Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Computing separability elements for the sentence-ambient algebra of split ideal codes ☆

José Gómez-Torrecillas [a], F.J. Lobillo [a], Gabriel Navarro [b]

[a] Department of Algebra and CITIC, University of Granada, Spain
[b] Department of Computer Science and AI, and CITIC, University of Granada, Spain

ARTICLE INFO

Article history:
Received 2 November 2015
Accepted 30 April 2016
Available online xxxx

MSC:
16S36
16Z05
68P30

Keywords:
Split ideal code
Separable automorphism
Separable ring extension

ABSTRACT

Cyclic structures on convolutional codes are modeled using an Ore extension $A[z;\sigma]$ of a finite semisimple algebra A over a finite field $\mathbb{F}$. In this context, the separability of the ring extension $\mathbb{F}[z] \subset A[z;\sigma]$ implies that every ideal code is a split ideal code. We characterize this separability by means of σ being a separable automorphism of the $\mathbb{F}$-algebra A. We design an algorithm that decides if such a given automorphism σ is separable. In addition, it also computes a separability element of $\mathbb{F}[z] \subset A[z;\sigma]$, which is important because it can be used to find an idempotent generator of each ideal code with sentence-ambient $A[z;\sigma]$.

1. Introduction

Convolutional codes are error correcting codes with memory, i.e. each output block of the encoding sequence depends on several previous input blocks of the information sequence, in contrast to block codes, where each output depends on only one input block. Convolutional codes are widely used in engineering because their error correction capability can be beyond the Singleton bound for given dimension and length. The encoding process is much better understood in the case of linear codes. If the alphabet is $\mathbb{F} = \mathbb{F}_q$, a finite field, then the underlying structure of a block linear code,

☆ Research supported by grants MTM2013-41992-P and TIN2013-41990-R from the Ministerio de Economía y Competitividad and from FEDER.

E-mail addresses: gomezj@ugr.es (J. Gómez-Torrecillas), jlobillo@ugr.es (F.J. Lobillo), gnavarro@ugr.es (G. Navarro).

http://dx.doi.org/10.1016/j.jsc.2016.11.012
0747-7171/

Please cite this article in press as: Gómez-Torrecillas, J., et al. Computing separability elements for the sentence-ambient algebra of split ideal codes. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.11.012

a vector subspace of $\mathbb{F}^n$, was exploited from the very beginning. However, the algebraic structure of convolutional codes was unknown until Forney clarified it in his pioneering paper in 1970. They can be understood as direct summands of free modules of finite rank over the polynomial ring $\mathbb{F}[z]$ (see Johannesson and Zigangirov, 1999 for details).

Endowing the word-ambient space $\mathbb{F}^n$ with an additional algebraic structure produces linear block codes with better code parameters, parity check matrices used in syndrome decoding, etc. For instance, cyclic block codes are ideals of the commutative semisimple algebra $\mathbb{F}[x]/\langle x^n - 1\rangle$ (with n coprime with the characteristic of $\mathbb{F}$). Therefore, such a code is generated by an idempotent element of the algebra, whose orthogonal complement directly allows parity checking. A straightforward extension of the notion of a cyclic linear code to convolutional codes does not work properly as the paper of Piret (1976) shows. One way of enriching the algebraic structure of the free $\mathbb{F}[z]$-module $\mathbb{F}[z]^n$ is with a non-commutative multiplication. Concretely, given a (possibly non-commutative) $\mathbb{F}$-algebra A of finite dimension n, and σ an $\mathbb{F}$-algebra automorphism of A, we can build the ring $A[z;\sigma]$ of Ore polynomials over A. The elements of $A[z;\sigma]$ are polynomials in z with coefficients in A written on the right, and the multiplication is derived from the rule $az = z\sigma(a)$ for all $a \in A$. The action given by left multiplication of $\mathbb{F}[z]$ on $A[z;\sigma]$ makes $A[z;\sigma]$ a free $\mathbb{F}[z]$-module of rank n. Recall from López-Permouth and Szabo (2013) that an *ideal code* is a left ideal $I \leq A[z;\sigma]$ such that I is a direct summand of $A[z;\sigma]$ as an $\mathbb{F}[z]$-module. So, ideal codes are convolutional codes. This additional algebraic structure has been studied from the perspective of cyclic convolutional codes by Gluesing-Luerssen and Schmale (2004), when A is commutative, López-Permouth and Szabo (2013) and Gómez-Torrecillas et al. (2014), where the semisimplicity hypothesis on the ground algebra A plays a prominent role. We call A the *word-ambient algebra*, and $A[z;\sigma]$ the *sentence-ambient algebra*.

Analogously to the cyclic block case, if an ideal code is a direct summand as left ideal (and not just as an $\mathbb{F}[z]$-module), then it is generated by an idempotent of the sentence-ambient algebra, and its orthogonal complement can be used for parity checking. Ideal codes which are direct summands as left ideals are called *split ideal codes* in Gómez-Torrecillas et al. (2015a, Definition 2.15). So, a central problem is to decide whether a given ideal code I is a split ideal code, and how to compute a generating idempotent. This problem is addressed in Gómez-Torrecillas et al. (2014, 2015b) by means of a new systematic approach based on the notion of a separable ring extension. Recall from Hirata and Sugano (1966) that a ring extension $C \subset D$ is called *separable* if the multiplication map $\mu : D \otimes_C D \to D$ is a split epimorphism of D-bimodules, i.e. if there exists a homomorphism of D-bimodules $\beta : D \to D \otimes_C D$ such that $\mu\beta(f) = f$ for all $f \in D$. Equivalently, there exists $p \in D \otimes_C D$ satisfying $rp = pr$ for all $r \in D$, and $\mu(p) = 1$. Obviously, in this case, $\beta(1) = p$. The element p is called a *separability element* of the extension. If C is a subring of the center of D, then the extension $C \subset D$ is separable if and only if D is a separable C-algebra in the sense of DeMeyer and Ingraham (1971).

By Gómez-Torrecillas et al. (2014, Proposition 17), if $\mathbb{F}[z] \subset A[z;\sigma]$ is a separable ring extension then each ideal code is a direct summand as left ideal of $A[z;\sigma]$, and therefore it is generated by an idempotent, which can be computed using Gómez-Torrecillas et al. (2014, Algorithm 1) once a separability element is known. On the other hand, by Theorem 8 of this paper, $\mathbb{F}[z] \subset A[z;\sigma]$ is separable if and only if there is a separability element of $\mathbb{F} \subset A$ fixed under the map $\sigma \otimes \sigma$. In Gómez-Torrecillas et al. (2014) an automorphism satisfying that property is called *separable*. Observe that, since $\mathbb{F}$ is a finite field, the $\mathbb{F}$-algebra A is separable if and only if it is semisimple. So that this leads to a computational problem: given a semisimple $\mathbb{F}$-algebra A, is it possible to decide if a given $\mathbb{F}$-automorphism of algebras σ is separable?

In Gómez-Torrecillas et al. (2015a) an answer for the case of matrix algebras $A = \mathcal{M}_n(\mathbb{F})$ is given, which has been extended in Gómez-Torrecillas et al. (2015c), the authors' contribution to ISSAC '15, to cover matrix $\mathbb{F}$-algebras $A = \mathcal{M}_n(\mathbb{K})$, where $\mathbb{F} \subset \mathbb{K}$ is an extension of finite fields of degree t. In this paper we provide a complete solution to the case of any semisimple finite $\mathbb{F}$-algebra A. To this end, we prove that $\mathbb{F}[z] \subset A[z;\sigma]$ is a separable ring extension if and only if σ is separable (Theorem 8) and we design an algorithm to decide whether or not such an automorphism is separable (Algorithm 2). This algorithm also computes a separability element of the extension, if it exists. Algorithm 2 is based on the description of the automorphisms in terms of the Artin–Wedderburn decomposition of A, and it uses as a subroutine the algorithm presented in ISSAC'15 (see Algorithm 1).

Please cite this article in press as: Gómez-Torrecillas, J., et al. Computing separability elements for the sentence-ambient algebra of split ideal codes. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.11.012