References

[1] A. H. Banihashemi and I. F. Blake, "Minimal trellis diagrams of lattices," in *Proc. IEEE Int. Symp. Information Theory* (Ulm, Germany, June 29–July 4, 1997), p. 434.

[2] ——, "Trellis complexity and minimal trellis diagrams of lattices," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1829–1847, Sept. 1998.

[3] Y. Berger and Y. Be'ery, "The twisted squaring construction, trellis complexity, and generalized weights of BCH and QR codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1817–1827, Nov. 1996.

[4] I. F. Blake and V. Tarokh, "On the trellis complexity of the densest lattice packings in $\mathbb{R}^n$," *SIAM J. Discr. Math.*, vol. 9, no. 4, pp. 597–601, Nov. 1996.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1993.

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

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

[8] ——, "Density/length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1753–1772, Nov. 1994.

[9] 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, Sept. 1993.

[10] G. B. Horn and F. R. Kschischang, "On the intractability of permuting a block code to minimize trellis complexity," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2042–2048, Nov. 1996.

[11] G. A. Kabatyanskii and V. I. Levenshtein, "Bounds for packings on a sphere and in space," *Probl. Inform. Transm.*, vol. 14, no. 1, pp. 1–17, Mar. 1978.

[12] 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.

[13] ——, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1057–1064, May 1993.

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

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

[16] J. H. Lindsey II, "Sphere packing in R^3," *Mathematika*, pt. 1, vol. 33, pp. 137–147, June 1986.

[17] R. Lucas, M. Bossert, and M. Breitbach, "On iterative soft decision decoding of linear binary block codes and product codes," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 276–296, Feb. 1998.

[18] I. Reuven and Y. Be'ery, "Entropy/length profiles, bounds on the minimal covering of bipartite graphs, and trellis complexity of nonlinear codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 580–598, Mar. 1998.

[19] C. A. Rogers, "The packing of equal spheres," *Proc. London Math. Soc.*, vol. 3, no. 8, pp. 609–620, 1958.

[20] V. R. Sidorenko, "The Euler characteristic of the minimal code trellis is maximum," *Probl. Inform. Transm.*, vol. 33, pp. 72–77, 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, pp. 2048–2053, Nov. 1996.

[22] V. Tarokh and I. F. Blake, "Trellis complexity versus the coding gain of lattices I," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1796–1807, Nov. 1996.

[23] ——, "Trellis complexity versus the coding gain of lattices II," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1808–1816, Nov. 1996.

[24] V. Tarokh and A. Vardy, "Upper bounds on trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1294–1300, July 1997.

[25] A. Vardy, "A new sphere packing in 20 dimensions," *Invent. Math.*, vol. 121, pp. 119–133, 1995.

[26] A. Vardy and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2027–2034, Nov. 1996.

[27] V. V. Vazirani, H. Saran, and B. S. Rajan, "An efficient algorithm for constructing minimal trellises for codes over finite abelian groups," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1839–1854, Nov. 1996.

[28] V. K. Wei and K. Yang, "On the generalized Hamming weights of product codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1709–1713, Sept. 1993.

The Preparata and Goethals Codes: Trellis Complexity and Twisted Squaring Constructions

Yaron Shany and Yair Be'ery, *Senior Member, IEEE*

***Abstract*—The trellis complexity of the Preparata and Goethals codes is examined. It is shown that at least for a given set of permutations these codes are rectangular. Upper bounds on the state complexity profiles of the Preparata and Goethals codes are given. The upper bounds on the state complexity of the Preparata and Goethals codes are determined by the DLP of the extended primitive double- and triple-error-correcting BCH codes, respectively. A twisted squaring construction for the Preparata and Goethals codes is given, based on the double- and triple-error-correcting extended primitive BCH codes, respectively.**

***Index Terms*— BCH codes, Goethals codes, Preparata codes, trellis complexity, twisted squaring construction.**

I. Introduction

We examine the trellis complexity of two interesting families of nonlinear codes: the Preparata codes and the Goethals codes. The Preparata codes [17], [1], [5] are binary nonlinear codes of length 2^{m+1} (for odd $m \geq 3$) and with minimum distance six that contain the maximum possible number of codewords for these parameters. These codes contain twice as many codewords as the corresponding extended primitive double-error-correcting BCH codes. For odd $m \geq 5$ the Goethals codes [17], [1] are nonlinear binary codes having the same length as the Preparata codes, and with minimum distance eight. These codes contain four times the number of codewords of the corresponding extended primitive triple-error-correcting BCH codes.

Trellis diagrams of block codes are employed for efficient soft-decision decoding. The theory of trellis diagrams of nonlinear block codes was considered in [8], [18], [16], [15], [14], [19], [21], and [22]. The structure and complexity of the trellis representations of specific nonlinear codes were given in [8], [16], [19] for relatively small codes, and in [20] for the Kerdock and Delsarte–Goethals codes.

Generally speaking, a nonlinear code under a given coordinate ordering may not have a trellis representation minimizing the vertex count at all indices simultaneously [15], [14]. However, when a nonlinear code satisfies certain conditions (namely, it is *rectangular*), it admits a unique *biproper* trellis representation. This biproper trellis minimizes both the edge and vertex counts at all indices simultaneously [15], [14]. Furthermore, as proved in [23] and [21] the biproper trellis minimizes also the total number of addition-equivalent operations required to perform the Viterbi algorithm.

Manuscript received October 1, 1997; revised January 5, 1999.

The authors are with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel (e-mail: ybeery@eng.tau.ac.il).

Communicated by F. Kschischang, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)04172-3.

It is known that permuting the code's coordinates changes its trellis representation. Lower bounds on the trellis complexity of a nonlinear code under any coordinate ordering were given in [18], [16], and recently in [19], where a new connection between trellis complexity and information theory was introduced. A code that is rectangular under a given coordinate ordering may not be rectangular under other coordinate orderings, as exemplified in [19].

In this correspondence we consider the trellis complexity of the Preparata and Goethals codes. It is shown that these codes are rectangular at least for some bit orders. An upper bound on the state complexity profile of these codes is derived as a function of the *DLP* [9] of BCH codes. A *twisted squaring construction* [8], [3] for these codes is also given.

In a paper from 1994 [12], Hammons et al. presented two families of nonlinear binary codes, the "Preparata" and "Goethals" codes, which are the image under the Gray map of linear codes over $\mathbb{Z}_4$. The "Preparata" and "Goethals" codes are not equivalent to the original Preparata and Goethals codes, but they have the same parameters (respectively).

Some authors utilized the $\mathbb{Z}_4$-linearity of the quaternary codes to find properties of their binary images. For example, Sidorenko *et al.* [22] mentioned the immediate result that under a correct bit order, the binary image of a $\mathbb{Z}_4$-linear code will have a rectangular past/future relation at every *second* index. However, there is no result known to the authors that proves the existence of a bit order for which the binary image of a $\mathbb{Z}_4$-linear code admits a rectangular past/future relation at *every* index.

Carlet [6] gave a simple description of the binary "Preparata" codes. This description is similar to the one that Baker *et al.* [1] gave for the Preparata codes. However, applying the simple methods used in the present work to the binary "Preparata" codes is not trivial: Even proving that these codes are rectangular appears to be a difficult task.

The correspondence is arranged as follows. In Section II we give the basic definitions relevant for the succeeding sections. We repeat the simple definition of the Preparata and Goethals codes given by Baker *et al.* in [1]. In Section III we show that for some bit orders both the Preparata and the Goethals codes are rectangular. In Section IV we examine the trellis complexity of the codes. An upper bound (which may not be achieved at all indices simultaneously) on the trellis complexity of the Preparata (resp., Goethals) codes is determined from the DLP of extended primitive double- (resp., triple-) error-correcting BCH codes. The given bound is shown to be equal (at each index) to the minimum possible state complexity profile over all bit orders for which we proved that the codes are rectangular. Using the same methods, we present a lower bound on the first half of the *conditional ELP* profile [19] of these codes. A twisted squaring construction is given for both codes in Section V.

II. Preliminaries

A. Trellis Diagrams for Block Codes

An *edge-labeled directed graph* is the triple (V, A, E) where V is a set of *vertices*, A is a finite set (the *alphabet*), and E is the set of *edges*, i.e., the set of ordered triples (v, v', α), where $v, v' \in V$, $\alpha \in A$. A trellis diagram $G(V, A, E)$ is an edge-labeled directed graph with the property that the set V can be decomposed into $n+1$ disjoint subsets $V = V_0 \cup V_1 \cup \cdots \cup V_n$, such that if $(v, v', \alpha) \in E$ then $v \in V_i$, $v' \in V_{i+1}$ for some $i \in \{0, 1, \cdots, n-1\}$. The set V_i, $i \in \{0, 1, \cdots, n\}$, is referred to as the set of vertices at index i. Moreover, two additional conditions are required:

1) There is a single initial vertex, and a single final vertex: $|V_0| = |V_n| = 1$.
2) Each state $v \in V$ lies on some length-n path connecting the initial vertex with the final vertex.

When an edge-labeled directed graph $G(V, A, E)$ is a trellis diagram, we use the notation *states* for vertices, and the notation *branches* for edges. In such a case we denote $S = V$ and $S_i = V_i$.

Any path in the trellis connecting the initial state with a state $s \in S_i$, $i \in \{1, 2, \cdots, n\}$, defines an i-tuple $(\alpha_1, \alpha_2, \cdots, \alpha_i)$, $\alpha_j \in A$, $1 \le j \le i$. A trellis diagram is said to be *proper* if for each $i \in \{1, 2, \cdots, n\}$ no two distinct length-i paths beginning at the initial state represent the same i-tuple. A trellis diagram is said to be biproper if both the trellis itself and the reverse trellis are proper.

In what follows, we consider the case $A = \mathrm{GF}(2)$. The *state complexity* at index i is defined as $s_i = \log_2 |S_i|$.

A binary block code of length n is a subset of $\mathrm{GF}(2)^n$. The notation $[n, k, d]$ code stands for a linear binary block code of length n, dimension k, and minimum distance d. We denote a length-n (nonlinear) binary block code with M codewords, and with minimum distance d as an (n, M, d) code.

Let G be a trellis diagram, and let $\mathcal{C}$ be a binary block code of length $n > 1$, under a given bit order. G is said to be a trellis representation of $\mathcal{C}$, $G(\mathcal{C})$, iff the set of n-tuples corresponding to all length-n paths in G is identical to $\mathcal{C}$.

Let $\boldsymbol{c} = (c_1, c_2, \cdots, c_n)$ be a codeword of $\mathcal{C}$. For $0 < i \le n$, we denote the *past projection* of $\boldsymbol{c}$ by $\Pi_{i-}(\boldsymbol{c}) = (c_1, c_2, \cdots, c_i)$. Similarly, for $0 \le i < n$ we denote the *future projection* of $\boldsymbol{c}$ by $\Pi_{i+}(\boldsymbol{c}) = (c_{i+1}, c_{i+2}, \cdots, c_n)$. The past and future projections of the code $\mathcal{C}$ are defined as

$$\Pi_{i-}(\mathcal{C}) = \bigcup_{\boldsymbol{c} \in \mathcal{C}} \Pi_{i-}(\boldsymbol{c})$$

and

$$\Pi_{i+}(\mathcal{C}) = \bigcup_{\boldsymbol{c} \in \mathcal{C}} \Pi_{i+}(\boldsymbol{c})$$

respectively. When $\mathcal{C}$ is a linear code, it is of interest to define the *past code* of $\mathcal{C}$ at index $i \in \{1, 2, \cdots, n-1\}$ as

$$\mathcal{C}_i = \{(c_1, c_2, \cdots, c_i) : (c_1, c_2, \cdots, c_n) \in \mathcal{C}, (c_{i+1}, c_{i+2}, \cdots, c_n) = (0, 0, \cdots, 0)\}.$$

By convention we take $\mathcal{C}_n = \mathcal{C}$.

Let $\boldsymbol{a} = (a_1, a_2, \cdots, a_{l_a})$, $l_a \ge 1$, and $\boldsymbol{b} = (b_1, b_2, \cdots, b_{l_b})$, $l_b \ge 1$ be two binary vectors. We denote the *concatenation* of the vectors as $\boldsymbol{a} \cdot \boldsymbol{b} = (a_1, a_2, \cdots, a_{l_a}, b_1, b_2, \cdots, b_{l_b})$. The *support* of the vector $\boldsymbol{a}$ is defined as $\mathrm{supp}\,(\boldsymbol{a}) = \{j : a_j \ne 0\}$.

$\mathcal{C}$ is said to be rectangular [14] if, at each $i \in \{1, 2, \cdots, n-1\}$, $\{\boldsymbol{a} \cdot \boldsymbol{c}, \boldsymbol{a} \cdot \boldsymbol{d}, \boldsymbol{b} \cdot \boldsymbol{c}\} \subset \mathcal{C}$ implies $\boldsymbol{b} \cdot \boldsymbol{d} \in \mathcal{C}$, where $\boldsymbol{a}, \boldsymbol{b} \in \Pi_{i-}(\mathcal{C})$ and $\boldsymbol{c}, \boldsymbol{d} \in \Pi_{i+}(\mathcal{C})$. A rectangular code admits a unique biproper trellis representation, which minimizes both the state complexity and the edge complexity at all indices simultaneously. It was shown in [23], [21] that this trellis minimizes also the total number of addition-equivalent operations required to perform the Viterbi algorithm.

Define $s_{\max}$ to be the minimum value that $\max_{i \in \{1, 2, \cdots, n\}} s_i$ attains when going through all the trellis representations of all the permutations of $\mathcal{C}$. This definition is valid both for rectangular and nonrectangular codes.

B. The Preparata and Goethals Codes

For $m \ge 1$, let $I = \{1, 2, \cdots, 2^m\}$. Let T: $\mathrm{GF}(2^m) \to I$ be one-to-one, and let $A = \{a_1, a_2, \cdots, a_l\}$, $l \le 2^m$, be a subset of $\mathrm{GF}(2^m)$. We define the transformation T on the set A as

$$T(A) = \{T(a_1), T(a_2), \cdots, T(a_l)\}.$$

A length-2^m binary vector, $\chi_T(A)$, is associated with the set A in the following way: for each $1 \le j \le 2^m$, the jth entry of $\chi_T(A)$

is 1 iff $j \in T(A)$. For a set $A = \{a_1, a_2, \cdots, a_l\}$ and an integer $1 \le i_0 \le n-1$ which satisfy

$$\min[T(A)] \ge i_0$$

and

$$\max[T(A)] \le i_0 + i - 1$$

we define $\chi_T^{i;i_0}(A)$ to be a length-i binary vector, having ones in the coordinates $\{j - i_0 + 1 : j \in T(A)\}$ and zeroes in the remaining coordinates. $\chi_T^{i;i_0}(A)$ is simply $(x_{i_0}, x_{i_0+1}, \cdots, x_{i_0+i-1})$, where $(x_1, x_2, \cdots, x_{2^m}) = \chi_T(A)$.

For odd $m \ge 3$, let σ be a power of 2 such that $(\sigma \pm 1, 2^m - 1) = 1$. Thus $x \mapsto x^\sigma$ is an automorphism of GF(2^m), and both $x \mapsto x^{\sigma-1}$ and $x \mapsto x^{\sigma+1}$ are one-to-one. The *Preparata code* [1] $\mathcal{P}(T_1, T_2, \sigma)$ consists of the vectors $\chi_{T_1}(X) \cdot \chi_{T_2}(Y)$ for every $X, Y \subset$ GF(2^m) satisfying

$$|X| \text{ is even} \qquad |Y| \text{ is even,} \tag{1}$$

$$\sum_{x \in X} x = \sum_{y \in Y} y \tag{2}$$

and

$$\sum_{x \in X} x^{\sigma+1} + \left(\sum_{x \in X} x\right)^{\sigma+1} = \sum_{y \in Y} y^{\sigma+1} \tag{3}$$

where T_1, T_2: GF$(2^m) \rightarrow I$ are one-to-one. Obviously, given (2), we can rewrite (3) as

$$\sum_{x \in X} x^{\sigma+1} = \sum_{y \in Y} y^{\sigma+1} + \left(\sum_{y \in Y} y\right)^{\sigma+1}. \tag{4}$$

The length of the code is $n = 2^{m+1}$. It was shown in [1] that the minimum distance of $\mathcal{P}(T_1, T_2, \sigma)$ is 6, and that $|\mathcal{P}(T_1, T_2, \sigma)| = 2^k$, where $k = 2^{m+1} - 2m - 2$. It was mentioned in [1] and proved in [5] that for the special case $\sigma = 2$, the above definition of $\mathcal{P}(T_1, T_2, \sigma)$ gives a code which is equivalent to the standard definition of the Preparata code [17].

The *Goethals code* [1], $\mathcal{G}(T_1, T_2, r, s)$, consists of the words $\chi_{T_1}(X) \cdot \chi_{T_2}(Y)$ for every $X, Y \subset$ GF(2^m) satisfying (1) and (2), with the following two additional conditions:

$$\sum_{x \in X} x^r + \left(\sum_{x \in X} x\right)^r = \sum_{y \in Y} y^r \tag{5}$$

and

$$\sum_{x \in X} x^s + \left(\sum_{x \in X} x\right)^s = \sum_{y \in Y} y^s \tag{6}$$

where $r = \sigma_1 + 1$, $s = \sigma_2 + 1$, $r \ne s$, and both σ_1 and σ_2 satisfy the previously described conditions on σ.

It was proved in [1] that $\mathcal{G}(T_1, T_2, r, s)$ has minimum distance 8, and that $|\mathcal{G}(T_1, T_2, r, s)| = 2^l$, where $l = 2^{m+1} - 3m - 2$.

III. The Preparata and Goethals Codes Are Rectangular

In this section we show that at least for some bit orders, the Preparata and Goethals codes are rectangular.

Proposition 1: $\mathcal{P}(T_1, T_2, \sigma)$ is rectangular for any possible choice of T_1, T_2, and σ.

Proof: In order to establish the proof, it is sufficient to show that for every $i \in \{1, 2, \cdots, 2^{m+1} - 1\}$ it holds that if $\boldsymbol{x} \cdot \boldsymbol{y}$, $\boldsymbol{x} \cdot \boldsymbol{u}$, $\boldsymbol{v} \cdot \boldsymbol{y} \in \mathcal{P}(T_1, T_2, \sigma)$, then $\boldsymbol{v} \cdot \boldsymbol{u} \in \mathcal{P}(T_1, T_2, \sigma)$, where $\boldsymbol{x}, \boldsymbol{v} \in \Pi_{i-}[\mathcal{P}(T_1, T_2, \sigma)]$, and $\boldsymbol{y}, \boldsymbol{u} \in \Pi_{i+}[\mathcal{P}(T_1, T_2, \sigma)]$. We denote $\boldsymbol{v} \cdot \boldsymbol{u} = \chi_{T_1}(X') \cdot \chi_{T_2}(Y')$, and check whether $X', Y' \subseteq$ GF(2^m) satisfy (1)–(3).

Suppose $1 \le i \le n/2$. Then we can write

$$\boldsymbol{x} = \chi_{T_1}^{i;1}(a) \tag{7}$$

$$\boldsymbol{v} = \chi_{T_1}^{i;1}(b) \tag{8}$$

$$\boldsymbol{y} = \chi_{T_1}^{2^m - i; i+1}(\gamma) \cdot \chi_{T_2}(c) \tag{9}$$

$$\boldsymbol{u} = \chi_{T_1}^{2^m - i; i+1}(\delta) \cdot \chi_{T_2}(d) \tag{10}$$

where $a, b, c, \gamma, d, \delta \subset$ GF(2^m). From (8) and (10) it follows that

$$\boldsymbol{v} \cdot \boldsymbol{u} = \left[\chi_{T_1}^{i;1}(b) \cdot \chi_{T_1}^{2^m - i; i+1}(\delta)\right] \cdot \chi_{T_2}(d).$$

Hence $X' = b \cup \delta$ and $Y' = d$. Since

$$\boldsymbol{x} \cdot \boldsymbol{u} = \chi_{T_1}(a \cup \delta) \cdot \chi_{T_2}(d) \in \mathcal{P}(T_1, T_2, \sigma)$$

it holds that $|d|$ is even. In a similar way

$$-(|a| + |\gamma|) + (|a| + |\delta|) + (|b| + |\gamma|) = |b \cup \delta|$$

is even, and X', Y' satisfy (1).

Next we check whether

$$\sum_{x \in b \cup \delta} x = \sum_{y \in d} y.$$

Since $\boldsymbol{x} \cdot \boldsymbol{y} \in \mathcal{P}(T_1, T_2, \sigma)$, we have that

$$\sum_{x \in a \cup \gamma} x = \sum_{y \in c} y.$$

In a similar way we obtain that

$$\sum_{x \in a \cup \delta} x = \sum_{y \in d} y$$

and

$$\sum_{x \in b \cup \gamma} x = \sum_{y \in c} y.$$

Summing up the last three equations yields

$$\sum_{x \in b \cup \delta} x = \sum_{y \in d} y$$

and X', Y' satisfy (2).

It remains to show that X' and Y' satisfy (3) or (4). Again, since $\boldsymbol{x} \cdot \boldsymbol{y}, \boldsymbol{x} \cdot \boldsymbol{u}, \boldsymbol{v} \cdot \boldsymbol{y} \in \mathcal{P}(T_1, T_2, \sigma)$, we get

$$\sum_{x \in a \cup \gamma} x^{\sigma+1} = \sum_{y \in c} y^{\sigma+1} + \left(\sum_{y \in c} y\right)^{\sigma+1}$$

$$\sum_{x \in a \cup \delta} x^{\sigma+1} = \sum_{y \in d} y^{\sigma+1} + \left(\sum_{y \in d} y\right)^{\sigma+1}$$

$$\sum_{x \in b \cup \gamma} x^{\sigma+1} = \sum_{y \in c} y^{\sigma+1} + \left(\sum_{y \in c} y\right)^{\sigma+1}.$$

Summing up the last three equations establishes that X' and Y' satisfy (4) and completes the proof for $i \le n/2$.

For $i > n/2$ it can be proved in the same way that if $\chi_{T_1}(a) \cdot \chi_{T_2}(\alpha \cup c)$, $\chi_{T_1}(a) \cdot \chi_{T_2}(\alpha \cup d)$, $\chi_{T_1}(b) \cdot \chi_{T_2}(\beta \cup c) \in \mathcal{P}(T_1, T_2, \sigma)$, then also $\chi_{T_1}(b) \cdot \chi_{T_2}(\beta \cup d) \in \mathcal{P}(T_1, T_2, \sigma)$. □

The method used to prove Proposition 1 can also be applied to prove the following proposition.

Proposition 2: $\mathcal{G}(T_1, T_2, r, s)$ is rectangular for any possible choice of T_1, T_2, r, and s.

IV. The Vertex Count of the Preparata and Goethals Codes and the DLP of BCH Codes

A. Preparata Codes

Since $\mathcal{P}(T_1, T_2, \sigma)$ is rectangular, there exists a unique biproper trellis representation of the code for any fixed σ, T_1, and T_2. In this subsection we show that an upper bound on the state complexity profile of $\mathcal{P}(T_1, T_2, \sigma)$ can be determined from the dimensions of past codes of a linear code. As a result, an upper bound on the state complexity profile of $\mathcal{P}(T_1, T_2, 2)$, which is a function of the DLP [9] of an extended primitive double-error-correcting BCH code, is derived. Throughout this section we use the notation $n = 2^{m+1}$.

For $1 \leq i \leq n/2$, and for a given $\boldsymbol{u} \in \Pi_{i+}[\mathcal{P}(T_1, T_2, \sigma)]$ we examine the size of

$$\Xi_i(\boldsymbol{u}) = \{\boldsymbol{l} \in \Pi_{i-}[\mathcal{P}(T_1, T_2, \sigma)] : \boldsymbol{l} \cdot \boldsymbol{u} \in \mathcal{P}(T_1, T_2, \sigma)\}.$$

Let $\mathcal{L}$ be the linear binary code with parity-check matrix

$$H_{\mathcal{L}} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ T_1^{-1}(1) & T_1^{-1}(2) & \cdots & T_1^{-1}(2^m) \\ [T_1^{-1}(1)]^{\sigma+1} & [T_1^{-1}(2)]^{\sigma+1} & \cdots & [T_1^{-1}(2^m)]^{\sigma+1} \end{pmatrix}. \tag{11}$$

Lemma 3: For any choice of $\boldsymbol{u} \in \Pi_{i+}[\mathcal{P}(T_1, T_2, \sigma)]$, $1 \leq i \leq n/2$, we have

$$|\Xi_i(\boldsymbol{u})| = |\mathcal{L}_i| \tag{12}$$

where $\mathcal{L}_i$ is the past code of $\mathcal{L}$ at index i.

Proof: Denote $\boldsymbol{u} = \chi_{T_1}^{2^m-i;i+1}(\alpha) \cdot \chi_{T_2}(Y)$, $\boldsymbol{l} = \chi_{T_1}^{i;1}(a)$, (where $\boldsymbol{l} \in (\mathrm{GF}(2))^i$ and $a \subset \mathrm{GF}(2^m)$), and $X = a \cup \alpha$. $|\Xi_i(\boldsymbol{u})|$ is the number of different possible choices for the set $a \subset \mathrm{GF}(2^m)$ for which X, Y satisfy (1)–(3). Using (1), (2), and (4) we get

$$\sum_{x \in a} x^0 = \sum_{x \in \alpha} x^0 = \xi_0(\boldsymbol{u}) \tag{13}$$

$$\sum_{x \in a} x = \sum_{x \in \alpha} x + \sum_{y \in Y} y = \xi_1(\boldsymbol{u}) \tag{14}$$

$$\sum_{x \in a} x^{\sigma+1} = \sum_{x \in \alpha} x^{\sigma+1} + \sum_{y \in Y} y^{\sigma+1} + \left(\sum_{y \in Y} y\right)^{\sigma+1} = \xi_2(\boldsymbol{u}). \tag{15}$$

Define $\boldsymbol{s}(\boldsymbol{u}) = (\xi_0, \xi_1, \xi_2)$, and let $\boldsymbol{l} = \chi_{T_1}^{i;1}(a) = (l_1, l_2, \cdots, l_i)$. Then we can rewrite (13)–(15) in the following way:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ T_1^{-1}(1) & T_1^{-1}(2) & \cdots & T_1^{-1}(i) \\ [T_1^{-1}(1)]^{\sigma+1} & [T_1^{-1}(2)]^{\sigma+1} & \cdots & [T_1^{-1}(i)]^{\sigma+1} \end{pmatrix} \cdot \boldsymbol{l}^T = \boldsymbol{s}(\boldsymbol{u})^T. \tag{16}$$

Clearly, (16) always has a solution (since $\boldsymbol{u}$ is a future projection of at least one codeword) and $|\Xi_i(\boldsymbol{u})|$ is the total number of solutions for (16). However, (16) defines a binary coset of $\mathcal{L}_i$ in $[\mathrm{GF}(2^m)]^i$, and, therefore, the total number of solutions for this equation is $|\mathcal{L}_i|$, regardless of the choice of $\boldsymbol{u}$. □

We now apply the above results in order to derive an expression for the trellis complexity of the Preparata codes. Let $\delta_{i-}(s)$ be the number of length-i paths entering a state $s \in S_i$ of the biproper trellis representation of $\mathcal{P}(T_1, T_2, \sigma)$. Since the trellis is proper, it follows that

$$\sum_{s \in S_i} \delta_{i-}(s) = |\Pi_{i-}[\mathcal{P}(T_1, T_2, \sigma)]|.$$

Yet, from Lemma 3 and Proposition 1 we conclude that for $0 < i \leq n/2$, $\delta_{i-}(s)$ is not dependent on the choice of $s \in S_i$, and is equal to $|\mathcal{L}_i|$. Thus

$$|S_i| = \frac{|\Pi_{i-}[\mathcal{P}(T_1, T_2, \sigma)]|}{|\mathcal{L}_i|}, \qquad 0 < i \leq n/2. \tag{17}$$

This expression can be simplified by observing that $\Pi_{n/2-}[\mathcal{P}(T_1, T_2, \sigma)]$ consists of all even weight length-$n/2$ vectors. Therefore,

$$|\Pi_{i-}[\mathcal{P}(T_1, T_2, \sigma)]| = \begin{cases} 2^i, & 1 \leq i \leq n/2 - 1 \\ 2^{n/2-1}, & i = n/2 \end{cases}$$

regardless of the choice of T_1 and T_2, and (17) reads

$$|S_i| = \begin{cases} 2^i / |\mathcal{L}_i| & 1 \leq i \leq n/2 - 1 \\ 2^{n/2-1} / |\mathcal{L}|, & i = n/2. \end{cases} \tag{18}$$

Clearly, when $\sigma = 2$ the linear code $\mathcal{L}$ is the extended primitive double-error-correcting BCH code, $\mathcal{B}^{\mathrm{ext}}(2, m)$, of length 2^m. As mentioned before, $\mathcal{P}(T_1, T_2, 2)$ is the "usual" Preparata code, so this choice of σ is of special interest. Let $G(T_1, T_2)$ be the unique biproper trellis diagram of $\mathcal{P}(T_1, T_2, 2)$, and define s_i as the state complexity of $G(T_1, T_2)$ at depth i.

Theorem 4: There exists a choice of T_1 and T_2 for which

$$s_i = \begin{cases} i - k_i[\mathcal{B}^{\mathrm{ext}}(2, m)], & 1 \leq i \leq n/2 - 1 \\ 2m, & i = n/2 \\ n - i - k_{n-i}[\mathcal{B}^{\mathrm{ext}}(2, m)], & n/2 + 1 \leq i < n. \end{cases} \tag{19}$$

where $k_i(\mathcal{C})$ is the ith entry of the DLP of the linear code $\mathcal{C}$. The above profile may not be achieved simultaneously for all indices, that is, a different choice of T_1 and T_2 may be required for different choices of i. For each $i \in \{1, 2, \cdots, n-1\}$, the value of s_i from (19) is minimum over all choices of T_1 and T_2.

Proof: The part of (19) regarding $1 \leq i \leq n/2 - 1$ follows directly from (18) and the definition of the DLP: T_1 is chosen in a way that the support of the subcode of $\mathcal{B}^{\mathrm{ext}}(2, m)$ with support size $\leq i$ and maximum dimension will be in $\{1, 2, \cdots, i\}$. $\mathcal{L}_i$ is then obtained from this subcode by deleting the last (all-zero) $n - i$ positions. Since $k_i(\mathcal{C})$ ($\mathcal{C}$ is a linear code) is the maximum dimension of a subcode of $\mathcal{C}$ with support size i, it is clear that the value of s_i from (19) is the minimum value over all choices of T_1 and T_2. The term of (19) concerning $i = n/2$ follows from the fact that $k[\mathcal{B}^{\mathrm{ext}}(2, m)] = 2^m - 1 - 2m$ [17, Ch. 9].

A similar method can be used to prove the part regarding $n/2 + 1 \leq i < n$. □

We say that a length-l linear code, $\mathcal{C}$, satisfies the *one-way chain condition* iff there exists a coordinate ordering under which, for each $i \in \{1, 2, \cdots, l-1\}$, the dimension of $\mathcal{C}_i$ equals $k_i(\mathcal{C})$. Notice that the profile of (19) is achieved simultaneously iff $\mathcal{B}^{\mathrm{ext}}(2, m)$ satisfies the one-way chain condition.

Example 1: We calculate (19) for $\mathcal{P}(T_1, T_2, 2)$ when $m = 5$ (In the notation of [17] this code is referred to as $\mathcal{P}(6)$). From [7], where the complete GHW [24] of the nonextended $\mathcal{B}(2, m)$ is given for $m = 5$, we find that the DLP of this code is

i:	0–4	5–7	$8, 9$	$10, 11$	12	$13, 14$	15	16	17	18
k_i:	0	1	2	3	4	5	6	7	8	9

i:	$19, 20$	21	22	23	24	25	26	27	28	29	30	31
k_i:	10	11	12	13	14	15	16	17	18	19	20	21

where k_i stands for $k_i[\mathcal{B}(2,5)]$. Since $k_i(\mathcal{C}^{\text{ext}}) \geq k_{i-1}(\mathcal{C})$ ($\mathcal{C}$ is any linear code), we can obtain an upper bound on the values of (19) by replacing $k_i(\mathcal{C}^{\text{ext}})$ with $k_{i-1}(\mathcal{C})$.

i:	1	2	3	4	$5,6$	7	$8,9$	$10,11$	12–14	15–20	21–31
s_i:	1	2	3	4	5	6	7	8	9	10	11

and $s_{32} = 10$. The values of s_i for $33 \leq i < 64$ are obtained by replacing each entry in the "i" row above with $64 - i$, and leaving the "s_i" row unchanged. Therefore, the achievable state complexity at each index in the range $\{0, \cdots, n\}$ is not more than 11. This value is not an upper bound on $s_{\max}$ for this code, since the above profile may not be achieved at all indices simultaneously.

However, it is interesting to compare this number with $s_{\max}$ of the $[64, 51, 6]$ extended double-error-correcting BCH code, since the latter is a linear code of the same length and minimum distance as the discussed Preparata code and with half of its codewords. From [16] we obtain that $s_{\max}$ of the $[64, 51, 6]$ BCH code is 12, that is, one less than the *Wolf bound* [25], $s_{\max} \leq \min\{k, n-k\}$. If $s_{\max}$ of the examined Preparata code is indeed 11, then it is also one less than a "Wolf bound" for this code, obtained when replacing k with the base-2 logarithm of the code's cardinality (even though such a bound for high-rate nonlinear codes is not known to the authors).

The above suggests that in such a case this Preparata code is superior to the corresponding BCH code for the purpose of soft decision decoding: For the same length, it has a higher rate and the same minimum distance along with a smaller trellis complexity. There are two restrictions on the last statement. First, in order to complete the comparison between the error-correction performance of these codes (when a maximum-likelihood soft-decision decoder is employed), the complete distance distributions are required. Second, $s_{\max}$ is not necessarily an accurate measure of the Viterbi decoding algorithm complexity. We conjecture that in fact $s_{\max} = 11$ for this Preparata code.

In [19] Reuven and Be'ery introduced the *conditional entropy/length profile* (conditional ELP) of a block code. We hereby briefly repeat the definition. Let $\mathcal{C}$ be an (n, M, d) code. Regard $\mathcal{C}$ as the sample set of a uniformly distributed random vector X. Let J be a subset of $I = \{1, 2, \cdots, n\}$ and denote the complementary set of J in I as $I - J$. Define X_J to be the random vector obtained when projecting X onto the set of coordinates defined by J. The ith index of the conditional ELP $(0 \leq i \leq n)$, $h_i(\mathcal{C})$, is the maximum value that $H(X_J \mid X_{I-J})$ attains when going through all possible choices of J: $|J| = i$ (for further details the reader is referred to [19]). Since we found that for the discussed set of permutations $|\Xi_i(\boldsymbol{u})|$ does not depend on the choice of $\boldsymbol{u}$, and is equal to $|\mathcal{L}_i|$, we have the following proposition.

Proposition 5: For $1 \leq i \leq n/2$

$$h_i[\mathcal{P}(T_1, T_2, 2)] \geq k_i[\mathcal{B}^{\text{ext}}(2, m)].$$

B. Goethals Codes

Let $G'(T_1, T_2)$ be the unique biproper trellis diagram of $\mathcal{G}(T_1, T_2, 3, 5)$, and define s'_i as the state complexity of $G'(T_1, T_2)$ at depth i. Using the same methods as the ones used for the Preparata codes, we obtain the following theorem.

Theorem 6: There exists a choice of T_1 and T_2 for which

$$s'_i = \begin{cases} i - k_i[\mathcal{B}^{\text{ext}}(3,m)], & 1 \leq i \leq n/2 - 1 \\ 3m, & i = n/2 \\ n - i - k_{n-i}[\mathcal{B}^{\text{ext}}(3,m)], & n/2 + 1 \leq i < n, \end{cases} \tag{20}$$

where $\mathcal{B}^{\text{ext}}(3, m)$ is the primitive triple-error-correcting BCH code. The above profile may not be achieved simultaneously for all indices, that is, a different choice of T_1 and T_2 may be required for different choices of i. For each $i \in \{1, 2, \cdots, n-1\}$, the value of s'_i from (20) is minimum over all choices of T_1 and T_2.

Example 2: We examine the state complexity profile of $\mathcal{G}(T_1, T_2, 3, 5)$ with $m = 7$. This code consists of 2^{233} codewords, that is, four times the size of the $[256, 231, 8]$ comparable $\mathcal{B}^{\text{ext}}(3, 8)$ code. In order to calculate (20) in this case, the DLP of the $[128, 106, 8]$ $\mathcal{B}^{\text{ext}}(3, 7)$ is required. An upper bound on the first five entries of the GHW hierarchy of $\mathcal{B}^{\text{ext}}(3, 7)$ is obtained by adding 1 to the values from [11], corresponding to the nonextended code. The upper bound for the remaining indices is obtained from [3], [2]:

k:	6	7	8	9	10	11	12	13	14	15	16	17	18
d_k:	20	22	23	24	26	27	28	29	30	31	32	36	38

k:	19	20	21	22	$\cdots$	42	43	44	45	$\cdots$	105	106
d_k	39	40	42	43	$\cdots$	63	64	66	67	$\cdots$	127	128

The corresponding values of the lower bound on the DLP of the code are

i:	0–7	8–11	$12,13$	14	15	16–19	$20,21$	22	23
k_i:	0	1	2	3	4	5	6	7	8

i:	$24,25$	26	27	28	29	30	31	32–35	$36,37$	38
k_i:	9	10	11	12	13	14	15	16	17	18

i:	39	$40,41$	42	43	44	$\cdots$	62	63	$64,65$
k_i:	19	20	21	22	23	$\cdots$	41	42	43

i:	66	67	$\cdots$	127	128
k_i:	44	45	$\cdots$	105	106

Substituting the above DLP profile in (20) yields the following upper bound on the achievable state complexity profile:

i:	1	2	3	4	5	6	$7,8$	9	10	$11,12$	13–16	17	18
s_i:	1	2	3	4	5	6	7	8	9	10	11	12	13

i:	$19,20$	21–24	25–32	33	34	$35,36$	37–40	41–64
s_i:	14	15	16	17	18	19	20	21

i:	65–127
s_i:	22

and $s_{128} = 21$. It is of interest to compare the maximum value of the above profile to the parameter $s_{\max}$ of the $[256, 231, 8]$ BCH code, which is no more than 24 [3], that is, one less than the Wolf bound. It seems that this is in fact $s_{\max}$ for this BCH code [2]. As in Example 1, If $s_{\max} = 22$ for the examined Goethals code, it is also one less than a "Wolf bound" for this code. Again, in such a case, it suggests that this Goethals code is superior to the corresponding BCH code for the purpose of soft decision decoding (with the restrictions given in Example 1).

Example 3: The values of (20) are calculated for $\mathcal{G}(T_1, T_2, 3, 5)$ with $m = 5$ (a $(64, 2^{47}, 8)$ code). Note that in this case $\mathcal{B}^{\text{ext}}(3, m)$ is the $[32, 16, 8]$ Reed–Muller code, $\text{RM}(2, 5)$. The exact GHW hierarchy of the code is derived using the results from [24]. The corresponding DLP of $\mathcal{B}^{\text{ext}}(3, m)$ is

i:	0–7	8–11	$12,13$	14	15	16–19	$20,21$	22	23
k_i:	0	1	2	3	4	5	6	7	8

i:	$24,25$	26	27	28	29	30	31	32
k_i:	9	10	11	12	13	14	15	16

Substituting these values in (20) we obtain the following upper bound on the achievable state complexity of the relevant Goethals code:

i:	1	2	3	4	5	6	7, 8	9	10	11, 12	13–16	17	18
s_i:	1	2	3	4	5	6	7	8	9	10	11	12	13

i:	19, 20	21–24	25–31
s_i:	14	15	16

and $s_{32} = 15$. Notice that in this case (20) is achieved at all indices simultaneously, since all Reed–Muller codes satisfy the one-way chain condition [13]. Furthermore, it is known which permutation (which choice of T_1 and T_2) is required to achieve the above profile: For each $i \in \{1, 2, \cdots, 32\}$,

$$T_1^{-1}(i) = \sum_{j=0}^{4} v_{j+1}\alpha^j$$

where α is a primitive element in $\mathrm{GF}(2^5)$, and $\boldsymbol{v} = (v_1, v_2, v_3, v_4, v_5)$ is the binary expansion of $i - 1$ [13]. T_2 is determined in a similar way (with the exception that $\boldsymbol{v}$ is the binary expansion of $32 - i$). Again, the maximum value that the profile attains is one less than the "Wolf bound." Note that this value is indeed an upper bound on $s_{\max}$ of the discussed Goethals code. From [3], [2] we obtain that the parameter $s_{\max}$ of the comparable $[64, 45, 8]$ BCH code is at most 14 (five less than the Wolf bound). So for this case it appears that the decoding complexity of the BCH code is smaller than the one of the Goethals code.

Finally, we have the following proposition regarding the conditional ELP of the Goethals codes.

Proposition 7 For $1 \leq i \leq n/2$,

$$h_i[\mathcal{G}(T_1, T_2, 3, 5)] \geq k_i[\mathcal{B}^{\text{ext}}(3, m)].$$

V. The Twisted Squaring Construction of the Preparata and Goethals Codes

In this section it is shown that under all bit orders for which we proved that the codes are rectangular, both the Preparata and Goethals codes admit a twisted squaring construction. Note that a code admitting a twisted squaring construction can be decoded in the way described in [8, p. 1158].

Let S be a finite set, and let S/U denote the partition of S into M disjoint subsets $U_0, U_1, \cdots, U_{M-1}$, where $U_i \subset S$ for $i \in \{0, 1, \cdots, M-1\}$. The twisted squaring construction denoted by $\|S/U\|^2$ is defined as the union of M sets, $U_i \times U_{j_i}$ such that i and j_i run through $0, 1, \cdots, M-1$ [3].

In [8] Forney gave a twisted squaring construction for the Nordstrom–Robinson code $\mathcal{N}_{16}$. Recall that $\mathcal{N}_{16}$ is, in fact, $\mathcal{P}(T_1, T_2, 2)$ with $m = 3$ ($\mathcal{P}(4)$ in the notation of [17]). The following proposition extends Forney's result.

Proposition 8: $\mathcal{P}(T_1, T_2, 2) = \|S/U\|^2$, where S is the space of all binary 2^m-tuples of even weight, and S/U is the partition of S into the extended primitive double-error-correcting BCH code and its cosets in S.

Proof: It is clear from the proof of Lemma 3 that $\Xi_{\frac{n}{2}}(\boldsymbol{u})$ is the binary coset of $\mathcal{B}^{\text{ext}}(2, m)$ defined by the syndrome $(0, \xi_1, \xi_2)$, where

$$\xi_1 = \sum_{y \in Y} y$$

$$\xi_2 = \left(\sum_{y \in Y} y\right)^3 + \sum_{y \in Y} y^3$$

and $\boldsymbol{u} = \chi_{T_2}(Y)$. Denote this coset as $C_{T_1}(\xi_1, \xi_2)$. Each vector in the above coset can be concatenated with any $\boldsymbol{u}$ of even weight for which

$$\sum_{y \in Y} y = \xi_1$$

and

$$\sum_{y \in Y} y^3 = \xi_2 + \xi_1^3$$

to create a codeword of $\mathcal{P}(T_1, T_2, 2)$.

Let A be the set of syndromes corresponding to all the cosets of $\mathcal{B}^{\text{ext}}(2, m)$ in the space of all even weight 2^m-tuples. Thus we can write

$$\mathcal{P}(T_1, T_2, 2) = \bigcup_{(0, \xi_1, \xi_2) \in A} C_{T_1}(\xi_1, \xi_2) \times C_{T_2}\big(\xi_1, \xi_2 + \xi_1^3\big). \quad \square$$

Note that for a bijection T: $\mathrm{GF}(2^m) \rightarrow I$, $C_T(\xi_1, \xi_2)$ and $C_T(\xi_1, \xi_2 + \xi_1^3)$ are in the same coset of the extended Hamming code in the space of all even weight 2^m-tuples. This is due to the fact that the syndrome of $\boldsymbol{u} + \boldsymbol{v}$, $\boldsymbol{u} \in C_T(\xi_1, \xi_2)$, $\boldsymbol{v} \in C_T(\xi_1, \xi_2 + \xi_1^3)$ is $(0, 0, \xi_1^3)$.

Therefore, the twisted squaring construction for $\mathcal{P}(T_1, T_2, 2)$ could be partitioned into clusters, each of them consisting of $\|S'/U'\|^2$, where S' is a coset of the extended Hamming code, and S'/U' is the partition of S' into cosets of $\mathcal{B}^{\text{ext}}(2, m)$. In other words, the twisted squaring construction for the Preparata code corresponds to the two-level partition chain $\mathcal{E}(m)/\mathcal{H}^{\text{ext}}(m)/\mathcal{B}^{\text{ext}}(2, m)$ ($\mathcal{E}(m)$ and $\mathcal{H}^{\text{ext}}(m)$ are the length-2^m even-weight code and extended Hamming code, respectively).

Recall that for $m = 3$ and for a correct "twist," the *cubing construction* obtained from the above two-level partition gives the $[24, 12, 8]$ binary Golay code [8]. It can be verified that for odd $m \geq 5$ the cubing construction built from this partition gives a $(3 \cdot 2^m, 2^{3 \cdot (2^m - m - 1)}, 6)$ code (no matter which "twisting" is chosen): The minimum distance is obtained from the bounds of [8], and the cardinality is

$$|\mathcal{E}(m)/\mathcal{H}^{\text{ext}}(m)| \cdot |\mathcal{H}^{\text{ext}}(m)/\mathcal{B}^{\text{ext}}(2, m)|^2 \cdot |\mathcal{B}^{\text{ext}}(2, m)|^3.$$

This construction bears a close resemblance to the one from [10], and has the same parameters. For $m = 5$ the described construction gives a $(96, 2^{78}, 6)$ code. From [4] it follows that the maximum possible minimum distance of a linear code with the above length and cardinality is 6 or 7. So for this case the described cubing construction gives a good code.

Arguments similar to the ones from the proof of Proposition 8 establish the following proposition.

Proposition 9: $\mathcal{G}(T_1, T_2, 3, 5) = \|S/U\|^2$, where S is the space of all binary 2^m-tuples of even weight, and S/U is the partition of S into the extended primitive triple-error-correcting BCH code and its cosets in S.

As before, the twisted squaring construction for the Goethals code $\mathcal{G}(T_1, T_2, 3, 5)$ can be divided into smaller twisted squaring constructions, so that it corresponds to the two-level partition chain $\mathcal{E}(m)/\mathcal{H}^{\text{ext}}(m)/\mathcal{B}^{\text{ext}}(3, m)$.

VI. Conclusion

Using a convenient representation of the Preparata and Goethals codes [1], we examined the trellis complexity of these codes. At least for a given set of permutations, it was proved that both families of codes are rectangular. Upper bounds on the bit-level state complexity of the length-2^{m+1} (m odd) Preparata and Goethals codes were determined from the DLP of the double- and triple-error-correcting BCH codes of length 2^m, respectively. The given bounds are not necessarily achieved at all indices simultaneously, that is, different coordinate orderings may be required to achieve the bounds at different indices. Thus an upper bound on $s_{\max}$ cannot be determined from the bound on the state complexity profile.

However, the results of Example 1 suggest that $s_{\max}$ of the length-64 Preparata code is one less than that of the double-error-correcting BCH code of the same length. This hints at the superiority of this Preparata code over the corresponding BCH code for the purpose of soft-decision decoding.

Similarly, the maximum value of the upper bound on the state complexity of the length-256 Goethals code is smaller by two than $s_{\max}$ of the length-256 triple-error-correcting BCH code (Example 2). Again, it may imply that this Goethals code is a better choice than the triple-error-correcting BCH code of the same length for soft-decision decoding.

The parameter $s_{\max}$ of the length-64 Goethals code (Example 3) appears to be *larger* by two than that of the corresponding length-64 BCH code. This is due to the fact that $s_{\max}$ of this BCH code is no longer one less than the Wolf bound, while the maximum value of our state complexity profile is one less than a "Wolf bound" for the relevant Preparata code (as in Example 2).

Generalizing a result of Forney [8] regarding the Nordstrom–Robinson code (which is $\mathcal{P}(T_1, T_2, 2)$ when $m = 3$), a twisted squaring construction was given for all Preparata codes. Similarly, a twisted squaring construction was given for the Goethals codes.

Two main questions remain unsolved.

1) Are there other coordinate orderings for which the Preparata and Goethals codes are rectangular?
2) Is it possible to find coordinate orderings of the Preparata and Goethals codes that will induce a lower state complexity profile than the one from the described upper bound?

Acknowledgment

The authors wish to thank Yuval Berger for helpful discussions, and for providing computer search results for Examples 2 and 3. The authors also wish to thank Ilan Reuven for improving the final version of Theorem 4 and for helpful discussions.

References

[1] R. D. Baker, J. H. Van Lint, and R. M. Wilson, "On the Preparata and Goethals codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 342–345, May 1983.

[2] Y. Berger, personal communications, 1997.

[3] Y. Berger and Y. Be'ery, "The twisted squaring construction, trellis complexity, and generalized weights of BCH and QR codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1817–1827, Nov. 1996.

[4] 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.

[5] C. Carlet, "A simple description of Kerdock codes," in *Coding Theory and Applications, Lecture Notes in Computer Science*, vol. 388, G. Cohen and J. Wolfmann, Eds. Berlin, Germany: Springer-Verlag, 1989, pp. 202–208.

[6] ——, "On Z_4-duality," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1487–1494, Sept. 1995.

[7] G. Cohen, L. Huguet, and G. Zemor, "Bounds on generalized weights," in *Algebraic Coding, Lecture Notes in Computer Science*, vol. 781, G. Cohen, S. Litsyn, A. Lobstein, and G. Zemor, Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 270–277.

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

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

[10] M. P. C. Fossorier and S. Lin, "Some decomposable codes: The $|a+x|b+x|a+b+x|$ construction," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1663–1667, Sept. 1997.

[11] G. van der Geer and M. van der Vlugt, "Generalized Hamming weights of BCH(3) revisited," *IEEE Trans. Inform. Theory*, vol. 41, pp. 300–301, Jan. 1995.

[12] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–319, Mar. 1994.

[13] 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.

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

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

[16] A. Lafourcade and A. Vardy, "Lower bounds on trellis complexity of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1938–1954, Nov. 1995.

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

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

[19] I. Reuven and Y. Be'ery, "Entropy/length profiles, bounds on the minimal covering of bipartite graphs, and trellis complexity of nonlinear codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 590–598, Mar. 1998.

[20] Y. Shany, I. Reuven, and Y. Be'ery, "On the trellis representation of the Delsarte-Goethals codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1547–1554, July 1998.

[21] V. R. Sidorenko, "The Euler characteristic of the minimal code trellis is maximum," *Probl. Inform. Transm.*, vol. 33, no. 1, pp. 87–93, Mar. 1997.

[22] V. Sidorenko, I. Martin, and B. Honary, "On rectangularity of nonlinear block codes," preprint.

[23] A. Vardy and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2027–2034, Nov. 1996.

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

[25] 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.