On the Twisted Squaring Construction, Symmetric-Reversible Designs and Trellis Diagrams of Block Codes

Yuval Berger and Yair Be'ery

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

Abstract - **The structure of the twisted squaring construction is studied. We focus on the subclass of symmetric-reversible codes and show that it includes the extended primitive BCH codes. New results on the trellis complexity of these constructions, and the BCH codes in particular, are derived.**

I. Introduction

Trellis diagrams are primarily used for efficient soft-decision decoding [1]-[3]. The structure of the codes is a fundamental key for investigating the associated trellis diagrams [2],[4]-[7]. The *squaring construction* (SC) was employed by Forney [2] to derive trellis-oriented designs, particularly applied for RM codes and Barnes-Wall lattices. We are interested in the *twisted squaring construction* (TSC), a generalization of the SC [2]. The Nordstrom-Robinson code and a related packing are known examples of nonlinear TSC [2]. We classify several families of the TSC and focus on the *symmetric-reversible codes*. We show that they include the extended primitive BCH codes. The constructions are characterized and new results on the related trellis diagrams are developed.

II. The Twisted Squaring Construction

We follow the notations of [2]. Let *S/T* denote the partition of a discrete set S into $M = |S / T|$ disjoint subsets T_i, $i = 0,1,\cdots,M-1$. The *minimum distance* $d(S)$ is defined as the minimum nonzero *distance* $d(s_1,s_2)$ associated with any pair $(s_1,s_2) \in S$. We also define $d(T)$ as the minimum $d(T_i)$ among the subsets of S. Let T_i^2 denote the set of all pairs (s_1,s_2) where $s_1,s_2 \in T_i$. The SC is the union U of the M sets T_i^2, and $d(U) = \min\{d(T),2d(S)\}$ [2]. Let $C(n,k)$ denote a linear code over GF(q) with length n and dimension k. Let D be a subcode of C. The SC is labeled by $|C / D|^2$. It consists of codewords (d_1+b,d_2+b), where $d_1,d_2 \in D$ and b belongs to the space $B=[C/D]$ of cosets representatives of D in C. The TSC is the union W of M sets T_iT_j, where i and j cover all values between 0 and M. The lower bound $d(W) \geq \min\{d(T),2d(S)\}$ [2] suggests an improvement of the TSC over the SC. The TSC in terms of linear codes will be labeled by $\|C / D\|^2$. It consists of codewords (d_1+b,d_2+b'), where b and b' run through all elements of B. Let G_C and G_D denote the generator matrices of C and D, respectively. The generator matrix of $\|C / D\|^2$ is equivalent to

$$\begin{pmatrix} G_C & \tilde{G}_C \\ 0 & G_D \end{pmatrix},$$

where $\tilde{G}_C$ is obtained from G_C by elementary row operations.

III. Symmetric-Reversible and Related Codes

A code A is called *symmetric* if $(a_1,a_2) \in A$ implies that $(a_2,a_1) \in A$. We show that any symmetric code is a TSC, and $\tilde{G}_C = EG_C$ such that E is invertible and E^2 is equivalent to the identity matrix. A code is called *reversible* if it contains the reversed version of every codeword. A symmetric-reversible (SR) code is hereby defined as a code that is both symmetric and reversible. We show that part of the above properties are inherited to the subcodes C and D. A code is called *affine-invariant* (AI) if it is invariant under the affine permutation. This class includes the Reed-Muller (RM) and extended primitive BCH codes. We prove that AI codes are iterated SR codes (and obviously iterated TSC), i.e., the subcodes C and D are also SR codes. We characterize the constructions and show that the dual TSC and dual SR designs are, respectively, TSC and SR designs.

IV. Trellis Complexity

A general description of trellis diagrams of block codes is given in [1],[2]. For a given coordinate ordering, the *minimal trellis size* s is defined as the maximal state-space dimension of the *minimal trellis diagram* [2]. The minimal s over any permutation of a code A is labeled by $s(A)$. The general Wolf bound is $s(A) \leq \min\{k,n-k\}$ [1]. Let A be a TSC code $\|C / D\|^2$. A simple recurrence formula for the trellis complexity is given by

$$s(A) \leq s(D) + \dim(C) - \dim(D).$$

Improved bounds are derived for iterated SR codes such as primitive BCH codes. Upper bounds on the decoding complexity are thereby implied in conjunction with results of [3]. Some examples of binary primitive BCH codes are given in Table I. Actual s parameters were numerically obtained using computer program (see also [5],[6]).

TABLE I

Upper bounds on $s(A)$ for primitive BCH codes

Code	C	D	Wolf Bound	New Bound	s
(16,7,6)	(8,6)	(8,1)	7	6	6
(32,21,6)	(16,15)	(16,6)	11	10	10
(64,45,8)	(32,29)	(32,16)	19	15	14
(64,36,12)	(32,26)	(32,10)	28	21	19

Additional results are developed utilizing the highly structural constructions. Furthermore, the trellis complexity of long BCH codes may be evaluated. The constructions may also be useful for related applications such as the generalized weight hierarchy [8].

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*, vol. 40, pp. 764-773, 1994.

[4] 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.

[5] 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.

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

[7] Y. Berger and Y. Be'ery, "Trellis-oriented decomposition and trellis complexity of composite-length cyclic codes," *IEEE Trans. Inform. Theory*, to appear, July, 1995.

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