# Computing Free Distances of Idempotent Convolutional Codes[1]

J. Gómez-Torrecillas[†], F. J. Lobillo[†] and G. Navarro[‡]

[†]Department of Algebra and CITIC, University of Granada

[‡]Department of Computer Sciences and AI, and CITIC, University of Granada

UNIVERSIDAD
DE GRANADA



ISSAC 2018, July 17th, 2018

[1]Supported by grant MTM2016-78364-P from Agencia Estatal de Investigación (AEI) of the Government of Spain and Fondo Europeo de Desarrollo Regional (FEDER) of the European Union.

# Index

# Index

# Several definitions

- $\mathbb{F}$ a finite field,
- $\mathbb{F}[z]$ polynomials in $z$ over $\mathbb{F}$,
- $\mathbb{F}(z)$ rational functions,
- $\mathbb{F}((z))$ Laurent series.

A rate $k/n$ convolutional code can be equivalently defined as

1. A $k$-dimensional vector subspace $\mathcal{C} \leq \mathbb{F}((z))^n$ generated by $G(z) \in \mathcal{M}_{k\times n}\left(\mathbb{F}(z)\right)$.
2. A $k$-dimensional vector subspace $\mathcal{C} \leq \mathbb{F}(z)^n$.
3. A rank $k$ direct summand $\mathcal{C} \leq_{\oplus} \mathbb{F}[z]^n$, i.e. a rank $k$ submodule $\mathcal{C} \leq \mathbb{F}[z]^n$ such that $\mathbb{F}[z]^n/\mathcal{C}$ is torsionfree.

Series and polynomials are interesting because they model information and transmitted sequences via the identifications

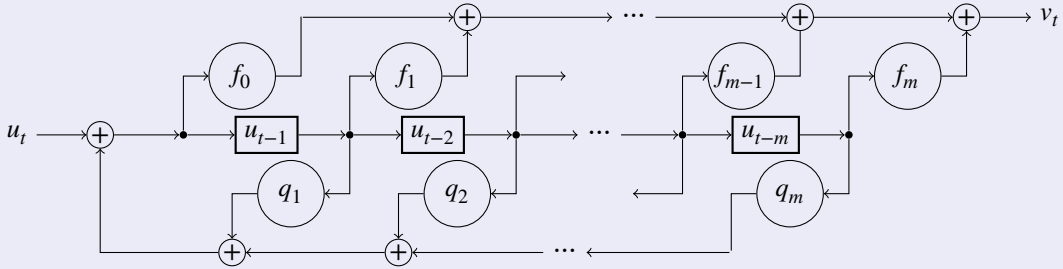
$$\mathbb{F}[z]^n \cong \mathbb{F}^n[z] \quad \mathbb{F}((z))^n \cong \mathbb{F}^n((z)).$$

# Rational transfer functions

Rational functions are interesting because multiplication by

$$\frac{f_0 + f_1 z + \cdots + f_m z^m}{1 + q_1 z + \cdots + q_m z^m} \in \mathbb{F}(z)$$

corresponds to the rational transfer function




For details, see

R. Johannesson and K. Sh. Zigangirov.
*Fundamentals of Convolutional Coding*.
Wiley-IEEE Press, 1999

# Rational functions and polynomials

## Proposition

*Let $k \leq n$. The map $\mathcal{D} \mapsto \mathcal{D} \cap \mathbb{F}^n[z]$ establishes a bijection between the set of $k$-dimensional vector subspaces of $\mathbb{F}(z)^n$ and the set of all $\mathbb{F}[z]$–submodules of $\mathbb{F}[z]^n$ of rank $k$ that are direct summands of $\mathbb{F}[z]^n$.*

This proposition is a module-theoretical and coordinate-free refinement of Theorem 3 in

G. D. Forney Jr.
Convolutional codes I: Algebraic structure.
IEEE Transactions on Information Theory 16(6), 720–738, (1970).

From now on, a rate $k/n$ convolutional code $\mathcal{C}$ is a rank $k$ direct summand of $\mathbb{F}^n[z]$. We also identify

$$\mathcal{M}_{k\times n}\left(\mathbb{F}[z]\right) \cong \mathcal{M}_{k\times n}\left(\mathbb{F}\right)[z].$$

to work with generator (and parity check) matrices.

# Index

# Hamming weight and free distance

The Hamming weight $\mathrm{w} : \mathbb{F}^n \to \mathbb{N}$ is defined as

$$\mathrm{w}(v_0 \cdots v_{n-1}) = |\{i \mid v_i \neq 0\}|.$$

It is a very important parameter for linear block codes (a.k.a. vector subspaces of $\mathbb{F}^n$) because its measures the detection and correction capability of the code.

The Hamming weight can be canonically extended to

$$\begin{aligned} \mathrm{w} : \mathbb{F}^n[z] &\to \mathbb{N} \\ \textstyle\sum_i z^i f_i &\mapsto \textstyle\sum_i \mathrm{w}(f_i). \end{aligned}$$

The free distance is defined as

$$\begin{aligned} \mathrm{d}_{\mathsf{free}}(\mathcal{C}) &= \min\{\mathrm{w}(f) \mid f \in \mathcal{C}, f \neq 0\} \\ &= \min\left\{\mathrm{w}(f) \mid f = \textstyle\sum_i z^i f_i \in \mathcal{C}, f_0 \neq 0\right\} \end{aligned}$$

# Classical row and column distances

Introduced by Costello in 1969.

For each $f = \sum_i z^i f_i$, we denote

$$f_{[0,j]} = \sum_{i=0}^{j} z^i f_i.$$

The $j$th column distance of $\mathcal{C}$ is defined as

$$d_j^c = \min\left\{\mathrm{w}(f_{[0,j]}) \mid f \in \mathcal{C}, f_0 \neq 0\right\}.$$

As observed in the proof of [Johannesson and Zigangirov'99, Theorem 3.1], this definition matches with the column distance defined there of any (rational) generator matrix $G$ of $\mathcal{C}$ such that $G(0)$ has full rank (e.g. when $G$ is a basic generator matrix).

The $j$th row distance of $\mathcal{C}$ with respect to a basic generator matrix $G = \sum_{i=0}^{m} z^i G_i$, of degree $m$ is defined as

$$d_j^r = \min\left\{\mathrm{w}(f) \mid f \in \mathcal{C}, f \neq 0, \deg(f) \leq j + m\right\}.$$

This definition depends on the degree $m$ of $G$ as a polynomial in $z$ with matrix coefficients. See [Johannesson and Zigangirov'99, p. 114] for more details.

# Computing the free distance I

**Theorem ([Johannesson and Zigangirov'99, Ch. 3])**

*For every index j,*

$$d_j^c \leq d_{j+1}^c \leq \mathrm{d}_{free}(C) \leq d_{j+1}^r \leq d_j^r,$$

*and* $d_s^c = \mathrm{d}_{free}(C) = d_s^r$ *for s big enough.*

The degree $m$ of $G$ should play some role in row and column distance sequences. In fact, each vector in the information sequence interacts only with the $m+1$ coefficients of $G$. This leads to the following natural question:

*Does the equality* $d_j^c = d_{j+m}^c$ *for some* $j \geq 0$ *imply* $d_j^c = \mathrm{d}_{free}(C)$*?*

# Computing the free distance II

## Example

Let $\mathcal{C}$ be the rate $2/4$ code generated by the basic matrix

$$G = \begin{pmatrix} z^4+z^2+1 & z^3+z^2+z+1 & z^4+z^3 & z^3+z^2+z \\ z^4+z^3+1 & z^3 & z^3+z+1 & 1 \end{pmatrix}.$$

With the aid of the computer software SageMath, we have computed the column distances, whose values are written in the following table:

| $j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $d_j^c$ | 2 | 3 | 4 | 5 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 7 |

So $d_5^c = d_{10}^c = 6$, but $\mathrm{d_{free}}(\mathcal{C}) \geq 7$. Actually, $\mathrm{d_{free}}(\mathcal{C}) = 8$.

# Index

# Naive approach and $\sigma$-cyclicity

## Proposition ([Piret'76])

*An ideal* $\mathcal{C} \subseteq \mathbb{F}^n[z] \cong \frac{\mathbb{F}[x]}{\langle x^n-1\rangle}[z]$ *that it is a direct summand* $\mathbb{F}[z]$*–submodule is generated by vectors in* $\mathbb{F}^n$*. Thus, Naive Cyclic Convolutional Codes are Block Codes.*

Cyclic structures over convolutional codes $\rightsquigarrow$ non commutative structures on $\mathbb{F}^n[z]$, that is, $\mathbb{F}^n[z] \cong \frac{\mathbb{F}[x]}{\langle x^n-1\rangle}[z;\sigma]$ [Piret'76, Roos'79, Gluesing and Schmale'04]



P. Piret.
Structure and constructions of cyclic convolutional codes.
*IEEE Trans. Inform. Theory*, 22 (1976).


C. Roos.
On the Structure of Convolutional and Cyclic Convolutional Codes.
*IEEE Trans. Inform. Theory*, 25 (1979).


H. Gluesing-Luerssen and W. Schmale.
On cyclic convolutional codes.
*Acta Appl. Math.*, 82 (2004).

# Ideal Codes

For each ring $A$, the Ore extension $A[z;\sigma]$ is the free right $A$–module with basis the powers of $z$ and multiplication defined by the rule $az = z\sigma(a)$ for all $a \in R$, where $\sigma$ is a ring endomorphism of $A$.

Let $A$ be a finite (dimensional) algebra of dimension $n$ over the finite field $\mathbb{F}$. Each $\mathbb{F}$–basis $\mathcal{B} = \{b_0, b_1, \ldots, b_{n-1}\}$ of $A$ becomes an $\mathbb{F}[z]$-basis of the left $\mathbb{F}[z]$–module $A[z;\sigma]$, and thus it provides an isomorphism of $\mathbb{F}[z]$–modules $\mathfrak{v} : A[z;\sigma] \to \mathbb{F}^n[z]$.

## Definition

An ideal code is a left ideal $I \leq A[z;\sigma]$ such that $\mathfrak{v}(I)$ is a direct summand of $\mathbb{F}^n[z]$. See

S. R. López-Permouth and S. Szabo.
Convolutional codes with additional algebraic structure.
*J. Pure Appl. Algebra*, 217 (2013).

We call $A$ is the word–ambient of the convolutional code, while $A[z;\sigma]$ is the sentence–ambient.

# Idemponent Convolutional Codes I

## Definition

Let $R = A[z;\sigma]$, and fix a basis $\mathcal{B}$ of $A$ over $\mathbb{F}$. A convolutional code $\mathcal{C} \subseteq \mathbb{F}^n[z]$ is said to be an idempotent convolutional code (ICC) if $\mathfrak{b}^{-1}(\mathcal{C})$ is a direct summand as left ideal of $R$, i.e. there exists an idempotent $\epsilon = \epsilon^2 \in R$ such that $\mathfrak{b}^{-1}(\mathcal{C}) = R\epsilon$. By a slight abuse of language, we will simply say that $\mathcal{C}$ is generated by $\epsilon$, and we write $\mathcal{C} = R\epsilon$.

- The isomorphism $\mathfrak{b} : A \to \mathbb{F}^n$ associated to $\mathcal{B}$ allows the extension of the weight from $\mathbb{F}^n$ to $A$, i.e. $\mathrm{w}(a) = \mathrm{w}(\mathfrak{b}(a))$ for all $a \in A$.
- This weight is therefore canonically extended to $A[z;\sigma]$.
- $\sigma$ is called isometry if $\mathrm{w}(\sigma(a)) = \mathrm{w}(a)$ for all $a \in A$.

Examples, as well as algorithms for their construction, of idempotent convolutional codes can be seen in

J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Generating idempotents in ideal codes,
ACM Communications in Computer Algebra, Vol 48, No. 3, Issue 189, September 2014, ISSAC poster abstracts, pp. 113-115.

# Idemponent Convolutional Codes II



J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Separable automorphisms on matrix algebras over finite field extensions: Applications to ideal codes.
In: Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation (ISSAC'15), Bath, UK.
ACM, New York, NY, USA, pp. 189–195.


J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Convolutional codes with a matrix-algebra word-ambient,
Advances in Mathematics of Communications, 10 (2016), 29-43


J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Computing separability elements for the sentence ambient algebra of split ideal codes,
Journal of Symbolic Computation, 83 (2017), 211–227.


J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Ideal codes over separable ring extensions,
IEEE Transactions on Information Theory 63 (5) (2017), 2796–2813.

# Parity check idempotent

Let $C = R\epsilon$ an ICC generated by an idempotent $\epsilon \neq 0, 1$ of $R$. Let $m$ be the degree of $\epsilon$ in $z$. Write

$$e = 1 - \epsilon = \sum_{i=0}^{m} z^i e_i,$$

which is also a non trivial idempotent of degree $m$ of $R$. Then

$$C = \mathrm{Ann}_R^{\ell}(e) = \{g \in R : ge = 0\}.$$

The idempotent $\epsilon$ is called an *idempotent generator* of $C = R\epsilon$, and $e = 1 - \epsilon$ is called a *parity check idempotent.*

# Associated idempotent matrices

Consider the following infinite matrix with coefficients in $A$:

$$E = \begin{pmatrix} e_0 & \sigma^{-1}(e_1) & \sigma^{-2}(e_2) & \cdots & \cdots & \cdots \\ & \sigma^{-1}(e_0) & \sigma^{-2}(e_1) & \sigma^{-3}(e_2) & \cdots & \cdots \\ & & \sigma^{-2}(e_0) & \sigma^{-3}(e_1) & \sigma^{-4}(e_2) & \cdots \\ & & & \ddots & \ddots & \ddots \end{pmatrix} = \left(\sigma^{-j}(e_{j-i})\right)_{0\leq i, 0\leq j}.$$

Let $E_l^c$ be the square submatrix of $E$ consisting in the first $l+1$ rows and columns, that is

$$E_l^c = \left(\sigma^{-j}(e_{j-i})\right)_{0\leq i,j\leq l}.$$

$E$, and consequently $E_l^c$, is an idempotent matrix.

# Cyclic column distances

## Definition

Let $l \geq 0$. The $l$th cyclic column distance of $\mathcal{C} = \mathrm{Ann}_R^{\ell}(e)$ is defined as

$$\delta_l^c = \mathrm{d}(K_l) = \min\{\mathrm{w}(a_0, \ldots, a_l) : (a_0, \ldots, a_l) \in K_l\},$$

where

$$K_l = \{(a_0, \ldots, a_l) \in \ker(\cdot E_l^c) : a_0 \neq 0\} \subseteq A^{l+1}.$$

# Main theorem

## Theorem

*For all $l \geq 0$, $\delta_l^c \leq \delta_{l+1}^c$. Moreover, if $\sigma$ is an isometry, then $\delta_l^c \leq \mathrm{d}_{\mathsf{free}}(C)$. If, in addition, $\delta_j^c = \delta_{j+m}^c$ for some $j$, then $\delta_j^c = \mathrm{d}_{\mathsf{free}}(C)$.*

## Some ideas of the proof

- The equality

$$E_{l+j}^c = \left(\begin{array}{c|c} E_l^c & \diagup \\ \hline 0 & \diagdown \end{array}\right),$$

  implies that if $(f_0, \ldots, f_l, f_{l+1}, \ldots, f_{l+j}) \in K_{l+j}$ then $(f_0, \ldots, f_l) \in K_l$. Hence $\delta_l^c \leq \delta_{l+j}^c$.
- The equality $\delta_l^c = \delta_{l+j}^c$ implies that both cyclic distances are reached in $(f_0, \ldots, f_l) \in K_l$ such that $(f_0, \ldots, f_l, 0, \ldots 0) \in K_{l+j}$.
- Finally, if $j = m$, we find an element in $\mathcal{C}$ with the same weight that $(f_0, \ldots, f_l)$. Therefore the free distance is reached.

# Index

# Framework

Each term $\delta_l^c$ of the cyclic column distances sequence is the minimum weight of $K_l \subseteq A^{l+1}$, which is of the form

$$K_l = N_l \setminus P_l,$$

where

$$N_l = \ker(\cdot E_l^c) \text{ and } P_l = \{(a_0, a_1, \dots, a_l) \in N_l : a_0 = 0\}.$$

Up to taking coordinates, our problem restricts to compute

$$\mathrm{d}(W \setminus V) = \min\{\mathrm{w}(v) \mid v \in W \setminus V\}$$

where $V \subseteq W \subseteq \mathbb{F}^s$.

# Brouwer–Zimmermann algorithm. I

We have developed an idea provided by Prof. A. Wassermann to us. Let $k = \dim W$ and $r = \dim V$. Without loss of generality we can assume that $W$ is generated by the rows of a matrix

$$G = \left( \frac{G_1}{G_2} \right)$$

where $G_1 \in \mathcal{M}_{(k-r)\times s}\left(\mathbb{F}\right)$, $G_2 \in \mathcal{M}_{r\times s}\left(\mathbb{F}\right)$ and the rows of $G_2$ generate $V$. Hence

$$W \setminus V = \{vG \mid v_{[0,k-r-1]} \neq 0\}.$$

We may apply the first part of the Brouwer-Zimmermann algorithm, as presented in

A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann.
*Error-Correcting Linear Codes*.
Algorithms and Computation in Mathematics, Vol. 18. Springer, 2006.

# Brouwer–Zimmermann algorithm. II

We thus obtain $t$ matrices $\Gamma_j$ such that $\Gamma_j = A_j G$, where $A_j$ is a $k \times k$ non-singular matrix, for any $j = 1, \ldots, t$. The matrix $\Gamma_j$ has the form

$$\Gamma_j = \left( \begin{array}{c|c|c} & I_{k_j} & L'_j \\ L_j & \hline 0 & 0 \end{array} \right),$$

and the columns where the identity matrix is placed are disjoint for any other matrix $\Gamma_d$ with $d \neq j$. In particular, the maximum Hamming weight for a vector in $W$ is $\sum_{j=1}^{t} k_j$.
Define the subsets

$$C_i = \{v\Gamma_j \in W \setminus V : \mathrm{w}(v) \leq i\} = \{v\Gamma_j \in W : \mathrm{w}(v) \leq i \text{ and } (vA_j)_{[0,k-r-1]} \neq 0\}.$$

Let $\overline{d}_i = \mathrm{d}(C_i)$. Hence,

$$C_1 \subseteq C_2 \subseteq \cdots \subseteq C_{k-1} \subseteq C_k = W \setminus V \quad \text{and} \quad \overline{d}_1 \geq \overline{d}_2 \geq \cdots \geq \overline{d}_{k-1} \geq \overline{d}_k = \mathrm{d}(W \setminus V).$$

Let $\underline{d}_i = \sum_{j=1}^{t}(i+1) - (k - k_j)$. Hence $\underline{d}_i < \underline{d}_{i+1}$. As in the linear Brouwer-Zimmermann algorithm, it can be shown that there exists a minimal $j_0$ such that

$$\overline{d}_{j_0} \leq \underline{d}_{j_0},$$

and thus $\mathrm{d}(W \setminus V) = \overline{d}_{j_0}$.

# Example

Let $\mathbb{F} = \mathbb{F}_2$ and $A = \mathbb{F}[x]/\langle x^7 - 1\rangle$. Let $\sigma : A \to A$ defined by $\sigma(x) = x^3$. It is easy to check that $\sigma$ is indeed an algebra map, with inverse $\sigma^{-1}(x) = x^5$. Let $R = A[z; \sigma]$,

$$\epsilon = z^5\left(x^4 + x^3 + x^2 + 1\right) + z\left(x^5 + x^2 + x + 1\right) + x^4 + x^2 + x + 1$$

and

$$e = 1 - \epsilon = z^5\left(x^4 + x^3 + x^2 + 1\right) + z\left(x^5 + x^2 + x + 1\right) + x^4 + x^2 + x,$$

which are the idempotent generator and the parity check idempotent of the ICC $\mathcal{C} = R\epsilon$. We have applied our methods getting the following sequence of cyclic distances:

| $j$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\delta_j^c$ | 4 | 6 | 8 | 8 | 8 | 10 | 12 | 12 | 12 | 12 | 12 | 12 |

Hence $\mathrm{d}_{\mathsf{free}}(\mathcal{C}) = \delta_6^c = \delta_{11}^c = 12$.

# Thank you!

questions?