

The Trapping Redundancy of Linear Block Codes

Stefan Ländner[‡], Thorsten Hehn[‡], Olgica Milenkovic[†], and Johannes B. Huber[‡],

[‡]University of Erlangen-Nuremberg, Erlangen, Germany

[†]University of Illinois at Urbana-Champaign, Urbana, IL, USA

Abstract

We study a generalization of the notion of the stopping redundancy of linear block codes, termed the trapping redundancy. The trapping redundancy quantifies the relationship between the number of redundant rows in any parity-check matrix of a given code and the size of its smallest trapping set. Trapping sets with certain parameter sizes are known to cause error-floors in the performance curves of iterative belief propagation decoders, and it is therefore important to identify decoding matrices that avoid such sets. Bounds on the trapping redundancy are obtained using probabilistic methods, and the analysis covers both the class of general and elementary trapping sets. Numerical values for these bounds are computed for the [2640, 1320] Margulis code and a class of projective geometry codes, and compared with some new code-specific trapping set size estimates.

Index Terms Belief Propagation, LDPC Codes, Margulis Codes, Projective Geometry Codes, Trapping Redundancy, Trapping Sets.

I. INTRODUCTION

The performance of linear error-correcting codes under iterative decoding depends on the choice of the parity-check matrix of the code. More precisely, the error rate of a code is influenced by a class of combinatorial entities associated with the parity-check matrix, such as stopping [1] and trapping sets [2], [3]. Stopping and trapping sets are defined in terms of constraints on the weights of rows in the parity-check matrix induced by subsets of its columns. Certain such restrictions on the weight distributions of the rows can only be satisfied if the parity-check matrix of the code has a sufficiently large number of judiciously chosen rows. Thus, recent work focused on introducing redundant rows into parity-check matrices of a code in order to ensure that the size of their smallest stopping sets are sufficiently large or equal to the minimum distance of the code [4], [5], [6], [7]. Since adding redundant rows to the parity-check matrix increases the decoding complexity of the code, it is important to understand the inherent trade-off between the stopping distance and the smallest number of rows in a parity-check matrix that allows for this distance to be achieved. Several ideas for addressing these issues that exploit properties of orthogonal arrays and covering arrays [8] were described in [6], [4], and [9].

The contributions of this work are three-fold. First, we generalize the notion of the stopping redundancy for the case of trapping sets, and term this combinatorial number the *trapping redundancy*. Second, we describe a simple probabilistic method for upper-bounding the trapping redundancy of binary, linear block codes. Third, we present new deterministic analytical techniques for estimating the sizes of small trapping sets in the family of projective geometry (PG) codes and the Margulis [2640, 1320] code, and compare these estimates with the upper bound.

The paper is organized as follows. Section II provides relevant definitions and introduces the terminology used throughout the paper. Section III contains the main results – upper bounds on the trapping redundancy of codes. Section IV describes the relationship between trapping sets and arcs in PG codes. In the same section, numerical results for the trapping redundancy of the Margulis [2640, 1320] and the family of PG codes are compared with the results concerning arcs and elementary trapping sets in the Margulis family. Concluding remarks are given in Section V.

II. DEFINITIONS, BACKGROUND, AND TERMINOLOGY

We start by providing a description of trapping sets and elementary trapping sets, and then proceed to define the notion of a redundant parity-check matrix.

Part of this work was presented at WirelessComm 2005, Maui, Hawaii, USA, and at the CISS Conference, Princeton 2006. This work was supported in part by NSF Grant CCF-0514921 awarded to Olgica Milenkovic, by a research fellowship from the Institute for Information Transmission, University of Erlangen-Nuremberg, Erlangen, Germany, awarded to Stefan Ländner, and by a German Academic Exchange Service (DAAD) fellowship awarded to Thorsten Hehn.

A. Near-Codewords and Trapping Sets

The error-floor phenomenon was first described by MacKay and Postol in [2], who observed that the bit error rate curve of the [2640, 1320] Margulis code exhibits a sudden change of slope at signal-to-noise ratios approximately equal to 2.4 dB. This change of slope was attributed to the existence of *near-codewords* in the Tanner graphs of the Margulis code with a parity-check matrix \mathbf{H} described in [10]. Near codewords are error vectors \mathbf{y} of small weight with syndromes $\mathbf{s}(\mathbf{y}) \equiv \mathbf{H}\mathbf{y}$ that also have small weight. In his seminal paper [3], Richardson analyzed the effect of near-codewords on the performance of various classes of decoders and for a group of channels. He also introduced the notion of *trapping sets* to describe configurations in Tanner graphs of codes that cause failures of specific decoding schemes. There exist many different groups of trapping sets. For example, trapping sets of maximum likelihood decoders are the *codewords* of the code; trapping sets of iterative decoders used for messages transmitted over the binary erasure channel are stopping sets [1]. For the additive white Gaussian noise (AWGN) channel and belief propagation (BP) decoding, no simple characterization of trapping sets is known. Nevertheless, extensive computer simulations revealed that a large number of trapping sets for this channel/decoder combination can be described in a simple and precise setting. Henceforth, we use the notion "trapping set" to refer exclusively to sets of the form described below. To define trapping sets, we first introduce the notion of the restriction of a matrix.

Definition 2.1: For a given $m \times n$ matrix $\mathbf{H} = (H_{i,j})$ with $1 \leq i \leq m$, $1 \leq j \leq n$, the restriction of a set of t columns indexed by j_1, j_2, \dots, j_t is defined as an $m \times t$ subarray of \mathbf{H} consisting of the elements $H_{i,j}$, $1 \leq i \leq m$, $j = j_1, j_2, \dots, j_t$.

For a given linear $[n, k, d]$ code \mathcal{C} , with parity-check matrix \mathbf{H} and corresponding Tanner graph $\mathcal{G}(\mathbf{H})$, trapping sets \mathcal{T} are defined as follows.

Definition 2.2: An (a, b) trapping set $\mathcal{T}(a, b)$ is a collection of a variable nodes for which the subgraph in $\mathcal{G}(\mathbf{H})$ induced by $\mathcal{T}(a, b)$ and its neighbors contains $b \geq 0$ odd-degree check nodes¹. Equivalently, an (a, b) trapping set $\mathcal{T}(a, b)$ of \mathbf{H} is a set of a columns of \mathbf{H} which contain b odd-weight rows.

The class of trapping sets that exhibits the strongest influence on the performance of iterative decoders is the class of *elementary* trapping sets.

Definition 2.3: An elementary (a, b) trapping set is a trapping set for which all check nodes in the subgraph induced by \mathcal{T} and its neighbors have either degree one or two, and there are exactly b degree-one check nodes. Alternatively, an elementary (a, b) trapping set is a trapping set for which all non-zero rows in the restriction have either weight one or two, and exactly b rows have weight one.

For a fixed value of the parameter a (or b), the problem of finding the trapping set with smallest parameter b (or a) in a given parity-check matrix is NP-hard, and NP-hard to approximate [11]. Nevertheless, recent studies suggest that trapping sets most detrimental to the code performance have small (a, b) parameters, usually such that $b < a < d$, where d denotes the minimum distance of the code [3], [12]. We therefore focus our attention on trapping sets with $a \leq d/2$ only, and in particular, elementary trapping sets which represent the dominant class of small trapping sets [13].

B. Redundant Parity-Check Matrices

A Tanner graph of a linear $[n, k, d]$ code \mathcal{C} can be described by parity-check matrices of different forms. The rows of a standard parity-check matrix represent a basis of the subspace corresponding to \mathcal{C}^\perp , but for iterative decoding, such a matrix may not be adequate. This is due to the fact that standard matrices are either irregular or contain a large number of stopping and trapping sets [6]). Consequently, many parity-check matrices used for iterative decoding are redundant - i.e., they contain more than $n - k$ rows, although they have row-rank equal to $n - k$. Examples for the Binary Erasure Channel include the matrices described in [6], [14], [15].

Henceforth, we use the phrase *redundant parity-check matrix* to describe a parity-check matrix with row-rank $n - k$ and more than $n - k$ rows. Clearly, a redundant parity-check matrix contains at least one row that represents a linear combinations of other rows. Rows of this form are termed redundant rows. On the other hand, a full row-rank parity-check matrix of dimension $(n - k) \times n$ is simply referred to as a *parity-check matrix*. Redundant parity-check matrices are used to impose specific constraints on the structure of their corresponding Tanner graphs. As was shown in [16], even one judiciously chosen redundant row can be used to lower the error floor of the Margulis code in an adaptive manner. This is achieved in terms of rendering the structure of a selected small trapping set so as to increase

¹The case $b = 0$ corresponds to codewords. Henceforth, we deal with the case $b > 0$ only.

the number of its corresponding unsatisfied parity-checks. In what follows, we consider the more general problem of determining the smallest number of redundant rows needed to achieve the same effect for a whole class of trapping sets. In this context, our results can be seen as a generalization of the findings in [6] for the case of trapping sets.

An analytical study of the trapping redundancy is presented in the following section.

III. THE TRAPPING REDUNDANCY: A PROBABILISTIC APPROACH

We investigate next the fundamental theoretical trade-offs between the number of rows in a redundant parity-check matrix of a code and the size of its smallest trapping sets from a given class. In all our subsequent derivations, we make use of the following definition.

Definition 3.1: ([8, p. 5]) An orthogonal array \mathcal{A} of strength t is an array of dimensions $m \times n$ such that every $m \times t$ subarray contains *each* possible t -tuple *the same number of times*. The codewords of an $[n, k, d]$ linear code \mathcal{C} form an orthogonal array of dimension $2^k \times n$ and strength $d^\perp - 1$, where d^\perp denotes the dual distance of \mathcal{C} . Note that if \mathcal{A} is an array of strength t , then \mathcal{A} is also an orthogonal array of strength s , for all integers $s < t$.

Let $T_H(a, b)$ denote the number of (a, b) trapping sets in the parity-check matrix \mathbf{H} . We have the following characterization for $T_H(a, b)$ corresponding to a matrix \mathbf{H} that consists of *all* codewords of the dual code.

Proposition 3.2: Let \mathbf{H} consist of all 2^{n-k} codewords of the dual of an $[n, k, d]$ linear code \mathcal{C} , for $n - k \geq 1$. Then $T_H(a, b) = 0$ for all pairs (a, b) such that $1 \leq a \leq d - 1$, and $b \neq 2^{n-k-1}$.

Proposition 3.2 shows that a parity-check matrix that consists of all codewords of the dual code cannot contain trapping sets with $1 \leq a \leq d - 1$ variables with less than or more than 2^{n-k-1} checks connected to them an odd number of times. This is a direct consequence of the fact that \mathbf{H} in this case represents an orthogonal array, so that each set of $1 \leq a \leq d - 1$ columns of \mathbf{H} contains each a -tuple the same number of times. Consequently, there are 2^{n-k-1} rows in the restriction of the a columns that have even weight, and 2^{n-k-1} rows that have odd weight.

However, it is of much larger importance to determine if there exist parity-check matrices with a number of rows significantly smaller than 2^{n-k} that are free of trapping sets with fixed parameters (a, s) , for all $s < b$. For this purpose, we introduce the notion of the (a, b) trapping redundancy of a code.

Definition 3.3: The (a, b) trapping redundancy of an $[n, k, d]$ linear code \mathcal{C} is the smallest number of rows m of a (redundant) parity-check matrix which does not contain trapping sets with parameters (a, s) , $1 \leq s < b$.

Theorem 3.4: Let \mathcal{C} be an $[n, k, d]$ code and \mathcal{C}^\perp its dual. Let $\mathcal{M}_{\mathcal{C}}(m)$ be the ensemble of all $m \times n$ matrices with rows chosen independently at random and with replacement from the set of 2^{n-k} codewords of \mathcal{C}^\perp . Furthermore, let $1 \leq a \leq \lfloor (d-1)/2 \rfloor$ be fixed and let $\Theta(a, b)$ be the number of trapping sets with parameters (a, s) , $1 \leq s < b$, in a randomly chosen matrix from $\mathcal{M}_{\mathcal{C}}(m)$. If

$$e \left(\binom{n}{a} - \binom{n-a}{a} \right) \left(\frac{1}{2} \right)^m \sum_{j=0}^{b-1} \binom{m}{j} \leq 1, \quad (1)$$

then $P\{\Theta(a, b) = 0\} > 0$. Consequently, if m satisfies (1), then there exists a parity-check matrix of \mathcal{C} with not more than $m + n - k - 2$ rows and $\Theta(a, b) = 0$.

Note that $m + n - k - 2$, for any m satisfying (1), represents an upper bound on the trapping redundancy of the code.

Proof: The proof of the claimed result is based on Lovász Local Lemma (LLL), stated below.

Lemma 3.5: [17] Let E_1, E_2, \dots, E_N be a set of events in an arbitrary probability space. Suppose that each event E_i is independent of all other events E_j , except for at most τ of them, and that $P\{E_i\} \leq p$ for all $1 \leq i \leq N$. If

$$e p (\tau + 1) \leq 1, \quad (2)$$

then $P\{\bigcap_{i=1}^N \overline{E_i}\} > 0$.

Let E_i be the event that the restriction of the i -th collection (out of $\binom{n}{a}$) of a columns from a randomly chosen matrix in $\mathcal{M}_{\mathcal{C}}(m)$ contains fewer than b odd rows. Then

$$P\{E_i\} = \left(\frac{1}{2} \right)^m \sum_{j=0}^{b-1} \binom{m}{j}. \quad (3)$$

Equation (3) follows from the fact that the codewords of the dual code form an orthogonal array of strength $d - 1$, and that consequently, even and odd weight rows in the restriction are equally likely. This is true independent of the

choice of a , provided that $1 \leq a \leq \lfloor (d-1)/2 \rfloor$. The restriction on the number of columns a to lie within a given range is imposed in order to ensure that any two events E_i and E_j are independent as long as they do not share one or more column indices. In the above setting, $P\{\bigcap \overline{E_i}\}$ denotes the probability that the randomly chosen matrix is free of trapping sets with parameters (a, s) , for all $1 \leq s < b$. In order to complete the proof, it suffices to observe that the dependence number of the events E_i equals

$$\tau + 1 = \sum_{l=1}^a \binom{a}{l} \binom{n-a}{a-l} = \binom{n}{a} - \binom{n-a}{a}, \quad (4)$$

The first equation in the above expression is a consequence of the fact that two collections of a columns are dependent if and only if they share at least one column. In other words, if one collection of a columns is fixed, another collection of the same size is independent of it if its columns are chosen from the remaining $n-a$ columns. The second equality arises from invoking the Vandermonde convolution formula,

$$\sum_l \binom{r}{t+l} \binom{s}{u-l} = \binom{r+s}{t+u},$$

where r, t, s, u denote non-negative integers.

In the worst case, additional $n-k-2$ rows may be required to make the randomly chosen matrix have full-row rank $n-k$. Note that appending $n-k-2$ rows to the selected set of m rows can only increase the number of odd weight rows in the projections, and hence cannot reduce the minimum trapping set size of the matrix. This completes the proof of the result. ■

Although Theorem 3.4 ensures the existence of at least one matrix in $\mathcal{M}_{\mathcal{C}}(m)$ that is free of trapping sets of given parameters, the actual probability of selecting such a matrix may be very small. It is therefore of interest to identify values of the parameter m for which the probability of drawing a matrix of the desired form from the ensemble $\mathcal{M}_{\mathcal{C}}(m)$ is close to one.

Theorem 3.6: For a linear code \mathcal{C} , let $\Theta(a, b)$ be the number of trapping sets with parameters (a, s) , $1 \leq s \leq b \leq m$, $1 \leq a \leq \lfloor (d-1)/2 \rfloor$, that exist in an $m \times n$ array from the $\mathcal{M}_{\mathcal{C}}(m)$ ensemble. If

$$\left(\frac{1}{2}\right)^m \sum_{j=0}^{b-1} \binom{m}{j} \leq \frac{\epsilon}{\binom{n}{a}} \left(1 - \frac{\epsilon}{\binom{n}{a}}\right)^{\tau}, \quad (5)$$

where τ is given by Equation (4), then $P\{\Theta(a, b) = 0\} > 1 - \epsilon$.

Consequently, if m satisfies (5), then one can find with high probability a (redundant) parity-check matrix for \mathcal{C} with not more than $m+n-k-2$ rows and $\Theta(a, b) = 0$.

Proof: The result in Equation (5) is obtained by using the high-probability variation of LLL, stated below.

Lemma 3.7: [17] Let E_1, E_2, \dots, E_N be a set of events in an arbitrary probability space, and let $0 < \epsilon < 1$. Suppose that each event E_i is independent of all other events E_j , except for at most τ of them. If

$$P\{E_i\} \leq \frac{\epsilon}{N} \left(1 - \frac{\epsilon}{N}\right)^{\tau}, \quad 1 \leq i \leq N,$$

then $P\{\bigcap_{i=1}^N \overline{E_i}\} > 1 - \epsilon$.

To prove the theorem, let E_i , $1 \leq i \leq N$ denote the event that the i -th collection of a columns contains at least b rows of odd weight. Replace the expression for $P\{E_i\}$ in the above result by the right hand side of Equation (3) and use the formula for τ stated in Equation (4). ■

Let us characterize next the trapping redundancy pertaining to elementary trapping sets only.

Theorem 3.8: Let \mathcal{C} be an $[n, k, d]$ code and \mathcal{C}^{\perp} its dual. Let $\mathcal{M}_{\mathcal{C}}(m)$ be the ensemble of all $m \times n$ matrices with rows chosen independently and at random, with replacement, from the set of 2^{n-k} codewords of \mathcal{C}^{\perp} . Furthermore, let $1 \leq a \leq \lfloor (d-1)/2 \rfloor$ be fixed and let $\Theta_e(a, b)$ be the number of elementary trapping sets with parameters (a, s) , $1 \leq s < b$, in a randomly chosen matrix of $\mathcal{M}_{\mathcal{C}}(m)$. If

$$e \left(\binom{n}{a} - \binom{n-a}{a} \right) \cdot \frac{1}{2^{(a+1) \cdot m}} \cdot \sum_{j=0}^{b-1} \left[\binom{m}{j} 2^j a^j \cdot (a^2 - a + 2)^{m-j} \right] \leq 1, \quad (6)$$

then $P\{\Theta_e(a, b) = 0\} > 0$. Consequently, if m satisfies (6), then there exists a parity-check matrix of \mathcal{C} with no more than $m + n - k - a$ rows and $\Theta_e(a, b) = 0$.

Similarly to the case of general trapping sets, we call the smallest number of rows in any (redundant) parity-check matrix of \mathcal{C} for which $\Theta_e(a, b) = 0$ the (a, b) *elementary trapping redundancy* of \mathcal{C} . Any $m + n - k - a$, with m satisfying (6) represents an upper bound on the elementary trapping redundancy.

Proof: The proof follows along the same lines of the proof of Theorem 3.4. Let E_i be the event that the restriction of the i -th collection of a columns from a randomly chosen matrix in $\mathcal{M}_\mathcal{C}(m)$ contains only rows of weight at most two. Among these rows, fewer than b rows are required to have weight one.

Let W_ω denote the number of rows of weight ω in the restriction of a columns. Then

$$\begin{aligned} P\{E_i\} &= \sum_{j=0}^{b-1} P\{W_1 = j, (W_0 + W_2) = (m - j)\} \\ &= \sum_{j=0}^{b-1} \left[\binom{m}{j} \left(\frac{a}{2^a}\right)^j \cdot \left(\frac{a^2 - a + 2}{2^{a+1}}\right)^{m-j} \right] \\ &= \frac{1}{2^{(a+1) \cdot m}} \cdot \sum_{j=0}^{b-1} \left[\binom{m}{j} 2^j a^j \cdot (a^2 - a + 2)^{m-j} \right], \end{aligned} \quad (7)$$

where the second equation follows from

$$\begin{aligned} P\{W_1 = j, (W_0 + W_2) = (m - j)\} &= \\ &= \binom{m}{j} \left(\frac{\binom{a}{1}}{2^a}\right)^j \sum_{s=0}^{m-j} \binom{m-j}{s} \left(\frac{1}{2^a}\right)^s \left(\frac{\binom{a}{2}}{2^a}\right)^{m-j-s}. \end{aligned}$$

Equation (7) follows from the observation that the codewords of the dual code form an orthogonal array of strength $d - 1$, and that therefore all 1 -, $\binom{a}{1}$ -, and $\binom{a}{2}$ -collections of rows of weight 0, 1, and 2, are equally likely, respectively. \blacksquare

Similarly, based on the high-probability variation of LLL, a bound can be derived on the number of rows necessary to guarantee that a randomly chosen matrix has no elementary trapping sets up to a given size with a certain probability $1 - \epsilon$. The following theorem is an analogue of Theorem 3.6 for the case of elementary trapping sets, i.e. for $P\{E_i\}$ as defined by Equation (7).

Theorem 3.9: For a linear code \mathcal{C} , let $\Theta_e(a, b)$ be the number of elementary trapping sets with parameters (a, s) , $1 \leq s \leq b \leq m$, $1 \leq a \leq \lfloor (d - 1)/2 \rfloor$, in an $m \times n$ array from the $\mathcal{M}_\mathcal{C}(m)$ ensemble. If

$$\begin{aligned} \frac{1}{2^{(a+1) \cdot m}} \sum_{j=0}^{b-1} \left[\binom{m}{j} 2^j a^j \cdot (a^2 - a + 2)^{m-j} \right] \\ \leq \frac{\epsilon}{\binom{n}{a}} \left(1 - \frac{\epsilon}{\binom{n}{a}} \right)^\tau, \end{aligned} \quad (8)$$

where τ is given in Equation (4), then $P\{\Theta_e(a, b) = 0\} > 1 - \epsilon$.

For m satisfying (8), there exists a parity-check matrix of \mathcal{C} with no more than $m + n - k - a$ rows and $\Theta_e(a, b) = 0$. If E_i , $1 \leq i \leq N$ is used to denote the event that the i -th collection of a columns contains only rows of weight at most two, and at least b rows of weight one, then the result represents a straightforward application of the high-probability variation of LLL. The proof is therefore omitted.

A. Asymptotic Formulas

Although there is no explicit formula for m as defined by Equations (5) and (6) that holds for all possible parameter values, such a formula can be found in the asymptotic regime ($m, n \rightarrow \infty$, $a = O(m)$, $b = O(m)$), by using the following results from [18, p. 240] and [19].

Let

$$A_m = \sum_{0 \leq i \leq \lambda m} \binom{m}{i},$$

where $0 \leq \lambda \leq 1$, and $b = \lambda m + 1$. Since small values for the parameter b are of special interest, assume that $\lambda < 1/2$. In this case we have

$$A_m \simeq \binom{m}{\lfloor \lambda m \rfloor} \cdot \frac{1}{1 - \frac{\lambda}{1-\lambda}},$$

where $A_m \simeq B_m$ denotes $\lim_{m \rightarrow \infty} A_m/B_m = 1$.

For $b < m/2 + 1$, with $b = \lfloor \lambda m \rfloor + 1$, and $\lambda < 1/2$, Equation (6) reduces to

$$e \left(\binom{n}{a} - \binom{n-a}{a} \right) \cdot \left(\frac{1}{2} \right)^m \cdot \binom{m}{\lfloor \lambda m \rfloor} \cdot \frac{1}{1 - \frac{\lambda}{1-\lambda}} \lesssim 1.$$

By invoking the well known asymptotic formula

$$\text{ld} \binom{m}{\lfloor \lambda m \rfloor} \simeq m H_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right), \quad (9)$$

where $H_2(\cdot)$ denotes Shannon's binary entropy function and $\text{ld}(\cdot)$ represents the logarithm with base two, it follows that $m \leq m'$ with

$$m' \simeq \frac{\text{ld} \left(e \left(\binom{n}{a} - \binom{n-a}{a} \right) \right) + \text{ld} \left(\frac{1}{1 - \frac{\lambda}{1-\lambda}} \right)}{1 - H_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right)}. \quad (10)$$

Also for $b < m/2 + 1$, with $b = \lfloor \lambda m \rfloor + 1$, and $\lambda < 1/2$, the high-probability variation of LLL given in Equation (5) reduces to

$$\left(\frac{1}{2} \right)^m \binom{m}{\lfloor \lambda m \rfloor} \frac{1}{1 - \frac{\lambda}{1-\lambda}} \lesssim \frac{\epsilon}{\binom{n}{a}} \left(1 - \frac{\epsilon}{\binom{n}{a}} \right)^{\left(\binom{n}{a} - \binom{n-a}{a} - 1 \right)}. \quad (11)$$

Applying again Equation (9) results in $m \leq m'$ with

$$m' \simeq \frac{1}{H_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right) - 1} \left[\text{ld} \left(1 - \frac{\lambda}{1-\lambda} \right) + \left(\binom{n}{a} - \binom{n-a}{a} - 1 \right) \text{ld} \left(\frac{\epsilon}{\binom{n}{a}} \left(1 - \frac{\epsilon}{\binom{n}{a}} \right) \right) \right]. \quad (12)$$

To find an explicit formula for m given by (6), we use the following asymptotic result taken from [19]

$$\sum_{k=N}^{rN} \binom{rN}{k} p^k q^{rN-k} \simeq \phi(p^{-1}) \binom{rN}{N} p^N q^{rN-N}, \quad (13)$$

where $p, q > 0$, $p + q = 1$, $r > 1$, N is an integer, and $\phi(y) = \frac{y-1}{y-r}$. By observing that

$$\sum_{j=0}^{b-1} \binom{m}{j} 2^j a^j (a^2 - a + 2)^{m-j} = (a^2 + a + 2)^m.$$

$$\sum_{u=m-b+1}^m \binom{m}{u} \left(\frac{2a}{a^2 + a + 2} \right)^{m-u} \left(\frac{a^2 - a + 2}{a^2 + a + 2} \right)^u,$$

it follows that

$$\sum_{j=0}^{b-1} \binom{m}{j} 2^j a^j (a^2 - a + 2)^{m-j} \simeq \phi \left(\frac{a^2 + a + 2}{a^2 - a + 2} \right) \cdot \binom{m}{m-b+1} \left(\frac{2a}{a^2 - a + 2} \right)^{b-1} (a^2 - a + 2)^m.$$

Using the above expression, Equation (6) reduces to

$$e \left(\binom{n}{a} - \binom{n-a}{a} \right) \cdot \phi \left(\frac{a^2 + a + 2}{a^2 - a + 2} \right) \binom{m}{m-b+1} \cdot \left(\frac{2a}{a^2 - a + 2} \right)^{b-1} \left(\frac{a^2 - a + 2}{2^{a+1}} \right)^m \lesssim 1.$$

This leads to a bound $m \leq m'$ with

$$m' \simeq \frac{-\text{ld} \left(e \left(\binom{n}{a} - \binom{n-a}{a} \right) \cdot \phi \left(\frac{a^2 + a + 2}{a^2 - a + 2} \right) \right)}{\text{H}_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right) + \text{ld}(a^2 - a + 2) - (a + 1)} - \frac{(b-1) \cdot \text{ld} \left(\frac{2a}{a^2 - a + 2} \right)}{\text{H}_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right) + \text{ld}(a^2 - a + 2) - (a + 1)}, \quad (14)$$

where we used Equation (9) to rewrite the right hand side of the above expression. Similarly, we obtain for the high-probability variation of LLL and for elementary trapping sets, i.e. as a consequence of Equation (8) we again obtain $m \leq m'$ with

$$m' \simeq \frac{\left(\binom{n}{a} - \binom{n-a}{a} - 1 \right) \cdot \text{ld} \left(\frac{\epsilon}{\binom{n}{a}} \left(1 - \frac{\epsilon}{\binom{n}{a}} \right) \right)}{\text{H}_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right) + \text{ld}(a^2 - a + 2) - (a + 1)} - \frac{\text{ld} \left(\phi \left(\frac{a^2 + a + 2}{a^2 - a + 2} \right) \right) - (b-1) \cdot \text{ld} \left(\frac{2a}{a^2 - a + 2} \right)}{\text{H}_2 \left(\frac{\lfloor \lambda m \rfloor}{m} \right) + \text{ld}(a^2 - a + 2) - (a + 1)}. \quad (15)$$

Remark: It should be pointed out that the matrices from the ensemble $\mathcal{M}_{\mathcal{C}}(m)$, for large m , may have highly non-uniform row and column weights. The variable and check node degrees of their corresponding Tanner graphs may be very large, leading to the emergence of short cycles. It is therefore of importance to compare the derived bounds with some benchmark values, the latter corresponding to redundant matrices that are known to have a small number of redundant rows, no short cycles, as well as no small trapping sets. Two such examples, including the aforementioned Margulis and projective geometry codes, are discussed in the next section.

IV. TRAPPING REDUNDANCY: ANALYTICAL COMPARISONS

We compare the probabilistic upper bounds derived in Section III with results obtained from a case-study of the Margulis code and the class of projective geometry codes. The goal of this comparison is to both assess the tightness of the bounds of Section III and to illustrate that structured LDPC codes with inherent row-redundancy may avoid both small trapping sets as well as short cycles in their Tanner graphs.

A. The [2640, 1320] Margulis Code

Numerical values of the trapping redundancy values derived in Section III for the [2640, 1320] Margulis code are listed in Tables I and II. The labels *LLL (std)*, *LLL (hp)* refer to the LLL- and high-probability variation of the LLL-result, respectively. The symbol m denotes the number of rows required by the LLL lemmas, while \hat{m} refers to the number of rows needed to make the redundant matrix of full rank.

The full-rank 1320×2640 parity-check matrix \mathbf{H} of the Margulis code, constructed in the standard manner [20], contains no cycles of size smaller than eight, but includes a large number of $(12, 4)$ and $(14, 4)$ elementary trapping sets [3], [12]. The LLL-based bounds reveal that there exists a matrix with at most 1342 rows that does not contain $(12, s)$ and $(14, s)$ elementary trapping sets, with $s < 5$.

It can also be seen from Table I that there exists a matrix of row-rank $n - k$ with $\hat{m} = 1393$ rows that is free of trapping sets of size $(6, s)$, $s < 5$. However, for a parity-check matrix free of elementary trapping sets of the same parameters, Table II shows that only $\hat{m} = 1346$ rows are needed.

TS size		\mathbf{H}	LLL (std)		LLL (hp) $\epsilon = 0.01$		LLL (hp) $\epsilon = 10^{-20}$	
a	b	$(n - k) \times n$	m	\hat{m}	m	\hat{m}	m	\hat{m}
6	5	1320×2640	75	1393	87	1405	150	1465
8	5	1320×2640	94	1412	105	1423	167	1485
12	5	1320×2640	129	1447	138	1456	200	1518
14	5	1320×2640	145	1463	154	1472	216	1534

TABLE I

UPPER BOUNDS ON THE (a, b) TRAPPING REDUNDANCY OF THE MARGULIS CODE.

TS size		\mathbf{H}	LLL (std)		LLL (hp) $\epsilon = 0.01$		LLL (hp) $\epsilon = 10^{-20}$	
a	b	$(n - k) \times n$	m	\hat{m}	m	\hat{m}	m	\hat{m}
6	5	1320×2640	32	1346	39	1353	70	1384
8	5	1320×2640	26	1338	29	1341	49	1361
12	5	1320×2640	19	1327	20	1328	31	1339
14	5	1320×2640	17	1323	18	1324	26	1332

TABLE II

UPPER BOUNDS ON THE (a, b) ELEMENTARY TRAPPING REDUNDANCY OF THE MARGULIS CODE.

B. Projective Geometry Codes

Projective geometry codes are linear block codes with many well known combinatorial parameters and properties. As will be shown next, it is also straightforward to characterize a large sub-family of trapping sets in these codes.

We start our derivations by introducing the relevant terminology.

Definition 4.1: [21] A finite projective geometry $\text{PG}(M, q)$ of dimension M and over a finite field $\text{GF}(q)$, for some prime power q , is a set of points and subsets thereof, called lines. The following axioms hold for the points and lines of a finite geometry:

- Two distinct points determine a unique line.
- Every line consists of more than two points.
- For every pair of distinct lines L_1 and L_2 , intersecting at some point r , there exist two pairs of points $(p_1, q_1) \in L_1$ and $(p_2, q_2) \in L_2$ that differ from r , such that the lines determined by (p_1, p_2) and (q_1, q_2) intersect as well.
- For each point and for each line, there exist at least two lines and two points that are not incident to them, respectively.

The points of a projective geometry $\text{PG}(M, q)$ can be represented by non-zero $(M + 1)$ -tuples $(a_0, a_1, a_2, \dots, a_M)$ such that $a_i \in \text{GF}(q)$. Points of the form $(a_0, a_1, a_2, \dots, a_M)$ and $(\delta a_0, \delta a_1, \delta a_2, \dots, \delta a_M)$, $\delta \in \text{GF}(q) \setminus \{0\}$, are considered equivalent. A line through two distinct points $(a_0, a_1, a_2, \dots, a_M)$ and $(b_0, b_1, b_2, \dots, b_M)$ consists of all points that

can be expressed as $(\alpha a_0 + \beta b_0, \dots, \alpha a_M + \beta b_M)$, where $\alpha, \beta \in \text{GF}(q)$ and are not both simultaneously zero. Consequently, a projective geometry $\text{PG}(M, q)$ has $(q^{M+1} - 1)/(q - 1)$ points, and each line in the geometry contains $q + 1$ points. The number of lines in a projective geometry is given by

$$(q^M + \dots + q + 1)(q^{M-1} + \dots + q + 1)/(q + 1). \quad (16)$$

It is straightforward to see that the number of lines and points coincide for $M = 2$, as $(q^2 + q + 1) = (q^3 - 1)/(q - 1)$ holds.

A type-I projective geometry code is defined in terms of a parity-check matrix representing the *line-point* incidence matrix of a projective geometry $\text{PG}(M, q)$ [22]. Throughout the remainder of the paper, we consider projective plane codes, $M = 2$, and codes based on projective geometries with $M = 3$ only.

Definition 4.2: An s -arc in $\text{PG}(2, q)$ is a collection of s points such that no three of them are collinear. The lines incident to an s -arc \mathcal{K} are either unisecants (they intersect the arc in exactly one point) or bisecants (they intersect the arc in exactly two points). Similarly, an s -cap in $\text{PG}(3, q)$ is a set of s points, no three of which are collinear. The following results are taken from [23, Ch. 8] and [24, Ch. 16].

Lemma 4.3: Let n_1 and n_2 denote the number of unisecants and bisecants of an s -arc \mathcal{K} in $\text{PG}(2, q)$, respectively. Then

$$n_1 = s(q + 2 - s), \quad \text{and} \quad n_2 = \frac{1}{2}s(s - 1). \quad (17)$$

Similarly, for an s -cap \mathcal{K} in $\text{PG}(3, q)$ it holds that

$$n_1 = s(q^2 + q + 2 - s), \quad (18)$$

where n_1 denotes the number of unisecants of \mathcal{K} .

Lemma 4.4: The largest arc in $\text{PG}(2, q)$ contains at most $q + 2$ points, for q even, and $q + 1$ points, for q odd. Arcs with $s = q + 1$ and $s = q + 2$ are called ovals and hyperovals, respectively. The size of any s -cap in $\text{PG}(3, q)$ satisfies $s \leq q^2 + 1$. For $q > 2$, a $(q^2 + 1)$ -cap is called an ovaloid.

The results of Lemma 4.3 and 4.4 can be used to establish the following simple results regarding trapping sets in the Tanner graph of type-I projective geometry codes. Note that all stated results restrict the parameter sets for which trapping sets may potentially exist, although they do not imply the existence of such sets.

Corollary 4.5: All elementary trapping sets of a $\text{PG}(2, q)$, type-I, projective geometry code have parameters $(s, s(q + 2 - s))$. Consequently, the number of degree-one check nodes of such trapping sets for q odd is necessarily larger than or equal to the number of variables in the trapping set. For even values of q , an exception to the aforementioned rule is a hyperoval, which represents a codeword. The trapping sets with the smallest ratio b/a have parameters $(q + 1, q + 1)$ (q odd) and $(q + 2, 0)$ (q even), respectively, and those with the largest parameters $(3, 3(q - 1))$, since $s \geq 3$.

Proof: Note that the parity-check matrix \mathbf{H} of a $\text{PG}(2, q)$ code is the point-line incidence matrix of the underlying PG. Arcs correspond to a collection of columns, the restriction of which has rows of weight at most two only, and exactly n_1 of these columns have weight one. This is equivalent to the definition of an (s, n_1) trapping set. Hyperovals have $s = q + 2$ points and $n_1 = (q + 2) \cdot (q + 2 - (q + 2)) = 0$ unisecants, and therefore correspond to $(q + 2, 0)$ trapping sets, which are codewords. ■

Corollary 4.6: All elementary trapping sets of a $\text{PG}(3, q)$, type-I projective geometry code have parameters $(s, s(q^2 + q + 2 - s))$. Provided that the PG contains an s -arc with $n_1 = s(q^2 + q + 2 - s)$, the trapping sets with the smallest and largest ratio b/a have parameters $(q^2 + 1, (q^2 + 1)(q + 1))$ and $(3, 3(q^2 + q - 1))$.

Proof: The proof follows along the lines of the proof of Corollary 4.5, with $n_1 = s(q^2 + q + 2 - s)$ for $\text{PG}(3, q)$. ■

A complete classification of trapping sets in projective geometry codes is probably an impossible task. This is due to the fact that very little is known about the number and existence of arcs and caps of different sizes in projective spaces. One aspect of this problem that is better understood is the existence and enumeration of *complete arcs* (and *caps*) - i.e. arcs and caps not contained in any larger arc or cap. The interested reader is referred to [23], [24] for more information regarding the problem of complete arc enumeration.

We compare next the upper bounds derived in Section III with the study described in this section. We consider elementary trapping sets only.

In order to apply the results of the lemmas in this section, one has to consider a parity-check matrix that represents a complete point-line incidence structure [22]. For this reason, the standard parity-check matrices of PG codes contain exactly n rows, and are therefore redundant.

Table III list the number of rows required to avoid elementary trapping sets of a given size, computed according to LLL and its high-probability variation. The values for \hat{m} are derived using the minimum distance and the rank results taken from [22].

Observe that Table III indicates that there exists a parity-check matrix for the PG(2, 16) code with at most 173 rows and no $(3, s)$, $s < 45$, elementary trapping sets. This is significantly less than $n = 273$. On the other hand, the LLL bound states that at most 516 rows are required to eliminate $(16, s)$, $s < 288$ trapping sets, a significantly larger number than n .

Code	TS size		compl. H	min. H	LLL (std)		LLL (hp) $\epsilon = 0.01$		LLL (hp) $\epsilon = 10^{-20}$	
	a	b	$\overline{m} = n$	$\underline{m} = n - k$	m	\hat{m}	m	\hat{m}	m	\hat{m}
PG(2, 16)	3	45	273	82	94	173	125	204	228	307
PG(2, 16)	8	80	273	82	80	154	80	154	80	154
PG(2, 32)	3	93	1057	244	115	356	178	419	338	579
PG(2, 32)	16	288	1057	244	288	516	288	516	288	516

TABLE III
UPPER BOUNDS ON THE (a, b) ELEMENTARY TRAPPING REDUNDANCY OF PG CODES.

V. CONCLUSIONS

We introduced the notion of the (a, b) trapping redundancy of a code, representing the smallest number of rows in any parity-check matrix of the code that avoids (a, s) trapping sets with $1 \leq s < b$. Upper bounds on these combinatorial numbers were derived using Lovász Local Lemma and variations thereof. Also presented were numerical results for the trapping redundancy of the Margulis [2640, 1320] and type-I PG codes.

REFERENCES

- [1] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. on Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.
- [2] D. MacKay and M. Postol, "Weaknesses of Margulis and Ramanujan-Margulis low-density parity-check codes," *Electronic Notes in Theoretical Computer Science*, vol. 74, 2003. [Online]. Available: <http://www.cs.toronto.edu/~mackay/margulis.pdf>
- [3] T. Richardson, "Error-floors of LDPC codes," in *Proceedings of the 41st Annual Allerton Conference on Communication, Control and Computing*, Sept. 2003, pp. 1426–1435.
- [4] J. Han and P. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. on Inform. Theory*, vol. 53, no. 1, pp. 90–104, January 2007.
- [5] R. Koetter, W.-C. W. Li, P. Vontobel, and J. Walker, "Characterizations of pseudo-codewords of ldpc codes," *accepted for Advances in Mathematics*, August 2006.
- [6] M. Schwartz and A. Vardy, "On the stopping distance and stopping redundancy of codes," *IEEE Trans. on Inform. Theory*, vol. 52, no. 3, pp. 922–932, March 2006.
- [7] J. Weber and K. Abdel-Ghaffar, "Stopping and dead-end set enumerators for binary Hamming codes," in *Proceedings of the Twenty-sixth Symp. on Inform. Theory in the Benelux*, Brussels, Belgium, May 2005, pp. 165–172.
- [8] A. Hedayat, N. Sloane, and J. Stufken, *Orthogonal Arrays: Theory and Applications*. New York: Springer Verlag, 1999.
- [9] O. Milenkovic, E. Soljanin, and P. Whiting, "Stopping and trapping sets in generalized covering arrays," in *Proceedings of the 40th annual Conference on Information Sciences and Systems (CISS)*, Princeton University, Princeton, New Jersey, USA, March 2006, pp. 259–264.
- [10] J. Rosenthal and P. Vontobel, "Constructions of regular and irregular LDPC codes using Ramanujan graphs and ideas from Margulis," in *Proc. Int. Symp. Inform. Theory (ISIT'01)*, Washington D.C., June 24–29 2001, p. 4.
- [11] A. McGregor and O. Milenkovic, "On the hardness of approximating stopping and trapping sets in LDPC codes," in *Proceedings of the IEEE Information Theory Workshop (ITW 2007)*, Lake Tahoe, September 2007.
- [12] S. Laendner and O. Milenkovic, "Algorithmic and combinatorial analysis of trapping sets in structured LDPC codes," in *Proceedings of the International Conference on Wireless Networks, Communications, and Mobile Computing (WirelessComm2005)*, Maui, Hawaii, June 2005.
- [13] O. Milenkovic, E. Soljanin, and P. Whiting, "Asymptotic spectra of trapping sets in regular and irregular LDPC code ensembles," *IEEE Trans. on Inform. Theory*, vol. 53, no. 1, pp. 39–55, January 2007.
- [14] H. Hollmann and L. Tolhuizen, "On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. on Inform. Theory*, vol. 53, no. 2, pp. 823–828, February 2007.

- [15] T. Hehn, S. Laendner, O. Milenkovic, and J. B. Huber, "The stopping redundancy hierarchy of cyclic codes," in *Proceedings of the 44th Annual Allerton Conference on Communication, Control and Computing*, Allerton House, UIUC, Illinois, USA, September 2006, pp. 1271–1280.
- [16] S. Laendner, T. Hehn, O. Milenkovic, and J. Huber, "When does one redundant parity-check equation matter?" in *Proceedings of the 49th annual IEEE Global Telecommunications Conference (GlobeCom 2006)*, San Francisco, California, USA, November 2006.
- [17] N. Alon and J. Spencer, *The Probabilistic Method*, ser. Interscience Series in Discrete Mathematics and Optimization. John Wiley, 2000.
- [18] M. Hofri, *Analysis of Algorithms*. Oxford University Press, 1995.
- [19] P. Brockwell, "An asymptotic expansion for the tail of the binomial distribution and its application in queuing theory," *J. Appl. Prob.*, vol. 1, no. 1, pp. 163–169, June 1964.
- [20] G. Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol. 2, no. 1, pp. 71–78, March 1982.
- [21] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.
- [22] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov 2001.
- [23] J. Hirschfeld, *Projective geometries over finite fields*. Oxford Mathematical Monographs, 1979.
- [24] —, *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs, 1985.