CONSTRUCTING AND DECODING A CLASS OF CONVOLUTIONAL CODES

JOSÉ GÓMEZ-TORRECILLAS, F. J. LOBILLO, AND GABRIEL NAVARRO

Convolutional codes (CCs) have been extensively used in practical error control applications on a variety of communication channels as, for instance, for deep space communications and satellite data transmissions or 3G/4G mobile telephony communications (as part of a concatenated code). Although they are frequently exploited efficiency, the algebraic structure of CCs is worst understood than the one of block codes (BCs). Mainly, because it needs to work over a free module $\mathbb{F}[t]^n$ of a polynomial ring $\mathbb{F}[t]$ over a finite field $\mathbb{F}$, whilst a BC is simply an $\mathbb{F}$-vector space. This gap is even larger when it comes to the notion of cyclicity. Very little is known about cyclic structures for convolutional codes and their possible impact on applications.

In this paper we show a novel approach to cyclicity for convolutional codes by introducing the so-called skew cyclic convolutional codes (SCCCs) [2]. The "skew" part of this codes comes from the non-commutativity of the working algebra which turns out to be an Ore extension. The underlying idea of deforming the usual product of the ring of (commutative) polynomials is due to Piret in [3], who realized that the standard notion of ciclycity (i.e. words closed under the shift operator) do not produce non-block codes. Piret's definition of cyclic convolutional codes, renamed as σ-cyclic convolutional codes (σ-CCCs) in [1], uses the isomorphism of left $\mathbb{F}[t]$-modules, $\mathbb{F}[t]^n \cong \mathbb{F}[x]/\langle x^n - 1\rangle[t;\sigma]$ in order to establish the Ore extension. However, managing σ-CCCs is complicated. This is so because most of the computational tools developed to handle Ore polynomials are available only when the base ring is a field (or at least a division ring). This represents an obstacle for finding effective and efficient decoding algorithms. Our new perspective considers the embedding of $\mathbb{F}[t]$ into its field of fractions $\mathbb{F}(t)$ so that the cyclicity is obtained from the invariance under the shift operator in $\mathbb{F}(t)^n$, that is, in principle, dealing with ideals of $\mathbb{F}(t)[x]/\langle x^n - 1\rangle$. Again, this does not produce new codes. We thus follow Piret's philosophy of deforming the product yielding an Ore extension, so our sentence-ambient algebra turns out to be the quotient algebra $\mathcal{R} = \mathbb{F}(t)[x;\sigma]/\langle x^n - 1\rangle$, where σ is an $\mathbb{F}$-automorphism of $\mathbb{F}(t)$ of order n. Now, the base ring of the Ore extension is a field so the arithmetic and manipulation of polynomials is well established. Analogously to the block case, an SCCC is then a CC whose image under the inverse of the coordinate map $\mathfrak{v} : \mathcal{R} \to \mathbb{F}(t)^n$ is a left ideal of $\mathcal{R}$. We shall propose a systematic procedure for constructing SCCCs of arbitrary dimension. In particular, we may construct some BCH-like SCCCs of designed Hamming distance. For these class of SCCCs we show a decoding algorithm, providing an alternative to the celebrated Viterbi algorithm.

References

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

[2] J. Gómez-Torrecillas, F. J. Lobillo and G. Navarro, A new perspective of cyclicity in convolutional codes, IEEE Transactions on Information Theory 2016. http://dx.doi.org/10.1109/TIT.2016.2538264.

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

University of Granada

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