Centrum voor Wiskunde en Informatica

REPORT*RAPPORT*

On the generalized Hamming weights of convolutional codes

J. Rosenthal and E.V. York

Department of Operations Reasearch, Statistics, and System Theory

BS-R9507 1995

Report BS-R9507
ISSN 0924-0659

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

On the Generalized Hamming Weights of Convolutional Codes

Joachim Rosenthal
Department of Mathematics, University of Notre Dame,
Notre Dame, Indiana 46556, USA
and
CWI, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
Joachim.Rosenthal@nd.edu

Eric Von York
Department of Mathematics, University of Notre Dame,
Notre Dame, Indiana 46556, USA
Eric.York@nd.edu

Abstract

Motivated by applications in cryptology K. Wei introduced in 1991 the concept of a generalized Hamming weight for a linear block code. In this paper we define generalized Hamming weights for the class of convolutional codes and we derive several of their basic properties. By restricting to convolutional codes having a generator matrix $G(D)$ with bounded Kronecker indices we are able to derive upper and lower bounds on the weight hierarchy.

AMS Subject Classification (1991): 94B10, 94B65, 93C05, 93C55.
Keywords & Phrases: Convolutional codes, generalized Hamming weights, weight hierarchy, dimension/length profile.
Note: The first author did this research while he was a visitor at CWI. Both authors were supported in part by the National Science Foundation under NSF grant DMS-9400965.

1. Introduction

An important set of code parameters defined for a linear block code are the so called generalized Hamming weights first introduced by Wei in [19]. By definition the r-th generalized Hamming weight $d_r(C)$ of a linear block code C is equal to the smallest support of any r-dimensional subcode of C. In particular $d_0(C) = 0$ and $d_1(C)$ is equal to the distance of C.

In this way every $[n, k]$ linear block code has associated a whole weight hierarchy

$$0 = d_0(C) < d_1(C) < \cdots < d_k(C) \leq n. \tag{1.1}$$

As already pointed out by Wei [19] a large weight hierarchy is desirable if one is interested in designing a wire tap channel of type II. Knowledge of the weight hierarchy of convolutional codes may aid in the design of a coding scheme for use with a channel of this type (i.e.: 1/n codes appear to be useful for these purposes).

From an applications point, probably most important is the determination of the weight hierarchy of codes for applications to trellis encoders and we refer to Wei [20] and Forney [3]. Forney [3] calls the generalized Hamming weights the length/dimension profile (LDP) of a code. As explained in detail in [3] there is a deep connection between LDP and the complexity of the minimal trellis diagram. In [3] Forney also points out that a study of LDP i.e. generalized Hamming weights of convolutional codes and other trellis codes would be desirable and this motivates in part the investigation of this paper.

Generalized Hamming weights have also a very natural geometric interpretation and this was pointed out in [6]. For this recall that a set of ordered points $\mathcal{P} := \{P_1, \ldots, P_n\}$ in a k-dimensional vector space V is called a $[n, k]$ system if $\mathcal{P}$ is not contained in any hyperplane $H \subset V$. Two $[n, k]$ systems $\mathcal{P}$ and $\mathcal{P}'$ are called equivalent if there is an isomorphism on V mapping $\mathcal{P}$ onto $\mathcal{P}'$. As explained in [18, Section 1.1.2] every block code $C \subset \mathbb{F}_q^n$ uniquely defines an equivalence class of $[n, k]$ systems. It can be shown (see [6]) that the r-th generalized Hamming weight is then geometrically described through the formula:

$$d_r(C) = |\mathcal{P}| - \max_{H_r \subset V} \{|H_r \cap \mathcal{P}|\},$$

where H_r is an arbitrary hyperplane of co-dimension r. Hence the generalized Hamming weights correspond to how well the subspaces of C are in 'general position'. The weight hierarchy of convolutional codes provide us with similar geometrical information about their structure as well, but we will not elaborate on this.

Since the appearance of Wei's original article several authors (see e.g. [3, 6, 20]) were studying the weight hierarchy of different classes of linear block codes. In this correspondence we will study the weight hierarchy of a convolutional code. After formally introducing this concept we will derive in the next section several of the basic properties. In particular we will show that the generalized Hamming weights form an infinite strictly increasing sequence $d_i(C)$ of positive integers and similar to the case of block codes the free distance of the code is exactly $d_1(C)$. As it is the case for any trellis code a large weight hierarchy is desirable in the design of encoders and this motivates in part the investigation of this paper.

In Section 3 we give an overview of current existing upper bounds for $d_r(C)$ of a block code. Those bounds prepare for the main results of this paper, which are given in Section 4. In this section we will derive some upper and lower bounds for the weight hierarchy of different classes of convolutional codes. The bounds we derive depend on the rate and complexity of the code as opposed to depending on the rate and memory (see e.g. [7]). More specific results are derived for the generalized Hamming weights of rate $\frac{1}{n}$ codes in which case the memory and the complexity are the same.

In the last section several illustrative examples are provided. In those examples we compute the complete weight hierarchy of several classes of codes. In this way, we are able to show that some of the bounds derived in Section 4 are tight for some classes of codes. We conclude the paper by providing several tables containing bounds for certain classes of convolutional codes.

2. The Generalized Hamming weights of convolutional codes, definitions and basic properties.

Let $\mathbb{F}_q$ be the Galois field of q elements, $\mathbb{F}_q[D]$ be the polynomial ring over $\mathbb{F}_q$ and $\mathbb{F}_q(D)$ the ring of rational functions. In the following it will be convenient to view elements of $\mathbb{F}_q(D)$ as infinite (periodic) power series of the form $\sum_{i=0}^{\infty} x_i D^i, x_i \in \mathbb{F}_q$. Let C be a rate k/n convolutional code represented through a non-catastrophic encoder

$$G(D) = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} \tag{2.1}$$

Without loss of generality we will assume that the matrix $G(D)$ which is defined over $\mathbb{F}_q[D]$ is in row proper form, in other words we will assume that the "high order coefficient matrix" has full row rank. We also will assume that $G(D)$ has ordered row (Kronecker) indices

$$\nu_1 \geq \cdots \geq \nu_k$$

where the indices ν_i are formally defined through:

$$\nu_i = \max\{\deg(g_{ij}) \mid 1 \leq j \leq n\}, \quad i = 1, \ldots, k.$$

We will denote the memory, complexity and constraint length of a convolutional code by m, c, and η respectively. In terms of the Kronecker indices we have: $m = \nu_1$, $c = \sum_{i=1}^{k} \nu_i$ and $\eta = n(\nu_1 + 1)$.

In an obvious way we can view C also as an (infinite dimensional) linear $\mathbb{F}_q$ vector space. Let

$$\{u_1(D), \ldots, u_r(D)\}$$

be r linearly independent vectors in $\mathbb{F}_q^k(D)$. Since $G(D)$ has by assumption linearly independent rows it follows that

$$\text{span}_{\mathbb{F}_q}\{u_1(D)G(D), \ldots, u_r(D)G(D)\} \subset C \subset \mathbb{F}_q^n(D)$$

defines an r-dimensional subspace of C and clearly every r-dimensional subspace $U \subset C$ is of this form.

DEFINITION 2.1 Let $U \subset C$ be a linear subspace of C. Then

$$\chi(U) := \{(i,j) \mid \exists \left(\sum x_{1j}D^j, \ldots, \sum x_{nj}D^j\right) \in U, x_{ij} \neq 0\}$$

is called *the support* of U and

$$d_r(C) := \min\{|\chi(U)| \mid U \subset C \text{ and } \dim U = r\}$$

is called the *rth generalized Hamming weight* of C.

Note that the generalized Hamming weights are well defined for any positive integer r and not just for $r = 0, \ldots, k$ as it is the case for block codes. Also note that if U is one dimensional and $u \in U$ is any nonzero codeword then $|\chi(U)|$ is nothing else than the usual Hamming weight $w(u)$ of the codeword u. In particular it follows in analogy to the block code case that $d_1(C)$ is equal to the free distance of C.

LEMMA 2.2 *Let C be a convolutional code of rate $\frac{k}{n}$ and memory m. In order to compute $d_i(C)$ it is enough to consider subspaces of the form*

$$U = \text{span}\{u_1(D)G(D), \ldots, u_r(D)G(D)\}$$

where $u_i(D) \subset \mathbb{F}_q^k[D]$ and the $\deg(u_i(D)) < (m^2 + mr)n$.

Proof If for some index i $u_i(D)$ is rational and not polynomial, i.e. $u_i(D) \subset \mathbb{F}_q^k(D) \setminus \mathbb{F}_q^k[D]$ then it follows that the support of U is infinite since we assumed that $G(D)$ is non-catastrophic.That $\deg(u_i(D))$ is bounded follows from the minimality of $d_i(C)$ and the fact that $d_i(C) < (\nu_1 + r)n$. □

The following Lemma is a natural generalization of Wei's monotonicity theorem [19, Theorem 1] for block codes.

Lemma 2.3 *The generalized Hamming weights of a convolutional code form a (strictly) increasing set of positive integers*

$$0 = d_0(C) < d_1(C) < d_2(C) < \cdots$$

Proof Obviously the sequence is weakly increasing. In order to show the strict inequality let $U \subset C$ have the property that $\dim U = r$ and $|\chi(U)| = d_r(C)$. Assume (i,j) is in the support of U, i.e. there is a codeword $\left(\sum x_{1j}D^j, \ldots, \sum x_{nj}D^j\right) \in U, x_{ij} \neq 0$. Let $D := \{c \in U \mid x_{ij} = 0\}$. But then one has $|\chi(D)| < |\chi(U)|$ and $\dim D = r - 1$. In other words $d_{r-1}(C) < d_r(C)$. □

In [20, Section IV], the authors define the *chain condition* for block codes. This definition is easily generalized to convolutional codes as follows:

Definition 2.1 A convolutional code C is said to satisfy the *chain condition* if there exists subcodes D_r for $1 \leq r \leq \infty$ such that $\mathrm{rank}(D_r) = r$, $|\chi(D_r)| = d_r(C)$, and $D_{r-1} \subset D_r$.

Similar to the block code case we can describe the numbers $d_r(C)$ also algebraically. For this consider a parity check matrix $H(D)$ of C and define:

$$H = \begin{pmatrix} H_0 & 0 & 0 & \cdots \\ H_1 & H_0 & 0 & \cdots \\ H_2 & H_1 & H_0 & \cdots \\ \vdots & H_2 & H_1 & \ddots \\ \vdots & \ddots & H_2 & \ddots \\ H_\alpha & \ddots & \ddots & \ddots \\ 0 & H_\alpha & \ddots & \ddots \\ 0 & 0 & H_\alpha & \ddots \\ \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

Then one has the immediate generalization of [19, Theorem 2]:

Theorem 2.4 *C has generalized Hamming weight $d_r(C) = d$ if and only if d is the smallest number with the property that there are d columns of H whose rank is $d - r$ or less.*

3. Bounds for the weight hierarchy of a block code

In this section we summarize the best general upper bounds known for the generalized Hamming weights of block codes. Those results will then be the basis in our investigation of the bounds of the generalized Hamming weights of convolutional codes.

The first bound was already given in [19] by Wei who called the bound the generalized Singleton bound.

Lemma 3.1 *For an $[n,k]$ code C one has*

$$d_r(C) \leq n-k+r.$$

The next bound is the well known Griesmer bound [4].

Lemma 3.2 *For a linear block code over $\mathbb{F}_q$ with rate $\frac{k}{n}$ and distance d we have*

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \leq n. \tag{3.1}$$

The following, given in [5, Theorem 5], is a generalization of the Griesmer bound to $d_r(C)$:

Theorem 3.3 *Let C be a binary, linear $[n,k]$ code. Then for $1 \leq r \leq k$ one has:*

$$d_r(C) + \sum_{i=1}^{k-r} \left\lceil \frac{d_r(C)}{(2^r-1)2^i} \right\rceil \leq n. \tag{3.2}$$

When the distance of a block code is known, the Griesmer bound can also be used as a lower bound. The following result is referred to in [6, pp. 276] as the *Griesmer-Wei Bound*:

Lemma 3.4 *For a linear block code over $\mathbb{F}_q$ with rate $\frac{k}{n}$ and distance d we have*

$$d_r(C) \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{3.3}$$

4. Bounds for the weight hierarchy of a convolutional code

In this section we will derive a set of upper bounds on the generalized Hamming weights which have to be satisfied for all convolutional codes. In order to properly pose the problem it is of course necessary to restrict to certain classes of convolutional codes.

The codes which we single out are all convolutional codes having a fixed rate k/n and having a basic encoder (see e.g. [13, Section 2.3]) with a fixed set of Kronecker indices $\nu = (\nu_1, \ldots, \nu_k)$. Clearly it is most natural to fix the rate. Moreover the set of encoders having a fixed set of Kronecker indices is most natural too. Indeed every encoder can be naturally identified with an associated Hermann-Martin map [11] from the projective line to a fixed Grassmann variety and the Kronecker indices correspond in this case exactly to the Grothendieck indices of the pull back of the tautological bundle. In system theory the Kronecker indices correspond to the observability indices of the associated MA representation and the complexity $c = \sum_{i=1}^{k} \nu_i$ is exactly the McMillan degree of the system. For readers interested in more details covering those interesting relations we refer to [2, 14, 17].

Because of the above mentioned reasons we seek upper bounds on the weight hierarchy in the class of convolutional codes having fixed rate k/n and having a basic encoder with a fixed set of Kronecker indices $\nu = (\nu_1, \ldots, \nu_k)$. Note that for $\nu_1 = 0$ (no memory) the problem is equivalent to estimating upper bounds of block codes as it was considered in the last section. In this way our problem can also be viewed as a natural generalization.

The basic strategy how we will go to accomplish upper bounds is as follows (compare also with [13, Section 3.1]): Let $V \subset \mathbb{F}_q^n[D]$ be any finite dimensional linear $\mathbb{F}_q$-subspace. Then

$$C_V := \{u(D)G(D) \mid u(D)G(D) \in V, u(D) \in \mathbb{F}_q^k[D]\} \subset C \subset \mathbb{F}_q^n[D]$$

defines a linear $[\mathcal{N}, \mathcal{K}]$ block code, where

$$\mathcal{N} = |\chi(C_V)| \leq |\chi(V)| \text{ and } \mathcal{K} = \dim C_V. \tag{4.1}$$

For every such linear block code C_V we then necessarily have that

$$d_r(C) \leq d_r(C_V) \qquad \forall r. \tag{4.2}$$

Clearly the bounds of $d_r(C_V)$ are expected to be small if the rate $\frac{\mathcal{K}}{\mathcal{N}}$ is large and because of this we will single out a set of subspaces V which have a maximal dimension for a given support. Specifically we will consider for each integer $\gamma \geq 0$ the subspace

$$V_\gamma := \{(x_1(D), \ldots, x_n(D)) \in \mathbb{F}_q^n[D] \mid \deg x_i(D) \leq \gamma, i = 1, \ldots, n\}. \tag{4.3}$$

Note that V_γ is in a natural way a $\mathbb{F}_q$ vector space of dimension $n\gamma + n$, indeed one has natural vector space isomorphisms

$$V_\gamma \simeq \mathbb{F}_q^{\gamma+1} \otimes \mathbb{F}_q^n \simeq \mathbb{F}_q^{n\gamma+n}. \tag{4.4}$$

The following Lemma establishes the block size of the codes C_{V_γ} which we will abbreviate with

$$C_\gamma := C_{V_\gamma}.$$

Lemma 4.1 *Let C be a rate k/n convolutional code represented by a basic encoder having Kronecker indices $\nu_1, \ldots, \nu_k$. Let $\mathcal{N} = |\chi(C_\gamma)|$. Then for each $\gamma \geq 0$ the code C_γ is a linear $[\mathcal{N}, \mathcal{K}]$ block code where*

$$\mathcal{N} \leq n\gamma + n, \tag{4.5}$$

$$\mathcal{K} = \sum_{i=1}^{k} \max(\gamma - \nu_i + 1, 0). \tag{4.6}$$

Proof The fact that C_γ is linear is obvious and the estimate (4.5) is a direct consequence of (4.1) and (4.4). Let $G(D)$ be a basic encoder with Kronecker indices $\nu_1, \ldots, \nu_k$. From the fact that the high order coefficient matrix of $G(D)$ has full row rank it follows that

$$\deg\left((u_1, u_2, \ldots, u_k) \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix} \right) = \max_{1 \leq i \leq k} \{\deg u_i + \nu_i\}.$$

In particular it follows that every $(u_1, u_2, \ldots, u_k)$ having the property that $\deg u_i \leq \gamma - \nu_i$ results in a valid element of C_γ and the map $u \mapsto uG$ induces a vector space isomorphism

$$C_\gamma \simeq \bigoplus_{i=1}^{k} \mathbb{F}_q^{\gamma - \nu_i + 1} \simeq \mathbb{F}_q^{\mathcal{K}},$$

where we made use of the convention $\mathbb{F}^\alpha = 0$ if $\alpha < 0$. □

The following examples illustrate the concepts introduced thus far.

EXAMPLE 4.2 Let $G(D) = (D^2 + D + 1, D + 1)$ be the generator matrix of the convolutional code C, then the rate of C_γ is $\frac{\gamma-1}{2\gamma+1}$ for any $\gamma \geq 2$. An arbitrary element of C_γ would be given by $y(D) = (a_\gamma D^\gamma + a_{\gamma-1}D^{\gamma-1} + \cdots a_1 D + a_0, b_{\gamma-1}D^{\gamma-1} + b_{\gamma-2}D^{\gamma-2} + \cdots b_1 D + b_0)$. The vector $y(D)$ can be naturally identified with the vector $(a_\gamma, a_{\gamma-1}, \cdots, a_1, a_0, b_{\gamma-1}, b_{\gamma-2}, \cdots, b_1, b_0)$ viewed as element of the vector space $\mathbb{F}_2^{2\gamma+1}$.

EXAMPLE 4.3 Let $G(D) = \begin{pmatrix} D^2+1 & D & D^2 \\ D+1 & 1 & D+1 \end{pmatrix}$ be the generator matrix of the convolutional code C, then the rate of C_γ is $\frac{2\gamma-1}{3\gamma+2}$ for $\gamma \geq 1$. An arbitrary element of C_2 would be given by $y(D) = (a_2 D^2 + a_1 D + a_0, b_1 D + b_0, c_2 D^2 + c_1 D + c_0)$. The vector $y(D)$ can be identified with the vector $(a_2, a_1, a_0, b_1, b_0, c_2, c_1, c_0)$ in $\mathbb{F}_2^8$. A generator matrix for the block code determined by C_2 is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

We would like to remark at this point that for many codes C the support $\mathcal{N} = |\chi(C_\gamma)|$ is strictly less than $n\gamma + n$ and only for a "generic code" in the class of rate k/n codes with indices ν equality holds in 4.5. It therefore follows that if one restricts the class of convolutionl codes further it is possible to achieve even sharper bounds than the bounds which we will derive shortly[1].

Before we derive several upper bounds for the generalized Hamming weights $d_r(C)$ of a convolutional code C we show through the next theorem that "optimal bounds" for the block codes C_γ result in "optimal bounds" for the convolutional code C.

THEOREM 4.4 *Let C be a rate k/n convolutional code. Then the vectorspaces*

$$C_0 \subset C_1 \subset C_2 \subset \ldots$$

form a direct system of vectorspaces with direct limit

$$\lim_{\gamma \to \infty} C_\gamma = C. \tag{4.7}$$

Moreover for every integer $r \geq 1$ exists a positive integer n_o only dependent on k, n, r, ν having the property that

$$d_r(C_\gamma) = d_r(C) \tag{4.8}$$

for all $\gamma \geq n_o$.

PROOF The first part is a direct consequence of the definition of C_γ and the definition of a direct limit. The second part follows from Lemma 2.2. □

The first upper bound which we will present is based on the generalized Griesmer bound as introduced in Theorem 3.3:

[1] In terms of the constraint length we say one only needs to consider the *effective constraint length* as pointed out by Costello in [1].

THEOREM 4.5 *Let C be a binary rate k/n convolutional code having a basic encoder with Kronecker indices $\nu = (\nu_1, \ldots, \nu_k)$. Let γ be a positive integer and let $\mathcal{K} = \sum_{i=1}^{k} \max(\gamma - \nu_i + 1, 0)$. Then the rth generalized Hamming weight of C satisfies*

$$d_r(C) + \sum_{i=1}^{\mathcal{K}-r} \left\lceil \frac{d_r(C)}{2^i(2^r - 1)} \right\rceil \leq n\gamma + n. \qquad (4.9)$$

For convolutional codes defined over an arbitrary field $\mathbb{F}_q$ we have the well known Griesmer bound:

THEOREM 4.6 *Let C be a convolutional code over $\mathbb{F}_q$ with rate $\frac{k}{n}$, then for all $\gamma \geq 0$ $d_1(C)$ must satisfy*

$$\sum_{i=0}^{\mathcal{K}-1} \left\lceil \frac{d_1(C)}{q^i} \right\rceil \leq n\gamma + n,$$

where $\mathcal{K}$ is determined by (4.6).

4.1 Bounds for codes of rate $\frac{1}{n}$.

Rate $\frac{1}{n}$ codes have been studied extensively, and there are several very effective techniques for constructing codes of this rate with *good* free distance (see e.g. [12, 8, 15]). In this section we study the properties of the generalized Hamming weights for these types of codes.

Let C be a convolutional code of rate $\frac{1}{n}$ and constraint length η. Then the fact that

$$d_i(C) \leq \eta + n(i - 1). \qquad (4.1)$$

is obvious.

LEMMA 4.7 *Let C be a convolutional code of rate $\frac{1}{n}$ generated by $G(D)$. Then*

$$d_i(C) + n \leq d_{i+1}(C). \qquad (4.2)$$

PROOF Suppose that $D \subset C$ has dimension $i+1$ and support $d_{i+1}(C)$. Then, by Lemma 2.2 there exists $i+1$ linearly independent vectors $u_s(D)$ such that

$$D = \mathbf{span}\{u_1(D)G(D), \ldots, u_{i+1}(D)G(D)\}.$$

Since the $u_s(D)$'s are linearly independent, by row reducing we can obtain the polynomials

$$\{\widetilde{u_1}(D), \widetilde{u_2}(D), \ldots, \widetilde{u_{i+1}}(D)\}$$

such that

$$D = \mathbf{span}\{\widetilde{u_1}(D)G(D), \ldots, \widetilde{u_{i+1}}(D)G(D)\}$$

and $\deg(\widetilde{u_1}(D)) < \deg(\widetilde{u_2}(D)) < \ldots < \deg(\widetilde{u_{i+1}}(D))$. The i dimensional subspace

$$\widetilde{D} = \mathbf{span}\{\widetilde{u_1}(D)G(D), \ldots, \widetilde{u}_i(D)G(D)\}$$

has

$$d_i(C) \leq |\chi(\widetilde{D})| \leq d_{i+1}(C) - n.$$

□

Corollary 4.8 *Let C be a convolutional code of rate $\frac{1}{n}$ and memory m. Then if*

$$d_i(C) = \eta + n(i-1)$$

for some $i \geq 1$ we have

$$d_j(C) = \eta + n(j-1), \quad \forall j > i.$$

5. Tables and Examples

In this section we will give several examples illustrating the concepts defined throughout this paper. We also present tables containing the bounds for $d_r(C)$ for some low rate codes with particular Kronecker indices.

Example 5.1 Consider the class of convolutional codes over $\mathbb{F}_2$ with rate $k/n = \frac{1}{2}$ and memory $m = \nu_1 = 16$. Using equation 4.6 and considering the elements in C_{19}, we obtain

$$\sum_{j=0}^{3} \left\lceil \frac{d_1(C)}{2^j} \right\rceil \leq 40.$$

This implies that $d_1(C) \leq 20$. In [9, pg. 330] it is shown that there exists a rate $\frac{1}{2}$ code having memory $m = 16$ and distance $d_1(C) = 20$. Our bound is therefore tight in this particular example.

Example 5.2 If C is generated by $G(D) = (D^2+D+1, D^2+1)$ then one has $d_0(C) = 0$, $d_1(C) = 5$. By Lemma 3.4 we must have $d_2(C) \geq 8$, hence by Corollary 4.8 we must have $d_i(C) = 2(i-1)+6, \quad \forall i > 1$. Furthermore, let $c_i(D) = D^{i-1}G(D)$, and set $D_r = \mathbf{span}\{c_1(D), c_2(D), \ldots, c_r(D)\}$. Then one can easily verify that $|\chi(D_r)| = d_r(C)$, hence C has optimal generalized Hamming weight and satisfies the chain condition for convolutional codes.

Example 5.3 Consider the class of convolutional codes over $\mathbb{F}_2$ with rate $\frac{2}{3}$, and $\nu = (2,3)$. Using equation 4.6 and considering the elements in C_3, we obtain

$$\sum_{j=0}^{2} \left\lceil \frac{d_1(C)}{2^j} \right\rceil \leq 12.$$

This implies that $d_1(C) \leq 6$. In [9, pg. 330] it is shown that the rate $\frac{2}{3}$, memory $m = 3$ code C which is generated by

$$G = \begin{pmatrix} D^2 + D^3 & 1 & 1 + D + D^2 + D^3 \\ 1 + D & D + D^2 & 1 + D + D^2 \end{pmatrix}$$

has a free distance $d_1(C)$ of 6. The bound $d_1(C) \leq 6$ is therefore tight for the class of rate $\frac{2}{3}$, codes having Kronecker indices $\nu = (2,3)$. Note: If one were to consider the class of rate $\frac{2}{3}$, codes having Kronecker indices $\nu = (3,3)$ then the Griesmer bound gives $d_1(C) \leq 8$, hence consideration of the Kronecker indices do give a refinement on existing bounds.

Next consider $c_1 = (0, 1+D)G(D)$, $c_2 = (1+D, 0)G(D)$ and $c_3 = (1, D^2)G(D)$. Then one can verify that

$$|\chi(\mathbf{span}\{c_1, c_2\})| = 9$$

and

$$|\chi(\mathbf{span}\{c_1, c_2, c_3\})| = 11.$$

It therefore follows that $d_2(C) \leq 9$ and $d_3(C) \leq 11$. By Lemma 3.4, $d_2(C) \geq 9$ and $d_3(C) \geq 11$ hence $d_2(C) = 9$ and $d_3(C) = 11$.

EXAMPLE 5.4 Let $\widetilde{C}$ be the $\frac{1}{4}$ code generated by $\widetilde{G} = (D+1, 1, D, 1)$. Let G be the matrix from example 5.3, then the $\frac{3}{7}$ code C' generated by

$$G' = \begin{pmatrix} \widetilde{G} & 0 \\ 0 & G \end{pmatrix}$$

has $d_1(C') = 5$ and by example 5.3 and Lemma 4.7 we have $d_2(C') = 9$ $d_3(C') = 11$ and any 3-dimensional subspace V that contains the vector $(D+1, 1, D, 1)$ must have $d_3(V) \geq 13$, hence C' does not satisfy the chain condition for convolutional codes.

EXAMPLE 5.5 Consider the rate $\frac{1}{4}$ code C given by

$$G(D) = (1 + D^2 + D^3, 1 + D + D^3, 1 + D + D^3, 1 + D + D^2 + D^3).$$

By consulting [9, pg. 330] we see that $d_1(C) = 13$. By Lemma 3.4 and equation 4.1 we have $20 \geq d_2(C) \geq 20$ hence by Corollary 4.8 we have

$$d_i(C) = 4(i-1) + 16, \qquad \forall i > 1$$

By considering the vectors $D^i G(D)$ one can show that the code C satisfies the chain condition as well.

The following tables were obtained using equation 4.9.

rate $\frac{1}{2}$					
ν_1	$d_1(C) \leq$	$d_2(C) \leq$	$d_3(C) \leq$	$d_4(C) \leq$	$d_5(C) \leq$
1	4	6	8	10	12
2	5	8	10	12	14
3	6	10	12	14	16
4	8	12	14	16	18
5	8	13	16	18	20

rate $\frac{1}{3}$					
ν_1	$d_1(C) \leq$	$d_2(C) \leq$	$d_3(C) \leq$	$d_4(C) \leq$	$d_5(C) \leq$
1	6	9	12	15	18
2	8	12	15	18	21
3	10	15	18	21	24
4	12	18	21	24	27
5	13	20	24	27	30

rate $\frac{2}{4}$					
(ν_1, ν_2)	$d_1(C) \leq$	$d_2(C) \leq$	$d_3(C) \leq$	$d_4(C) \leq$	$d_5(C) \leq$
$(1,0)$	4	6	8	11	12
$(1,1)$	5	8	11	12	15
$(2,0)$	6	9	11	12	15
$(2,1)$	6	10	12	15	16
$(3,0)$	4	8	12	15	16
$(2,2)$	8	12	14	16	19
$(3,1)$	8	12	14	16	19
$(4,0)$	4	8	12	16	19
$(3,2)$	8	13	16	19	20
$(4,1)$	8	12	16	19	20
$(5,0)$	4	8	12	16	20

rate $\frac{2}{3}$					
(ν_1, ν_2)	$d_1(C) \leq$	$d_2(C) \leq$	$d_3(C) \leq$	$d_4(C) \leq$	$d_5(C) \leq$
$(1,0)$	3	5	6	8	9
$(1,1)$	4	6	8	9	11
$(2,0)$	3	6	8	9	11
$(2,1)$	4	7	9	11	12
$(3,0)$	3	6	9	11	12
$(2,2)$	6	9	11	12	14
$(3,1)$	6	9	11	12	14
$(4,0)$	3	6	9	12	14
$(3,2)$	6	10	12	14	15
$(4,1)$	6	9	12	14	15
$(5,0)$	3	6	9	12	15

References

1. D. Costello (1974). Free Distance Bounds for Convolutional Codes. *IEEE Trans. Inform. Theory* IT-20, No. 3, 356–365.

2. G. D. Forney (1975). Minimal Bases of Rational Vector Spaces, with Applications to Multivariable Linear Systems. *SIAM J. Control Optim.* 13, No. 3, 493–520.

3. G. D. Forney (1994). Dimension/Length Profiles and Trellis Complexity of Linear Block Codes,. *IEEE Trans. Inform. Theory* IT-40, No. 6, 1741–1752.

4. J. H. Griesmer (1960). A Bound for Error-correcting Codes. *IBM Journal of Research and Development* 4, 532–542.

5. T. Helleseth, T. Kløve and Ø. Ytrehus (1992). Generalized Hamming Weights of Linear Codes. *IEEE Trans. Inform. Theory* IT-38, No. 3, 1133–1140.

6. J. W. P. Hirschfeld, M. A. Tsfasman and S. G. Vlăduţ (1994). The Weight Hierarchy of Higher Dimensional Hermitian Codes. *IEEE Trans. Inform. Theory* IT-40, No. 1, 275–278.

7. R. Johannesson and K. Zigangirov. Distances and Distance Bounds for Convolutional Codes – an Overview. In *Topics in Coding Theory. In honour of L. H. Zetterberg.*, Lecture Notes in Control and Information Sciences # 128. Springer Verlag, 1989, pp. 109–136.

8. J. Justesen (1975). An Algebraic Construction of Rate $1/\nu$ Convolutional Codes. *IEEE Trans. Inform. Theory* IT-21, No. 1, 577–580.

9. S. Lin and D. Costello (1983). *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, Englewood Cliffs, NJ.

10. F. J. MacWilliams and N. J.A. Sloane (1977). *The Theory of Error-Correcting Codes.* North Holland, Amsterdam.

11. C. F. Martin and R. Hermann (1978). Applications of Algebraic Geometry to System Theory: The McMillan Degree and Kronecker Indices as Topological and Holomorphic Invariants. *SIAM J. Control Optim.* 16, 743–755.

12. J. L. Massey, D.J. Costello and J. Justesen (1973). Polynomial Weights and Code Constructions. *IEEE Trans. Inform. Theory* IT-19, No. 1, 101–110.

13. Ph. Piret (1988). *Convolutional Codes, an Algebraic Approach.* MIT Press, Cambridge, MA.

14. M. S. Ravi and J. Rosenthal (1994). A Smooth Compactification of the Space of Transfer Functions with Fixed McMillan Degree. *Acta Appl. Math* 34, 329–352.

15. W.J. Reitsema (1973). A Lower Bound on the Free Distance of Convolutional Codes Related to Cyclic Codes. *IEEE Trans. Inform. Theory* IT-27, No. 5, 638–639.

16. S. Roman (1992). *Coding and Information Theory.* Graduate Text in Mathematics. Springer Verlag, New York - Berlin.

17. J. Rosenthal, M. Sain and X. Wang (1994). Topological Considerations for Autoregressive Systems with Fixed Kronecker Indices. *Circuits Systems Signal Process* 13, No. 2–3, 295–308.

18. M. A. Tsfasman and S. G. Vlăduţ (1991). *Algebraic Geometric Codes.* Mathematics and Its Application. Kluwer Academic Publishers, The Netherlands.

19. V. K. Wei (1991). Generalized Hamming Weights for Linear Codes. *IEEE Trans. Inform. Theory* IT-37, No. 5, 1412–1418.

20. V. K. Wei and K. Yang (1993). On the Generalized Hamming Weights of Product Codes. *IEEE Trans. Inform. Theory* IT-39, No. 5, 1709–1713.