# Analysis of Bipartite Graph Codes on the Binary Erasure Channel

Arya Mazumdar
Department of ECE
University of Maryland, College Park
email: arya@umd.edu

***Abstract*—We derive density evolution equations for codes on bipartite graphs (BG codes) for the binary erasure channel (BEC). We study the cases of local codes being introduced on only one side of the graph (Generalized LDPC codes) as well as on both sides. Each local code is assumed to correct up to a number of erasures one less than its distance. We define and enumerate stopping sets for BG codes, which serves an important tool for analysis of decoding thresholds on the BEC.**

## I. Introduction

Tanner's construction of codes on graphs [13] assumes that local constraints (codes) are imposed on the subsets of edges incident to every vertex of the graph. A variant of this construction was considered in [3], [7] where the graph was assumed bipartite with one side formed of variable nodes and the other side with local codes such as the one-error-correcting Hamming codes. This class of codes was termed Generalized Low Density Parity Check (GLDPC) codes. Codes on bipartite graphs in which local code constraints are imposed on both sides and the symbols transmitted correspond to graph's edges were studied in [12] and a number of follow-up works. This construction is called bipartite-graph (BG) codes.

Weight distribution of the versions of BG-codes discussed was computed in [3], [7], [2]. Later works considered other versions of this construction, such as codes constructed from protographs and computed their weight distributions [5], or analyzed their performance with exit charts [14].

Let $G(V_1 \cup V_2, E)$ be a bipartite graph. In the standard construction of LDPC codes, every $u \in V_1$ corresponds to a variable bit and every $v \in V_2$ corresponds to a $[\Delta_v, \Delta_v - 1, 2]$ single parity-check code $\mathcal{C}_2$, where $\Delta_v$ is the degree of $v$. Since the variable bit is replicated on every edge leaving the corresponding variable node $u \in V_1$, we can think of a $[\Delta_u, \Delta_u, 1]$ repetition code $\mathcal{C}_1$ associated with the variable node $u$ where $\Delta_u$ is its degree in $G$. Replacing the code $\mathcal{C}_2$ with general linear binary codes which may be different for different vertices $v$, we obtain GLDPC codes of [3], [7] (these papers assumed Hamming codes at every check vertex). If in addition the code $\mathcal{C}_1$ is replaced by nontrivial linear binary codes (different vertices may have different codes), we obtain the family of general BG codes. Theoretical analysis of BG codes previously was performed using graph expansion (see [12] and later works). Our purpose in this paper is to analyze them under message passing decoding.

Density evolution equations allow us to compute the decoding error probability for iterative decoding. These equations for an ensemble of LDPC codes for the binary erasure channel (BEC) are found in [11] and described in greater detail in [10]. With the help of these equations it was also shown that if the channel erasure probability is below some threshold, iterative decoding used on an average code in the ensemble defined by random graphs corrects erasures in the received vector in all but a small fraction of transmissions. Concentration analysis performed in [11] shows that the probability of deviation from the average approaches zero exponentially with the code's length.

Paper [4] introduced stopping sets as a combinatorial tool to characterize decoding failures and estimate the threshold of the message-passing algorithm (earlier these configurations were considered in [15]. The distribution of stopping sets for regular LDPC codes was found in [8] which also used it to estimate the block error probability of LDPC codes.

The paper is organized as follows. In Section II, we find density evolution equations on the BEC for the ensemble of BG codes. We consider separately the cases when non-trivial local codes are introduced in only one side and both sides of the graph. To decode the local codes we employ bounded distance decoding, assuming that each local code corrects $d-1$ erasures where $d$ is its distance. From the density evolution equations we obtain the threshold of iterative decoding for both cases. We also find an upper bound on the threshold by deriving a stability condition similar to the one discussed in [10].

In Section III we define and enumerate stopping sets for the regular ensemble of BG codes. Again we consider the cases of generalized LDPC and doubly generalized LDPC codes separately employing the decoding described above. We show that the average block erasure probability of the ensemble approaches zero at least polynomially in the block length $n$ if the erasure probability of the channel $p$ is less than some threshold $p_{\mathrm{th}}$, similar to the standard LDPC codes in [8]. For $p < p_{\mathrm{th}}$ the main contribution to the block erasure probability is from stopping sets of size sublinear in $n$ while the contribution from linearly-sized stopping sets declines exponentially in $n$. Section IV concludes the paper.

## II. Density evolution equations and Threshold

Our analysis will be performed assuming the Tree Channel defined in [10]. Asymptotic convergence of the bit error probability of BG codes to that of the tree channel can be proved similarly to that of the standard LDPC codes.

### A. Check-side generalized BG code

Consider transmission over the BEC($p$) with GLDPC codes. Our goal is to derive the density evolution equations for their iterative decoding under which in every even-numbered iteration all the local codes at the check nodes are decoded in parallel up to their minimum distance. Suppose that the ensemble is characterized by the degree distributions $\lambda$ and $\rho$, where $\lambda$ is a vector whose $j$th entry $\lambda_j$ is the fraction of edges incident to variable nodes of degree $j$ and $\rho$ is a matrix in which $\rho_{i,d}$ refers to the fraction of edges incident to check nodes of degree $i$ whose local codes have distance $d$. We assume that there exist linear codes of lengths equal to the degrees of the vertices given by $\rho$. Otherwise the code ensemble can be defined in the same way as standard irregular LDPC ensembles. This remark also applies to general BG codes below.

Denote

$$\begin{aligned} & f(p,x) \\ \triangleq \quad & p\sum_j \lambda_j \left[1-\sum_{i,d}\rho_{i,d}\sum_{k=0}^{d-2}\binom{i-1}{k}x^k(1-x)^{i-1-k}\right]^{j-1}. \end{aligned}$$

Denote by $x_l$ the average erasure probability of a bit after $l$ iterations.

**Theorem 1.** *$x_l$ satisfies the the following recurrence: $x_0 = p, x_l = f(p, x_{l-1}), l = 1, 2, \ldots$*

*Proof:* The proof is done by induction with $x_0 = p$ serving as its base.

We compute the average erasure probability of a bit after $l$ iterations. Consider a check node of degree $i$ and local code minimum distance $d$. Consider the message going out from this node. It will be an erasure if at least $d-1$ incoming messages among the remaining $i-1$ edges are erasures. The probability of this event equals

$$1-\sum_{k=0}^{d-2}\binom{i-1}{k}x_{l-1}^k(1-x_{l-1})^{i-1-k},$$

as $x_{l-1}$ is the probability of erasure after the $(l-1)^{th}$ iteration. The probability that the edge is incident to a vertex $v \in V_2$ of degree $i$ and local minimum distance $d$ equals $\rho_{i,d}$. Therefore, the probability that the message sent along this edge to the variable node is an erasure equals

$$\sum_{i,d}\rho_{i,d}\left[1-\sum_{k=0}^{d-2}\binom{i-1}{k}x_{l-1}^k(1-x_{l-1})^{i-1-k}\right] = \\ 1-\sum_{i,d}\rho_{i,d}\sum_{k=0}^{d-2}\binom{i-1}{k}x_{l-1}^k(1-x_{l-1})^{i-1-k}.$$

On the variable side consider a node of degree $j$. This node will send an erasure via an edge if the incoming messages on all the other $j-1$ edges are erasures and the received bit itself was an erasure which happens with probability

$$p\left[1-\sum_{i,d}\rho_{i,d}\sum_{k=0}^{d-2}\binom{i-1}{k}x_{l-1}^k(1-x_{l-1})^{i-1-k}\right]^{j-1}.$$

The probability that an edge coming out from a variable node of degree $j$ is $\lambda_j$. Together with the above this implies the theorem. ■

Our next goal is to examine some properties of the function $f(p, x)$.

**Lemma 1.** *$f(p, x)$ is increasing on both arguments for $p, x \in [0, 1]$.*

*Proof:* It is obvious that $f(p, x)$ is increasing on $p$. To show that $f(p, x)$ is increasing on $x$ it suffices to prove that the quantity

$$\nu_{i,d}(x) = \sum_{k=0}^{d-2}\binom{i-1}{k}x^k(1-x)^{i-1-k}$$

is decreasing on $x \in [0, 1]$ for all $i, d$.

We have

$$\begin{aligned} \frac{d\nu_{id}(x)}{dx} &= \sum_{k=0}^{d-2}\binom{i-1}{k}kx^{k-1}(1-x)^{i-1-k} \\ &\quad -\sum_{k=0}^{d-2}\binom{i-1}{k}(i-1-k)x^k(1-x)^{i-2-k} \\ &= \sum_{k=1}^{d-2}\binom{i-1}{k}kx^{k-1}(1-x)^{i-1-k} \\ &\quad -\sum_{k'=1}^{d-1}\binom{i-1}{k'-1}(i-k')x^{k'-1}(1-x)^{i-1-k'} \\ &= \sum_{k=1}^{d-2}x^{k-1}(1-x)^{i-1-k} \\ &\quad \cdot\left[k\binom{i-1}{k}-(i-k)\binom{i-1}{k-1}\right] \\ &\quad -\binom{i-1}{d-2}(i-d+1)x^{d-2}(1-x)^{i-d} \le 0, \end{aligned}$$

which proves the claim. ■

Let $P^{(1)}_{l,\lambda,\rho}(p)$ be the average probability of erasure after $l$ iterations for the ensemble if the channel erasure probability is $p$. The next two claims follow directly as a consequence of Lemma 1. Their proofs are similar to those for LDPC codes ([10], Ch. 3).

**Lemma 2.** *If $P^{(1)}_{l,\lambda,\rho}(p) \to 0$ as $l \to \infty$, and $p' \le p$, then $P^{1}_{l,\lambda,\rho}(p') \to 0$ as $l \to \infty$. Moreover, $x_l$ is monotone in $l$.*

**Theorem 2.** *$P^{(1)}_{l,\lambda,\rho}(p)$ converges to the nearest root of the equation $x = f(p, x)$ as $l \to \infty$.*

Using Lemma 2 we can define the threshold of iterative decoding for the erasure channel.

**Definition 1.** *Consider the ensemble of GLDPC codes characterized by the degree distribution $(\lambda, \rho)$. The threshold probability $p^*(\lambda, \rho)$ is defined as*

$$p^*(\lambda, \rho) = \sup\{p \in [0,1] : P^{(1)}_{l,\lambda,\rho}(p) \to 0 \ \textit{as} \quad l \to \infty\}. \tag{1}$$

Theorem 2 provides the following characterization of the threshold.

$$\begin{aligned} & p^*(\lambda, \rho) \\ = \ & \sup\{p \in [0,1] : x = f(p,x) \textit{ has no solutions in } (0,1]\} \\ = \ & \inf\{p \in [0,1] : x = f(p,x) \textit{ has a solution in } (0,1]\}. \end{aligned}$$

To determine the threshold numerically we plot $f(p,x) - x$. The largest value of $p$ for which the entire curve is below the $x$-axis gives us the threshold.

**Stability Condition:**

We have

$$x_l = f(p, x_{l-1}) = f(p,0) + \frac{\partial}{\partial x} f(p,0) x_{l-1} + O(x_{l-1}^2).$$

Assume that there are no nodes of degree 1, so $f(p,0) = 0$. By a calculation similar to the proof of Lemma 1, we have

$$\begin{aligned} & \frac{\partial}{\partial x} f(p,0) \\ & = p \sum_j \lambda_j \sum_{i,d} \rho_{i,d} \binom{i-1}{d-2} (i-d+1) x^{d-2} (1-x)^{i-d}|_{x=0} \\ & = p\lambda_2 \sum_i \rho_{i,2}(i-1) \end{aligned}$$

which gives

$$x_l = p\lambda_2 \sum_i \rho_{i,2}(i-1) x_{l-1} + O(x_{l-1}^2). \tag{2}$$

Notice that the only contribution to the linear term comes from check nodes whose local codes have distance 2. This gives a condition for the fixed point at 0 being stable. Formally speaking, we have

**Theorem 3.** *If $p\lambda_2 \sum_i \rho_{i,2}(i-1) > 1$ then $\lim_{l\to\infty} P^{(1)}_{l,\lambda,\rho}(p) > 0$. On the other hand if $p\lambda_2 \sum_i \rho_{i,2}(i-1) < 1$, then there exists $\zeta > 0$ such that $\lim_{l\to\infty} P^{(1)}_{l,\lambda,\rho}(p) = 0$ for all $p \in [0, \zeta)$.*

**Corollary 1.**

$$p^*(\lambda, \rho) \le \frac{1}{\lambda_2 \sum_i \rho_{i,2}(i-1)}. \tag{3}$$

### *B. General BG code*

We now consider the ensemble of BG codes with local constraints introduced on both sides of the graph $G$ used on the BEC($p$). In contrast to the LDPC code construction, the bits of the transmission are associated with the edges of $G$. Our purpose is to derive density evolution equations for message passing decoding assuming that the local codes are decoded up to their distance. The ensemble is characterized by two matrices $\lambda$ and $\rho$. The $(i,d)$th entry of $\lambda$ ($\rho$) denotes the fraction of edges incident to a left (resp., right) node of degree $i$ whose local code has distance $d$.

Let

$$f_\lambda(p,x) = p\left[1 - \sum_{i,d} \lambda_{i,d} \sum_{k=0}^{d-2} \binom{i-1}{k} x^k (1-x)^{i-1-k}\right]$$

and

$$f_\rho(p,x) = p\left[1 - \sum_{i,d} \rho_{i,d} \sum_{k=0}^{d-2} \binom{i-1}{k} x^k (1-x)^{i-1-k}\right].$$

We will assume that one iteration of decoding consists of decoding all the right codes in parallel, updating the bit values on the left and decoding all the left codes in parallel.

**Theorem 4.** *The erasure probability $x_l$ of a bit after $l$ iterations of message passing decoding satisfies the following recurrence: $x_0 = p, y_{l-1} = f_\rho(p, x_{l-1}), x_l = f_\lambda(p, y_{l-1})$.*

*Proof:* The proof again goes by induction. Its base holds true by definition. Suppose that the statement is true up to $l-1$ iterations. Let $y_{l-1}$ be the probability of erasure being sent to the left side along a randomly chosen edge in the $l^{th}$ iteration. Clearly, an edge will carry an erasure to left if it was erased in transmission and the right decoding involving it did not recover its value. Thus,

$$y_{l-1} = p\left[1 - \sum_{i,d} \rho_{i,d} \sum_{k=0}^{d-2} \binom{i-1}{k} x_{l-1}^k (1-x_{l-1})^{i-1-k}\right].$$

The expression for $x_l$ follows immediately. ■

**Lemma 3.** *The function $g(p,x) = f_\lambda(p, f_\rho(p,x))$ is increasing in both arguments for $p, x \in [0,1]$.*

*Proof:* From Lemma 1 it follows that both $f_\lambda(p,x)$ and $f_\rho(p,x)$ are increasing functions of $p$ and $x \in [0,1]$. ■

Let $P^{(2)}_{l,\lambda,\rho}(p)$ be the ensemble-average probability of erasure after $l$ iterations. We have the following:

**Lemma 4.** *If $P^{(2)}_{l,\lambda,\rho}(p) \to 0$ as $l \to \infty$, and $p' \le p$, then $P^{(2)}_{l,\lambda,\rho}(p') \to 0$ as $l \to \infty$. Moreover, $x_l$ is monotonic in $l$.*

**Theorem 5.** *$P^{(2)}_{l,\lambda,\rho}(p)$ converges to the nearest root of the equation $x = g(p,x)$, as $l \to \infty$.*

**Definition 2.** *Consider a BG code characterized by the distributions $(\lambda, \rho)$. The threshold probability $p^{**}(\lambda, \rho)$ equals*

$$p^{**}(\lambda, \rho) = \sup\{p \in [0,1] : P^{(2)}_{l,\lambda,\rho}(p) \to 0 \quad as \quad l \to \infty\}. \tag{4}$$

The threshold probability can be characterized as follows:

$$\begin{aligned} & p^{**}(\lambda, \rho) \\ = \ & \sup\{p \in [0,1] : x = g(p,x) \textit{ has no solution in } (0,1]\} \\ = \ & \inf\{p \in [0,1] : x = g(p,x) \textit{ has a solution in } (0,1]\}. \end{aligned}$$

**Stability Condition:** Writing out a quadratic Taylor polynomial for $g$ we obtain

$$\begin{aligned} x_l &= g(p, x_{l-1}) \\ &= g(p,0) + \frac{\partial}{\partial x} g(p,0) x_{l-1} + O(x_{l-1}^2). \end{aligned}$$

We get $g(p,0) = f_\lambda(p, f_\rho(p,0)) = 0$. Moreover,

$$\begin{aligned} \frac{\partial}{\partial x} g(p,0) &= f'_\lambda(p, f_\rho(p,0)) f'_\rho(p,0) \\ &= f'_\lambda(p,0) f'_\rho(p,0) \\ &= p \sum_i \lambda_{i2}(i-1) p \sum_i \rho_{i2}(i-1) \end{aligned}$$

which gives

$$x_l = p^2 \sum_i \lambda_{i,2}(i-1) \sum_i \rho_{i,2}(i-1) x_{l-1} + O(x_{l-1}^2). \quad (5)$$

Again only local codes with minimum distance 2 contribute to the linear term. We have the following stability condition for the fixed point at 0,

**Theorem 6.** *If* $p^2 \sum_i \lambda_{i,2}(i-1) \sum_i \rho_{i,2}(i-1) x_{l-1} > 1$ *then* $\lim_{l\to\infty} P^{(2)}_{l,\lambda,\rho}(p) > 0$. *On the other hand if* $p^2 \sum_i \lambda_{i,2}(i-1) \sum_i \rho_{i,2}(i-1) x_{l-1} < 1$, *then there is* $\zeta > 0$ *such that* $\lim_{l\to\infty} P^{(2)}_{l,\lambda,\rho}(p) = 0$ *for all* $p \in [0, \zeta)$.

An upper bound on the threshold probability is given in the next corollary.

**Corollary 2.**

$$p^{**}(\lambda, \rho) \leq \frac{1}{\sqrt{\sum_i \lambda_{i,2}(i-1) \sum_i \rho_{i,2}(i-1)}}.$$

### *C. Exit Charts*

An analysis of threshold probability can also be done using the exit charts. For the definition of exit function we refer the reader to Chapter 3 of [10]. In the following analysis we consider bi-regular bipartite graph codes with constant left degree be $\Delta_1$ and right degree $\Delta_2$. The analysis though can be easily generalized to irregular bipartite graph with a given degree distribution. Let us assume that we have the codes $C_1[\Delta_1, k_1]$ and $C_1[\Delta_2, k_2]$ on the left and right nodes respectively. Moreover we assume that, these codes are chosen from an ensemble of random linear codes of the same parameters. An analysis similar to the one below appears in [9].

The exit function of a linear code with parameters $[n, k]$ in an erasure channel is given by Equation (40) of [1],

$$\begin{aligned} H_{n,k}(x) &= \frac{1}{n} \sum_{g=1}^{n} (1-x)^{g-1} x^{n-g} \\ &\quad .[g.\tilde{e}_{g,n,k} - (n-g+1).\tilde{e}_{g-1,n,k}] \quad (6) \end{aligned}$$

where, $\tilde{e}_{h,n,k}$ is the unnormalized information function defined in [6] for a code with parameters $[n, k]$.

For random linear codes with parameters $[n, k]$, the expected information function is given by,

$$\begin{aligned} & E(\tilde{e}_{h,n,k}) \\ &= \frac{\binom{n}{h}}{\begin{bmatrix} n \\ k \end{bmatrix}} \sum_{r=0}^{h} r \begin{bmatrix} h \\ r \end{bmatrix} \begin{bmatrix} n-h \\ k-r \end{bmatrix} 2^{r(n-h-k+r)} \end{aligned}$$

where $\begin{bmatrix} a \\ r \end{bmatrix}$ is the Gaussian binomial coefficient defined by

$$\begin{bmatrix} a \\ r \end{bmatrix} = \prod_{j=1}^{r-1} \frac{2^a - 2^j}{2^r - 2^j}.$$

Consider transmission over BEC(p). In this case the exit function from the left hand side of the bipartite graph to an edge is

$$H_{E1}(x) = H_{\Delta_1, k_1}(x). \quad (7)$$

The exit function from the right hand vertices, $H_{E2,p}$ is

$$H_{E2,p}(x) = p H_{\Delta_2, k_2}(px). \quad (8)$$

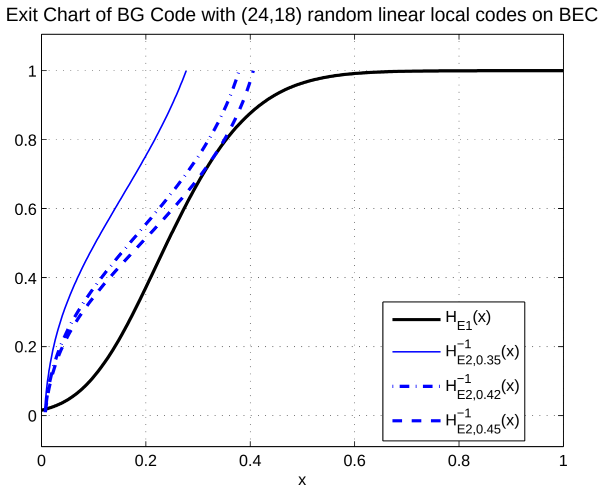

Fig. 1. The Exit Chart for a Bipartite Graph Code with random linear component codes

In Fig. 1 we have plotted the exit chart for a bipartite graph code with parameters $\Delta_1 = \Delta_2 = 24$ and $k_1 = k_2 = 18$. The exit functions are average of all linear codes of parameters $[24, 18]$. The figure shows the chart for a channel with erasure probabilities $p = 0.35$, $p = 0.42$ and $p = 0.45$.

From the exit chart analysis, the threshold probability for the above mentioned code is given by $p^{**} = 0.45$. The code has rate $> 2.\frac{18}{24} - 1 = 0.5$.

## III. Stopping Sets and Their Enumeration

Let us define stopping sets in the context of iterative decoding on the BEC.

**Definition 3.** *A subset of edges is called a stopping set if erasures in these edges submitted to the next iteration* *of iterative decoding are not recovered in this iteration. By definition, empty set is a stopping set.*

For GLDPC codes stopping sets can be equivalently defined as subsets of variable nodes. The set of stopping sets will be denoted by $\Gamma$.

Consider an ensemble of BG codes of length $n$. Define the normalized ensemble-average stopping set distribution $\gamma(\alpha), \alpha \in [0,1]$ as follows

$$\gamma(\alpha) \triangleq \lim_{n\to\infty} \frac{1}{n} \ln E[|\{S \in \Gamma : |S| = \alpha n\}|]. \tag{9}$$

Let

$$\begin{aligned} p_{\mathrm{th}} \triangleq\ & \sup\{p : \max_{\alpha\in[0,1]} [\gamma(\alpha) \\ & +(1-\alpha)h\left(\frac{p-\alpha}{1-\alpha}\right) - h(p)] < 0\} \end{aligned} \tag{10}$$

where, $h(.)$ is the binary entropy function in nats. Let $P_B(C^{(n)}, p)$ be the block erasure probability of a code $C^{(n)}$ from the ensemble on the BEC($p$).

**Theorem 7.** *Let $p < p_{\mathrm{th}}$. Then $\exists a_n$ such that*

$$E[P_B(C^{(n)}, p)] \leq \sum_{i=1}^{a_n} E[|\{S \in \Gamma : |S| = i\}|]p^i + \exp\left(-\Theta(n)\right) \tag{11}$$

*where the expectation is over the ensemble of BG codes of length $n$ and $\lim_{n\to\infty} \frac{a_n}{n} = 0$.*

For standard LDPC codes this result appears in [8]. The proof for the generalized case is completely analogous. Moreover it is known that for regular LDPC codes, the right-hand side of (11) goes to 0 polynomially with $n$. We will show that the same holds for general BG codes and will also find an expression for $\gamma(\alpha)$. These results imply a computable bound on the threshold for block error rate of BG codes.

The quantitative definition of stopping sets depends on the local decoding employed adopted in the iterative algorithm. In our results below we again assume that a local code can correct up to $d-1$ erasures, where $d$ is its distance.

In the following we consider regular BG codes with left degree $\Delta_1$ and right degree $\Delta_2$. Moreover we assume that all the local codes on one side are the same (it suffices to assume that they have the same minimum distance or are decoded up to the same number of erasure). Extension of the results to the case of irregular BG codes with given left and right degree distributions as well as different code distances is straightforward although the results become more cumbersome.

### *A. GLDPC codes*

Consider regular GLDPC codes with left degree $\Delta_1$ and right degree $\Delta_2$. Let $V_2$ and $V_1$ be the sets of check nodes and variable nodes respectively. Let $d$ denote the minimum distance of the local codes at the vertices $v \in V_1$. In each iteration these codes are decoded up to $d-1$ erasures. Denote by $N_R(S)$ the neighborhood in $V_2$ of a subset of vertices $S \subseteq V_1$. From Definition 3 we have the following

**Definition 4.** *A stopping set $S \subseteq V_1$ is a subset of vertices such that any vertex $v \in N_R(S)$ is connected to at least $d$ vertices in $S$.*

According to the above definition, the set of stopping sets is closed under the union operation. So every subset of variable nodes has a unique maximal stopping set which can be an empty set. If $\Omega \subset V_1$ is the set of bits (variable nodes) erased in transmission, then the set of erasures which remains when the decoder stops is equal to the unique maximal stopping set contained in $\Omega$.

**Theorem 8.** *The expected number of stopping sets of size $s$ in the regular ensemble of GLDPC codes is given by,*

$$\begin{aligned} & E[|\{S \in \Gamma : |S| = s\}|] \\ & = \binom{n}{s} \frac{\mathrm{coef}\left[\left((1+x)^{\Delta_2} - \sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i\right)^{\frac{n\Delta_1}{\Delta_2}}, x^{s\Delta_1}\right]}{\binom{n\Delta_1}{s\Delta_1}} \end{aligned} \tag{12}$$

*where $\mathrm{coef}(f(x), x^i)$ denotes the coefficient of $x^i$ in $f(x)$.*

*Proof:* Let $E$ be the set of edges of $G$. Given a check node $c$ the number of ways of choosing $k$ of its sockets is $\binom{\Delta_2}{k} = \mathrm{coef}((1+x)^{\Delta_2}, x^k)$. The number of ways of choosing $k$ of its sockets such that $k = 0$ or $k \geq d$ equals $\mathrm{coef}((1+x)^{\Delta_2} - \sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i, x^k)$. So the number of ways of choosing $e$ check node sockets from all the sockets of $V_2$, such that every check node connected to the sockets is connected to at least $d$ of them, is given by $\mathrm{coef}([(1+x)^{\Delta_2} - \sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i]^{|V_2|}, x^e)$. Let $U \subset V_1$, $|U| = s$. The number of edges incident to $U$ is $e = s\Delta_1$. The probability that these $e$ edges are such that $U$ becomes a stopping set equals

$$\begin{aligned} Pr(U \in \Gamma) &= \frac{\mathrm{coef}([(1+x)^{\Delta_2} - \sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i]^{|V_2|}, x^e)}{\binom{|E|}{e}} \\ &= \frac{\mathrm{coef}\left[((1+x)^{\Delta_2} - \sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i)^{\frac{n\Delta_1}{\Delta_2}}, x^{s\Delta_1}\right]}{\binom{n\Delta_1}{s\Delta_1}}. \end{aligned}$$

Finally there are $\binom{n}{s}$ ways of choosing $U$, which proves the theorem. ■

**Theorem 9.** *The normalized average stopping set distribution is given by*

$$\gamma(\alpha) = \frac{\Delta_1}{\Delta_2} \ln \frac{1 + \sum_{k=d}^{\Delta_2}\binom{\Delta_2}{k}x_0^k}{x_0^{\alpha\Delta_2}} - h(\alpha)(\Delta_1 - 1), \tag{13}$$

*where $x_0$ is the positive solution of the equation*

$$\alpha\Delta_2 + \sum_{k=d}^{\Delta_2}\binom{\Delta_2}{k}(\alpha\Delta_2 - k)x_0^k = 0.$$

*Proof:* From the definition of $\gamma(\alpha)$ we have

$$
\begin{aligned}
\gamma(\alpha) = \lim_{n\to\infty}\frac{1}{n}\ln\Bigg[\binom{n}{\alpha n} \\
\cdot\frac{\operatorname{coef}\Big[((1+x)^{\Delta_2}-\sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i)^{\frac{n\Delta_1}{\Delta_2}}, x^{\alpha\Delta_1 n}\Big]}{\binom{n\Delta_1}{\alpha\Delta_1 n}}\Bigg]
\end{aligned}
$$

$$
\begin{aligned}
&= -h(\alpha)(\Delta_1-1)+\lim_{n\to\infty}\frac{1}{n}\ln\operatorname{coef}\Bigg[((1+x)^{\Delta_2} \\
&\quad -\sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i)^{\frac{n\Delta_1}{\Delta_2}}, x^{\alpha\Delta_1 n}\Bigg] \\
&= -h(\alpha)(\Delta_1-1)+\lim_{n\to\infty}\frac{1}{n}\sum_{x_d,x_{d+1},\ldots,x_{\Delta_2}:\sum_{j=d}^{\Delta_2}jx_j=\alpha\Delta_1 n} \\
&\quad \binom{\frac{n\Delta_1}{\Delta_2}}{x_d,x_{d+1},\ldots,x_{\Delta_2},\frac{n\Delta_1}{\Delta_2}-\sum_{j=d}^{\Delta_2}x_j}\prod_{j=d}^{\Delta_2}\binom{\Delta_2}{j}^{x_j}.
\end{aligned}
$$

Let $y_k = \frac{x_k\Delta_2}{n\Delta_1}$. Noticing that the above sum contains a number of terms polynomial in $n$ and using asymptotic properties of multinomial coefficients, we have

$$
\begin{aligned}
\gamma(\alpha) = -h(\alpha)(\Delta_1-1)+\frac{\Delta_1}{\Delta_2}\max_{y_d,y_{d+1},\ldots,y_{\Delta_2}:\sum_{j=d}^{\Delta_2}jy_j=\alpha\Delta_2} \\
\left[h(y_d,y_{d+1},\ldots,y_{\Delta_2},1-\sum_{j=d}^{\Delta_2}y_j)+\sum_{j=d}^{\Delta_2}y_j\ln\binom{\Delta_2}{j}\right]
\end{aligned}
$$

where $h(z_1,\ldots,z_t)\triangleq\sum_{i=1}^{t}z_i\ln(1/z_i)$. Evaluating the maximum, we obtain the claim of the theorem. ■

Next let us use the above results to estimate the threshold of block error rate for iterative decoding of GLDPC codes. We need the following lemma.

**Lemma 5.** *Let $j < m$ and $d > 1$, then*

$$
\begin{aligned}
\operatorname{coef}\left[((1+x)^{\Delta_2}-\sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i)^m, x^j\right] \\
\le (\lfloor\frac{j}{d}\rfloor-\lceil\frac{j}{\Delta_2}\rceil+1)\binom{m}{\lfloor\frac{j}{d}\rfloor}(2\Delta_2-3)^j.
\end{aligned}
$$

*Proof:* The proof proceeds in the same way of counting as in Lemma 18 of [8], which gives a similar statement for $d = 2$. Except generalizing this, we use the following bound, $\sum_{l=\lceil\frac{j}{\Delta_2}\rceil}^{\lfloor\frac{j}{d}\rfloor}\binom{m}{l}\le(\lfloor\frac{j}{d}\rfloor-\lceil\frac{j}{\Delta_2}\rceil+1)\binom{m}{\lfloor\frac{j}{d}\rfloor}$. ■

**Theorem 10.** *Let $p \in [0,1]$, then*

$$
\sum_{i=1}^{a_n}E[|\{S\in\Gamma:|S|=i\}|]p^i = O\left(\frac{1}{n^{\Delta_1(1-1/d)-1}}\right) \qquad (14)
$$

$\forall a_n$ *such that* $\lim_{n\to\infty}\frac{a_n}{n}=0$.

*Proof:* We use the bound of the above lemma as follows,

$$
\begin{aligned}
&\sum_{s=1}^{a_n}E[|\{S\in\Gamma:|S|=s\}|]p^s \\
&= \sum_{s=1}^{a_n}\binom{n}{s}\frac{\operatorname{coef}\Big[((1+x)^{\Delta_2}-\sum_{i=1}^{d-1}\binom{\Delta_2}{i}x^i)^{\frac{n\Delta_1}{\Delta_2}}, x^{s\Delta_1}\Big]}{\binom{n\Delta_1}{s\Delta_1}}p^s \\
&\le \sum_{s=1}^{a_n}\binom{n}{s}\frac{(\lfloor\frac{s\Delta_1}{d}\rfloor-\lceil\frac{s\Delta_1}{\Delta_2}\rceil+1)\binom{\frac{n\Delta_1}{\Delta_2}}{\lfloor\frac{s\Delta_1}{d}\rfloor}(2\Delta_2-3)^{s\Delta_1}}{\binom{n\Delta_1}{s\Delta_1}}p^s
\end{aligned}
$$

which can be bounded above by decreasing geometric sequences, for all $a_n = o(n)$. Therefore,

$$
\sum_{s=1}^{a_n}E[|\{S\in\Gamma:|S|=s\}|]p^s = O\left(\frac{1}{n^{\Delta_1(1-1/d)-1}}\right)
$$

which proves the theorem. ■

The above theorem along with Equation (11) establishes $p_{\text{th}}$ as the threshold of block erasure probability below which the expected block erasure probability goes to 0 with $n$. Numerical values of $p_{\text{th}}$ can be easily computed from Equations (10) and (13).

### *B. General BG codes*

Consider regular BG codes with left degree $\Delta_1$ and right degree $\Delta_2$. Let $E$ be the set of edges of $G$, $|E| = n = |V_1|\Delta_1 = |V_2|\Delta_2$. Consider the ensemble of graphs obtained by connecting the vertices in $V_1$ with the vertices in $V_2$ using all permutations on the set of $n$ edges. Denote by $d_1$ and $d_2$ the local distances at the vertices of $V_1$ and $V_2$, respectively. In iterations, the local codes will be decoded to correct $d-1$ erasures, where $d = d_1$ or $d_2$ as appropriate.

**Definition 5.** *Let $S \subseteq E$ be a subset of edges and let $V_1(S)$ and $V_2(S)$ be the sets of left and right nodes to which they are incident. Then $S$ is called a stopping set if every $u \in V_1(S)$ has $S$-degree at least $d_1$ in $S$ and every $v \in V_2(S)$ has $S$-degree at least $d_2$.*

As before, the set of stopping sets is closed under taking the union. Therefore, every subset of edges has a unique maximal stopping set which can be an empty set. If $\Omega \subset E$ is the subset of bits erased in transmission, then the set of erasures which remains when the decoder stops is equal to the unique maximal stopping set of $\Omega$.

**Theorem 11.** *The expected number of stopping sets of size $s$ in the $(\Delta_1,\Delta_2)$-biregular ensemble of BG codes is given by*

$$
\begin{aligned}
&E[|\{S\in\Gamma:|S|=s\}|] \\
&= \frac{\prod_{l=1}^{2}\operatorname{coef}\Big[((1+x)^{\Delta_l}-\sum_{i=1}^{d_l-1}\binom{\Delta_l}{i}x^i)^{\frac{n}{\Delta_l}}, x^s\Big]}{\binom{n}{s}}.
\end{aligned}
$$

*Proof:* Consider an $s$-subset $U \subset E$. From Theorem 8, the number of ways of choosing $s$ right node sockets from all the sockets of $V_2$, such that every right node connected to the sockets is connected to at least $d_2$ of them, is given by

$\operatorname{coef}([(1+x)^{\Delta_2}-\sum_{i=1}^{d_2-1}\binom{\Delta_2}{i}x^i]^{|V_2|},x^s)$. A similar expression can be found for the left side. If the graph is chosen randomly then the events of $U$ satisfying the constraints on the left side and the right side are independent. So we have

$$Pr[U \in \Gamma] = \frac{\prod_{l=1}^{2} \operatorname{coef}\left[((1+x)^{\Delta_l} - \sum_{i=1}^{d_l-1}\binom{\Delta_l}{i}x^i)^{\frac{n}{\Delta_l}}, x^s\right]}{\binom{n}{s}^2}$$

because $|V_1| = \frac{n}{\Delta_1}$ and $|V_2| = \frac{n}{\Delta_2}$. Since there are $\binom{n}{s}$ ways of choosing $U$, this completes the proof. ■

**Theorem 12.** *The normalized average stopping set distribution is given by*

$$\gamma(\alpha) = \sum_{l=1}^{2}\left[\frac{1}{\Delta_l}\ln\frac{1+\sum_{k=d_l}^{\Delta_l}\binom{\Delta_l}{k}x_l^k}{x_l^{\alpha\Delta_l}}\right] - h(\alpha)$$

*where* $x_l, l = 1, 2$ *is the positive solution of the equation*

$$\alpha\Delta_l + \sum_{k=d}^{\Delta_l}\binom{\Delta_l}{k}(\alpha\Delta_l - k)x_l^k = 0.$$

*Proof:* From the definition of $\gamma(\alpha)$ we have,

$$\begin{aligned}
&\gamma(\alpha) = \lim_{n\to\infty}\frac{1}{n}\cdot\\
&\ln\left[\frac{\prod_{l=1}^{2}\operatorname{coef}\left[((1+x)^{\Delta_l}-\sum_{i=1}^{d_l-1}\binom{\Delta_l}{i}x^i)^{\frac{n}{\Delta_l}},x^{\alpha n}\right]}{\binom{n}{\alpha n}}\right]\\
&= -h(\alpha) + \lim_{n\to\infty}\\
&\frac{1}{n}\sum_{l=1}^{2}\ln\operatorname{coef}\left[((1+x)^{\Delta_l}-\sum_{i=1}^{d_l-1}\binom{\Delta_l}{i}x^i)^{\frac{n}{\Delta_l}},x^{\alpha n}\right].
\end{aligned}$$

We proceed the same way as Theorem 9, obtaining

$$\begin{aligned}
&\gamma(\alpha) = -h(\alpha) + \sum_{l=1}^{2}\frac{1}{\Delta_l}\max_{y_{d_l},y_{d_l+1},\ldots,y_{\Delta_l}:\sum_{j=d_l}^{\Delta_l}jy_j=\alpha\Delta_l}\\
&\left[h(y_{d_l},y_{d_l+1},\ldots,y_{\Delta_l},1-\sum_{j=d_l}^{\Delta_l}y_j)+\sum_{j=d_l}^{\Delta_l}y_j\ln\binom{\Delta_l}{j}\right].
\end{aligned}$$

Evaluating the maximum, we obtain the statement of the theorem. ■

**Theorem 13.** *Let* $p \in [0, 1]$, *then*

$$\sum_{i=1}^{a_n}E[|\{S\in\Gamma:|S|=i\}|]p^i = O\left(\frac{1}{n^{1-\lfloor 1/d_1\rfloor-\lfloor 1/d_2\rfloor}}\right) \tag{15}$$

$\forall a_n$ *such that* $\lim_{n\to\infty}\frac{a_n}{n} = 0$.

*Proof:* We use the bound of the Lemma 5, to have,

$$\begin{aligned}
&\sum_{s=1}^{a_n}E[|\{S\in\Gamma:|S|=s\}|]p^s = \sum_{s=1}^{a_n}p^s\\
&\cdot\frac{\prod_{l=1}^{2}\operatorname{coef}\left[((1+x)^{\Delta_l}-\sum_{i=1}^{d_l-1}\binom{\Delta_l}{i}x^i)^{\frac{n}{\Delta_l}},x^s\right]}{\binom{n}{s}}\\
&\leq\sum_{s=1}^{a_n}\frac{\prod_{l=1}^{2}(\lfloor\frac{s}{d_l}\rfloor-\lceil\frac{s}{\Delta_l}\rceil+1)\binom{\frac{n}{\Delta_l}}{\lfloor\frac{s}{d_l}\rfloor}(2\Delta_l-3)^s}{\binom{n}{s}}p^s
\end{aligned}$$

which can be bounded from above by decreasing geometric sequences for $a_n = o(n)$. Therefore,

$$\sum_{s=1}^{a}E[|\{S\in\Gamma:|S|=s\}|]p^s = O\left(\frac{1}{n^{1-\lfloor 1/d_1\rfloor-\lfloor 1/d_2\rfloor}}\right).$$

■

From (11), if the erasure probability satisfies $p < p_{\text{th}}$, the expected block error probability goes to 0 with $n$. We can compute $p_{\text{th}}$ numerically using Equation (10) and Theorem 12.

## IV. Concluding remarks

**1**. We notice from both equations (2) and (5), that for an ensemble of BG codes with local code minimum distance at least 3, the linear terms disappear, making $x_l = O(x_{l-1}^2)$. This means that the fixed point of density evolution equations at 0 is always stable in these cases. In case of conventional LDPC codes, the stability condition imposes an upper bound on the threshold probability, but in an ensemble of BG codes with local code minimum distance at least 3 no such constraint is imposed on the threshold.

If we take an ensemble of graphs with given degree distribution and consider GLDPC codes on it, we obtain a better threshold from the density evolutions compared to that of LDPC codes on the same ensemble. The same applies for the threshold ($p_{\text{th}}$) for the average block error probability. Consider a biregular ensemble of bipartite graphs with left and right degrees $\Delta_1$ and $\Delta_2$ respectively. For GLDPC codes, if the rate of the local codes at the check node is fixed at $R_L$, then the overall rate of the code is $\geq 1 - \Delta_1(1 - R_L)$, which is lower than LDPC codes on the same graph. Thus the better decoding threshold of these codes is at the expense of decreasing the rate. For a general BG code on a biregular graph, the overall rate is $\geq R_1 + R_2 - 1$, where codes of rate $R_1$ and $R_2$ are used on the left and right nodes respectively. These codes have better rate and thresholds compared to GLDPC codes.

**2**. The stopping set distribution above is derived in the context of bounded distance decoding. If we know the rank distribution of the local codes, then it is also possible to find the stopping set distribution under ML decoding at the vertices. For a given vertex $v$ let $C_v$ be the local code associated with it. Denote by $E(v)$ and $N_L(v)$, respectively the set of edges incident to $v$ and the set of variable nodes connected to $v$. The definitions of stopping sets in this case should be modified as follows.

**Definition 6. Stopping sets for GLDPC codes with local ML decoding:** *Let $S \subseteq V_1$ and let $N_R(S)$ be the set of check nodes connected to $S$. $S$ is called a stopping set if for every $v \in N_R(S)$ the set of edges $N_L(v) \setminus S$ does not contain an information set of $C_v$.*

**Definition 7. Stopping sets for general BG codes with local ML decoding:** *A subset $S \subset E$ is called a stopping set if for any $u \in V_1(S)$, the set $E(u) \setminus S$ does not contain an information set of $C_u$, and for any $v \in V_2(S)$, the set $E(v) \setminus S$ does not contain an information set of $C_v$.*

In a future work, we plan to study the performance of BG codes under message passing decoding on the binary symmetric channel and other discrete channels.

*Acknowledgement*

The author is grateful to Alexander Barg for numerous helpful discussions. This research is supported in part by NSF grant CCF0515124.

## References

[1] A. Ashikhmin, G. Kramer and S. ten Brink, "Extrinsic Information Transfer Functions: Model and Erasure Channel Properties," *IEEE Transactions on Information Theory*, Vol. 50, No. 11, November 2004.

[2] A. Barg and G. Zémor, "Distance Properties of Expander Codes," *IEEE Transactions on Information Theory*, Vol. 52, No. 1, January 2006.

[3] J. Boutros, O. Pothier and G. Zémor, "Generalized Low Density (Tanner) Codes," *Proceedings of IEEE International Conference on Communications (ICC)*, Vol. 1, Vancouver, BC, Canada, 1999, pp. 441-445.

[4] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson and R. L. Urbanke, "Finite-Length Analysis of Low Density Parity-Check Codes on Binary Erasure Channel," *IEEE Transactions on Information Theory*, Vol. 48, No. 6, June 2002.

[5] D. Divsalar, "Ensemble Weight Enumerators for Protograph LDPC codes," *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Seattle, USA, July, 2006, pp. 1554-1558.

[6] T. Helleseth, T. Klove and V. I. Levenshtein, "On the Information Function of an Error-Correcting Code," *IEEE Transactions on Information Theory*, Vol. 43, No. 2, March 1997.

[7] M. Lentmaier and K. Sh. Zigangirov, "On Generalized Low Density Parity Check Codes Based on Hamming Component Codes," *IEEE Communication Letters*, Vol. 3, No. 8, 1999.

[8] A. Orlitsky, K. Viswanathan and J. Zhang, "Stopping Set Distribution of LDPC code ensembles," *IEEE Transactions on Information Theory*, Vol. 51, No. 3, March 2005.

[9] E. Paolini, M. Fossorier and M. Chiani "Analysis of Generalized LDPC Codes with Random Component Codes for the Binary Erasure Channel," *International Symposium on Information Theory and its Applications (ISITA)*, Seoul, Korea, October 29 - November 1, 2006.

[10] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*, available online at http://lthcwww.epfl.ch/mct/index.php.

[11] T. J. Richardson, M. A. Shokrollahi and R. L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," *IEEE Transactions on Information Theory*, Vol. 47, No. 2, February 2002.

[12] M. Sipser and D. A. Spielman, "Expander Codes," *IEEE Transactions on Information Theory*, Vol. 42, No. 6, November 1996.

[13] R. M. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Transactions on Information Theory*, Vol. IT-26, No. 5, September 1981.

[14] Y. Wang and M. Fossorier, "Doubly Generalized LDPC codes," *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, Seattle, USA, July, 2006, pp. 669-673.

[15] V. V. Zyablov and M. S. Pinsker, "Complexity of Decoding Low-Density Codes in Transmission Over a Channel with Erasures," *Probl. Inform. Trans.*, Vol. 10, no. 1, 1974, 15–28.