CONVOLUTIONAL CODES WITH A MATRIX-ALGEBRA
WORD-AMBIENT

José Gómez-Torrecillas and F. J. Lobillo
Department of Algebra and CITIC
Universidad de Granada
E18071 Granada, Spain

Gabriel Navarro
Department of Computer Sciences and AI, and CITIC
Universidad de Granada
E51001 Ceuta, Spain

(Communicated by Paolo Vettori)

Abstract. Let $M_n(F)$ be the algebra of $n \times n$ matrices over the finite field $F$. In this paper we prove that the dual code of each ideal convolutional code in the skew-polynomial ring $M_n(F)[z;\sigma_U]$ which is a direct summand as a left ideal, is also an ideal convolutional code over $M_n(F)[z;\sigma_U^T]$ and a direct summand as a left ideal. Moreover we provide an algorithm to decide if $\sigma_U$ is a separable automorphism and returns the corresponding separability element, when pertinent.

1. Introduction and algebraic preliminaries

The algebraic structure of convolutional codes is known since the pioneer paper [2], which can be understood [3] as direct summands of a free module of finite rank $F[z]^n$ over the (commutative) polynomial ring $F[z]$, where $F$ is a finite field. We deal with convolutional codes with cyclic structures from the perspective promoted by Gluesing-Luersen and Schmale [3] and extended by López-Permouth and Szabo [9]. An ideal code over the alphabet $F$ is defined to be a left ideal of a skew polynomial ring $A[z;\sigma]$, where $\sigma$ is an automorphism of a finite $F$–algebra $A$, which is a direct summand as an $F[z]$–submodule of $A[z;\sigma]$. The cyclicity of the code is then expressed by means its word-ambient $A$ and its sentence-ambient $A[z;\sigma]$. When the word-ambient is $A = F[x]/(x^n-1)$ (with $n$ coprime with the characteristic of $F$), we obtain the $\sigma$–cyclic convolutional codes, whose study has been systematized in [3]. This kind of cyclic structures were introduced by Piret in [11]. According to [9], we could go beyond and consider (possibly non–commutative) semisimple finite algebras as word-ambient. We will focus on the case of a matrix algebra over $F$.

An open question is left in [9]: when is an ideal code a direct summand of $A[z;\sigma]$ as a left ideal? This in particular would imply that the code is generated by an idempotent. A sufficient condition appears in [4, 5], where it is shown that, if there is a certain separability element for the ring extension $F[z] \subseteq A[z,\sigma]$, then

2010 Mathematics Subject Classification: Primary: 94B10; Secondary: 94B15, 16S36.
Key words and phrases: Convolutional code, Ideal code, dual code, skew polynomial.

Research supported by grants MTM2013-41992-P and TIN2013-41990-R from the Ministerio de Economía y Competitividad of the Spanish Government and from Fondo Europeo de Desarrollo Regional FEDER, and by grant mP-TIC-14 (2014) from CEI-BioTic Granada.
every ideal code is a direct summand as a left ideal, and an algorithm to compute explicitly the generating idempotent of each ideal code is designed.

In [9], it is shown that, for a large class of skew polynomial rings $A[z;\sigma]$, when $A$ is a semisimple finite group algebra, the duals of many ideal codes are also ideal codes with respect to a different skew polynomial algebra. In this paper we give an answer for the same question when $A$ is a matrix algebra. We also include an algorithm that computes a separability element of degree zero for the ring extension $F[z] \subseteq A[z;\sigma]$, whenever it exists.

By $\mathcal{M}_{n \times m}(F)$ we denote the vector space of all matrices of size $n \times m$ with entries in the finite field $F$. A basis for this vector space is the set $\mathcal{B} = \{E_{ij} \mid 0 \leq i \leq n-1, 0 \leq j \leq m-1\}$ of matrix units, where $E_{ij}$ is the matrix with 1 in position $i, j$ and 0 otherwise. The canonical map $\nu : \mathcal{M}_{n \times m}(F) \to F^{n \times m}$ in this basis, writes each matrix as a concatenation of rows, i.e.

$$\nu(M) = (m_{0,0}, m_{0,1}, \ldots, m_{0,m-1}, m_{1,0}, \ldots, m_{1,m-1}, \ldots, m_{n-1,0}, \ldots, m_{n-1,m-1}).$$

We also denote $p = \nu^{-1}$.

Let $M \in \mathcal{M}_{n \times m}(F)$ and $N \in \mathcal{M}_{p \times q}(F)$. The Kronecker product $M \otimes N$ is the matrix

$$\begin{pmatrix}
m_{0,0}N & m_{0,1}N & \cdots & m_{0,m-1}N \\
m_{1,0}N & m_{1,1}N & \cdots & m_{1,m-1}N \\
\vdots & \vdots & \ddots & \vdots \\
m_{n-1,0}N & m_{n-1,1}N & \cdots & m_{n-1,m-1}N
\end{pmatrix} \in \mathcal{M}_{np \times mq}(F).$$

We refer to [7, Chapter 4] as a source of well known properties of the Kronecker product that we will use. For the convenience of the reader, we summarize some of them. Let $M, N, P, Q$ be matrices over $F$ of appropriate sizes to allow products or inverses. Then

(i) $MPN = Q \iff \nu(P)(M^T \otimes N) = \nu(Q)$.

(ii) $(M \otimes N)(P \otimes Q) = (MP) \otimes (NQ)$.

(iii) $(M \otimes N)^T = M^T \otimes N^T$.

(iv) $(M \otimes N)^{-1} = M^{-1} \otimes N^{-1}$.

The Kronecker product has a direct connection with the tensor product of linear maps. For any pair of $F$–vector spaces $V$ and $W$, its tensor product over $F$ is denoted by $V \otimes W$. The map $\mathcal{M}_{n \times m}(F) \otimes \mathcal{M}_{p \times q}(F) \to \mathcal{M}_{np \times mq}(F)$, defined by $M \otimes N$, is an $F$–linear isomorphism, see [8, Proposition 4.10]. Let $f : F^n \to F^m$ and $g : F^p \to F^q$ be linear maps represented by the matrices $M \in \mathcal{M}_{n \times m}(F)$ and $N \in \mathcal{M}_{p \times q}(F)$. The matrix representing $f \otimes g$ with respect to the canonical bases of $F^n \otimes F^p$ and $F^m \otimes F^q$ is $M \otimes N$. The usual notation for the Kronecker product in the literature is $\otimes$ instead of $\otimes$. We adopt this change of notation because in Sections 3 and 4 we have to deal with both situations, i.e. given $a, b \in \mathcal{M}_n(F)$, we have to handle both $a \otimes b \in \mathcal{M}_n(F) \otimes \mathcal{M}_n(F)$, and $a \otimes b \in \mathcal{M}_n(F)$.

**Remark 1.1.** We denote by $K_{r,s}$ the matrix with respect to the canonical bases of the isomorphism $\mathcal{M}_r(F) \otimes \mathcal{M}_s(F) \cong \mathcal{M}_{r,s}(F)$ provided by the Kronecker product. This is a permutation matrix.

Let $A = \mathcal{M}_n(F)$ and $\sigma \in \text{Aut}_F(A)$, where $\text{Aut}_F(A)$ denotes the set of $F$–automorphisms of the algebra $A$. By the Skolem-Noether Theorem [8, Theorem 4.9 and Corollary], there exists a non singular matrix $U \in A$ such that $\sigma(a) = UaU^{-1}$, i.e. $\sigma = \sigma_U$, the inner automorphism associated to $U$. As usual $A[z;\sigma]$ denotes the algebra of skew polynomials over $A$. Its elements are polynomials in $z$ (with
coefficients on the right) and the product is determined by the rule \( az = z \sigma(a) \), for all \( a \in A \). The inclusion \( F \subseteq A \) as scalar matrices is extended to an inclusion \( F[z] \subseteq A[z; \sigma] \). The action given by left multiplication of \( F[z] \) on \( A[z; \sigma] \) makes \( A[z; \sigma] \) a free \( F[z] \)-module whose basis is also \( B \). We will always consider this \( F[z] \)-module structure. Although \( A[z; \sigma_U] \) is also a right \( F[z] \)-module, left and right actions of \( F[z] \) on \( A[z; \sigma_U] \) are different, so \( A[z; \sigma_U] \) is not an \( F[z] \)-algebra.

The canonical isomorphism \( \mathcal{M}_n(F)[z] \cong \mathcal{M}_n(F[z]) \) allows to extend \( \psi : A \to F^{n^2} \) to an \( F[z] \)-linear isomorphism \( \psi : A[z; \sigma] \to F[z]^{n^2} \). Its inverse is the corresponding extension of \( p \).

2. Duality and ideal codes

In this section the word-ambient of the (cyclic) convolutional codes will be the matrix algebra \( A = \mathcal{M}_n(F) \). We know that every algebra automorphism of \( A \) is inner, so we fix a non-singular matrix \( U \in A \) and the corresponding inner automorphism \( \sigma_U : A \to A \) defined by \( \sigma_U(a) = U a U^{-1} \). Let \( R = A[z; \sigma_U] \). Recall from [9] that an ideal code is a left ideal \( I \leq R \) such that \( \psi(I) \) is a direct summand of \( F[z]^{n^2} \).

So, ideal codes are convolutional codes. In our investigation of the dual code of an ideal code, we will make use of left and right annihilator ideals. Let us recall this basic construction.

For each \( X \subseteq R \), the left and the right annihilator of \( X \) are defined as

\[
\text{Ann}_R^l(X) = \{ f \in R \mid f x = 0 \ \forall x \in X \}, \\
\text{Ann}_R^r(X) = \{ f \in R \mid x f = 0 \ \forall x \in X \},
\]

respectively. They are a left ideal and a right ideal of \( R \), respectively.

**Lemma 2.1.** The left annihilator of any subset of \( R \) is an ideal code.

**Proof.** Let \( X \) be any subset of \( R \). By [3, Proposition 2.2] it is enough to prove that if \( fg \in \text{Ann}_R^l(X) \) for some \( f \in F[z] \setminus \{0\} \), \( g \in R \), then \( g \in \text{Ann}_R^r(X) \). This is clear because \( R \) is a torsionfree \( F[z] \)-module.

Our next aim is to get an efficient representation in coordinates with respect to \( B \) of the basic algebraic operations of the word-ambient \( A \) (like the product or the action of \( \sigma_U \)). To this end, we use the Kronecker product.

For each \( F \)-linear map \( \lambda : A \to A \), let \( M_\lambda \) be the matrix of \( \lambda \) with respect to \( B \). Writing the coordinates as row vectors, we know that \( M_\lambda \) is defined by

\[
\psi(\lambda(x)) = \psi(x) M_\lambda,
\]

for all \( x \in A \).

By basic linear algebra,

\[
M_\lambda = \begin{pmatrix}
\psi(\lambda(E_{0,0})) \\
\vdots \\
\psi(\lambda(E_{0,n-1})) \\
\psi(\lambda(E_{n-1,0})) \\
\vdots \\
\psi(\lambda(E_{n-1,n-1}))
\end{pmatrix}
\]
For each $a \in A$, let $\rho_a : A \to A$ be the left $A$–module map (and hence $F$–linear) defined by $\rho_a(x) = xa$. In this case we also denote $M_a = M_{\rho_a}$. Next lemma describes this matrix in terms of the Kronecker product.

**Lemma 2.2.** For all $a \in A$, $M_a = I_n \boxtimes a$.

**Proof.** For each $a = (a_{ij}) \in A$, it is straightforward to check that

\[
E_{kl}a = \begin{pmatrix}
0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 \\
\end{pmatrix}
\]

i.e. $E_{kl}a$ is the matrix whose only non zero row is the $k$-th, in which appears the $l$-th row of $a$. The result follows directly from this observation. \(\square\)

Let us collect a number of identities needed along the paper.

**Lemma 2.3.** The following properties hold:

(i) $M_{\sigma^{-1}} = M_{\sigma^{-1}} = M^{-1}.$

(ii) $M_{\sigma} = U^T \boxtimes U^{-1}.$

(iii) $M_{\sigma} = M_{\sigma}.$

(iv) $v(a)M_b = v(ab)$.

(v) $M_{ab} = M_aM_b.$

(vi) $M_{\sigma}(a) = M^{-1}M_aM_{\sigma}$.

**Proof.** Items (i) to (v) are direct consequences of the properties of Kronecker product, Lemma 2.2 and equation (1). Since

\[
M_{\sigma}^{-1}M_aM_{\sigma} = ((U^{-1})^T \boxtimes U)(I_n \boxtimes a)(U^T \boxtimes U^{-1})
\]

\[
= I_n \boxtimes (UaU^{-1})
\]

\[
= I_n \boxtimes \sigma_U(a)
\]

\[
= M_{\sigma}(a)
\]

we also have (vi). \(\square\)

With these tools at hand, we are ready to give a good representation of the relevant operations of the sentence-ambient $R$.

For each $f \in R = A[z; \sigma_U]$, define

\[
M_R(f) = \begin{pmatrix}
v(E_{0,0} f) \\
v(E_{0,n-1} f) \\
\vdots \\
v(E_{n-1,0} f) \\
\vdots \\
v(E_{n-1,n-1} f)
\end{pmatrix}.
\]

Since $B$ is also a basis of $R$ as an $F[z]$–module, it follows that $M_R(f)$ is the matrix associated to the $F[z]$–module map defined by right multiplication by $f$, and its rows generate $Rf$ as $F[z]$–submodule of $F[z]^n$. 

---

**Advances in Mathematics of Communications**

**Volume 10, No. 1 (2016), 29–43**
Given any \( f \in R \), we use the notation \( f = \sum_k z^k f_k \).

**Proposition 2.4.** For all \( f, g \in R \) we have:

(i) \( \psi(g)M_R(f) = \psi(gf) \).

(ii) \( M_R(gf) = M_R(g)M_R(f) \).

(iii) \( M_R(f) = \sum_k (zM_{\sigma_U})^k M_{f_k} \).

(iv) The map \( \hat{M}_R : R \to \mathcal{M}_n(\mathbb{F}[z]) \) is \( \mathbb{F} \)-linear and injective.

**Proof.** This proof is adapted and simplified from [9, Propositions 4.7 and 4.8]. (i) and (ii) follow from the fact that \( M_R(f) \) is the matrix representing the morphism of \( \mathbb{F}[z] \)-modules defined as right multiplication by \( f \) in the basis \( B \).

Since \( \psi \) is an \( \mathbb{F}[z] \)-linear map,

\[
\psi(g) \sum_k (zM_{\sigma_U})^k M_{f_k} = \psi \left( \sum_l z^l g_l \right) \sum_k (zM_{\sigma_U})^k M_{f_k} \\
= \sum_{l,k} z^l z^k \psi(g_l) M_{\sigma_U} M_{f_k} \\
= \sum_{l,k} z^l z^k \psi(g_l(z^k f_k)) \quad \text{by Lemma 2.3} \\
= \psi \left( \sum_l z^l \sum_k z^k \sigma_U^k(g_l) f_k \right) \\
= \psi \left( \sum_l z^l \sum_k g_l(z^k f_k) \right) \\
= \psi \left( \sum_l z^l g_l \sum_k z^k f_k \right) \\
= \psi(gf).
\]

Hence (iii) follows from (i).

In order to prove (iv) observe first that the linearity is clear. If \( M_R(f) = 0 \) then, for all \( k \geq 0 \), \( M_{\sigma_U}^k M_{f_k} = 0 \), which implies that \( M_{f_k} = 0 \) since \( M_{\sigma_U} \) is non-singular. By Lemma 2.2, \( f_k = 0 \) for all \( k \geq 0 \), hence \( f = 0 \) and \( M_R \) is injective.

For each matrix \( M \in \mathcal{M}_{p \times q}(\mathbb{F}[z]) \), we denote \( \cdot M : \mathbb{F}[z]^p \to \mathbb{F}[z]^q \) the map given by right multiplication by \( M \); \( \text{im}(\cdot M) \) and \( \text{ker}(\cdot M) \) are the image and the kernel of this linear map. As we will see, many ideal codes are principal left ideals of \( R \), generated by some skew polynomial \( f \). The following corollary will enable to get the generating matrix of the code from the coefficients of \( f \).

**Corollary 2.5.** For all \( f \in R \), \( \text{im}(\cdot M_R(f)) = \psi(Rf) \).

**Proof.** It follows directly from Proposition 2.4.

We are now in position to address the main problem in this section, namely, under which conditions the dual code of an ideal code with sentence-ambient \( R \) is an ideal code with a sentence-ambient of the same kind? To this end, we build a suitable skew polynomial ring \( S \) over \( A \).

**Definition 2.6.** Let \( \theta : A \to A \) given by \( \theta(a) = a^T \), the transpose of \( a \), which is an \( \mathbb{F} \)-linear involution. For each \( \sigma \in \text{Aut}_\mathbb{F}(A) \), we define \( \sigma_\theta = \theta \sigma^{-1} \theta \).

**Remark 2.7.** Direct consequences of this definition are:

(i) For all \( a \in A \), \( \sigma_\theta(a) = \sigma(a)^T \).

(ii) \( \sigma_{\theta U} = \sigma_{U\sigma} \).

(iii) \( M_{\sigma_{\theta \sigma} U} = M_{\sigma_{\theta}} U \).

(iv) \( M_{\sigma_{\theta \sigma} (a)} = M_{\sigma_{\theta \sigma}} U M_{\sigma_{\theta \sigma} U} \).
Definition 2.8. For all $f \in R = A[z; \sigma_U]$, it follows from the multiplication rule of $R$ that $f = \sum_k z^k f_k = \sum_k \sigma_U^{-k}(f_k) z^k$. We define the map $\hat{\cdot} : A[z; \sigma_U] \to A[z; \hat{\sigma}_U]$ by $\hat{f} = \sum_k z^k \sigma_U^{-k}(f_k)t \in A[z; \hat{\sigma}_U]$.

The automorphism $\hat{\sigma}_U$ allows to build a new sentence-ambient $S = A[z; \hat{\sigma}_U]$ with the same word-ambient. Our aim is to describe the dual code of a given ideal code over $R$ as an ideal code over $S$. Next propositions are the key-tools for this purpose.

Proposition 2.9. Let $R = A[z; \sigma_U]$ and $S = A[z; \hat{\sigma}_U]$. Then $M_R(f)^T = M_S(\hat{f})$.

Proof. First observe that, by Lemma 2.3,

\[
M_{\sigma_U^{-k}(f_k)} M_k = M_{\sigma_U^{-k}(f_k)} M_{\sigma_U} M_k = M_{\sigma_U^{-k}(f_k)} M_k,
\]

hence,

\[
M_R(f)^T = \sum_k (z M_{\sigma_U})^k M_{\sigma_U} M_{\sigma_U^{-k}(f_k)} T
\]

by Proposition 2.4

\[
= \sum_k z^k M_{\sigma_U} M_{\sigma_U^{-k}(f_k)} T
\]

by (2)

\[
= \sum_k z^k (M_{\sigma_U})^t M_{\sigma_U^{-k}(f_k)} T
\]

by Lemma 2.3

\[
= \sum_k z^k (M_{\sigma_U})^t M_{\sigma_U^{-k}(f_k)} T
\]

by Remark 2.7

\[
= M_S(\hat{f}) \quad \text{by Proposition 2.4},
\]

as desired. \qed

Proposition 2.10. The map $\hat{\cdot} : A[z; \sigma_U] \to A[z; \hat{\sigma}_U]$ is an $F$–linear algebra anti-isomorphism.

Proof. This proof is adapted from [9, Proposition 4.18]. By Proposition 2.4, $M_S$ is an injective $F$–linear map, so let $\Phi$ be a left inverse. By Propositions 2.4 and 2.9,

\[
\hat{f} h = \Phi \left( M_S(\hat{f} h) \right)
\]

\[
= \Phi \left( M_R(f h)^T \right)
\]

\[
= \Phi \left( M_R(h)^T M_R(f)^T \right)
\]

\[
= \Phi \left( M_S(\hat{h}) M_S(\hat{f}) \right)
\]

\[
= \Phi \left( M_S(\hat{h} \hat{f}) \right)
\]

\[
= \hat{h} \hat{f}
\]

as desired. \qed

Corollary 2.11. If $e \in A[z; \sigma_U]$ is idempotent then $\hat{e} \in A[z; \hat{\sigma}_U]$ is idempotent.
For each convolutional code $C \subseteq \mathbb{F}[z]^{m}$, recall that the dual code is defined as
\[ C^\perp = \{ w \in \mathbb{F}[z]^{m} \mid vw^T = 0 \ \forall v \in C \}. \]

We can now prove the main result of this section.

**Theorem 2.12.** Let $A = M_n(\mathbb{F})$ and $\sigma_U \in \text{Aut}_\mathbb{F}(A)$ be the inner automorphism defined by $\sigma_U(a) = UaU^{-1}$ for some unit $U \in A$. Let $f, h \in R = A[z; \sigma_U]$ such that $\text{Ann}_R(Rf) = hR$ and $\text{Ann}_R(hR) = Rf$. Then
\begin{enumerate}[(i)]  
  
  \item $C = \mathfrak{v}(Rf) \subseteq \mathbb{F}[z]^{n^2}$ is an ideal code.
  
  \item $C = \text{im}(\cdot M_R(f)) = \ker(\cdot M_R(h))$.
  
  \item $C^\perp = \text{im}(\cdot M_R(h)^T) = \ker(\cdot M_R(f)^T)$.
  
  \item $C^\perp = \text{im}(\cdot M_S(\hat{h})) = \ker(\cdot M_S(\hat{f}))$.
  
  \item $\mathfrak{p}(C^\perp) = \hat{S}h$, and $C^\perp$ is an ideal code.
\end{enumerate}

**Proof.** By Lemma 2.1, $C$ is an ideal code because $Rf$ is an annihilator left ideal. Consider the following commutative diagram of $\mathbb{F}[z]$-modules.

\[
\begin{array}{ccc}
\mathbb{F}[z]^{n^2} \underset{\cdot M_R(f)}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_R(h)} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_S(\hat{h})}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_S(\hat{f})} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_R(f)}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_R(h)} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_S(\hat{h})}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_S(\hat{f})} & \mathbb{F}[z]^{n^2} \\
\end{array}
\]

The equality $Rf = \text{Ann}_R(hR)$ is equivalent to say that the first row of (3) is exact. Since $\mathfrak{v}$ is an isomorphism of $\mathbb{F}[z]$-modules, the second row is also exact. This implies that $C = \text{im}(\cdot M_R(f)) = \ker(\cdot M_R(h))$. From Proposition 2.10 it follows that $\text{Ann}_S(\hat{S}h) = \hat{f}S$ and $\hat{S}h = \text{Ann}_S(\hat{f}S)$, where $S = A[z; \sigma_U]$. Using a diagram similar to (3), we get from $\hat{S}h = \text{Ann}_S(\hat{f}S)$ that
\[
\begin{array}{ccc}
\mathbb{F}[z]^{n^2} \underset{\cdot M_S(\hat{h})}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_S(\hat{f})} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_R(h)^T}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_R(f)^T} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_S(\hat{h})}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_S(\hat{f})} & \mathbb{F}[z]^{n^2} \\
\mathbb{F}[z]^{n^2} \underset{\cdot M_R(h)^T}{\longrightarrow} \mathbb{F}[z]^{n^2} & \xrightarrow{\cdot M_R(f)^T} & \mathbb{F}[z]^{n^2} \\
\end{array}
\]

is exact, i.e. $\text{im}(\cdot M_S(\hat{h})) = \ker(\cdot M_S(\hat{f}))$. By Proposition 2.9 we conclude that $\text{im}(\cdot M_R(h)^T) = \ker(\cdot M_R(f)^T)$. So
\[
w \in C^\perp \iff wM_R(f)^T = 0 \iff w \in \text{im}(\cdot M_R(h)^T),
\]

therefore $C^\perp = \text{im}(\cdot M_R(h)^T) = \ker(\cdot M_R(f)^T)$. By Corollary 2.5 we have that $\mathfrak{p}(C^\perp) = \hat{S}h$. By Lemma 2.1, $C^\perp$ is an ideal code. \hfill \square

**Corollary 2.13.** In the conditions of Theorem 2.12, $C^\perp$ is generated by the columns of $M_R(h)$.

**Remark 2.14.** If $\mathfrak{p}(C) = Rf$ is a direct summand as a left ideal of $R$ then $Rf = Re$, for some idempotent $e \in R$. Therefore, $\text{Ann}_R(Re) = (1-e)R$ and $\text{Ann}_R((1-e)R) = Re$. Hence $C$ satisfies the hypothesis of Theorem 2.12. This suggests the following definition.

**Definition 2.15.** Let $R = A[z; \sigma]$, where $A$ is any finite (dimensional) algebra over $\mathbb{F}$. An ideal code $I \subseteq R$ is called a split ideal code if $I$ is a direct summand of $R$ as a left ideal.

When the word-ambient $A$ is the group algebra of a finite group $G$, the split ideal codes are just the $(G, \sigma)$-convolutional codes from [1].
Corollary 2.16. Let $A$ and $U$ be as in Theorem 2.12. If $C \subseteq \mathbb{F}[z]^{n \times n}$ is a split ideal code, then $C^\perp$ is a split ideal code.

3. Duality and separable automorphisms.

In this section we consider the following problem: When is every ideal code a split ideal code? We will give a sufficient condition, in terms of the non singular matrix $U$, based on the general results from [4, 5].

Let us consider a ring extension $C \subseteq R$. We use $\otimes_C$ to denote the tensor product of a right and a left $C$–modules. The multiplication on $R$ can be viewed as an $R$–bimodule map $\mu : R \otimes_C R \rightarrow R$. Recall from [6] that $C \subseteq R$ is called separable if $\mu$ is an splitting morphism of $R$–bimodules, i.e. there exists a homomorphism of $R$–bimodules $\beta : R \rightarrow R \otimes_C R$ such that $\mu(\beta(f)) = f$ for all $f \in R$. Or equivalently there exists $p \in R \otimes_C R$ satisfying $rp = pr$ for all $r \in R$, and $\mu(p) = 1$. Obviously, in this case, $\beta(1) = p$. The element $p$ is called a separability element.

The extension $\mathbb{F} \subseteq M_n(\mathbb{F})$ is separable (see, e.g. [10, Example A, pp. 183]). We provide a complete description of all separability elements of this extension in Proposition 4.1. We feel that such a description may already be known to specialists in separable extensions but we were not able to find any reference to it in the literature.

If the extension $\mathbb{F}[z] \subseteq A[z;\sigma_U]$ is separable, then every ideal code of $A[z;\sigma_U]$ is a split ideal code. With this motivation, the separability of these ring extensions has been investigated in [4, 5].

Definition 3.1. An automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ is called a separable automorphism if there exists a separability element $p$ such that $\sigma^\circ(p) = p$, where $\sigma^\circ(a \otimes b) = \sigma(a) \otimes \sigma(b)$.

We collect some results of [4, 5] in the next proposition.

Proposition 3.2. Let $A = M_n(\mathbb{F})$ and $\sigma_U \in \text{Aut}_{\mathbb{F}}(A)$ for some regular matrix $U \in A$. If $\sigma_U$ is a separable automorphism then $\mathbb{F}[z] \subseteq A[z;\sigma_U]$ is a separable extension. Hence, in this case, each ideal code is also a split ideal code. In particular, for each ideal code $C$, $p(C)$ is generated by an idempotent $e \in A[z;\sigma_U]$, i.e. $p(C) = A[z;\sigma_U]e$. Moreover $\text{Ann}^1(A[z;\sigma_U]e) = (1-e)A[z;\sigma_U]$ and $\text{Ann}^1((1-e)A[z;\sigma_U]) = A[z;\sigma_U]e$.

Proof. See [4, Theorem 6 and Proposition 17] or [5, Theorems 1 and 2].

Remark 3.3. In the conditions of Proposition 3.2, the idempotent $e$ that generates $p(C)$ can be explicitly computed from a set of generators of $p(C)$ as a left ideal (see [5, Algorithm 1]).

The following theorem, which is now a direct consequence of Theorem 2.12 and Proposition 3.2, summarizes the good behavior of ideal codes when $\sigma_U$ is separable.

Theorem 3.4. Let $A$ and $\sigma_U$ be as in Theorem 2.12 such that $\sigma_U$ is a separable automorphism. Then for each ideal code $C$, $C^\perp$ is also an ideal code, and both are split ideal codes.

Two questions arise at this point.

- How can we check wether $\sigma_U$ is a separable automorphism?
- If $C$ inherits its ideal structure from $A[z;\sigma_U]$ then the left ideal structure of $C^\perp$ comes from $\widetilde{A}[z;\sigma_U]$. If $\sigma_U$ is separable, is $\sigma_U$ also a separable automorphism?
We are going to answer the second question right now, and we postpone the first one to Section 4.

**Theorem 3.5.** Let \( p = \sum_i a_i \otimes b_i \in A \otimes_B A \) be a separability element such that \( \sigma_U \otimes (p) = p \). Let \( \tilde{p} = \sum_i b_i^T \otimes a_i^T \in A \otimes_B A \). Then \( \tilde{p} \) is a separability element such that \( \tilde{\sigma}_U \otimes (\tilde{p}) = \tilde{p} \).

**Proof.** Let \( \mu : A \otimes_B A \to A \) be the \( A \)-bimodule map defined by \( \mu(a \otimes b) = ab \), and let \( \tau : A \otimes_B A \to A \) be the \( F \)-linear map defined by \( \tau(a \otimes b) = b \otimes a \). The identity morphism on \( A \) is also denoted by \( Id_A \), i.e. \( Id_A : A \to A \) is defined by \( Id_A(a) = a \). Consider the \( A \)-bimodule map defined by \( \beta(1) = p = \sum_i a_i \otimes b_i \). The condition \( rp = \sum_i ra_i \otimes b_i = \sum_i a_i \otimes b_i r = pr \) is equivalent to the equality

\[
(\mu \otimes Id_A)(Id_A \otimes \beta) \eta = (Id_A \otimes \mu)(\beta \otimes Id_A) \tau \eta.
\]

Hence

\[
(\theta \otimes \theta) \tau (\mu \otimes Id_A)(Id_A \otimes \beta) \eta = (\theta \otimes \theta) \tau (Id_A \otimes \mu)(\beta \otimes Id_A) \tau \eta,
\]

which is equivalent to say that

\[
\sum_i b_i^T \otimes (sa_i)^T = \sum_i (b_i s)^T \otimes a_i^T \quad \text{for all} \quad s \in A.
\]

Therefore

\[
r \sum_i b_i^T \otimes a_i^T = \sum_i (r^T b)^T \otimes a_i^T
\]

\[
= \sum_i (b_i r^T)^T \otimes a_i^T
\]

\[
= \sum_i b_i^T \otimes (r^T a_i)^T \quad \text{by (4)}
\]

\[
= \sum_i b_i^T \otimes a_i^T (r^T)^T
\]

\[
= \sum_i b_i^T \otimes a_i^T r.
\]

On the other side,

\[
\sum_i b_i^T a_i^T = \sum_i (a_i b_i)^T = \left( \sum_i a_i b_i \right)^T = 1^T = 1,
\]

hence \( \tilde{p} \) is a separability element. Finally \( \sigma_U \otimes (p) = p \) if and only if \( \sigma_U^{-1} \otimes (p) = p \), i.e.

\[
\sum_i \sigma_U^{-1}(a_i) \otimes \sigma_U^{-1}(b_i) = \sum_i a_i \otimes b_i,
\]

which can be rewritten, as a composition of morphisms, as

\[
(\sigma_U^{-1} \otimes \sigma_U^{-1}) \beta \eta = \beta \eta.
\]
Hence
\[
(\sigma_U \otimes \sigma_U)\tau(\theta \otimes \theta)\beta \eta = (\theta \otimes \theta)(\sigma_U^{-1} \otimes \sigma_U^{-1})(\theta \otimes \theta)\tau(\theta \otimes \theta)\beta \eta
\]
\[
= (\theta \otimes \theta)(\sigma_U^{-1} \otimes \sigma_U^{-1})\tau \beta \eta
\]
\[
= (\theta \otimes \theta)(\sigma_U^{-1} \otimes \sigma_U^{-1})\beta \eta
\]
\[
= (\theta \otimes \theta)\tau \beta \eta
\]
\[
= \tau(\theta \otimes \theta)\beta \eta,
\]
which in terms of elements means that
\[
\hat{\sigma}_U \otimes \sum_i b_i^T \otimes a_i^T = \sum_i b_i^T \otimes a_i^T,
\]
as desired. \qed

4. Computing a separability element

Let \( \sigma_U \) be an algebra automorphism of \( A = M_n(\mathbb{F}) \). Our aim in this section is to design an algorithm for computing a separability element \( p \in A \otimes_\mathbb{F} A \) such that \( \sigma_U \otimes p = p \), whenever it does exist. The set
\[
E = \{ p \in A \otimes_\mathbb{F} A : ap = pa, \forall a \in A \}
\]
is an \( \mathbb{F} \)-vector subspace of \( A \otimes_\mathbb{F} A \). For \( i, j \in \{0, \ldots, n-1\} \), define
\[
p_{ij} = \sum_{k=0}^{n-1} E_{ki} \otimes E_{jk}
\]
Recall that \( \mu : A \otimes_\mathbb{F} A \to A \) is the multiplication map sending \( a \otimes b \in A \otimes_\mathbb{F} A \) onto its product \( ab \).

In order to design an algorithm to compute our desired separability element, we prove in the following proposition that the set of all separability elements of \( A \otimes_\mathbb{F} A \) is a affine subspace of \( E \). It is explicitly described.

**Proposition 4.1.** The set \( P = \{ p_{ij} : 0 \leq i, j \leq n-1 \} \) is a basis of \( E \) as a vector space over \( \mathbb{F} \) and, hence, \( E \) is of dimension \( n^2 \). Let \( E_0 = \{ p \in E : \mu(p) = 0 \} \) and \( E_1 = \{ p \in E : \mu(p) = 1 \} \). Then \( E_0 \) is a vector subspace of \( E \) and \( E_1 \) is an affine subspace of \( E \) both of dimension \( n^2 - 1 \). Moreover \( E_1 = \{ p + p_{00} : p \in E_0 \} \).

**Proof.** Let us first observe that \( P \subseteq E \). To this end, it suffices to check that \( E_{ab}p_{ij} = p_{ij}E_{ab} \) for all \( i, j, a, b \in \{1, \ldots, n\} \), which is an easy computation. The linear independence of \( P \) is deduced from the fact that \( \{ E_{ki} \otimes E_{ij} : 0 \leq i, j, k, l \leq n-1 \} \) is linearly independent. In fact, this set is a basis of \( A \otimes_\mathbb{F} A \) as an \( \mathbb{F} \)-vector subspace, so that, given any \( p \in E \), there exists a unique representation
\[
p = \sum_{i,j,k,l=0}^{n-1} \alpha_{ij}^{kl} E_{ki} \otimes E_{lj}, \tag{5}
\]
where \( \alpha_{ij}^{kl} \in \mathbb{F} \) for all \( i, j, k, l \in \{0, \ldots, n-1\} \). Now, imposing the conditions \( E_{ab}p = pE_{ab} \) for every \( a, b \in \{0, \ldots, n-1\} \) in (5) and equalizing coefficients, we get that, for every \( i, j \in \{0, \ldots, n-1\} \), \( \alpha_{ij}^{00} = 0 \) if \( k \neq l \), and \( \alpha_{ij}^{kk} = \alpha_{ij}^{ll} \) for any \( k, l = 0, \ldots, n-1 \). Therefore,
\[
p = \sum_{i,j=0}^{n-1} \sum_{k=0}^{n-1} \alpha_{ij}^{kk} E_{ki} \otimes E_{jk} = \sum_{i,j=0}^{n-1} \sum_{k=0}^{n-1} \alpha_{ij}^{00} E_{ki} \otimes E_{jk} = \sum_{i,j=0}^{n-1} \sum_{k=0}^{n-1} \alpha_{ij}^{00} p_{ij},
\]
and thus $\mathcal{P}$ spans $E$.

Observe that $E_1$ is a non empty set. Indeed, $p_{ii} \in E_1$ for every $i = 0, \ldots, n - 1$. On the other hand, $\mu(p) \in \mathbb{F}$ for all $p \in E$; if $a \in A$, then $a\mu(p) = \mu(ap) = \mu(pa) = \mu(p)a$, and, hence, $\mu(p)$ is a scalar matrix. Therefore, the restriction of $\mu$ to $E$ gives a linear form $\mu_E : E \rightarrow \mathbb{F}$, hence $E_0$ is the vector subspace defined by the linear equation $\mu_E(p) = 0$, $E_1$ becomes the affine hyperplane of $E$ given by the condition $\mu_E(p) = 1$, and $E_1 = \{ p + p_{00} : p \in E_0 \}$. Since $\dim \mathcal{P} = n^2$, both dimensions of $E_0$ and $E_1$ are $n^2 - 1$.

We denote the linear span of any subset $X$ of an $\mathbb{F}$–vector space by $\langle X \rangle$.

\begin{algorithm}
\caption{Separable Automorphism}
\begin{algorithmic}[1]
\State \textbf{Input:} A regular matrix $U \in A$ providing the inner automorphism $\sigma_U$.
\State \textbf{Output:} A separability element invariant under $\sigma_U^\otimes$ if $\sigma_U$ is a separable automorphism. 0 otherwise.
\For{$0 \leq i, j \leq n - 1$}
\State $\mathcal{E} = \{ \}$
\EndFor
\For{$0 \leq i, j \leq n - 1$}
\If{$i = j$}
\State $\mathcal{E} = \mathcal{E} \cup \{ p_{00} - p_{ii} \}$
\Else
\State $\mathcal{E} = \mathcal{E} \cup \{ p_{ij} \}$
\EndIf
\EndFor
\State Delete the initial zero in $\mathcal{E}$.
\State $M_{\sigma_U} = U^T \otimes U^{-1}$
\State $M_{\sigma_U^\otimes} = K_{n,n}^{-1}(M_{\sigma_U} \otimes M_{\sigma_U})K_{n,n}$
\State $\mathcal{G} = \{ \}$
\For{$q \in \mathcal{E}$}
\State $\mathcal{G} = \mathcal{G} \cup \{ (I_n^s - M_{\sigma_U^\otimes}) \}$
\EndFor
\If{$\mathbf{v}(p_{00}) \cdot (M_{\sigma_U^\otimes} - I_n^s) \in \langle \mathcal{G} \rangle$}
\State Compute $\{ \alpha_{ij} \mid 0 \leq i \neq j \leq n - 1 \} \cup \{ \alpha_{ii} \mid 1 \leq i \leq n - 1 \} \subseteq \mathbb{F}$ such that
\State \[ \mathbf{v}(p_{00}) \cdot (M_{\sigma_U^\otimes} - I_n^s) = \sum_{i \neq j} \alpha_{ij} \left( \mathbf{v}(p_{ij}) \cdot (I_n^s - M_{\sigma_U^\otimes}) \right) + \sum_i \alpha_{ii} \left( \mathbf{v}(p_{00} - p_{ii}) \cdot (I_n^s - M_{\sigma_U^\otimes}) \right) \]
\State \textbf{return} $p_{00} + \sum_{i \neq j} \alpha_{ij} p_{ij} + \sum_i \alpha_{ii} (p_{00} - p_{ii})$
\Else
\State \textbf{return} 0
\EndIf
\end{algorithmic}
\end{algorithm}

\textbf{Theorem 4.2.} Algorithm 1 correctly decides if $\sigma_U \in \text{Aut}_\mathbb{F}(A)$ is a separable automorphism. If it is, it also correctly returns a separability element invariant under $\sigma_U^\otimes$.
Proof. Recall that $A \otimes_T A$ is isomorphic to $M_{n^2}(\mathbb{F})$, via the Kronecker product, as vector spaces. Under this isomorphism $E_{ki} \otimes E_{jl} = E_{kn+j,n+i} \in M_{n^2}(\mathbb{F})$. By Lemma 2.3, $M_{\mathbb{U}} = U^T \otimes U^{-1}$, and by the properties of the Kronecker product $M_{\mathbb{U}} \otimes M_{\sigma_\mathbb{U}} = K_{n,n}(M_{\mathbb{U}} \otimes M_{\sigma_\mathbb{U}})K_{n,n}$.

Using Proposition 4.1, it is straightforward to check that a basis of $E_0$ is $\mathcal{E} = \{p_{ij} : 0 \leq i \neq j \leq n - 1\} \cup \{p_{00} - p_{ii} : 1 \leq i \leq n - 1\}$.

Now $\sigma_\mathbb{U}$ is a separable automorphism if and only if there exists $p \in E_1$ such that $\sigma_\mathbb{U}(p) = p$. This is equivalent to the existence of $q \in E_0$ such that $\sigma_\mathbb{U}(p_{00} + q) = p_{00} + q$, i.e. $(\sigma_\mathbb{U} \circ \text{id})(p_{00}) \in (\text{id} \circ \sigma_\mathbb{U})(E_0)$. Since $\mathcal{E}$ is a basis for $E_0$, $\mathcal{G}$ is a generator set for $(\text{id} \circ \sigma_\mathbb{U})(E_0)$. By (1), we conclude that $\sigma_\mathbb{U}$ is a separable isomorphism if and only if $\nu(p_{00}) \cdot (M_{\sigma_\mathbb{U}} - I_{n^2}) \in (\mathcal{G})$.

If

$$
\nu(p_{00}) \cdot (M_{\sigma_\mathbb{U}} - I_{n^2}) = \sum_{i \neq j} \alpha_{ij} \left( \nu(p_{ij}) \cdot (I_{n^4} - M_{\sigma_\mathbb{U}}) \right) + \sum_i \alpha_i \left( \nu(p_{00} - p_{ii}) \cdot (I_{n^4} - M_{\sigma_\mathbb{U}}) \right),
$$

it follows that $p = \sum_{i \neq j} \alpha_{ij} p_{ij} + \sum_i \alpha_i (p_{00} - p_{ii}) \in E_0$ satisfies $\sigma_\mathbb{U}(p_{00} + p) = p_{00} + p$, hence Algorithm 1 works correctly. \hfill $\square$

5. Examples

Our first example explains how Theorem 2.12 can be used to compute the dual code of a given ideal code.

Example 5.1. This example is a continuation of [4, Examples 9 and 25]. Let $\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(\alpha^3 + \alpha + 1)$ be the field of 8 elements. We write the elements of $\mathbb{F}_8 \setminus \{0,1\}$ as powers of the primitive element $\alpha$, and not as polynomials. Let $A = M_2(\mathbb{F}_8)$ and $\sigma_\mathbb{U} \in \text{Aut}_{\mathbb{F}_8}(A)$ the inner automorphism defined by the regular matrix

$$
U = \begin{pmatrix}
\alpha^4 & 1 \\
1 & \alpha
\end{pmatrix}.
$$

Let $R = A[z; \sigma_\mathbb{U}]$ and let $I$ be the left ideal of $R$ generated by $g$, where

$$
g = z^2 \left( \frac{\alpha^5}{\alpha} - \frac{\alpha^6}{1} \right) + z \left( \frac{\alpha^5}{\alpha} - \frac{\alpha^4}{1} \right) + \left( \frac{1}{\alpha^6} - \frac{0}{0} \right).
$$

Hence,

$$
M_R(g) = \begin{pmatrix}
\alpha^6 z^2 + \alpha^5 z & \alpha^5 z^2 + \alpha z & \alpha^6 z^2 + \alpha z \\
\alpha^5 z^2 + \alpha^6 & \alpha^3 z^2 + \alpha^4 z & \alpha^2 z^2 + \alpha^2 z \\
\alpha^5 z^2 + \alpha z & \alpha^6 z^2 + \alpha z & \alpha^2 z^2 + \alpha^2 z
\end{pmatrix}.
$$

As checked in [4, Example 25], $I$ is a direct summand of $R$ as left ideal generated by the idempotent

$$
e = z^3 \left( \frac{\alpha^6}{\alpha^5} - \frac{1}{\alpha^6} \right) + z^2 \left( \frac{\alpha^3}{\alpha^2} - \frac{\alpha^2}{\alpha^6} \right) + z \left( \frac{\alpha^4}{1} - \frac{\alpha^4}{0} \right) + \left( \frac{1}{\alpha^6} - \frac{0}{0} \right),
$$

so the code is also generated by the generator matrix

$$
M_R(e) = \begin{pmatrix}
\alpha^6 z^2 + \alpha^5 z + \alpha^4 z & \alpha^5 z^2 + \alpha^3 z & \alpha^5 z^2 + \alpha^2 z \\
\alpha^5 z^2 + \alpha^6 & \alpha^3 z^2 + \alpha^4 z & \alpha^2 z^2 + \alpha^2 z \\
\alpha^5 z^2 + \alpha z & \alpha^6 z^2 + \alpha z & \alpha^2 z^2 + \alpha z
\end{pmatrix}.
$$
We obtain some consequences from Theorem 2.12 and Proposition 3.2. A parity check matrix for this code is $M_R(1 - e)$. Since
\[ 1 - e = z^{3} \left( \frac{\alpha^6}{\alpha^3} \right) + z^{2} \left( \frac{\alpha^3}{\alpha^2} \right) + z \left( \frac{\alpha^4}{1} \right) + \left( \frac{0}{\alpha^6} \right), \]
we have
\[ M_R(1 - e) = \begin{pmatrix} \alpha^6 z^3 + \alpha^3 z^2 + \alpha^4 z & \alpha^3 z^2 + z & \alpha^2 z^2 + z & \alpha z^2 + z \\ \alpha^3 z + \alpha^5 z & \alpha^6 z + \alpha^5 z & \alpha^4 z & \alpha^2 + z \\ \alpha^2 + z & \alpha z^2 + z & \alpha + z & 0 \\ \end{pmatrix}. \]

The dual code is generated by $M_S(1 - e)$, where $S = A[z; \tilde{\sigma}_U]$ and $\tilde{\sigma}_U = \sigma_{UT}$. We can easily compute
\[ 1 - e = z^{3} \left( \frac{\alpha^6}{\alpha^3} \right) + z^{2} \left( \frac{\alpha^3}{\alpha^2} \right) + z \left( \frac{\alpha^4}{1} \right) + \left( \frac{0}{\alpha^6} \right). \]
From this,
\[ M_S(1 - e) = \begin{pmatrix} \alpha^6 z^3 + \alpha^3 z^2 + \alpha^4 z & \alpha^3 z^2 + z & \alpha^2 z^2 + z & \alpha z^2 + z \\ \alpha^3 z + \alpha^5 z & \alpha^6 z + \alpha^5 z & \alpha^4 z & \alpha^2 + z \\ \alpha^2 + z & \alpha z^2 + z & \alpha + z & 0 \\ \end{pmatrix}. \]
Observe that $M_S(1 - e) = M_R(1 - e)^T$ as expected.

Next example illustrates the execution of Algorithm 1 for two automorphisms. We will conclude that the first one is separable, and a corresponding separability element is provided, whilst the second automorphism is not.

**Example 5.2.** We apply Algorithm 1 to automorphisms in the smallest non–trivial case, $A = M_2(F_2)$. For this algebra we have that
\[ \mathcal{P} = \{ p_{00} = (0 0) \otimes (0 0), p_{01} = (0 0) \otimes (0 1) \}, \]
\[ p_{10} = (0 1) \otimes (0 0), p_{11} = (0 1) \otimes (0 1) \}, \]
but using the Kronecker product to identify $A \otimes F_2 A$ with $M_4(F_2)$, we have
\[ \mathcal{P} = \{ p_{00} = (0 0 0 0), p_{01} = (0 0 0 0), p_{10} = (0 0 0 0), p_{11} = (0 0 0 0) \}, \]
and consequently
\[ \mathcal{E} = \{ p_{01} = (0 0 0 0, p_{10} = (0 0 0 0), p_{00} - p_{11} = (0 0 0 0) \}. \]

Now consider $U = (\frac{1}{1} \frac{1}{0})$. The matrix associated to the linear map id $-\sigma_U^T$ is
\[ I_{16} - M_{\sigma_U^T} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ \end{pmatrix}, \]
and therefore the linear subspace $\langle G \rangle$ is generated by the rows of the matrix
\[ \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ \end{pmatrix}. \]
Since

\[ \mathbf{v}(p_{00}) \cdot (M_{\sigma_U} \otimes I_{16}) = (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \]

is the sum of the first two rows of the matrix generating \( \langle G \rangle \), Algorithm 1 returns \( p_{00} + p_{01} + p_{10} \). Hence \( \sigma_U \) is a separable automorphism.

Finally, let us consider the inner automorphism associated to \( V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). Then

\[ I_{16} - M_{\sigma_V} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \]

\( \langle G \rangle \) is generated by the rows of

\[ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \]

and

\[ \mathbf{v}(p_{00}) \cdot (M_{\sigma_V} \otimes I_{16}) = (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \]

which does not belong to \( \langle G \rangle \). The algorithm returns 0 and \( \sigma_V \) is not a separable automorphism.

6. Conclusions and Future Work

In this paper we improve the knowledge of the algebraic structure of some convolutional codes. Concretely, we deal with split ideal codes, in the sense of Definition 2.15, over the matrix algebra \( A = M_n(\mathbb{F}) \). The main result asserts that if \( C \) is a split ideal code of \( R = A[z; \sigma_U] \), where \( U \in A \) is a regular matrix, then the dual code \( C^\perp \) is also a split ideal code of the algebra \( S = A[z; \hat{\sigma}_U] \). Furthermore, a generating matrix for \( C^\perp \) can be computed from the generating idempotent of \( C \). If the automorphism \( \sigma_U \) is separable, then every ideal code is a split ideal code ([4, 5]).

We design an algorithm (Algorithm 1) to compute a separability element in \( A \otimes \mathbb{F} A \) making \( \sigma_U \) a separable automorphism whenever it does exist.

Future work should extend Theorem 2.12 and Algorithm 1 to more general classes of semisimple algebras \( A \) over finite fields. Some special cases when \( A \) is a group algebra are considered in [9]. On the other hand, following the theory developed in this paper, the separability elements we are looking for have degree zero over \( z \), viewed in \( A[z; \sigma_U] \otimes \mathbb{F}[z] A[z; \sigma_U] \). Example 5.2 shows that for some automorphisms, such a separable element does not exist. An interesting problem is to study if the extension \( \mathbb{F}[z] \subseteq A[z; \sigma_U] \) is separable finding separability elements of higher degree. This could help to determine if any ideal code over a semisimple algebra is a split ideal code, as conjectured in [4, 9].

Acknowledgments

The authors would like to thank the anonymous referees for their suggestions which helped to improve the presentation of the paper.
REFERENCES

[1] S. Estrada, J. R. García-Rozas, J. Peralta and E. Sánchez-García, Group convolutional codes, *Adv. Math. Commun.*, 2 (2008), 83–94.

[2] G. D. Forney Jr., Convolutional codes I: Algebraic structure, *IEEE Trans. Inf. Theory*, 16 (1970), 720–738.

[3] H. Gluesing-Luerssen and W. Schmale, On cyclic convolutional codes, *Acta Appl. Math.*, 82 (2004), 183–237.

[4] J. Gómez-Torrecillas, F. J. Lobillo and G. Navarro, Ideal codes over separable ring extensions, preprint, arXiv:1408.1546

[5] J. Gómez-Torrecillas, F. J. Lobillo and G. Navarro, Cyclic convolutional codes over separable extensions, in *Coding Theory and Applications* (eds. R. Pinto, P. Rocha Malonek and P. Vettori), Springer, 2015, 209–215.

[6] K. Hirata and K. Sugano, On semisimple extensions and separable extensions over non commutative rings, *J. Math. Soc. Japan*, 18 (1966), 360–373.

[7] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge Univ. Press, 1994.

[8] N. Jacobson, *Basic Algebra: II*, W. H. Freeman Company, 1980.

[9] S. R. López-Permouth and S. Szabo, Convolutional codes with additional algebraic structure, *J. Pure Appl. Algebra*, 217 (2013), 958–972.

[10] R. Pierce, *Associative Algebras*, Springer-Verlag, 1982.

[11] P. Piret, Structure and constructions of cyclic convolutional codes, *IEEE Trans. Inf. Theory*, 22 (1976), 147–155.

Received November 2014; revised July 2015.

E-mail address: gomezj@ugr.es
E-mail address: jlobillo@ugr.es
E-mail address: gnavarro@ugr.es