Discrete Mathematics 342 (2019) 784–792

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

The predictable degree property and minimality in multidimensional convolutional coding

Vakhtang Lomadze

A. Razmadze Mathematical Institute, Mathematics Department of I. Javakhishvili State University, Georgia

ARTICLE INFO

Article history:
Received 15 September 2017
Received in revised form 18 August 2018
Accepted 13 November 2018
Available online 30 November 2018

Keywords:
Convolutional code
Filtered module
PD property
Proper representation
Minimality
Graded module

ABSTRACT

Convolutional codes inherit from polynomials a natural structure of a filtered module, which is a fundamental structure and therefore should be taken into account. Pursuing this idea, we define higher-dimensional analogs of the predictable degree property, Forney's indices and overall constraint length; also, we address the important issue of minimality.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

Multidimensional convolutional codes are natural generalizations of classical (one-dimensional) convolutional codes and are used to transmit multidimensional data. They have been studied quite a bit in the literature and we refer the reader to Fornasini and Valcher [5], Valcher and Fornasini [13], Weiner [14] and more recent works Charoenlarpnopparut [2], Climent et al. [3], Jangisarakul and Charoenlarpnopparut [7], Kitchens [8], Napp Avelli et al. [11,12], Zerz [15].

In this article, we would like to offer a new view-point on some fundamental issues of algebraic character related to multidimensional convolutional codes.

Throughout, $\mathbb{F}$ is an arbitrary (finite) field and n a fixed positive integer. Let $D_1, \ldots, D_n$ be indeterminates and $S = \mathbb{F}[D_1, \ldots, D_n]$ the ring of polynomials in these indeterminates. We remind that the degree of a monomial $D_1^{i_1} \ldots D_n^{i_n}$ is the sum $i_1 + \cdots + i_n$, and the degree of a (nonzero) polynomial f is the maximum of the degrees of the nonzero terms of f. (The degree of the zero polynomial is defined to be $-\infty$.) For every $d \in \mathbb{Z}$, we shall write $S_{\leq d}$ to denote the space of polynomials of degree $\leq d$. (It is worth noting that $S_{\leq d} = \{0\}$ for every negative d.)

Following Weiner [14] and other authors, a convolutional code of length q is a submodule of S^q. (In dimension 1, all convolutional codes are free, and therefore some authors impose the freeness condition. However, this condition is too restrictive in higher dimensions.) A desirable property of a convolutional code is non-catastrophicity, but we shall not require this property in the sequel. (It can be shown that a convolutional code $C \subseteq S^q$ is non-catastrophic if and only if polynomials with nonzero constant term are not zero divisors on S^q/C.)

A convolutional code $C \subseteq S^q$ gives rise to a family of block codes $(C_{\leq d})_{d \geq 0}$ defined as

$$C_{\leq d} = C \cap S^q_{\leq d}.$$

E-mail address: vakhtang.lomadze@tsu.ge.

https://doi.org/10.1016/j.disc.2018.11.010
0012-365X/© 2018 Elsevier B.V. All rights reserved.

These block codes are of great importance, and they form, what is called in Algebra, a filtration. As we shall see, they lead naturally to integer invariants of C such as the input number, the overall constraint length and the Forney indices.

A representation (or a generator matrix) of a convolutional code C is a polynomial matrix G (with no zero column) such that $GS^p = C$, where p is the number of columns in G. The point of view we pursue in this article is that attention should be focused exclusively on those representations that represent each $C_{\le d}$ individually, that is, those representations G for which

$$\forall d \ge 0, \quad G(\bigoplus_{i=1}^{p} S_{\le d-a_i}) \;=\; C_{\le d},$$

where p is the column number of G and $a_1, \dots, a_p$ are the column degrees. This property is fundamental, and we call it the predictable degree (PD) property. It is a higher dimensional analog of Forney's classical predictable degree property.

By means of filtrations, we introduce the concept of minimality, and show that for a given convolution code there always exists a unique (up to equivalence) minimal proper representation. We then give numerical characterizations of minimality; namely, we show that minimal proper representations are precisely those proper representations that have the least column number or the least total column degree.

In some extent, we use in the article *graded* modules. The point is that convolutional codes admit a *homogenization*, which captures the structure of a filtered module. Graded modules are easier to work with than filtered modules, and there is a very nice theory for them (see Eisenbud [4]). For a convenience of the reader, we recall in Appendix A a few facts about graded modules.

This article is a simplified adapted version of [10]. The latter is quite involved and is addressed to system theorists, and we have thought it worthwhile to make its most relevant material available for the coding theory community in a self-contained form.

2. Filtrations, and the PD property

Filtrations are widely used in Algebra (and in many other fields of Mathematics). In this paper, we consider filtrations on modules (see Ch.III, §2.1 in Bourbaki [1]).

Let M be a module over S. A filtration on M is an ascending chain

$$M_{\le 0} \subseteq M_{\le 1} \subseteq M_{\le 2} \subseteq \cdots$$

of linear subspaces of M such that

$$M = \bigcup M_{\le d} \quad \text{and} \quad D_k M_{\le d} \subseteq M_{\le d+1} \; \forall k, d.$$

A module with a filtration is called a filtered module.

By a twisting function of length p, we shall mean any function of $[1, p]$, the set of integers from 1 to p, into $\mathbb{Z}_+$. If a is a twisting function of length p, then, for $f \in S^p$ with components $f_1, \dots, f_p$, we set

$$\deg_a(f) = \max_i \{a(i) + \deg(f_i)\}.$$

(When $a = 0$, we certainly get the usual degree $\deg(f)$.)

Example 1. A twisting function $a : [1, p] \to \mathbb{Z}_+$ determines on S^p a filtration consisting of the spaces

$$S^p[-a]_{\le d} = \{f \in S^p \mid \deg_a(f) \le d\} \quad (d \ge 0).$$

The module S^p equipped with this filtration is denoted by $S^p[-a]$. (If $a = 0$, we shall write simply S^p instead of $S^p[-0]$.)

A homomorphism of filtered modules $M \to N$ is a module homomorphism $u : M \to N$ such that

$$\forall d \ge 0, \quad u(M_{\le d}) \subseteq N_{\le d}.$$

Example 2. Let G be a polynomial matrix of size $q \times p$ and with column degree function a (i.e., the function that assigns to every $j \in [1, p]$ the degree of the jth column of G). Then, G determines a homomorphisms of filtered modules

$$S^p[-a] \to S^q.$$

One has an obvious notion of isomorphisms between filtered modules. The following lemma can be found in [10]. (For the sake of completeness, we present its proof.)

Lemma 1. *Let $a_1 : [1, p_1] \to \mathbb{Z}_+$ and $a_2 : [1, p_2] \to \mathbb{Z}_+$ be two twisting functions. If*

$$S^{p_1}[-a_1] \;\simeq\; S^{p_2}[-a_2],$$

then $p_1 = p_2$ and $a_1 = a_2$ (up to permutation).

Proof. That $p_1 = p_2$ is obvious (since an isomorphism $S^{p_1}[-a_1] \simeq S^{p_2}[-a_2]$ yields a module isomorphism $S^{p_1} \simeq S^{p_2}$). Let this common value denote by p.

Next, we certainly may assume that a_1 and a_2 are increasing functions. Suppose that $a_1 \neq a_2$, and let i be the smallest number such that $a_1(i) \neq a_2(i)$. Say that $a_1(i) < a_2(i)$. Letting $d = a_1(i)$, we have:

$$S^p[-a_1]_{\leq d} \simeq S^p[-a_2]_{\leq d}.$$

But the left side here is equal to

$$S_{\leq d-a_1(1)} \oplus \cdots \oplus S_{\leq d-a_1(i-1)} \oplus \mathbb{F} \oplus \cdots$$

and the right side is

$$S_{\leq d-a_2(1)} \oplus \cdots \oplus S_{\leq d-a_2(i-1)}.$$

We get a contradiction. □

Definition. Let G be a polynomial matrix of size $q \times p$ and with column degree function a, and let $C = GS^p$. Say that G has the PD property if the linear map

$$S^p[-a]_{\leq d} \xrightarrow{G} C_{\leq d}$$

is surjective for all $d \geq 0$. A polynomial matrix having the PD property will be called proper.

Remark. In the classical 1-dimensional case, it is customary to introduce the concept of PD property for full column rank polynomial matrices only. Here, the full column rank assumption is not made even when $n = 1$.

Example 3. Let $n = 1$ (and write D instead of D_1). Consider the convolutional code

$$C = \{\begin{pmatrix} x \\ Dy \end{pmatrix} \mid x, y \in S\}.$$

The following two polynomial matrices

$$G_1 = \begin{bmatrix} 1 & 0 \\ 0 & D \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & D & D \end{bmatrix}$$

are representations of C. The column degrees of these matrices are respectively $(0, 1)$ and $(0, 1, 1)$. It is easily seen that, for each $d \geq 0$,

$$G_1(S_{\leq d} \oplus S_{\leq d-1}) = C_{\leq d} \quad\text{and}\quad G_2(S_{\leq d} \oplus S_{\leq d-1} \oplus S_{\leq d-1}) = C_{\leq d}.$$

Hence, both of the matrices are proper. (Notice that the matrix G_2 is not of full column rank !)

Example 4. Let $n = 2$, and consider the convolutional code

$$C = \{\begin{pmatrix} x \\ D_1x + D_2y \\ x + y \end{pmatrix} \mid x, y \in S\}.$$

(This is taken from Example 1 in Climent et al. [3].) The simplest representation of this code is the polynomial matrix

$$\begin{bmatrix} 1 & 0 \\ D_1 & D_2 \\ 1 & 1 \end{bmatrix}.$$

However, this does not have the PD property. Indeed, the codeword

$$\begin{bmatrix} 1 & 0 \\ D_1 & D_2 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} D_2 \\ -D_1 \end{pmatrix} = \begin{pmatrix} D_2 \\ 0 \\ D_2 - D_1 \end{pmatrix}$$

belongs to $C_{\leq 1}$, but this codeword cannot be obtained from a constant input.

Now, consider the matrix

$$G = \begin{bmatrix} 1 & D_2 & 0 \\ D_1 & 0 & D_2 \\ 1 & D_2 - D_1 & 1 \end{bmatrix}.$$

From the relations

$$G\begin{bmatrix}1&0\\0&0\\0&1\end{bmatrix}=\begin{bmatrix}1&0\\D_1&D_2\\1&1\end{bmatrix}\quad\text{and}\quad\begin{bmatrix}1&0\\D_1&D_2\\1&1\end{bmatrix}\begin{bmatrix}1&D_2&0\\0&-D_1&1\end{bmatrix}=G,$$

one can see that G also represents C. We claim that it has the PD property. Indeed, assume that $\begin{pmatrix}x\\D_1x+D_2y\\x+y\end{pmatrix}$ is a codeword in $C_{\le d}$. Denote by f and g the homogeneous d-parts of x and y, respectively. Since $D_1x+D_2y\in S_{\le d}$, it follows that $D_1f+D_2g=0$. It is easily seen that $f=D_2h$ and $g=-D_1h$ for some $h\in S_{\le d-1}$. We then have:

$$\begin{pmatrix}x-f\\h\\y-g\end{pmatrix}\in S^3_{\le d-1}\ \text{and}\ G\begin{pmatrix}x-f\\h\\y-g\end{pmatrix}=\begin{pmatrix}x\\D_1x+D_2y\\x+y\end{pmatrix}.$$

Two proper representations G_1 and G_2 of a convolutional code C are said to be equivalent if there exists an isomorphism $S^{p_1}[-a_1]\to S^{p_2}[-a_2]$ making the diagram

$$\begin{tikzcd}S^{p_1}[-a_1] \arrow[r, "G_1"] \arrow[d] & C \arrow[d, equal] \\ S^{p_2}[-a_2] \arrow[r, "G_2"] & C\end{tikzcd}$$

commutative. (Here p_i is the column number of G_i and a_i the column degree function.) By Lemma 1, if G_1 and G_2 are equivalent, then $p_1=p_2$ and $a_1=a_2$ (up to permutation).

3. The input number, the overall constraint length and the forney indices

Let M be a filtered module. If $d\ge 1$, then

$$M_{\le d-1}+D_1M_{\le d-1}+\cdots+D_nM_{\le d-1}$$

is the part of $M_{\le d}$ that contains nothing "essentially new". It is natural therefore to consider the quotients

$$\Gamma_d(M)=\frac{M_{\le d}}{M_{\le d-1}+D_1M_{\le d-1}+\cdots+D_nM_{\le d-1}}.$$

Notice that these are linear spaces over $\mathbb{F}$. (We put $\Gamma_0(M)=M_0$.)

Example 5. Let k and d be nonnegative integers. Then,

$$\Gamma_d(S[-k])=\begin{cases}\mathbb{F} & \text{when } d=k;\\ \{0\} & \text{when } d\ne k.\end{cases}$$

The following theorem is important; it permits us to introduce important integer invariants in an intrinsic way.

Theorem 1. *If C is a convolutional code, then all the linear spaces $\Gamma_d(C)$ have finite dimension. Moreover, they all are trivial except for a finite number.*

Proof. See Appendix B. □

Definition. Let C be a convolutional code. For every $d\ge 0$, set

$$\gamma_C(d)=\dim(\Gamma_d(C)),$$

and define the input number $\gamma(C)$ of C and the overall constraint length $\delta(C)$ respectively by the formulas

$$\gamma(C)=\sum_{d\ge 0}\gamma_C(d)\quad\text{and}\quad\delta(C)=\sum_{d\ge 0}d\gamma_C(d).$$

Call each $d\ge 0$, for which $\gamma_C(d)\ne 0$, a Forney index (or a constraint length) and the number $\gamma_C(d)$ its multiplicity. Define the memory as the maximal Forney index.

We close the section by the following proposition.

Proposition 1. *Let C be a convolutional code, and let m be its memory. Then C can be recovered from $C_{\le m}$.*

Proof. We have $\Gamma_d(C) = 0$ for all $d > m$. In other words, for all such d,

$$C_{\le d} = C_{\le d-1} + D_1 C_{\le d-1} + \cdots + D_n C_{\le d-1}.$$

From this, we can see that knowledge of $C_{\le m}$ implies knowledge of all $C_{\le d}$ with $d > m$. It remains to notice that, for every nonnegative integer N,

$$C = \bigcup_{d \ge N} C_{\le d}.$$

The proof is complete. □

4. Minimality

Let $u : M \to N$ be an epimorphism of filtered modules. Say that u is minimal if the linear map

$$\Gamma_d(u) : \Gamma_d(M) \to \Gamma_d(N)$$

is bijective for all $d \ge 0$.

Theorem 2. *Let C be a convolutional code of length q. There exists a proper representation G such that the epimorphism*

$$G : S^p[-a] \to C,$$

where p is the column number of G and a the column degree function, is minimal. Moreover, such a representation is uniquely determined (up to equivalence).

Proof. (Existence) We construct a canonical proper representation of C extending the "greedy" construction presented in Section 4 of Forney et al. [6].

Let d be any nonnegative integer. Choose elements in $C_{\le d}$ that define a basis of $\Gamma_d(C)$. Clearly they all have degree d since they do not belong to $C_{\le d-1}$. These elements are columns in S^p, and hence they form a polynomial matrix of size $q \times \gamma(d)$, which we denote by G_d. (For simplicity, we write $\gamma(d)$ instead of $\gamma_C(d)$.) Remark that G_d can be viewed as a linear map $\mathbb{F}^{\gamma(d)} \to C_{\le d}$ that induces an isomorphism

$$\mathbb{F}^{\gamma(d)} \simeq \Gamma_d(C).$$

Varying d, we get a matrix

$$G = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots \end{bmatrix}.$$

Because $\gamma(d) = 0$ for all but finitely many d, this in fact is a finite matrix. It determines a homomorphism of filtered modules

$$G : \bigoplus_k S[-k]^{\gamma(k)} \to S^q.$$

We are going to show that G is a minimal proper representation of C.

Put

$$V_d = \bigoplus_k S[-k]^{\gamma(k)}_{\le d} = S^{\gamma(0)}_{\le d} \oplus S^{\gamma(1)}_{\le d-1} \oplus \cdots \oplus S^{\gamma(d-1)}_{\le 1} \oplus S^{\gamma(d)}_{\le 0}.$$

We claim that

$$\begin{bmatrix} G_0 & G_1 & \cdots & G_d \end{bmatrix} : V_d \to C_{\le d}$$

is surjective for each $d \ge 0$. This is so when $d = 0$ since, by construction, $G_0 : \mathbb{F}^{\gamma(0)} \to C_{\le 0}$ is bijective. Assume that the surjectivity holds for $d - 1$ with $d \ge 1$. For every $k \ge 1$, $S_{\le k} = S_{\le k-1} + D_1 S_{\le k-1} + \cdots + D_n S_{\le k-1}$, and using this, we can easily see that

$$V_d = (V_{d-1} + D_1 V_{d-1} + \cdots + D_n V_{d-1}) + S^{\gamma(d)}_{\le 0}.$$

By the induction assumption, it follows that the image of $V_{d-1} + D_1 V_{d-1} + \cdots + D_n V_{d-1}$ under $\begin{bmatrix} G_0 & G_1 & \cdots & G_{d-1} \end{bmatrix}$ is equal to

$$C_{\le d-1} + D_1 C_{\le d-1} + \cdots + D_n C_{\le d-1}.$$

Next, by construction, the image of $S^{\gamma(d)}_{\le 0} = \mathbb{F}^{\gamma(d)}$ under G_d is the complement of the above space to $C_{\le d}$. The claim is proved.

Now, the filtered module $\bigoplus S[-k]^{\gamma(k)}$ can be rewritten as $S^p[-a]$, where $p = \sum \gamma(k)$ and $a : [1,\ p] \to \mathbb{Z}_+$. (The function a is uniquely determined up to permutation.) Then, the homomorphism G takes the form

$$S^p[-a] \to S^q.$$

Minimality is obvious. Indeed, by Example 5,

$$\Gamma_d(\bigoplus S[-k]^{\gamma(k)}) = \mathbb{F}^{\gamma(d)}$$

and, as already remarked, the linear map $G_d : \mathbb{F}^{\gamma(d)} \to C_{\leq d}$ induces an isomorphism

$$\mathbb{F}^{\gamma(d)} \simeq \Gamma_d(C).$$

(Uniqueness) See Appendix B. □

Any G satisfying the condition of Theorem 2 is called a minimal proper representation of C.

If G is a polynomial matrix, we let $\gamma(G)$ denote the number of columns of G and $\delta(G)$ the total column degree of G (i.e., the sum of all its column degrees.)

Theorem 3. *Let C be a convolutional code of length q, and let G be any its proper representation. Then*

$$\gamma(G) \geq \gamma(C) \quad \textit{and} \quad \delta(G) \geq \delta(C).$$

The following three conditions are equivalent:
(a) G is minimal;
(b) $\gamma(G) = \gamma(C)$;
(c) $\delta(G) = \delta(C)$.

Proof. Let p be the column number of G and a the column degree function. For each $d \geq 0$, let $\gamma_G(d)$ denote the number of values of a equal to d. Then

$$\gamma(G) = \sum \gamma_G(d) \quad \text{and} \quad \delta(G) = \sum d\gamma_G(d).$$

In view of Example 5, $\gamma_G(d) = \dim \Gamma_d(S^p[-a])$. And because the linear map $\Gamma_d(S^p[-a]) \to \Gamma_d(C)$ is surjective, we get $\gamma_G(d) \geq \gamma_C(d)$. We therefore have

$$\gamma(G) = \sum \gamma_G(d) \geq \sum \gamma_C(d) = \gamma(C),$$

and likewise

$$\delta(G) = \sum d\gamma_G(d) \geq \sum d\gamma_C(d) = \delta(C).$$

Certainly, (b) and (c) hold if and only if $\gamma_G(d) = \gamma_C(d)$ for every d. But this, in turn, is equivalent to bijectivity of all the linear maps $\Gamma_d(S^q[-a]) \to \Gamma_d(C)$.

The proof is complete. □

Corollary 1. *The Forney indices of a convolutional code are equal to the column degrees of any its minimal proper representation.*

Proof. As shown in the above proof, if G is a minimal proper representation of a convolutional code C, then $\gamma_C(d) = \gamma_G(d)$ for every d.

This implies what we want. □

Corollary 2. *(a) A minimal proper representation is a one that has minimal column number (among all proper representations).*

(b) A minimal proper representation is a one that has minimal total column degree (among all proper representations).

Remark. In dimension 1, the property of minimality and the property of having full column rank are equivalent for proper polynomial matrices. But this is not the case in higher dimensions. (See the following example.)

Example 6. Let C and G be as in Example 4. We have seen that G is a proper representation, i.e., the linear maps $S^3_{\leq d-1} \to C_{\leq d}$ are surjective for all $d \geq 0$. Now, we claim that G is minimal (though it is not of full column rank). First of all, $C_{\leq 0} = \{0\}$ and, consequently, the isomorphism $\Gamma_0(S^3[-1]) \simeq \Gamma_0(C)$ is trivial. Next, for $d \geq 2$, we have

$$\begin{aligned} C_{\leq d} &= G(S^3_{\leq d-1}) = G(S^3_{\leq d-2} + D_1 S^3_{\leq d-2} + D_2 S^3_{\leq d-2}) \\ &= G(S^3_{\leq d-2}) + D_1 G(S^3_{\leq d-2}) + D_2 G(S^3_{\leq d-2}) = C_{\leq d-1} + D_1 C_{\leq d-1} + D_2 C_{\leq d-1}, \end{aligned}$$

and consequently, $\Gamma_d(C) = \{0\}$. So, for all $d \geq 2$, we have trivial isomorphisms $\Gamma_d(S^3[-1]) \simeq \Gamma_d(C)$. Further, $S^3_{\leq 0} = \mathbb{F}^3$, and it is easily seen that the linear map $\mathbb{F}^3 \to C_{\leq 1}$ is not only surjective, but injective as well. Hence, we have an isomorphism $\Gamma_1(S^3[-1]) \simeq \Gamma_1(C)$. We see that C has the input number 3, the Forney indices (1, 1, 1), and its overall constraint length is equal to 3.

Appendix A. Graded modules

Introduce an extra ("homogenizing") indeterminate D_0, and define

$$T = \mathbb{F}[D_0, D_1, \dots, D_n].$$

Let I denote the ideal of T generated by $D_0, D_1, \dots, D_n$. This is a maximal ideal and $T/I = \mathbb{F}$.

A graded module over T is a module M together with a gradation, i.e., a sequence $M_0, M_1, M_2, \dots$ of $\mathbb{F}$-linear subspaces of M such that

$$M = \oplus M_d \quad \text{and} \quad D_k M_d \subseteq M_{d+1}\ \forall k, d.$$

A twisting function a of length p determines on T^p the gradation consisting of the spaces

$$T^p(-a)_d = \{f \in T^p |\ \deg(f_i) = d - a(i)\} \quad (d \geq 0).$$

The module T^p equipped with this gradation will be denoted by $T^p(-a)$.

A graded free module is a one that is isomorphic to a graded module of the form $T^p(-a)$.

A homomorphism of graded modules $M \to N$ is a module homomorphism $u : M \to N$ such that $u(M_d) \subseteq N_d$ for all $d \geq 0$.

Given a graded module M, we set $\overline{M} = M/IM$. The following lemma plays a key role in the theory of graded modules.

Lemma 2 (*"Nakayama's Lemma"*). *Let M be a graded module over T. If $\overline{M} = \{0\}$, then $M = \{0\}$.*

Proof. Assume not, and take a homogeneous element $m \in M$ of the smallest degree. Since elements of I have degree > 0, it is clear that $m \notin IM$. And we get $\overline{M} \neq \{0\}$. □

A homomorphism $u : L \to M$ of graded modules induces in an obvious way a linear map $\overline{L} \to \overline{M}$, denoted by $\overline{u}$. A homomorphism u is called minimal if $\overline{u}$ is bijective.

Corollary 3. *Let $u : L \to M$ be a homomorphism of graded modules. Then u is an epimorphism if and only if so is $\overline{u}$.*

Proof. Let N denote the cokernel of u. The exact sequence $L \to M \to N \to 0$ yields the exact sequence $\overline{L} \to \overline{M} \to \overline{N} \to 0$, and the statement follows by Nakayama's Lemma. □

Corollary 4. *Let $u : F_1 \to F_2$ be a homomorphism of graded free modules. Then u is an isomorphism if and only if so is $\overline{u}$.*

Proof. We need to show the "If" part. By the previous corollary, u is surjective. Next, because F_1 and F_2 are free, $rk(F_1) = \dim(\overline{F_1}) = \dim(\overline{F_2}) = rk(F_2)$. It follows that $Ker(u)$ has rank 0. On the other hand, $Ker(u)$ is torsion free (as a submodule of a free module). We conclude that $Ker(u) = \{0\}$. □

If M is a graded module, for every $d \geq 0$, we set

$$\Gamma_d(M) = \frac{M_d}{D_0 M_{d-1} + D_1 M_{d-1} + \cdots + D_n M_{d-1}}.$$

Lemma 3. *If M is a finitely generated graded module, then all the spaces $\Gamma_d(M)$ have finite dimension and all of them are trivial except for finitely many d.*

Proof. $\overline{M}$ is a finitely generated graded module. Hence, it is finite-dimensional as a linear space over $\mathbb{F}$. This completes the proof since $\overline{M} = \oplus_{d \geq 0} \Gamma_d(M)$. □

If $u : L \to M$ is a homomorphism of graded modules, then, for each $d \geq 0$, we have a canonical linear map $\Gamma_d(u) : \Gamma_d(L) \to \Gamma_d(M)$. Saying that $u : L \to M$ is minimal is the same as saying that all the linear maps $\Gamma_d(u)$ are bijective.

Appendix B. Proofs of Theorem 1 and uniqueness part of Theorem 2

The homogenization in degree d is the bijective linear map

$$S_{\leq d} \to T_d \ : \quad f \mapsto D_0^d f(D_1/D_0, \dots, D_n/D_0).$$

Example 7. The homogenization in degree 4 of the polynomial $2D_1^3 D_n + 1$ is $2D_1^3 D_n + D_0^4$ and the homogenization in degree 5 is $2D_0 D_1^3 D_n + D_0^5$.

If $C \subseteq S^q$ is a convolutional code, the homogenization C^h of C is defined to be

$$C^h = \bigoplus_{d \geq 0} C_d^h,$$

where C_d^h is the image of $C_{\leq d} = C \cap S_{\leq d}^q$ under the homogenization operator $S_{\leq d}^q \to T_d^q$. This is a graded submodule of T^q (a "homogeneous" convolutional code of length q).

If G is a polynomial matrix with column number p and column degree function a, the homogenization of G is defined to be

$$G^h = G(D_1/D_0, \ldots, D_n/D_0)\mathrm{diag}(D_0^{a(1)}, \ldots, D_0^{a(p)}).$$

Lemma 4. *Let $C \subseteq S^q$ be a convolutional code, and let G be its representation with column number p and column degree function a. Then*

(a) G is a proper representation if and only if $G^h T^p(-a) = C^h$;

(b) the homomorphism $G : S^p[-a] \to C$ is minimal if and only if so is the homomorphism $G^h : T^p(-a) \to C^h$.

Proof. The first assertion follows from the commutative diagrams

$$\begin{tikzcd} S^p[-a]_{\leq d} \arrow[r, "G"] \arrow[d] & S_{\leq d}^q \arrow[d] \\ T^p(-a)_d \arrow[r, "G^h"] & T_d^q \end{tikzcd} \quad (d \geq 0).$$

The second one follows from the commutative diagrams

$$\begin{tikzcd} \Gamma_d(S^p[-a]) \arrow[r, "\Gamma_d(G)"] \arrow[d] & \Gamma_d(C) \arrow[d] \\ \Gamma_d(T^p(-a)) \arrow[r, "\Gamma_d(G^h)"] & \Gamma_d(C^h) \end{tikzcd} \quad (d \geq 0).$$

The proof is complete. □

Proof of Theorem 1. It is easily seen that $\Gamma_d(C) \simeq \Gamma_d(C^h)$. The graded module C^h is finitely generated by Hilbert's basis theorem (see Theorem 4.1 in Ch. IV of Lang [9]), and it remains to apply the previous lemma. □

Proof of Uniqueness Part of Theorem 2. Suppose that G_1, G_2 are two minimal proper representations of C. Let p_1, p_2 be their column numbers and a_1, a_2 the column degree functions. The homogenizations of these matrices determine the homomorphisms of graded modules

$$G_1^h : T^{p_1}(-a_1) \to C^h \quad \text{and} \quad G_2^h : T^{p_2}(-a_2) \to C^h.$$

In view of Lemma 4, these homomorphisms are minimal. Because $T^{p_1}(-a_1)$ is free and because G_2^h is surjective, we can find a homomorphism $U : T^{p_1}(-a_1) \to T^{p_2}(-a_2)$ of graded modules that makes the diagram

$$\begin{tikzcd} T^{p_1}(-a_1) \arrow[r, "G_1^h"] \arrow[d, "U"'] & C^h \arrow[d, equal] \\ T^{p_2}(-a_2) \arrow[r, "G_2^h"] & C^h \end{tikzcd}$$

commutative. Using this diagram, we can see that $\overline{G_2^h}\,\overline{U} = \overline{G_1^h}$. It follows that $\overline{U}$ is an isomorphism. Then, by Corollary 4, U also is an isomorphism. Now, U is, in fact, a homogeneous polynomial matrix. Putting $D_0 = 1$ in this matrix, we get an isomorphism $S^{p_1}[-a_1] \simeq S^{p_2}[-a_2]$, which, in turn, determines an equivalence between G_1 and G_2.

The proof is complete. □

References

[1] N. Bourbaki, Commutative Algebra, Springer-Verlag, New-York, 1989, (Chapters 1–7).

[2] C. Charoenlarpnopparut, Applications of Gröbner bases to the structural description and realization of multidimensional convolutional code, Sci. Asia 35 (2009) 95–105.

[3] J.-J. Climent, D. Napp Avelli, C. Perea, R. Pinto, MDS 2D convolutional codes, in: 20th International Symposium on Mathematical Theory of Networks and Systems, Melbourne, Australia, 2012, pp. 9–13.

[4] D. Eisenbud, The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra, Springer-Verlag, New York, 2005.

[5] E. Fornasini, M.E. Valcher, Algebraic aspects of two-dimensional convolutional codes, IEEE Trans. Inform. Theory 40 (1994) 1068–1082.

[6] D. Forney, R. Johannesson, Z. Wan, Minimal and canonical rational generator matrices for convolutional codes, IEEE Trans. Inform. Theory 42 (1996) 1865–1880.

[7] P. Jangisarakul, C. Charoenlarpnopparut, Algebraic decoder of a multidimensional convolutional code: constructive algorithms for determining syndrome decoder and decoder matrix based on Gröbner basis, Multidimens. Syst. Signal Process. 22 (2011) 67–81.

[8] B. Kitchens, Multidimensional convolutional codes, SIAM J. Discrete Math. 15 (2002) 367–381.

[9] S. Lang, Algebra, Springer-Verlag, New-York, 2002.

[10] V. Lomadze, Reduced polynomial matrices in several variables, SIAM J. Control Optim. 51 (2013) 3258–3273.

[11] D. Napp Avelli, C. Perea, R. Pinto, Column distances for 2D-convolutional codes, in: Proceedings of the 19th International Symposium on MTNS, Budapest, Hungary, 2010.

[12] D. Napp Avelli, C. Perea, R. Pinto, Input-state-output representations and constructions of finite-support 2D convolutional codes, Adv. Math. Commun. 4 (2010) 533–545.

[13] M.E. Valcher, E. Fornasini, On 2D finite support convolutional codes: an algebraic approach, Multidimens. Syst. Signal Process. 5 (1994) 231–243.

[14] P. Weiner, Multidimensional Convolutional Codes (Ph.D. dissertation), University of Notre Dame, USA, 1998.

[15] E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, Asian J. Control 12 (2010) 117–236.