

Product convolutional codes from linear system point of view*

Joan-Josep Climent¹, Victoria Herranz² and Carmen Perea²

Abstract—In this work, from a controllable and observable input-state-output representation of two convolutional codes, we present an input-state-output representation of a convolutional product code. We also establish a lower bound on the free distance of the product code in terms of the free distance of the constituent codes.

I. INTRODUCTION

Combining known codes is a powerful method to obtain a new code with better error correction capability avoiding the exponential increase of decoding complexity. For convolutional codes, we can find in the literature some powerful combining methods as turbo codes [1] and woven convolutional codes [2], [3]. More recently, as a natural extension of the direct product codes introduced by Elias [4], Bossert, Medina and Sidorenko [5] introduce the product of convolutional codes and they show that every convolutional product code can be represented as a woven code.

On the other hand, Climent, Herranz and Perea [6] and Herranz [7], using the input-state-output representation of convolutional codes introduced by Rosenthal and York [8], introduce the input-state-output representation of different serial and parallel concatenation convolutional codes. With this concatenated convolutional codes they also present a construction of new codes with prescribed distance.

The paper is structured as follows. In Section II we review the way in which convolutional codes have been described in the context of linear systems theory. We also describe how product convolutional codes are constructed as convolutional counterpart of the direct product of block codes. In Section III we present an input-state-output representation of a product code from the input-state-output representations of the constituent codes. We also give a lower bound of the free distance of the product code in terms of the free distances of the constituent codes. Finally, conclusions are presented in Section IV.

II. PRELIMINARIES

A. Input-State-Output Representation of a Convolutional Code

In this paper, we denote by \mathbb{F} a finite field and by $\mathbb{F}[z]$ the polynomial ring on the variable z with coefficients in \mathbb{F} .

*This work was partially supported by Spanish grant MTM2011-24858 of the Ministerio de Ciencia e Innovación of the Gobierno de España.

¹Joan-Josep Climent is with the Departament d'Estadística i Investigació Operativa, Universitat d'Alacant, Apartat de Correus 99, E-03080 Alacant, Spain. jcliment@ua.es

²Victoria Herranz and Carmen Perea are with the Centro de Investigación Operativa, Departamento de Estadística, Matemáticas e Informática, Universidad Miguel Hernández de Elche, Avenida del Ferrocarril, s/n. E-03202 Elche, Spain. mavi.herranz@umh.es, perea@umh.es

A convolutional code of rate k/n is a submodule \mathcal{C} of $\mathbb{F}^n[z]$ with rank k . So, there exists an $n \times k$ polynomial encoder matrix $G(z) \in \mathbb{F}[z]^{n \times k}$, which is basic and minimal, such that

$$\mathcal{C} = \{v(z) \in \mathbb{F}[z]^n \mid v(z) = G(z)u(z) \text{ with } u(z) \in \mathbb{F}[z]^k\}.$$

A convolutional code is *observable* if one, and therefore any, generator matrix $G(z)$ is right prime (see [9]). Furthermore, if $G(z)$ is a generator matrix of an observable convolutional code, then $G(z)$ is a noncatastrophic generator matrix (see [9]). The *degree* or *complexity* of \mathcal{C} is the sum of the column degrees of one, and hence any, minimal basic generator matrix. A convolutional code \mathcal{C} of rate k/n and degree δ , called an (n, k, δ) -code, can be given by the *input-state-output (ISO) representation* (see [10], [11], [8], [12])

$$\begin{aligned} \mathbf{x}_{t+1} &= A\mathbf{x}_t + B\mathbf{u}_t, \\ \mathbf{y}_t &= C\mathbf{x}_t + D\mathbf{u}_t, \\ \mathbf{v}_t &= \begin{pmatrix} \mathbf{y}_t \\ \mathbf{u}_t \end{pmatrix}, \quad \mathbf{x}_0 = \mathbf{0}, \end{aligned} \tag{1}$$

where for each instant t , $\mathbf{x}_t \in \mathbb{F}^\delta$ is the *state vector*, $\mathbf{u}_t \in \mathbb{F}^k$ is the *information vector*, $\mathbf{y}_t \in \mathbb{F}^{n-k}$ is the *parity vector*, and $\mathbf{v}_t \in \mathbb{F}^n$ is a codeword of \mathcal{C} . In this case, \mathcal{C} is said to be generated by (A, B, C, D) and denoted by $\mathcal{C}(A, B, C, D)$. Here, A , B , C , and D are matrices of sizes $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ and $(n-k) \times k$, respectively; that is, (A, B, C, D) is a *minimal representation* and it is characterized through the condition that the pair (A, B) is *controllable*. Note that the concept of minimality of an ISO representation is different from the concept of minimality of a representation in classical linear systems theory. In fact, if (A, B) is controllable, then the observability of (A, C) ensures that the linear system (1) describes a noncatastrophic convolutional code (see [8, Lemma 2.11]).

The *free distance* of a convolutional code \mathcal{C} can be characterized (see [10]) as

$$d_{free}(\mathcal{C}) = \min \left(\sum_{t=0}^{\infty} \text{wt}(\mathbf{u}_t) + \sum_{t=0}^{\infty} \text{wt}(\mathbf{y}_t) \right)$$

where the minimum has to be taken over all possible nonzero codewords and where wt denotes the Hamming weight. The free distance of an (n, k, δ) -code \mathcal{C} is always upper-bounded (see [13]) by the *generalized Singleton bound*

$$d_{free}(\mathcal{C}) \leq (n-k) \left(\left\lceil \frac{\delta}{k} \right\rceil + 1 \right) + \delta + 1.$$

In addition, the convolutional code \mathcal{C} is called *maximum-distance separable (MDS)* if its free distance is equal to the generalized Singleton bound.

B. Product Convolutional Codes

Let \mathcal{C}^+ and \mathcal{C}^- be “vertical” (n^+, k^+, δ^+) and “horizontal” (n^-, k^-, δ^-) -codes respectively. Then, the *product convolutional code* $\mathcal{C}^+ \otimes \mathcal{C}^-$ is defined to be the convolutional code whose codewords consist of all $n^+ \times n^-$ matrices with all columns in \mathcal{C}^+ and all rows in \mathcal{C}^- (see [5], [14]). It is an $(n^+n^-, k^+k^-, \delta^+k^- + \delta^-k^+)$ -code.

Encoding of the product convolutional code $\mathcal{C}^+ \otimes \mathcal{C}^-$ can be done as follows (see [5], [14]). Let $G^+(z)$ and $G^-(z)$ be generator matrices of the component convolutional codes \mathcal{C}^+ and \mathcal{C}^- , respectively. Denote by $U(z)$ a $k^+ \times k^-$ information matrix over $\mathbb{F}[z]$. Now, every column of $U(z)$ is encoded using $G^+(z)$, and then every row of the resulting matrix is encoding using $G^-(z)$. Thus, the encoded codeword matrix $V(z)$ is given by

$$V(z) = G^+(z)U(z)G^-(z)^T.$$

Note that $V(z)$ can be described in terms of the Kronecker product of the generator matrices $G^+(z)$ and $G^-(z)$ as follows:

$$\text{vect}(V(z)) = (G^-(z) \otimes G^+(z)) \text{vect}(U(z))$$

where $\text{vect}(\cdot)$ denotes the vectorization of a matrix formed by stacking its columns into a single column vector.

III. INPUT-STATE-OUTPUT REPRESENTATION OF A PRODUCT CONVOLUTIONAL CODE

In this section we obtain the matrices that describes an ISO representation of the product code from ISO representations of the vertical and horizontal codes \mathcal{C}^+ and \mathcal{C}^- .

Assume that (A^+, B^+, C^+, D^+) is an ISO representation of the vertical (n^+, k^+, δ^+) code \mathcal{C}^+ . Analogously, let (A^-, B^-, C^-, D^-) be an ISO representation of the horizontal (n^-, k^-, δ^-) code \mathcal{C}^- . Assume also that the $k^+ \times k^-$ matrix U_t is the information matrix of the product code $\mathcal{C}^+ \otimes \mathcal{C}^-$.

By using the vertical code \mathcal{C}^+ , we can encode the columns of U_t as

$$\begin{aligned} \mathbf{x}_{t+1}^{(1)} &= A_1 \mathbf{x}_t^{(1)} + B_1 \mathbf{u}_t^{(1)}, \\ \mathbf{y}_t^{(1)} &= C_1 \mathbf{x}_t^{(1)} + D_1 \mathbf{u}_t^{(1)}, \\ \mathbf{v}_t^{(1)} &= \begin{pmatrix} \mathbf{y}_t^{(1)} \\ \mathbf{u}_t^{(1)} \end{pmatrix}, \quad \mathbf{x}_0^{(1)} = \mathbf{0}, \end{aligned} \quad (2)$$

where $\mathbf{u}_t^{(1)} = \text{vect}(U_t)$ and

$$\begin{aligned} A_1 &= I_{k^-} \otimes A^+, & B_1 &= I_{k^-} \otimes B^+, \\ C_1 &= I_{k^-} \otimes C^+, & D_1 &= I_{k^-} \otimes D^+. \end{aligned}$$

Note that $A_1, B_1, C_1,$ and D_1 are matrices of sizes $\delta^+k^- \times \delta^+k^-$, $\delta^+k^- \times k^+k^-$, $(n^+ - k^+)k^- \times \delta^+k^-$, and $(n^+ - k^+)k^- \times k^+k^-$, respectively.

Now, by using the horizontal code \mathcal{C}^- , we can encode the rows of U_t . For this, we need transform each row of matrix U_t in an appropriate column vector; we can carry out this

process as $\mathbf{u}_t^{(2)} = Q\mathbf{u}_t^{(1)}$ where Q is the permutation matrix given by

$$Q = \begin{pmatrix} I_{k^-} \otimes \mathbf{e}_1^T \\ I_{k^-} \otimes \mathbf{e}_2^T \\ \vdots \\ I_{k^-} \otimes \mathbf{e}_{k^+}^T \end{pmatrix}.$$

Here \mathbf{e}_i is the k^+ -column vector with a 1 in the i th entry and 0 otherwise. So, the horizontal code \mathcal{C}^- encodes the vector $\mathbf{u}_t^{(2)}$ as

$$\begin{aligned} \mathbf{x}_{t+1}^{(2)} &= A_2 \mathbf{x}_t^{(2)} + B_2 \mathbf{u}_t^{(2)}, \\ \mathbf{y}_t^{(2)} &= C_2 \mathbf{x}_t^{(2)} + D_2 \mathbf{u}_t^{(2)}, \\ \mathbf{v}_t^{(2)} &= \begin{pmatrix} \mathbf{y}_t^{(2)} \\ \mathbf{u}_t^{(2)} \end{pmatrix}, \quad \mathbf{x}_0^{(2)} = \mathbf{0}, \end{aligned} \quad (3)$$

where

$$\begin{aligned} A_2 &= I_{k^+} \otimes A^-, & B_2 &= I_{k^+} \otimes B^-, \\ C_2 &= I_{k^+} \otimes C^-, & D_2 &= I_{k^+} \otimes D^-. \end{aligned}$$

Note that $A_2, B_2, C_2,$ and D_2 are matrices of sizes $\delta^-k^+ \times \delta^-k^+$, $\delta^-k^+ \times k^+k^-$, $(n^- - k^-)k^+ \times \delta^-k^+$, and $(n^- - k^-)k^+ \times k^+k^-$, respectively.

Following a reciprocal process to the one used to obtain the column vector $\mathbf{u}_t^{(1)}$ from the matrix U_t ; that is, $\mathbf{u}_t^{(1)} = \text{vect}(U_t)$, we obtain the matrix Y_t from the parity vector $\mathbf{y}_t^{(1)}$; that is, $\mathbf{y}_t^{(1)} = \text{vect}(Y_t)$. Then, by using again the horizontal code \mathcal{C}^- we can encode the rows of Y_t . Similarly to the previous case, we consider the column vector $\mathbf{u}_t^{(3)} = P\mathbf{y}_t^{(1)}$ where P is the permutation matrix given by

$$P = \begin{pmatrix} I_{k^-} \otimes \mathbf{d}_1^T \\ I_{k^-} \otimes \mathbf{d}_2^T \\ \vdots \\ I_{k^-} \otimes \mathbf{d}_{n^+ - k^+}^T \end{pmatrix}$$

where \mathbf{d}_i is the $(n^+ - k^+)$ -column vector with a 1 in the i th entry and 0 otherwise. So, the horizontal code \mathcal{C}^- encodes the vector $\mathbf{u}_t^{(3)}$ as

$$\begin{aligned} \mathbf{x}_{t+1}^{(3)} &= A_3 \mathbf{x}_t^{(3)} + B_3 P\mathbf{y}_t^{(1)}, \\ \mathbf{y}_t^{(3)} &= C_3 \mathbf{x}_t^{(3)} + D_3 P\mathbf{y}_t^{(1)}, \\ \mathbf{v}_t^{(3)} &= \begin{pmatrix} \mathbf{y}_t^{(3)} \\ \mathbf{u}_t^{(3)} \end{pmatrix}, \quad \mathbf{x}_0^{(3)} = \mathbf{0}, \end{aligned} \quad (4)$$

where

$$\begin{aligned} A_3 &= I_{n^+ - k^+} \otimes A^-, & B_3 &= I_{n^+ - k^+} \otimes B^-, \\ C_3 &= I_{n^+ - k^+} \otimes C^-, & D_3 &= I_{n^+ - k^+} \otimes D^-. \end{aligned}$$

Note that $A_3, B_3, C_3,$ and D_3 are matrices of sizes $(n^+ - k^+)\delta^- \times (n^+ - k^+)\delta^-$, $(n^+ - k^+)\delta^- \times (n^+ - k^+)k^-$, $(n^+ - k^+)(n^- - k^-) \times (n^+ - k^+)\delta^-$, and $(n^+ - k^+)(n^- - k^-) \times (n^+ - k^+)k^-$, respectively.

Finally, taking into account that the state vector of the product code is $\mathbf{x}_t = (\mathbf{x}_t^{(3)}, \mathbf{x}_t^{(2)}, \mathbf{x}_t^{(1)})^T$ and that the parity vector is $\mathbf{y}_t = (\mathbf{y}_t^{(3)}, \mathbf{y}_t^{(2)}, \mathbf{y}_t^{(1)})^T$, from expressions (2), (3), and (4) we obtain an ISO representation of the product code.

Theorem 1: Assume that (A^1, B^1, C^1, D^1) is an ISO representation of the vertical (n^1, k^1, δ^1) code C^1 . Analogously, let (A^-, B^-, C^-, D^-) be an ISO representation of the horizontal (n^-, k^-, δ^-) code C^- . Then an ISO representation for the product code $C^1 \otimes C^-$ is given by (1), with

$$A = \begin{pmatrix} I_{n^1-k^1} \otimes A^- & O & (I_{n^1-k^1} \otimes B^-)P(I_{k^-} \otimes C^1) \\ O & I_{k^1} \otimes A^- & O \\ O & O & I_{k^-} \otimes A^1 \end{pmatrix},$$

$$B = \begin{pmatrix} (I_{n^1-k^1} \otimes B^-)P(I_{k^-} \otimes D^1) \\ (I_{k^1} \otimes B^-)Q \\ I_{k^-} \otimes B^1 \end{pmatrix},$$

$$C = \begin{pmatrix} I_{n^1-k^1} \otimes C^- & O & (I_{n^1-k^1} \otimes D^-)P(I_{k^-} \otimes C^1) \\ O & I_{k^1} \otimes C^- & O \\ O & O & I_{k^-} \otimes C^1 \end{pmatrix},$$

$$D = \begin{pmatrix} (I_{n^1-k^1} \otimes D^-)P(I_{k^-} \otimes D^1) \\ (I_{k^1} \otimes D^-)Q \\ I_{k^-} \otimes D^1 \end{pmatrix},$$

where O denotes the null matrix of the appropriate size.

Once we have obtained an ISO representation of the product code $C^1 \otimes C^-$, we are interested in the properties to be satisfied by matrices $A^1, B^1, C^1, D^1, A^-, B^-, C^-$ and D^- . The next example shows that is not enough for the pairs (A^1, B^1) and (A^-, B^-) to be controllable in order to get a controllable pair (A, B) for the product code.

Example 1: Let α be a primitive element of the Galois field $\mathbb{F} = GF(8)$ with $\alpha^3 + \alpha + 1 = 0$, and consider the $(6, 4, 2)$ -vertical code $C^1(A^1, B^1, C^1, D^1)$, where

$$A^1 = \begin{pmatrix} \alpha^3 & \alpha \\ \alpha & \alpha^4 \end{pmatrix}, \quad B^1 = \begin{pmatrix} 1 & \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix},$$

$$C^1 = \begin{pmatrix} 1 & \alpha \\ \alpha & 1 \end{pmatrix}, \quad D^1 = \begin{pmatrix} \alpha^3 & \alpha^4 & \alpha^3 & \alpha^4 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

and a $(5, 2, 1)$ -horizontal code $C^-(A^-, B^-, C^-, D^-)$, where

$$A^- = (\alpha), \quad B^- = (\alpha^3 \ 0),$$

$$C^- = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad D^- = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha & 0 \end{pmatrix}.$$

For all $z \in \mathbb{F}$ we have that

$$\text{rank}(zI_{\delta^1} - A^1 \ B^1) = 2$$

$$\text{rank}(zI_{\delta^-} - A^- \ B^-) = 1$$

and therefore, the pairs (A^1, B^1) and (A^-, B^-) are controllable.

Now, if we compute the matrices A and B of the product code, we observe that

$$\text{rank}(\alpha I_{10} - A \ B) = 8,$$

so the pair (A, B) is not controllable.

We provide, in the next theorem, a lower bound for the free distance of $C^1 \otimes C^-$ in terms of the free distances of C^1 and C^- .

Theorem 2: Let C^1 and C^- be (n^1, k^1, δ^1) and (n^-, k^-, δ^-) codes. Then, the free distance of the product code $C^1 \otimes C^-$ verifies

$$d_{free}(C^1 \otimes C^-) \geq k^- d_{free}(C^1) + k^1 d_{free}(C^-) - k^- k^1.$$

IV. CONCLUSIONS

The results introduced in this paper show an input-state-output representation of a product code and a lower bound on its free distance. This representation will allow us to introduce, from a given vertical and horizontal codes, a new product convolutional code with fixed distance.

REFERENCES

- [1] K. Sripimanwat, Ed., *Turbo Code Applications. A Journey from a Paper to Realization*. The Netherlands: Springer, 2005.
- [2] V. Zyablov, S. Shavgulidze, O. Skopintsev, S. Höst, and R. Johannesson, "On the error exponent for woven convolutional codes with outer warp," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1649–1653, 1999.
- [3] V. V. Zyablov, S. Shavgulidze, and R. Johannesson, "On the error exponent for woven convolutional codes with inner warp," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1195–1199, 2001.
- [4] P. Elias, "Error free coding," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 29–37, 1954.
- [5] M. Bossert, C. Medina, and Sidorenko, "Encoding and distance estimation of product convolutional codes," in *Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 2005)*. Adelaide, Australia: IEEE, Sept. 2005, pp. 1063–1066.
- [6] J.-J. Climent, V. Herranz, and C. Perea, "A first approximation of concatenated convolutional codes from linear systems theory viewpoint," *Linear Algebra and its Applications*, vol. 425, pp. 673–699, 2007.
- [7] V. Herranz, "Estudio y construcción de códigos convolucionales: Códigos perforados, códigos concatenados desde el punto de vista de sistemas," Ph.D. dissertation, Departamento de Estadística, Matemáticas e Informática, Universidad Miguel Hernández, Elche, Spain, Mar. 2007.
- [8] J. Rosenthal and E. V. York, "BCH convolutional codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1833–1844, 1999.
- [9] J. Rosenthal and R. Smarandache, "Construction of convolutional codes using methods from linear systems theory," in *Proceedings of the 35th Allerton Conference on Communications, Control and Computing*, Allerton House, Monticello, IL, Sept. 1997, pp. 953–960.
- [10] R. Hutchinson, J. Rosenthal, and R. Smarandache, "Convolutional codes with maximum distance profile," *Systems & Control Letters*, vol. 54, no. 1, pp. 53–63, 2005.
- [11] J. Rosenthal, J. M. Schumacher, and E. V. York, "On behaviors and convolutional codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1881–1891, 1996.
- [12] J. Rosenthal, "Connections between linear systems and convolutional codes," in *Codes, Systems and Graphical Models*, ser. The IMA Volumes in Mathematics and its Applications, B. Marcus and J. Rosenthal, Eds. New York: Springer-Verlag, 2001, vol. 123, pp. 39–66.
- [13] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, pp. 15–32, 1999.
- [14] C. Medina, V. R. Sidorenko, and V. V. Zyablov, "Error exponents for product convolutional codes," *Problems of Information Transmission*, vol. 42, no. 3, pp. 167–182, 2006.