ARTICLE IN PRESS LAA:14410

Linear Algebra and its Applications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes ☆

Noemí DeCastro-García[a,*], M.I. García-Planas[b]

[a] *Departamento de Matemáticas, Universidad de León, Spain*
[b] *Departament de Matemàtiques, Universitat Politècnica de Catalunya, Spain*

A R T I C L E I N F O

Article history:
Received 15 December 2016
Accepted 12 December 2017
Available online xxxx
Submitted by M. Van Barel

MSC:
13C10
15A21
93B10
93B55
93C05
05A17

Keywords:
Linear systems
Convolutional codes
Concatenation
Control properties
Linear representations

A B S T R A C T

We present a generalization of the theory of concatenated linear systems to commutative rings with identity. Moreover, we highlight sufficient conditions to obtain reachable and observable concatenated linear systems. This approach provides us with minimal input-state-output representations by means of which we can construct observable concatenated families of convolutional codes with different parameters over some particular rings. This work focuses on the characterization of models of serial, systematic serial and parallel concatenation.

☆ This work has been partially supported by the Spanish National Institute of Cyber-Security (INCIBE) accordingly to the rule 19 of The Digital Confidence Plan and the Universidad de León under the contract A18.

* Corresponding author.
E-mail addresses: ncasg@unileon.es (N. DeCastro-García), maria.isabel.garcia@upc.edu (M.I. García-Planas).

https://doi.org/10.1016/j.laa.2017.12.009
0024-3795/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

The algebraic theory of discrete-time linear systems over arbitrary fields was introduced by Kalman in 1965 (see [13]). In particular, the class of discrete time-invariant linear systems over commutative rings with identity has been extensively studied by different authors (see [1,14,25,26], among others). This class of systems provides us with an input/state/output (I/S/O) representation of the behavior of the system. The part of the state-space representation provides detailed descriptions of the internal behavior of the system, and the input/output part gives information about the external behavior of the system. Moreover, in the case of finite-dimensional dynamical systems, many qualitative properties can be studied in terms of initial-value problems.

One of the most recent applications of discrete time-invariant linear systems has been proposed by Rosenthal et al. in [22–24,28]. They show that for a convolutional code over a finite field exists a unique and minimal I/S/O representation (a reachable linear system) that describes the code. They use this connection to construct observable convolutional codes with good distance properties. From these works, there is a considerable body of literature about the construction of convolutional codes using the approach of linear systems. In particular, some authors as [4,5,9,10,27] had exploited this relation for the construction of concatenated convolutional codes and, to deduce control properties.

In coding theory, concatenated convolutional codes are a class of convolutional codes that are obtained by combining an inner code and an outer code. They were conceived by Forney in [8] to solve the problem of under-utilization of memory since with concatenation, it is possible to join two encoders in a single block. In turn, it provides a solution to the problem of finding a code that has both exponentially decreasing error probability with increasing block length and polynomial time decoding complexity. This type of codes is used to detect, correct and hide information, and they are handy when it is necessary to communicate highly sensitive topics. An important example of concatenated convolutional codes is the turbo codes.

The study of error-correcting codes initially took place in the setting of vector spaces over finite fields. Nevertheless, recently, the research of linear codes over finite rings has become increasingly important, that is due to the realization that many significant and apparently non-linear codes are, in fact, equivalent to linear codes over a modular integer ring. Regarding its applications, for example, in [17] an encoder over $\mathbb{Z}/4\mathbb{Z}$ is developed for decoding MPEG-4 images. Recently, in [12], a steganographic protocol has been performed based on convolutional codes over the ring $\mathbb{Z}/4\mathbb{Z}$.

Massey and Mittelholzer developed the first approach to convolutional codes over rings in [18] and [19] where they showed that the convolutional codes over $\mathbb{Z}_n$ are usually more appropriate for some contexts as the phase modulation. They also focused on the study of minimal and systematic encoders over rings. Minimal encoders, properties or trellis representations of convolutional codes over rings have been developed in [7,11,15,16] or [29], among others.

Please cite this article in press as: N. DeCastro-García, M.I. García-Planas, Concatenated linear systems over rings and their application to construction of concatenated families of convolutional codes, Linear Algebra Appl. (2018), https://doi.org/10.1016/j.laa.2017.12.009