On the Trellis Complexity of Certain Binary Linear Block Codes

Øyvind Ytrehus*, Member IEEE

IEEE Trans. IT, March 1995, pp. 559–560

Abstract — The trellis complexity $s(\mathcal{C})$ of an $[n, k, d]$-code $\mathcal{C}$ is investigated, in the case where the weights of nonzero codewords in $\mathcal{C}$ are confined to $\{d, \ldots, 2d-1\} \cup \{n\}$. It is shown that $s(\mathcal{C}) \geq k-1$. Furthermore, $s(\mathcal{C}) = k-1$ if the code is self-complementary. If the nonzero weights are confined to $\{d, \ldots, 2d-3\}$, then $s(\mathcal{C}) = k$.

Keywords — Block codes, trellis structure, soft-decision decoding

***University of Bergen,**
Department of informatics,
Høyteknologisenteret,
N-5020 Bergen, Norway.

Partially supported by the Norwegian Research Council (NFR). This

Throughout this correspondence, let $\mathcal{C}$ be a binary linear $[n, k, d]$-code with $d \geq 3$. Assume that the dual code of $\mathcal{C}$ has minimum distance at least two.

I. Introduction

Wolf [1] observed that any block code $\mathcal{C}$ can be described by a trellis, for the purpose of performing soft decision decoding by use of the Viterbi algorithm. The trellis complexity $s(\mathcal{C})$, defined in [2, 3] and in the next section, is important for characterizing the complexity of the decoder. Muder [2] suggested that the trellis complexity should be considered as one of the fundamental parameters of a code, along with its length, dimension and minimum distance. For this reason, the problem of determining $s(\mathcal{C})$ has attracted considerable attention in recent years. For examples, see references [2, 3, 4, 5, 6, 7].

An overview of definitions and known results is provided in the next section. New results are presented in Section III. These apply to codes whose nonzero codewords have weights in $\{d, \ldots, 2d-1\} \cup \{n\}$ and, through a well known duality result (Lemma 4), to their dual codes. Note that the trellis complexity of a number of well known codes is determined by these new results, for instance many BCH codes. Also, a number of recent bounds by Vardy and Be'ery [5] are improved.

II. Definitions and background

A *trellis* for a block code $\mathcal{C}$ is a directed graph. The set of nodes or *states* of the graph can be partitioned into subsets $\mathcal{S}_0 = \{S_0\}, \mathcal{S}_1, \ldots, \mathcal{S}_{n-1}, \mathcal{S}_n = \{S_n\}$. An edge from a state in $\mathcal{S}_{i-1}$ terminates at a state in $\mathcal{S}_i$, $1 \leq i \leq n$. For binary codes, each edge is labeled by 0 or 1, such that $\mathcal{C}$ is the set of edge label sequences obtained by traversing all paths from S_0 to S_n. For a linear code, each $\mathcal{S}_i$ is a vector space (cf. [2, 3]).

Maximum–likelihood soft decision decoding of the code can be achieved by applying the Viterbi algorithm to the trellis. The complexity of this decoding is essentially determined by the maximum state space dimension

$$s^*(\mathcal{C}) = \max_{0 \le i \le n} \dim(\mathcal{S}_i). \tag{1}$$

Computing $s^*(\mathcal{C})$ for a given code and a given coordinate ordering is relatively easy. However, we are also interested in finding the *trellis complexity*,

$$s(\mathcal{C}) = \min_{\pi} s^*(\pi\mathcal{C}), \tag{2}$$

where the minimization is performed over all permutations π acting on the coordinate positions of $\mathcal{C}$. Wolf [1] observed that $s(\mathcal{C}) \le \min\{k, n-k\}$.

We shall make use of some definitions from Forney's paper [3]. Let $S_{i,0}$ be the state in $\mathcal{S}_i$ that corresponds to the all zero path from S_0. Then the sets of label sequences associated with the sets of paths from S_0 to $S_{i,0}$, and from $S_{i,0}$ to S_n, are called the *past subcode* $\mathcal{C}_p^{(i)}$ and the *future subcode* $\mathcal{C}_f^{(i)}$, respectively. Note that [2, 3]

$$\dim(\mathcal{S}_i) = k - \dim\left(\mathcal{C}_p^{(i)}\right) - \dim\left(\mathcal{C}_f^{(i)}\right). \tag{3}$$

We will also need the concept of the *residual code*. The residual code of a code $\mathcal{C}$ with respect to a codeword $\mathbf{c} \in \mathcal{C}$ is denoted Res($\mathcal{C}$,$\mathbf{c}$) and is obtained by deleting the coordinates for which $\mathbf{c}$ is nonzero.

Let $w(\mathbf{c})$ denote the Hamming weight of $\mathbf{c}$.

Lemma 1 [8]. *Assume that $w(\mathbf{c}) = w < 2d$. Then Res($\mathcal{C}$,$\mathbf{c}$) is an $[n-w, k-1, d_1]$-code, where $d_1 \ge d - \lfloor w/2 \rfloor$.*

Finally, we will refer to the *weight set* of a code $\mathcal{C}$, defined as $W(\mathcal{C}) = \{w(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}$.

III. Bounds on $s(\mathcal{C})$

In this section certain bounds on $s(\mathcal{C})$ for binary linear codes will be shown. We start with

Lemma 2.

(a) (in [5]) If $d \geq (n+2)/3$, *then* $s(\mathcal{C}) \geq k-2$.

(b) (in [5]) If $d \geq 2(n+2)/5$, *then* $s(\mathcal{C}) \geq k-1$.

(c) If $W(\mathcal{C}) \subseteq \{d, \ldots, 2d-3\}$, *then* $s(\mathcal{C}) = k$.

Proof. (a) and (b) were shown by Vardy and Be'ery [5]. To prove (c), note that by linearity the condition implies that any two codewords overlap in at least two positions. Thus, for any coordinate permutation, there is a position i where both $\mathcal{C}_p^{(i)}$ and $\mathcal{C}_f^{(i)}$ have dimension zero. The result follows from (3).

□

The following is a simple lemma already used implicitly in [3, 4, 5]. It is worth stating this explicitly, however.

Lemma 3. *If* $n \in W(\mathcal{C})$, *i. e., the code is self-complementary, then* $s(\mathcal{C}) \leq k-1$, *provided k>1.*

Proof. Let $\mathbf{c}$ be any codeword of weight w. Apply the permutation π such that $\pi\mathbf{c}$ has 1's in the first w coordinates. Then, for $0 \leq i \leq n$, either $\pi\mathbf{c} \in (\pi\mathcal{C})_p^{(i)}$ or $(\mathbf{1}+\pi\mathbf{c}) \in (\pi\mathcal{C})_f^{(i)}$, where $\mathbf{1}$ denotes the all-one vector. Again the result follows from (3).

□

The *span* of a vector $\mathbf{c} = (c_1, \ldots, c_n)$ is the integer interval $sp(\mathbf{c}) = \{m, \ldots, l\}$ such that $c_m = c_l = 1$ and $c_i = 0$ if $1 \leq i < m$ or $l < i \leq n$. Similarly, the span of an r-dimensional subcode $< \mathbf{c}_1, \ldots, \mathbf{c}_r >$ generated by $\mathbf{c}_1, \ldots, \mathbf{c}_r$ is given by $\cup_{j=1}^{r} sp(\mathbf{c}_i)$.

Theorem 1. *Let* $W(\mathcal{C}) \subseteq \{d, \ldots, 2d-1\} \cup \{n\}$. *Then* $s(\mathcal{C}) \geq k-1$.

Proof. If $k < 3$ the result is trivial, so assume that $k \geq 3$.

Suppose, on the contrary, that $s(\mathcal{C}) \leq k-2$. Define i by $\dim\left(\mathcal{C}_p^{(i)}\right) = 2$ and $\dim\left(\mathcal{C}_p^{(i-1)}\right) = 1$.

Now let $< \mathbf{c}_1, \mathbf{c}_2 >= \mathcal{C}_p^{(i)}$, and assume that $\mathbf{c}_1 \in \mathcal{C}_p^{(i-1)}$. Then $sp(\mathbf{c}_1) = \{1, \ldots, j\}$ for some $j < i$. By assumption, there is another codeword, $\mathbf{c}_3$, such that $\mathbf{c}_3 \in \mathcal{C}_f^{(i-1)}$. Note that $sp(\mathbf{c}_3) \cap sp(\mathcal{C}_p^{(i)}) \subseteq \{i\}$. Since the supports of $\mathbf{c}_1$ and $\mathcal{C}_f^{(j)}$ are disjoint, it follows from the conditions in the theorem that $\mathcal{C}_f^{(j)}$ contains at most one nonzero codeword $\mathbf{c}_3$, which is the complement of $\mathbf{c}_1$. This is possible only if $j = i-1$ and $\mathbf{c}_1$ has weight j. Consider the following graphical description of $\mathcal{C}_p^{(i)}$ and $\mathbf{c}_3$:

$$\begin{array}{lccccccc} & & & & (i-1) & (i) & & \\ \mathbf{c}_1: & 1 & \cdots & & 1 & 0 & \cdots & 0 \\ \mathbf{c}_2: & 0 & \cdots 01 \cdots & & & 1 & 0 \cdots & 0 \\ \mathbf{c}_3: & 0 & \cdots & & 0 & 1 & \cdots & 1 \end{array} \tag{4}$$

From Lemma 1, considering Res($\mathcal{C}$,$\mathbf{c}_1$) and $\mathbf{c}_2$, we get $1 \geq d - \left\lfloor \frac{w(\mathbf{c}_1)}{2} \right\rfloor = d - \left\lfloor \frac{n - w(\mathbf{c}_3)}{2} \right\rfloor$, implying $w(\mathbf{c}_3) \leq n - 2d + 2 \leq d + 1$. The last inequality follows from the conditions of the theorem, which imply that $n - d \leq 2d - 1$.

Next, consider *any* codeword $\mathbf{c}_4$ not in $< \mathbf{c}_1, \mathbf{c}_3 >$. Applying Lemma 1 to Res($\mathcal{C}$,$\mathbf{c}_3$), the restriction of $\mathbf{c}_4$ to the first $i-1$ coordinate positions has weight at least $d - \lfloor (d+1)/2 \rfloor = \lfloor d/2 \rfloor$. The relationship between $\mathbf{c}_1, \mathbf{c}_3$, and $\mathbf{c}_4$ can now be illustrated in the following

manner:

$$\begin{array}{lccccccccc} & & & & \geq \lfloor d/2 \rfloor & & (i) & & \\ \mathbf{c}_1: & 1 & \cdots & \overbrace{\cdots\cdots\cdots 1} & & 0 & \cdots & 0 & \\ \mathbf{c}_4: & & & 1\cdots\cdots\cdots & & & & & \\ \mathbf{c}_3: & 0 & \cdots & & 0 & & 1 & \cdots & \end{array} \tag{5}$$

Observe that $\dim\left(\mathcal{C}_p^{(i-2)}\right) = 0$. If $d \geq 4$, then it follows from (5) that $\dim\left(\mathcal{C}_f^{(i-2)}\right) = 1$, so $s(\mathcal{C}) \geq k-1$. If $d = 3$, we have $W(\mathcal{C}) \subseteq \{3,4,5\} \cup \{n\}$, $n \leq 8, k \leq 4$. A close inspection of the possibilities gives the desired result also for $d = 3$.

□

Lemma 4 [3]. *Let $\{\mathcal{S}_i^{\perp}\}$ be the state spaces associated with the dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$. Then* $\dim(\mathcal{S}_i) = \dim\left(\mathcal{S}_i^{\perp}\right), 0 \leq i \leq n$.

Remark. Lemma 2c) and Theorem 1 apply to a wide range of well known and commonly used block codes. For instances,

- t-error correcting BCH codes have dual codes that satisfy the condition in Lemma 2c) provided the length is sufficiently large (MacWilliams and Sloane [9, pp. 280–281]: The Carlitz-Uchiyama bound), thus
- extended t-error correcting BCH codes have dual codes that satisfy the condition in Theorem 1 provided the length is sufficiently large.
- All self-complementary codes of minimum distance $> n/3$ satisfy the condition in Theorem 1.
- In particular, the lower bounds on the trellis complexity s for [16,7,6], [32,21,6], [32,11,12], [64,51,6], [64,18,22], and [64,16,24] codes in Table 4 of [5] are increased by one, determining $s(\mathcal{C})$ in those cases.

Acknowledgment

This work was done during a visit to IBM Almaden Research Center. The author

would like to thank Alexander Vardy for helpful comments. Also thanks to Kjell Jørgen Hole who proofread the paper (and who must share the blame for any remaining errors).

References

[1] J. K. Wolf, "Efficient maximum-likelihood decoding of linear block codes," *IEEE Transactions on Information Theory*, vol. IT-24, pp. 76–80, January 1978.

[2] D. J. Muder, "Minimal trellises for block codes," *IEEE Transactions on Information Theory*, vol. IT-34, pp. 1049–1053, September 1988.

[3] G. D. Forney, Jr., "Coset codes II: Binary lattices and related codes," *IEEE Transactions on Information Theory*, vol. IT-34, pp. 1152–1187, September 1988.

[4] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams of binary linear codes," *IEEE Transactions on Information Theory*, vol. IT-39, pp. 242–245, January 1993.

[5] A. Vardy and Y. Be'ery, "Maximum-likelihood soft decision decoding of BCH codes," *IEEE Transactions on Information Theory*, vol. IT-40, pp. 546–554, March 1994.

[6] A. Lafourcade and A. Vardy, "Asymptotically good codes have infinite trellis complexity," *IEEE Transactions on Information Theory*, vol. IT-41, pp. 555–558, March 1995.

[7] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Transactions on Information Theory*, vol. IT-40, pp. 1741–1752, November 1994.

[8] H. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," *Discrete Math.*, vol. 33, pp. 197–207, 1981.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.