Dual convolutional codes and the MacWilliams identities

Bocharova, Irina; Hug, Florian; Johannesson, Rolf; Kudryashov, Boris

Published in:
Problems of Information Transmission

DOI:
10.1134/S0032946012010036

2012

A Note on Duality and MacWilliams-type Identities for Convolutional Codes[1]

I. E. Bocharova[a], F. Hug[b], R. Johannesson[b], and B. D. Kudryashov[a]

[a] *St. Petersburg State University of Information Technologies, Mechanics and Optics (ITMO)*
irina@eit.lth.se boris@eit.lth.se
[b] *Lund University, Sweden*
florian@eit.lth.se rolf@eit.lth.se

Abstract—A recursion for sequences of spectra of truncated as well as tailbitten convolutional codes and their duals is derived. The order of this recursion is shown to be less than or equal to the rank of the weight adjacency matrix (WAM) for the minimal encoder of the convolutional code. It is enough to know a finite number of spectra of these terminated convolutional codes in order to obtain an infinitely long sequence of spectra of their duals.

Key words: Convolutional codes, free distance spectrum, MacWilliams identity, spectrum, Viterbi spectrum

1. INTRODUCTION

Following [1] we define a rate $R = b/c$ binary convolutional code over the field $\mathbb{F}_2$ as the image set of the linear mapping represented by

$$\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D)$$

where the code sequence $\boldsymbol{v}(D)$ and information sequence $\boldsymbol{u}(D)$ are c- and b-tuples over the fields of Laurent series, $\mathbb{F}_2^c((D))$ and $\mathbb{F}_2^b((D))$, respectively, and the generator matrix $G(D)$, over the field of rational functions $\mathbb{F}_2(D)$, has full rank.

Convolutional codes are often thought of as nonblock linear codes over a finite field. Sometimes, however, it is an advantage to regard convolutional codes as block codes over certain infinite fields; that is, as the $\mathbb{F}_2(D)$ row space of $G(D)$ or, in other words, as a rate $R = b/c$ block code over the infinite field of Laurent series encoded by $G(D)$. From this point of view it seems rather natural that convolutional codes would have similar properties as block codes and satisfy proper reformulations of theorems valid for block codes.

Let the free distance be denoted by d_{free}. Then the path weight enumerator of a convolutional encoder introduced by Viterbi [2] is the generating function $T(W) = \sum_{i=0}^{\infty} n_{d_{\text{free}}+i} W^{d_{\text{free}}+i}$ of the Hamming weights of the paths which diverge from the allzero path at the root in the trellis representation of the encoder and terminate in the zero state, but do not merge with the allzero path until their termini. In the sequel we call the sequence $n_{d_{\text{free}}+i}$, $i = 0, 1, 2, \ldots$, the *free distance spectrum* or *Viterbi spectrum* in order to distinguish it from the spectrum of block codes. It is well-known, starting with the paper by Shearer and McEliece [3], that MacWilliams identity [4] does not

[1] Supported in part by the Swedish Research Council, Grant no. 621-2007-6281.

hold for the free distance spectra of convolutional encoders. In [5], [6], and [7], MacWilliams-type identities were established, not for the free distance spectrum but for the so-called weight adjacency matrix (WAM) [8]. In particular, a MacWilliams-type identity with respect to WAMs for the encoders of an arbitrary convolutional code and its dual was formulated in [6] and proved in [7] by Gluesing-Luerssen and Schneider. Their work inspired Forney, and in [9] and [10] he proved their results in terms of the "constraint" code corresponding to each node of the trellis diagram and its dual. Moreover, he generalized them to the complete WAM (CWAM) and to group codes defined on graphs.

In [11] we showed that the MacWilliams identity is valid for the spectra of truncated convolutional codes and their reverse-truncated duals. Forney [12] extended this approach to tailbiting as a termination procedure. The recursive nature of convolutional encoders led us to study an infinite sequence of spectra of truncated or tailbitten convolutional codes and a relation between the infinite sequences of spectra obtained by truncating or tailbiting a convolutional code and its dual. Since in practice we always deal with some kind of terminated convolutional code it is important to know the spectra of the corresponding terminations (block codes) of different lengths. Certainly, they can be computed for both the parent convolutional code and its dual via their encoder WAMs with complexity of order $|\Sigma| = 2^{\nu}$, where ν is the overall constraint length of the minimal encoder. However, the sparsity of WAMs, that is, the number of nonzero terms in each row of a WAM can be very different for convolutional codes and their duals. This circumstance motivated us to search for a procedure which would yield an arbitrary long sequence of spectra of terminations of a dual code by using only the WAM of the encoder of the corresponding convolutional code and applying a MacWilliams-type identity to the finite sequence of spectra of its terminations.

The rest of the paper is organized as follows. Notions of duality for convolutional codes as well as different MacWiliams-type identities valid for convolutional codes are revisited in Section 2. In Section 3, we prove that the spectra of a truncated or tailbitten convolutional code and the spectra of the corresponding terminations of its dual satisfy recursions of an order less than or equal to the rank r of the WAM of the minimal encoder of the convolutional code. It is shown that it is enough to know $2r$ consecutive spectra of block codes obtained by truncating or tailbiting a convolutional code at lengths $c, 2c, \ldots, 2rc$ in order to find the infinite sequence of spectra of block codes which are terminations of the corresponding dual and vice-versa. Some final remarks are given in Section 4.

2. MACWILLIAMS-TYPE IDENTITIES

We start with recalling MacWilliams identity for block codes [4]:

Let $\mathcal{C}$ be a binary block code of rate $R = k/n$ and let $\mathcal{C}^{\perp}$ be its dual of rate $R = (n-k)/n$. Then their spectra satisfy

$$\mathcal{S}_{\mathcal{C}^{\perp}}(x, y) = \frac{1}{2^k}\mathcal{S}_{\mathcal{C}}(x+y, x-y) \tag{1}$$

where

$$\mathcal{S}_{\mathcal{C}}(x, y) = \sum_{\boldsymbol{v}\in\mathcal{C}} x^{n-w_{\mathrm{H}}(\boldsymbol{v})} y^{w_{\mathrm{H}}(\boldsymbol{v})}$$

and $w_{\mathrm{H}}(\boldsymbol{v})$ is the Hamming weight of the sequence $\boldsymbol{v}$.

Consider the rate $R = b/c$ convolutional code $\mathcal{C}$ encoded by the semi-infinite generator matrix $\boldsymbol{G}$ of memory m

$$\boldsymbol{G} = \begin{pmatrix} G_0 & G_1 & G_2 & \cdots & G_m & & \\ & G_0 & G_1 & \cdots & G_{m-1} & G_m & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}$$

where G_i, $i = 0, 1, \ldots, m$, is a binary matrix of size $b \times c$. The corresponding polynomial generator matrix is given by

$$G(D) = G_0 + G_1 D + \cdots + G_{m-1} D^{m-1} + G_m D^m.$$

A natural approach to study duality and MacWilliams-type identities for convolutional codes is based on obtaining sequences of block codes from a parent convolutional code and applying the MacWilliams identity to these block codes. The simplest method is called *truncation* and yields a block code with codewords corresponding to the paths of code trellis starting in the zero state at time 0 and ending in any state after t branches. The corresponding generator matrix is

$$\boldsymbol{G}_t^{(\mathrm{tr})} = \begin{pmatrix} G_0 & G_1 & G_2 & \cdots & G_m & & & \\ & G_0 & G_1 & \cdots & G_{m-1} & G_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & G_0 & G_1 & G_2 & \cdots & G_m \\ & & & & G_0 & G_1 & \cdots & G_{m-1} \\ & & & & & \ddots & \ddots & \vdots \\ & & & & & & & G_0 \end{pmatrix}.$$

Zero-tail termination produces a block code whose codewords are represented by the paths starting in the zero state and ending in the zero state after $t + m$ branches. Its generator matrix has the form

$$\boldsymbol{G}_t^{(\mathrm{zt})} = \begin{pmatrix} G_0 & G_1 & G_2 & \cdots & G_m & & & \\ & G_0 & G_1 & \cdots & G_{m-1} & G_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & G_0 & G_1 & \cdots & G_{m-1} & G_m \end{pmatrix}.$$

Finally, using *tailbiting* [1] at length t, we obtain a block code whose generator matrix is given by

$$\boldsymbol{G}_t^{(\mathrm{tb})} = \begin{pmatrix} G_0 & G_1 & G_2 & \cdots & G_m & & & \\ & G_0 & G_1 & \cdots & G_{m-1} & G_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & G_0 & G_1 & G_2 & \cdots & G_m \\ G_m & & & & G_0 & G_1 & \cdots & G_{m-1} \\ \vdots & \ddots & & & & \ddots & \ddots & \vdots \\ G_1 & \cdots & G_m & & & & & G_0 \end{pmatrix}.$$

This code contains the codewords corresponding to the paths in the code trellis starting in any state at time 0 and ending after t branches in the same state as they started in.

Next we discuss two definitions of duality for convolutional codes [13].

Definition 1. A *dual code* $\mathcal{C}^\perp$ to a rate $R = b/c$ convolutional code $\mathcal{C}$ is the set of all c-tuples of sequences $\boldsymbol{v}^\perp$ such that the inner product

$$(\boldsymbol{v}, \boldsymbol{v}^\perp) = \boldsymbol{v}(\boldsymbol{v}^\perp)^{\mathrm{T}} = 0 \tag{2}$$

that is, $\boldsymbol{v}$ and $\boldsymbol{v}^\perp$ are orthogonal for all $\boldsymbol{v}$ in $\mathcal{C}$.

The dual code $\mathcal{C}^\perp$ of a rate $R = b/c$ convolutional code is a rate $R = (c-b)/c$ convolutional code encoded by the semi-infinite generator matrix $\boldsymbol{G}^\perp$ which satisfies

$$\boldsymbol{G}\left(\boldsymbol{G}^\perp\right)^{\mathrm{T}} = \boldsymbol{0}. \tag{3}$$

Moreover, it is a vector space of dimension $c - b$ over $\mathbb{F}_2((D))$. In [7], the *dual code* $\mathcal{C}^\perp$ is called *sequence space dual*.

Definition 2. The *convolutional dual code* $\mathcal{C}_\perp$ to a convolutional code $\mathcal{C}$, which is encoded by the rate $R = b/c$ generator matrix $G(D)$, is the set of all codewords encoded by any rate $R = (c-b)/c$ generator matrix $G_\perp(D)$ such that

$$G(D)G_\perp^{\mathrm{T}}(D) = \mathbf{0}. \tag{4}$$

In [7], the *convolutional dual code* $\mathcal{C}_\perp$ is called *module-theoretic dual*.

In other words, Definition 1 is related to the orthogonality of the vectors $(G_0,G_1,\ldots,G_m)$ and $(G_0^\perp,G_1^\perp,\ldots,G_{m^\perp}^\perp)$ while Definition 2 is based on the orthogonality of the polynomials $G(D)$ and $G_\perp(D)$. Notice that for two arbitrary polynomials $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ and $b(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ it follows from the equality $a(x)b(x) = 0$, that $(\boldsymbol{a}, \overleftarrow{\boldsymbol{b}}) = 0$ but in general $(\boldsymbol{a}, \boldsymbol{b}) \neq 0$, where $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\overleftarrow{\boldsymbol{b}} = (b_{n-1}, b_{n-2}, \ldots, b_0)$.

Since we deal with a particular case of the above statement, it can be easily shown that the polynomial generator matrix $G^\perp(D)$ of the *dual code* $\mathcal{C}^\perp$ is the *reversal* with respect to the polynomial generator matrix $G_\perp(D)$ of the *convolutional dual code* $\mathcal{C}_\perp$, that is,

$$G^\perp(D) = G_\perp(D^{-1})D^{m_\perp} = \overleftarrow{G}_\perp(D)$$

where

$$G^\perp(D) = G_0^\perp + G_1^\perp D + \cdots + G_{m^\perp}^\perp D^{m^\perp}$$

and

$$\overleftarrow{G}_\perp(D) = G_{m_\perp,\perp} + G_{m_\perp-1,\perp}D + \cdots + G_{0,\perp}D^{m_\perp}$$

from which $G_j^\perp = G_{m_\perp-j,\perp}$, $j = 0,1,\ldots,m^\perp$ and $m_\perp = m^\perp$ follow. In general, the *dual code* and the corresponding *convolutional dual code* are different.

Next, we show that MacWilliams identity for convolutional codes can be interpreted in different ways. First, we consider how it can be applied to the sequence of terminated codes $\mathcal{C}_t$ and analyze which termination procedure does not violate (2).

It is easy to verify that for zero-tail terminating as well as tailbiting (2) is not violated. However, duals of zero-tail terminated convolutional codes are not zero-tail terminated convolutional dual codes since terminations to length $t+m$ and $t+m^\perp$ of $\boldsymbol{G}$ and $\boldsymbol{G}^\perp$, respectively, yield generator matrices of the two block codes of rates $tb/(t+m)c$ and $t(c-b)/(t+m^\perp)c$ which are not duals of each other.

At the same time, it can be easily shown that truncation by t of $\boldsymbol{G}$ and $\boldsymbol{G}^\perp$ yields the $t \times t$ matrices $\boldsymbol{G}_t^{(\mathrm{tr})}$ and $\boldsymbol{G}_t^{(\mathrm{tr})\perp}$, respectively, such that

$$\boldsymbol{G}_t^{(\mathrm{tr})}(\boldsymbol{G}_t^{(\mathrm{tr})\perp})^{\mathrm{T}} \neq \mathbf{0}$$

that is, the truncated versions of $\mathcal{C}$ and $\mathcal{C}^\perp$ are not orthogonal since the last $t-m+1$ rows of $\boldsymbol{G}_t^{(\mathrm{tr})}$ as well as the last $t-m^\perp+1$ rows of $\boldsymbol{G}_t^{(\mathrm{tr})\perp}$ are not complete, that is, they do not contain all submatrices G_i, $i = 0,1,\ldots,m$, and not all submatrices $G_i^\perp$, $i = 0,1,\ldots,m^\perp$, respectively. The products of these incomplete rows are equal to incomplete matrix convolutions.

Let

$$\overleftarrow{\boldsymbol{G}}_t^{(\mathrm{tr})\perp} = \begin{pmatrix} G_{m^\perp}^\perp & & & & & & \\ G_{m^\perp-1}^\perp & G_{m^\perp}^\perp & & & & & \\ \vdots & \vdots & \ddots & & & & \\ G_0^\perp & G_1^\perp & \cdots & G_{m^\perp}^\perp & & & \\ & G_0^\perp & \cdots & G_{m^\perp-1}^\perp & G_{m^\perp}^\perp & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & G_0^\perp & \cdots & G_{m^\perp-1}^\perp & G_{m^\perp}^\perp \end{pmatrix} \tag{5}$$

be the generator matrix of the dual code $\mathcal{C}^\perp$ reverse-truncated by t. Then we obtain

$$\boldsymbol{G}_t^{(\mathrm{tr})}(\overleftarrow{\boldsymbol{G}}_t^{(\mathrm{tr})\perp})^{\mathrm{T}} = \boldsymbol{0}.$$

Remark: Notice that $\overleftarrow{\boldsymbol{G}}_t^{(\mathrm{tr})\perp}$ is *not* a generator matrix of a truncated convolutional code. However, if we write both the rows and the columns of $\overleftarrow{\boldsymbol{G}}_t^{(\mathrm{tr})\perp}$ in reversed order we obtain the truncated reversal of $\boldsymbol{G}_t^{(\mathrm{tr})\perp}$ as

$$\begin{pmatrix}
G_{m^\perp}^\perp & \cdots & G_1^\perp & G_0^\perp & & & \\
 & G_{m^\perp}^\perp & \cdots & G_1^\perp & G_0^\perp & & \\
 & & \ddots & \ddots & \ddots & \ddots & \\
 & & & G_{m^\perp}^\perp & \cdots & G_1^\perp & G_0^\perp \\
 & & & & G_{m^\perp}^\perp & \cdots & G_1^\perp \\
 & & & & & \ddots & \vdots \\
 & & & & & & G_{m^\perp}^\perp
\end{pmatrix}$$

which is a generator matrix of a truncated convolutional code.

Since terminated (truncated and tailbitten) convolutional codes and their duals are block codes, clearly their spectra satisfy MacWilliams identity.

The spectra of the corresponding zero-tail terminated, truncated, and tailbitten convolutional codes can be computed via the $2^\nu \times 2^\nu$ weight adjacency matrix $A(W) \in \mathbb{Z}[W]^{|\Sigma|\times|\Sigma|}$, $|\Sigma| = 2^\nu$ of the encoder of the parent convolutional code (see, e.g., [8]), whose entries are generating functions of the formal variable W. Its (i,j)th entry is a sum of monomials, $\sum_w W^w$, whose degrees w are determined by the Hamming weights w of all parallel branches connecting states i and j in the state diagram. Such an entry is a monomial in case of only one connecting branch and zero if there is no connection.

Since the (i,j)th entry of $A(W)^t$ is a generating function of the Hamming weights of paths of length t branches going from state i to state j, the spectra of the corresponding zero-tail terminated, truncated, and tailbitten convolutional codes are

$$B_t^{(\mathrm{zt})}(W) = \boldsymbol{z}A(W)^t\boldsymbol{z}^{\mathrm{T}} \tag{6}$$

$$B_t^{(\mathrm{tr})}(W) = \boldsymbol{z}A(W)^t\boldsymbol{1}^{\mathrm{T}} \tag{7}$$

$$B_t^{(\mathrm{tb})}(W) = \mathrm{Tr}\left(A(W)^t\right) \tag{8}$$

where $\boldsymbol{z}$=(1 0 ... 0) and $\boldsymbol{1}$=(1 1 ... 1) are row vectors of length 2^ν, $B_t^{(\cdot)}(W) \in \mathbb{Z}[W]$.

It was shown in [11] that t-truncated convolutional codes and their duals, which are block codes of rates b/c and $(c-b)/c$, respectively, satisfy (1) with $n = ct$ and $k = bt$. Equivalently, (1) can be written as

$$\sum_{i=0}^{ct} A_i^\perp x^{ct-i}y^i = \frac{1}{2^{bt}}\sum_{i=0}^{ct} A_i(x+y)^{ct-i}(x-y)^i$$

with

$$\boldsymbol{z}A(W)^t\boldsymbol{1}^{\mathrm{T}} = \sum_{i=0}^{ct} A_i W^i \tag{9}$$

and

$$\boldsymbol{1}A^\perp(W)^t\boldsymbol{z}^{\mathrm{T}} = \sum_{i=0}^{ct} A_i^\perp W^i \tag{10}$$

where $A(W)$ and $A^{\perp}(W)$ are WAMs obtained from the state-transition diagrams for the minimal encoders of $\mathcal{C}$ and $\mathcal{C}^{\perp}$, respectively. In [10] it was shown that the same holds for tailbiting codes.

In [7] and [10] another interpretation of MacWilliams-type identities for convolutional codes is considered. In particular, MacWilliams-type identities with respect to the WAMs of the minimal encoders of the dual code $C^{\perp}$ and convolutional dual code $\mathcal{C}_{\perp}$ are proven. For simplicity of notations we present the results of [7], [10] for binary convolutional codes only. It is shown that

$$A^{\perp}(W) = 2^{-b}(1+W)^{c} H A\left(\frac{1-W}{1+W}\right) H^{\mathrm{T}} \tag{11}$$

and

$$A_{\perp}(W) = 2^{-b}(1+W)^{c} H A^{\mathrm{T}}\left(\frac{1-W}{1+W}\right) H^{\mathrm{T}} \tag{12}$$

where

$$H = \left\{(-1)^{(\boldsymbol{u}_i, \boldsymbol{u}_j)}\right\},\ i,j = 0,1,\ldots,2^{\nu}-1$$

is the Hadamard transform matrix, ν is the overall constraint length of the convolutional code $\mathcal{C}$, and $\boldsymbol{u}_i$ is a binary row vector of length ν.

The following example illustrates the considered notions of duality for the convolutional code analyzed in [3] where the absence of the MacWilliams identity for the free distance spectra was stated.

Example 1. Shearer and McEliece [3] considered the rate $R = 1/3$ convolutional code encoded by the polynomial generator matrix

$$G(D) = \begin{pmatrix} 1 & D & 1+D \end{pmatrix} \tag{13}$$

and its convolutional dual code encoded by the polynomial generator matrix

$$G_{\perp}(D) = \begin{pmatrix} 1 & 1 & 1 \\ D & 1 & 0 \end{pmatrix}. \tag{14}$$

They showed that the MacWilliams identity does not hold for the free distance spectra of their minimal encoders. We consider, however, the generator matrix of the dual of (13) given in minimal-basic form

$$G^{\perp}(D) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1+D & 1 \end{pmatrix}. \tag{15}$$

It is easy to verify that $G(D)(G^{\perp}(D))^{\mathrm{T}} \neq \mathbf{0}$ but for the corresponding codewords we have

$$\boldsymbol{v}\left(\boldsymbol{v}^{\perp}\right)^{\mathrm{T}} = 0.$$

The WAM for (13) realized in controller canonical form is

$$A(W) = \begin{pmatrix} 1 & W^2 \\ W^2 & W^2 \end{pmatrix}. \tag{16}$$

Applying (11) and (12) with

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{17}$$

yields the WAM of the minimal encoder of the convolutional dual and dual of (13)

$$A_{\perp}(W) = A^{\perp}(W) = \begin{pmatrix} 1+W^3 & W+W^2 \\ W+W^2 & W+W^2 \end{pmatrix} \tag{18}$$

which are, in general, the transpose of each other.

3. INFINITE SEQUENCES OF SPECTRA

In this section a recursion for spectra of sequences of truncated as well as tailbitten convolutional codes is derived. It is proven that the order of this recursion is less than or equal to the rank of the WAM of the minimal encoder of the parent convolutional code.

Let the sequence of (block code) spectra for both terminations be given by

$$B_t(W) = B_0 + B_1 W + \cdots + B_{ct} W^{ct},\ t = 0, 1, 2, \ldots$$

where

$$B_i = \begin{cases} A_i, & \text{for truncated codes} \\ T_i, & \text{for tailbiting codes} \end{cases}$$

with

$$\mathrm{Tr}\left(A(W)^t\right) = \sum_{i=0}^{ct} T_i W^i.$$

Remark 1. The spectral components B_k can be obtained from the spectral components $B_i^{\perp}$, $i = 0, 1, \ldots, ct$, of the dual code $\mathcal{C}_t^{\perp}$ as

$$B_k = \frac{1}{2^{ct}} \sum_{i=0}^{ct} B_i^{\perp} P_k(i),\ k = 0, 1, \ldots, ct \tag{19}$$

where $P_k(i)$ is a Krawtchouk polynomial [4].

Then the following theorem holds:

Theorem 1. *Let $\mathcal{C}$ be a rate $R = b/c$ convolutional code whose minimal encoder WAM $A(W)$ has rank r and let $\mathcal{C}_t$ be a truncation or tailbiting of $\mathcal{C}$. Then there exists an integer $l \leq r$ such that the (block code) spectra of $\mathcal{C}_t$ satisfy*

$$B_t(W) = \sum_{i=1}^{l} a_i(W) B_{t-i}(W),\ t = l, l+1, \ldots$$

where $a_i(W)$, $i = 1, 2, \ldots, r$, are the coefficients of the characteristic equation for $A(W)$.

Proof. Any matrix over a commutative ring satisfies its Hamilton-Cayley (characteristic) equation [14, Ch. 7, p.62]. Since $A(W)$ has size $2^\nu \times 2^\nu$ it satisfies the equation

$$\det\left(A(W) - \lambda I\right) = \lambda^{2^\nu} - \sum_{i=1}^{2^\nu} a_i(W) \lambda^{2^\nu - i} = 0 \tag{20}$$

where λ is a formal variable. Thus, we have

$$A(W)^{2^\nu} = \sum_{i=1}^{2^\nu} a_i(W) A(W)^{2^\nu - i}. \tag{21}$$

Multiplying both sides of (21) by $A(W)^k$, $k = 0, 1, 2, ...$, yields the following recurrent equation

$$A(W)^t = \sum_{i=1}^{2^\nu} a_i(W) A(W)^{t-i},\ t = 2^\nu, 2^\nu + 1, \ldots. \tag{22}$$

Assuming $A(W)$ has rank r, all of its minors of order higher than or equal to $r+1$ are zero and there exists at least one nonzero minor of order r. It is straightforward to show that the coefficient

Table 1. Coefficients of the recursions in Example 2

i	$a_i(W)$	$a_i^{\perp}(W)$
1	$1+W^2$	$1+W+W^2+W^3$
2	W^4-W^2	$2W^3-W^5-W$
3	W^2-W^6	$W+W^2-W^3-W^4-W^5-W^6+W^7+W^8$
4	$3W^6-2W^4-W^2$	$-W-3W^2-W^3+4W^4+2W^5-2W^6+2W^7+$ $4W^8-W^9-3W^{10}-W^{11}$
5	$W^{12}+W^{10}-3W^8-W^6+2W^4$	$3W^2-W^3-5W^4-W^5-2W^6+6W^7+6W^8-2W^9$ $-W^{10}+5W^{11}-W^{12}+3W^{13}$
6	$-W^{14}-W^{12}+2W^{10}$ $+2W^8-W^6-W^4$	$-2W^2+2W^4+6W^6-6W^8-6W^{10}$ $+6W^{12}+2W^{14}-2W^{16}$
7	0	0
8	$W^{16}-W^{14}-2W^{12}+2W^{10}$ $+W^8-W^6$	$-W^3-2W^4+6W^5+8W^6-8W^8-8W^9-$ $8W^{10}+6W^{11}+20W^{12}+6W^{13}-8W^{14}$ $-8W^{15}-8W^{16}+8W^{18}+3W^{19}-2W^{20}-W^{21}$
9	$-W^{18}+3W^{14}-3W^{10}+W^6$	$W^3+3W^4-8W^6-9W^7-3W^8+8W^9+24W^{10}$ $+18W^{11}-10W^{12}-24W^{13}-24W^{14}-10W^{15}+18W^{16}$ $+24W^{17}+8W^{18}-3W^{19}-9W^{20}-8W^{21}+3W^{23}+W^{24}$

$a_i(W)$ of the characteristic equation (20) is completely determined by the $\binom{2^\nu}{i}$ principal minors of order i. Thus, we can conclude that all $a_i(W)$ for $i=r+1,r+2,\ldots,2^\nu$ are zero and that (22) can be reduced to

$$A(W)^t=\sum_{i=1}^{r}a_i(W)A(W)^{t-i},\ t=r,r+1,\ldots. \tag{23}$$

Multiplying both sides of (23) by $\boldsymbol{z}$ and $\mathbf{1}^{\mathrm{T}}$ from the left and right, respectively, we obtain that the spectrum $B_t^{(\mathrm{tr})}(W)=\boldsymbol{z}A(W)^t\mathbf{1}^{\mathrm{T}}$ satisfies the main statement of Theorem 1.

Denote by $\boldsymbol{e}_k$ a row vector of length 2^ν with a one in the kth position and zeros elsewhere. Multiplying (23) by $\boldsymbol{e}_k$ and $\boldsymbol{e}_k^{\mathrm{T}}$ from the left and right, respectively, we obtain that the statement of Theorem 1 is valid for $\boldsymbol{e}_kA(W)^t\boldsymbol{e}_k^{\mathrm{T}}$.

Taking into account that

$$\sum_{k=1}^{2^\nu}\boldsymbol{e}_kA(W)^t\boldsymbol{e}_k^{\mathrm{T}}=\mathrm{Tr}\left(A(W)^t\right)$$

we obtain

$$\mathrm{Tr}\left(A(W)^t\right)=\sum_{i=1}^{r}a_i(W)\,\mathrm{Tr}\left(A(W)^{t-i}\right),\ t=r,r+1,\ldots. \tag{24}$$

Thus, we conclude that the main statement of Theorem 1 is valid for the spectra $B_t^{(\mathrm{tb})}$ of tailbiting codes. If a nonzero minor of order r is not a principal minor of $A(W)$, then the order of (23) can be less than r. □

It follows from Theorem 1 that for the spectra of truncation as well as tailbiting both codes, $\mathcal{C}_t$ and $\mathcal{C}_t^{\perp}$, satisfy the recursion of the same order l but with different coefficients, namely the coefficients of the Hamilton-Cayley equations for $A(W)$ and $A^{\perp}(W)$, respectively. Since the coefficients of a recurrent equation over $\mathbb{Z}[W]$ of order l can be found from $2l$ output values by solving a system of l linear equations, $2l$ spectra of terminated codes are enough to find the recursion for the sequence

of the spectra of their duals and vice versa. Notice that in general such a system of linear equations can be solved with reduced complexity by applying the Berlekamp-Massey algorithm [15][1].

The following example illustrates the statement of Theorem 1.

Example 2. Consider a rate $R = 1/3$ convolutional code encoded by the generator matrix

$$G(D) = \left(\begin{array}{ccc} 1 + D + D^2 + D^3 + D^4 & 1 + D + D^4 & 1 + D^3 \end{array} \right).$$

The WAM of its minimal encoder realized in controller canonical form is

$$A(W) = \left(\begin{array}{cccccccccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ W^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & W & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & W^2 \end{array} \right).$$

The matrix $A(W)$ does not have full rank $2^\nu = 2^4 = 16$, but rank $r = 12$. (The eight rows i and $i + 1$, $i = 5, 7, 9, 11$, of $A(W)$ are pairwise linearly dependent.) It is easy to verify that the spectra of the sequence of the truncated convolutional codes satisfy the system of linear equations

$$B_t^{\rm tr}(W) = \sum_{i=1}^{l} a_i(W) B_{t-i}^{\rm tr}(W),\ t = l, l + 1, \ldots, 2l - 1 \tag{25}$$

of order $l = 9$, where the spectrum $B_t^{\rm tr}(W)$ is computed according to (7). By solving (25) we obtain the coefficients $a_i(W)$, $i = 1, 2, \ldots, 9$. Thus, according to Theorem 1, for any finite t the spectra of the truncated sequence of the convolutional codes satisfy the equation of order $l = 9$ with coefficients $a_i(W)$, $i = 1, 2, \ldots, 9$, presented in the second column of Table 1.

By applying MacWilliams identity to the sequence of the spectra $B_0^{\rm tr}$, $B_1^{\rm tr}$,...,$B_{2l-1}^{\rm tr}$ we find the sequence of the spectra $B_0^{{\rm tr}\perp}$, $B_1^{{\rm tr}\perp}$,...,$B_{2l-1}^{{\rm tr}\perp}$ of the corresponding reverse truncations of the dual code. Inserting them into (25) with coefficients $a_i^\perp(W)$, $i = 1, 2, \ldots, 9$, yields the coefficients $a_i^\perp(W)$, $i = 1, 2, \ldots, 9$. Thus, the dual spectra satisfy the equation of order $l = 9$ with coefficients $a_i^\perp(W)$, $i = 1, 2, \ldots, 9$, presented in the third column of the same table. Notice that the WAM of the minimal encoder of the dual code which is not presented here contains four nonzero entries in each row since the dual code has rate 2/3.

[1] Although the coefficients $a_i(W)$ belong to a polynomial ring, they can be found by computations over the field of rational functions. Alternatively, the inversion-free modification of the Berlekamp-Massey algorithm [16] can be used.

4. CONCLUSION

We have shown that it is enough to know the first $2r$ spectral components of truncated or tailbitten convolutional codes, where r is the rank of the minimal encoder WAM of the parent convolutional code, in order to find the coefficients of the recurrent equation generating an arbitrary long sequence of spectra of dual truncated or dual tailbitten convolutional codes.

ACKNOWLEDGEMENT

The authors are grateful to G. David Forney, Jr. for detailed and helpful comments on earlier versions of this paper and to the reviewer for comments and suggestions that led to improvements in the presentation.

REFERENCES

1. R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding.* Piscataway, NJ: IEEE Press, 1999.
2. A. J. Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans. Commun. Technol.*, vol. COM-19, no. 5, pp. 751–772, Oct. 1971.
3. J. B. Shearer and R. J. McEliece, "There is no MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 6, pp. 775–776, Nov. 1977.
4. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North Holland, 1977.
5. K. A. S. Abdel-Ghaffar, "On unit constraint-length convolutional codes," *IEEE Trans. Inf. Theory*, vol. IT-38, no. 1, pp. 200–206, Jan. 1992.
6. H. Gluesing-Luerssen and G. Schneider, "On the MacWilliams identity for convolutional codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1536–1550, Apr. 2008.
7. H. Gluesing-Luerssen and G. Schneider, "A MacWilliams identity for convolutional codes: The general case," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2920–2930, Jul. 2009.
8. R. J. McEliece, "How to compute weight enumerators for convolutional codes," in *Communications and Coding (P. G. Farrell 60th Birthday Celebration)*, M. Darnell and B. Honary, Eds. New York: Wiley, 1998, pp. 121–141.
9. G. D. Forney, Jr., "MacWilliams identities for codes on graphs," in *Proc. IEEE Information Theory Workshop (ITW09)*, Taormina, Italy, Oct. 11–16, 2009, pp. 120–124.
10. G. D. Forney, Jr., "Codes on Graphs: Duality and MacWilliams identities," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1382–1397, Mar. 2011.
11. I. E. Bocharova, F. Hug, R. Johannesson, and B. D. Kudryashov, "On weight enumerators and MacWilliams identity for convolutional codes," in *Proc. Information Theory and Applications Workshop (ITA)*, San Diego, CA, Jan. 31 – Feb. 5, 2010, pp. 1–6.
12. G. D. Forney, Jr., "MacWilliams identities for terminated convolutional codes," in *Proc. IEEE International Symposium on Information Theory (ISIT10)*, Austin, Texas, U.S.A., Jun. 13–18, 2010.
13. G. D. Forney, Jr., "Structural analysis of convolutional codes via dual codes," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 512–518, Jul. 1973.
14. W. C. Brown, *Matrices over commutative rings.* New York: Marcel Dekker, 1993.
15. R. E. Blahut, *Fast Algorithms for Digital Signal Processing.* Addison-Wesley Publishing Co., 1985.
16. I. Reed, M. Shih, and T. Truong, "VLSI design of inverse-free Berlekamp-Massey algorithm," *Computers and Digital Techniques, IEE Proceedings-E*, vol. 138, no. 5, pp. 295–298, 1991.