Which Codes Have 4-Cycle-Free Tanner Graphs?

Thomas R. Halford, Alex J. Grant and Keith M. Chugg

***Abstract*— Let $\mathcal{C}$ be an $[n,k,d]$ binary linear code with rate $R=k/n$ and dual $\mathcal{C}^{\perp}$. In this correspondence, it is shown that $\mathcal{C}$ can be represented by a 4-cycle-free Tanner graph only if:**

$$pd^{\perp} \leq \left\lfloor \sqrt{np(p-1)+\frac{n^2}{4}}+\frac{n}{2} \right\rfloor$$

where $p=n-k$ and $d^{\perp}$ is the minimum distance of $\mathcal{C}^{\perp}$. By applying this result, it is shown that 4-cycle-free Tanner graphs do not exist for many classical binary linear block codes.

***Index Terms*— Cycles, girth, graphical models of codes, iterative decoding, Tanner graphs.**

I. Introduction

The study of graphical models of codes is of great current interest. This work considers a specific, well-known, family of graphical models of binary linear block codes: Tanner graphs [1]. Briefly, let $\mathcal{C}$ be an $[n,k,d]$ binary linear block code with $n-k \times n$ parity check matrix $H=[h_{ij}]$. Associated with H is a bipartite graph, $G_H(\mathcal{U} \cup \mathcal{W}, \mathcal{E})$, with disjoint vertex classes $\mathcal{U}=\{u_i\}_{i=1}^{n-k}$ and $\mathcal{W}=\{w_j\}_{j=1}^{n}$ corresponding to the rows and columns of H, respectively. An edge connects u_i and w_j in G_H if and only if $h_{ij}=1$. Note that since there exist multiple parity check matrices for $\mathcal{C}$, there are, likewise, multiple Tanner graphs which represent $\mathcal{C}$.

Iterative decoding on Tanner graphs has been widely studied, particularly in the context of low-density parity-check (LDPC) codes. It is now widely accepted that there is a relationship between the graph theoretic properties of a graphical code model and the performance of the iterative decoding algorithm implied by that model. Specifically, a number of authors have stressed the importance of designing LDPC codes with Tanner graphs that have no cycles of length four [2], [3], [4]. Furthermore, a number of authors have noted that Tanner graphs for classical linear block codes tend to contain 4-cycles and have thus investigated techniques for obtaining 4-cycle-free graphical models based on generalized parity check matrices [5], [6].

Inspired by the work of Etzion, Trachtenberg and Vardy concerning codes with cycle-free Tanner graphs [7], the present correspondence addresses the question: which codes have 4-cycle-free Tanner graphs? The remainder of this correspondence is organized as follows. The main result on the existence of 4-cycle-free Tanner graphs is proved in Section III. The main result follows directly from results in graph theory which are reviewed in Section II. In Section IV, the tightness of the main result is considered. The main result is applied to a number of classical linear block code families in Section V. Specifically, it is shown that the following binary codes do not have 4-cycle-free Tanner graphs:

1) The $[23,12,7]$ binary Golay and $[24,12,8]$ extended binary Golay codes.
2) Those $[n=2^m,k,d=2^{m-r}]$ Reed-Muller (RM) codes with rate $R \geq 1/2$ and minimum distance $d>2$ for $3 \leq m \leq 9$.
3) Those $[n=2^m-1,k,d]$ primitive Bose-Chaudhuri-Hocquenghem (BCH) codes with rate $R \geq 1/2$ for $3 \leq m \leq 8$.
4) The binary image of those $[n=2^m-1,k,d=n-k+1]$ Reed-Solomon (RS) codes with rate $1/2 \leq R \leq 1-2/n$ for $3 \leq m \leq 5$.
5) The binary image of those $[n=2^m-1,k,d=n-k+1]$ RS codes with rate $1/3 \leq R \leq 1-2/n$ for $m \geq 6$.

Concluding remarks are given in Section VI.

II. Preliminaries from Graph Theory

In the following, $G(\mathcal{U} \cup \mathcal{W}, \mathcal{E})$ denotes a bipartite graph with vertex classes $\mathcal{U}=\{u_i\}_{i=1}^{n_u}$ and $\mathcal{W}=\{w_j\}_{j=1}^{n_w}$ and with edge set $\mathcal{E} \subseteq \mathcal{U} \times \mathcal{W}$[1]. The *size* of G is $n_e=|\mathcal{E}|$. The degree of a vertex $v \in \mathcal{U} \cup \mathcal{W}$ is denoted $d(v)$.

Propositions 1 and 2 are well-known; the proofs presented below are due to Neuwirth [8] and are given for completeness.

Proposition 1: Let $G(\mathcal{U} \cup \mathcal{W}, \mathcal{E})$ be a 4-cycle-free bipartite graph. Then:

$$\sum_{j=1}^{n_w} \binom{d(w_j)}{2} \leq \binom{n_u}{2} \tag{1}$$

where $\binom{x}{y}$ is the binomial coefficient.

Proof: Define $\widetilde{G}(\mathcal{U}, \widetilde{\mathcal{E}})$ as the graph with vertex set $\mathcal{U}$ and edge set:

$$\widetilde{\mathcal{E}} = \Big\{ \{x,z\} \in \mathcal{U} \times \mathcal{U} \Big| \exists\ y \in \mathcal{W} \text{ so that } \{x,y\} \in \mathcal{E} \text{ and } \{z,y\} \in \mathcal{E} \Big\}. \tag{2}$$

Because G is 4-cycle-free, there is at most one $y \in \mathcal{W}$ such that $\{x,y\} \in \mathcal{E}$ and $\{z,y\} \in \mathcal{E}$ for each $\{x,z\} \in \mathcal{U} \times \mathcal{U}$. Thus, $\widetilde{G}$ contains no multiple edges and $|\widetilde{\mathcal{E}}| \leq \binom{n_u}{2}$. The proposition then follows by noting that there is a bijection between edges in $\widetilde{G}$ and pairs of vertices incident on vertices $w_j \in \mathcal{W}$ in G. □

Proposition 2: Let $G(\mathcal{U} \cup \mathcal{W}, \mathcal{E})$ be a 4-cycle-free bipartite graph such that $n_w > \binom{n_u}{2}$. Then there are at least $n_w - \binom{n_u}{2}$ vertices in $\mathcal{W}$ with degree 0 or 1.

Proof: Let $\mathcal{W}_2 = \{w_j \in \mathcal{W} | d(w_j) \geq 2\}$. By Proposition 1, since $\binom{0}{2}=\binom{1}{2}=0$ and $\binom{d(w_j)}{2} \geq 1\ \forall\ w_j \in \mathcal{W}_2$:

$$|\mathcal{W}_2| \leq \sum_{j=1}^{n_w} \binom{d(w_j)}{2} \leq \binom{n_u}{2}. \tag{3}$$

[1]The results presented hold for general bipartite graphs; however, we consider the case where $n_w \geq n_u$. In the context of Tanner graphs, $\mathcal{W}$ thus corresponds to the variable node set and $\mathcal{U}$ to the check node set.

Because $n_w > \binom{n_u}{2}$, there must be at least $n_w - \binom{n_u}{2}$ vertices in $\mathcal{W} \setminus \mathcal{W}_2$. □

Theorem 3 is well-known as Reiman's inequality [9]; the proof presented here is adopted from Bollobas [10].

Theorem 3: Let $G(\mathcal{U} \cup \mathcal{W}, \mathcal{E})$ be a 4-cycle-free bipartite graph with $n_u \leq n_w$. Then the size of G satifies:

$$n_e \leq \sqrt{n_w n_u (n_u - 1) + \frac{n_w^2}{4}} + \frac{n_w}{2}. \tag{4}$$

Proof: Let $z = \sqrt{n_w n_u (n_u - 1) + \frac{n_w^2}{4}} + \frac{n_w}{2}$ and note that:

$$\frac{z(z - n_w)}{2n_w} = \frac{n_u(n_u - 1)}{2} = \binom{n_u}{2}. \tag{5}$$

Suppose that G has size strictly greater than z so that:

$$\sum_{j=1}^{n_w} d(w_j) = n_e > z. \tag{6}$$

Proposition 1 implies the following series of inequalities:

$$\binom{n_u}{2} \geq \sum_{j=1}^{n_w} \binom{d(w_j)}{2} \tag{7}$$

$$= \frac{1}{2} \sum_{j=1}^{n_w} (d(w_j))^2 - \frac{1}{2} \sum_{j=1}^{n_w} d(w_j) \tag{8}$$

$$\geq \frac{1}{2n_w} n_e^2 - \frac{n_e}{2} \tag{9}$$

$$> \frac{z(z - n_w)}{2n_w} \tag{10}$$

$$= \binom{n_u}{2}. \tag{11}$$

Note that (9) follows from (8) via the Cauchy-Schwarz inequality. Since $\binom{n_u}{2} \not> \binom{n_u}{2}$, $n_e \not> z$ proving the Theorem. □

Neuwirth noted that equality holds in Theorem 3 if and only if G is the incidence graph of a Steiner system (see, for example, [11]), $S(2, k; n_u)$, on n_u points with block degree k satisfying $n_w k(k-1) = n_u(n_u - 1)$ [8].

III. Proof of the Main Result

Theorem 4: Let $\mathcal{C}$ be an $[n, k, d]$ binary linear block code with dual $\mathcal{C}^\perp$. Then $\mathcal{C}$ can be represented by a 4-cycle-free Tanner graph only if:

$$pd^\perp \leq \left\lfloor \sqrt{np(p-1) + \frac{n^2}{4}} + \frac{n}{2} \right\rfloor \tag{12}$$

where $p = n - k$ and $d^\perp$ is the minimum distance of $\mathcal{C}^\perp$.

Proof: Let H be a $p \times n$ parity check matrix for $\mathcal{C}$ and let $\mathrm{wt}(H)$ denote the number of 1's in H. The Tanner graph corresponding to H, G_H, is bipartite with $n_w = n$, $n_u = p$ and $n_e = \mathrm{wt}(H)$. By Theorem 3, in order for G_H to be 4-cycle-free its size must satisfy:

$$\mathrm{wt}(H) \leq \left\lfloor \sqrt{np(p-1) + \frac{n^2}{4}} + \frac{n}{2} \right\rfloor. \tag{13}$$

Since H generates $\mathcal{C}^\perp$, any row of H is a nonzero codeword in $\mathcal{C}^\perp$ and contains at least $d^\perp$ 1's. Thus, *any* parity check matrix for H must satisfy $\mathrm{wt}(H) \geq pd^\perp$ completing the proof. □

Theorem 4 immediately implies the following corollary which is given without proof.

Corollary 5: Let $\mathcal{C}$ be an $[n, k, d]$ binary linear block code for which a 4-cycle-free Tanner graph does not exist. Then the number of 4-cycles in any Tanner graph representing $\mathcal{C}$ is lower-bounded by:

$$pd^\perp - \left\lfloor \sqrt{np(p-1) + \frac{n^2}{4}} + \frac{n}{2} \right\rfloor \tag{14}$$

where $p = n - k$ and $d^\perp$ is the minimum distance of $\mathcal{C}^\perp$.

As an example, consider the $[7, 4, 3]$ Hamming code, $\mathcal{C}_{[7,4,3]}$, with $d^\perp = 4$. Any parity check matrix for $\mathcal{C}_{[7,4,3]}$ contains the 7 nonzero binary vectors of length 3 and is thus isomorphic (under permutation of columns) to [12]:

$$H_{[7,4,3]} = \begin{bmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{bmatrix}. \tag{15}$$

The Tanner graph corresponding to $H_{[7,4,3]}$ clearly contains 3 4-cycles. Indeed, for this code:

$$pd^\perp = 12 \tag{16}$$

while:

$$\left\lfloor \sqrt{np(p-1) + \frac{n^2}{4}} + \frac{n}{2} \right\rfloor = 10 \tag{17}$$

precluding the existence of a 4-cycle-free Tanner graph while requiring that any Tanner graph for $H_{[7,4,3]}$ contains at least 2 4-cycles.

IV. Remarks on the Main Result

Two questions arise naturally from the bound provided by Theorem 4:

1) How tight is the bound?
2) Do there exist codes with 4-cycle-free Tanner graphs which meet the bound with equality?

Hoory noted that Reiman's inequality is the tightest known bound on the size of a 4-cycle-free bipartite graph [13]. However, Theorem 3 provides only a *necessary* condition for the existence of a 4-cycle-free bipartite graph - it is not clear that a 4-cycle-free Tanner graph can be found for any code that satisfies Theorem 4.

Neuwirth noted that graphs which meet the bound of Theorem 3 with equality are necessarily the incidence graphs of certain Steiner systems [8]. A number of authors have used Steiner systems as a tool for designing algebraically constructed LDPC codes (see, for example, [14]). A search for codes which meet the bound of Theorem 4 thus begins by examining codes with duals generated by the incidence matrices of Steiner systems.

v	$pd^{\perp}$	$\left\lfloor \sqrt{np(p-1)+\frac{n^2}{4}}+\frac{n}{2} \right\rfloor$
2	4	4
3	9	9
4	16	17
5	25	26
6	36	37
7	49	51
8	64	66
9	81	83
10	100	103

TABLE I

APPLICATION OF THEOREM 4 TO THE $\mathcal{C}'_{S(2,2;v)}$ FAMILY OF CODES FOR $2 \leq v \leq 10$.

Let $\mathcal{C}_{S(2,3;9)}$ be the code with parity check matrix:

$$H_{S(2,3;9)} = \begin{bmatrix} 1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1 \\ 0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0 \end{bmatrix}. \quad (18)$$

Equation (18) defines the incidence matrix of the Steiner system $S(2,3;9)$ and the Tanner graph corresponding to $\mathcal{C}_{S(2,3;9)}$ meets the bound of Theorem 3 with equality. However, the minimum distance of the code generated by $H_{S(2,3;9)}$ is 2, which is not equal to the minimum row weight of $H_{S(2,3;9)}$. Therefore, $\mathcal{C}_{S(2,3;9)}$ does not meet the bound of Theorem 4 with equality. In general, the codes generated by the incidence matrices of Steiner systems do not have minimum distance equal to the minimum row weight of those matrices and an alternate approach is required to meet the bound of Theorem 4 with equality.

Let $\mathcal{C}'_{S(2,2;v)}$ be the code with parity check matrix:

$$H'_{S(2,2;v)} = \left[I \; H_{S(2,2;v)} \right] \quad (19)$$

where $H_{S(2,2;v)}$ is the $v \times \binom{v}{2}$ incidence matrix of the $S(2,2;v)$ Steiner system and I is the $v \times v$ identity matrix. It is readily verified that $\mathcal{C}'_{S(2,2;v)}$ has length $n = v + \binom{v}{2}$, dimension $k = \binom{v}{2}$ and minimum dual distance $d^{\perp} = v$. Table I summarizes the application of Theorem 4 to this family of codes for $2 \leq v \leq 10$. Note the $\mathcal{C}'_{S(2,2;2)}$ and $\mathcal{C}'_{S(2,2;3)}$ meet Theorem 4 with equality while the remaining codes *nearly* meet the bound. $\mathcal{C}'_{S(2,2;2)}$ is the length 3 repetition code with parity check matrix:

$$H'_{S(2,2;2)} = \begin{bmatrix} 1\,0\,1 \\ 0\,1\,1 \end{bmatrix} \quad (20)$$

while $\mathcal{C}'_{S(2,2;3)}$ is a $[6,3,3]$ code with parity check matrix:

$$H'_{S(2,2;3)} = \begin{bmatrix} 1\,0\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1 \end{bmatrix}. \quad (21)$$

Code	$pd^{\perp}$	$\left\lfloor \sqrt{np(p-1)+\frac{n^2}{4}}+\frac{n}{2} \right\rfloor$
$[8,4,4]$	16	14
$[16,11,4]$	40	27
$[32,26,4]$	96	50
$[32,16,8]$	128	105
$[64,57,4]$	224	92
$[64,42,8]$	352	206
$[128,120,4]$	512	170
$[128,99,8]$	928	392
$[128,64,16]$	1024	785
$[256,219,8]$	2368	725
$[256,136,16]$	5952	1613
$[256,93,32]$	5216	2731
$[512,502,4]$	2048	562
$[512,466,8]$	5888	1316
$[512,382,16]$	8320	3197
$[512,256,32]$	8192	6042

TABLE II

APPLICATION OF THEOREM 4 TO REED-MULLER CODES.

V. APPLICATION OF THE MAIN RESULT

A. The Golay Code

The duals of both the $[23,12,7]$ binary Golay code and the $[24,12,8]$ extended binary Golay code have minimum distance 8 [12]. Neither code satisfies Theorem 4 and thus any Tanner graph for either code must contain 4-cycles.

B. Reed-Muller Codes

An $[n = 2^m, k, d = 2^{m-r}]$ RM code has dimension $k = \sum_{i=0}^{r} \binom{m}{i}$ and its dual has minimum distance 2^{r+1} [12]. Table II summarizes the application of Theorem 4 to those Reed-Muller codes with rate $R \geq 1/2$ and minimum distance $d > 2$ for $3 \leq m \leq 9$. Note that the existence of a 4-cycle-free Tanner graph is precluded by Theorem 4 for all of these codes. Note also that the $[256,93,32]$ code is an example of an $R < 1/2$ RM code for which a 4-cycle-free Tanner graph cannot exist.

C. Primitive BCH Codes

Table III summarizes the application of Theorem 4 to those $[n = 2^m - 1, k, d]$ primitve BCH codes with rate $R \geq 1/2$ for $3 \leq m \leq 8$ [12]. Determining $d^{\perp}$ is difficult when $m \geq 5$ and lower bounds have been used. The lower bounds labeled *, $'$ and † correspond to Sikel'nikov's bound [12], Theorem 5 of [15] and Schaub's bound [16] (as reported in [15]), respectively. Note that the existence of 4-cycle-free Tanner graphs is precluded by Theorem 4 for all of the codes in Table III. Note also that there exist a number of length 127 and 255 BCH codes with $R < 1/2$ without 4-cycle-free Tanner graphs.

D. Reed-Solomon Codes

Corollary 6 follows from Theorem 4.

Corollary 6: Let $\mathcal{C}$ be the binary image of a rate $1/2 \leq R \leq 1 - 2/n$, $[n = 2^m - 1, k, d = n - k + 1]$ RS code for $m \geq 4$. Then there exists no 4-cycle-free Tanner graph for $\mathcal{C}$.

Code	$d^\perp$	$pd^\perp$	$\left\lfloor \sqrt{np(p-1)+\frac{n^2}{4}}+\frac{n}{2} \right\rfloor$
$[7,4,3]$	4	12	10
$[15,11,3]$	8	32	22
$[31,26,3]$	$\geq 16^\star$	≥ 80	44
$[31,21,5]$	$\geq 8^\star$	≥ 80	70
$[31,16,7]$	$\geq 8^\star$	≥ 120	97
$[63,57,3]$	$\geq 32^\star$	≥ 192	85
$[63,51,5]$	$\geq 16^\star$	≥ 192	127
$[63,45,7]$	$\geq 16^\star$	≥ 288	173
$[63,39,9]$	$\geq 12'$	≥ 288	220
$[63,36,11]$	$\geq 12'$	≥ 324	244
$[127,120,3]$	$\geq 64^\dagger$	≥ 448	160
$[127,113,5]$	$\geq 56^\dagger$	≥ 784	228
$[127,106,7]$	$\geq 48^\dagger$	≥ 1008	303
$[127,99,9]$	$\geq 40^\dagger$	≥ 1120	379
$[127,92,11]$	$\geq 32^\dagger$	≥ 1120	457
$[127,85,13]$	$\geq 30^\dagger$	≥ 1260	535
$[127,78,15]$	$\geq 28^\dagger$	≥ 1372	613
$[127,71,19]$	$\geq 22^\dagger$	≥ 1232	692
$[127,64,21]$	$\geq 20^\dagger$	≥ 1260	770
$[127,57,23]$	$\geq 16^\dagger$	≥ 1120	849
$[127,50,27]$	$\geq 14^\dagger$	≥ 1078	927
$[127,43,31]$	$\geq 12^\dagger$	≥ 1008	1006
$[255,247,3]$	$\geq 128^\dagger$	≥ 1024	302
$[255,239,5]$	$\geq 112^\dagger$	≥ 1792	405
$[255,231,7]$	$\geq 96^\dagger$	≥ 2304	523
$[255,223,9]$	$\geq 88^\dagger$	≥ 2816	646
$[255,215,11]$	$\geq 64^\dagger$	≥ 2560	770
$[255,207,13]$	$\geq 64^\dagger$	≥ 3072	896
$[255,199,15]$	$\geq 60^\dagger$	≥ 3360	1022
$[255,191,17]$	$\geq 42^\dagger$	≥ 2688	1149
$[255,187,19]$	$\geq 42^\dagger$	≥ 2856	1212
$[255,179,21]$	$\geq 40^\dagger$	≥ 3040	1339
$[255,171,23]$	$\geq 32^\dagger$	≥ 2688	1466
$[255,163,25]$	$\geq 32^\dagger$	≥ 2944	1594
$[255,155,27]$	$\geq 32^\dagger$	≥ 3200	1721
$[255,147,29]$	$\geq 28^\dagger$	≥ 3024	1848
$[255,139,31]$	$\geq 26^\dagger$	≥ 3016	1976
$[255,131,37]$	$\geq 22^\dagger$	≥ 2728	2103
$[255,123,39]$	$\geq 22^\dagger$	≥ 2904	2231
$[255,115,43]$	$\geq 20^\dagger$	≥ 2800	2358
$[255,107,45]$	$\geq 20^\dagger$	≥ 2960	2486

TABLE III

APPLICATION OF THEOREM 4 TO PRIMITIVE BCH CODES.

Proof: $\mathcal{C}$ is an $[mn, mk, d' \geq d]$ binary code while $\mathcal{C}^\perp$ is an $[mn, m(n-k), d^\perp \geq k+1]$ binary code. It thus suffices to show that:

$$k+1 > \sqrt{mn\left(1-\frac{1}{m(n-k)}\right)+\frac{n^2}{4(n-k)^2}}+\frac{n}{2(n-k)} \tag{22}$$

or, equivalently:

$$g\left(n,R\right) = \left(Rn+1\right)^2\left(1-R\right) - Rn > mn\left(1-R\right) \tag{23}$$

where $R = k/n$. It is readily verified that $\partial^2 g(n,R)/\partial R^2 \leq 0$ for $1/2 \leq R \leq 1-2/n$ and it thus suffices to verify only that $g(n,R) > mn(1-R)$ at $R = 1/2$ and $R = 1-2/n$. When $m = 4$, $n = 15$, the lowest possible code rate that is greater or equal to $1/2$ is $8/15$ and:

$$g(15, 8/15) = 149/5 > 28 \tag{24}$$

More generally, since $n/4 > m$ when $m \geq 5$,

$$g(n, 1/2) = \frac{n^2}{8}+\frac{1}{2} > \frac{mn}{2}. \tag{25}$$

Finally, it is readily verified that for $m \geq 4$:

$$g(n, 1-2/n) = n-2+\frac{2}{n} > 2m. \tag{26}$$

□

The proof technique of Corollary 6 can be readily extended to show that if $m \geq 6$, then any Tanner graph corresponding to the binary image of a rate $1/3 \leq R \leq 1-2/n$, $[n = 2^m-1, k, d = n-k+1]$ RS code contains 4-cycles.

Corollary 6 does not extend to the binary image of length 7 Reed-Solomon codes. Specifically, evaluating Theorem 4 for the binary image of the $[7,5,3]$ RS code, $\mathcal{C}_{[7,5,3]}$, with $d^\perp \geq 6$ yields $m(n-k)d^\perp \geq 36$ and:

$$\left\lfloor \sqrt{m^2n(n-k)(m(n-k)-1)+\frac{m^2n^2}{4}}+\frac{mn}{2} \right\rfloor = 37. \tag{27}$$

The following alternate argument establishes that any Tanner graph representing the binary image of the $\mathcal{C}_{[7,5,3]}$ must indeed contain a 4-cycle.

Suppose a 4-cycle-free Tanner graph does exist for $\mathcal{C}_{[7,5,3]}$. The parity check matrix corresponding to this graph, $H_{[21,15,3]}$, has 21 columns and 6 rows. By Proposition 2, $H_{[21,15,3]}$ must contain at least 6 weight 1 columns. Since the minimum distance of the dual of $\mathcal{C}_{[7,5,3]}$ is at least 3, $H_{[21,15,3]}$ must contain exactly 6 weight 1 columns. Now consider the bipartite graph corresponding to the remaining 15 columns. Since the minimum distance of the dual of $\mathcal{C}_{[7,5,3]}$ is at least 6, this graph must contain at least 30 edges. On the other hand, Theorem 3 states that this graph contains at most 30 edges with equality if only if the graph corresponds to the incidence matrix of the Steiner system $S(2,2;6)$. We have thus shown that if a 4-cycle-Tanner graph exists for $\mathcal{C}_{[7,5,3]}$, then $\mathcal{C}_{[7,5,3]}$ must be isomorphic to $\mathcal{C}'_{S(2,2;6)}$ with parity check matrix:

$$H'_{S(2,2;6)} = \begin{bmatrix} 1&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&1&0&0&0 \\ 0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&0&1&1&0 \\ 0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&1 \end{bmatrix}.$$

MacWilliams and Sloane show that the code with parity check matrix $H'_{S(2,2;6)}$ can be interpreted as the binary image of a $[7,5,3]$ maximum distance separable (MDS) code over $GF(8)$ which is *not* a RS code ([12], Ch. 10.5). Thus, $\mathcal{C}'_{S(2,2;6)}$ is *not* isomorphic to a binary image of the $[7,5,3]$ RS code and no 4-cycle-free Tanner graph exists for $\mathcal{C}_{[7,5,3]}$.

VI. CONCLUSION

This work provides a necessary condition for the existence a 4-cycle-free Tanner graph corresponding to a given binary linear block code. It was thus shown that many well-known classical codes can not be represented by 4-cycle-free Tanner graphs. This result, however, does not preclude the existence of other simple 4-cycle-free graphical models for these codes.

For example, there exist 4-cycle-free graphical models for *all* binary linear block codes corresponding to generalized parity check matrices containing only binary hidden variables [6].

It is now known which codes cannot support cycle-free and 4-cycle-free Tanner graphs. In [13], Hoory provided an upper bound on the size of a bipartite graph with given girth g which reduces to that of Theorem 3 when $g = 6$. Hoory's bound thus provides a recipe for the development of a necessary condition for the existence of a $(g-2)$-cycle-free Tanner graph for a given code.

VII. Acknowledgments

The authors wish to acknowledge the help of the anonymous reviewers in clarifying the proof of Corollary 6.

References

[1] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Information Theory*, vol. IT-27, pp. 533–547, September 1981.

[2] D. J. C. MacKay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Information Theory*, vol. 45, pp. 399–431, February 1999.

[3] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Information Theory*, vol. 47, no. 7, pp. 2711–2736, November 2001.

[4] J.-L. Kim, U. N. Peled, I. Perepelitsa, V. Pless, and S. Friedland, "Explicit construction of families of LDPC codes with no 4-cycles," *IEEE Trans. Information Theory*, vol. 50, no. 10, pp. 2378–2388, October 2004.

[5] J. S. Yedidia, J. Chen, and M. C. Fossorier, "Generating code representations suitable for belief propagation decoding," in *Proc. Allerton Conf. Commun., Control, Comp.*, Monticello, IL, October 2002.

[6] S. Sankaranarayanan and B. Vasić, "Iterative decoding of linear block codes: A parity-check orthogonalization approach," *IEEE Trans. Information Theory*, vol. 51, no. 9, pp. 3347–3353, September 2005.

[7] T. Etzion, A. Trachtenberg, and A. Vardy, "Which codes have cycle-free Tanner graphs?" *IEEE Trans. Information Theory*, vol. 45, no. 6, pp. 2173–2181, September 1999.

[8] S. Neuwirth, "The size of bipartite graphs with girth eight," February 2001, arXiv:math/0102210.

[9] I. Reiman, "Über ein problem von K. Zarankiewicz," *Acta. Math. Acad. Sci. Hungary*, vol. 9, pp. 269–273, 1958.

[10] B. Bollobas, *Extremal Graph Theory*. New York, NY: Academic Press, 1978.

[11] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. Cambridge University Press, 1999.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1978.

[13] S. Hoory, "The size of bipartite graphs with a given girth," *J. Comb. Theory, Series B*, vol. 86, no. 2, pp. 215–220, 2002.

[14] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Communications*, vol. 51, no. 9, pp. 1413–1419, September 2003.

[15] D. Augot and F. L. vit Vehel, "Bounds on the minimum distance of the duals of BCH codes," *IEEE Trans. Information Theory*, vol. 42, no. 4, pp. 1257–1260, July 1996.

[16] T. Schaub, "A linear complexity approach to cyclic codes," Ph.D. dissertation, Swiss Federal Institute of Technology, Zurich, CH, 1998.