The $(120, 6, 78)$ QT code has weight distribution

Weight	0	78	81	87	96
Count	1	528	80	96	24

B. Four Good Quasi-Twisted Codes Over GF(3)

The defining polynomials for four additional codes are given in Table III. The $(114, 6, 73)$ QT code has weight distribution

Weight	0	73	74	75	76	78	81	82	83	91	92
Count	1	156	264	36	108	36	8	48	48	12	12

The $(70, 7, 42)$ QT code has weight distribution

Weight	0	42	45	48	51	54	57	63
Count	1	560	518	658	238	196	14	2

The $(56, 8, 31)$ QT code has weight distribution (see the bottom of the previous page). The $(72, 8, 42)$ QT code has weight distribution

Weight	0	42	45	48	51	54	57
Count	1	1008	1472	1648	1488	816	128

C. A Three-Weight Quasi-Twisted Code

For $m = 6$ and $p = 21$, a three-weight QT code exists with parameters $(126, 6, 81)$. The $b_i(x)$ are 102, 1201, 1211, 11221, 12211, 1122, 11211, 1221, 1222, 11111,1001, 1021, 1121, 112, 1212, 1102, 1112, 10122, 112211, 111, 10121. The weight distribution is

Weight	0	81	90	99
Count	1	488	228	12

IV. Summary

The construction of quasi-twisted (QT) codes over GF(3) has been presented. The minimum distance of many of the codes constructed equals the known lower bound on the maximum–minimum distance. Two new optimal ternary codes were found, along with four other codes which improve the bounds. These other codes may also be proven to be optimal if the upper bounds are lowered. An optimal three-weight code was also presented. The rate $1/p$ codes considered here are contained in a subclass of QT codes termed 1-generator QT codes. Several of the $m = 4$ QT codes were found independently by Hill and Greenough [3].

Acknowledgment

The author wishes to thank Dr. F. Kschischang of the University of Toronto for providing the derivation of the number of orbits under ternary constacyclic shifts. This substantially improved the quality of the manuscript.

References

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

[2] V. Chepyzhov, "A Gilbert–Varshamov bound for quasi-twisted codes of rate $1/n$," in *Proc. Joint Swedish-Russian Int. Workshop on Information Theory* (Mölle, Sweden, Aug. 1993), pp. 214–218.

[3] R. Hill and P. P. Greenough, "Optimal quasi-twisted codes," in *Proc. Int. Workshop on Algebraic and Combinatorial Coding Theory* (Voneshta Voda, Bulgaria, June 1992), pp. 92–97.

[4] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw Hill, 1968.

[5] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227–246, Mar. 1992.

[6] R. N. Daskalov, R. Hill, and P. Lizak, "Table of bounds on linear codes over GF(3)," preprint, Tech. Univ., Gabrovo, Bulgaria, 1992.

[7] N. J. A. Sloane, "Tables of lower bounds on $d_{\max}(n, k)$ for linear codes over fields of order 3," to appear in V. Pless, *et al.*, *Handbook of Coding Theory*.

[8] A. E. Brouwer, "Table of minimum-distance bounds for linear codes over GF(3)," lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, The Netherlands.

[9] G. E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," preprint, Royal Military College of Canada, Kingston, ON, 1991.

[10] P. P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Des., Codes Cryptogr.*, vol. 2, pp. 81–91, 1992.

[11] F. S. Roberts, *Applied Combinatorics*. Englewood Cliffs, NJ: Prentice-Hall, 1984.

[12] E. H. L. Aarts and P. J. M. van Laarhoven, "Local search in coding theory," *Discrete Math.*, vol. 106/107, pp. 11–18, 1992.

[13] T. A. Gulliver and V. K. Bhargava, "Some best rate $1/p$ and $(p-1)/p$ quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369–1374, July 1992.

[14] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes," *Inf. Contr.*, no. 8, pp. 170–179, 1965.

Trellis-Oriented Decomposition and Trellis Complexity of Composite-Length Cyclic Codes

Yuval Berger and Yair Be'ery, *Member, IEEE*

***Abstract*—The trellis complexity of composite-length cyclic codes (CLCC's) is addressed. We first investigate the trellis properties of concatenated and product codes in general. Known factoring of CLCC's into concatenated subcodes is thereby employed to derive upper bounds on the minimal trellis size and state-space profile. New decomposition of CLCC's into product subcodes is established and utilized to derive further upper bounds on the trellis parameters. The coordinate permutations that correspond to these bounds are exhibited. Additionally, new results on the generalized Hamming weights of CLCC's are obtained. The reduction in trellis complexity of many CLCC's leads to soft-decision decoders with relatively low complexity.**

***Index Terms*— Trellis diagrams, soft-decision decoding, cyclic codes, concatenated codes, constacyclic codes, product codes, generalized Hamming weights.**

I. Introduction

The trellis diagrams of block codes are prominently used for soft-decision decoding [1]–[3]. The need to reduce the decoding complexity stimulated a considerable research in the field of trellis theory [2]–[10]. A general construction of the trellis diagram was given in [1]. It is in fact the unique *minimal trellis diagram* of the code [2], [4], i.e., the number of states in each level is minimal. Forney [2] demonstrated that the minimal trellis complexity may vary with respect to different ordering of coordinates. An optimal

Manuscript received May 31, 1994; revised December 5, 1994. The material in this correspondence was presented in part at the International Symposium on Information Theory, Trondheim, Norway, June 27–July 1, 1994.

The authors are with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat Aviv 69978, Tel-Aviv, Israel.

IEEE Log Number 9411960.

ordering, if exists, is characterized by a minimal number of states at each level. A major objective in [2], [5], [7], [10] was to find a "good" permutation in this sense. The logarithms of the state-space dimensions compose the *state-space profile* (SSP) of the code. The maximal dimension in the SSP, denoted by s, is called the *minimal trellis size*. s is closely related to the branch complexity of the code [8], and is widely used to measure the trellis complexity in sense of the decoding complexity [1]–[5], [7], [9], [10].

Let $C(n, k, d)$ denote a linear code of length n, dimension k, and minimum distance d. The minimal s attainable by any ordering of the coordinates is called the *absolute minimal trellis size*, and denoted by $s(C)$. The well known Wolf bound [1] is

$$s(C) \leq \min(k, n-k). \tag{1}$$

An improved bound

$$s(C) \leq \min[k - J_\nu + \nu + 1, n - k - J_{\nu^\perp} + \nu^\perp + 1] \tag{2}$$

was obtained in [5], where ν is the *contraction index* [11] of a subcode of dimension J_ν, and similarly $\nu^\perp$ is the contraction index related to the dual code of C. A general lower bound on $s(C)$ was obtained in [4] and improved in [7]. The bound of [7] is based on the *generalized Hamming weight* (GHW) hierarchy [12], also called the *length/dimension profile* (LDP) of the code [8], originally applied for the Type II wire-tap channel [12]. This bound may be alternatively written as

$$s(C) \geq \max_{i=0}^{n} \{k - r_i - r_{n-i}\} \tag{3}$$

using the *dimension/length profile* (DLP) [8], denoted by $\{r_i\}$, where r_i is defined as the largest dimension of any subcode of C with support i for $i = 0, 1, \cdots, n$. Notice that each one of the DLP or LDP can be determined from the other.

Inherent characteristics of some well-known classes of codes, such as the Reed–Muller (RM) and BCH codes, were utilized by several researchers to obtain further results on their trellis properties. First, the *squaring construction* of RM codes was exploited in [2]. This design accomplishes the optimal coordinate ordering for these codes [7]. The corresponding absolute minimal trellis size was evaluated in [5]. The trellis complexity of BCH codes was addressed in [7], [10]. The particular class of BCH codes with composite length was also considered in [10]. Specific ordering of coordinates was used to expose direct sum of subcodes with nonoverlapping support. This structure was used to upper-bound the minimal trellis size. Finally, the unique direct sum design of *decomposable* generalized concatenated codes was used in [9] to analyze their trellis parameters. Among these codes are also many cyclic and BCH codes.

In this study we focus on the trellis complexity of composite-length cyclic codes. This class contains cyclic codes of length nN for $n, N > 1$. The interest in the trellis characteristics and the decoding complexity of these codes is motivated by the fact that many of them are comparable (sometimes superior) to related BCH codes in sense of their error-correcting capabilities [16], [20].

The structure of CLCC's was investigated in [16], [18]–[21]. It was proved that any CLCC is composed of several concatenated codes, in which the inner codes are cyclic. We utilize this structure to derive trellis-oriented permutations for the CLCC's. New decompositions are also developed on the basis of subcodes which are direct products of cyclic codes. The trellis properties of general concatenated and product codes are investigated and utilized to improve the known upper bounds on the SSP and minimal trellis size of CLCC's. The bounds are constructively derived, and related to definite coordinate permutations.

This paper is organized as follows. The trellis properties of concatenated and direct product codes are studied in Section II. Trellis-oriented decompositions and upper bounds on the trellis complexity of CLCC's are developed in Section III. The best bounds obtained for several CLCC's are presented in Section IV, and compared to previously known bounds. The resulted decoding complexity is estimated. Finally, it is shown that the foregoing decompositions may also be used to evaluate the GHW hierarchy and DLP of CLCC's.

II. Trellis Complexity of Concatenated and Product Codes

Let $C(N, K)$ denote a code over GF (q^m), and define $R \triangleq N - K$. C may also be exhibited as a code over GF (q) using vector space representation of GF (q^m) over GF (q). Let $\tilde{G}$ denote the generator matrix of a certain equivalent code of C over GF (q).

Lemma 1: A $C(N, K)$ code over GF (q^m) is equivalent to a code with generator matrix $\tilde{G}$ over GF (q) such that

$$\tilde{G} = \begin{bmatrix} I_m & A_{11} & \cdots & A_{1R} & 0 & 0 & \cdots & 0 \\ 0 & I_m & A_{21} & \cdots & A_{2R} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & & & & & 0 \\ 0 & \cdots & 0 & I_m & A_{K1} & \cdots & & A_{KR} \end{bmatrix}$$

where A_{ij} is an $m \times m$ matrix, I_m is the $m \times m$ identity matrix, and A_{KR} is nonzero.

Proof: Consider a certain ordering of coordinates such that the generator matrix G possesses the *double echelon* form [14]

$$G = \begin{bmatrix} 1 & x & x & & \cdots & & x & 0 & 0 & & \cdots & 0 \\ 0 & 1 & x & x & & \cdots & & x & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & & & \cdot & & & & \cdot & & & \\ \cdot & & & \cdot & & \cdot & & & & \cdot & & \\ \cdot & & & & \cdot & & \cdot & & & & \cdot & 0 \\ 0 & 0 & & \cdots & & 0 & 1 & x & x & \cdots & x & y \end{bmatrix} \tag{4}$$

where x and y designate arbitrary elements of GF (q^m) and y is nonzero. Let a denote a primitive element of GF (q^m). Then the set of elements $\{a^0, a^1, \cdots, a^{m-1}\}$ forms a basis of the vector space GF (q^m) over GF (q). Each element $\lambda \in$ GF (q^m) may be represented by the m-tuple $\psi[\lambda] \triangleq (\beta_0, \beta_1, \cdots, \beta_{m-1})$ such that $\lambda = \Sigma_i \beta_i a^i$, where $\psi[\lambda] \in$ GF $(q)^m$. Let $c \triangleq (c_1, c_2, \cdots, c_N)$ denote the codeword located in the ith row of G, for $i = 1, 2, \cdots, K$. Then $c_j = 0$ for $1 \leq j < i$ and $N - K + i < j \leq N$, and $\psi[c_i] = (1, 0, 0, \cdots, 0)$. Let $c(x)$ denote the polynomial description of c. Obviously, $ac(x)$ is also a codeword. Similarly, c defines m codewords $\{c^{(j)}\}$, for $j = 1, 2, \cdots, m$, such that $\psi[c_i^{(j)}]$ consists of a single nonzero element in position j. $\tilde{G}$ is thus constructed by employing the mK codewords, defined by the rows of G, over GF (q). □

Let C_1 and C_2, respectively, denote (N, K) and (n, k) codes over GF (q^k) and GF (q). C_2 is isomorphic to the additive group of GF (q^k). The *concatenated code* $C = C_1 \bigstar C_2$ is constructed by replacing each symbol of a codeword $c \in C_1$ by its mapping in C_2. C is with length nN and dimension kK. The straightforward upper bound implied by the Wolf bound (1) is $s(C) \leq \min(kK, nN - kK)$. Yet, it has been noticed [1], [14] that many concatenated codes may be decoded with significantly lower decoding complexity than expected by this bound. We shall demonstrate that the trellis complexity is indeed significantly lower in those cases.

Theorem 1—The Generalized Wolf Bound for Concatenated Codes: Let $C_1(N, K)$ be a code over GF (q^k) and $C_2(n, k)$ be a code over GF (q). Denote by C the concatenated code $C_1 \bigstar C_2$. For

$i = 0, 1, \cdots, nN$, let $t \equiv i \bmod n$ and $z = (i-t)/n$. Then

$$s_i \le \begin{cases} kz + \min(k, t), & 0 \le z < \min(N-K, K) \\ k(N-K-1) + \min(k, t) + \min(k, n-t), & N-K \le z < K, \quad N < 2K \\ Kk, & K \le z < N-K, \quad N > 2K \\ k(K-1) + \min(k, n-t), & K = z, \quad N = 2K \\ k(N-z-1) + \min(k, n-t), & \max(N-K, K) \le z \le N \end{cases} \tag{5a}$$

$$s(C) \le \min\{k(N-K) + \min(k, n-k), kK\}. \tag{5b}$$

Proof: Let G_1 and G_2 denote the generator matrices of C_1 and C_2, respectively. Let $f(\lambda) = w$ define the isomorphism between GF (q^k) and the vector space C_2 such that $\psi[\lambda]G_2 = w$ for any $\lambda \in$ GF (q^k), where $w \in C_2$. It may be easily verified [14], [17] that $G = \tilde{G}_1 \overline{G}_2$ for some coordinate ordering of C, where $\tilde{G}_1$ is given by Lemma 1 and

$$\overline{G}_2 = \begin{bmatrix} G_2 & & & 0 \\ & G_2 & & \\ & & \ddots & \\ 0 & & & G_2 \end{bmatrix}. \tag{6}$$

Therefore

$$G = \begin{bmatrix} G_2 & A_{11}G_2 & \cdots & A_{1R}G_2 & 0 & 0 \cdots & 0 \\ 0 & G_2 & A_{21}G_2 & \cdots & A_{2R}G_2 & 0 \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & & \vdots \\ & & & & & & 0 \\ 0 & 0 & \cdots & G_2 & A_{K1}G_2 & \cdots & A_{KR}G_2 \end{bmatrix}.$$

Denote by k_i^- and k_i^+ the dimensions of the codes obtained by truncating the coordinates $\{i+1, i+2, \cdots, nN\}$ and $\{1, 2, \cdots, i\}$ of C, respectively. It follows that

$$k_i^- \le \begin{cases} kz + \min(k, t), & 0 \le z < K \\ kK, & K \le z \le N \end{cases}$$

$$k_i^+ \le \begin{cases} kK, & 0 \le z < N-K \\ k(N-z-1) + \min(k, n-t), & N-K \le z \le N. \end{cases}$$

The upper bound on s_i in (5a) is obtained by employing the relation $s_i = k_i^- + k_i^+ - kK$ [2]. Maximizing s_i for $0 \le i \le nN$ results in the upper bound on $s(C)$. □

Example 1: The concatenation of the Reed–Solomon (RS) code (12, 7, 6) over GF (2^4) and the binary RM (8, 4, 4) code produces the (96, 28, 24) code, denoted by C. The Wolf bound (1) implies $s(C) \le 28$. Theorem 1 provides the improved bound $s(C) \le 24$.

Let $C_1(N, K)$ and $C_2(n, k)$ be two codes over GF (q). The generator matrix G of the *direct product code* $C = C_1 \otimes C_2$ is the Kronecker product $G_1 \otimes G_2$ [15, p. 569]. Consider a permutation for which G_1 possesses the double echelon structure as in (4). The generalized Wolf bound for C is established following the constructive proof of Theorem 1, in which $G_1 \otimes G_2$ is used instead of $\tilde{G}_1 \overline{G}_2$.

Theorem 2—The Generalized Wolf Bound for Direct Product Codes: Let $C_1(N, K)$ and $C_2(n, k)$ be codes over GF (q), and define $C = C_1 \otimes C_2$. Let $t \equiv i \bmod n$ and $z = (i-t)/n$ for $i = 0, 1, \cdots, nN$. Then s_i and $s(C)$ are bounded according to (5).

Example 2: Let C denote the direct product of the even-weight codes $C_1(5, 4, 2)$ and $C_2(3, 2, 2)$. Then C is a cyclic (15, 8, 4) code [15, p. 570]. The upper bound on the SSP, provided by Theorem 2, is $\{0, 1, 2, 2, 3, 3, 2, 3, 3, 2, 3, 3, 2, 2, 1, 0\}$. In fact, it coincides with the actual SSP associated with the coordinate ordering of the theorem. The Wolf bound (1) implies $s(C) \le 7$. However, Theorem 2 provides the improved bound $s(C) \le 3$.

The generalized Wolf bounds in Theorems 1 and 2 do not utilize any inherent characteristics of the codes, other than the length and dimension. The generating codes, C_1 and C_2, often possess efficient trellis-oriented ordering of coordinates (in the sense of trellis complexity). This information will be employed in the forthcoming theorems to improve the upper bounds for the combined code.

Theorem 3: Let $C_1(N, K)$ and $C_2(n, k)$ be codes over GF (q^k) and GF (q), respectively. Define $C = C_1 \bigstar C_2$. Let $t \equiv i \bmod n$ and $z = (i-t)/n$ for $i = 0, 1, \cdots, nN$. Denote by $s_i^{(j)}$, $k_i^{-(j)}$, and $k_i^{+(j)}$ the trellis parameters of C_j at level i, for $j = 1, 2$. Then

$$s_i \le \begin{cases} ks_z^{(1)} + k_t^{-(2)}, & s_z^{(1)} = s_{z+1}^{(1)} - 1 \\ ks_z^{(1)} + s_t^{(2)}(k_{z+1}^{-(1)} - k_z^{-(1)}), & s_z^{(1)} = s_{z+1}^{(1)} \\ ks_z^{(1)} + k_t^{+(2)} - k, & s_z^{(1)} = s_{z+1}^{(1)} + 1 \end{cases} \tag{7a}$$

$$s(C) \le ks(C_1) + s(C_2). \tag{7b}$$

Proof: Assume the design $G = \tilde{G}_1 \overline{G}_2$, where $\tilde{G}_1$ is the q-ary form of G_1 and $\overline{G}_2$ is given by (6). Clearly, $k_z^- = kk_z^{-(1)}$ and $k_z^+ = kk_z^{+(1)}$. If $s_z^{(1)} = s_{z+1}^{(1)} - 1$ then, due to the monotonicity of k_z^-, necessarily $k_z^{-(1)} = k_{z+1}^{-(1)} - 1$ and $k_z^{+(1)} = k_{z+1}^{+(1)}$. Hence, $s_i \le ks_z^{(1)} + k_t^{-(2)}$. Otherwise, if $s_z^{(1)} = s_{z+1}^{(1)}$ then either $k_z^{-(1)} = k_{z+1}^{-(1)}$ and $k_z^{+(1)} = k_{z+1}^{+(1)}$, or $k_z^{-(1)} = k_{z+1}^{-(1)} - 1$ and $k_z^{+(1)} = k_{z+1}^{+(1)} + 1$. These cases similarly correspond to $s_i \le ks_z^{(1)}$ and $s_i \le ks_z^{(1)} + s_t^{(2)}$, respectively. Finally, if $s_z^{(1)} = s_{z+1}^{(1)} + 1$ then $k_z^{-(1)} = k_{z+1}^{-(1)}$ and $k_z^{+(1)} = k_{z+1}^{+(1)} + 1$. Hence, $s_i \le k(s_z^{(1)} - 1) + k_t^{+(2)}$. The upper bound on $s(C)$ follows from the extreme case of $s_z^{(1)} = s_{z+1}^{(1)}$, assuming that the coordinates of C_1 and C_2 are efficiently ordered to attain the absolute minimal trellis size. □

Example 1 (cont.): The absolute minimal trellis size of the RM (8, 4, 4) code is 3 [5]. Applying Theorem 3 yields an improved bound $s(C) \le 23$.

The next theorem can be proved by using the decomposition $G = G_1 \otimes G_2$ and following the proof of Theorem 3.

Theorem 4: Let $C_1(N, K)$ and $C_2(n, k)$ be codes over GF (q), and define $C = C_1 \otimes C_2$. Let $t \equiv i \bmod n$ and $z = (i-t)/n$ for $i = 0, 1, \cdots, nN$. Then s_i and $s(C)$ are bounded according to (7).

Example 3: Denote the binary (3, 2, 2) code by C_1. The direct product of C_1 with itself results with a (9, 4, 4) code, denoted by C_2. It follows from Theorem 2 that $s(C_2) \le 3$. The (27, 8, 8) code C is designed by the direct product of (3, 2, 2) and (9, 4, 4). The upper bound provided by Theorem 2 coincides with the Wolf bound $s(C) \le 8$. However, since $s(C_2) \le 3$, Theorem 4 implies that $s(C) \le 7$.

It is a known fact that the direct product codes $C_1 \otimes C_2$ and $C_2 \otimes C_1$ are equivalent [15]. We conclude the following.

Corollary 1: A different permutation of C in Theorems 2 and 4 leads to similar form of upper bounds on s_i and $s(C)$ in which n_1 and k_1 are, respectively, interchanged by n_2 and k_2.

III. Trellis Complexity of Composite-Length Cyclic Codes

The trellis complexity of CLCC's will be investigated, based on certain decompositions that include concatenated and product codes. The results of the previous section are employed to derive upper bounds on the trellis parameters and to construct the related ordering of coordinates.

Let C_1 be a minimal cyclic (N, K) code over GF (q^k) and let C_2 be a minimal cyclic (n, k) code over GF (q). Assume throughout this section that a is a primitive (nN)th root of unity, $\beta = a^N$ is a primitive nth root of unity, and $\gamma = a^n$ is a primitive Nth root of unity. It is well known that $C = C_1 \bigstar C_2$ is a minimal cyclic code [16], provided that $\gcd(n, N) = 1$. Conversely, any minimal

CLCC of length nN, for which $\gcd(n, N) = 1$, is a concatenation of two minimal cyclic codes [19]. Jensen [21] recently demonstrated that if $\gcd(n, N) > 1$ then the CLCC is also a concatenated code, where the inner code is cyclic and the outer code is a *constacyclic code* (also known as *pseudocyclic code*). A constacyclic code over GF (q) was defined by Berlekamp [13] as follows. If $(b_1, b_2, \cdots, b_n)$ is a codeword then $(hb_n, b_1, \cdots, b_{n-1})$ is also a codeword for some fixed nonzero element $h \in$ GF (q). The codewords in polynomial form constitute an ideal in the ring GF $(q)[y]/(y^N - h)$. h is called the *defining field-isomorphism* [21]. The following theorem is based on the foregoing decompositions from [16], [18]–[21].

Theorem 5: Let C be a minimal CLCC of length nN over GF (q). Then C is a concatenated code $C_1 \bigstar C_2$, where $C_1(N, K)$ is over GF (q^k) and $C_2(n, k)$ is a minimal cyclic code over GF (q). If $\gcd(n, N) = 1$ then C_1 is a minimal cyclic code, and the nonzeros of C are $\beta^j\gamma^i$ for any nonzero γ^i of C_1 and nonzero β^j of C_2. Otherwise, C_1 is a minimal constacyclic code with defining field-isomorphism β^j, where β^j is a nonzero of C_2, and γ^{iz} is a nonzero of C iff γ^i is a nonzero of C_1, for $z = q^t$ and $t = 0, 1, \cdots, k-1$.

The *defining set* of C, denoted by $\mathbb{C}$, contains by definition the minimal element of every cyclotomic coset that corresponds to a zero of C. $\overline{\mathbb{C}}$ is the notation for the complement set of $\mathbb{C}$. Denote hereafter by D_i the minimal q-ary cyclic code associated with the defining set $\mathbb{D}_i$ such that $\overline{\mathbb{D}}_i = \{i\}$. G_i will denote the generator matrix of D_i.

Lemma 2 [15]: A cyclic code C is equivalent to the direct sum of the minimal codes $\{D_i\}_{i \in \overline{\mathbb{C}}}$.

Theorem 6: Let C be a CLCC of length nN. Then $C = \cup_{i \in \Omega} C^{(i)}$, where $C^{(i)} = E^{(i)} \bigstar D_i$ and $\{D_i\}_{i \in \Omega}$ contains the minimal cyclic inner codes of the concatenated minimal subcodes of C. Also $s_j \le \Sigma_{i \in \Omega} s_j^{(i)}$ and $s(C) \le \Sigma_{i \in \Omega} s^{(i)}$, where the trellis parameters $s_j^{(i)}$ and $s^{(i)}$ of $C^{(i)}$ are bounded using Theorems 1 and 3.

Proof: Lemma 2 and Theorem 5 imply that C is direct sum of minimal concatenated subcodes. Let $E^{(i)}$ be the direct sum of the outer codes which are concatenated with a common inner code D_i. The subcode $E^{(i)} \bigstar D_i$, denoted by $C^{(i)}$, is also a concatenated code, and Theorems 1 and 3 may therefore be applied on its trellis size parameters. s_j and $s(C)$ are bounded by the sum of the corresponding parameters related to the subcodes of C, subjected to a common permutation. □

Example 4: Let C denote the CLCC $(85, 53, 10)$ with $\mathbb{C} = \{3, 5, 7, 15\}$ [22]. The nonzeros of an equivalent code of C are defined by $\overline{\mathbb{C}} = \{0, 1, 9, 13, 17, 21, 29, 37\}$. Suppose that $N = 17$ and $n = 5$. Then D_0 and D_1 are the cyclic $(5, 1, 5)$ and $(5, 4, 2)$ codes, respectively. Denote by E_i the minimal binary cyclic code of length 17 for $i \in \{0, 1, 3\}$, and by F_i the minimal cyclic code over GF (2^4) for $i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Then, according to $\overline{\mathbb{C}}$, Theorems 5 and 6 imply the factoring $C \cong (E_0 \bigstar D_0) \oplus (F_0 \bigstar D_1) \oplus (F_3 \bigstar D_1) \oplus (F_4 \bigstar D_1) \oplus (F_5 \bigstar D_1) \oplus (F_6 \bigstar D_1) \oplus (F_7 \bigstar D_1) \oplus (F_8 \bigstar D_1) = (E_0 \bigstar D_0) \oplus ((F_0 \oplus F_3 \oplus F_4 \oplus F_5 \oplus F_6 \oplus F_7 \oplus F_8) \bigstar D_1)$, where "$\cong$" means that the codes are equivalent. Therefore, C is equivalent to the direct sum of the concatenated codes $E^{(0)} \bigstar D_0$ and $E^{(1)} \bigstar D_1$, where $E^{(0)}$ and $E^{(1)}$ are the $(17, 1)$ and $(17, 13)$ codes, respectively. The minimal trellis size of $E^{(1)}$ is upper-bounded by 4, and consequently, due to Theorem 3, the minimal trellis size of $(17, 13) \bigstar (5, 4)$ is upper-bounded by 17. Hence $s(C) \le 18$. The wolf bound (1) is $s(C) \le 32$.

Example 5: Let C denote the composite-length BCH $(63, 38, 10)$ code with $\mathbb{C} = \{0, 1, 3, 15, 31\}$ and $\overline{\mathbb{C}} = \{5, 7, 9, 11, 13, 21, 23, 27\}$. Assume that $N = 21$ and $n = 3$. D_0 and D_1 are the cyclic $(3, 1, 3)$ and $(3, 2, 2)$ codes, respectively. The splitting field of the outer constacyclic codes is GF (2^6). Consider now the code $C^\perp$ equivalent to the dual code of C. Denote by F_i the minimal constacyclic code of length 21 with nonzero a^i, for $i \in \mathbb{C}$. Its defining field-isomorphism is $h = (a^i)^N = a^{21i}$ [21]. The inner code in each concatenated minimal subcode of $C^\perp$ is the minimal cyclic code with nonzero h. Consequently, Theorems 5 and 6 imply that $C^\perp = ((F_0 \oplus F_3 \oplus F_{15}) \bigstar D_0) \oplus ((F_1 \oplus F_{31}) \bigstar D_1)$. Thus $C^\perp$ is the direct sum of $E^{(0)} \bigstar D_0$ and $E^{(1)} \bigstar D_1$, where $E^{(0)}$ and $E^{(1)}$ are the $(21, 13)$ and $(21, 6)$ codes, respectively. $E^{(0)}$ is a binary CLCC with defining set $\{3, 7, 9\}$. Its dual code includes the $(7, 6) \bigstar (3, 1)$ code as a subcode, and therefore the minimal trellis size of $E^{(0)}$ is upper-bounded by 4. It follows, due to Theorem 6, that the minimal trellis size of $(21, 13) \bigstar (3, 1)$ is upper-bounded by 5. Hence $s(C) \le 17$. The wolf bound (1) and the design of [10] give $s(C) \le 25$.

Theorem 6 provides, in view of Theorems 1 and 3, new permutations and upper bounds on the SSP and $s(C)$ for many CLCC's. Since little knowledge of the trellis properties is available for most of the nonbinary codes, the bound of Theorem 3 on each concatenated subcode of G is often degenerated to the generalized Wolf bound of Theorem 1. However, in many cases, the concatenated structure of C leads to a possibly different decomposition that consists of direct products codes.

Theorem 7: Let C be a CLCC of length nN over GF (q) such that $C = \cup_{i \in \Omega} C^{(i)}$, where $C^{(i)} = E^{(i)} \bigstar D_i$. Define $\hat{C}^{(i)} \triangleq \hat{E}^{(i)} \otimes D_i$, where $\hat{E}^{(i)}$ is the subfield subcode of $E^{(i)}$. Then $\cup_{i \in \Omega} \hat{C}^{(i)} \subseteq C$, $s_j \le \Sigma_{i \in \Omega} s_j^{(i)} + \Delta$, and $s(C) \le \Sigma_{i \in \Omega} s^{(i)} + \Delta$, where $\Delta \triangleq |C / \cup_{i \in \Omega} \hat{C}^{(i)}|$. The trellis parameters $s_j^{(i)}$ and $s^{(i)}$ of $\hat{C}^{(i)}$ are upper-bounded using Theorems 2 and 4.

Proof: We begin with the decomposition of the concatenated codes $C^{(i)}$ described in Theorem 6. Let $|\hat{E}^{(i)}|$ denote the dimension of $\hat{E}^{(i)}$. Denote by $\tilde{G}^{(i)}$ and $\hat{G}^{(i)}$ the generator matrices over GF (q) of the codes $E^{(i)}$ and $\hat{E}^{(i)}$, respectively. Let $\hat{b}$ denote a codeword of $\hat{E}^{(i)}$. There exists a codeword $b(x)$ in $E^{(i)}$ such that $\psi[b_j] = (\hat{b}_j, 0, 0, \cdots, 0)$, for $j = 1, 2, \cdots, N$. In general, $a^z b(x)$ is also a codeword for $z = 0, 1, \cdots, k-1$, where $k = |D_i|$. A similar design, constructed by a set of $|\hat{E}^{(i)}|$ linearly independent codewords of $\hat{E}^{(i)}$, produces the direct product code $\hat{E}^{(i)} \otimes V_k$, where V_k is the notation for the vector space GF $(q)^k$. $\hat{E}^{(i)} \otimes V_k$ is thus a subcode of the q-ary version of $E^{(i)}$. Using the notation of (6), it follows that $(\hat{G}^{(i)} \otimes I_k)\overline{G}_i$ generates a subcode of $C^{(i)}$. Clearly (6) implies that $\overline{G}_i = I_N \otimes G_i$. Therefore, we conclude from the identity $(X \otimes Y)(W \otimes Z) = (XW) \otimes (YZ)$ [15, p. 422] that $(\hat{G}^{(i)} \otimes I_k)(I_N \otimes G_i) = \hat{G}^{(i)} \otimes G_i$ generates a subcode of $C^{(i)}$. The trellis parameters of $C^{(i)}$ are therefore bounded using Theorems 2 and 4. The bounds on the SSP and $s(C)$ readily follow from the properties of direct sum code. ■

Example 6: Denote by C the binary cyclic $(105, 35, 24)$ code with $\mathbb{C} = \{5, 7, 9, 11, 13, 15, 17, 21, 35, 45\}$ and $\overline{\mathbb{C}} = \{0, 1, 3, 25, 49\}$ [20]. Choose $N = 21$ and $n = 5$. D_0 and D_1 are the cyclic $(5, 1, 5)$ and $(5, 4, 2)$ codes, respectively. Denote by E_i a minimal binary cyclic code of length 21, and by F_i a minimal cyclic code of the same length over GF (2^4). Theorems 5 and 6, with correspondence to $\overline{\mathbb{C}}$, imply that $C \cong ((E_0 \oplus E_5) \bigstar D_0) \oplus ((F_5 \oplus F_9 \oplus F_{14}) \bigstar D_1)$. Thus C is the direct sum of $E^{(0)} \bigstar D_0$ and $E^{(1)} \bigstar D_1$, where $E^{(0)}$ and $E^{(1)}$ are $(21, 7)$ codes. The method of [10] gives $s(C) \le 34$. Theorem 7 implies, however, that the subcode $(21, 7) \bigstar (5, 1)$ is in fact the direct product of the binary $(21, 7)$ and $(5, 1)$ codes. The outer code $E^{(1)}$ of $(21, 7) \bigstar (5, 4)$ over GF (2^4) is associated with the defining set $\{0, 1, 2, 3, 7, 10\}$. It follows from Theorem 7 that $E^{(1)}$ includes the direct product code $(21, 3) \otimes (5, 4)$ as subcode. Theorem 4 implies that the minimum trellis size of this subcode is upper-bounded by 6. Hence $s(C) \le 29$.

Example 7: Let C denote the CLCC $(15, 6, 6)$ code with $\mathbb{C} = \{0, 1, 7\}$ and $\overline{\mathbb{C}} = \{3, 5\}$. Suppose that $N = 5$ and $n = 3$.

Denote by E_i a minimal binary cyclic code of length 5, and by F_i a minimal cyclic code of length 5 over GF(2^2). Then $C^\perp = (E_0 \bigstar D_0) \oplus ((F_1 \oplus F_2) \bigstar D_1)$, i.e., $C^\perp$ is the direct sum of $(5, 1)\bigstar(3, 1)$ and $(5, 4)\bigstar(3, 2)$. Again, the Wolf bound (1) and [10] give $s(C) \leq 6$. Theorem 7 implies that $C^\perp$ contains the product subcodes $(5, 1)\otimes(3, 1)$ and $(5, 4)\otimes(3, 2)$. It follows from Theorem 4 that the minimum trellis size of $(5, 4) \otimes (3, 2)$ is upper-bounded by 3. Hence $s(C) = s(C^\perp) \leq 4$.

We shall show now that previous results [10], [18] on composite-length codes are special cases of Theorem 7. Consider first the case $\gcd(n, N) = 1$. Let $D^{(i,j)}$ denote the concatenated minimal cyclic code over GF(q) such that the outer code of length N is the minimal cyclic code E_i with nonzero γ^i and the inner code is the minimal cyclic code D_j with nonzero β^j. Let Γ be the set $\{\gamma^r : r = iq^z, 0 \leq z \leq m-1\}$, where GF$(q^m)$ is the splitting field of $x^N - 1$. Denote by $\check{E}_i$ the cyclic code over GF(q) with nonzeros Γ. The nonzeros of E_i form a subset Λ of Γ. Theorem 7 implies the following.

Lemma 3: If $\Lambda = \Gamma$ then $\check{E}_i = \hat{E}_i$ and $D^{(i,j)} = \hat{E}_i \otimes D_j$. Otherwise, $D^{(i,j)} \subseteq \check{E}_i \otimes D_j$.

Define $\overline{\mathbb{C}}_1 = \cup_{j\in\overline{\mathbb{C}}} \min_r \{i : i \equiv jq^r \bmod N\}$ and $\overline{\mathbb{C}}_2 = \cup_{j\in\overline{\mathbb{C}}} \min_r \{i : i \equiv jq^r \bmod n\}$. Kasami [18] proved that C is a subcode of $C_1 \otimes C_2$, provided that $\gcd(n, N) = 1$. We shall show that this result may be easily derived from Theorem 7 and Lemma 3. Theorem 5 states that $\gamma^i\beta^j$ is a nonzero of C iff $D^{(i,j)} \subseteq C$. The Chinese remainder theorem [15, p. 570] states that for any integer $\rho[i, j] \in \{0, 1, \cdots, nN-1\}$ there exist particular i and j such that $\rho[i, j] \equiv i \bmod N$ and $\rho[i, j] \equiv j \bmod n$. Let $\sigma = \beta\gamma$ denote a primitive (nN)th root of unity, and assume the notation ρ for $\rho[i, j]$. Hence, there exist integers a, b such that $\gamma^i\beta^j = \gamma^{i+aN}\beta^{j+bn} = \sigma^\rho$. Clearly, $C = \cup_{\rho\in\overline{\mathbb{C}}} D^{(i,j)}$, and thereby $C \subseteq \cup_{\rho\in\overline{\mathbb{C}}}(\check{E}_i \otimes D_j)$. However, $C_1 \otimes C_2$ is the direct sum of the direct product codes $\{\check{E}_i \otimes D_j\}_{\rho\in\overline{\mathbb{C}}}$. Thus $C \subseteq C_1 \otimes C_2$.

The design of [10] for composite-length BCH codes may be straightforwardly applied also for the wider class of CLCC's. It is essentially a direct sum decomposition of subcodes with nonoverlapping supports. Let C denote a CLCC of length n_1n_2. Formally, it may be shown that there may exist codes $C_1(n_1, k_1)$ and $C_2(n_2, k_2)$ such that $V_{n_1} \otimes C_2$ and $V_{n_2} \otimes C_1$ are subcodes of an equivalent code of C. We establish the following bound

$$s(C) \leq k - \max[n_2k_1 - s(C_1), n_1k_2 - s(C_2)] \tag{8}$$

based on this decomposition. This design is also a direct consequence of Theorem 7. We distinguish between two cases. In the first case, $(\hat{E} \otimes D_i) \subseteq C$ for a certain subfield subcode $\hat{E}$ and every minimal code D_i. In this case, $\cup_i(\hat{E} \otimes D_i) = \hat{E} \otimes V_{n_2} \cong V_{n_2} \otimes \hat{E}$. In the second case, $(E_i \otimes D) \subseteq C$ for a certain code D and every minimal q-ary code E_i of length n_1. Then $\cup_i(E_i \otimes D) = V_{n_1} \otimes D$. Notice that these unique cases do not appear in many codes, and (8) then fails to improve the Wolf bound (1).

IV. Results

A. Trellis Complexity

The duality theorem [2] states that the trellis complexities of C and $C^\perp$ are identical. Theorems 6 and 7 should then be used to factorize a CLCC code and its dual code into their concatenated and direct product code designs. These decompositions lead to particular coordinate permutations and provide upper bounds on the trellis complexity. The best bounds obtained for several codes are reported in Tables I and II for the cases of $\gcd(n, N) = 1$ and $\gcd(n, N) > 1$, respectively. The new bound for each code, related to the best decomposition found from Theorem 6 and 7, is denoted by B. B′ denotes the bound of (8), derived from the direct-sum structure of [10], and calculated for both the code and its dual. B_W denotes the Wolf bound (1). Codes marked by "▷" have the largest known minimum distance according to [23]. An asterisk indicates that the upper bound meets the lower bound of (3).

The minimal trellis size is deeply related to the trellis-based decoding complexity. An upper bound on the number of real addition-equivalent operations needed to decode a binary code using coset-trellis decoder [3] is

$$2^{s-1}(3n - 6s + 5). \tag{9}$$

The decoding complexity is indicated in Tables I and II by $\mathcal{D} = \log_{10}(\mathcal{N})$, where $\mathcal{N}$ is the normalized upper bound on the number of operations per information symbol (obtained by dividing the value of (9) by k).

Observe that the decoding complexity in Tables I and II for many high-rate CLCC's is relatively attractive for soft-decision trellis-based decoding. Notice that efficient soft-decoding methods often lead in practice to significantly lower complexity then guaranteed by $\mathcal{D}$ [3].

Several efficient soft-decoding methods are known in the literature also for medium- and low-rate codes [2], [10], [11], [14]. They include generalized Viterbi algorithms over sectionalized trellis diagrams [2] and various *coset-decoding* techniques [2], [10], [11]. Yet, it was observed that trellis-oriented ordering of coordinates is generally well-suited also for most of these decoding schemes. Moreover, it was demonstrated [10], [11], [14] that sophisticated use of structures such as nonoverlapping direct sum usually lead to significant reduction in decoding complexity. The product codes structures provided in this study may as well be exploited to further improve the soft-decoding schemes.

The combination of good, and sometimes superior, error-correction capabilities with relatively low trellis complexity of many CLCC's sets the class of CLCC's as a valuable competitive to primitive BCH and RM codes [2], [7], [10]. It also significantly enlarges the amount of codes which are practical candidates for soft-decision decoding applications.

B. Generalized Hamming Weights and Dimension/Length Profiles

The unique decomposition formulated in Theorem 7 may be also utilized to establish new results on the GHW hierarchy and DLP of CLCC's. The results for some CLCC's will be demonstrated in the following examples, where several theorems of Wei and Yang [24] are employed in compliance with the product codes design of the codes.

Example 2 (cont.): C is the direct product of the parity-check codes (5, 4) and (3, 2). According to Theorem 4 of [24], the GHW hierarchy of C is $\{0, 4, 6, 8, 9, 11, 12, 14, 15\}$. The DLP of C is thereby $\{0, 0, 0, 0, 1, 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8\}$. As a consequence, according to (3), the SSP is lower-bounded by $\{0, 1, 2, 2, 2, 3, 2, 3, 3, 2, 3, 2, 2, 2, 1, 0\}$. Notice that the actual SSP which is accomplished by the coordinate ordering of Theorem 3, and met by its upper bound, is $\{0, 1, 2, 2, 3, 3, 2, 3, 3, 2, 3, 3, 2, 2, 1, 0\}$.

Example 6 (cont.): C contains the subcode $E^{(0)} \otimes D_0$, where $E^{(0)}$ is the binary BCH (21, 3, 12) code with defining set $\{0, 1, 3, 5, 7\}$ and D_0 is the (5, 4, 2) code. Theorem 7 implies that $E^{(0)} = (3, 1, 3) \otimes (7, 3, 4)$. Clearly $d_1(E^{(0)}) = 12$ and $d_3(E^{(0)}) = 21$. It follows from [24, Theorem 3] that $d_2(E^{(0)}) = 18$. Applying the theorem again on C, with the aid of monotonicity [12] and the tables of [23], yields $d_1(C) = 24$, $d_2(C) = 36$, $d_3(C) = 42$, $45 \leq d_4(C) \leq 54$, $47 \leq d_5(C) \leq 62$, $d_6(C) \leq 63$, $d_7(C) \leq 77$, $d_8(C) \leq 78$, $d_9(C) \leq 79, \cdots, d_{34}(C) \leq 104$, $d_{35}(C) = 105$.

TABLE I
UPPER BOUNDS ON THE ABSOLUTE MINIMAL TRELLIS SIZE FOR $\gcd(n, N) = 1$

	Code		n	N	$\mathfrak{C}$	B_W	B'	B	$\mathscr{D}$
▹	BCH	(15,6,6)	3	5	0,1,7	6	6	4*	1.5
▹	Cyclic	(15,8,4)	3	5	0,3,5	7	3*	3*	1.2
▹	Cyclic	(21,15,4)	3	7	0,3,7	6	4*	4*	1.4
	BCH	(35,20,6)	7	5	1,5	15	15	9	2.9
▹	BCH	(35,28,4)	7	5	5,7	7	7	5*	1.7
▹	BCH	(51,26,10)	3	17	0,1,3,19	25	25	17	5.1
▹	Cyclic	(55,30,10)	5	11	0,1,11	25	21	21	6.2
	BCH	(57,21,14)	3	19	1,3	21	19	19	5.9
▹	Cyclic	(63,24,16)	7	9	0,1,5,7,9,11,15,21,27	24	24	18	5.7
▹	Cyclic	(63,27,16)	7	9	0,1,5,7,11,15,21,27	27	27	21	6.4
▹	Cyclic	(85,36,18)	17	5	0,1,5,7,9,13,15	36	33	30	9.1
▹	Cyclic	(85,45,14)	5	17	5,9,13,15,29	40	40	26	7.8
▹	Cyclic	(85,49,12)	5	17	3,5,9,15,17	36	36	22	6.7
▹	Cyclic	(85,53,10)	5	17	3,5,7,15	32	32	18	5.6
▹	Cyclic	(85,73,4)	5	17	17,37	12	12	10	3.2
▹	BCH	(87,31,22)	3	29	1,3	31	29	29	8.9
▹	Cyclic	(93,22,30)	3	31	0,1,3,5,7,9,11,15,17,33	22	22	21	6.9
▹	Cyclic	(93,46,16)	3	31	11,17,21,23,31,33,45	46	36	36	10.7
▹	Cyclic	(93,70,8)	3	31	0,21,23,31,45	23	21	21	6.4
	Cyclic	(105,23,28)	5	21	0,1,3,5,9,13,15,17,21,25,35	23	23	19	6.4
▹	Cyclic	(105,35,24)	5	21	5,7,9,11,13,15,17,21,35,45	35	34	29	9.1
	BCH	(111,39,22)	3	37	1,3	39	37	37	9.2
▹	BCH	(119,108,4)	7	17	17,21	11	11	9	2.9

TABLE II
UPPER BOUNDS ON THE ABSOLUTE MINIMAL TRELLIS SIZE FOR $\gcd(n, N) > 1$

	Code		n	N	$\mathfrak{C}$	B_W	B'	B	$\mathscr{D}$
	BCH	(25,4,10)	5	5	0,1	4	2*	2*	1.5
	Cyclic	(45,9,12)	3	15	1,5,7,9,15	9	7	5	2.3
	BCH	(45,22,8)	15	3	0,1,3,5	22	10	10	3.3
▹	BCH	(63,38,10)	3	21	0,1,3,15,31	25	25	17	5.2
	Cyclic	(63,39,8)	21	3	0,1,3,7,21,27	24	10	10	3.2
▹	Cyclic	(63,43,8)	3	21	1,7,9,21,27	20	16	14	4.3
▹	Cyclic	(63,45,8)	3	21	0,1,3,15,31	18	18	17	5.1
▹	Cyclic	(63,47,6)	21	3	0,1,3,27	16	10	10	3.2
	Cyclic	(63,48,5)	21	3	1,3,27	15	9	9	2.9

Example 7 (cont.): C is the direct sum of $C^{(1)} \triangleq (5, 4) \otimes (3, 1)$ and $C^{(2)} \triangleq (5, 1) \otimes (3, 2)$. Applying Theorem 3 on $C^{(1)}$ and $C^{(2)}$ yields the upper bounds $\{0, 1, 1, 1, 2, 2, 1, 2, 2, 1, 2, 2, 1, 1, 0\}$ and $\{0, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 1, 0\}$ on their SSP's, respectively. The upper bound $\{0, 1, 2, 3, 4, 4, 3, 4, 4, 3, 4, 4, 3, 2, 1, 0\}$ on the SSP of C is thereby derived. According to [24, Theorem 7], the GHW of $C^{(1)}$ and $C^{(2)}$ are $\{6, 9, 12, 15\}$ and $\{10, 15\}$, respectively. Clearly, $d_{i+j}(C) \leq d_i(C^{(1)}) + d_j(C^{(2)})$. Applying the tables of [23] and monotonicity [12] yields $d_1(C) = 6$, $d_2(C) = 9$, $11 \leq d_3(C) \leq 12$, $12 \leq d_4(C) \leq 13$, $d_5(C) = 14$, $d_6(C) = 15$. The GHW hierarchy leads to the DLP $\{0, 0, 0, 0, 0, 0, 1, 1, 1, 2, 2, \leq 3, \leq 4, 4, 5, 6\}$. The lower bound $\{0, 1, 2, 2, 3, 4, 3, 4, 4, 3, 4, 3, 2, 2, 1, 0\}$ on the SSP is readily derived by (3).

Following the above few examples, further results on the GHW hierarchy and DLP can be obtained for the codes in Tables I and II and for many other CLCC's.

ACKNOWLEDGMENT

The authors wish to thank G. D. Forney for providing manuscripts of his papers.

REFERENCES

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

[2] G. D. Forney, Jr., "Coset codes—part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, 1988.

[3] Y. Berger and Y. Be'ery, "Soft trellis-based decoder for linear block codes," *IEEE Trans. Inform. Theory,* vol. 40, pp. 764–773, 1994.
[4] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory,* vol. 34, pp. 1049–1053, 1988.
[5] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes," *IEEE Trans. Inform. Theory,* vol. 39, pp. 203–209, 1993.
[6] G. D. Forney, Jr., and M. D. Trott, "The dynamics of group codes: State spaces, trellis diagrams and canonical encoders," *IEEE Trans. Inform. Theory,* vol. 39, pp. 1491–1513, 1993.
[7] 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, 1993.
[8] G. D. Forney, Jr., "Dimension/length profiles and trellis complexity of linear block codes," preprint, submitted to *IEEE Trans. Inform. Theory.*
[9] T. Fujiwara, T. Kasami, R. Morelos-Zaragoza, and S. Lin, "The state complexity of trellis diagram for a class of generalized concatenated codes," in *16th Symp. on Information Theory and its Applications* (Kanazawa, Japan, Oct. 1993).
[10] A. Vardy and Y. Be'ery, "Maximum-likelihood soft-decision decoding of BCH codes," *IEEE Trans. Inform. Theory,* vol. 40, pp. 546–554, 1994.
[11] J. Snyders and Y. Be'ery, "Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes," *IEEE Trans. Inform. Theory,* vol. 35, pp. 963–975, 1989.
[12] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory,* vol. 37, pp. 1412–1418, Sept. 1991.
[13] E. R. Berlekamp, *Algebraic Coding Theory.* Laguna Hills, CA: Aegean Park Press, 1984.
[14] Y. Be'ery and J. Snyders, "A recursive Hadamard transform optimal soft decision decoding algorithm," *SIAM J. Alg. Disc. Math.,* vol. 8, no. 4, pp. 778–789, 1987.
[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North Holland, 1977.
[16] E. R. Berlekamp and J. Justesen, "Some long cyclic linear binary codes are not so bad," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 351–356, 1974.
[17] Y. Be'ery, "Optimal decoding of error correcting codes based on fast transforms," Ph.D. dissertation, Faculty of Electrical Engineering, Tel-Aviv Univ., Tel-Aviv, Israel, 1985.
[18] T. Kasami, "Some lower bounds on the minimum weight of cyclic codes of composite length," *IEEE Trans. Inform. Theory,* vol. IT-14, pp. 814–818, 1968.
[19] ——, "Construction and decomposition of cyclic codes of composite length," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 680–683, 1974.
[20] J. M. Jensen, "The concatenated structure of cyclic and abelian codes," *IEEE Trans. Inform. Theory,* vol. IT-31, pp. 788–793, 1985.
[21] ——, "Cyclic concatenated codes with constacyclic outer codes," *IEEE Trans. Inform. Theory,* vol. 38, pp. 950–959, 1992.
[22] G. Promhouse and S. E. Tavares, "The minimum distance of all binary cyclic codes of odd lengths from 69 to 99," *IEEE Trans. Inform. Theory,* vol. IT-24, pp. 438–442, 1978.
[23] 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, 1993.
[24] V. K. Wei and K. Yang, "On the generalized Hamming weights of product codes," *IEEE Trans. Inform. Theory,* vol. 39, pp. 1709–1713, 1993.

Constructing a Better Cyclic Code than Cyclic Reed–Solomon Code

Czesław Kościelny

***Abstract*— Problems of computing the generator polynomial for a $(q+1, q-d+2)$ reversible cyclic BCH code over GF(q), $q = p^m$, having the minimum Hamming distance d, are presented. The considered code is almost as short as a Reed–Solomon (RS) code but it generates codewords with two information symbols more than the codewords of RS code with the same minimum Hamming distance.**

***Index Terms*—Cyclic codes, Reed–Solomon codes, reversible codes, self-reciprocal polynomials.**

I. Introduction

The Reed–Solomon (RS) code has been widely used recently in many communication and computer systems [1], [2]. It has been noticed [4], however, that two information symbols can be added to the codeword of an RS code without diminishing the guaranteed minimum Hamming distance of this code. Another observation [1, p. 220] shows that these two extra symbols can be used either as information or redundancy components. Thus by adding two symbols to the RS code one can increase either the rate of this code or its minimum distance. Codes, modified in this manner, are commonly known as extended Reed–Solomon codes over GF(q). This means that there exists a code, with a better code ratio than the RS, namely, a $(q+1, q-d+2)$ code over GF(q).

Up to now, only a noncyclic form of the extended RS cyclic codes have been considered. As is known, the scope of applications of noncyclic codes is very limited. Therefore, the author has proved the existence of the cyclic form of $(q+1, q-d+2)$ extended RS codes, considering the effect of increasing the code rate only, and has shown that these codes can be easily constructed.

II. Computing the Generator Polynomial of a $(q+1, q-d+2)$ Cyclic Code over GF(q)

Let $q = p^m, p$ be a prime number, m a positive integer ≥ 2 if $p = 2$ and ≥ 1 if $p > 2$. It can be proved that over GF(q) there exists a factorization

$$x^{q+1} - 1 = \prod_{i=0}^{i_{\max}} m_i(x) \tag{1}$$

where

$$i_{\max} = \begin{cases} q/2. & \text{if } p = 2 \\ (q+1)/2, & \text{if } p > 2. \end{cases} \tag{2}$$

In (1), the symbol $m_i(x)$ denotes the minimum function for element $\beta^i, \beta = \omega^{q-1}$, where ω is primitive element of GF(q^2). Since $(\beta^i)^{q+1} = 1$, then $\beta^{iq} = \beta^{-i}$. This means that all factors of (1) are irreducible self-reciprocal polynomials, except for m_0 when $p > 2$.

Manuscript received October 11, 1993; revised September 24, 1994.

The author was with the Technical University of Wrocław, Institute of Engineering Cybernetics, 50-372 Worcław, Poland. He is now with the Department of Robotics and Software Engineering, Technical University of Zielona Góra, 65-246 Zielona Góra, Poland.

IEEE Log Number 9411963.