Separable algebras and Convolutional Codes

José Gómez-Torrecillas[⋆] and **F. J. Lobillo**[⋆] and **Gabriel Navarro**[†]
[⋆]Department of Algebra, [†]Department of Computer Sciences and Artificial Intelligence
Universidad de Granada
gomezj@ugr.es, jlobillo@ugr.es, gnavarro@ugr.es

Convolutional codes and cyclicity

Most of the codes used in engineering support a vector space structure (linear block codes) or become a direct summand of a free module over a polynomial ring (convolutional codes). In the linear case, the benefits are amplified if we also consider cyclicity, since the ambient space is also endowed with an algebra structure and cyclic codes come to be ideals. Over convolutional codes, this notion requires something more sophisticated than a simple extension of the block one [1], and the underlying working algebra is no longer a polynomial ring but an skew polynomial ring. In general, the role of cyclicity in convolutional codes is played by *ideal codes* as defined in [3]. Concretely, let A be a finite semisimple algebra over a finite field $\mathbb{F}$. Any $\mathbb{F}$–basis $\mathcal{B}$ of A induces a natural isomorphism of $\mathbb{F}[z]$–modules $\mathfrak{v} : A[z;\sigma,\delta] \to \mathbb{F}[z]^n$. **An ideal code is a left ideal $I \leq A[z;\sigma,\delta]$ such that $\mathfrak{v}(I)$ is a direct summand of $\mathbb{F}[z]^n$.**

Are ideal codes direct summands as left ideals?

A positive answer to this question is known for σ–cyclic convolutional codes (σ-CCC), which are developed in [1]. They are ideal codes of $A[z;\sigma]$, where $A = \mathbb{F}[x]/(x^n - 1)$ with $(\mathrm{char}(\mathbb{F}), n) = 1$, and $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. Another positive answer appears in [3] whenever A is a separable group algebra of a finite group over a finite field. **It is unknown in general.**

Separable extensions and ideal codes

A non commutative ring extension $S \subseteq R$ is called separable if $\exists p = \sum_i a_i \otimes b_i \in R \otimes_S R$ such that $\sum_i a_i b_i = 1$ and $\forall r \in R$, $rp = pr$. This element is called a *separability element*. **In a separable extension, R–submodules which are S–direct summands are also R–direct summands**, as proved in [2].
For each $\sigma \in \mathrm{Aut}(R)$ with $\sigma(S) \subseteq S$, let $\sigma^{\otimes} : R \otimes_S R \to R \otimes_S R$ given by $\sigma^{\otimes}(a \otimes b) = \sigma(a) \otimes \sigma(b)$.

Theorem 1. *Let $S \subseteq R$ be a separable extension with separability element $p = \sum_i a_i \otimes_S b_i \in R \otimes_S R$ and $\sigma \in \mathrm{Aut}(R)$ with $\sigma(S) \subseteq S$. If $\sigma^{\otimes}(p) = p$, then $S[z;\sigma_{|S}] \subseteq R[z;\sigma]$ is separable and a separability element of the extension is given by $\overline{p} = \sum_i a_i \otimes_{S[z;\sigma_{|S}]} b_i \in R[z;\sigma] \otimes_{S[z;\sigma_{|S}]} R[z;\sigma]$.*

A finite semisimple algebra A over a finite field $\mathbb{F}$ is isomorphic to a direct product of matrix rings over finite field extensions of $\mathbb{F}$, so, by [2], $\mathbb{F} \subseteq A$ is separable. Hence

Corollary 2. *Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ with $\sigma^{\otimes}(p) = p$. Then $\mathbb{F}[z] \subseteq A[z;\sigma]$ is a separable extension. In particular each ideal code is a direct summand of $A[z;\sigma]$ and it is generated by an idempotent.*

Can we compute a generator for an ideal code?

In general **it is not known if ideal codes are even principal**. However, as pointed out in Corollary 2, if the ideal code is a direct summand as left ideal then it is generated by an idempotent. This generator **can be effectively computed under the separability conditions.**

Computing a generating idempotent

Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ with $\sigma^{\otimes}(p) = p$. Let I be the left ideal of $A[z;\sigma]$ generated by the set $G = \{g_0, \ldots, g_{t-1}\}$. Observe that $A[z;\sigma]$ is generated as $\mathbb{F}[z]$–module by $\mathcal{B} = \{v_0, \ldots, v_{n-1}\}$, so a generator matrix $M(G)$ for $\mathfrak{v}(I)$ has as rows the vectors $\{\mathfrak{v}(v_i g_j) \mid 0 \leq i \leq n-1, 0 \leq j \leq t-1\}$. We recall that $\mathfrak{v}(I)$ is a direct summand of $\mathbb{F}[z]^n$ if and only if the Smith form of $M(G)$ is a basic matrix, i.e. it has the form $H = \left(\begin{smallmatrix} I_k & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Algorithm 1. Computation of a generating idempotent:
Input: $G = \{g_0, \ldots, g_{t-1}\} \subseteq A[z;\sigma]$ non-zero. **Assumption**. $\mathbb{F} \subseteq A$ is finite semisimple with separability element $p = \sum_i a_i \otimes b_i$ in the conditions of Corollary 2.
Output: An idempotent $e \in R$ such that $Re = Rg_0 + \cdots + Rg_{t-1}$, or zero if it does not exist.

1: Compute the matrix $M(G)$
2: Compute the Smith form decomposition $H = PM(G)Q$
3: **if** H is not basic **then**
4: **return** 0
5: **end if**
6: $V \leftarrow \left(\begin{smallmatrix} 0 \\ I_{n-k} \end{smallmatrix}\right)$, where $k = \mathrm{rank}(H)$ and $n = \dim_{\mathbb{F}}(A)$
7: $M_h \leftarrow QV$, $M_s \leftarrow V^T Q^{-1}$, $M \leftarrow M_h M_s$
8: Compute $p_i = \mathfrak{v}^{-1}(\mathfrak{v}(b_i) \cdot M)$ for all i
9: $f \leftarrow \sum_i a_i p_i$
10: **return** $e = 1 - f$

Examples

Example 3. This example comes from [1]. The same ideas can be applied to any σ-CCC. Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ and

$$A = \mathbb{F}_4[x]/(x^5 - 1) \cong \underbrace{\mathbb{F}_4[x]/(x+1)}_{K_0} \times \underbrace{\mathbb{F}_4[x]/(x^2+\alpha x+1)}_{K_1} \times \underbrace{\mathbb{F}_4[x]/(x^2+\alpha^2 x+1)}_{K_2}.$$

We use the automorphisms

$$\psi : \mathbb{F}_4[x]/(x^2+\alpha x+1) \rightleftarrows \mathbb{F}_4[x]/(x^2+\alpha^2 x+1) : \psi^{-1}$$
$$x \mapsto \psi(x) = \alpha^2 x + 1$$
$$\psi^{-1}(x) = \alpha x + \alpha \hookleftarrow x$$

Let $\sigma : A \to A$ be the automorphism defined by

$$\sigma(x) \equiv \sigma(1,x,x) = (1, \psi^{-1}(x)^4, \psi(x)^4) \equiv x^4 + \alpha^2 x^3 + \alpha x^2 + x,$$

Given dual bases $\{a_i\}_i$ and $\{b_i\}_i$ of a finite field extension, $\sum_i a_i \otimes b_i$ is a separability element.

- $\{1\}$ is a self-dual normal basis of K_0.
- $\{x, x^4\}$ and $\{\alpha x, (\alpha x)^4\}$ are normal dual bases for K_1.
- Applying ψ, $\{\alpha^2 x + 1, (\alpha^2 x + 1)^4\}$ and $\{x + \alpha, (x+\alpha)^4\}$ are normal dual bases for K_2.

By using Chinese Remainder Theorem, it is straightforward to calculate all these elements in A and compute a separability element p:

$$\begin{aligned} p = {} & (x^4+x^3+x^2+x+1) \otimes (x^4+x^3+x^2+x+1) \\ & + (\alpha^2 x^4 + \alpha^2 x^3 + \alpha x^2 + \alpha) \otimes (x^4 + x^3 + \alpha^2 x^2 + \alpha^2) + (\alpha x^3 + \alpha^2 x^2 + \alpha^2 x + \alpha) \otimes (\alpha^2 x^3 + x^2 + x + \alpha^2) \\ & + (\alpha^2 x^4 + \alpha^2 x^2 + \alpha x + \alpha) \otimes (x^4 + x^2 + \alpha^2 x + \alpha^2) + (\alpha x^4 + \alpha^2 x^3 + \alpha^2 x + \alpha) \otimes (\alpha^2 x^4 + x^3 + x + \alpha^2) \end{aligned}$$

By construction, $\sigma^{\otimes}(p) = p$, so $\overline{p}$ is a separability element for the extension $\mathbb{F}_4[z] \subseteq A[z;\sigma]$.

Example 4. Let $A = \mathcal{M}_2(\mathbb{F}_8)$, where $\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(\alpha^3 + \alpha + 1)$. Let $\sigma : A \to A$ be the inner automorphism given by $\sigma(X) = UXU^{-1}$, where $U = \left(\begin{smallmatrix} \alpha^4 & 1 \\ 1 & \alpha \end{smallmatrix}\right)$. The order of σ is 3. It is well-known that $\mathbb{F}_8 \subset A$ is a separable extension and $q = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ is a separability element. Hence, since $(\mathrm{char}(\mathbb{F}_8), |\sigma|) = 1$, $p = |\sigma|^{-1}(q + \sigma^{\otimes}(q) + (\sigma^2)^{\otimes}(q))$ is also a separability element of the extension such that $\sigma^{\otimes}(p) = p$. Concretely

$$\begin{aligned} p = {} & \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} \alpha & 1 \\ \alpha^4 & \alpha^3 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} \alpha & 1 \\ \alpha^4 & \alpha^3 \end{smallmatrix}\right) \\ & + \left(\begin{smallmatrix} \alpha^4 & \alpha^3 \\ \alpha^5 & \alpha^4 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 & \alpha^4 \\ \alpha^3 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} \alpha & \alpha^4 \\ 1 & \alpha^3 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} \alpha & \alpha^4 \\ 1 & \alpha^3 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & \alpha^3 \\ \alpha^4 & 1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} \alpha^4 & \alpha^5 \\ \alpha^3 & \alpha^4 \end{smallmatrix}\right). \end{aligned}$$

This last trick can be used for the group algebras discussed in [3].

Examples

Example 5 (*continuation of Example 3*)**.** Let I be the left ideal generated by the Ore polynomial

$$g = z^2(\alpha^2 x^4 + \alpha x^3 + \alpha x^2 + \alpha^2 x) + z(x^4 + x^3 + x^2 + x) + (\alpha^2 x^4 + \alpha x^3 + \alpha x^2 + \alpha^2 x + 1).$$

One may compute $M(g)$, which is called the σ-circulant matrix of g in [1],

$$M(g) = \begin{pmatrix} 1 & \alpha^2 z^2 + z + \alpha^2 & \alpha z^2 + z + \alpha & \alpha z^2 + z + \alpha & \alpha^2 z^2 + z + \alpha^2 \\ \alpha^2 z^2 + z + \alpha^2 & 1 & \alpha^2 z^2 + \alpha^2 z + \alpha^2 & \alpha z^2 + \alpha z + \alpha & \alpha z^2 + \alpha \\ \alpha z^2 + z + \alpha & \alpha^2 z^2 + \alpha^2 z + \alpha^2 & 1 & \alpha^2 z^2 + \alpha^2 & \alpha z^2 + \alpha z + \alpha \\ \alpha z^2 + z + \alpha & \alpha z^2 + \alpha z + \alpha & \alpha^2 z^2 + \alpha^2 & 1 & \alpha^2 z^2 + \alpha^2 z + \alpha^2 \\ \alpha^2 z^2 + z + \alpha + 1 & \alpha z^2 + \alpha & \alpha z^2 + \alpha z + \alpha & \alpha^2 z^2 + \alpha^2 z + \alpha^2 & 1 \end{pmatrix},$$

whose Smith form decomposition is $H = PM(g)Q$, where $H = \left(\begin{smallmatrix} I_3 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Therefore, I is a σ-cyclic convolutional code of dimension 3 and length 5. The output of Algorithm 1 is

$$e = z^3(\alpha^2 x^4 + \alpha^2 x^3 + x^2 + 1) + z^2(\alpha x^4 + x^2 + \alpha^2 x) + z(\alpha x^4 + x^3 + \alpha x^2 + 1) + (\alpha^2 x^4 + \alpha x^3 + \alpha x^2 + \alpha^2 x + 1).$$

This is a $(5,3,2)_4$ convolutional code. The free distance of I, $d_{\mathsf{free}}(I) = 5$ and it is an MDS code.
Example 6 (*continuation of Example 4*)**.** Let I be the left ideal of $\mathcal{M}_2(\mathbb{F}_8)[z;\sigma]$ generated by the polynomial $g = z^2 \left(\begin{smallmatrix} \alpha^5 & \alpha^6 \\ 0 & 0 \end{smallmatrix}\right) + z \left(\begin{smallmatrix} \alpha^5 & \alpha^4 \\ \alpha & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 0 \\ \alpha^6 & 0 \end{smallmatrix}\right)$. Hence,

$$M(g) = \begin{pmatrix} \alpha^6 z^2 + \alpha^5 z + 1 & z^2 + \alpha^5 z & \alpha^5 z^2 + \alpha z & \alpha^6 z^2 + \alpha z \\ \alpha^2 z^2 + \alpha^6 & \alpha^3 z^2 + \alpha^4 z & \alpha z^2 & \alpha^2 z^2 + z \\ \alpha^5 z^2 + \alpha z & \alpha^6 z^2 + \alpha z & \alpha^2 z^2 + \alpha^2 z + 1 & \alpha^3 z^2 + \alpha^2 z \\ \alpha z^2 & \alpha^2 z^2 + z & \alpha^5 z^2 + \alpha^6 & \alpha^6 z^2 + \alpha z \end{pmatrix}$$

with Smith form decomposition $H = PM(g)Q$, where $H = \left(\begin{smallmatrix} I_2 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Therefore, I is an ideal code of dimension 2 and length 4. Following Algorithm 1, the generating idempotent q is given by $e = z^3 \left(\begin{smallmatrix} \alpha^6 & 1 \\ \alpha^5 & \alpha^6 \end{smallmatrix}\right) + z^2 \left(\begin{smallmatrix} \alpha^3 & \alpha^2 \\ \alpha^2 & \alpha^6 \end{smallmatrix}\right) + z \left(\begin{smallmatrix} \alpha^4 & \alpha^4 \\ 1 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 0 \\ \alpha^6 & 0 \end{smallmatrix}\right)$. In this case $d_{\mathsf{free}}(I) = 4$.

Support Research partially supported by grant MTM2010-20940-C02-01 from the Ministerio de Ciencia e Innovación of the Spanish Government and from FEDER, and by grant mP-TIC-14 (2014) from CEI-BioTic Granada.

References

[1] Heide Gluesing-Luerssen and Wiland Schmale. On cyclic convolutional codes. *Acta Applicandae Mathematicae*, 82(2):183–237, 2004.

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

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