

*Corollary 2:* The generalized Delsarte–Goethals code defined by Definition 6, relation (4) is a

$$(2^{m+k-1}, 2^K, d \geq 2^{m+k-2} - 2^{m/2+k-2}(\Delta - 1))$$

(nonlinear) binary code, where

$$K = k(m+1) + m \sum_{j=1}^{k-1} ((k-j)|I_j|)$$

and

$$\Delta = \max(2^{k-1}, \max\{(2i+1)2^{k-1-j}; j = 1, \dots, k-1; i \in I_j\}).$$

Notice that the generalized Kerdock  $\mathbf{Z}_8$ -linear code is included in a generalized Delsarte–Goethals code for which the bound given by (7) is the same: take  $k = 3$ ; the functions  $ax$  and  $ax + 4bx^3$  have same weighted degree 4; thus the generalized Kerdock code is a

$$(2^{m+2}, 2^{3m+3}, d \geq 2^{m+1} - 3 \cdot 2^{(m+2)/2})$$

(nonlinear) code and the generalized Delsarte–Goethals code corresponding to  $\text{Tr}_3(ax + 4bx^3) + b$  is a

$$(2^{m+2}, 2^{4m+3}, d \geq 2^{m+1} - 3 \cdot 2^{(m+2)/2})$$

(nonlinear) code. Notice that the function  $ax + 4bx^3 + 4cx^5$  has weighted degree 5; therefore, the generalized Delsarte–Goethals code corresponding to  $\text{Tr}_3(ax + 4bx^3 + 4cx^5) + b$  is a

$$(2^{m+2}, 2^{5m+3}, d \geq 2^{m+1} - 2^{(m+6)/2})$$

(nonlinear) code. To make a comparison with the parameters of known codes of same length and comparable cardinalities, we may consider, for instance, the dual of the extended 4-error (respectively, 5-error) correcting Bose–Chaudhuri–Hocquengham (BCH) code, that is a

$$[2^{m+2}, 4m+9, d \geq 2^{m+1} - 3 \cdot 2^{(m+2)/2}]$$

(respectively,  $[2^{m+2}, 5m+11, d \geq 2^{m+1} - 2^{(m+6)/2}]$ ) linear code.

## V. CONCLUSION

A generalization of the Gray map has allowed us to introduce new codes: the generalized Kerdock and Delsarte–Goethals codes. We see three directions for further research:

- an improvement of the bounds given by Corollaries 1 and 2 could imply that the generalized Kerdock codes and/or the generalized Delsarte–Goethals codes have better parameters than the duals of the BCH codes;
- other  $\mathbf{Z}_{2^k}$ -linear codes may be better than those introduced in the present correspondence;
- other generalizations of the Gray map are to be investigated, at least for  $k > 3$ .

## REFERENCES

- [1] A. R. Calderbank and N. J. A. Sloane, "Modular and  $p$ -adic cyclic codes," *Des., Codes, Cryptogr.*, vol. 6, pp. 21–35, 1995.
- [2] A. R. Calderbank, W.-C. W. Li, and B. Poonen, "A 2-adic approach to the analysis of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 977–986, May 1997.
- [3] C. Carlet, "On  $\mathbf{Z}_4$ -duality," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1487–1495, 1995.
- [4] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The  $\mathbf{Z}_4$ -linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301–320, Jan. 1994.
- [5] T. Helleseth, P. V. Kumar, O. Moreno, and A. G. Shanbhag, "Improved estimates via exponential sums for the minimum distance of  $\mathbf{Z}_4$ -linear trace codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1212–1216, 1996.
- [6] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inform. Theory*, vol. 41, pp. 456–468, Mar. 1995.
- [7] B. R. MacDonald, *Finite Rings With Identity*. New York: Dekker, 1974.
- [8] A. A. Nechaev, "The Kerdock code in a cyclic form," *Discr. Math. Appl.*, vol. 1, pp. 123–139, 1989.
- [9] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

## On the Trellis Representation of the Delsarte–Goethals Codes

Yaron Shany, Ilan Reuven, *Student Member, IEEE*,  
and Yair Be'ery, *Member, IEEE*

**Abstract**—In this correspondence, the trellis representation of the Kerdock and Delsarte–Goethals codes is addressed. It is shown that the states of a trellis representation of  $\mathcal{DG}(m, \delta)$  under any bit-order are either strict-sense nonmerging or strict-sense nonexpanding, except, maybe, at indices within the code's distance set. For  $\delta \geq 3$  and for  $m \geq 6$ , the state complexity,  $s_{\max}[\mathcal{DG}(m, \delta)]$ , is found. For all values of  $m$  and  $\delta$ , a formula for the number of states and branches of the biproper trellis diagram of  $\mathcal{DG}(m, \delta)$  is given for some of the indices, and upper and lower bounds are given for the remaining indices. The formula and the bounds refer to the Delsarte–Goethals codes when arranged in the standard bit-order.

**Index Terms**—Biproper trellis, Delsarte–Goethals code, Kerdock code, rectangular codes, trellis complexity.

## I. INTRODUCTION

We consider the structure and complexity of the trellis diagram of the Kerdock and Delsarte–Goethals codes. For even  $m \geq 4$  and for  $2 \leq \delta \leq m/2$  the Delsarte–Goethals code  $\mathcal{DG}(m, \delta)$  is a nonlinear code which contains more codewords than any known linear code with the same length and minimum distance. The Kerdock code,  $\mathcal{K}(m)$ , is a special case of the Delsarte–Goethals code obtained when  $\delta = m/2$ . For the particular situation where  $m = 4$  and  $\delta = 2$  (the Nordstrom–Robinson code), the structure and complexity of the trellis diagram of the code were studied in papers such as [2], [9], and [13].

The main conceptions regarding the construction of a trellis diagram of nonlinear block codes were investigated in several papers, such as [2], [7]–[9], [12], and [13]. Kschischang and Sorokine [8] showed that for an arbitrary nonlinear code in a given bit-order, there need not necessarily exist a trellis diagram which minimizes the vertex count at all indices simultaneously. The sufficient conditions

Manuscript received June 29, 1997; revised December 15, 1997. The material in this correspondence was presented in part at the 3rd Mediterranean Workshop on Coding and Information Integrity, Ein Boqeq, Israel, October 27–29, 1997.

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).

Publisher Item Identifier S 0018-9448(98)03481-6.

that a nonlinear code has to satisfy in order to admit such a trellis diagram are examined in [7], [8], and [14]. A code satisfying the above conditions is called *rectangular* (or *separable* in [14]). For a rectangular code in a given bit-order, there exists a unique *biproper* trellis diagram which minimizes both the vertex count and the edge count at all indices simultaneously [7]. It was shown in [15] that the biproper trellis diagram of a rectangular code (in a given bit-order) also minimizes the total number of additions and comparisons required to implement the Viterbi decoding algorithm.

It is well known that the minimum vertex count at a specific index of a trellis diagram of a nonlinear code  $C$  depends on the order of the coordinates in  $C$ . A lower bound on the bit-level vertex count of a trellis diagram of a nonlinear code (for any bit-order) was first derived in the work of Muder [12], in which the only property of the code being used is its minimum distance. Following the bounds derived by Forney [3] for trellis complexity of linear block codes, Lafourcade and Vardy [9] presented a bound on the trellis complexity of nonlinear block codes which is essentially tighter than the one in [12] since it makes use of the code's structure. Reuven and Be'ery [13] introduced an even tighter bound by a further use of the code's structure.

The Delsarte–Goethals codes consist of cosets of the first-order Reed–Muller code,  $RM(1, m)$ , in the second-order Reed–Muller code,  $RM(2, m)$ . The trellis diagram of Reed–Muller codes was examined among others in [1], [2], [5], [6], and [10].

In this correspondence, we examine the trellis representation of the Delsarte–Goethals codes. We derive the maximal vertex count of the biproper trellis representation of  $\mathcal{DG}(m, \delta)$  for the bit-order that minimizes this quantity. The structure of any trellis representation of the Delsarte–Goethals codes is addressed for any given bit-order. Finally, a partial formula is derived for the state and branch complexity of the trellis diagram of the Delsarte–Goethals codes when arranged in the standard bit-order.

The correspondence is organized as follows. In Section II we present the terms and definitions relevant for the succeeding sections. In Section III we use the distance set of the Delsarte–Goethals codes in order to derive the maximal vertex count of the biproper trellis representation of  $\mathcal{DG}(m, \delta)$  for the bit-order that minimizes this quantity. Several properties of the structure of any trellis diagram of the Delsarte–Goethals codes are derived.

In Section IV, motivated by the results of Section III and the well-known optimality of the *standard bit-order* for constructing trellis diagrams for the Reed–Muller codes [5], we examine the bit-level state complexity of the trellis diagram of the Delsarte–Goethals codes when arranged in this specific bit-order. A formula for the (partial) bit-level complexity of the biproper trellis representation of  $\mathcal{DG}(m, \delta)$  is derived. The formula applies to an increasing number of indices as the value of  $\delta$  increases towards  $m/2$  (corresponding to the Kerdock code). We observe that finding the vertex count at the indices for which the above formula is irrelevant is a subproblem of deriving any of the bounds from [9] or [13]. Therefore, we use properties of  $RM(1, m)$  and  $RM(2, m)$  to derive upper and lower bounds on the vertex count of the trellis diagram of the Delsarte–Goethals codes at these indices.

## II. PRELIMINARIES

This section includes several definitions and notations that will be used throughout the following sections. A trellis diagram is an edge-labeled directed graph  $T = (V, A, E)$ , where  $V$  is a set of *vertices* (also referred to as *states*),  $A$  is a finite alphabet, and  $E$  is the set of ordered triples  $(v, v', \alpha)$ , where  $v, v' \in V$  and  $\alpha \in A$ . The ordered triples in  $E$  are referred to as *edges* (or *branches*). Moreover, the set of vertices  $V$  can be expressed as the union of  $n + 1$  disjoint subsets,  $V = \bigcup_{i=0}^n V_i$ , such that if  $(v, v', \alpha) \in E$  then  $v \in V_i$  and

$v' \in V_{i+1}$  for some  $i \in \{0, 1, \dots, n-1\}$ . The set  $V_i$ ,  $0 \leq i \leq n$ , is referred to as the set of vertices at index  $i$ . The cardinality of the set  $V_i$  is called the *vertex count* of the trellis diagram at index  $i$ . For  $i \in \{1, 2, \dots, n\}$  let  $E_i$  be the set of edges connecting vertices of  $V_{i-1}$  to those of  $V_i$ . The cardinality of the set  $E_i$  is referred to as the *edge count* of the trellis diagram at index  $i$ . For codes over a field  $A = GF(q)$ , the base- $q$  logarithm of the vertex count at an index  $i \in \{0, 1, \dots, n\}$  is called the *state complexity* of the trellis diagram at index  $i$ . Also, the *branch complexity* of the trellis diagram at index  $i \in \{1, 2, \dots, n\}$  is the base- $q$  logarithm of the edge count at index  $i$ . Any path from  $V_0$  to  $V_n$  defines an  $n$ -tuple  $(\alpha_1, \alpha_2, \dots, \alpha_n)$ , where  $\alpha_i \in A$  for  $1 \leq i \leq n$  is the label of the edge connecting a vertex at index  $i-1$  to a vertex at index  $i$ .

We will confine our scope to trellis diagrams satisfying the following conditions.

- 1) The trellis has a single initial vertex and a single final vertex:  $|V_0| = |V_n| = 1$ .
- 2) Every vertex of  $T$  lies on some length- $n$  path.

A trellis  $T$  is called *one-to-one* if no two distinct length- $n$  paths from the initial vertex to the final vertex of  $T$  represent the same  $n$ -tuple. A *proper* trellis is a trellis in which no two distinct length- $i$  paths from the origin correspond to the same  $i$ -tuple for every  $i \in \{1, 2, \dots, n\}$ .

Denote a block code  $C$  over  $A$  with  $M$  codewords of length  $n$  and minimum distance  $d$  as an  $(n, M, d)$  code. A trellis diagram  $T$  is said to be a trellis diagram of  $C$  if and only if the set of  $n$ -tuples corresponding to all the length- $n$  paths from the initial vertex to the final vertex in  $T$  is identical to  $C$ . Since the codes discussed in this correspondence are over  $GF(2)$ , we focus only on the case  $A = GF(2)$ .

Let  $\underline{c} = (c_1, c_2, \dots, c_n)$  be a codeword of  $C$ . For  $i \in \{1, 2, \dots, n\}$  let

$$P_{i-}(\underline{c}) = (c_1, c_2, \dots, c_i)$$

be the *past projection* of the codeword, and for  $i \in \{0, 1, \dots, n-1\}$  let

$$P_{i+}(\underline{c}) = (c_{i+1}, c_{i+2}, \dots, c_n)$$

be the *future projection* of the codeword. Let

$$P_{i-}(C) = \{P_{i-}(\underline{c}) : \underline{c} \in C\}$$

denote the past projection of the code, and let

$$P_{i+}(C) = \{P_{i+}(\underline{c}) : \underline{c} \in C\}$$

denote the future projection of the code at index  $i$ .

The *Cartesian array* for  $C$  at index  $i$  is a representation of the code as a set of points on a rectangular array with  $|P_{i-}(C)| \times |P_{i+}(C)|$  squares, as presented by Kschischang and Sorokine in [8]. The rows of the array correspond to past projections of the code, and the columns are identified with future projections of the code. For  $1 \leq a \leq |P_{i-}(C)|$  let  $P_{i-}^a(C)$  be the past projection corresponding to the  $a$ th row of the array, and for  $1 \leq b \leq |P_{i+}(C)|$  let  $P_{i+}^b(C)$  be the future projection corresponding to the  $b$ th column. A point is placed on the  $(a, b)$  square of the array if and only if  $(P_{i-}^a(C), P_{i+}^b(C)) \in C$ .

For convenience we will sometimes refer to a codeword as a *point*, referring to the point on the Cartesian array which is associated with this codeword. As shown in [8], a set of points (codewords) can pass through a single state of the trellis diagram of the code at index  $i$  only if its points form a *complete rectangle* on the Cartesian array at that index, that is, the set of points is identical to the Cartesian product of its past and future projections. Thus the problem of minimizing

the vertex count of the trellis for a specific index  $i$  is equivalent to finding the minimum number of complete rectangles that cover all the points on the array. The problem with this concept is that minimizing the vertex count at one index might impose an augmentation of the vertex count at another index, as exemplified in [8].

For

$$\underline{a} = (a_1, a_2, \dots, a_l), \quad l \geq 1$$

and for

$$\underline{b} = (b_1, b_2, \dots, b_k), \quad k \geq 1$$

we denote the *concatenation* of  $\underline{a}$  and  $\underline{b}$  as

$$\underline{ab} = (a_1, a_2, \dots, a_l, b_1, b_2, \dots, b_k).$$

A code  $C$  of length  $n > 1$  is said to be *rectangular* [7] if, at each  $i \in \{1, 2, \dots, n-1\}$ ,  $\{\underline{ac}, \underline{ad}, \underline{bc}\} \subset C$  implies  $\underline{bd} \in C$ , for distinct  $\underline{a}, \underline{b} \in P_{i-}(C)$  and distinct  $\underline{c}, \underline{d} \in P_{i+}(C)$ . Schematically,  $C$  is rectangular if for each  $i \in \{1, 2, \dots, n-1\}$  there exists a certain row and column permutation of the corresponding Cartesian array for which it consists of nonoverlapping complete rectangles, none sharing the same row or column. In general, for a given nonlinear code, there need not be a trellis diagram of the code minimizing the vertex count or the edge count at all indices simultaneously. Nevertheless, when a code is rectangular there exists a unique biproper trellis diagram of the code. It has been shown in [15] that this biproper trellis minimizes both the vertex count and the edge count at all indices simultaneously. Also, this trellis minimizes the quantity  $2|E| - |V| + 1$  [15], which is the total number of addition-equivalent operations required to implement the Viterbi decoding algorithm.

There is a one-to-one correspondence between the states of this biproper trellis at an index  $0 < i < n$  and the maximal nonoverlapping rectangles in the Cartesian array of  $C$  at that specific index. When  $C$  is rectangular, the notations  $S_i(C) = |V_i|$  (vertex count),  $s_i(C) = \log_2[S_i(C)]$  (state complexity),  $B_i(C) = |E_i|$  (edge count), and  $b_i(C) = \log_2[B_i(C)]$  (branch complexity) will refer to the unique biproper trellis diagram of  $C$ . For a code which is rectangular under any given bit-order, it is also of interest to define  $S_{\max}(C)$  as the minimum value that  $\max_{0 < i < n} [S_i(\tilde{C})]$  attains when  $\tilde{C}$  varies through all coordinate permutations of  $C$ . In a similar way to the above notations, we denote  $s_{\max}(C) = \log_2[S_{\max}(C)]$ .

As defined by Reuven and Be'ery in [13], we will refer to a state at index  $i$  that has only one length- $i$  path entering it as a *strict-sense nonmerging state*, and to a state at index  $i$  that has only one length- $(n-i)$  path leaving it as a *strict-sense nonexpanding state*. The term "strict sense" in the above definition emphasizes the fact that there is only one *path* entering (or leaving) the state, and not merely one edge entering (or leaving) the state. A state that is strict-sense nonmerging, or strict-sense nonexpanding, or both, will be called a *simple state*. Note that if all the complete rectangles in the Cartesian array at index  $i \in \{1, 2, \dots, n-1\}$  are either rows, or columns, or both, it implies that every  $v \in V_i$  is a simple state. Likewise, we call a state  $v \in V_i$  a *butterfly state* if it has exactly two length- $i$  paths entering it, and exactly two length- $(n-i)$  paths leaving it. Obviously, a nonsimple state that has exactly four codewords passing through it is a butterfly state.

For even  $m \geq 4$  and for  $2 \leq \delta \leq m/2$  the Delsarte and Goethals code [11, Ch. 15],  $\mathcal{DG}(m, \delta)$ , is a

$$(2^m, 2^{(m-1)(m/2-\delta+1)+m+1}, 2^{m-1} - 2^{m-1-\delta})$$

nonlinear subcode of  $\text{RM}(2, m)$  which consists of  $\text{RM}(1, m)$  and  $2^{(m-1)(m/2-\delta+1)} - 1$  cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$ . We denote the minimum distance of this code by

$$d_{\min}^{m, \delta} = 2^{m-1} - 2^{m-\delta-1}.$$

The distance set of  $\mathcal{DG}(m, \delta)$  is

$$D_{m, \delta} = \{0, 2^m\} \cup D'_{m, \delta}$$

where

$$D'_{m, \delta} = \{2^{m-1}, 2^{m-1} \pm 2^{m-h-1} : \delta \leq h \leq m/2\}.$$

We denote

$$d_{\max}^{m, \delta} = 2^{m-1} + 2^{m-\delta-1}$$

which refers to the largest entry in the distance set of  $\mathcal{DG}(m, \delta)$  except for  $2^m$ .

The Kerdock code,  $\mathcal{K}(m)$ , is the special case of  $\mathcal{DG}(m, \delta)$  obtained when  $\delta = m/2$ . This code consists of  $\text{RM}(1, m)$  and  $2^{m-1} - 1$  cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$ .

### III. OBSERVATIONS REGARDING THE TRELLIS STRUCTURE AND COMPLEXITY OF $\mathcal{DG}(m, \delta)$ UNDER ANY BIT-ORDER

Using the distance set of  $\mathcal{DG}(m, \delta)$ ,  $D_{m, \delta}$ , we find

$$S_{\max}[\mathcal{DG}(m, \delta)], \quad \text{for } m \geq 6 \text{ and } \delta \geq 3.$$

We observe that for any bit-order, the states of a trellis diagram of  $\mathcal{DG}(m, \delta)$  at any index  $i \notin D'_{m, \delta}$  are simple. If there exist nonsimple states at an index  $i \in D'_{m, \delta}$ , then they are necessarily butterfly states.

We begin with a slightly modified version of the proof to [14, Theorem 12]. This proof was independently derived before we became aware of [14].

*Theorem 1:* For any bit-order,  $\mathcal{DG}(m, \delta)$ ,  $m \geq 4$ ,  $2 \leq \delta \leq m/2$ , is rectangular and therefore admits a biproper trellis representation.

*Proof:* In order to establish the proof it is sufficient to show that for each  $i \in \{1, 2, \dots, n-1\}$ ,  $\{\underline{ac}, \underline{ad}, \underline{bc}\} \subset \mathcal{DG}(m, \delta)$  implies  $\underline{bd} \in \mathcal{DG}(m, \delta)$ , for distinct  $\underline{a}, \underline{b} \in P_{i-}[\mathcal{DG}(m, \delta)]$  and distinct  $\underline{c}, \underline{d} \in P_{i+}[\mathcal{DG}(m, \delta)]$ . Clearly

$$\text{dist}(\underline{ac}, \underline{bd}) = \text{dist}(\underline{ac}, \underline{bc}) + \text{dist}(\underline{ac}, \underline{ad}) \quad (3.1)$$

where  $\text{dist}(\underline{u}, \underline{v})$  stands for the Hamming distance between the binary vectors  $\underline{u}$  and  $\underline{v}$ . Therefore,

$$\text{dist}(\underline{ac}, \underline{bd}) \geq 2d_{\min}^{m, \delta} \geq 2^m - 2^{m-2} > 2^{m-1} + 2^{m-3} \geq d_{\max}^{m, \delta} \quad (3.2)$$

for all legal values of  $m$  and  $\delta$ . Thus  $\text{dist}(\underline{ac}, \underline{bd}) = 2^m$ , which implies that  $\underline{bd} \in \mathcal{DG}(m, \delta)$  since  $\underline{bd}$  is in the same coset of  $\text{RM}(1, m)$  with  $\underline{ac}$ .  $\square$

Since the Delsarte–Goethals codes admit a biproper trellis representation for any bit-order, it is of interest to address  $S_{\max}[\mathcal{DG}(m, \delta)]$ .

*Proposition 2:* For  $m \geq 6$  and  $\delta \geq 3$

$$S_{\max}[\mathcal{DG}(m, \delta)] = \frac{1}{2} |\mathcal{DG}(m, \delta)| = 2^{(m-1)(m/2-\delta+1)+m}. \quad (3.3)$$

*Proof:* We denote  $d = d_{\min}^{m, \delta}$ , and apply Muder's lower bound [12] at the index  $i = d - 1$ .

$$S_{d-1}[\mathcal{DG}(m, \delta)] \geq \frac{|\mathcal{DG}(m, \delta)|}{A(d-1, d)A(n-d+1, d)} \quad (3.4)$$

where  $A(n, d)$  is the maximum number of codewords of a block code of length  $n$  and minimum distance  $d$  over  $\text{GF}(2)$ . Clearly,  $A(d-1, d) = 1$ . We will use the Plotkin bound in order to upper-bound  $A(n-d+1, d)$ . Indeed, since

$$2d > 2^m - 2^{m-\delta} - (2^{m-1} - 2^{m-1-\delta} - 2^{m-\delta} - 1) = n - d + 1$$

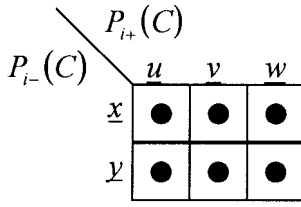


Fig. 1. A complete rectangle with more than four points.

the Plotkin bound is applicable. Hence

$$A(n-d+1, d) \leq 2 \left\lfloor \frac{d}{3d-n-1} \right\rfloor = 2 \left\lfloor 1 + \frac{n+1-2d}{3d-n-1} \right\rfloor. \quad (3.5)$$

By substituting  $n = 2^m$  and  $d = 2^{m-1} - 2^{m-\delta-1}$  into (3.5) it can be verified that  $A(n-d+1, d) \leq 2$  when  $\delta \geq 3$  and  $m \geq 6$ . Therefore, for any bit-order

$$S_{d-1}[\mathcal{D}\mathcal{G}(m, \delta)] \geq \frac{1}{2} |\mathcal{D}\mathcal{G}(m, \delta)| = 2^{(m-1)(m/2-\delta+1)+m}.$$

Conversely, it is known from [1] that there exists a bit-order for which the maximal vertex count of the minimal trellis diagram of RM(1, m) is exactly  $2^m$ . For this specific bit-order we have

$$S_i[\mathcal{D}\mathcal{G}(m, \delta)] \leq 2^{(m-1)(m/2-\delta+1)+m}, \quad i \in \{0, 1, \dots, n\}$$

since  $\mathcal{D}\mathcal{G}(m, \delta)$  consists of  $2^{(m-1)(m/2-\delta+1)}$  cosets of RM(1, m) in RM(2, m). Combining the last two results we establish the proposition.  $\square$

The following proposition concerns the structure of a trellis diagram of the Delsarte–Goethals codes, under any given bit-order.

*Proposition 3:* Under any bit-order, the states of a trellis diagram of  $\mathcal{D}\mathcal{G}(m, \delta)$  are simple states at each  $i \notin D'_{m, \delta}$ . If there exist nonsimple states at an index  $i \in D'_{m, \delta}$ , then these states are necessarily butterfly states.

*Proof:* A nonsimple state at index  $i \in \{1, 2, \dots, n-1\}$  in the trellis diagram of the code implies the existence of three codewords,  $\{\underline{ac}, \underline{ad}, \underline{bc}\} \subset \mathcal{D}\mathcal{G}(m, \delta)$ , for distinct  $a, b \in P_{i-}[\mathcal{D}\mathcal{G}(m, \delta)]$ , and distinct  $c, d \in P_{i+}[\mathcal{D}\mathcal{G}(m, \delta)]$ . We denote  $d_x = \text{dist}(\underline{ac}, \underline{bc})$ , and  $d_y = \text{dist}(\underline{ac}, \underline{ad})$ . From the proof of Theorem 1 we know that  $d_x + d_y = 2^m$ . However, for  $i \notin D'_{m, \delta}$  both  $d_x < i$  and  $d_y < 2^m - i$ , establishing the first part of the proposition. Note that even though the states at these indices are simple, they are not all necessarily the same kind of simple states, that is, there may be a combination of strict-sense nonexpanding states and strict-sense nonmerging states.

It is clear from the distance set of the Delsarte–Goethals codes that the above argument does not hold for  $i \in D'_{m, \delta}$ . However, the existence of a nonsimple state with more than four codewords passing through it (as illustrated in Fig. 1) implies that both  $\underline{xu}$  and  $\underline{xw}$  are the bitwise complementary of  $\underline{yv}$ . Obviously, this cannot occur for distinct  $\underline{u}, \underline{w}$ .  $\square$

Clearly, for  $0 < i < d_{\min}^{m, \delta}$  no two codewords can share the same future projection, since the distance between two binary  $n$ -tuples sharing the same future projection at these indices is smaller than the minimum distance of the code. Thus at these indices the array will consist of (one-point height) complete rectangles, none sharing the same column with the other. It follows that the minimum vertex count at each  $0 < i < d_{\min}^{m, \delta}$  is  $|P_{i-}[\mathcal{D}\mathcal{G}(m, \delta)]|$ . Similarly, the minimum vertex count at each  $n - d_{\min}^{m, \delta} < i < n$  is  $|P_{i+}[\mathcal{D}\mathcal{G}(m, \delta)]|$ , where  $n = 2^m$ . These counts are achieved simultaneously, and they do not induce any constraints on the vertex assignment at the remaining indices.

For  $i \notin D_{m, \delta}$ ,  $d_{\min}^{m, \delta} < i < n - d_{\min}^{m, \delta}$ , we did not eliminate the possibility of having both rows and columns of points in the Cartesian array, so it is possible to have at these indices

$$S_i[\mathcal{D}\mathcal{G}(m, \delta)] < \min\{|P_{i-}[\mathcal{D}\mathcal{G}(m, \delta)]|, |P_{i+}[\mathcal{D}\mathcal{G}(m, \delta)]|\}$$

for a trellis diagram having both strict-sense nonexpanding states and strict-sense nonmerging states. At these indices, the minimum vertex count is the cardinality of the largest set of nonconcurring codewords at these indices (a set of codewords is called nonconcurring at an index  $i$ , if any two codewords in it have both different past projections at the index  $i$  and different future projections at this index [13]). We will denote this set as  $N_i$ . From Proposition 3 and the fact that no two nonconcurring codewords can be in the same row or column in the array, we know that the minimum number of states at these indices is at least  $|N_i|$ . In [13] it is shown that there exists a trellis construction that achieves this vertex count, so this is indeed the minimum vertex count for each of these indices. The fact that these codes are rectangular ensures that the above counts are achieved at all indices simultaneously.

It can be confirmed that in the trellis diagram of the Nordstrom–Robinson code (which is, in fact,  $\mathcal{K}(4)$ ) presented in [13], this actually occurs at indices 7 and 9. The number of states at these two indices is equal to the cardinality of the largest set of nonconcurring codewords at these indices, which is less than  $\min\{|P_{i-}[\mathcal{K}(4)]|, |P_{i+}[\mathcal{K}(4)]|\}$  when  $\mathcal{K}(4)$  is arranged in the specific bit-order determined in [13].

#### IV. THE BIT-LEVEL TRELLIS COMPLEXITY OF THE DELSARTE–GOETHALS CODES WHEN ARRANGED IN THE STANDARD BIT-ORDER

In this section we use the Boolean polynomial representation of the codewords of  $\mathcal{D}\mathcal{G}(m, \delta)$  (and in particular  $\mathcal{K}(m)$ ), to derive a formula for the bit-level complexity of the biproper trellis diagram of these codes under the standard bit-order [5], [6]. It is known [5] that this bit-order is optimal for RM( $r, m$ ) in the sense that at each  $i \in \{1, 2, \dots, n-1\}$  the vertex count of the biproper trellis diagram of the code under this bit-order is not larger than that of the biproper trellis diagram of the code under any different bit-order. This fact, along with the result that the nonsimple states in a trellis for  $\mathcal{D}\mathcal{G}(m, \delta)$  (under any bit-order) have only four codewords passing through them (Proposition 3) suggests that this bit-order is probably a good one for constructing a trellis for  $\mathcal{D}\mathcal{G}(m, \delta)$  having a small componentwise vertex count. However, this bit-order is not optimal componentwise as shown in [13] for the Nordstrom–Robinson code,  $\mathcal{K}(4)$ .

The terms in this section follow the ones from [11, Chs. 13–15]. Let  $\underline{v} = (v_1, v_2, \dots, v_m)$  be an  $m$ -tuple of binary variables, and let  $f(\underline{v})$  be a Boolean function of these  $m$  variables. We will denote the space of all binary  $m$ -tuples as  $V^m$ . A length  $2^m$  vector,  $\underline{f}$ , is related to the function  $f(\underline{v})$  by placing (in a specific order) the values that the function attains when  $\underline{v}$  varies through all vectors in  $V^m$ . For  $1 \leq i \leq 2^m$ , let  $x_i$  be the value of  $f(\underline{v})$  where  $\underline{v}$  is the standard binary expansion of  $i-1$ ,  $v_1$  being the LSB. The vector  $\underline{f}$  is said to be in the standard bit-order when it is arranged as follows:

$$\underline{f} = (x_1, x_2, \dots, x_{2^m}) \quad (4.1)$$

similarly to the definition presented by Kasami *et al.* in [5] and [6] (with the exception that the LSB is  $v_1$  instead of  $v_m$ ). In the standard bit-order, the vector related to the function  $v_l$ ,  $1 \leq l \leq m$ , has a “period” of  $2^l$ . Each period consists of  $2^{l-1}$  zeros followed by  $2^{l-1}$  ones. Throughout this section, we will assume that a vector related to a given function is in the standard bit-order. Also, we denote by  $\log a$  the base-2 logarithm of  $a$ .

The  $r$ th-order Reed–Muller code consists of the vectors related to all the Boolean polynomials of degree  $r$  or less. Let  $\underline{l} = (l_1, l_2, \dots, l_m)$  be a binary vector, let  $Q = (q_{ij})$  be an upper triangular  $m \times m$  binary matrix with an all-zero diagonal, and let  $\varepsilon$  be a binary variable. A typical codeword in  $\text{RM}(2, m)$  can be expressed as the vector related to the quadratic polynomial

$$c(\underline{v}) = \underline{v}Q\underline{v}^T + \underline{l}\underline{v}^T + \varepsilon \quad (4.2)$$

where the linear polynomial,  $\underline{l}\underline{v}^T + \varepsilon$ , corresponds to a codeword of  $\text{RM}(1, m)$ , and the quadratic form,  $\underline{v}Q\underline{v}^T$ , determines which coset of  $\text{RM}(1, m)$  contains the codeword  $\underline{c} \in \text{RM}(2, m)$ . Particularly, when  $Q$  is the zero matrix,  $c(\underline{v})$  corresponds to a codeword of  $\text{RM}(1, m)$ . Thus there is a one-to-one correspondence between all the possible values of the matrix  $Q$  and all the cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$ . We henceforth use the notations  $L(\underline{v}) = \underline{l}\underline{v}^T$  and  $Q(\underline{v}) = \underline{v}Q\underline{v}^T$ .

We will refer to a quadratic polynomial,  $c(\underline{v})$ , as a polynomial of rank  $2\delta$  if  $\text{rank}(B) = 2\delta$ , where  $B = Q + Q^T$  and  $Q$  is defined in (4.2). It is clear [11, Ch. 15] that the matrix  $B$  will always be of even rank, and the above definition assigns a rank to each quadratic Boolean polynomial. For even  $m \geq 4$  and for  $2 \leq \delta \leq m/2$ , the Delsarte–Goethals code,  $\mathcal{DG}(m, \delta)$ , is then composed of  $\text{RM}(1, m)$  and cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$  corresponding to the maximal set of quadratic forms such that the rank of every form is at least  $2\delta$ , and the rank of the sum of any two forms is also at least  $2\delta$  [11, Ch. 15].

In what follows we shall use properties of quadratic Boolean polynomials and the above definition of the Delsarte–Goethals codes to find a set of indices in which the biproper trellis representation of  $\mathcal{DG}(m, \delta)$  is composed of parallel sections, each corresponding to a different coset of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$ .

We first observe that if the vectors related to two quadratic Boolean polynomials share the same past projection, then the two quadratic polynomials must agree on some monomials (single-term polynomials). In other words, there are some monomials that can never appear in the sum of the above two quadratic polynomials.

*Lemma 4:* Let

$$c_1(\underline{v}) = \underline{v}Q_1\underline{v}^T + L_1\underline{v}^T + \varepsilon_1$$

and

$$c_2(\underline{v}) = \underline{v}Q_2\underline{v}^T + L_2\underline{v}^T + \varepsilon_2$$

be two quadratic Boolean polynomials. If at an index  $1 \leq i \leq 2^m$   $P_{i-}(\underline{c}_1) = P_{i-}(\underline{c}_2)$ , then

$$c_{\Delta}(\underline{v}) = \begin{cases} \sum_{\substack{\log i+1 \leq j \leq m \\ 1 \leq k < j}} q_{kj}^{\Delta} v_k v_j + \sum_{\log i+1 \leq j \leq m} l_j^{\Delta} v_j, \\ \text{if } i \text{ is a power of } 2 \\ \sum_{\substack{j = \lfloor \log i \rfloor + 1 \\ \lfloor \log i' \rfloor < k < j}} q_{kj}^{\Delta} v_k v_j + \sum_{\substack{\lfloor \log i \rfloor + 2 \leq j \leq m \\ 1 \leq k < j}} q_{kj}^{\Delta} v_k v_j \\ + \sum_{\lfloor \log i \rfloor + 2 \leq j \leq m} l_j^{\Delta} v_j, \text{ otherwise} \end{cases} \quad (4.3)$$

where

$$c_{\Delta}(\underline{v}) = c_1(\underline{v}) + c_2(\underline{v}) = \underline{v}Q_{\Delta}\underline{v}^T + L_{\Delta}\underline{v}^T + \varepsilon_{\Delta} \quad (4.4)$$

$i' = i - 2^{\lfloor \log i \rfloor}$ ,  $l_j^{\Delta}$  is the  $j$ th entry of  $L_{\Delta}$  and  $q_{kj}^{\Delta}$  is the  $(k, j)$  entry of  $Q_{\Delta}$ .

The proof to this lemma is given in the Appendix.

Recall that the first  $2^{l-1}$  indices of  $\underline{v}_l$  are zeros. The following corollary readily follows.

Fig. 2. The symplectic matrix  $B$  for a quadratic polynomial  $c_1(\underline{v})$  that has  $P_{i-}(\underline{c}_1) = 0$ . If  $i$  is not a power of 2, then the column numbered  $\lfloor \log i \rfloor + 1$  has zero entries for the rows in the range  $[1, \lfloor \log i' \rfloor]$ , where  $i'$  is defined in Lemma 4. If  $i$  is a power of 2, the latter column does not necessarily have zero entries.

*Corollary 5:* If at  $1 \leq i \leq 2^m$   $P_{i-}(\underline{c}_1) = P_{i-}(\underline{c}_2)$ , then  $P_{x-}(\underline{c}_1) = P_{x-}(\underline{c}_2)$ , and  $P_{x-}(\underline{Q}_1) = P_{x-}(\underline{Q}_2)$ , where

$$x = \begin{cases} i, & \text{if } i \text{ is a power of } 2 \\ 2^{\lfloor \log i \rfloor + 2^{\lfloor \log i' \rfloor}}, & \text{otherwise} \end{cases} \quad (4.5)$$

and  $\underline{c}_1, \underline{c}_2, \underline{Q}_1, \underline{Q}_2$ , and  $i'$  are defined in Lemma 4.

*Lemma 6:* Let  $c(\underline{v})$  be a quadratic function of rank  $2\delta$  or more, where  $\underline{v} = (v_1, v_2, \dots, v_m)$ , and  $m \geq 4$  is an even integer. Then  $P_{i-}(\underline{c}) \neq \underline{0}$  for  $\frac{3}{2}2^{m-\delta} + 1 \leq i \leq n$ , where  $n = 2^m$ , and  $\underline{0}$  is the length- $i$  vector of all zeroes.

*Proof:* Suppose that there exists  $c_1(\underline{v}) = Q_1(\underline{v}) + L_1(\underline{v}) + \varepsilon_1$  which has rank  $2\delta$  or more, and that  $P_{i-}(\underline{c}_1) = \underline{0}$ . By choosing  $c_2(\underline{v})$  to be zero, we get from Lemma 4 that the  $m \times m$  symplectic matrix  $B = Q_1 + Q_1^T$  will have zero entries at the indices specified in Fig. 2.

Evidently, if an  $m \times m$  matrix contains an  $(m-\delta+1) \times (m-\delta+1)$  submatrix which has only zero entries, its rank is less than  $2\delta$ . Thus if  $\lfloor \log i \rfloor = m - \delta$  and  $\lfloor \log i' \rfloor = m - \delta$ , then the matrix  $B$  cannot be of rank  $2\delta$  or more, contradicting our basic assumption. Consequently, the smallest index  $i$  for which the last two identities hold is  $\frac{3}{2}2^{m-\delta} + 1$ .  $\square$

*Corollary 7:* If  $\underline{c}_1$  and  $\underline{c}_2$  are two codewords from different cosets of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$ , and  $\mathcal{DG}(m, \delta)$  is arranged in the standard bit-order then

$$P_{i-}(\underline{c}_1) \neq P_{i-}(\underline{c}_2), \quad \text{for } \frac{3}{2}2^{m-\delta} + 1 \leq i \leq n.$$

*Proof:* We recall that the rank of the quadratic polynomial related to  $\underline{c}_1 + \underline{c}_2$  is at least  $2\delta$ . Applying Lemma 6 to this polynomial establishes the proof.  $\square$

While Corollary 7 refers to past projections, the same results hold for future projections by replacing  $i$  with  $n - i$ . This is due to the fact that if  $(c_1, c_2, \dots, c_n) \in \mathcal{DG}(m, \delta)$  and thus related to a quadratic polynomial, then also  $(c_n, c_{n-1}, \dots, c_1) \in \mathcal{DG}(m, \delta)$ , since it is related to the quadratic polynomial  $\tilde{c} = c(\underline{1} + \underline{v})$ . Clearly  $\underline{c} = (c_1, c_2, \dots, c_n)$  and  $\tilde{c} = (c_n, c_{n-1}, \dots, c_1)$  are in the same coset of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$ .

We can finally get to the main results of this section.

*Theorem 8. Structure and Partial Complexity of the Minimal Trellis:* The biproper trellis diagram of  $\mathcal{DG}(m, \delta)$  under the standard

bit-order has the following (partial) bit-level state complexity

$$s_i[\mathcal{DG}(m, \delta)] = \begin{cases} i, & 1 \leq i \leq d'_{m, \delta} - 1 \\ (m-1)(m/2 - \delta + 1) + \lceil \log i \rceil + 1, & \frac{3}{2}2^{m-\delta} + 1 \leq i < n/2 \\ (m-1)(m/2 - \delta + 1) + m - 1, & i = n/2 \\ (m-1)(m/2 - \delta + 1) + \lceil \log(n-i) \rceil + 1, & n/2 < i \leq n - \frac{3}{2}2^{m-\delta} - 1 \\ n - i, & n - d'_{m, \delta} + 1 \leq i \leq n - 1 \end{cases} \quad (4.6)$$

where

$$d'_{m, \delta} = \begin{cases} 6, & \delta = m/2 \\ 8, & \text{otherwise} \end{cases}$$

is the dual distance of  $\mathcal{DG}(m, \delta)$  [4], [11, Ch. 15].

The above trellis will have strict-sense nonmerging states for  $0 < i < n/2$ , butterfly states at  $i = n/2$ , and strict-sense nonexpanding states for  $n/2 < i < n$ .

*Proof:* We begin by proving (4.6). Using Corollary 7 and the corresponding result for future projections, we conclude that at every index in the range  $[\frac{3}{2}2^{m-\delta} + 1, n - \frac{3}{2}2^{m-\delta} - 1]$  both the past projections and the future projections of any two distinct cosets of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$  are disjoint. Thus for indices in this range we have

$$s_i[\mathcal{DG}(m, \delta)] = s_i[\text{RM}(1, m)] + (m-1)(m/2 - \delta + 1). \quad (4.7)$$

The second term in the RHS of (4.7) is the logarithm of the number of cosets of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$ . Substituting the state complexity of  $\text{RM}(1, m)$  from [10] in (4.7) we prove the three middle terms of (4.6).

The fact that for a code having dual distance  $d'$ , any set of  $d' - 1$  positions in the code comprises all possible  $2^{d'-1}$  different  $(d' - 1)$ -tuples [11, p. 139] establishes the first and last part of (4.6).

Similarly to the proof of Proposition 3, it is clear that any trellis diagram of  $\mathcal{DG}(m, \delta)$  will have strict-sense nonmerging states for  $i < d_{\min}^{m, \delta}$  and strict-sense nonexpanding states for  $i > n - d_{\min}^{m, \delta}$ .

Clearly, for the indices in the range  $[\frac{3}{2}2^{m-\delta} + 1, n - \frac{3}{2}2^{m-\delta} - 1]$  the minimal trellis for  $\mathcal{DG}(m, \delta)$  has the same structure as the minimal trellis for  $\text{RM}(1, m)$ . Also, it is easily verified that for  $\delta \geq 3$

$$[d_{\min}^{m, \delta}, n - d_{\min}^{m, \delta}] \subset \left[ \frac{3}{2}2^{m-\delta} + 1, n - \frac{3}{2}2^{m-\delta} - 1 \right].$$

Combining these two results we prove the statement about the structure of the trellis for  $\delta \geq 3$ . For  $\delta = 2$ , we have

$$[d_{\min}^{m, \delta}, n - d_{\min}^{m, \delta}] = \left[ \frac{3}{2}2^{m-\delta}, n - \frac{3}{2}2^{m-\delta} \right]$$

so we have to check whether the states at  $i = \frac{3}{2}2^{m-\delta}$  are strict-sense nonmerging. Since the trellis structure implies that at  $i = \frac{3}{2}2^{m-\delta} + 1$  no two codewords share the same future projection, this is obviously true also at  $i = \frac{3}{2}2^{m-\delta}$ , completing the proof of the theorem.  $\square$

It is readily confirmed from (4.6) that  $S_{\max}[\mathcal{DG}(m, \delta)]$  found in Proposition 2 for  $\delta \geq 3$  is attained for this bit-order. The structure of the biproper trellis diagram presented in Theorem 8 implies that at  $1 \leq i \leq n/2 - 1$  each state has a single edge entering it, and thus the branch complexity at these indices is  $b_i = s_i$ . At  $n/2 + 1 \leq i < n$ , each state has a single edge leaving it, so at  $n/2 + 2 \leq i \leq n$ , the branch complexity is  $b_i = s_{i-1}$ . Similarly,

$$b_{n/2} = b_{n/2+1} = s_{n/2} + 1 = \log |\mathcal{DG}(m, \delta)| - 1$$

since the structure of the biproper trellis implies that at  $i = n/2$  each state has exactly two edges entering it, and two edges leaving it.

It follows from Corollary 5 that if two codewords from different cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$  share the same past projection at  $1 \leq i \leq n/2 - 1$ , then these words share the same past projection at  $x$ , where  $x$  is defined in (4.5). In addition, the past projections of two distinct cosets are either identical or disjoint. Denote the set of all coset representatives of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$  which are related to quadratic forms (including the zero vector) as  $Q_{\mathcal{DG}(m, \delta)}$ . We therefore have

$$|P_{i-}[\mathcal{DG}(m, \delta)]| = |P_{x-}[Q_{\mathcal{DG}(m, \delta)}]| \cdot |P_{x-}[\text{RM}(1, m)]|, \quad 1 \leq i \leq n. \quad (4.8)$$

From Theorem 8 we know that

$$S_i[\mathcal{DG}(m, \delta)] = |P_{i-}[\mathcal{DG}(m, \delta)]|, \quad \text{for } 1 \leq i < n/2$$

since the biproper trellis diagram of the code consists of strict-sense nonmerging states at these indices. Similarly,

$$S_i[\mathcal{DG}(m, \delta)] = |P_{i+}[\mathcal{DG}(m, \delta)]|, \quad \text{for } n/2 < i < n.$$

Since the problem of finding the cardinality of past projections is a subproblem of finding values of the CLP [9] or the ELP [13], there is no use in applying bounds from [9] or [13]. We will therefore use (4.8) in order to derive an upper bound on the vertex count at the indices that (4.6) does not cover.

*Proposition 9. An Upper Bound:* For the minimal trellis of  $\mathcal{DG}(m, \delta)$  mentioned in Theorem 8, the state complexity at any index  $d'_{m, \delta} \leq i \leq \frac{3}{2}2^{m-\delta}$  is upper-bounded by

$$s_i[\mathcal{DG}(m, \delta)] \leq \begin{cases} \min[\alpha, \frac{1}{2} \log i (\log i - 1)] + \log i + 1, & \text{if } i \text{ is a power of } 2 \\ \min[\alpha, \frac{1}{2} \lceil \log i \rceil (\lceil \log i \rceil - 1) + \lceil \log(i - 2^{\lceil \log i \rceil}) \rceil] & \\ + \lceil \log i \rceil + 1, & \text{otherwise} \end{cases} \quad (4.9)$$

where  $\alpha \equiv (m-1)(m/2 - \delta + 1)$ .

Also, for  $n - \frac{3}{2}2^{m-\delta} \leq i \leq n - 1$  the upper bound is obtained by replacing  $i$  with  $n - i$  in the RHS of (4.9).

*Proof:* Clearly

$$|P_{i-}[Q_{\mathcal{DG}(m, \delta)}]| \leq |Q_{\mathcal{DG}(m, \delta)}| = 2^{(m-1)(m/2 - \delta + 1)}.$$

Denote by  $QF(m)$  the code obtained from taking the vectors related to all the quadratic forms in  $\text{RM}(2, m)$ . Let  $Q = (q_{kj})$  vary through all upper triangular  $m \times m$  binary matrices. It follows from Lemma 4 that there is a one-to-one correspondence between

$$\begin{cases} \{q_{kj}\}_{\substack{2 \leq j \leq \log i, \\ 1 \leq k < j}}, & \text{if } i \text{ is a power of } 2 \\ \{q_{kj}\}_{\substack{2 \leq j \leq \lceil \log i \rceil \\ 1 \leq k < j}} \cup \{q_{kj}\}_{\substack{j = \lceil \log i \rceil + 1, \\ 1 \leq k \leq \lceil \log i \rceil}}, & \text{otherwise} \end{cases} \quad (4.10)$$

and  $P_{x-}[QF(m)]$ . Hence,

$$\log |P_{x-}[QF(m)]| = \begin{cases} \frac{1}{2} \log i (\log i - 1), & \text{if } i \text{ is a power of } 2 \\ \frac{1}{2} \lceil \log i \rceil (\lceil \log i \rceil - 1) + \lceil \log(i - 2^{\lceil \log i \rceil}) \rceil, & \text{otherwise} \end{cases}$$

which is the number of free binary variables in (4.10). Combining the fact that

$$|P_{x-}[Q_{\mathcal{DG}(m, \delta)}]| \leq |P_{x-}[QF(m)]|$$

with the results from [10] we establish the part concerning indices in the range  $[1, n/2)$ . Using similar arguments the second part of the proposition can be proved.  $\square$

TABLE I  
A COMPARISON BETWEEN THE ACTUAL VERTEX COUNT AND THE DERIVED UPPER AND LOWER BOUNDS FOR SEVERAL DELSARTE–GOETHALS CODES

$i$ :	6	7, 8	9	10	11, 12	13-16	17	18	19, 20	21-24	25-32	33	34	35, 36	37-40	41-48
UB	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$											
$S_i[\kappa(6)]$	$2^6$	$2^7$	$2^8$	$2^9$	$\frac{3}{4} \cdot 2^{10}$											
LB	$2^5$	$2^6$	$2^7$	$2^8$	$2^9$											
UB	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{13}$	$2^{13}$						
$S_i[\kappa(8)]$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$\frac{21}{32} \cdot 2^{13}$	$\frac{13}{16} \cdot 2^{13}$	$\frac{7}{8} \cdot 2^{13}$						
LB	$2^4$	$2^4$	$2^5$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$						
UB	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$	$2^{16}$	$2^{16}$	$2^{16}$	$2^{16}$	$2^{16}$	$2^{16}$
$S_i[\kappa(10)]$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$\frac{7}{8} \cdot 2^{13}$	$\frac{21}{32} \cdot 2^{14}$	$\frac{3}{4} \cdot 2^{14}$	$\frac{3}{4} \cdot 2^{15}$	$\frac{3}{4} \cdot 2^{16}$	$\frac{53}{64} \cdot 2^{16}$	$\frac{7}{8} \cdot 2^{16}$	$\frac{29}{32} \cdot 2^{16}$	$\frac{15}{16} \cdot 2^{16}$
LB	$2^4$	$2^4$	$2^5$	$2^5$	$2^5$	$2^5$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$
UB			$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$	$2^{16}$	$2^{17}$	$2^{18}$	$2^{19}$	$2^{20}$	$2^{21}$
$S_i[\mathcal{D}\mathcal{G}(8,3)]$			$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$	$2^{16}$	$2^{17}$	$2^{18}$	$2^{19}$	$\frac{7}{8} \cdot 2^{20}$	$\frac{3}{4} \cdot 2^{21}$
LB			$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$	$2^{15}$	$2^{16}$	$2^{17}$	$2^{18}$	$2^{19}$	$2^{20}$

*Proposition 10:* For the minimal trellis of  $\mathcal{D}\mathcal{G}(m, \delta)$  mentioned in Theorem 8, the vertex count at any index  $1 < i < n/2$  satisfies

$$S_{i-1}[\mathcal{D}\mathcal{G}(m, \delta)] = S_i[\mathcal{D}\mathcal{G}(m, \delta)], \quad \text{if } w_2(i-1) > 2 \quad (4.11)$$

where  $w_2(i)$  is the Hamming weight of the standard binary expansion of the integer  $i$ . For  $n/2 < i < n-1$  the vertex count satisfies

$$S_{i+1}[\mathcal{D}\mathcal{G}(m, \delta)] = S_i[\mathcal{D}\mathcal{G}(m, \delta)], \quad \text{if } w_2(n-i-1) > 2. \quad (4.12)$$

*Proof:* Let  $i_1 = 2^{l_1} + 2^{l_2} < n/2$ , and let  $i_2$  be the largest integer satisfying  $i_2 = 2^{l_3} + 2^{l_4} < i_1$ , where  $l_1, l_2, l_3, l_4$  are positive integers. It is clear from Corollary 5 that there is a one-to-one correspondence between  $P_{i_1-1}(C_2)$  and  $P_{i_2-1}(C_2)$  for  $i_2 < i < i_1$ , where  $C_2$  is any subcode of  $\text{RM}(2, m)$ , and (4.11) is established. By using similar arguments, the statement concerning  $n/2 < i < n-1$  is established.  $\square$

Obviously, for  $1 < i < n/2$  the vertex count of the biproper trellis from Theorem 8 satisfies

$$S_{i-1}[\mathcal{D}\mathcal{G}(m, \delta)] \geq \max\left\{\frac{1}{2} S_i[\mathcal{D}\mathcal{G}(m, \delta)], S_{i-1}[\text{RM}(1, m)]\right\} \quad \text{if } w_2(i-1) \leq 2. \quad (4.13)$$

For  $n/2 < i < n-1$ , the vertex count satisfies the expression

$$S_{i+1}[\mathcal{D}\mathcal{G}(m, \delta)] \geq \max\left\{\frac{1}{2} S_i[\mathcal{D}\mathcal{G}(m, \delta)], S_{i+1}[\text{RM}(1, m)]\right\} \quad \text{if } w_2(n-i-1) \leq 2. \quad (4.14)$$

We can use (4.11) together with (4.13) to formulate a lower bound on the vertex count at  $1 < i < n/2$ . We use the relation

$$S_{(3/2)2^{m-\delta+1}} = 2^{(m-1)(m/2-\delta+1)+m-\delta+2}$$

from (4.6) as an initial value of the state complexity in the above lower bound. The lower bound on the vertex count at  $n/2 < i < n-1$ , is obtained by replacing  $i$  with  $n-i$  in the lower bound at  $1 < i < n/2$ .

A comparison between the actual vertex count (obtained from a computer search) and the upper and lower bounds on the state complexity (calculated from (4.9), (4.13), and (4.11)), is given in Table I for several Delsarte–Goethals codes. The rows marked “UB” and “LB” correspond to the upper and lower bounds, respectively. We give the results only for the indices in which (4.6) does not apply, and only for  $i < n/2$ , since

$$S_i[\mathcal{D}\mathcal{G}(m, \delta)] = S_{n-i}[\mathcal{D}\mathcal{G}(m, \delta)]$$

and the bounds obey the same rule of symmetry. Evidently, the lower bound is not tight for  $\mathcal{K}(10)$ .

*Remark:* Since  $d'_{m, m/2-1} = 8$ , the first index not covered by (4.6) is  $i = 8$ . However, it is clear from arguments similar to the ones in the proof of Proposition 10 that  $S_8[\mathcal{D}\mathcal{G}(8, 3)] = S_7[\mathcal{D}\mathcal{G}(8, 3)] = 2^7$ . We therefore begin our calculations from  $i = 9$ .

## V. CONCLUSION

In this correspondence, we have examined the structure and complexity of the trellis diagram of the Kerdock and Delsarte–Goethals codes. Although these codes are nonlinear they admit a biproper trellis diagram under any given bit-order.

It was proved that at each  $i \notin D'_{m, \delta}$  the states of any trellis diagram of the Delsarte–Goethals codes (under any given bit-order) are simple. At indices within  $D'_{m, \delta}$ , the states are either simple states or butterfly states or a combination of both.

Combining the properties of quadratic Boolean polynomials with the property that the sum of any two codewords of  $\mathcal{D}\mathcal{G}(m, \delta)$  from different cosets of  $\text{RM}(1, m)$  in  $\text{RM}(2, m)$  is of rank  $2\delta$  or more, we derived a partial formula for the vertex count of the biproper trellis diagram of these codes when arranged in the standard bit-order. The number of indices for which this formula holds grows as the value of  $\delta$  grows, and therefore reaches its maximum for  $\delta = m/2$ , corresponding to the Kerdock code. In this case, the formula applies to  $2(n/2 - \frac{3}{2}\sqrt{n} + 4) + 1$  indices (excluding  $i = 0, n$ ).

For  $\delta \geq 3$ , we observe that when  $\mathcal{D}\mathcal{G}(m, \delta)$  is in the standard bit-order, the maximum vertex count in the biproper trellis representation of the code achieves  $S_{\max}[\mathcal{D}\mathcal{G}(m, \delta)] = \frac{1}{2} \cdot |\mathcal{D}\mathcal{G}(m, \delta)|$ . For all values of  $m$  and  $\delta$  the states of the biproper trellis diagram of  $\mathcal{D}\mathcal{G}(m, \delta)$  are strict-sense nonmerging states for  $1 \leq i \leq n/2 - 1$ , strict-sense nonexpanding states for  $n/2 + 1 \leq i \leq n - 1$ , and butterfly states at  $i = n/2$ .

The upper and lower bounds derived, using mainly the properties of  $\text{RM}(2, m)$ , are tighter for small values of  $\delta$ , since in these cases  $\mathcal{D}\mathcal{G}(m, \delta)$  is a larger subcode of  $\text{RM}(2, m)$ . For the Kerdock codes, it appears that when going in a descending order of indices from  $i = \frac{3}{2}\sqrt{n}$ , the vertex count will decrease in small amounts at the indices described in (4.13) that are close to  $i = \frac{3}{2}\sqrt{n}$ , as observed from Table I. It suggests that the lower bound will not be tight for the Kerdock codes.

It is noteworthy to remark that the results of Theorem 8 suggest that for values of  $\delta$  that are close to 2, only a small portion of the trellis representation of  $\mathcal{D}\mathcal{G}(m, \delta)$  is composed of parallel sections, each corresponding to a different coset of  $\text{RM}(1, m)$  in  $\mathcal{D}\mathcal{G}(m, \delta)$ . Therefore, when  $\delta$  is close to 2 and  $\mathcal{D}\mathcal{G}(m, \delta)$  is in the standard bit-order, the Viterbi decoding by means of biproper trellis may be fairly more efficient than *coset decoding*. Coset decoding consists

of Viterbi decoding (in turn) each of the cosets of  $\text{RM}(1, m)$  in  $\mathcal{DG}(m, \delta)$ , and retaining the best codeword. The number of addition-equivalent operations required to decode the Delsarte–Goethals codes described in Table I was calculated for both mentioned algorithms. Viterbi decoding by means of biproper trellis required up to 10% less operations than coset decoding. The number of addition-equivalent operations required for Viterbi decoding was calculated directly from the formula  $2|E| - |V| + 1$ . It should be noted that it is possible to reduce the decoding complexity of both methods by the use of trellis sectionalization.

In [13] it was shown that the vertex count of  $\mathcal{DG}(4, 2)$  (the Nordstrom–Robinson code), under the standard bit-order is not minimal componentwise. However, the question whether there exists a bit-order for which the trellis diagram of  $\mathcal{DG}(m, \delta)$  is minimal componentwise remains pending.

#### APPENDIX PROOF OF LEMMA 4

We decompose  $c_\Delta(\underline{v})$  into

$$c_\Delta(\underline{v}) = \varepsilon_\Delta + \left( \sum_{1 \leq k < j \leq \lfloor \log i \rfloor} q_{kj}^\Delta v_k v_j + \sum_{1 \leq j \leq \lfloor \log i \rfloor} l_j^\Delta v_j \right) + \left( \sum_{\substack{\lfloor \log i \rfloor + 1 \leq j \leq m \\ 1 \leq k < j}} q_{kj}^\Delta v_k v_j + \sum_{\lfloor \log i \rfloor + 1 \leq j \leq m} l_j^\Delta v_j \right). \quad (\text{A.1})$$

For  $\lfloor \log i \rfloor + 1 \leq l \leq m$  we have  $P_{(2^{\lfloor \log i \rfloor})_-(\underline{v}_l)} = \underline{0}$  and thus the vector related to the last term in the RHS of (A.1) is zero for its first  $2^{\lfloor \log i \rfloor}$  indices. We define

$$\tilde{c}_\Delta(v_1, v_2, \dots, v_{\lfloor \log i \rfloor}) = \left( \sum_{1 \leq k < j \leq \lfloor \log i \rfloor} q_{kj}^\Delta v_k v_j + \sum_{1 \leq j \leq \lfloor \log i \rfloor} l_j^\Delta v_j \right) + \varepsilon_\Delta. \quad (\text{A.2})$$

From the above arguments, and since  $P_{i_-(\underline{c}_\Delta)} = \underline{0}$ , it follows that

$$\tilde{\underline{c}}_\Delta = P_{(2^{\lfloor \log i \rfloor})_-(\underline{c}_\Delta)} = \underline{0}. \quad (\text{A.3})$$

From (A.3) we have that all the values taken by the  $\lfloor \log i \rfloor$ -variable quadratic polynomial  $\tilde{c}_\Delta(v_1, v_2, \dots, v_{\lfloor \log i \rfloor})$  when its argument goes through *all* the elements of  $V^{\lfloor \log i \rfloor}$  are zero. This is possible only if

$$\tilde{c}_\Delta(v_1, v_2, \dots, v_{\lfloor \log i \rfloor}) = 0$$

that is,  $q_{kj}^\Delta = 0$  for  $1 \leq k < j \leq \lfloor \log i \rfloor$ , and  $l_j^\Delta = 0$  for  $1 \leq j \leq \lfloor \log i \rfloor$ , and  $\varepsilon_\Delta = 0$ , establishing the first part of (4.3).

For an  $i$  that is not a power of two, we will examine the vector  $\underline{c}_\Delta$  at the indices in the range  $[2^{\lfloor \log i \rfloor + 1}, 2^{\lfloor \log i \rfloor + 1}]$ . From the above discussion it follows, that the only elements of  $c_\Delta(\underline{v})$  that may not be zero at these indices (i.e., when  $\underline{v}$  is the binary expansion of these indices) can be written as

$$\tilde{c}_\Delta(v_1, v_2, \dots, v_{\lfloor \log i \rfloor}, v_{\lfloor \log i \rfloor + 1}) = \sum_{1 \leq k \leq \lfloor \log i \rfloor} q_{k, \lfloor \log i \rfloor + 1} v_k v_{\lfloor \log i \rfloor + 1} + l_{\lfloor \log i \rfloor + 1} v_{\lfloor \log i \rfloor + 1}. \quad (\text{A.4})$$

Yet,  $v_{\lfloor \log i \rfloor + 1}$  is one for all indices in the range

$$[2^{\lfloor \log i \rfloor + 1}, 2^{\lfloor \log i \rfloor + 1}]$$

(the second half of its first period), so (A.4) reads

$$\tilde{c}_\Delta(v_1, v_2, \dots, v_{\lfloor \log i \rfloor}) = \sum_{1 \leq k \leq \lfloor \log i \rfloor} q_{k, \lfloor \log i \rfloor + 1} v_k + \varepsilon', \quad \varepsilon' = l_{\lfloor \log i \rfloor + 1} \quad (\text{A.5})$$

which is a linear Boolean polynomial. From the lemma's assumptions, it follows that the vector related to this linear function has zero entries in the range  $[1, i']$ , where  $i'$  is defined in Lemma 4. Using arguments similar to the ones mentioned above, it can be shown that if the vector related to a linear polynomial has zero entries in the range  $[1, i']$  it actually has zero entries in the whole range  $[1, 2^{\lceil \log i' \rceil}]$ . It also follows that both

$$q_{k, \lfloor \log i \rfloor + 1} = 0, \quad 1 \leq k \leq \lceil \log i' \rceil$$

and  $\varepsilon' = 0$ , completing the proof of Lemma 4.  $\square$

#### ACKNOWLEDGMENT

The authors wish to thank the anonymous referees for helpful comments.

#### REFERENCES

- [1] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 203–209, Jan. 1993.
- [2] G. D. Forney, Jr., "Coset codes—Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.
- [3] —, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1741–1752, Nov. 1994.
- [4] F. B. Hergert, "On the Delsarte–Goethals codes and their formal duals," *Discr. Math.*, vol. 83, pp. 249–263, 1990.
- [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, Jan. 1993.
- [6] —, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1057–1064, May 1993.
- [7] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1828–1838, Nov. 1996.
- [8] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1924–1937, Nov. 1995.
- [9] A. Lafourcade and A. Vardy, "Lower bounds on trellis complexity of block codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1938–1954, Nov. 1995.
- [10] C.-C. Lu and S.-H. Huang, "On bit-level trellis complexity of Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2061–2064, Nov. 1995.
- [11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North Holland, 1977.
- [12] D. J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1049–1053, Sept. 1988.
- [13] 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.
- [14] V. Sidorenko, I. Martin, and B. Honary, "On separability of nonlinear block codes," preprint.
- [15] 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.