The convoluted history of minimal encoders

Hans-Andrea Loeliger
Endora Tech AG, Gartenstrasse 120
CH-4052 Basel, Switzerland

email: haloeliger@access.ch

Abstract: Kalman's classic formula *"minimal ⇔ controllable and observable"* fundamentally solves the minimality problem of linear systems theory. However, it took 35 years until Kalman's formula was found to apply also to convolutional encoders.

1 Introduction

A convolutional encoder is a linear sequential circuit as shown in Fig. 1. In mathematical terms, an encoder is described by a set of equations

$$\begin{array}{rcrcl} \mathbf{x}(j+1) & = & A\mathbf{x}(j) & + & B\mathbf{u}(j), \\ \mathbf{y}(j) & = & C\mathbf{x}(j) & + & D\mathbf{u}(j), \end{array} \tag{1}$$

where $j \in Z$ is the discrete time index, where $\mathbf{u}(j) = [u_1(j), \ldots, u_k(j)]$ are the time-j input variables, $\mathbf{y}(j) = [y_1(j), \ldots, y_n(j)]$ are the output variables, $\mathbf{x}(j) = [x_1(j), \ldots, x_m(j)]$ are the state variables, and where A, B, C, and D are matrices of the appropriate dimensions; the equation is over the binary field GF(2) (or over any field).

An encoder as in Fig. 1 or, equivalently, as in (1) is *minimal* if no smaller encoder, (i.e., with a smaller number m of delay cells) produces the same set of possible output sequences. (For an in-depth discussion of minimality, see [1].)

How can we test whether a given encoder is minimal? Kalman's formula [2] [3]

$$\textit{minimal} \Leftrightarrow \textit{controllable and observable} \tag{2}$$

has long been known to give the answer for the *different* notion of minimality in traditional linear systems theory: there, a system (1) (over the real numbers or over any field) is minimal if no such system with a smaller state space dimension m gives the same *transfer function,* i.e., the same set of input/output sequence pairs. In that theory, a system (1) is *controllable* if the block matrix $\mathcal{C} \triangleq [B, AB, \ldots, A^{m-1}B]$ has full rank m; it is *observable* if the block matrix $\mathcal{O} \triangleq [C^T, A^TC^T, \ldots, (A^T)^{m-1}C^T]$ has full rank m. Clearly, the rank test of $\mathcal{C}$ and $\mathcal{O}$ is *not* a minimality test for a convolutional encoder.

2 Detours

The mentioned facts were well understood when the system-theoretic study of convolutional encoders began [4]. However, the subsequent work (most notably [5]) shifted away from (1) and focussed on the sequence equation

$$\mathbf{y}(D) = G(D)\mathbf{u}(D) \tag{3}$$

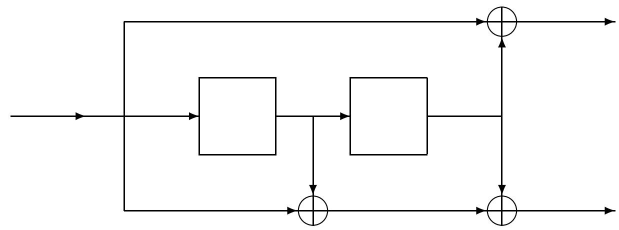

Figure 1: A binary convolutional encoder (with $k = 1$, $n = 2$, and $m = 2$).

where $\mathbf{y}(D)$ and $\mathbf{u}(D)$ are formal Laurent series and where the *generator matrix* (or *encoding matrix*) $G(D)$ is a polynomial or rational matrix in D. Various notions of minimality were defined for such matrices [5] [7], the relation of which to the minimality of (1) is subtle (see [1, Section V.A]). Moreover, the unfortunate custom of referring also to $G(D)$ as "encoder" has confused many students of the subject to the extent that few engineers know how to test whether a general encoder (1) is minimal.

We shall not further use $G(D)$ in this paper.

3 Observability Revisited

A *trellis section* is a four-tuple $X = (G, S, S', B)$, where G is the *label alphabet,* S and S' are the *left state space* and the *right state space,* respectively, and the *branches* B are a subset of $S \times G \times S'$. In this paper, we will assume $S = S'$. A *trellis* is a sequence $\mathcal{X} = \{X_j\}_{j \in Z}$ of trellis sections $X_j = (G_j, S_j, S'_j, B_j)$ such that $S_j = S'_{j-1}$ for all $j \in Z$.

Any system of the form (1) gives rise to a trellis with time-j branches

$$B_j = \{(\mathbf{s}(j), [\mathbf{u}(j), \mathbf{y}(j)], \mathbf{s}(j+1))\}, \tag{4}$$

where the branches are labelled with input-output pairs $[\mathbf{u}(j), \mathbf{y}(j)]$; this trellis will be referred to as the *input-output trellis* of the system. Alternatively, we can label the branches with the output symbols $\mathbf{y}(j)$ only, in which case we will refer to the *output trellis* of the system.

The natural definition of observability for a trellis is the following.

Definition [8]**:** A trellis is *ℓ-observable* if any length-ℓ path segment (sequence of branches) is uniquely determined by the corresponding sequence of branch labels.

This definition is consistent with the traditional system theory notion of observability: the input-output trellis (4) of an ABCD-system (1) is ℓ-observable if and only if the block matrix $[C^T, A^TC^T, \ldots, (A^T)^{\ell-1}C^T]$ has rank m, and it is ℓ-observable for any $\ell \geq m$ if and only if it is m-observable. (The first claim follows from noting that the path segment is uniquely determined by the initial state and the subsequent inputs; the second claim follows from the descending-chain results of [8] or from the Cayley-Hamilton theorem.)

The corresponding matrix condition for the *output* trellis (where the branches are labelled with output symbols $\mathbf{y}(j)$ only) is the following: that trellis is ℓ-observable if and only if the block matrix

$$\begin{bmatrix} C & D & 0 & & \ldots & 0 \\ CA & CB & D & 0 & \ldots & 0 \\ & & \ldots & & & \\ CA^{\ell-1} & CA^{\ell-2}B & \ldots & CAB & CB & D \end{bmatrix} \tag{5}$$

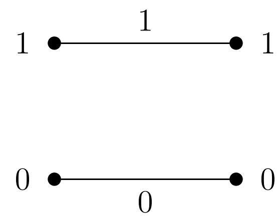

Figure 2: A (section of a) minimal(?) uncontrollable trellis.

has rank $m + \ell k$ (the number of columns); it is ℓ-observable for any $\ell \geq m$ if and only if it is m-observable [1].

4 Controllability Optional

There is also a natural trellis definition of controllability: any state can be reached from any other state in ℓ steps. Other than with observability, its application to ABCD-systems (1) does not dinstinguish between the input-output trellis and the output-only trellis: either trellis is ℓ-controllable if and only if the block matrix $[B, AB, \ldots, A^{\ell-1}B]$ has rank m, and it is ℓ-controllable for any $\ell \geq m$ if and only if it is m-controllable.

On the other hand, the behavioral approach to system theory [9] [10] has revealed that controllability is, in a sense, optional. This is illustrated in Fig. 2: the trellis is minimal for the code that consists of the all-zeros sequence and the all-ones sequence. Rather than ruling out such codes a priori, you may freely choose whether or not to consider bi-infinite sequences through unreachable states as part of the valid behavior. In any case, it is at least required that the trellis is *state-trim*, which means that every state has both a successor and a predecessor (i.e., a bi-infinite path exists through every state); for ABCD-systems (1), the former is automatic and the latter holds if and only if the block matrix $[A, B]$ has rank m.

5 Minimality Simplified

A main result of [8] is a general version of Kalman's theorem (2) for group trellises. Its specialization to linear trellises reads as follows:

Theorem: ([8, Theorem 9], [1, Theorem 5.2]) A time-invariant linear trellis with an m-dimensional state space is minimal if and only if it is state-trim and m-observable.

The theorem applies both to traditional linear systems theory and to convolutional encoders: in the former case, the relevant trellis is the input-output trellis and observability is tested by the rank test of the observability matrix $\mathcal{O}$; in the latter case, the relevant trellis is the output-only trellis and observability is tested by the rank test of the matrix (5).

As discussed in Section 4, you may wish to replace state-trimness by the stronger condition of m-controllability.

6 Conclusion

By a suitable definition of observability, Kalman's formula *"minimal* $\Leftrightarrow$ *controllable and observable"* is now seen to apply also to convolutional encoders. The 35 years long separation between minimality in linear systems and minimality of convolutional encoders is finally overcome.

References

[1] H.-A. Loeliger and T. Mittelholzer, "Convolutional codes over groups," *IEEE Trans. Inform. Theory,* vol. 42, pp. 1660–1686, Nov. 1996.

[2] T. Kailath, *Linear Systems,* Prentice-Hall, 1980.

[3] R. E. Kalman, "On the general theory of control systems," in *Proc. First Int. Congress on Automatic Control,* Butterworth's, London, 1960, pp. 481–493.

[4] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.,* vol. 17, pp. 330–337, April 1968.

[5] G. D. Forney, Jr., "Convolutional codes I: algebraic structure," *IEEE Trans. Inform. Theory*, vol. 16, pp. 720–738, Nov. 1970, and vol. 17, p. 360, May 1971.

[6] G. D. Forney, Jr., "Correction to 'Convolutional Codes I: Algebraic Structure'," *IEEE Trans. Inform. Theory,* vol. 17, pp. 360, May 1971.

[7] G. D. Forney, Jr., R. Johannesson, and Z.-x. Wan, "Minimal and canonical rational generator matrices for convolutional codes," *IEEE Trans. Inform. Theory,* vol. 42, pp. 1865–1880, Nov. 1996.

[8] H.-A. Loeliger, G. D. Forney, Jr., T. Mittelholzer, and M. D. Trott, "Minimality and observability of group systems," *Linear Algebra* & *Appl.*, vol. 205–206, pp. 937–963, July 1994.

[9] J. C. Willems, "Models for dynamics," in *Dynamics Reported*, vol. 2, U. Kirchgraber and H. O. Walther, Eds., Wiley and Teubner, 1989.

[10] J. C. Willems, "Paradigms and puzzles in the theory of dynamical systems," *IEEE Trans. Aut. Contr.,* vol. 36, pp. 259–294, March 1991.