On the Trellis Complexity of Composite-Length Cyclic Codes

Yuval Berger and Yair Be'ery

Department of Electrical Engineering - Systems, Tel Aviv University, Ramat Aviv 69978, Tel Aviv, Israel

***Abstract* - The trellis complexity of block codes is closely related to their soft-decision decoding complexity. We investigate the trellis properties of composite-length cyclic codes. Trellis-oriented decompositions are presented, and improved upper bounds on the trellis complexity are derived.**

I. Introduction

The research on trellis diagrams of block codes is strongly motivated by the increased interest in efficient trellis-based soft-decision decoding algorithms [1]-[3]. The main objective is to reduce the trellis complexity.

Denote by $C(n,k)$ a linear block code of length n and dimension k. Denote by s_i the logarithm of the state space dimension at position i. Define the *minimal trellis size* by $s=\max\{s_i\}$. Let $s(C)$ denote the minimal s, related to the unique *minimal trellis* [4], attainable by any permutation on C. The well known Wolf bound [1] is $s(C)\leq\min(k,n-k)$. This bound was improved in [5]. A general lower bound on $s(C)$ was given in [4], and improved in [6]. Further results on the trellis properties were derived in [2],[5]-[7] for the classes of Reed-Muller and BCH codes.

In this study we focus on the trellis complexity of composite-length cyclic codes (CLCCs). We employ known decomposition into concatenated codes [8],[9], and derive new decomposition based on direct product codes. Trellis-oriented coordinate permutations and upper bounds on the trellis complexity parameters are established [10].

II. Trellis complexity of combined codes

Theorem 1: Denote by $C_1(N,K)$ a code over $GF(q^k)$, and let $C_2(n,k)$ denote a code over $GF(q)$. Let C be the concatenated code $C_1 * C_2$. Then

$$s(C) \leq ks(C_1) + s(C_2). \qquad (1)$$

If $s(C_1)$ and $s(C_2)$ are replaced in (1) with the Wolf bound, then a generalized Wolf bound

$$s(C) \leq \min\{k(N-K)+\min(k,n-k)\ ,\ kK\} \qquad (2)$$

is obtained. In many cases the bound in (2) significantly improves the Wolf bound $s(C)\leq\min(kK,nN-kK)$.

Theorem 2: Let $C_1(N,K)$ and $C_2(n,k)$ be codes over $GF(q)$. Let C be the direct product code $C_1 \otimes C_2$. Then $s(C)$ is upper bounded as indicated in (1) and (2).

The code $C_2 \otimes C_1$ is equivalent to $C_1 \otimes C_2$. Therefore, alternative bounds on $s(C)$ are obtained by interchanging C_1 and C_2 in (1) and (2).

III. Trellis complexity of CLCCs

The concatenated structure of CLCCs in which $\gcd(n,N)=1$ was determined in [8]. Recently, a similar decomposition was established in [9] for the case of $\gcd(n,N)>1$. In both cases, a minimal CLCC is a concatenation of an outer code over $GF(q^k)$ and an inner minimal cyclic code over $GF(q)$. Denote by D_l the minimal cyclic code of length n over $GF(q)$ with nonzero α^i, where α is a primitive n^{th} root of unity.

Theorem 3: Let C be a CLCC. Then $C=\bigcup_{l\in\Theta} C^{(l)}$, where $C^{(l)} = E^{(l)} * D_l$ and $\{D_l\}_{l\in\Theta}$ contains the minimal inner codes of the concatenated minimal subcodes of C. Also $s(C)\leq\sum_{l\in\Theta} s^{(l)}$, where $s^{(l)}$ denotes the minimal trellis size of $C^{(l)}$.

The decomposition of Theorem 3 is used to derive the following result.

Theorem 4: Let C denote a CLCC. Define $\hat{C}^{(l)} = \hat{E}^{(l)} \otimes D_l$, where $\hat{E}^{(l)}$ is the subfield subcode of $E^{(l)}$. Then $\bigcup_{l\in\Theta} \hat{C}^{(l)} \subseteq C$. Also $s(C)\leq\sum_{l\in\Theta}\hat{s}^{(l)} + |C / \bigcup_{l\in\Theta}\hat{C}^{(l)}|$, where $\hat{s}^{(l)}$ is the minimal trellis size of $\hat{C}^{(l)}$.

Upper bounds on the trellis complexity are obtained by determining trellis-oriented permutations, according to Theorems 1 and 2, in view of Theorems 3 and 4.

The best bounds on $s(C)$ attained for several CLCCs are listed in Table I, and referred by B*. The bounds are compared to the Wolf bound (B_W) [1] and to the bound derived from the work of Vardy and Be'ery (B_{VB}) [7].

TABLE I
UPPER BOUNDS ON $s(C)$ FOR BINARY CLCCs

Code	n	N	Roots	B_W	B_{VB}	B*
BCH (25,4,10)	5	5	0,1	4	2	2
BCH (35,28,4)	5	7	5,7	7	7	5
Cyclic (45,9,12)	3	15	1,5,7,9,15	9	7	5
Cyclic (63,42,8)	9	7	0,1,7,9,21,27	20	16	14
Cyclic (85,49,12)	5	17	3,5,9,15,17	36	36	22
Cyclic (105,35,24)	5	21	5,7,9,11,13,15, 17,21,35,45	35	34	29

References

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

[2] G. D. Forney, Jr., "Cosets 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*, to appear, May, 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] 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.

[7] A. Vardy and Y. Be'ery, "Maximum-likelihood soft-decision decoding of BCH codes," *IEEE Trans. Inform. Theory*, to appear, March, 1994.

[8] E. R. Berlekamp and J. Justesen, "Some long cyclic linear binary codes are not so bad," *IEEE Trans. Inform. Theory*, vol. 20, pp. 351-356, 1974.

[9] J. M. Jensen, "Cyclic concatenated codes with constacyclic outer codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 950-959, 1992.

[10] Y. Berger and Y. Be'ery, "Trellis-oriented decomposition and trellis complexity of composite-length cyclic codes,", submitted to *IEEE Trans. Inform. Theory*, 1994.