Constructions of Generalized Concatenated Codes and Their Trellis-Based Decoding Complexity

Robert H. Morelos-Zaragoza
LSI LOGIC Corp., robert.morelos-zaragoza@sjsu.edu

Toru Fujiwara
Osaka University

Tadao Kasami
Nara Institute of Science and Technology

Shu Lin
University of Hawaii at Manoa

[10] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pt. 2, pp. 1924–1937, Nov. 1995.

[11] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inform. Theory*, vol. 42, pt. 1, pp. 1828–1838, Nov. 1996.

[12] V. I. Levenshtein, "The application of Hadamard matrices to a problem in coding," *Probl. Kibern.*, vol. 5, pp. 123–136, 1961; *Problems of Cybernetics*, vol. 5, pp. 166–184, 1964 (Engl. transl.).

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

[14] J. L. Massey, "Foundations and methods of channel coding," in *Proc. Int. Conf. Inform. Theory Syst.*, NTG-Fachberichte, Berlin, Germany, Sept. 1978, vol. 65, pp. 148–157.

[15] R. J. McEliece, "On the BCJR trellis for linear block codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1072–1092, July 1996.

[16] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049–1053, Sept. 1988.

[17] A. A. Nechaev, "The Kerdock code in a cyclic form," *Diskret. Math.*, vol. 1, pp. 123–139, 1989; *Diskrete Math. Appl.*, vol. 1, pp. 365–384, 1991 (Engl. transl.).

[18] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Inform. Contr.*, vol. 11, pp. 613–616, 1967.

[19] R. E. A. C. Paley, "On orthogonal matrices," *J. Math. Phys.*, vol. 12, pp. 311–320, 1933.

[20] V. Sidorenko, "The Euler characteristic of the minimal code trellis," *Problems Inform. Transm.*, vol. 33, no. 1, pp. 87–93, Jan./Mar. 1997.

[21] V. Sidorenko, G. Markarian, and B. Honary, "Minimal trellis design for linear codes based on the Shannon product," *IEEE Trans. Inform. Theory*, vol. 42, pt. 1, pp. 2048–2053, Nov. 1996.

[22] N. J. A. Sloane and J. J. Seidel, "A new family of nonlinear codes obtained from conference matrices," *Ann. NY Acad. Sci.*, Article 1, vol. 175, pp. 363–365, 1970.

[23] A. Vardy and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the optimality of the minimal trellis," *IEEE Trans. Inform. Theory*, vol. 42, pt. 1, pp. 2027–1834, Nov. 1996.

[24] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. 13, pp. 260–269, Apr. 1967.

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

[26] J. K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76–80, Jan. 1978.

[27] V. Zyablov and V. Sidorenko, "Bounds on complexity of trellis decoding of linear block codes," *Problems Inform. Transm.*, vol. 29, no. 3, pp. 3–9, July–Sept. 1993.

Constructions of Generalized Concatenated Codes and Their Trellis-Based Decoding Complexity

Robert Morelos-Zaragoza, *Senior Member, IEEE*, Toru Fujiwara, *Member, IEEE*, Tadao Kasami, *Life Fellow, IEEE*, and Shu Lin, *Fellow, IEEE*

***Abstract*—In this correspondence, constructions of generalized concatenated (GC) codes with good rates and distances are presented. Some of the proposed GC codes have simpler trellis complexity than Euclidean geometry (EG), Reed–Muller (RM), or Bose–Chaudhuri–Hocquenghem (BCH) codes of approximately the same rates and minimum distances, and in addition can be decoded with trellis-based multistage decoding up to their minimum distances. Several codes of the same length, dimension, and minimum distance as the best linear codes known are constructed.**

***Index Terms*— Generalized concatenated codes, multistage decoding, trellis complexity.**

I. Introduction

The trellis structure of linear block codes was first introduced in [1] and later studied in [2]. In [2] it is shown that every binary linear (n, k) code has an n-section trellis diagram with at most $2^{\min\{k, n-k\}}$ states. Later on, the trellis structure of Reed–Muller (RM) codes was analyzed in [3], where a minimal trellis construction for linear block codes was presented. Since then, there has been a considerable amount of research effort devoted to the study and applications of the trellis structure of linear block codes.

A trellis diagram (or a trellis) for a linear block code with the minimum number of states is said to be minimal. A minimal trellis is unique up to graph isomorphism [3]–[5]. It has been shown [3]–[6] that the state complexity of a minimal trellis for a linear block code depends on the order of its code symbol positions. However, symbol ordering does not affect the trellis state complexity of maximum-distance-separable (MDS) codes. (This result will be particularly useful in this correspondence, as many of the outer codes used in the proposed concatenated constructions are MDS codes.)

Generalized concatenated (GC) codes were introduced by Zinoviev [7] and by Blokh and Zyablov [8] in 1976, and form a powerful family of error-correcting codes that can correct both random errors and random bursts of errors. In addition, GC codes are a class of multilevel codes that are amenable to *multistage decoding*, which provides a good tradeoff between error performance and decoding complexity.

Manuscript received April 11, 1996; revised September 22,1996. This work was supported in part by NSF under Grant NCR-9415374, NASA under Grant NAG 5-931 and the Ministry of Education, Japan, under Grant (C) 06650416. The material in this correspondence was presented in part at the 1993 Symposium on Information Theory and its Applications, Kanazawa, Japan, October 1993, and at the 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, June 1994.

R. Morelos-Zaragoza is with LSI LOGIC Corp., Milpitas, CA 95035 USA.

T. Fujiwara is with the Faculty of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531 Japan.

T. Kasami was with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Nara 630-0101 Japan. He is now with the Faculty of Information Science, Hiroshima City University, Hiroshima 731-3194 USA.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822 USA.

Communicated by A. Vardy, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)01385-1.

In this correspondence, good GC codes are constructed. These codes are good in the sense that they have lower trellis-based decoding complexities compared with permuted Bose–Chaudhuri–Hocquanghem (BCH), RM, and Euclidean geometry (EG) codes of the same lengths, the same (or approximately the same) rates and minimum distances, and that they can be decoded with trellis-based multistage decoding up to their minimum distances. The decoding complexity of a GC code C is measured both by the maximum number of states in an n-section trellis for C and by the number of addition-equivalent operations required in a Viterbi decoder using a minimal trellis for C.

II. Minimal Trellises and State Complexities of Decomposable Codes

In this section, the connection between symbol orderings of linear codes and reduced upper bounds on the state complexity of their trellis diagrams is pointed out. A sufficient condition on the minimality of the product of trellises is also presented. In a later section, it is shown that if for each component code of a decomposable code there is an optimal ordering, then the ordering is also optimal for the overall code.

Throughout the correspondence, (n, k, d) is used to denote the parameters of a linear block code of length n, dimension k, and minimum distance d. Let C be an (n, k, d) linear code over GF(q). Suppose that C is a decomposable code, defined, in terms of its linear (n, k_i, d_i) subcodes C_i with $1 \le i \le M$, by the following conditions:

(S) $C = C_1 + C_2 + \cdots + C_M \triangleq \{\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_M : \boldsymbol{u}_i \in C_i$ with $1 \le i \le M\}$.

(D) For $\boldsymbol{u}_i \in C_i$ with $1 \le i \le M$, $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_M = \mathbf{0}$ (the zero codeword) if and only if $\boldsymbol{u}_1 = \boldsymbol{u}_2 = \cdots = \boldsymbol{u}_M = \mathbf{0}$.

Then it follows from (S) and (D) that

$$k = k_1 + k_2 + \cdots + k_M. \tag{1}$$

Let T and T_i with $1 \le i \le M$ denote the minimal trellis diagrams for C and C_i, respectively. As defined in [10] and [11], the direct product of M trellis diagrams, $T_1, T_2, \cdots, T_M$, denoted $T_1 \otimes T_2 \otimes \cdots \otimes T_M$, is a trellis diagram defined as follows: The states in the product are M-tuples $(s_1, s_2, \cdots, s_M)$, where s_i is a state of trellis T_i, $1 \le i \le M$, and there exists a branch of label $\ell = \ell_1 \oplus \ell_2 \oplus \cdots \oplus \ell_M$ with initial state $(s_1, s_2, \cdots, s_M)$ and final state $(s'_1, s'_2, \cdots, s'_M)$ if, and only if, there is a branch of label ℓ_i from state s_i to state s'_i in trellis T_i, $i = 1, 2, \cdots, M$.

Given a code symbol ordering for a code C, there is a unique trellis diagram (or trellis) with the minimum number of states for C, called the *minimal trellis diagram* (or minimal trellis) for C. For $1 \le j \le n$ and $1 \le i \le M$, let $s_j(T)$ and $s_j(T_i)$ denote the logarithms base q of the numbers of states of T and T_i just after the jth code symbol. These numbers are known as the *state complexities* of T and T_i. Since the product of T_i with $1 \le i \le M$ is a trellis for C, we have that

$$s_j(T) \le \sum_{i=1}^{M} s_j(T_i), \qquad \text{for } 1 \le j \le n. \tag{2}$$

For a linear code C of length n, let $s_{\max}(T)$ denote the maximum number of states at any bit position of a minimal n-section trellis T for C. The quantity $s_{\max}(T)$ will be referred to as the *state complexity* of code C. It follows from (2) and Wolf's bound [2] that

$$s_{\max}(T) \triangleq \max_{0 \le j \le n} s_j(T) \le \sum_{i=1}^{M} \min(k_i, n - k_i). \tag{3}$$

For several classes of codes such as RM codes or their subcodes and repetition codes, and their dual codes, there are known code symbol orderings [6], [9] which result in reduced upper bounds on the state complexity of their trellis diagrams compared with Wolf's bound. If there is such a code among C_i with $1 \le i \le M$, then we can adopt the corresponding symbol ordering and evaluate the state complexity of trellis diagram for C by applying upper bounds which are independent of any symbol ordering of each remaining component code.

Suppose that

$$C^{j-} = C_1^{j-} + \cdots + C_M^{j-} \tag{4}$$
$$C^{j+} = C_1^{j+} + \cdots + C_M^{j+} \tag{5}$$

where

$$C_i^{j-} \triangleq \{\boldsymbol{u} \in C : u_\ell = 0, 1 \le \ell \le j\}$$

and

$$C_i^{j+} \triangleq \{\boldsymbol{u} \in C : u_\ell = 0, j < \ell \le n\}$$

are the *past* and *future* subcodes of C_i, $1 \le i \le M$, respectively. Then it follows from (4), (5), and property (D) that

$$k(C^{j-}) = k(C_1^{j-}) + \cdots + k(C_M^{j-}) \tag{6}$$
$$k(C^{j+}) = k(C_1^{j+}) + \cdots + k(C_M^{j+}). \tag{7}$$

Equations (6) and (7) imply that, under the assumptions (4) and (5)

$$s_j(T) = \sum_{i=1}^{M} s_j(T_i) \tag{8}$$

for any j with $1 \le j \le n$.

A sufficient condition for (4) (or (5)) to hold is given by

(P) For $\boldsymbol{u}_i \in C_i^{j-}$ (or C_i^{j+}) with $1 \le i \le M$, $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_M = \mathbf{0}$, if and only if $\boldsymbol{u}_i = \mathbf{0}$ for $1 \le i \le M$.

Example 1: Suppose that for $1 \le M' \le M$, the supports [12] of $C_1, C_2, \cdots, C_{M'}$ are mutually disjoint (this property is called "DS structure" in [13]). Let $m(C_i)$ denote the *effective length* of C_i, i.e., the size of the support of C_i, $1 \le i \le M'$. If we use a symbol ordering such that for $1 \le i \le M'$, any codeword of C_i has nonzero components only from the $(\sum_{h=1}^{i-1} m(C_h) + 1)$th to $(\sum_{h=1}^{i} m(C_h))$th symbol positions, then the logarithm of the number of states at any symbol position of the minimal trellis T for $C = C_1 + C_2 + \cdots + C_{M'}$ is upper-bounded by

$$s_{\max}(T) = \max_{1 \le h \le M'} \min\{k_h, m(C_h) - k_h\}.$$

Note that C satisfies the definition of direct-sum in [14]. □

III. Constructions of Generalized Concatenated Codes

Suppose that n is the product of two integers n_I and n_O greater than one. For $1 \le i \le M$, let C_{Ii} be an (n_I, k_{Ii}) linear code over GF(q) such that

(D$_\mathrm{I}$) for $\boldsymbol{u}_i \in C_{Ii}$ with $1 \le i \le M$, $\boldsymbol{u}_1 + \boldsymbol{u}_2 + \cdots + \boldsymbol{u}_M = \mathbf{0}$, if and only if $\boldsymbol{u}_i = \mathbf{0}$ for $1 \le i \le M$.

Let δ_i be the minimum Hamming distance of $C_{Ii} + C_{Ii+1} + \cdots + C_{IM}$. Let C_{Oi} be an (n_O, k_{Oi}, d_{Oi}) linear code over GF$(q^{k_{Ii}})$ and let C_i^* denote the concatenated code over GF(q) with C_{Ii} as the inner code and C_{Oi} as the outer code. The n code symbol positions in C_i^* are divided into n_O consecutive sections of length n_I in such a way that each section of a codeword in C_i^* is a codeword in C_{Ii}. Let the generalized concatenated code C be defined as

$$C \triangleq C_1^* + C_2^* + \cdots + C_M^*. \tag{9}$$

Then, the condition (D) on C follows from the condition ($\mathrm{D_I}$). The minimum Hamming distance d of C is lower-bounded [15] as

$$d \geq \min_{1 \leq i \leq M} \delta_i d_{Oi} \tag{10}$$

and a multistage decoding [15] up to the distance given by the right-hand side of (10) is possible.

Let $T^{(n_O)}$ and $T_i^{(n_O)}$, with $1 \leq i \leq M$, denote the minimal n_O-section trellis diagrams for C and C_i^*, respectively, for which each section has length n_I. Then the assumption ($\mathrm{D_I}$) guarantees that if j is a multiple of n_I then property (P) holds. Therefore, at each end of a section,

$$s_j(T^{(n_O)}) = \sum_{i=1}^{M} s_j(T_i^{(n_O)}). \tag{11}$$

The above result means that, if there is a common optimal ordering of sections that gives the smallest state complexity of an n_O-section trellis diagram for each component code C_i^*, then the ordering of sections is optimal for the whole code C. See also [16, Theorem 8.1].

A particular class of binary GC codes over $\mathrm{GF}(q)$ can be constructed as follows. An (n_I, k_1, d_1) code C_1, over $\mathrm{GF}(q)$, is partitioned into a chain of M (n_I, k_i, d_i) subcodes C_i, $i = 2, 3, \cdots, M+1$, such that

$$C_1 \supset C_2 \supset \cdots \supset C_{M+1}$$

where, for convenience, we define $C_{M+1} \triangleq \{\bar{0}\}$, and $d_{M+1} \triangleq \infty$. Let $C_{Ii} = [C_i/C_{i+1}]$ denote an (n_I, k_{Ii}, δ_i) subcode of C_i, a set of coset representatives of C_{i+1} in C_i, of dimension $k_{Ii} = k_i - k_{i+1}$, and minimum Hamming distance $\delta_i \geq d_i$. Then C_1 has the following *coset decomposition* [3]:

$$C_1 = C_{I1} + C_{I2} + \cdots + C_{IM}. \tag{12}$$

Let C_{Oi} denote an (n_O, k_{Oi}, d_{Oi}) code C_{Oi} over $\mathrm{GF}(q^{k_{Ii}})$, where

$$k_{Ii} = \dim(C_i/C_{i+1}) = k_i - k_{i+1}, \qquad i = 1, 2, \cdots, M.$$

A GC code C is constructed from (9) as a direct sum of concatenated codes

$$C = C_{O1} * C_{I1} + C_{O2} * C_{I2} + \cdots + C_{OM} * C_{IM}$$

where $C_{Oi} * C_{Ii}$ denotes a concatenated code with C_{Oi} as outer code and C_{Ii} as inner code, $1 \leq i \leq M$. It was shown in [8] that C is an $(n_O n_I, k, d)$ linear block code of dimension and minimum Hamming distance

$$k = \sum_{i=1}^{M} k_{Ii} k_{Oi} \quad \text{and} \quad d \geq \min_{1 \leq i \leq M} \{\delta_i d_{Oi}\} \tag{13}$$

respectively. Note that equality holds in (13) when C_{Ii}, $1 \leq i \leq M$, contains the all-zero codeword, which is the case for all the codes presented in this correspondence.

Example 2: In this example, the trellis structure of a simple binary GC code is illustrated. Let $n_I = n_O = 4$, and consider the binary code $C_I = \mathrm{RM}_{2,2}$. Then $M = 3$ and $C_I = C_{I1} + C_{I2} + C_{I3}$, where $C_{I1} = \mathrm{RM}_{2,2}/\mathrm{RM}_{2,1}$ with generator matrix $G_{I1} = (0001)$, $C_{I2} = \mathrm{RM}_{2,1}/\mathrm{RM}_{2,0}$ with $G_{I2} = \binom{0101}{0011}$, and $C_{I3} = \mathrm{RM}_{2,0}$ with $G_{I3} = (1111)$. Let C_{O1} be a binary $(4, 1, 4)$ repetition code, C_{O2} be a nonbinary $(4, 3, 2)$ over $\mathrm{GF}(2^2)$, and C_{O3} be a binary $(4, 4, 1)$ universal code. Then $C = C_{O1} * C_{I1} + C_{O2} * C_{I2} + C_{O3} * C_{I3}$ is a binary GC $(16, 11, 4)$ code. The four-section trellis diagrams of codes $C_{Oj} * C_{Ij}$, $j = 1, 2, 3$ are shown in Fig. 1 where $\mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$, with $\alpha^2 = 1 + \alpha$. In the subtrellis for Fig. 1(b), each element in the binary vector space $\{0, 1\}^2$, isometric to $\mathrm{GF}(2^2)$, is mapped onto a codeword in C_{I2}. As a result, the following four-bit vector representation of $\mathrm{GF}(2^2)$ is obtained: $0 = 0000$, $1 = 0011$, $\alpha = 0101$, and $\alpha^2 = 0110$.

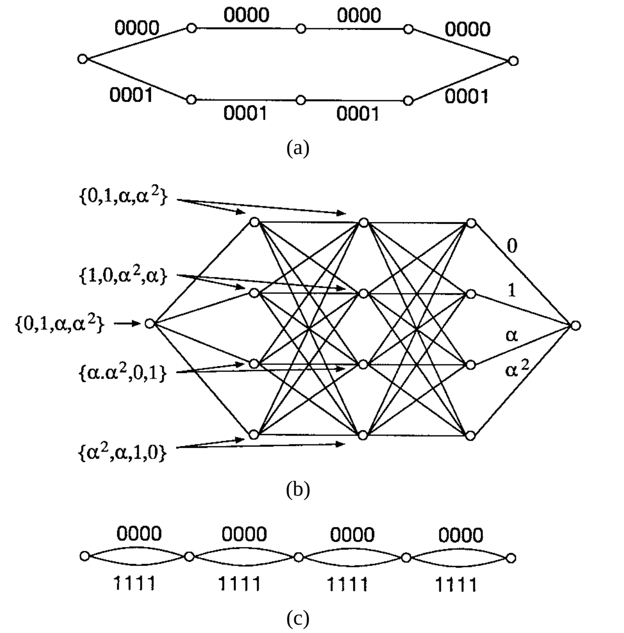

Fig. 1. Component subtrellises for a binary GC $(16, 11, 4)$ code. (a) $C_{O1} * C_{I1}$. (b) $C_{O2} * C_{I2}$. (c) $C_{O3} * C_{I3}$.

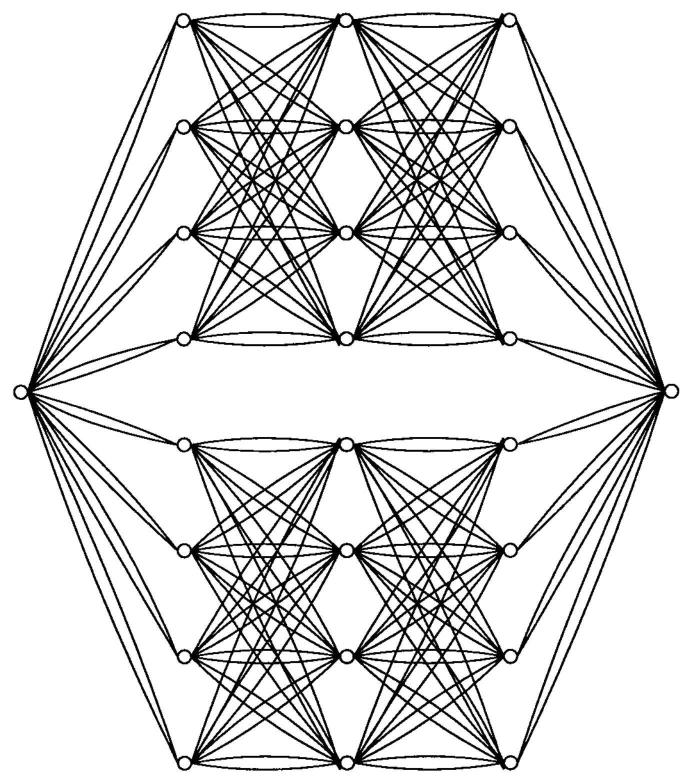

Fig. 2. A four-section trellis for the binary GC $(16, 11, 4)$ code.

The corresponding four-section diagram of the binary GC $(16, 11, 4)$ code is shown in Fig. 2. It consists of two parallel and identical, up to branch labeling, subtrellises. Each subtrellis is in turn isometric, up to parallel branches, to the subtrellis of code

$C_{O2} * C_{I2}$. Also, each set of parallel branches has labels

$$\{(b_0b_1b_2b_3),\,(b_0b_1b_2b_3)+(1111)\} = \{(b_0b_1b_2b_3),\,(\bar{b}_0\bar{b}_1\bar{b}_2\bar{b}_3)\}.$$

The two parallel subtrellises have branch labels that differ by (0001), i.e., if $(b_0b_1b_2b_3)$ is the label of a brance in the upper subtrellis, the $(b_0b_1b_2b_3)+(0001) = (b_0b_1b_2\bar{b}_3)$ is the label of a branch in the lower subtrellis. □

Let $s(T_i^{(n_O)})$ denote the logarithm base q of the maximum number of states of a minimal n_O-section trellis for the ith-level concatenated code $C_{Oi} * C_{Ii}$, $1 \le i \le M$, and let $s(T^{(n_O)})$ denote the logarithm base q of the maximum number of states of an n_O-section trellis for the overall GC code. Then it follows from (11) and Wolf's bound [2] that

$$s(T^{(n_O)}) = \sum_{i=1}^{M} s(T_i^{(n_O)}) \le \sum_{i=1}^{M} k_{Ii}\,\min\{k_{Oi},\,n_O - k_{Oi}\}. \quad (14)$$

In the following, several good binary GC codes are constructed that can be decoded using a multistage decoding up to their minimum distances. The GC construction is best explained by considering the following example.

Example 3: A binary $(q = 2)$ GC code of length 63 will be constructed. Let $n_I = 7$ and $n_O = 9$. Consider the partition of a $(7,\,7,\,1)$ binary code C_1 into the following subcode chain:

$$(7,\,7,\,1) \supset (7,\,6,\,2) \supset (7,\,3,\,4) \supset \{\bar{0}\}.$$

Then $M = 3$ and C_1 can be expressed as $C_1 = C_{I1} + C_{I2} + C_{I3}$, where $C_{I1} = [(7,\,7,\,1)/(7,\,6,\,2)]$ is a $(7,\,1,\,1)$ code with codewords $\{0000000,\,0000001\}$, $C_{I2} = [(7,\,6,\,2)/(7,\,3,\,4)]$ is a $(7,\,3,\,2)$ code and has a generator matrix

$$G_{I2} = \begin{pmatrix} 0010001 \\ 0000101 \\ 0000011 \end{pmatrix}$$

and $C_{I3} = [(7,\,3,\,4)/\{\bar{0}\}]$ is equivalent to the dual of a Hamming code of length 7 with a generator matrix

$$G_{I3} = \begin{pmatrix} 1010101 \\ 0110011 \\ 0001111 \end{pmatrix}.$$

Let C_{O1} be a binary $(9,\,2,\,6)$ code, the product of a $(3,\,1,\,3)$ binary code and a $(3,\,2,\,2)$ binary code, and let C_{O2} and C_{O3} be $(9,\,7,\,3)$ and $(9,\,8,\,2)$ maximum-distance-separable (MDS) codes over GF$\,(2^3)$, respectively. Then it follows from (9) and (13) that C is a binary $(63,\,47,\,6)$ GC code. □

Table I lists good GC codes constructed using this technique. The parameters of the code in Example 3 are listed in the first entry of Table I. The binary $(63,\,43,\,8)$ GC code, the second entry of Table I, was constructed using the same inner code C_1, and its subcode chain, as in Example 3 above. The third entry of Table I is a binary $(63,\,24,\,16)$ GC code that was constructed based on the $(7,\,6,\,2)$ parity-check code and its $(7,\,3,\,4)$ subcode. For all the other binary GC codes presented in Table I, C_1 is the $(8,\,8,\,1)$ code and its chain of RM subcodes

$$\mathrm{RM}_{3,\,3} \supset \mathrm{RM}_{3,\,2} \supset \mathrm{RM}_{3,\,1} \supset \mathrm{RM}_{3,\,0} \supset \{\bar{0}\}$$

where $\mathrm{RM}_{m,\,r}$ denotes the binary RM code of length 2^m and minimum Hamming distance 2^{m-r}. Then $C_{Ii} = [\mathrm{RM}_{3,\,3-i+1}/\mathrm{RM}_{3,\,3-i}]$, $1 \le i \le 4$, $\mathrm{RM}_{3,\,-1} \triangleq \{\bar{0}\}$. It follows from (12) that

$$\begin{aligned}\mathrm{RM}_{3,\,3} &= [\mathrm{RM}_{3,\,3}/\mathrm{RM}_{3,\,2}] + [\mathrm{RM}_{3,\,2}/\mathrm{RM}_{3,\,1}] \\ &\quad + [\mathrm{RM}_{3,\,1}/\mathrm{RM}_{3,\,0}] + \mathrm{RM}_{3,\,0}.\end{aligned}$$

TABLE I

CONSTRUCTIONS OF GENERALIZED CONCATENATED CODES

C	M	i	$C_{Oi} \star C_{Ii}$	δ_i	$\delta_i d_{Oi}$	$s(T_i^{(n_O)})$	$s(T^{(n_O)})$
$(63,47,6)$	3	1	$(9,2,6) \star (7,1)$	1	6	2	11
		2	$(9,7,3) \star (7,3)$	2	6	6	
		3	$(9,8,2) \star (7,3)$	4	8	3	
$(63,43,8)$	3	1	$(9,1,9) \star (7,1)$	1	9	1	13
		2	$(9,6,4) \star (7,3)$	2	8	9	
		3	$(9,8,2) \star (7,3)$	4	8	3	
$(63,24,16)$	2	1	$(9,2,8) \star (7,3)$	2	16	6	15
		2	$(9,6,4) \star (7,3)$	4	16	9	
$(72,52,8)$	4	1	$(9,1,9) \star \mathrm{RM}_{3,3}/\mathrm{RM}_{3,2}$	1	9	1	13
		2	$(9,6,4) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	8	9	
		3	$(9,8,2) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	8	3	
		4	$(9,9,1) \star \mathrm{RM}_{3,0}$	8	8	0	
$(72,32,16)$	3	1	$(9,2,8) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	16	6	16
		2	$(9,6,4) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	16	9	
		3	$(9,8,2) \star \mathrm{RM}_{3,0}$	8	16	1	
$(64,45,8)$	4	1	$(8,1,8) \star \mathrm{RM}_{3,3}/\mathrm{RM}_{3,2}$	1	8	1	13
		2	$(8,5,4) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	8	9	
		3	$(8,7,2) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	8	3	
		4	$(8,8,1) \star \mathrm{RM}_{3,0}$	8	8	0	
$(64,25,16)$	3	1	$(8,1,8) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	16	3	13
		2	$(8,5,4) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	16	9	
		3	$(8,7,2) \star \mathrm{RM}_{3,0}$	8	16	1	
$(64,48,6)$	4	1	$(8,1,8) \star \mathrm{RM}_{3,3}/\mathrm{RM}_{3,2}$	1	8	1	10
		2	$(8,6,3) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	6	6	
		3	$(8,7,2) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	8	3	
		4	$(8,8,1) \star \mathrm{RM}_{3,0}$	8	8	0	
$(64,37,10)$	3	1	$(8,4,5) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	10	12	19
		2	$(8,6,3) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	12	6	
		3	$(8,7,2) \star \mathrm{RM}_{3,0}$	8	16	1	
$(64,34,12)$	3	1	$(8,3,6) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	12	9	16
		2	$(8,6,3) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	12	6	
		3	$(8,7,2) \star \mathrm{RM}_{3,0}$	8	16	1	
$(64,28,14)$	3	1	$(8,2,7) \star \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$	2	14	6	16
		2	$(8,5,4) \star \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0}$	4	16	9	
		3	$(8,7,2) \star \mathrm{RM}_{3,0}$	8	16	1	

The last three codes in Table I of this correspondence were also presented (up to a possible permutation of positions) in [18]. All codes listed in Table I, except the last row, have the same parameters n, k, and d, as the *best linear codes* known [17]. The $(64,\,45,\,8)$ GC code has the same rate, minimum distance and decoding complexity (see next section) as a $(64,\,45,\,8)$ extended and permuted BCH code. Apparently, these codes are equivalent, as are the $(64,\,37,\,10)$ GC code and a $(64,\,37,\,10)$ extended and permuted EG code, according to [18]. Some of the GC codes in Table I have either smaller decoding complexities than BCH or EG codes of comparable rate, as it is shown in the next section, or more information bits for the same minimum distance.

Table II lists the parameters of other binary GC codes of longer lengths constructed based on other choices of the inner code C_1. The first three codes listed in Table II are constructed based on a $(5,\,5,\,1)$ code and its $(5,\,4,\,2)$ subcode, while the remaining codes are based on $\mathrm{RM}_{4,\,r}$, $r = 4,\,3,\,2,$ and its RM subcodes. It is important to note that, for binary GC codes in general, equality in (10) does not always hold. This is to say that the right-hand side (RHS) of (10) is in most cases significantly lower than the actual minimum distance d. For all the codes listed in Tables I and II, however, equality holds in (10) and a trellis-based *multistage decoding up to their minimum distances* can be employed.

IV. DECODING COMPLEXITY

In this section, the decoding complexity of some of the proposed GC codes is analyzed and compared with that of RM, BCH, or EG codes of the same lengths and the same, or approximately the same, rates and minimum distances.

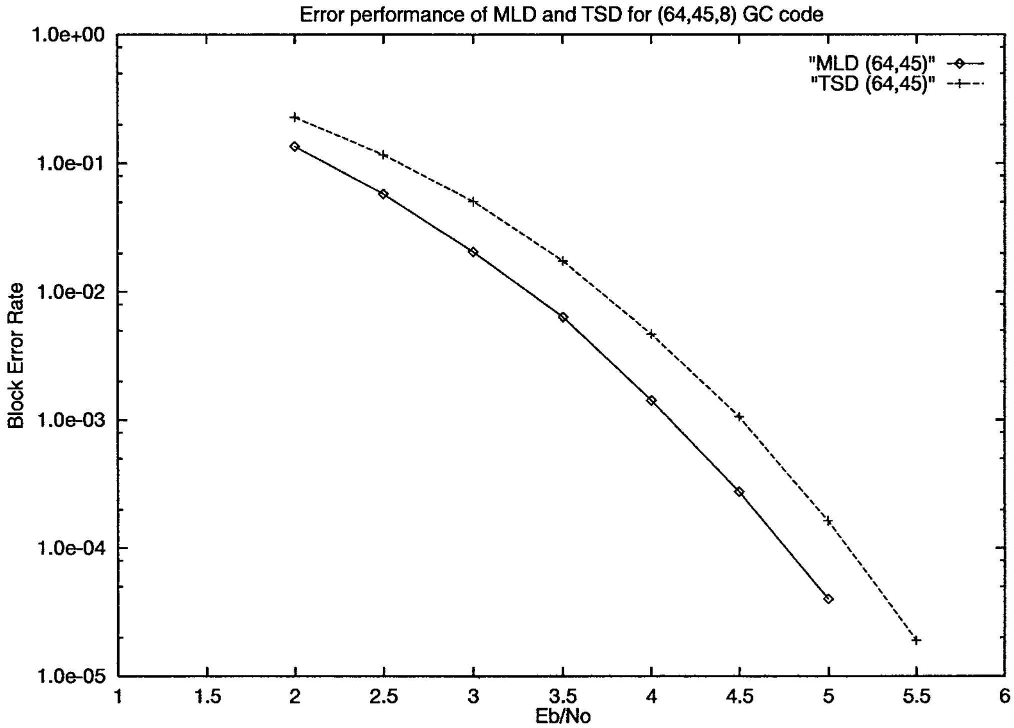

Fig. 3. Simulation results for a binary GC $(64, 45, 8)$ code.

TABLE II
ADDITIONAL CONSTRUCTIONS OF GENERALIZED CONCATENATED CODES

C	M	i	$C_{Oi} \star C_{Ii}$	δ_i	$\delta_i d_{Oi}$	$s(T_i^{(no)})$	$s(T^{(no)})$
$(85, 53, 10)$	2	1	$(17, 1, 17) \star (5, 1)$	1	17	1	17
		2	$(17, 13, 5) \star (5, 4)$	2	10	16	
$(85, 49, 12)$	2	1	$(17, 1, 17) \star (5, 1)$	1	17	1	21
		2	$(17, 12, 7) \star (5, 4)$	2	12	20	
$(85, 45, 14)$	2	1	$(17, 1, 17) \star (5, 1)$	1	17	1	25
		2	$(17, 11, 7) \star (5, 4)$	2	14	24	
$(128, 103, 8)$	5	1	$(8, 1, 8) \star \mathrm{RM}_{4,4}/\mathrm{RM}_{4,3}$	1	8	1	19
		2	$(8, 5, 4) \star \mathrm{RM}_{4,3}/\mathrm{RM}_{4,2}$	2	8	12	
		3	$(8, 7, 2) \star \mathrm{RM}_{4,2}/\mathrm{RM}_{4,1}$	4	8	6	
		4	$(8, 8, 1) \star \mathrm{RM}_{4,1}/\mathrm{RM}_{4,0}$	8	8	0	
		5	$(8, 8, 1) \star \mathrm{RM}_{4,0}$	16	16	0	
$(128, 33, 32)$	3	1	$(8, 1, 8) \star \mathrm{RM}_{4,2}/\mathrm{RM}_{4,1}$	4	32	6	19
		2	$(8, 5, 4) \star \mathrm{RM}_{4,1}/\mathrm{RM}_{4,0}$	8	32	12	
		3	$(8, 7, 2) \star \mathrm{RM}_{4,0}$	16	32	1	
$(144, 118, 8)$	5	1	$(9, 1, 9) \star \mathrm{RM}_{4,4}/\mathrm{RM}_{4,3}$	1	9	1	19
		2	$(9, 6, 4) \star \mathrm{RM}_{4,3}/\mathrm{RM}_{4,2}$	2	8	12	
		3	$(9, 8, 2) \star \mathrm{RM}_{4,2}/\mathrm{RM}_{4,1}$	4	8	6	
		4	$(9, 9, 1) \star \mathrm{RM}_{4,1}/\mathrm{RM}_{4,0}$	8	8	0	
		5	$(9, 9, 1) \star \mathrm{RM}_{4,0}$	16	16	0	
$(256, 222, 8)$	4	1	$(16, 13, 4) \star \mathrm{RM}_{4,3}/\mathrm{RM}_{4,2}$	2	8	12	18
		2	$(16, 15, 2) \star \mathrm{RM}_{4,2}/\mathrm{RM}_{4,1}$	4	8	6	
		3	$(16, 16, 1) \star \mathrm{RM}_{4,1}/\mathrm{RM}_{4,0}$	8	8	0	
		4	$(16, 16, 1) \star \mathrm{RM}_{4,0}$	16	16	0	
$(272, 237, 8)$	4	1	$(17, 14, 4) \star \mathrm{RM}_{4,3}/\mathrm{RM}_{4,2}$	2	8	12	18
		2	$(17, 16, 2) \star \mathrm{RM}_{4,2}/\mathrm{RM}_{4,1}$	4	8	6	
		3	$(17, 17, 1) \star \mathrm{RM}_{4,1}/\mathrm{RM}_{4,0}$	8	8	0	
		4	$(17, 17, 1) \star \mathrm{RM}_{4,0}$	16	16	0	

Consider a *binary* linear block code and its trellis-based soft-decision decoding using the Viterbi algorithm. To update the branch metrics, one addition operation is performed per branch, except for the first code symbol. On the other hand, the number of comparisons at each state, to determine the survivor branch sequence, equals the number of arriving branches minus one. It follows that the *total number of addition-equivalent decoding operations* is

$$\psi(T) \triangleq \sum_{j=1}^{n} 2 \times 2^{b_j(T)} - 2^{s_j(T)} - 2^{b_1(T)} \tag{15}$$

where $b_j(T)$ denotes logarithm base 2 of the number of branches in T for the jth code symbol position.

The number of addition-equivalent decoding operations can be reduced dramatically by using the recursive MLD algorithm proposed in [19]. In this correspondence, the number of addition-equivalent decoding operations by the recursive MLD algorithm, denoted $\psi_{\min}^{(0)}$ in [19], is also used as a complexity measure. In comparing the constructed GC codes with BCH and EG codes, the permutations presented in [19] are considered.

Table III lists the state complexity, $s_{\max}(T)$, (3), and the total number of addition-equivalent decoding operations for both Viterbi decoding, $\psi(T)$, and recursive MLD using optimally sectionalized trellis diagrams, $\psi_{\min}^{(0)}$, of some of the GC codes constructed in the previous section, compared with those of permuted RM, EG, or BCH codes of approximately the same rates and minimum distances. The $(63, 47, 6)$ and $(64, 48, 6)$ GC codes have a *considerably reduced decoding complexity* compared to either EG or BCH codes of about the same rate and minimum distance. The last two codes listed in the table, $(64, 34, 12)$ and $(64, 28, 14)$ GC codes, although of slightly smaller rate, both have reduced decoding complexity in comparison with BCH codes of the same minimum distance.

V. TWO-STAGE SOFT–DECISION DECODING

The multilevel structure of the GC codes constructed in this correspondence allows for the use of a suboptimal trellis-based multistage decoding. Consider the following trellis-based two-stage soft-decision decoding of a GC code C. Let C be expressed as a

TABLE III
THE DECODING COMPLEXITY OF SELECTED GC CODES

Code, C	Basis	$s_{\max}$	$\psi(T)$	$\psi_{\min}^{(0)}$	$\psi_{\mathrm{TSD}}^{(0)}$
GC $(63,47,6)$	—	12	259,065	223,561	18,198
EG $(63,48,5)$	B	13	453,049	256,841	—
GC $(63,43,8)$	—	14	1,186,809	954,761	49,942
RM $(63,42,7)$	—	14	763,961	320,801	—
BCH $(63,45,7)$	C	14	1,072,185	762,409	—
GC $(63,24,16)$	—	18	4,251,769	1,524,613	25,510
RM $(63,22,16)$	—	14	425,081	78,197	—
BCH $(63,24,15)$	B	16	1,327,225	271,733	—
GC $(72,52,8)$	—	14	1,417,977	1,196,601	50,554
GC $(72,32,16)$	—	19	12,534,009	5,817,521	249,746
GC $(64,45,8)$	—	14	1,082,105	893,489	34,842
BCH $(64,45,8)$	C	14	1,082,105	893,489	—
RM $(64,42,8)$	—	14	773,881	326,017	—
GC $(64,25,16)$	—	16	1,126,649	507,009	85,042
RM $(64,22,16)$	—	14	425,209	78,209	—
BCH $(64,24,16)$	B	16	1,327,353	271,745	—
GC $(64,48,6)$	—	11	214,777	185,057	10,650
EG $(64,48,6)$	B	13	456,441	282,353	—
BCH $(64,51,6)$	A	12	340,217	312,721	—
GC $(64,37,10)$	—	20	26,296,569	19,448,641	25,410
EG $(64,37,10)$	C	20	26,296,569	19,448,641	—
BCH $(64,39,10)$	C	20	38,436,857	24,741,161	—
GC $(64,34,12)$	—	19	10,240,249	5,751,649	17,794
BCH $(64,36,12)$	C	20	18,710,521	9,995,617	—
GC $(64,28,14)$	—	19	8,929,529	4,048,001	194,370
BCH $(64,30,14)$	C	21	35,028,985	16,091,009	—

direct sum $C = C_{s1} + C_{s2}$, where

$$C_{s1} \triangleq C_{O1} * C_{I1} + C_{O2} * C_{O1} + \cdots + C_{OL} * C_{IL},$$
$$C_{s2} \triangleq C_{O(L+1)} * C_{I(L+1)} + C_{O(L+2)} * C_{I(L+2)} + \cdots + C_{OM} * C_{IM}$$

with $1 \le L < M$.

Example 4: Let C be the $(64, 45, 8)$ GC code in Table III and let

$$C_{s1} = (8, 1, 8) * \mathrm{RM}_{3,3}/\mathrm{RM}_{3,2} + (8, 5, 4) * \mathrm{RM}_{3,2}/\mathrm{RM}_{3,1}$$
$$C_{s2} = (8, 7, 2) * \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0} + (8, 8, 1) * \mathrm{RM}_{3,0}.$$

Then $M = 4$ and $L = 2$. □

As a general design rule of an M-level GC code, the component codes $C_{Oi} * C_{Ii}$ at the first L partition levels $(i = 1, 2, \cdots, L, L \le M)$ should be selected so as to have a large minimum Hamming distance, and yet a simple trellis structure. This is in order to guarantee that decisions are correct in the first decoding stage with high probability, resulting in good error performance.

The first decoding stage is MLD for the super code $C_{s1} + C'_{s2}$, where $C_{s2} \subset C'_{s2}$. Code C'_{s2} is chosen such that it has smaller decoding complexity than C_{s2}. For all the codes presented in Table III, code C'_{s2} has the same inner codes as C_{s2}, and a single $(n_O, n_O, 1)$ or $(n_O, n_O - 1, 2)$ code as outer code. After the most likely codeword is determined in this stage, the first $k_1 = \sum_{i=1}^{L} k_{Ii} k_{Oi}$ information bits are decoded.

Note that the minimum distance of code $C_{s1} + C'_{s2}$ is smaller than or equal to the minimum distance d of C. However, for all the GC codes in Table III, the codewords of $C_{s1} + C'_{s2}$, in correspondence to different values of the first k_1 information bits, are at a distance at least d. In other words, in this first stage, the information bits are decoded up to the minimum distance of the code.

Example 4 (Cont.): For the $(64, 45, 8)$ GC code

$$C'_{s2} = (8, 8, 1) * \mathrm{RM}_{3,1}/\mathrm{RM}_{3,0} + (8, 8, 1) * \mathrm{RM}_{3,0} = (8, 8, 1) * \mathrm{RM}_{3,1}.$$

The minimum distance of C'_{s2} is 4. However, the codewords of $C_{s1} + C'_{s2}$ in correspondence to different values of the first 16 information bits, are at a minimum distance 8. □

In the second decoding stage, a codeword in C_{s1}, in correspondence to the k_1 information bits decoded in the first stage, $\overline{u} = (u_1, u_2, \cdots, u_n)$, is used to obtain a modified received sequence $\overline{r}' = (r'_1, r'_2, \cdots, r'_n)$, where $r'_i = (-1)^{u_i} r_i$ (assuming binary-phase shift keying (BPSK) modulation over an additive white Gaussian noise (AWGN) channel). An MLD for code C_{s2} is used. At the end of this final decoding stage, the $k_2 = \sum_{i=L+1}^{M} k_{Ii} k_{Oi}$ remaining information bits are decoded.

For $i = 1, 2$, let $\psi_i^{(0)}$ denote the number of addition-equivalent decoding operations in the ith decoding stage for the recursive MLD using optimally sectionalized trellis diagrams. Let $\psi_{\mathrm{TSD}}^{(0)}$ denote the total number of addition-equivalent decoding operations in the above two-stage soft-decision decoding procedure. Then it follows that

$$\psi_{\mathrm{TSD}}^{(0)} = \psi_1^{(0)} + \psi_2^{(0)}.$$

It should be noted that this reduced decoding complexity comes at the expense of a moderate loss due to an increased number of nearest neighbors (NN).

The values of $\psi_{\mathrm{TSD}}^{(0)}$ for selected GC codes are shown in the last column of Table III. Note the dramatic reduction in decoding complexity using two-stage soft-decision decoding. As an example, note that for the $(64, 45, 8)$ GC code, two-stage decoding $(\psi_{\mathrm{TSD}}^{(0)} = 34, 842)$ is about one order of magnitude less computationally intensive than optimal trellis-based recursive maximum-likelihood decoding of the $(64, 42, 8)$ RM code $(\psi_{\min}^{(0)} = 326, 017)$. It is also worthwhile to note that, although suboptimal, the above two-stage decoding of the GC codes in Table III is *up to the minimum distance* of the code. To illustrate the loss due to the increased NN, Fig. 3 shows simulation results on the error performance of the $(64, 45, 8)$ GC code, with both MLD and TSD. The loss is only about 0.3 dB compared to optimum MLD.

VI. CONCLUSIONS

In this correspondence, binary generalized concatenated (GC) codes with very low decoding complexity have been constructed. The decoding complexity was measured both by the maximum number of states of a minimal trellis diagram and by the number of addition-equivalent operations of a Viterbi decoder. Many of the GC codes presented have the same parameters as the best linear codes known. In addition, some of the GC codes have significantly smaller trellis-based decoding complexity than that of BCH and EG codes of the same length and approximately the same rate and minimum distance. Moreover, a trellis-based two-stage soft-decision decoding up the minimum distance was presented. The procedure was shown to drastically reduce the decoding effort, compared to maximum-likelihood decoding. The GC codes presented in this correspondence offer an excellent tradeoff between decoding complexity and error performance.

REFERENCES

[1] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 284–287, Mar. 1974.
[2] J. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76–80, Jan. 1978.
[3] G. D. Forney, Jr., "Coset codes—Part 2: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.
[4] D. Muder, "Minimal trellis for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049–1053, Sept. 1988.

[5] J. L. Massey, "Foundations and methods of channel coding," in *Proc. Int. Conf. Information Theory* (Berlin, Germany, Sept. 1978).

[6] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 242–245, Jan. 1993.

[7] V. A. Zinoviev, "Generalized cascade codes," *Probl. Pered. Inform.*, vol. 12, no. 1, pp. 5–15, 1976.

[8] E. L. Blokh and V. V. Zyablov, *Generalized Concatenated Codes.* Moscow, USSR: Nauka, 1976.

[9] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1741–1752, Nov. 1994.

[10] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924–1937, Nov. 1995.

[11] V. Sidorenko, G. Markarian, and B. Honary, "Minimal trellis design for linear block codes based on the Shannon product," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2048–2053, Nov. 1996.

[12] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1412–1418, Sept. 1991.

[13] A. Vardy and Y. Be'ery, "Maximum likelihood soft decision decoding of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 546–554, Mar. 1994.

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

[15] T. Takata, Y. Yamashita, T. Fujiwara, T. Kasami, and S. Lin, "On a suboptimum decoding of decomposable block codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1392–1406, Sept. 1994.

[16] S. Lin, T. Kasami, T. Fujiwara, and M. Fossorier, *Trellises and Trellis-Based Decoding Algorithms for Linear Codes.* Boston, MA: Kluwer, 1998.

[17] A. E. Brouwer and T. Verhoeff, "An updated table of minimum distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 662–677, Mar. 1993.

[18] B. Liesenfeld and B. G. Dorsch, "On the equivalence of some generalized concatenated codes and extended cyclic codes," in *Proc. 1993 Int. Symp. Information Theory* (San Antonio, TX, Jan. 1993), p. 399.

[19] T. Fujiwara, H. Yamamoto, T. Kasami, and S. Lin, "A trellis-based recursive maximum likelihood decoding algorithm for linear block codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 714–729, Mar. 1998.

[20] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1057–1064, May 1993.

A Low-Weight Trellis-Based Iterative Soft-Decision Decoding Algorithm for Binary Linear Block Codes

Takuya Koumoto, Toyoo Takata, Tadao Kasami, *Life Fellow, IEEE,* and Shu Lin, *Fellow, IEEE*

***Abstract*— This paper presents a new low-weight trellis-based soft-decision iterative decoding algorithm for binary linear block codes. The algorithm is devised based on a set of optimality conditions and the generation of a sequence of candidate codewords for an optimality test. The initial candidate codeword is generated by a simple decoding method. The subsequent candidate codewords, if needed, are generated by a chain of low-weight trellis searches, one at a time. Each search is conducted through a low-weight trellis diagram centered around the latest candidate codeword and results in an improvement over the previous candidate codewords that have been already tested. This improvement is then used as the next candidate codeword for a test of optimality. The decoding iteration stops whenever a candidate codeword is found to satisfy a sufficient condition on optimality or the latest low-weight trellis search results in a repetition of a previously generated candidate codeword. A divide-and-conquer technique is also presented for codes that are not spanned by their minimum-weight codewords. The proposed decoding algorithm has been applied to some well-known codes of lengths 48, 64, and 128. Simulation results show that the proposed algorithm achieves either practically optimal error performance for the example codes of length 48 and 64 or near optimal error performance for the (128, 29, 32) RM code with a significant reduction in computational decoding complexity.**

***Index Terms*—Iterative decoding, low-weight subtrellis, optimality.**

I. Introduction

The application of trellis-based maximum likelihood decoding (MLD) algorithms is limited due to the prohibitively large trellises for codes of long block lengths. To overcome the state and branch complexity problems of large trellises for long block codes, several new approaches have been proposed [1]–[8]. Most recently, Moorthy *et al.* have shown that the minimum-weight subtrellis of a code is sparsely connected and has much simpler state and branch complexities than the full-code trellis [9]. Based on this fact, they proposed a minimum-weight subtrellis-based iterative decoding algorithm for linear block codes to achieve suboptimum error performance with a drastic reduction in decoding complexity compared with a trellis-based MLD algorithm, using a full-code trellis. The Moorthy–Lin–Kasami (MLK) algorithm is devised based on the following: 1) generation of a sequence of candidate codewords based on a set of test error patterns using the Chase Algorithm II [10] and an algebraic decoder; 2) two test conditions: one to test the optimality of a candidate codeword and the other to test whether the most likely (ML) codeword is at a distance no greater than the minimum distance from the tested candidate codeword; and 3) a minimum-weight

Manuscript received August 5, 1997; revised August 10, 1998. This work was supported under NSF under Grant NCR-9415374, NASA under Grant NAG5-931, and the Ministry of Education, Japan, Grant 06650416.

T. Koumoto is with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan.

T. Takata is with the Faculty of Software and Information Science, Iwate Prefectural University, Iwate, Japan.

T. Kasami is with the Faculty of Information Science, Department of Computer Science, Hiroshima City University, Hiroshima, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HA 96822 USA.

Communicated by A. Vardy, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)01416-9.