In V.D. Blondel, E.D. Sontag, M. Vidyasager and J.C. Willems editors,
Open Problems in Mathematical Systems and Control Theory,
Chapter 38, pages 192–201, Springer Verlag, 1998.

38

An optimal control theory for systems defined over finite rings

Joachim Rosenthal[1]
Department of Mathematics
University of Notre Dame
Notre Dame, IN 46556
USA
Rosenthal.1@nd.edu

1 Introduction

A fundamental problem of coding theory is the efficient decoding of certain classes of convolutional codes. It would be highly desirable to develop efficient algorithms which are capable of decoding classes of convolutional codes with particular algebraic properties. In this article we do formulate the problem in terms of linear systems theory and we show that the posed question is connected to some classical problems of systems theory.
A convolutional code can be viewed as a discrete time linear system defined over a finite field $\mathbb{F}$ and we will say more about it in Section 2. Sometimes it is too restrictive to work over a finite field $\mathbb{F}$ and because of this several authors did recently consider codes over a finite ring R (such as the ring $\mathbb{Z}_q$ consisting of the integers modulo q e.g.) or even codes over arbitrary finite groups (see e.g. [3]).
Convolutional codes are widely used in the transmission of data over noisy channels. In conjunction with data compression and modulation schemes they are nowadays integral part of many communication devices. As an example we want to mention the transmission of pictures and other data from deep space, where NASA has used convolutional codes in a most successful way.
In the literature one can find several decoding algorithms. Probably the most widely implemented algorithm is the Viterbi decoding algorithm and we refer to the textbooks [2, 13] for details. Under some natural assumption

[1]Supported in part by NSF grant DMS-96-10389.

on the statistics of the error pattern this algorithm is capable of decoding a received message in a 'maximum likelihood' fashion. The disadvantage of this algorithm lies in the fact that practically the algorithm is too complex for convolutional codes whose McMillan degree is more than 20. On the side of the Viterbi algorithm there exist several 'suboptimal algorithms'. These algorithms do in general not compute the code word in a maximum likelihood fashion. We refer again to the textbooks [2, 6, 13].

The reader might wonder why we pose the decoding problem and why we believe that progress can be done in this area. The reasons are as follows. First note that convolutional codes naturally generalize block codes. Indeed we can view a block code as a convolutional code of McMillan degree zero. For block codes there exist a wealth of algebraic decoding algorithms which take advantage of the algebraic properties of the block code. In contrast to the situation of block codes convolutional codes of nonzero McMillan degree are typically found by computer searches and the existing algorithms do not take advantage of any algebraic structure. Actually most books in coding theory treat convolutional codes in a mainly graph theoretical way and systems theoretic properties of the code are only remarked on the side. It is the author's believe that it should be possible to algebraically construct convolutional codes (linear systems) which come in conjunction with some powerful decoding algorithm. Such an algorithm most likely will employ systems theoretic properties of the underlying code. A first attempt to carry through such a program was reported in [10]. We also see the possibility that existing algorithms in the area of filtering [1] and modeling [7, 8] might lead to improvements in the area of decoding.

The paper is structured as follows: In the next section we introduce the class of convolutional codes defined over a finite ring R. In Section 3 we explain the decoding problem in the situation where the data has been transmitted over the so called q-ary symmetric channel. Finally we explain in Section 4 the decoding problem if data has been transmitted over a Gaussian channel.

We did make an attempt that the paper is self contained. Because of space limitations we did present the problem as a systems theoretic problem. The reader interested in issues of coding theory is referred to the literature. A standard reference on convolutional codes is the textbook by Lin and Costello [2]. The algebraic structure of convolutional codes in the way it is treated in the coding literature is probably best described in the monograph of Piret [6]. One of the most comprehensive reference on linear block codes is the book by MacWilliams and Sloane [4]. The connection of convolutional codes to linear systems theory was first recognized by Massey and Sain [5]. More details on this connection and the way we present the problem are given in the recent papers [9, 11, 12] and the dissertation of York [16].

2 Convolutional codes defined over a Galois ring R

Let R be a finite ring. R is sometimes referred to as a *Galois ring* since this class of rings naturally generalizes the class of Galois fields.
It is the goal of coding theory to transmit data over some noisy channel. For this assume that a vector $v_t \in R^n$ is transmitted at time $t = 0, 1, 2, \ldots$. In this way we arrive at a time series

$$v = \{v_0, v_1, v_2, \ldots\} \in (R^n)^{\mathbb{Z}_+}. \tag{38.1}$$

In order to allow the possibility of error correction it will be necessary to restrict the set of all possible trajectories in $(R^n)^{\mathbb{Z}_+}$ to some subset $\mathcal{C}$ and add in this way some redundancy. A natural way to do such a restriction is as follows:
A subset $\mathcal{C} \subset (R^n)^{\mathbb{Z}_+}$ is called *right shift invariant* if

$$\{v_0, v_1, v_2, \ldots\} \in \mathcal{C} \Longrightarrow \{0, v_0, v_1, v_2, \ldots\} \in \mathcal{C}.$$

The property of right shift invariance allows a time delay in the transmission of the data without confusing the receiver.
Set theoretically $(R^n)^{\mathbb{Z}_+}$ is isomorphic to the direct product $\prod_{i=0}^{\infty} R^n$. In this way $(R^n)^{\mathbb{Z}_+}$ has a natural R-module structure and we define:

Definition 1 A R-linear and right shift invariant subset $\mathcal{C} \subset (R^n)^{\mathbb{Z}_+}$ is called a convolutional code.

The following two examples illustrate two important cases of convolutional codes.

Example 2 Assume $M \subset R^n$ is a R submodule of R^n. If $\mathcal{C}$ is of the form

$$\mathcal{C} = \prod_{i=0}^{\infty} M \subset \prod_{i=0}^{\infty} R^n \cong (R^n)^{\mathbb{Z}_+}$$

then we call $\mathcal{C}$ a linear block code. Alternatively $\mathcal{C}$ consists of all sequences $v = \{v_0, v_1, v_2, \ldots\} \in (R^n)^{\mathbb{Z}_+}$ having the property that $v_t \in M, t = 0, 1, 2 \ldots$. One disadvantage of block codes lies in the fact that so called *burst errors*, these are errors which affect a whole block, are in general badly protected unless the block size is very large. Despite this disadvantage block codes are widely implemented and there are many known techniques of constructing and decoding block codes even if the block length n is very large (see e.g. [4]).

Example 3 The set of code words are often generated by particular input-output systems. For this consider matrices A, B, C, D with entries in R and consider the discrete time system defined over R:

$$x_{t+1} = Ax_t + Bu_t, \quad y_t = Cx_t + Du_t, \quad x_0 = 0. \tag{38.2}$$

Equation (38.2) forms the state space realization of a 'systematic encoder'. (Compare with [2, 9]). One verifies that the collection of all possible trajectories

$$v_t := \begin{pmatrix} u_t \\ y_t \end{pmatrix}, \ t = 0, 1, 2, \ldots$$

defines a convolutional code $\mathcal{C}$. If the matrices A, B, C, D have size $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ and $(n-k) \times k$ respectively one says that $\mathcal{C}$ has complexity (=McMillan degree) δ and transmission rate k/n. Convolutional codes having the form (38.2) are very convenient since in the encoding process u_t can be chosen freely whereas y_t describes the added redundancy. This explains also the word transmission rate since for every k symbols n symbols have to be transmitted.
If the complexity $\delta = 0$ there is the same linear constraint $y_t = Du_t$ at each time instance t and we deal again with a linear block code.

The reader who is familiar with the behavioral literature [14] will observe the close connection to the presented approach. We would like however to stress that our definition of convolutional code does not quite coincide with the notion of linear behavior of Willems [14]. Indeed we have not imposed (and we follow here [3, 11]) that the code has to be complete, a basic requirement for a linear behavior.
Instead of imposing completeness one might want to impose that a code sequence $v = \{v_t\}_{t \in \mathbb{Z}_+}$ has finite support, i.e. v_t is zero with the exception of finitely many time instances. This approach has been taken in [11, 12, 16] and it is based on the reasoning that every data transmission will end at some time. By requiring that a convolutional code has finite support we achieve a duality between convolutional codes on one side and linear behaviors on the other side and we refer to [11] for details. In particular it will still be possible to employ known systems theoretic descriptions for convolutional codes.

3 The problem of decoding convolutional codes on the symmetric channel

The optimal way of decoding a convolutional code depends on the error statistics of the transmission channel. In this section we explain the decoding problem if the transmission channel consists of the so called *q-ary symmetric channel* which we will define in a moment:
Assume the ring R consists of the q symbols $r_1, \ldots, r_q$. The q-ary symmetric channel assumes that during the transmission process every element $r_j, j = 1, \ldots, q$ might change into some element different of r_j with some fixed probability p. In this way the receiver will obtain a time series $\hat{v} = \{\hat{v}_t\}_{t \in \mathbb{Z}_+} \subset (R^n)^{\mathbb{Z}_+}$ and the decoding task is to find the time series

$v \in \mathcal{C}$ which comes 'closest' to the received time series $\hat{v}$. In order to specify what close means in our context we will have to introduce the notion of *Hamming metric*:
If $w \in R^n$ is any vector one defines its Hamming weight as the number of nonzero components of the n-vector w. We will denote the Hamming weight of w by $\mathrm{Ham}\,(w)$. If $w, \hat{w} \in R^n$ are any two vectors one defines their Hamming distance through the formula $\mathrm{dist}\,(w, \hat{w}) := \mathrm{Ham}\,(w - \hat{w})$. One immediately verifies that 'dist' satisfies all axioms of a metric on the (finite) set R^n.
Assume that a certain code word $v = \{v_t\}_{t \in \mathbb{Z}_+}$ was sent and that the message word $\hat{v} = \{\hat{v}_t\}_{t \in \mathbb{Z}_+}$ has been received. The decoding problem then asks for the minimization of the error

$$\mathrm{error} := \min_{v \in \mathcal{C}} \sum_{t \in \mathbb{Z}_+} \mathrm{dist}\,(v_t, \hat{v}_t)\,. \tag{38.3}$$

In the concrete setting of Example 3 the decoding problem asks for the minimization of the error

$$\mathrm{error} = \min \left(\sum_{t=0}^{\infty} (\mathrm{dist}\,(u_t, \hat{u}_t) + \mathrm{dist}\,(y_t, \hat{y}_t)) \right), \tag{38.4}$$

where we denote as before with $\{v_t\}_{t \geq 0} = \left\{ \binom{u_t}{y_t} \right\}_{t \geq 0}$ a particular code word and with $\{\hat{v}_t\}_{t \geq 0} = \left\{ \binom{\hat{u}_t}{\hat{y}_t} \right\}_{t \geq 0}$ a received message word.
Theoretically a correct decoding can always be achieved as long as the error magnitude is at most $1/2$ of the so called *free distance*. The free distance of a code measures the smallest distance between any two different code words and it is formally defined as:

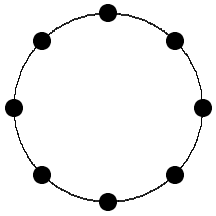
$$d_{\mathrm{free}} := \min_{\substack{u, v \in \mathcal{C} \\ u \neq v}} \sum_{t \in \mathbb{Z}_+} \mathrm{dist}\,(u_t, v_t)\,. \tag{38.5}$$

Note that the decoding problem is essentially a discrete 'tracking problem' where the received message word $\hat{v} = \{\hat{v}_t\}_{t \geq 0}$ has to be tracked by the 'nearest valid code word'. If no transmission error did occur then $\hat{v} = \{\hat{v}_t\}_{t \geq 0}$ is a valid trajectory and the error value in (38.4) can be made zero. It is also possible to view the decoding problem as a 'discrete filtering problem' where the error sequence $e_t := \hat{v}_t - v_t$ has to be filtered out from the received sequence $\hat{v}_t$. In the literature about digital filters (see e.g. [1]) one finds sometimes the appropriate term 'deconvolution'. The problem as we pose it here is formally also closely connected to a global least square modeling problem as it has been recently studied by Roorda [7] and Roorda and Heij [8].
Unfortunately it is not easy to connect either to above literature since the underlying metric is not the Euclidean metric but rather the Hamming metric. As mentioned in the introduction the predominant algorithm applied in

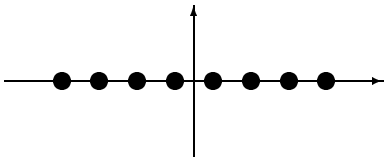
the coding area is the Viterbi decoding algorithm. This algorithm applies the principal of dynamic programming to above situation. The Viterbi algorithm is always applicable but it becomes computationally infeasible as soon as the complexity of the encoder (38.2) is more than a fairly small number like 20. Indeed the number of possible states of an encoder with complexity δ is q^δ, where q is the cardinality of the ring R. The Viterbi algorithm requires a search in a graph which has more than q^δ vertices and this is in terms of complexity not feasible if the complexity and the cardinality of R are too large.

4 Decoding on the Gaussian channel

In many transmission situations such as transmissions over telephone lines and transmission in deep space the signal alphabet is mapped into points of the complex plane $\mathbb{C}$. If $re^{i\theta} \in \mathbb{C}$ is a particular point in the complex plane the transmission is done by assigning to the signal a phase angle of θ and an amplitude of r. The mapping of the signal alphabet into the complex plane $\mathbb{C}$ (or even into some Cartesian product $\mathbb{C}^i$ of $\mathbb{C}$) is called a *modulation*. In the sequel we explain the most basic of these ideas and we refer the interested reader to the textbooks [13, 15] for further reading.
In practice there are two widely implemented modulation schemes. The first is called *q-ary phase shift keying* abbreviated by q-PSK. In this modulation scheme the amplitude of each signal is the same and the modulation is done by assigning to each letter of the alphabet R some phase angle.
The second method is called *q-ary amplitude modulation* usually abbreviated by q-AM. In this scheme the phase angle is left constant. The following picture depicts a typical phase shift modulation scheme and a typical amplitude modulation scheme.



8-PSK Constellation



8-AM Constellation

The 8-PSK constellation can be viewed as the image of the ring $\mathbb{Z}_8$ of integers modulo 8 under the mapping

$$\varphi : \mathbb{Z}_8 \longrightarrow \mathbb{C}, \qquad t \longmapsto e^{\frac{2\pi i t}{8}}.$$

The 8-AM constellation can be viewed as the image under the mapping

$$\psi : \{0, 1, \ldots, 7\} \longrightarrow \mathbb{C}, \qquad t \longmapsto \frac{2t}{7} - 1.$$

In general a modulation $\varphi : R \longrightarrow \mathbb{C}$ induces an embedding of the code $\mathcal{C} \subset (R^n)^{\mathbb{Z}_+}$ into the space $(\mathbb{C}^n)^{\mathbb{Z}_+}$. If the transmission error has the statistics of additive white Gaussian noise (AWGN) as it is approximately the case in many communication systems then the decoding problem asks for the minimization of the error

$$\text{error} := \min_{v \in \mathcal{C}} \sum_{t \in \mathbb{Z}_+} ||v_t - \hat{v}_t||^2. \tag{38.6}$$

As in Section 3 $\hat{v} = \{\hat{v}_t\}_{t \in \mathbb{Z}_+} \subset (\mathbb{C}^n)^{\mathbb{Z}_+}$ denotes the received message sequence. In contrast to (38.3) the Hamming distance is this time replaced with the Euclidean distance to the square. Decoding can always be achieved as long as the error is less than $1/2$ of the value

$$d^2_{\min} := \min_{\substack{u,v \in \mathcal{C} \\ u \neq v}} \sum_{t \in \mathbb{Z}_+} ||u_t - v_t||^2. \tag{38.7}$$

At first sight it seems that the problem of decoding on the Gaussian channel is covered by algorithms available in the systems literature such as e.g. [1, 7, 8]. Unfortunately there is a distinct difference: Although the code $\mathcal{C} \subset (R^n)^{\mathbb{Z}_+}$ is by definition R-linear it is obviously not true that the embedding into the sequence space $(\mathbb{C}^n)^{\mathbb{Z}_+}$ results into a $\mathbb{C}$-linear subspace.
In practice decoding is usually performed (as on the symmetric channel) using the Viterbi decoding algorithm. Once again this algorithm is limited to codes of fairly small McMillan degrees because of complexity considerations.
The problems presented in sections 3 and 4 seem to be hard in full generality. Indeed the problem contain the general problem of decoding linear block codes (transmitted over the symmetric or over the Gaussian channel) as a special instance. What seems to be feasible however is the construction of special classes of convolutional codes which come with efficient decoding algorithms. A step in this direction was done in [10]. It is the authors believe that progress towards the solution of above problem has significant implications for the way data is encoded and transmitted through various noisy communication channels. It would be a significant progress if any of the algorithms developed in the systems literature could be adapted to the problems presented in this paper.

Acknowledgments.
The author would like to thank Roxana Smarandache and Oscar Takeshita for helpful discussions during the preparation of this paper.

References

[1] C. G. Goodwin and K. S. Sin. *Adaptive Filtering Prediction and Control.* Prentice Hall, 1984.

[2] S. Lin and D. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, Englewood Cliffs, NJ, 1983.

[3] H. A. Loeliger and T. Mittelholzer. Convolution codes over groups. *IEEE Trans. Inform. Theory*, 42(6):1660–1686, 1996.

[4] F. J. MacWilliams and N. J.A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.

[5] J. L. Massey and M. K. Sain. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Automat. Contr.*, AC-12(6):644–650, 1967.

[6] Ph. Piret. *Convolutional Codes, an Algebraic Approach*. MIT Press, Cambridge, MA, 1988.

[7] B. Roorda. Algorithms for global total least squares modelling of finite multivariable time series. *Automatica J. IFAC*, 31(3):391–404, 1995.

[8] B. Roorda and C. Heij. Global total least squares modeling of multivariable time series. *IEEE Trans. Automat. Control*, 40(1):50–63, 1995.

[9] J. Rosenthal. Some interesting problems in systems theory which are of fundamental importance in coding theory. In *Proc. of the 36th IEEE Conference on Decision and Control*, pages 4574–4579, San Diego, California, 1997.

[10] J. Rosenthal. An algebraic decoding algorithm for convolutional codes. Preprint, January 1998.

[11] J. Rosenthal, J. M. Schumacher, and E.V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6):1881–1891, 1996.

[12] M.E. Valcher and E. Fornasini. On 2D finite support convolutional codes: an algebraic approach. *Multidim. Sys. and Sign. Proc.*, 5:231–243, 1994.

[13] S.B. Wicker. *Error Control Systems for Digital Communication and Storage*. Prentice Hall, New Jersey, 1995.

[14] J. C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Trans. Automat. Control*, AC-36(3):259–294, 1991.

[15] S.G. Wilson. *Digital Modulation and Coding*. Prentice Hall, New Jersey, 1996.

[16] E.V. York. *Algebraic Description and Construction of Error Correcting Codes, a Systems Theory Point of View.* PhD thesis, University of Notre Dame, 1997. Available at http://www.nd.edu/~rosen/preprints.html.