Информационные процессы, Том 1, № 1, 2004, стр. 8–12.
© *2004 Trushkin.*

State diagram approach to feedback encoders for tailbiting codes

A.V.Trushkin

Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia;
trushkin@iitp.ru

Received January 5, 2004

Abstract—An algorithm for finding the starting state of a feedback tailbiting encoder is proposed, based solely on the properties of the encoder state diagram. With this approach, conditions for the existence of a tailbiting code generated by such an encoder are naturally tested in the process of preparing a certain permutation table for the starting state determination algorithm. A tailbiting failure for a given information sequence length L is detected when this table fails to be a permutation, which occurs if L is divisible by a length of any zero-branch cycle through nonzero states of the state diagram.

1. INTRODUCTION

Tailbiting codes are block codes obtained from convolutional codes in such a way that the initial state of the convolutional encoder at the beginning of the codeword is equal to the final state at the end of the codeword. In [1], a rate $R = b/c$ tailbiting encoder with a rational generator matrix $G(D) = (g_{ij}(D)/q(D))$, where

$$g_{ij}(D) = g_{ij}^{(0)} + g_{ij}^{(1)}D + \cdots + g_{ij}^{(m)}D^m$$

and

$$q(D) = q^{(0)} + q^{(1)}D + \cdots + q^{(m)}D^m,$$

with $q^{(0)} = 1$, is described algebraically by the formula

$$\mathbf{v}(D) = \mathbf{u}(D)G(D) \mod 1 + D^L, \tag{1}$$

which maps length $K = bL$ binary information sequences

$$\mathbf{u}(D) = \mathbf{u}_0 + \mathbf{u}_1D + \cdots + \mathbf{u}_{L-1}D^{L-1}$$

to length $N = cL$ binary code sequences

$$\mathbf{v}(D) = \mathbf{v}_0 + \mathbf{v}_1D + \cdots + \mathbf{v}_{L-1}D^{L-1},$$

where $\mathbf{u}_t = (u_t^{(1)}, u_t^{(2)}, \ldots, u_t^{(b)})$ and $\mathbf{v}_t = (v_t^{(1)}, v_t^{(2)}, \ldots, v_t^{(c)})$.

Formula (1) can be realized (see [1, Fig. 1]) by a feedback convolutional encoder in controller canonical form with feedback polynomial $q(D)$ and tap coefficients $g_{ij}^{(k)}$, which generate code bit sequences $v_t^{(j)}$ using cyclic convolutions of $g_{ij}^{(k)}$ with state sequences $\sigma_t^{(i)}$ according to the formula

$$v_t^{(j)} = \sum_{i=0}^{b}\sum_{k=0}^{m} g_{ij}^{(k)}\sigma_{((t-k))}^{(i)}.$$

Here $((t-k)) = t-k \mod L$ and the ith state binary sequence $\sigma_t^{(i)}$ is implicitly defined by the ith information binary sequence $u_t^{(i)}$ via the equation

$$u_t^{(i)} = \sum_{k=0}^{m} q^{(k)} \sigma_{((t-k))}^{(i)}. \tag{2}$$

To realize the tailbiting coding rule embodied in (2), the starting state, i.e., the initial contents $(\sigma_{-1}^{(i)}, \sigma_{-2}^{(i)}, \ldots, \sigma_{-m}^{(i)})$, of each of the b encoder shift registers must be chosen in such a way that the final state $(\sigma_{L-1}^{(i)}, \sigma_{L-2}^{(i)}, \ldots, \sigma_{L-m}^{(i)})$ obtained by the recurrent formula

$$\sigma_t^{(i)} = u_t^{(i)} - \sum_{k=1}^{m} q^{(k)} \sigma_{t-k}^{(i)}.$$

is the same as the starting state. This can always be easily done in the case of a pure polynomial encoder, i.e., if $q(D) \equiv 1$, setting $\sigma_{-k}^{(i)} = u_{L-k}^{(i)}$, $k = 1, \ldots, m$. But this in neither so easy nor always possible in the case of a nontrivial feedback polynomial $q(D)$.

Theorem 1 in [1] states that a necessary and sufficient condition for the tailbiting code to exist is the requirement for both $q(D)$ and the determinant of $G(D)$ (as follows from [2, Th. 2.4]) to be relatively prime to the polynomial $1 + D^L$. But, actually, only the first condition—that $q(D)$ and $1 + D^L$ are relatively prime—is essential for the possibility of constructing the tailbiting code. The other simply guarantees that this code is nondegenerate, i.e., does not contain duplicate code vectors.

If $q(D)$ is relatively prime to $1 + D^L$, it is proposed in [1] to construct the starting state of the ith encoder shift register corresponding to a given ith information binary vector

$$u^{(i)}(D) = u_0^{(i)} + u_1^{(i)} D + \cdots + u_{L-1}^{(i)} D^{L-1}$$

from the m last bits $(\sigma_{L-1}^{(i)}, \sigma_{L-2}^{(i)}, \ldots, \sigma_{L-m}^{(i)})$ of the ith state binary vector

$$\sigma^{(i)}(D) = \sigma_0^{(i)} + \sigma_1^{(i)} D + \cdots + \sigma_{L-1}^{(i)} D^{L-1}$$

obtained from the equation

$$\sigma^{(i)}(D) = a(D) u^{(i)}(D) \mod 1 + D^L, \tag{3}$$

where $a(D)$ is the inverse of $q(D)$ modulo $1 + D$.

It is easy to see that the complexity of computing $a(D)$ by Euclid's algorithms (and thereby checking whether $q(D)$ and $1 + D^L$ are relatively prime) may amount to not less than $L - m + 1$ bit testings and additions of m-dimensional binary vectors, and that of solving equation (3) to L bit testings and additions of m-dimensional binary vectors. Since the former computation is solely needed on the preliminary stage of a preparation for the subsequent repeated usage of the tailbiting encoding/decoding, just the latter essentially determines the complexity of the practical solution of the starting state problem by the approach described. Also note that for moderate values of m—when m bits can be packed in one integer word—operations on m-dimensional binary vectors can be performed in their integer representation.

In the present paper, we consider another approach to the problem of finding the starting state for a feedback tailbiting encoder, of a comparable complexity but very natural from the practical point of view and based on investigating the properties of the encoder state diagram.

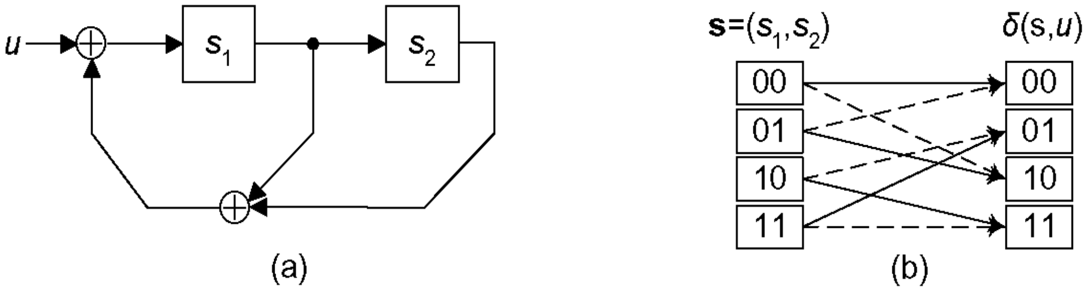

Fig. 1.
(a) The controller canonical form of a shift register for the feedback polynomial $q(D) = 1 + D + D^2$.
(b) The corresponding mapping $\delta(\mathrm{s}, u)$: solid and dotted lines denote edges for information bit $u = 0$ and $u = 1$, respectively.

2. STATE DIAGRAM AND STARTING STATE FOR TAILBITING

In what follows, we confine our consideration to the case of a rate $R = 1/c$ feedback encoder only. A generalization for the case of $R = b/c$ is straightforward.

Let S denote the set of all possible states of the encoder shift register, which are indexed by m-dimensional binary vectors $\mathrm{s} = (s_1, s_2, \ldots, s_m)$.

Definition 1. Let $\delta(\mathrm{s}, u)$ be the state after an information bit u is fed into the encoder being in a state s. Thus, $\mathrm{s}' = \delta(\mathrm{s}, u)$ is the result of the transition from the state s along the branch corresponding to the input u in the state diagram.

Since the problem of finding the starting state satisfying the tailbiting condition depends not on the generator polynomials defining the code bit values on the branches of the state diagram, but exclusively on the feedback polynomial $q(D)$, we consider solely the transition properties of the state diagram, which are represented by the function $\delta(\mathrm{s}, u)$. If $\mathrm{s}' = (s'_1, s'_2, \ldots, s'_m)$, then, obviously, $s'_i = s_{i-1}$, $i = 2, 3, \ldots, m$, and

$$s'_1 = u + \sum_{k=1}^{m} q^{(k)} s_k.$$

As an example, in Fig. 1, we show a shift register and the corresponding state diagram for the feedback polynomial $q(D) = 1 + D + D^2$.

Definition 2. Given an information sequence $\mathbf{u} = (u_0, u_1, \ldots, u_{L-1})$, let $\delta(\mathbf{s}, \mathbf{u})$ denote the final state after $\mathbf{u}$ is fed into the encoder being in a starting state s.

The following obvious linearity properties of $\delta(\mathbf{s}, u)$ and $\delta(\mathbf{s}, \mathbf{u})$ play the central role in the whole approach presented below.

Proposition 1. *If* $\mathrm{s} = \mathrm{s}' + \mathrm{s}''$, $u = u' + u''$, *and* $\mathbf{u} = \mathbf{u}' + \mathbf{u}''$, *then*

$$\delta(\mathrm{s}, u) = \delta(\mathrm{s}', u') + \delta(\mathrm{s}'', u'') \quad \text{and} \quad \delta(\mathrm{s}, \mathbf{u}) = \delta(\mathrm{s}', \mathbf{u}') + \delta(\mathrm{s}'', \mathbf{u}''). \tag{4}$$

Definition 3. Denote by $\delta_0(\mathrm{s})$ the state after a zero bit is fed into the encoder being in a state s:

$$\delta_0(\mathrm{s}) = \delta(\mathrm{s}, 0).$$

Thus, δ_0 is a linear operator in the linear space S, and its Lth power will be denoted by δ_0^L:

$$\delta_0^L(\mathrm{s}) = \delta(\mathrm{s}, \mathbf{0}),$$

where $\mathbf{0}$ denotes the all-zero information sequence of length L.

It follows from the linearity property that, for any $\mathbf{s}$ and $\mathbf{u}$,

$$\delta(\mathbf{s}, \mathbf{u}) = \delta(\mathbf{0}, \mathbf{u}) + \delta_0^L(\mathbf{s}),$$

where $\mathbf{0}$ denotes the zero starting state. Therefore, to find the starting state satisfying the tailbiting condition for the given information sequence $\mathbf{u}$, we need to solve the following tailbiting equation

$$\mathbf{s} - \delta_0^L(\mathbf{s}) = \delta(\mathbf{0}, \mathbf{u}). \tag{5}$$

Thus, if the linear operator

$$\varphi(\mathbf{s}) = \mathbf{s} - \delta_0^L(\mathbf{s}) \tag{6}$$

is nondegenerate, i.e., determines a linear permutation on the state space S, then its inverse, i.e., the operator ψ such that

$$\varphi(\psi(\mathbf{s})) \equiv \mathbf{s}, \tag{7}$$

can be tabulated in advance and used repeatedly in the following algorithm.

Algorithm for Finding the Starting State. The tailbiting starting state $\mathbf{s}$ can be found by applying the operator ψ to the final state after feeding the given information sequence $\mathbf{u}$ into the encoder starting from the zero state:

$$\mathbf{s} = \psi(\delta(\mathbf{0}, \mathbf{u}))). \tag{8}$$

Otherwise, if φ is degenerate, equation (5) has no solution for some $\mathbf{u}$'s and multiple solutions for the others, which makes tailbiting impossible. In the next section, we consider how the length L determines the validity of the tailbiting technique and how the operator ψ can be tabulated in an efficient way.

3. TAILBITING PREPARATION AND CONDITIONS OF ITS FAILURE

To begin with, let us note that the degree μ of the feedback polynomial $q(D)$ may be less than m. Denote by S^0 the space of all states $\mathbf{s}$ whose components $s_k = 0$, $k = 1, \dots, \mu$. It can be easily seen that, on the one hand, $\delta_0^{m-\mu}(\mathbf{s}) = \mathbf{0}$ for any $\mathbf{s} \in S^0$, and on the other, if $\mathbf{s} \notin S^0$, $\delta_0^k(\mathbf{s}) \neq \mathbf{0}$ for all k. Also denote by S' the set of all nonzero states that belong to cycles of the operator δ_0, i.e., that are such that the cycle length function

$$\ell(\mathbf{s}) = \min\{k > 0 : \delta_0^k(\mathbf{s}) = \mathbf{s}\}$$

is defined for them.

Obviously, if we start from an arbitrary nonzero state $\mathbf{s}$, then, for certain (as small as possible) nonnegative k and positive l, we will have that

$$\delta_0^k(\mathbf{s}) = \delta_0^{k+l}(\mathbf{s}).$$

Then, for any $k' \geq k$ and $\mathbf{s}' = \delta_0^{k'}(\mathbf{s})$, we have that $\mathbf{s}' \in S'$ and $\ell(\mathbf{s}') = l$. Denoting $l' = -k \mod l$, $k' = k + l'$, $\mathbf{s}' = \delta_0^{k'}(\mathbf{s})$, and $\mathbf{s}'' = \mathbf{s} - \mathbf{s}'$, we see that $k' \equiv 0 \pmod l$, whence $\delta_0^k(\mathbf{s}') = \delta_0^{k'}(\delta_0^k(\mathbf{s})) = \delta_0^k(\mathbf{s})$, so that $\delta_0^k(\mathbf{s}'') = 0$. Thus, it appears that $\mathbf{s} = \mathbf{s}' + \mathbf{s}''$, where $\mathbf{s}' \in S'$ and $\mathbf{s}'' \in S^0$. Since $\delta_0^m(\mathbf{s}'') = \mathbf{0}$ for any $\mathbf{s}'' \in S^0$, we obtain that $\delta_0^m(\mathbf{s}) \in S'$ for any $\mathbf{s} \in S$.

As a result, we obtain that, for any $\mathbf{s}$ and $\mathbf{s}' = \delta_0^m(\mathbf{s})$, we have two alternatives: either $\mathbf{s}' = \mathbf{0}$, which means that $\mathbf{s} \in S^0$, or $\mathbf{s}' \in S'$. In this way, we can distinguish states belonging to S' among all states not belonging to S^0. Knowing that a state $\mathbf{s}' \in S'$, we can effectively determine all other elements in its cycle and the length of the cycle.

Thus, during the preparatory stage, we can indicate for every state $\mathbf{s}$ whether it belongs to S^0, to S' (remembering its cycle length and the position in the cycle, which is also kept in memory), or to neither of them (pointing out the value of $\mathbf{s}' = \delta_0^m(\mathbf{s}) \in S'$). Afterwards, given a specific value of the information sequence length $L \geq m$, we can use this information in order to compile a table of values of the operator ψ and determine conditions for tailbiting failure as follows.

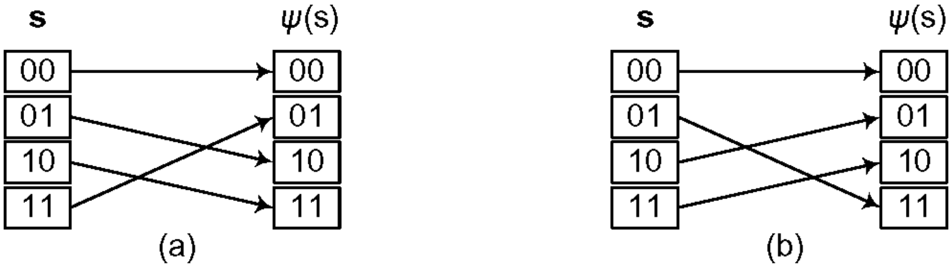

Fig. 2. Mapping $\psi(\mathrm{s})$ for $q(D) = 1 + D + D^2$ in the cases of (a) $L \equiv 1 \pmod 3$ and (b) $L \equiv 2 \pmod 3$.

Tailbiting Preparation and Failure Conditions for a Specific L. For filling the table of values of the operator ψ for a given $L \geq m$, we need to know the values $\delta_0^L(\mathrm{s})$. If $\mathrm{s} \in S^0$, then $\delta_0^L(\mathrm{s}) = \mathbf{0}$. If $\mathrm{s} \in S'$ and we already know its cycle length and the index n of s in an array $\mathbf{c}$ representing the corresponding cycle, then $\delta_0^L(\mathrm{s}) = \mathbf{c}[(n + L) \mod \ell(\mathrm{s})]$. Finally, if $\mathrm{s} \notin S^0 \cup S'$ and we already know the state value $s' = \delta_0^m(\mathrm{s}) \in S'$, then $\delta_0^L(\mathrm{s}) = \delta_0^{L-m}(\mathrm{s}')$. Next, we put the value s in the table for ψ at the position with index $\varphi(\mathrm{s})$ given by (6). Such a procedure defines all values of the operator ψ if φ is nondegenerate, which is true if and only if the operator δ_0^L has no nonzero fixed points, i.e., no $\mathrm{s} \in S'$ with $\delta_0^L(\mathrm{s}) = \mathrm{s}$. Thus, the necessary and sufficient condition for tailbiting to fail is that L is a multiple of the length of some cycle of the operator δ_0.

In the example of $q(D) = 1 + D + D^2$, as can be seen from Fig. 1, $S^0 = \{\mathbf{0}\}$, $S' = S \setminus S^0$, and $\ell(\mathrm{s}) = 3$ for all $\mathrm{s} \neq \mathbf{0}$. Thus, δ_0^L is always a permutation, which has no fixed points in S' if $L \not\equiv 0 \pmod 3$. For these cases, the form of the mapping ψ is shown in Fig. 2.

4. CONCLUSION

In the paper, it is shown that a feedback convolutional encoder of memory m can generate a tailbiting code for a specific information sequence length L if and only if L is not divisible by the lengths of all zero-branch cycles of the encoder state diagram. The corresponding starting state for a given information sequence is found in L operations of information bit testing and state diagram transition followed by reading an element in a length 2^m table of m-dimensional binary vectors.

Actually, the whole construction for finding the starting state of a tailbiting code and the conditions of its existence are valid for any linear trellis code with identical sections generated by an arbitrary time-invariant linear state diagram, i.e., by any $\delta(\mathrm{s}, u)$ that satisfies (4).

The author is grateful to V.R.Sidorenko for invoking the author's interest to the problem and some considerations concerning the form of the solution and to Prof. R.Johannesson for valuable comments.

REFERENCES

1. Stahl P., Anderson J.B., Johannesson R. A Note on Tailbiting Codes and Their Feedback Encoders. *IEEE Trans. Inf. Theory*, 2002, vol. 48, no. 2, pp. 529–534.

2. Johannesson R., Zigangirov K.Sh. *Fundamentals of Convolutional Coding*, Piscataway, NJ:IEEE Press, 1999.

This paper was recommended for publication by V.V.Zyablov, a member of the Editorial Board