrg. Comm. Comput.* (to appear).
5. V. Lomadze, Linear dynamical systems: An axiomatic approach. *Georgian Math. J.* (to appear).
6. J. Rosenthal, J. M. Schumacher, and E. V. York, On behaviors and convolutional codes. *IEEE Trans. Inform. Theory* **42**(1996), 1881–1891.
7. J. C. Willems, Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Automat. Control* **36**(1991), 259–294.

(Received 25.06.2001; revised 24.07.2001)

Author's address:
A. Razmadze Mathematical Institute
Georgian Academy of Sciences
1, M. Aleksidze St., Tbilisi 380093
Georgia
E-mail: loma@rmi.acnet.ge