Bol. Soc. Esp. Mat. Apl.
nº 42(2008), 183–193

CODE DECOMPOSITION IN THE ANALYSIS OF A CONVOLUTIONAL CODE

E. FORNASINI*, R. PINTO†

*Department of Information Engineering, University of Padua, 35131 Padova, ITALY. E-mail: fornasini@dei.unipd.it.
†Department of Mathematics, University of Aveiro, 3810-193 Aveiro, PORTUGAL. E-mail: raquel@ua.pt.

Abstract

A convolutional code can be decomposed into smaller codes if it admits decoupled encoders. In this paper, we show that if a code can be decomposed into smaller codes (subcodes) its column distances are the minimum of the column distances of its subcodes. Moreover, the j-th column distance of a convolutional code $\mathcal{C}$ is equal to the j-th column distance of the convolutional codes generated by the truncation of the canonical encoders of $\mathcal{C}$ to matrices which entries have degree smaller or equal than j. We show that if one of such codes can be decomposed into smaller codes, so can be all the other codes.

Key words: *Convolutional codes, decoupled encoders, code decomposition, free distance, column distance*
AMS subject classifications:

1 Introduction

Some convolutional codes can be decomposed into smaller codes (subcodes). This happens if they admit decoupled encoders among its encoders [2]. The free distance and the column distances are the most common distance measures for a convolutional code. It was shown in [1] that the free distance of a code is equal to the minimum of the free distances of its subcodes. In this paper, we will show that similarly to the free distance, the j-th column distance of a convolutional code $\mathcal{C}$ is equal to the minimum of the j-th column distances of its subcodes. Moreover, to calculate the j-th column distance of $\mathcal{C}$ we can consider the truncation of the entries of a canonical encoder of $\mathcal{C}$ to polynomials of degree smaller or equal than j (truncation to degree j). Such obtained matrix generates a different convolutional code with same i-th column distances than $\mathcal{C}$, for $i \leq j$. So, if $\mathcal{C}$ admits a canonical encoder which truncation to degree j is

† Supported in part by the Portuguese Science Foundation (FCT) through the Unidade de Investigação Matemática e Aplicações of the University of Aveiro, Portugal.

a decoupled encoder, $G_d(d)$, we have that the j-th column distance of $\mathcal{C}$ is equal to the minimum of the column distances of the subcodes of the convolutional code generated by $G_d(d)$. We will see that if a convolutional code has such a canonical encoder, all the convolutional codes generated by the truncation to degree j of canonical encoders of $\mathcal{C}$ also admit decoupled encoders.

2 Convolutional codes

We will consider convolutional codes constituted by left compact sequences of $(\mathbb{F}^p)^{\mathbb{Z}}$, where $p \in \mathbb{N}$ and $\mathbb{F}$ is a finite field. Such sequences are naturally represented by Laurent power series $\hat{\mathbf{w}}(d) = \sum \mathbf{w}_t d^t \in \mathbb{F}((d))^p$, and we are allowed to multiply any left compact support sequence by a scalar Laurent series $s(d) = \sum s_t d^t \in \mathbb{F}((d))$. In fact, $\mathbb{F}((d))^p$ is a vector space over the field $\mathbb{F}((d))$. $\mathbb{F}[d]$ and $\mathbb{F}(d)$ will denote, as usually, the ring of polynomials and the field of rational functions with coefficients in $\mathbb{F}$, respectively.

A $[p, m]$-*convolutional code* is an m-dimensional subspace of $\mathbb{F}((d))^p$, which has a rational (and polynomial) basis, i.e., that is generated by a full row rank rational matrix $G(d) \in \mathbb{F}(d)^{m \times p}$,

$$\mathcal{C} = Im\, G(d) = \{\hat{\mathbf{w}}(d) : \hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d),\ \hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m\}.$$

$\mathcal{C}$ is said to have *rate* $\frac{m}{p}$ and $G(d)$ is called an *encoder* of $\mathcal{C}$. $G(d)$ produces a codeword $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ corresponding to each information sequence $\hat{\mathbf{u}}(d) \in \mathbb{F}((d))^m$. A convolutional code admits many encoders. Two encoders that generate the same code are called *equivalent encoders* and are related by a nonsingular rational left factor in $\mathbb{F}(d)^{m \times m}$. The encoders that can be realized by a physical device are called *causal encoders*. A causal encoder induces a "non-anticipatory" input-output map, i.e., produces codewords that start at the same time or after the corresponding information sequences. Among the causal encoders of a convolutional code we have the polynomial encoders and in the class of the polynomial encoders we distinguish the *canonical encoders* which are the left prime and row reduced ones. Two canonical encoders of a convolutional code $\mathcal{C}$ have the same row degrees $\phi_i,\ i = 1, \ldots, m$, up to a row permutation, and these row degrees are called *Forney indices* of $\mathcal{C}$. The maximum of the Forney indices is the *memory* of $\mathcal{C}$ and is represented by ν [3, 5].

The *free distance* of a convolutional code $\mathcal{C}$ [5] is defined as

$$d_{free}(\mathcal{C}) := \min\{w_H(\hat{\mathbf{w}}(d)) = \sum w_H(\mathbf{w}_t) : \hat{\mathbf{w}}(d) = \sum \mathbf{w}_t d^t \in \mathcal{C} \backslash \{0\}\},$$

where $w_H(\mathbf{w}_t)$ represents the Hamming weight of $\mathbf{w}_t$, and is bounded by

$$d_{free}(\mathcal{C}) \leq (p - m)(\lfloor \frac{\nu}{m} \rfloor + 1) + \nu + 1.$$

Such a bound is called the *generalized Singleton bound*. If the free distance of $\mathcal{C}$ is equal to the corresponding generalized Singleton bound, then $\mathcal{C}$ is said to be an *MDS-code* [6].

A distance measure associated to each causal encoder of a convolutional code $\mathcal{C}$ is the *column distance* [5].

Definition 2.1 *The j-th order column distance of a causal encoder $G(d) \in \mathbb{F}(d)^{m\times p}$ is the minimum of the Hamming weights of $\hat{\mathbf{w}}(d)|_{[0,j]}$ [1] where $\hat{\mathbf{w}}(d)$ is a codeword corresponding to an information sequence $\hat{\mathbf{u}}(d) = \sum_{t\geq 0} \mathbf{u}_t d^t$ such that $\mathbf{u}_0 \neq 0$.*

The column distance is an encoder property and two equivalent causal encoders can have different column distances. However the causal encoders of a convolutional code which are delay-free (i.e., that produce codewords that start at the same time as the corresponding information sequences) have the same column distances, which leads to the definition of column distance of the code. In this definition we only refer to polynomial encoders for simplicity. A polynomial encoder $G(d)$ is delay-free if and only if $G(0)$ has full row rank. Observe that a convolutional code always admit such encoders, being the canonical encoders an example of delay-free polynomial encoders.

Definition 2.2 *The j-th order column distance of a convolutional code is the j-th order column distance of any polynomial encoder $G(d)$ of $\mathcal{C}$ such that $G(0)$ is full row rank.*

Let $G(d) = G_0 + G_1 d + \cdots + G_\ell d^\ell$, $G_i \in \mathbb{F}^{m\times p}$, $i = 1, \ldots, \ell$, be a polynomial encoder of degree ℓ [2] of the convolutional code $\mathcal{C}$, with $G(0) = G_0$ full row rank, and

$$\mathbf{M}(G(d)) = \begin{bmatrix} G_0 & G_1 & \cdots & \cdots & G_\ell & & \\ & G_0 & G_1 & \cdots & \cdots & G_\ell & \\ & & \ddots & \ddots & & & \ddots \end{bmatrix}$$

the corresponding semi-infinite matrix. Denote by $\mathbf{M}_j^c(G(d))$ the truncation of $\mathbf{M}(G(d))$ after $j+1$ (block) columns

$$\mathbf{M}_j^c(G(d)) = \begin{bmatrix} G_0 & G_1 & G_2 & \cdots & G_j \\ & G_0 & G_1 & \cdots & G_{j-1} \\ & & G_0 & & G_{j-2} \\ & & & \ddots & \vdots \\ & & & & G_0 \end{bmatrix} \tag{1}$$

where $G_i = 0$ for $i > \ell$. Then the j-th order column distance of $\mathcal{C}$ is

$$d_j^c(\mathcal{C}) = \min_{\mathbf{u}_0 \neq 0} \{ w_H([\mathbf{u}_0\, \mathbf{u}_1 \ldots \mathbf{u}_j]\mathbf{M}_j^c(G(d))) \},$$

[1] If $\hat{\mathbf{w}}(d) = \sum_{t\geq k} \mathbf{w}_t d^t$ then $\hat{\mathbf{w}}(d)|_{[0,j]} = \sum_{t=0}^{j} \mathbf{w}_t d^t$ where $\mathbf{w}_t = 0$ for $t < k$, if $k > 0$.

[2] We consider the degree of a polynomial matrix as the maximum of the degrees of its entries. If $G(d)$ is an $m \times p$ polynomial matrix of degree ℓ, we can write $G(d) = G_0 + G_1 d + \cdots + G_\ell d^\ell$, with $G_i \in \mathbb{F}^{m\times p}$, $i = 1, \ldots, \ell$, and $G_\ell \neq 0$.

with $\mathbf{u}_i \in \mathbb{F}^m$, $i = 0, 1, \ldots, j$, for all $j \in \mathbb{N}$ [5]. For every $j \geq 0$, the j-th column distance of a $[p, m]$-convolutional code $\mathcal{C}$ is bounded by [4]

$$d_j^c(\mathcal{C}) \leq (p - m)(j + 1) + 1.$$

3 Decoupled encoders and code decomposition

A convolutional code is decomposable into smaller codes if it admits encoders in block diagonal form, called *decoupled encoders*. In this section we present a brief introduction to such encoders. For more details see [2].

Definition 3.1 *Let $p_1, \ldots, p_k$ be positive integers such that $\sum_{i=1}^k p_i = p$ and P a permutation matrix. An encoder $G(d)$ of $\mathcal{C}$ is said to be a $(p_1, \ldots, p_k)$-decoupled encoder of $\mathcal{C}$ associated with P if there exist positive integers $m_1, \ldots, m_k$ with $\sum_{i=1}^k m_i = m$ such that*

$$G(d)P = \operatorname{diag}\{G^{(1)}(d), \ldots, G^{(k)}(d)\}, \tag{2}$$

with $G^{(i)}(d) \in \mathbb{F}(d)^{m_i \times p_i}$, $i = 1, \ldots, k$.

If $G(d)$ is a $(p_1, \ldots, p_k)$-decoupled encoder that satisfies (2) and $\hat{\mathbf{u}}(d) = [\hat{\mathbf{u}}_1(d) \cdots \hat{\mathbf{u}}_k(d)] \in \mathbb{F}((d))^m$, with $\hat{\mathbf{u}}_i(d) \in \mathbb{F}((d))^{m_i}$, an information sequence, then its corresponding codeword $\hat{\mathbf{w}}(d) = \hat{\mathbf{u}}(d)G(d)$ is of the form

$$\hat{\mathbf{w}}(d) = [\hat{\mathbf{w}}_1(d) \cdots \hat{\mathbf{w}}_k(d)]P,$$

where $\hat{\mathbf{w}}_i(d) = \hat{\mathbf{u}}_i(d)G^{(i)}(d)$, $i = 1, \ldots, k$. Consequently, up to a permutation of the components of the codewords of $\mathcal{C}$,

$$\mathcal{C} = \mathcal{C}^{(1)} \times \cdots \times \mathcal{C}^{(k)},$$

where $\mathcal{C}^{(i)}$ is the $[p_i, m_i]$-convolutional code generated by $G^{(i)}(d)$, $i = 1, \ldots, k$, and we say that $\mathcal{C}$ is *decomposable* into $\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(k)}$. If $\mathcal{C}$ does not have a (p_1, p_2)-decoupled encoder, for some $p_1, p_2 \in \mathbb{N}$, then $\mathcal{C}$ is said to be an *undecomposable code*.

Definition 3.2 *A $(p_1, \ldots, p_k)$-decoupled encoder $G(d)$ of $\mathcal{C}$ associated with a permutation matrix P,*

$$G(d) = \operatorname{diag}\{G^{(1)}(d), \ldots, G^{(k)}(d)\}P^{-1},$$

with $G^{(i)}(d) \in \mathbb{F}(d)^{m_i \times p_i}$, $i = 1, \ldots, k$ and $\sum_{i=1}^k m_i = m$, is said to be maximally-decoupled if $\mathcal{C}^{(i)} = Im\, G^{(i)}(d)$ is undecomposable, $i = 1, \ldots, k$.

The determination of a decoupled encoder of a $[p, m]$-convolutional code $\mathcal{C}$ is directly related with a partition of the columns of the encoders of $\mathcal{C}$. We

will consider that the columns of any encoder of $\mathcal{C}$ constitute a set of nonzero generators of $\mathbb{F}((d))^m$. [3]

Definition 3.3 *A set of nonzero generators of* $\mathbb{F}((d))^m$,

$$\mathcal{G} = \{\hat{\mathbf{v}}_1(d), \hat{\mathbf{v}}_2(d), \ldots, \hat{\mathbf{v}}_p(d)\}$$

and a decomposition of $\mathbb{F}((d))^m$ *in direct sum*

$$\mathbb{F}((d))^m = V_1 \oplus V_2 \oplus \cdots \oplus V_k, \tag{3}$$

are compatible if every vector of $\mathcal{G}$ *belongs to a summand of (3) (and, obviously, to only one).*

If a generator set $\mathcal{G}$ is compatible with (3), then

(i) $\mathcal{G}_1 \dot{\cup} \mathcal{G}_2 \dot{\cup} \ldots \dot{\cup} \mathcal{G}_k$ with $\mathcal{G}_i := V_i \cap \mathcal{G}$, $i = 1 \ldots, k$, is a partition of $\mathcal{G}$ and $V_i = \text{span}(\mathcal{G}_i)$, $i = 1, \ldots, k$.

(ii) if $\mathrm{B} := \{\hat{\mathbf{v}}_{i_1}(d), \ldots, \hat{\mathbf{v}}_{i_m}(d)\} \subset \mathcal{G}$ is a basis of $\mathbb{F}((d))^m$, $\mathrm{B}_i := \mathcal{G}_i \cap \mathrm{B}$ is a basis of $\text{span}(\mathcal{G}_i)$.

(iii) there exists a unique finest direct sum decomposition

$$V = \bar{V}_1 \oplus \bar{V}_2 \oplus \cdots \oplus \bar{V}_h \tag{4}$$

compatible with $\mathcal{G}$. Each summand of any other compatible decomposition of $\mathbb{F}((d))^m$ can be expressed as a suitable sum of some $\bar{V}_i$s in (4).

The following algorithm determines the partition of $\mathcal{G} = \{\hat{\mathbf{v}}_1(d) \ldots \hat{\mathbf{v}}_p(d)\}$ associated with (4).

Algorithm 1:
Input: $G(d) = [\hat{\mathbf{v}}_1(d) \ldots \hat{\mathbf{v}}_p(d)]$.
Step 1: Select an $m \times m$ nonsingular submatrix $B(d)$ of $G(d)$ and put

$$X(d) = B(d)^{-1} G(d).$$

Step 2: Construct the $m \times p$ boolean matrix A defined by

$$A_{ij} = \begin{cases} 1 & if \quad X_{ij} \neq 0 \\ 0 & if \quad X_{ij} = 0 \end{cases}.$$

Step 3: Compute $(A^T A)^{p-1}$ and determine a permutation matrix $P \in \mathbb{F}^{p \times p}$ such that

$$P^T (A^T A)^{p-1} P = \text{diag}\{N^{(1)}, \ldots, N^{(h)}\},$$

[3] If the i-th column of an encoder of $\mathcal{C}$ is zero, the same happens for all equivalent encoders and, moreover, the i-th component of all codewords of $\mathcal{C}$ is also zero. Therefore to determine the decoupled encoders of $\mathcal{C}$ it is sufficient to consider the subcode of $\mathcal{C}$ constituted by its codewords without the i-th component, which encoders are the encoders of $\mathcal{C}$ without the i-th column.

where $N^{(i)} = \begin{bmatrix} 1 & \dots & 1 \end{bmatrix}^T \begin{bmatrix} 1 & \dots & 1 \end{bmatrix} \in \mathbb{F}^{p_i \times p_i}$, $i = 1, \dots, h$.

Step 4: Partitionate $P = [P_1 | \dots | P_h]$ where $P_i \in \mathbb{F}^{p \times p_i}$, $i = 1, \dots, h$ and define $\mathcal{P} := [GP_1 | GP_2 | \dots | GP_h]$.

Output: $\mathcal{P}$ and P.

Let $G(d)$ be an encoder of $\mathcal{C}$, $\mathcal{P} = [G_1(d) | \dots | G_h(d)]$, with $G_i(d) \in \mathbb{F}(d)^{m \times p_i}$, $i = 1, \dots, h$, be the partition of the columns of $G(d)$ obtained by applying Algorithm 1 and P be the corresponding permutation matrix. Then $[G_1(d) | \dots | G_h(d)] = G(d)P$ with

$$\mathbb{F}((d))^m = span\, G_1(d) \oplus \cdots \oplus span\, G_h(d).$$

Let also $[B_1(d) | \dots | B_h(d)]$ be an $m \times m$ nonsingular matrix such that $B_i(d) \in \mathbb{F}(d)^{m \times m_i}$ is a submatrix of $G_i(d)$, with $m_i = rank\, G_i(d)$, $i = 1, \dots, h$. Then

$$\bar{G}(d) := [B_1(d) | \dots | B_h(d)]^{-1} G(d) = \mathrm{diag}\{\bar{G}^{(1)}(d), \dots, \bar{G}^{(h)}(d)\} P^{-1} \qquad (5)$$

with $\bar{G}^{(i)}(d) \in \mathbb{F}(d)^{m_i \times p_i}$, $i = 1, \dots, h$. $\bar{G}(d)$ is a $(p_1, \dots, p_h)$-decoupled encoder of $\mathcal{C}$ which is *maximally-decoupled* since $[G_1(d) | \dots | G_h(d)]$ is the partition of the columns of $G(d)$ associated with the finest direct sum decomposition of $\mathbb{F}((d))^m$, which implies that the $[p_i, m_i]$-convolutional codes $\mathcal{C}^{(i)} = Im\, \bar{G}^{(i)}(d)$, $i = 1, \dots, h$, are undecomposable. Moreover, any other maximally-decoupled encoder of $\mathcal{C}$, $\tilde{G}(d)$, is such that $\tilde{G}(d)P = \mathrm{diag}\{\tilde{G}_1(d), \dots, \tilde{G}_h(d)\}$, with $\tilde{G}_i(d) \in \mathbb{F}(d)^{m_i \times p_i}$, $i = 1, \dots, h$.

Proposition 3.1 *If $\mathcal{C}$ admits a $(p_1, \dots, p_k)$-decoupled encoder associated with a permutation matrix P then it also admits a $(p_1, \dots, p_k)$-decoupled encoder associated with P which is canonical.*

The following result is immediate.

Corollary 3.1 *A convolutional code admits maximally-decoupled canonical encoders.*

4 Code decomposition in the analysis of a convolutional code

Let $\mathcal{C}$ be a $[p, m]$-convolutional code with free distance $d_{free}(\mathcal{C})$. Suppose that $\mathcal{C}$ can be decomposed into smaller codes, i.e., that admits a decoupled encoder

$$G(d) = \mathrm{diag}\{G^{(1)}(d), \dots, G^{(k)}(d)\} P,$$

with $k \geq 2$, $G^{(i)}(d) \in \mathbb{F}(d)^{m_i \times p_i}$, $i = 1, \dots, k$, $\sum_{i=1}^{k} m_i = m$, $\sum_{i=1}^{k} p_i = p$ and P a permutation matrix. Let $\mathcal{C}^{(i)}$ be the $[p_i, m_i]$-convolutional code generated by $G^{(i)}(d)$, $i = 1, \dots, k$. It is easy to see that [1]

$$d_{free}(\mathcal{C}) = \min_{1 \leq i \leq k} d_{free}(\mathcal{C}_i). \qquad (6)$$

So, if we have a code $\mathcal{C}$ which can be decomposed into smaller codes with different free distances, we obtain a better code just by considering the smaller subcode with better free distance. If all the subcodes have the same free distance but different rates, $\mathcal{C}$ will have rate smaller than the subcode with higher rate. Moreover, if $\mathcal{C}$ is an MDS-code, it can not be decomposable into smaller codes, as stated in the following proposition.

Proposition 4.1 *If $\mathcal{C}$ is an MDS-code then $\mathcal{C}$ is undecomposable.*

Proof: Assume by contradiction that $\mathcal{C}$ is an MDS-code that admits a (p_1, p_2)-decoupled encoder $G(d) \in \mathbb{F}(d)^{m\times p}$ for some positive integers p_1, p_2 such that $p_1 + p_2 = p$. Then $\mathcal{C}$ also admits a canonical (p_1, p_2)-decoupled encoder $G_c(d)$ such that

$$G_c(d)P = \begin{bmatrix} G^{(1)}(d) & 0 \\ 0 & G^{(2)}(d) \end{bmatrix},$$

for some permutation matrix P and $G^{(i)}(d) \in \mathbb{F}(d)^{m_i\times p_i}$, $i = 1, 2$, with $m_1 + m_2 = m$.

Let $\mathcal{C}^{(i)} = \text{Im } G^{(i)}(d)$ and represent $\nu_1 = \deg(\mathcal{C}^{(1)})$, $\nu_2 = \deg(\mathcal{C}^{(2)})$ and $\nu = \deg(\mathcal{C})$. Observe that $\nu_1 + \nu_2 = \nu$. Since $\mathcal{C}$ is an MDS-code,

$$d_{free}(\mathcal{C}) = (p - m)(\lfloor\frac{\nu}{m}\rfloor + 1) + \nu + 1.$$

Let us consider two cases: $\nu_2 m_1 \geq \nu_1 m_2$ and $\nu_2 m_1 < \nu_1 m_2$.

Case 1: $\nu_2 m_1 \geq \nu_1 m_2$. Since $p_1 + p_2 = p$, $m_1 + m_2 = m$ and $\nu_1 + \nu_2 = \nu$, we have that

$$d_{free}(\mathcal{C}) = (p_1 + p_2 - m_1 - m_2)(\lfloor\frac{\nu_1 + \nu_2}{m_1 + m_2}\rfloor + 1) + \nu_1 + \nu_2 + 1 =$$

$$= (p_1 - m_1)(\lfloor\frac{\nu_1}{m_1}\rfloor + 1) + \nu_1 + 1 + (p_1 - m_1)(\lfloor\frac{\nu_1 + \nu_2}{m_1 + m_2}\rfloor - \lfloor\frac{\nu_1}{m_1}\rfloor)+$$

$$+(p_2 - m_2)(\lfloor\frac{\nu_1 + \nu_2}{m_1 + m_2}\rfloor + 1) + \nu_2.$$

But $d_{free}(\mathcal{C}^{(1)}) \leq (p_1 - m_1)(\lfloor\frac{\nu_1}{m_1}\rfloor + 1) + \nu_1 + 1$ which implies that

$$d_{free}(\mathcal{C}) \geq d_{free}(\mathcal{C}^{(1)}) + (p_1 - m_1)(\lfloor\frac{\nu_1 + \nu_2}{m_1 + m_2}\rfloor - \lfloor\frac{\nu_1}{m_1}\rfloor)+$$

$$+(p_2 - m_2)(\lfloor\frac{\nu_1 + \nu_2}{m_1 + m_2}\rfloor + 1) + \nu_2$$

and therefore $d_{free}(\mathcal{C}) > d_{free}(\mathcal{C}^{(1)})$ since $(p_2 - m_2)(\lfloor\frac{\nu_1+\nu_2}{m_1+m_2}\rfloor + 1) + \nu_2 \geq 1$ which contradicts (6).

Case 2: $\nu_2 m_1 < \nu_1 m_2$. Proceeding the same way we conclude that $d_{free}(\mathcal{C}) > d_{free}(\mathcal{C}^{(2)})$ which also contradicts (6), and we conclude that $\mathcal{C}$ is undecomposable. □

Observe that the converse of the above lemma is not true as it is shown in the next example.

Example 4.1 *Consider the* $[4,2]$*-convolutional code* $\mathcal{C}$ *over the binary field such that*

$$G_c(d) = \begin{bmatrix} 1 & 0 & d & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

is a canonical encoder of $\mathcal{C}$*. We can easily see that* $\mathcal{C}$ *is an undecomposable code which is not an MDS-code since it has free distance* 2 *but the corresponding generalized Singleton bound is* 4*.*

A similar result to (6) holds for the column distances of a convolutional code that can be decomposed into smaller codes, as stated in the following proposition.

Proposition 4.2 *Let* $G(d)$ *be a* $(p_1, \ldots, p_k)$*-decoupled encoder of* $\mathcal{C}$ *associated with a permutation matrix* P*,*

$$G(d)P = \operatorname{diag}\{G^{(1)}(d), \ldots, G^{(k)}(d)\}, \;\; G^{(i)}(d) \in \mathbb{F}(d)^{m_i \times p_i},$$

and $\mathcal{C}^{(i)}$ *be the* $[p_i, m_i]$*-convolutional code generated by* $G^{(i)}(d)$*,* $i = 1, \ldots, k$*. Then* $d_j^c(\mathcal{C}) = min_{1 \le i \le k}\, d_j^c(\mathcal{C}^{(i)})$*.*

Proof: By Proposition 3.1 we can assume without loss of generality that $G(d)$ is canonical. Representing $G^{(i)}(d) = G_0^{(i)} + G_1^{(i)} d + \cdots + G_\nu^{(i)} d^\nu$, $G_r^{(i)} \in \mathbb{F}^{m_i \times p_i}$, $i = 1, \ldots, k$, $r = 0, \ldots, \nu$, we have that

$$G(d) = \operatorname{diag}\{G_0^{(1)}, \ldots, G_0^{(k)}\}P + \operatorname{diag}\{G_1^{(1)}, \ldots, G_1^{(k)}\}Pd +$$

$$+ \cdots + \operatorname{diag}\{G_\nu^{(1)}, \ldots, G_\nu^{(k)}\}Pd^\nu$$

and then for all $j \ge 0$ there exist permutation matrices P_1 and P_2 such that

$$\mathbf{M}_j^c(G(d)) = P_1 \operatorname{diag}\{\mathbf{M}_j^c(G^{(1)}(d)), \ldots, \mathbf{M}_j^c(G^{(k)}(d))\}\, P_2,$$

where P_1 is such that if $\mathbf{u}_n = [\mathbf{u}_n^{(1)} \ldots \mathbf{u}_n^{(k)}]$, $\mathbf{u}_n^{(i)} \in \mathbb{F}^{m_i}$, $i = 1, \ldots, k$, $n = 0, \ldots, j$, then

$$[\mathbf{u}_0 \; \cdots \; \mathbf{u}_j]P_1 = [\mathbf{u}_0^{(1)} \; \cdots \; \mathbf{u}_j^{(1)} | \cdots | \mathbf{u}_0^{(k)} \; \cdots \; \mathbf{u}_j^{(k)}].$$

Consequently, for $\mathbf{u}_n \in \mathbb{F}^m$, $n = 0, \ldots, j$,

$$[\mathbf{u}_0 \; \cdots \; \mathbf{u}_j]\mathbf{M}_j^c(G(d)) =$$

$$= [\mathbf{u}_0^{(1)} \; \cdots \; \mathbf{u}_j^{(1)} | \cdots | \mathbf{u}_0^{(k)} \; \cdots \; \mathbf{u}_j^{(k)}] \operatorname{diag}\{\mathbf{M}_j^c(G^{(1)}(d)), \ldots, \mathbf{M}_j^c(G^{(k)}(d))\}\, P_2,$$

which implies that $d_j^c(\mathcal{C}) = \min_{1 \le i \le k_j} d_j^c(\mathcal{C}^{(i)})$. □

Let $G_c(d) = G_0 + G_1 d + \cdots + G_\nu d^\nu$, with $G_i \in \mathbb{F}^{m \times p}$, $i = 1, \ldots, \nu$, be a canonical encoder of $\mathcal{C}$ and define

$$G_c(d)|_{[0,j]} = G_0 + G_1 d + \cdots + G_j d^j, \tag{7}$$

for $j = 0, 1, \ldots, \nu$. Since $G_c(d)$ is left prime, G_0 is full row rank and then so it is $G_c(d)|_{[0,j]},\ j = 0, 1, \ldots, \nu$. Therefore we can define $\mathcal{C}_{[j]}$ to be the $[p, m]$-convolutional code generated by $G_c(d)|_{[0,j]},\ j = 0, 1, \ldots, \nu$. It is immediate to see that

$$d_j^c(\mathcal{C}) = d_j^c(\mathcal{C}_{[j]}),\ j = 0, 1, \ldots, \nu.$$

Observe that if $G_c(d)$ and $\tilde{G}_c(d)$ are equivalent canonical encoders and $\mathcal{C}_{[j]}$ and $\tilde{\mathcal{C}}_{[j]}$ are the convolutional encoders generated by $G_c(d)|_{[0,j]}$ and $\tilde{G}_c(d)|_{[0,j]}$, respectively, it is not true that $\mathcal{C}_{[j]}$ and $\tilde{\mathcal{C}}_{[j]}$ are the same as it is shown in the following example.

Example 4.2 *Consider the* $[5, 3]$*-convolutional code* $\mathcal{C}$ *generated by the equivalent canonical encoders*

$$G_c(d) = \begin{bmatrix} 1 & 0 & d^2 & d^3 & 0 \\ 0 & d & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1+d \end{bmatrix}$$

and

$$\tilde{G}_c(d) = \begin{bmatrix} 1 & d^2 & d^2+d & d^3+d^2 & d^3+d^2 \\ 0 & d & 1 & 1 & 1+d \\ 0 & d & 1 & -1 & -1-d \end{bmatrix}$$

and let $j = 1$*. It is easy to see that the convolutional codes*

$$\mathcal{C}_{[1]} = Im\, G_c(d)|_{[0,1]} = Im \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & d & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1+d \end{bmatrix}$$

and

$$\tilde{\mathcal{C}}_{[1]} = Im\, \tilde{G}_c(d)|[0, 1] = Im \begin{bmatrix} 1 & 0 & d & 0 & 0 \\ 0 & d & 1 & 1 & 1+d \\ 0 & d & 1 & -1 & -1-d \end{bmatrix}$$

are distinct.

However, these codes $\mathcal{C}_{[j]}$ and $\tilde{\mathcal{C}}_{[j]}$ have similar properties of decoupling as stated in the following proposition.

Proposition 4.3 *Let* $G_c(d)$ *and* $\tilde{G}_c(d)$ *in* $\mathbb{F}[d]^{m\times p}$ *be equivalent canonical encoders of degree* ν *and let* $\mathcal{C}_{[j]}$ *and* $\tilde{\mathcal{C}}_{[j]}$ *be the convolutional codes generated by* $G_c(d)|_{[0,j]}$ *and* $\tilde{G}_c(d)|_{[0,j]}$*, respectively, for* $j = 0, 1, \ldots, \nu$*. Then if* $G_c(d)|_{[0,j]}P = \mathrm{diag}\{G^{(1)}(d), \ldots, G^{(k)}(d)\}$*,* $G^{(i)}(d) \in \mathbb{F}[d]^{m_i\times p_i}$*,* $i = 1, \ldots, k$*, with* $\sum_{i=1}^{k} m_i = m$*,* $\sum_{i=1}^{k} p_i = p$ *and* P *a permutation matrix, then* $\mathrm{diag}\{G^{(1)}(d), \ldots, G^{(k)}(d)\}P^{-1}$ *is also an encoder of* $\tilde{\mathcal{C}}_{[j]}$*.*

Proof: Since $G_c(d)$ and $\tilde{G}_c(d)$ are equivalent canonical encoders, there exists a unimodular matrix $U(d) \in \mathbb{F}[d]^{m\times p}$ such that $G_c(d) = U(d)\tilde{G}_c(d)$. Therefore $\bar{G}(d) := U(d)\tilde{G}_c(d)|_{[0,j]}$ is an encoder of $\tilde{\mathcal{C}}|_{[0,j]}$ such that $\bar{G}(d)|_{[0,j]}P = (U(d)\tilde{G}_c(d)|_{[0,j]})|_{[0,j]}P = (U(d)\tilde{G}_c(d))|_{[0,j]}P = G_c(d)|_{[0,j]}P = \mathrm{diag}\{G^{(1)}(d),\dots,G^{(k)}(d)\}$. □

Propositions 4.2 and 4.3 immediately imply the following result.

Corollary 4.1 *Let $\mathcal{C}$ be a $[p,m]$-convolutional code. If $d_j^c(\mathcal{C}) = (p-m)(j+1)+1$ for some $j \geq 0$ then $\mathcal{C}$ does not have a canonical encoder $G_c(d)$ such that $\mathcal{C}_{[j]} := Im\, G_c(d)|_{[0,j]}$ is decomposable into $k \geq 2$ smaller codes.*

5 Conclusions

We have showed that, similarly to the free distance, a convolutional code that can be decomposed into smaller codes has j-th column distance equal to the minimum of the j-th column distances of its subcodes. Moreover, a convolutional code $\mathcal{C}$ can be undecomposable and admit a canonical encoder $G_c(d)$ such that $G_c(d)_{[0,j]}$ is decoupled for some j (as in Example 4.2 where $\mathcal{C}$ is undecomposable and $G_c(d)|_{[0,1]}$ is a $(3,2)$-decoupled encoder). The j-th column distance of such code $\mathcal{C}$ is equal to the j-th column distance of $\mathcal{C}_{[j]} := Im\, G_c(d)_{[0,j]}$ which can be decomposed into smaller codes and, consequently, the j-th column distance of $\mathcal{C}$ is equal to the minimum of the j-th column distances of the subcodes of $\mathcal{C}_{[j]}$. A subject of future investigation is the study of these codes. Although they seem not to be the best codes in terms of their distances, they seem to present good performance in terms of decoding.

References

[1] J-J. Climent, V. Herrandez, C. Perea, *New convolutional codes from old convolutional codes, Electronic Proceedings of the 16th International Symposium on Mathematical Theory and Systems (MTNS2004)* (2004).

[2] E. Fornasini, R. Pinto, *Matrix fraction descriptions in convolutional coding, Linear Algebra and its Applications* (2004), 392, 119-158.

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

[4] H. Gluesing-Luerssen, J. Rosenthal, R. Smarandache, *Strongly-MDS convolutional codes, IEEE Trans. Inform. Theory* (2006) 52:2, 584-598.

[5] R. Johannesson, K. Zigangirov, *Fundamentals of convolutional coding, Piscataway. NJ: IEEE Press* (1999).

[6] J. Rosenthal, R. Smarandache, *Maximum distance separable convolutional codes, Applicable Algebra in Engineering, Communication and Computing* (1999), 10(1), 15-32.