Separable Automorphisms on Matrix Algebras over Finite Field Extensions. Applications to Ideal Codes.[1]

J. Gómez-Torrecillas *, F. J. Lobillo * and G. Navarro ♯

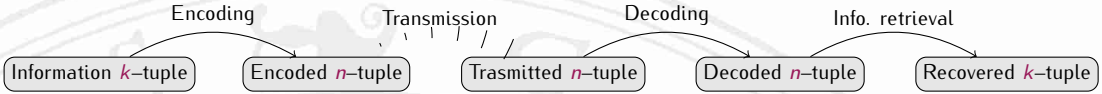
*Department of Algebra and CITIC, University of Granada

♯Dep. of Computer Sciences and AI, and CITIC, University of Granada

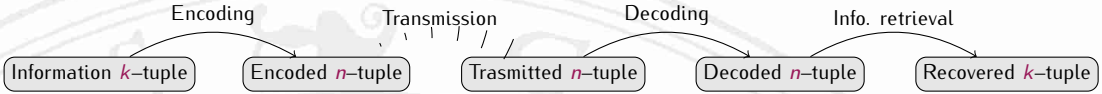
ISSAC 2015, July 9th, 2015

[1]Research partially supported by grants MTM2013-41992-P and TIN2013-41990-R from Ministerio de Economía y Competitividad of the Spanish Government and from FEDER

An extremely short overview of coding theory



An extremely short overview of coding theory

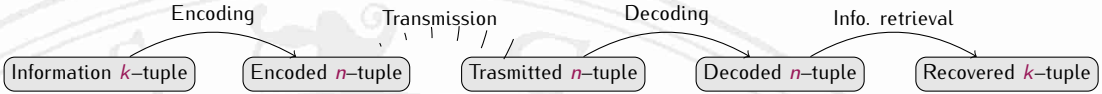


Block (linear) codes

The encoding process is provided by a linear map, i.e. there is a right invertible matrix $G \in \mathcal{M}_{k\times n}(\mathbb{F})$ such that the encoding is $v_t = u_t G \in \mathbb{F}^n$ for each information word $u_t \in \mathbb{F}^k$.

Additional algebraic structure improves encoding and decoding, $\mathbb{F}^n \cong \mathbb{F}[x]/\langle x^n - 1\rangle$, e.g. Reed-Solomon codes.

An extremely short overview of coding theory

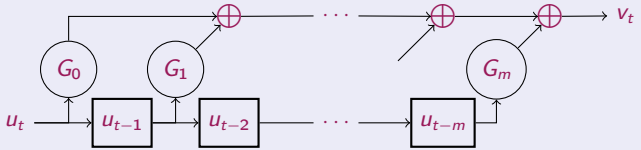


Block (linear) codes

The encoding process is provided by a linear map, i.e. there is a right invertible matrix $G \in \mathcal{M}_{k\times n}(\mathbb{F})$ such that the encoding is $v_t = u_t G \in \mathbb{F}^n$ for each information word $u_t \in \mathbb{F}^k$.

Additional algebraic structure improves encoding and decoding, $\mathbb{F}^n \cong \mathbb{F}[x]/\langle x^n - 1\rangle$, e.g. Reed-Solomon codes.

Convolutional codes



Convolutional codes and cyclicity

Cyclicity in convolutional codes $\rightsquigarrow$ non commutative structures on $\mathbb{F}[z]^n$.
[Piret'76, Gluesing and Schmale'04, Lopez-Permouth and Szabo'13, GLN'14b]

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

Let A be a finite semisimple algebra of dimension n over a finite field $\mathbb{F}$. Each $\mathbb{F}$–basis $\mathcal{B}$ of A induces a natural isomorphism of $\mathbb{F}[z]$–modules $\mathfrak{v} : A[z;\sigma,\delta] \to \mathbb{F}[z]^n$. A is the word–ambient of the convolutional code, while $A[z;\sigma,\delta]$ is the sentence–ambient.

Definition 1 ([Lopez-Permouth and Szabo'13])

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

We focus ourselves in the case $\delta = 0$, i.e. skew polynomials.

Two questions about ideal codes

Are ideal codes direct summands as left ideals?

- A positive answer is shown in [GLN'14b, GLN ISSAC'14 Poster] if $\mathbb{F}[z] \subseteq A[z;\sigma]$ is a separable ring extension.
- This answer generalizes previous works [Gluesing and Schmale'04] when the word–ambient is a commutative semisimple $\mathbb{F}$–algebra, and [Lopez-Permouth and Szabo'13] whenever it is a separable group algebra of a finite group over a $\mathbb{F}$.

Two questions about ideal codes

Are ideal codes direct summands as left ideals?

- A positive answer is shown in [GLN'14b, GLN ISSAC'14 Poster] if $\mathbb{F}[z] \subseteq A[z;\sigma]$ is a separable ring extension.
- This answer generalizes previous works [Gluesing and Schmale'04] when the word–ambient is a commutative semisimple $\mathbb{F}$–algebra, and [Lopez-Permouth and Szabo'13] whenever it is a separable group algebra of a finite group over a $\mathbb{F}$.

Can we compute a generator for an ideal code?

- In general it is not known if ideal codes are even principal.
- If the ideal code is a direct summand as left ideal, which we call a *split ideal code*, then it is principal and generated by an idempotent.
- This generator can be effectively computed under the separability conditions, see [GLN'14b, Algorithm 1] and [GLN ISSAC'14 Poster, Algorithm 1]

Separable extensions

Definition 2

A non commutative ring extension $S \subseteq R$ is called separable if the multiplication map

$$\begin{aligned} \mu : R \otimes_S R &\longrightarrow R \\ \textstyle\sum_i a_i \otimes b_i &\longmapsto \textstyle\sum_i a_i b_i \end{aligned}$$

splits, or equivalently if there exists

$$p = \sum_i a_i \otimes b_i \in R \otimes_S R$$

such that

$$\mu(p) = \sum_i a_i b_i = 1 \text{ and } \forall r \in R,\ rp = pr.$$

This element is called a *separability element*.

Proposition 3 ([Hirata and Sugano'66])

In a separable extension, R–submodules which are S–direct summands are also R–direct summands.

Separability and skew polynomials

- A is a separable $\mathbb{F}$–algebra and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$,
- $\sigma^{\otimes} : A \otimes_{\mathbb{F}} A \to A \otimes_{\mathbb{F}} A$ is defined by $\sigma^{\otimes}(a \otimes b) = \sigma(a) \otimes \sigma(b)$.

Corollary 4

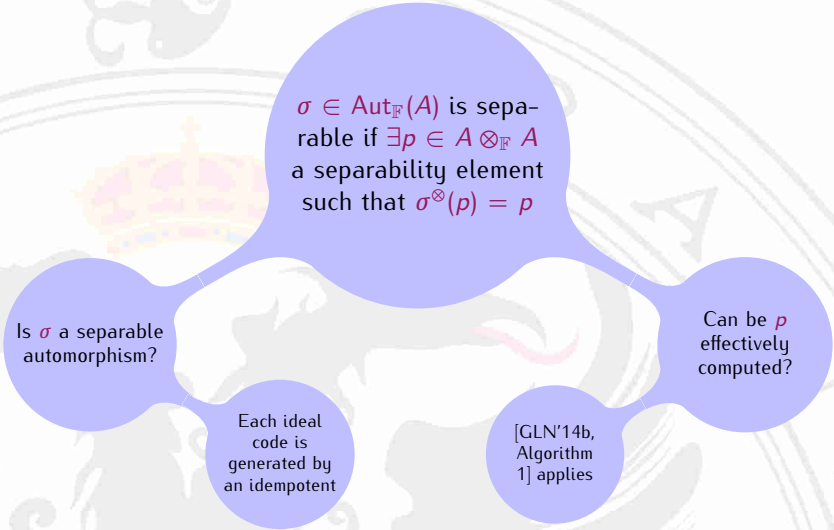
Let $\mathbb{F}$ be a finite field and let A be a separable $\mathbb{F}$–algebra with separability element $p = \sum_i a_i \otimes_{\mathbb{F}} b_i \in A \otimes_{\mathbb{F}} A$. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ such that $\sigma^{\otimes}(p) = p$. Then $\mathbb{F}[z] \subseteq A[z;\sigma]$ is a separable extension and a separability element is given by

$$\overline{p} = \sum_i a_i \otimes_{\mathbb{F}[z]} b_i \in A[z;\sigma] \otimes_{\mathbb{F}[z]} A[z;\sigma].$$

In particular each ideal code is a split ideal code and it is generated by an idempotent.

This corollary follows from [GLN'14b, Theorem 6].

Computational problems



Framework and target

- $\mathbb{F} \subseteq \mathbb{K}$ is a finite fields extension with dual normal bases $\{\alpha^{q^0}, \ldots, \alpha^{q^{t-1}}\}$ and $\{\beta^{q^0}, \ldots, \beta^{q^{t-1}}\}$.
- Word–ambient is $A = \mathcal{M}_n(\mathbb{K})$.
- The center of an A–bimodule M is $M^A = \{m \in M \mid rm = mr \ \forall r \in A\}$.

The desired $p \in A \otimes_{\mathbb{F}} A$ must satisfy

(P1) $p \in (A \otimes_{\mathbb{F}} A)^A$

(P2) $p \in E_1 = \left\{ \sum_i a_i \otimes b_i \in (A \otimes_{\mathbb{F}} A)^A \mid \sum_i a_i b_1 = 1 \right\}$

(P3) $p \in \ker(Id_{A \otimes_{\mathbb{F}} A} - \sigma^{\otimes})$

(P1) $(A \otimes_{\mathbb{F}} A)^A$

For each $0 \leq i,j \leq n-1$ and all $0 \leq k \leq t-1$, we denote

$$p_{ijk} = \sum_{l=0}^{n-1} \sum_{h=0}^{t-1} E_{li} \alpha^{q^k} \alpha^{q^h} \otimes \beta^{q^h} E_{jl} \in A \otimes_{\mathbb{F}} A.$$

Lemma 5

The dimension of $(A \otimes_{\mathbb{F}} A)^A$ as an $\mathbb{F}$–vector space is $n^2 t$. An $\mathbb{F}$–basis for $(A \otimes_{\mathbb{F}} A)^A$ is $\{p_{ijk} \mid 0 \leq i,j \leq n-1, 0 \leq k \leq t-1\}$.

(P2) $E_1 = \left\{ \sum_i a_i \otimes b_i \in (A \otimes_{\mathbb{F}} A)^A \mid \sum_i a_i b_1 = 1 \right\}$

Let

$$E_0 = \{p \in (A \otimes_{\mathbb{F}} A)^A \mid \mu(p) = 0\}$$

and

$$E_1 = \{p \in (A \otimes_{\mathbb{F}} A)^A \mid \mu(p) = 1\}.$$

Then E_1 is the set of all separability elements of the extension $\mathbb{F} \subseteq A$. Let $p_1 = \sum_{k=0}^{t-1} \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\beta) p_{00k}$.

Proposition 6

E_0 is an $\mathbb{F}$–vector subspace of $(A \otimes_{\mathbb{F}} A)^A$ and E_1 is an affine subspace of $(A \otimes_{\mathbb{F}} A)^A$ both of dimension $(n^2-1)t$. An $\mathbb{F}$–basis of E_0 is

$$\mathcal{E} = \{p_{ijk} \mid 0 \leq i \neq j \leq n-1, 0 \leq k \leq t-1\} \cup \{p_{00k} - p_{iik} \mid 1 \leq i \leq n-1, 0 \leq k \leq t-1\}.$$

Moreover $E_1 = \{p_1 + q \mid q \in E_0\}$.

(P3) $\ker(Id_{A\otimes_{\mathbb{F}} A} - \sigma^{\otimes})$ I

Recall

$$E_0 = \{p \in (A \otimes_{\mathbb{F}} A)^A \mid \mu(p) = 0\}$$

and

$$E_1 = \{p \in (A \otimes_{\mathbb{F}} A)^A \mid \mu(p) = 1\}.$$

Linearizing the problem

$$\exists p \in E_1 \cap \ker(Id_{A\otimes_{\mathbb{F}} A} - \sigma^{\otimes})$$

$$\Updownarrow$$

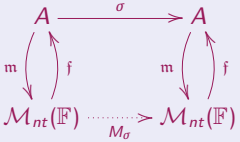
$$\exists q \in E_0 \mid \sigma^{\otimes}(p_1 + q) = p_1 + q$$

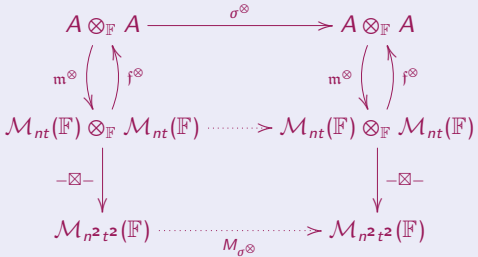
$$\Updownarrow$$

$$(\sigma^{\otimes} - Id_{A\otimes_{\mathbb{F}} A})(p_1) \in (Id_{A\otimes_{\mathbb{F}} A} - \sigma^{\otimes})(E_0)$$

(P3) $\ker(Id_{A\otimes_{\mathbb{F}} A} - \sigma^{\otimes})$ II

Converting to matrices





Example I

- The field extension is $\mathbb{F} = \mathbb{F}_2 \subset \mathbb{F}_4 = \mathbb{K}$.
- The base algebra is $A = \mathcal{M}_2(\mathbb{K})$.
- We fix the normal basis $\mathcal{B} = \{a, a^2\}$, which is also self-dual.
- Two canonical inclusions, $A \to \mathcal{M}_4(\mathbb{F})$ and $A \otimes_{\mathbb{F}} A \to \mathcal{M}_{16}(\mathbb{F})$
- The basis $\{p_{ijk}\}$ of $A \otimes_{\mathbb{F}} A^A$ can now be constructed. For example

$$p_{001} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a^2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix},$$

and via the canonical inclusion

$$p_{001} = \begin{pmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

Example II

- The basis of E_0 is

$$\mathcal{E} = \{p_{010}, p_{011}, p_{100}, p_{101}, p_{000} + p_{110}, p_{001} + p_{111}\}$$

and $E_1 = p_1 + E_0$ where

$$p_1 = p_{000} + p_{001} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

- The automorphism is $\sigma = \sigma_U \widehat{\tau}$, where $U = \begin{pmatrix} 1 & a \\ a^2 & a \end{pmatrix}$ and τ is the Frobenius automorphism.

Example III

- The matrix M_σ is

$$M_\sigma = \begin{pmatrix}
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1
\end{pmatrix},$$

  and the matrix $M_{\sigma^\otimes}$ has size 256×256.

- In order to check if $(\sigma^\otimes - \mathrm{id})(p_1) \in (\mathrm{id} - \sigma^\otimes)(E_0)$, we had to solve the non homogeneous linear system of size 256×6

$$\mathfrak{v}(p_1) \cdot (M_{\sigma^\otimes} - I_{256}) = \sum_{0 \le i \ne j \le 1} \sum_{0 \le k \le 1} \alpha_{ijk} \left(\mathfrak{v}(p_{ijk}) \cdot (I_{256} - M_{\sigma^\otimes}) \right) + \sum_{0 \le i \le 1} \sum_{0 \le k \le 1} \alpha_{ik} \left(\mathfrak{v}(p_{00k} - p_{iik}) \cdot (I_{256} - M_{\sigma^\otimes}) \right)$$

  whose solution is $(0, 0, 1, 0, 1, 0)$.

Example IV

- The desired separability element is $p = p_1 + p_{100} + p_{000} + p_{110} = p_{100} + p_{110} + p_{001}$. Concretely,

$$p = \begin{pmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0
\end{pmatrix},$$

Viewed as a tensor product of matrices in $\mathcal{M}_2(\mathbb{K})$,

$$\begin{aligned}
p = &\begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a^2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a^2 \end{pmatrix} \otimes \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix} \\
&+ \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ a^2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a^2 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & a^2 \end{pmatrix} \\
&+ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} a^2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & a^2 \\ 0 & 0 \end{pmatrix}.
\end{aligned}$$

Summary, conclusions, further work...

Summary and conclusions.

- This paper concerns about convolutional codes with word–ambient matrices over a finite field extension of the symbol–ambient finite field.
- We have presented a complete computational answer to decide if a given automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ is separable, computing a suitable separability element.
- If the answer in positive, the separability element can be used to compute an idempotent generator of any ideal code.
- This idempotent allows an easy parity check of transmitted sentences.

Summary, conclusions, further work...

Summary and conclusions.

- This paper concerns about convolutional codes with word–ambient matrices over a finite field extension of the symbol–ambient finite field.
- We have presented a complete computational answer to decide if a given automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ is separable, computing a suitable separability element.
- If the answer in positive, the separability element can be used to compute an idempotent generator of any ideal code.
- This idempotent allows an easy parity check of transmitted sentences.

Improvements not explained here and further work.

- We have also proved that $\mathbb{F}[z] \subseteq A[z;\sigma]$ is a separable extension if and only if σ is a separable automorphism.
- From the idempotent generator, the dual code can be easily computed if it is also an ideal code over the same word–ambient. This has been also completed.
- Distance profiles of these codes have to be computed.

Selected bibliography


H. Gluesing-Luerssen and W. Schmale.
On cyclic convolutional codes.
Acta Applicandae Mathematica, 82(2):183–237, 2004.


J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Generating idempotents in ideal codes.
In W.-S. Lee, editor, *ISSAC 2014 Poster Abstract*, volume 48, number 3, issue 189 of *ACM Communications in Computer Algebra*. ACM-SIGSAM, 2014.


J. Gómez-Torrecillas, F. J. Lobillo, and G. Navarro.
Ideal codes over separable ring extensions.
`arXiv:1408.1546`, 2014.


K. Hirata and K. Sugano.
On semisimple extensions and separable extensions over non commutative rings.
Journal of the Mathematical Society of Japan, 18(4):360–373, 10 1966.


S. R. López-Permouth and S. Szabo.
Convolutional codes with additional algebraic structure.
Journal of Pure and Applied Algebra, 217(5):958 – 972, 2013.


P. Piret.
Structure and constructions of cyclic convolutional codes.
IEEE Transactions on Information Theory, 22(2):147–155, 1976.