Convolutional Codes Over Rings

Michael Wood, B.Sc.Eng. Queens University.

Abstract

Elementary information about convolutional codes over finite fields is introduced, and various motivations for extension to convolutional codes over finite rings are discussed. The recent primary motivation is found to be for use over phase modulation signals. Such ring codes enjoy the special property of phase weight equal to phase distance equal to the squared Euclidean distance between phase modulation sequences. Various properties of ring codes are discussed, including conditions for catastrophic encoders, systematic encoders and rotational invariant behaviour. Performance analysis of ring codes and comparable field codes is given. Ring codes are found to be superior when employed over phase modulation signals. Finally, some open problems are discussed.

Keywords

convolutional codes over rings, rational matrices, phase modulation, dynamical systems over rings

Michael Wood is in the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON, Canada K7L 3N6 (email: 9mmw1@qlink.queensu.ca).

I. Introduction

Convolutional codes were introduced by Peter Elias [14] in 1955. These codes operate on serial data, one or a few bits at a time. Convolutional codes are usually described by their code rate and constraint length. Longer constraint lengths produce more powerful codes but cause maximum likelihood decoding complexity to increase exponentially.

A convolutional code can be viewed as a discrete time linear system defined over a finite field $\mathbb{F}$. Because it is sometimes too restrictive to work over a finite field, many researchers have begun to consider codes over finite rings.[5] Of particular interest is the ring $\mathbb{Z}_p$ where p is prime. Extension to ring codes can raise some new difficulties such as catastrophic encoders, but can also provide some uniquely desirable behaviours. Significant gains have been achieved by combining coding and modulation, and some properties only achievable by ring codes have been found to compliment this aim.

A. Applications

Convolutional codes are an integral part of many communication devices, and are widely used in the transmission of data over noisy channels. An extremely successful example of the use of convolutional codes is in the transmission of data from deep space by NASA.

The Cassini orbiter uses two error-correcting codes in its communication to Earth. It first does Reed-Solomon encoding of science data, and then does the convolutional encoding of the Reed-Solomon symbols. The convolutional code used is either (k=7,r=1/2) or (k=15,r=1/6) and typically provides a bit error rate of about one per two hundred. The concatenated coding scheme provides a bit error rate of about one per million, which is what the Cassini needs.

B. Limitations

The Viterbi decoding algorithm is probably the most widely implemented algorithm for decoding convolutional codes. It is capable of decoding a received message in a 'maximum likelihood' manner. Unfortunately it is too complex for convolutional codes whose McMillan degree is greater than 20. Convolutional codes naturally generalize block codes, and block codes can be represented as convolutional codes of McMillan degree zero.[5]

The McMillian degree of a rational matrix $A(\rho) \in R(\rho)^{p\times m}$ is defined as the total number of poles in $C \cup \{\infty\}$ of $A(\rho)$. From another perspective, the McMillian degree of a full rank, non-square polynomial matrix is defined to be the highest degree of its full size minors.

Because the complexity of the Viterbi decoding algorithm increases exponentially with constraint length, several sequential decoding algorithms are used for high constraint length codes. These algorithms are not maximum likelihood, but their complexity increases only slightly with constraint length.

II. Motivation

Many encodes for codes over fields are feed-forward and not homeomorphic; however, homeomorphism can be a desirable trait. Unlike codes over fields, group codes over $\mathbb{Z}_M$ provide encoders that are both rational and homeomorphic. Since codes over $\mathbb{Z}_M$ generalize to codes over rings, this provides motivation for the study of convolutional codes over rings.[7]

Another motivation for the extension of convolutional codes to rings is the possibility of algebraically constructing convolutional codes such that they are paired with powerful decoding algorithms. Currently many existing algorithms for the construction of convolutional codes are found by computer searches and do not take advantage of any algebraic structure.

The recent interest in convolutional codes over rings, however, is linked to the discovery that many efficient trellis coded modulation schemes can be described as orbits of group codes in the Euclidean space. An example of such is group codes over $\mathbb{Z}_M$ and are found to be a natural approach for coding over MPSK constellations.[7]

It turns out that convolutional codes over rings are particularly suitable for representing codes over phase modulation signals. The generator matrices or encoders for such codes are defined by rational matrices over rings. These generator matrices are of the following types: non-catastrophic, minimal, systematic and basic.

III. Phase Modulation

Many researchers have began their investigations into convolutional codes over rings, not out of a desire to employ rigid algebraic structures, but out of necessity forced upon them by investigation of codes for M-ary phase modulation.

If one intends to employ linear codes over phase-modulated signals in a natural way, then one is forced to consider codes over the ring $\mathbb{Z}_M$. This follows from the fact that $\mathbb{Z}_M$ is the unique algebraic system with several desirable features. [1]

In the appropriate two-dimensional Euclidean signal space, the signal points for M-ary phase modulation are equally-spaced around the unit circle. These signal points can be represented as $(e^{\frac{j2\pi}{M}})^i$ for $i = 0 \, .. \, M-1$. Hereafter let $W_M = e^{\frac{j2\pi}{M}}$. [1]

Note that because W_M is a primitive Mth root of unity in the complex plane, the difference $j-i$ in the following can be treated as a $modulo - M$ difference. Now, let us define the squared Euclidean distance between signal points i and j as $d_E^2(i,j) = |W_M^j - W_M^i|^2 = |1 - W_M^{j-i}|^2$, where $|a|$ is the absolute value of a.

Let us consider i and j to be elements of $\mathbb{Z}_M$ (the ring of integers $modulo - M$), and let us define the *phase weight* of element i by $w(i) = |1 - W_M^i|^2$, and the phase distance between elements i and j as $d(i,j) = w(j-i)$.

Now, let us consider the respective phase distance between two sequences $\underline{x}$ and $\underline{y}$ of elements of $\mathbb{Z}_M$. This can be aptly represented as the sum of the weights in each component, which yields $d(\underline{x},\underline{y}) = w(\underline{y} - \underline{x})$.

From this, it should be clear that $d(x_1, y_1) = w(y_1 - x_1) = |1 - W_M^{y_1 - x_1}|^2 = d_E^2(x_1, y_1)$. And extrapolating to the vector, $d(\underline{x},\underline{y}) = d_E^2(\underline{x},\underline{y})$. Thus the phase weight of a sequence, or the respective phase distance between two sequences is exactly the squared Euclidean distance between the corresponding sequences of modulation symbols.

Hence, $\mathbb{Z}_M$ is essentially the unique algebraic system where if we employ linear codes then the phase weight will equal the phase distance and this phase distance exactly equals the squared Euclidean distance between phase modulation sequences. The latter feature does not occur for codes over finite fields. [1]

IV. Definition and Properties

Generalizing from block codes, (n,k) linear convolutional codes over $\mathbb{Z}_M$ are defined as rank k free submodules of the free R-module R^n where R is the ring of fractions whose numerators and denominators are polynomials with coefficients in $\mathbb{Z}_M$ and whose denominators have 1 as the trailing coefficient. From this definition, and related work on linear block codes over $\mathbb{Z}_M$, it follows that the minimum phase distance between two sequences with differing initial information digits d_{free} is equal to the minimum phase weight of all non zero encoded sequences w_{free}. [1]

A. Catastrophic Encoders

Convolutional codes over rings can display bad behaviour in cases that could not exist in their field counterparts. This is primarily due to an inability to reduce the degree of the polynomials in the generator by removing a common factor, as would be possible in the associated field code. [1] provides the following theorem:

A polynomial encoder $G(D)$ over the ring $\mathbb{Z}_M$, where $M = p^m$ and p is prime, is catastrophic if and only if, when the coefficients of the polynomials in $G(D)$ are each reduced modulo p, the resulting polynomial encoder over the finite field $GF(p)$ is catastrophic.

B. Systematic Encoders

Another property of convolutional codes is systematicity. To discuss this, it is first necessary to introduce the causal subcode M_c and the start module M_0 of a convolutional code M. Define M_c as the submodule of M that contains only causal codewords. Also, define M_0 as the R-module of all *Rary* n-tuples which when evaluated at D form codewords in M_c. [2] demonstrates the following proposition:

A convolutional code is systematic if and only if one can select k components M' such that the n-tuples in M'_0 form the free module R^k.

C. Rotational Invariance

As above, let $W_M = e^{\frac{j2\pi}{M}}$, and assume that element i of $\mathbb{Z}_M$ is mapped to W_M^i. A minimum phase shift of the signals, that leaves the signal set unchanged, can then be represented by the transform $i \rightarrow i + 1$ in $\mathbb{Z}_M$. By definition of rotational invariance for a trellis code for phase modulation, this minimum phase shift, when applied to all codewords, must produce codewords differing in finitely many positions from the originals. [2] demonstrates the following proposition:

A convolutional code over $R = \mathbb{Z}_M$ is rotationally invariant if and only if it contains a codeword, each of whose components differs from $1/(1 - D)$ by a polynomial.

V. Performance

When comparing convolutional codes over rings against convolutional codes over fields, we must specify some constraints. First, let us only compare codes of the same rate, measured in bits of information per modulation symbol. Second, let us only compare codes having the same number of encoder states, thereby ensuring similar encoding complexities.

Since we are looking for a use for codes over rings, lets compare them, where the work best: that is, by the Euclidean distance achieved for M-ary phase modulation. In the case of ties we will count the smallest number of occurrences of this distance. Under these criteria, in the words of Massey and Mittelholzer: "ring codes appear to win hands down". They found that ring codes beat field codes even when the ring codes are constrained to be phase invariant (which cannot be attained with linear field codes). [1]

VI. Other Applications

When considering the asymptotic performance, maximum likelihood (ML) and MAP criteria yield the same results. For this reason, binary convolutional codes have generally been designed by exhaustive or heuristic search over all non catastrophic convolutional codes of a given constraint length. In this case it is desired to maximize the squared Euclidean distance d^2_{free} of the code. This design is made signal-to-noise ratios (SNRs) in mind and yields the best performance under such conditions.

The code design process can be simplified by decomposing a continuous phase modulation system into a continuous phase encoder (CPE) and a memoryless modulator. Using a mapper to convert bits to m-ary symbols one can incorporate a convolutional code into a trellis-coded modulation (TCM) system. This is motivated by resulting good coding gain for bandwidth constrained channels.

In considering the special application of low power personal communication systems operating in a fading environment, the system receives the new constraints of lower SNR and limited computational power. The latter excludes long constraint length codes because of the increased decoding complexity. For this application gains can perhaps be best achieved by using joint source-channel coding. In [3], they employed the hidden Markov model view-point of Miller and Park to develop a MAP decoder for the MPEG-4 codec. This utilizes the residual redundancy in the source, by designing a source-controlled channel decoder.

[3] designs ring convolutional codes explicitly for the CPFSK TCM system with MAP decoding. They found codes, for a given constraint length, that provide the best performance for symbol error rates on the range 10^{-2} to 10^{-4}. Their proposed methodology yields optimal codes under the assumption of low SNR. Their process incorporates the source transition matrix into the branch metrics used in the trellis search.

In the system designed by [3], two reasons are given for the use of polynomial, non systematic, ring convolutional codes over $\mathbb{Z}_M$. First, upon comparison to the best systematic ring convolutional codes found in [4], they observed that the best non systematic polynomial ring convolutional encoders provide the larger d^2_{free}. Secondly, in order to perform MAP decoding at the receiver, the source transition matrix must be incorporated into the branch metrics. The trellis diagram of the convolutional encoder and continuous phase encoder combined simplify this process.

Unfortunately, the polynomial convolutional encoder over $\mathbb{Z}_M$ can be catastrophic; consequently, a test is required to determine catastrophism of proposed designs. [3] use the theorem of [1] presented above to accomplish that goal.

VII. Recent Work and Open problems

A fundamental of coding theory is the efficient decoding of various classes of convolutional codes. Much of the literature in coding theory sideline the system theoretic properties of convolutional codes, and focus on their graph theoretic properties. [5] argues that existing algorithms in the areas of filtering and modeling might lead to improvements in the decoding of convolutional codes. Using a largely systems theoretic approach, [5] demonstrates the difficulties in algebraically constructing convolutional codes over rings such that they are paired with powerful decoding algorithms. The connection of convolutional codes to liner systems theory was first recognized by Massey and Sain.[6]

The problem of finding more efficient decoding algorithms is very hard in full generality. In fact it contains the problem of decoding linear block codes as a special case. A more feasible endevour is the construction of special classes of convolutional ring codes, paired with efficient decoding algorithms. [5] argues that it would be a significant progress if any of the algorithms developed in the systems literature could be adapted to achieve this goal.

The case of convolutional ring codes classically treated in literature restricts the input sequence space to a free module. In fact, for the more general case, when the input sequence is simply a module, almost no work has been done. [7] provides the following example, which suggest that in general it might be a serious restriction to constrain the input space to a free module: "the code over $\mathbb{Z}_M$ containing all the sequences having even value at each time has as input sequence space a module which is not free".

A. Recent Work

In an attempt to develop a complete structural analysis of convolutional codes over rings, [7] studies rational matrices over rings (which form the generators for such codes) and describes some special classes of such codes from a systems theoretic point of view.

Based on a rigorous definition of a rational matrix over a Noetherian ring, [7] defines a convolutional code as the module of Laurent power series generated by a rational matrix. This is the generator matrix of the convolutional ring code. Previous papers have defined convolutional codes as the module of rational functions generated by a rational matrix. A fundamental contribution of [7] is to show that for convolutional codes over Noetherian rings these two approaches are completely equivalent. This was previously known for the field case, but several technical difficulties had to be solved to extend the equivalence to the ring case.

As a preliminary result, [7] provides the following useful equivilance relation, where two generator matrices are considered equal if they generate the same convolutional code.

Let R be a Noetherian ring and let $G(D) \in R(D)^{l\times q}$ and $G'(D) \in R(D)^{l'\times q}$. Then $G(D)$ and $G'(D)$ are equivalent generator matrices if and only if l=$l = l'$ and there exists and invertible matrix $T(D) \in R(D)^{l\times l}$ such that $G(D) = T(D)G'(D)$.

In their analysis of the structural properties of non catastrophic, minimal, basic and systematic generator matrices over $\mathbb{Z}_{p^r}$, several particularly relevant results emerged. Among these, they proved the following theorem which characterizes the minimal generator matrices for convolutional codes over rings. This same result was previously know to be true for the more specific case of fields:

Let $R = \mathbb{Z}_{p^r}$ and let $G(D) \in R_r(D)^{l\times q}$ be a realizable generator matrix. Then $G(D)$ is minimal if and only if there exists $X(D) \in R[D]^{q\times l}$ and $Y(D) \in R(D^{-1})^{q\times l}$ such that $G(D)X(D) = I$ and $G(D)Y(D) = I$[7]

VIII. Summary

Convolutional codes over finite fields have been introduced, and various motivations for extension to convolutional codes over finite rings were discussed. The recent primary motivation was found to be for use over phase modulation signals. Such ring codes were found to enjoy the special property of phase weight equal to phase distance equal to the squared Euclidean distance between phase modulation sequences. Various properties of ring codes were discussed, including conditions for catastrophic encoders, systematic encoders and rotational invariant behaviour. Performance analysis of ring codes and comparable field concluded that ring codes beat field codes hands down when used over phase modulation signals. Finally, there remain open problems in the implementation of convolutional codes over rings.

References

[1] J.L.Massey and T.Mittelholzer. Convolutional codes over rings. *In Proceedings of the Joint Swedish-Soviet International Workshop on Information Theory* pages 1418, Gotland, Sweden, 1989.

[2] J.L.Massey and T.Mittelholzer. Systematicity and rotational invariance of convolutional codes over rings. *In Proc. Int. Workshop on Alg. and Combinatorial Coding Theory,* pages 154158, Leningrad, 1990.

[3] Srijidtra Mahapakulchai and Robert E. Van Dyck. Design of Ring Convolutional Trellis Codes for MAP Decoding of MPEG-4 Imagery. *National Institute of Standards and Technology, Gaithersburg, MD*

[4] R. H. Yang, and D. P. Taylor. Trellis-coded continuous-phase frequency-shift keying with ring convolutional codes. *IEEE Trans. Information Theory,* vol. 40, pp. 1057-1067, July 1994.

[5] Joachim Rosenthal. An optimal control theory for systems defined over finite rings. *Open Problems in Mathematical Systems and Control Theory,* Chapter 38, pages 192-201, Springser Verlag, 1998.

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

[7] F. Fagnani and S. Zampieri. System theoretic properties of convolutional codes over rings. *Preprint,* http://www.dei.unipd.it/~zampi/

[8] G.D.Forney. Geometrically uniform codes. *IEEE Trans. Information Theory,* IT-37:12411260,1991.

[9] R.Johannesson and Z.Wan. A linear algebra approach to minimal convolutional encoders. *IEEE Trans. Information Theory,* IT-39:12191233,1993.

[10] R.Johannesson, Z.Wan, and E.Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Trans. Information Theory,* IT-44:839845,1998.

[11] T.Mittelholzer. Minimal encoders for convolutional codes over rings. *In Communication Theory and Applications: Systems, Signal Processing and Error Control Coding,* pages 3036. HW Comm. Ltd., 1993.

[12] T.Mittelholzer. Convolutional codes over rings and the two chain conditions. *In Proc. Int. Symp. on Inform. and Coding Theory,* page 285, Ulm, Germany, 1997.

[13] E.Wittenmark and Z.Wan. Convolutional codes from a dynamical system point of view. *In Proc. IEEE Int. Symposium on Information Theory,* page 160, Trondheim, Norway,1994.

[14] P.Elias. Coding for Noisy Channels. *IRE International Convention Record* pt.4, pp.37-46, 1955.