Finite Fields and Their Applications 55 (2019) 1–20

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On duals and parity-checks of convolutional codes over $\mathbb{Z}_{p^r}$

M. El Oued[a], Diego Napp[b,*], Raquel Pinto[b], Marisa Toste[b,c]

[a] FSMMath Department, University of Monastir, Monastir 5050, Tunisia
[b] CIDMA – Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Aveiro, Portugal
[c] Superior School of Technologies and Management of Oliveira do Hospital, Polytechnic Institute of Coimbra, Coimbra, Portugal

ARTICLE INFO

Article history:
Received 9 November 2017
Received in revised form 7 August 2018
Accepted 23 August 2018
Available online xxxx
Communicated by Chaoping Xing

MSC:
94B05
94B10
13F10
13F20

Keywords:
Finite rings
Convolutional codes over finite rings
Dual codes
Matrix representations

ABSTRACT

A convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}((D))$ is a $\mathbb{Z}_{p^r}((D))$-submodule of $\mathbb{Z}_{p^r}^n((D))$ that admits a polynomial set of generators, where $\mathbb{Z}_{p^r}((D))$ stands for the ring of (semi-infinity) Laurent series. In this paper we study several structural properties of its dual $\mathcal{C}^\perp$. We use these results to provide a constructive algorithm to build an explicit generator matrix of $\mathcal{C}^\perp$. Moreover, we show that the transpose of such a matrix is a parity-check matrix (also called syndrome former) of $\mathcal{C}$.

* Corresponding author.
E-mail addresses: Mohamed.Eloued@isimm.rnu.tn (M. El Oued), diego@ua.pt (D. Napp), raquel@ua.pt (R. Pinto), marisa.toste@estgoh.ipc.pt (M. Toste).

https://doi.org/10.1016/j.ffa.2018.08.012
1071-5797/© 2018 Published by Elsevier Inc.

1. Introduction

Convolutional codes form a fundamental class of linear codes that are widely used in applications (see also the related notion of sequential cellular automata [2]). They are typically described by means of a generator matrix, which is a polynomial matrix with coefficients in a finite field or a finite ring, depending on the application. Yet, the state of the art is totally different for these two classes of convolutional codes. The mathematical theory of convolutional codes over finite fields is much developed and has produced many sophisticated classes of codes. On the other hand, the mathematical theory of convolutional codes over finite rings is still in the beginnings. Many results and notions that are well-known for linear convolutional codes over finite fields have not been fully investigated in the context of finite rings. One of these notions is the one of dual code. Dual codes of convolutional codes over a finite field have been extensively studied, see e.g. the work of Forney and McEliece in [7,13] where they showed that when $\mathcal{C}$ is defined over $\mathbb{F}((D))$, $\mathbb{F}$ a finite field, then, the dual code of $\mathcal{C}$ is again a convolutional code and $\mathcal{C}$ always admits a parity-check representation.

In our quest to extend these results over finite fields, we consider in this paper convolutional codes $\mathcal{C}$ over $\mathbb{Z}_{p^r}((D))$ which are a particular class of linear codes and investigate their dual codes $\mathcal{C}^\perp$. We derive fundamental structural properties of $\mathcal{C}^\perp$ and show that they possess the structure of a convolutional code. Moreover, we present a constructive methodology to derive a generator matrix for $\mathcal{C}^\perp$ which will lead to an explicit construction of a parity-check matrix for $\mathcal{C}$. Hence, this work completes previous results in [3,16,14] and can be considered a generalization and an extension, to the ring case, of the work previously done for convolutional codes over a finite field.

The outline of this paper is as follows. In Section 2 we present fundamental results on the structure of convolutional codes over the finite ring $\mathbb{Z}_{p^r}((D))$. We also present some results on free convolutional codes. In Section 3 we address and solve the main problems of the paper. We divide this section in three parts. The first treats the simpler case of free convolutional codes over $\mathbb{Z}_{p^r}((D))$ and then we address the general case. We conclude this section presenting a constructive algorithm to build a generator matrix of the dual code. Some of the most technical proof are presented in the appendix to ease readability.

2. Preliminaries results

In this section we present the setting and the necessary results to address the problems in the next section. Following most the literature on convolutional codes over a finite ring, we consider an approach in which code sequences are semi-infinite Laurent series, *i.e.*, convolutional codes constituted by left compact sequences in $\mathbb{Z}_{p^r}$, see [4,8–10,12]. Hence, the elements of the code (codewords) will be of the form