

Decay of Correlations: An Application to Low-Density Parity Check codes

Shrinivas Kudekar and Nicolas Macris

EPFL, School of Computer and Communication Sciences, Lausanne 1015, Switzerland

Email: shrinivas.kudekar@epfl.ch, nicolas.macris@epfl.ch

Abstract—Recently the decay of correlations between bits of low density generator matrix (LDGM) codes have been investigated by using high temperature expansions from statistical physics [8]. In this work we apply these ideas to a special class of low density parity check codes (LDPC) on the binary input gaussian white noise channel (BIAWGNC). We give a rigorous derivation of the MAP GEXIT curve (the derivative with respect to the noise parameter of the input-output conditional entropy) for high values of the noise. Our result agrees with the formal expressions obtainable from replica calculations, and is the first result that fully justifies the replica formulas beyond the binary erasure channel (BEC). It also shows that the MAP and BP-GEXIT curves are equal in the high noise regime. The ensemble of LDPC codes considered here is constructed by adding randomly a sufficient fraction p of degree one variable nodes to a standard irregular LDPC(Λ, P) Tanner graphs.

I. INTRODUCTION

Recent connections between statistical physics and communication science have provided us with various conjectures concerning exact expressions of relevant quantities in the analysis of low-density parity check codes (LDPC). Although the replica method has been applied successfully to the maximum a posteriori (MAP) analysis of communication over binary memoryless symmetric (BMS) channels using sparse graph codes, rigorous results are scarce. Tight lower bounds on the conditional input-output entropy have been proven [2][4], and these match the replica expression giving strong support to the conjectured equality. In [6] the authors provide a combinatorial proof of the exactness of the replica formulas for the case of transmission over binary erasure channel (BEC) using regular LDPC codes and in [7] the authors provide such a proof for Poisson LDPC codes, still on the BEC, using an interpolation method developed in spin glass theory.

More recently a new method based on correlation decay techniques was put forward in [8] for the analysis of low density generator matrix codes (LDGM) and enabled to prove the correctness of the replica formulas in the high noise regime for a class of BMS channels. However it is still unclear how to apply techniques of correlation decay to standard LDPC ensembles. In this work, we show that results of [8] can be applied to a special class of LDPC codes.

Our application concerns a special class of LDPC ensembles which contain a sufficient fraction of degree one variable nodes. This code construction is equivalent to a mixture of LDGM and LDPC check nodes which eventually allows us to control the decay of correlations. Although this code

construction is not a good code (in particular the bit MAP probability of error is always non-zero) there is a non-trivial phase transition (a jump in the MAP-GEXIT curve) and our analysis constitutes a step towards proving the correctness of the replica formulas in the most general case. In this paper we illustrate our methods for the BIAWGN channel for which the combinatorial methods do not extend. We also provide a numerical illustration of the phase transition on the BEC channel.

II. CORRELATION DECAY FOR A GENERAL MODEL ON A GRAPH

In this paragraph we reformulate the main results of [8] in a suitable way for the present analysis. It is convenient to define a general model on a bi-partite Tanner graph consisting as usual of variable nodes and check nodes. The main difference with the usual LDPC case is that the check nodes do not necessarily enforce hard constraints on the variable nodes, but they enforce a more general “soft” type of constraint.

We use the usual mapping of bits to spins $\sigma_i = (-1)^{x_i}$. We denote the check nodes by c and ∂c denotes the set of variable nodes attached to the check node c . We also set $\sigma_{\partial c} = \prod_{i \in \partial c} \sigma_i$. Our general model is a spin system with a Gibbs measure

$$\mu(\underline{\sigma}) = \frac{1}{Z} \prod_c \frac{1}{2} (1 + \sigma_{\partial c} \tanh J_c) \prod_i e^{l_i \sigma_i}$$

For the moment l_i and J_c are fixed real numbers (possibly infinite), and

$$Z = \sum_{\underline{\sigma}} \prod_c \frac{1}{2} (1 + \sigma_{\partial c} \tanh J_c) \prod_i e^{l_i \sigma_i}$$

Note in particular that if $J_c = \infty$ then the check node function is a hard constraint enforcing the usual parity check constraint. Check nodes with J_c finite are called “soft”. The average of $\sigma_X = \prod_{i \in X} \sigma_i$ with respect to $\mu(\underline{\sigma})$ is denoted as $\langle \sigma_X \rangle$.

For later use, we explain a correlation decay lemma adapted from [8].

Definition 1: A walk w between two variable nodes v_α, v_β , is a sequence $v_1, c_1, v_2, c_2, \dots, c_l, v_{l+1}$ of variable nodes (denoted by v_1, v_2, \dots, v_{l+1}) and checks (denoted by c_1, c_2, \dots, c_l) such that $v_1 = v_\alpha, v_{l+1} = v_\beta$ and $\{v_i, v_{i+1}\} \in c_i$. We say that the walk is *self-avoiding* if $v_i \neq v_j, c_i \neq c_j$ for $i \neq j$. We also say that two variable nodes v_α, v_β are

connected if and only if there exists a self-avoiding walk from v_α to v_β .

The length of the walk is the number of clauses in it. If $v_\alpha = v_\beta$ then a self-avoiding walk from v_α to v_β is the trivial walk v_α : we define its length as zero.

Let $W_{\alpha\beta}$ denote the set of all self-avoiding walks between variable nodes v_α, v_β , and $W_{AB} = \cup_{v_\alpha \in A, v_\beta \in B} W_{\alpha\beta}$ where $A, B \subset \{1, \dots, n\}$.

Now fix some number $H > 0$. Denote by \mathbb{B} the set of all check nodes c , such that $|J_c| > H$. Thus $\mathbb{B} = \{c \mid |J_c| > H\}$.

Lemma 1: (Correlation bound) Consider the spin system defined above and two fixed non intersecting sets $A, B \subset \{1, \dots, n\}$. We have

$$|\langle \sigma_A \sigma_B \rangle - \langle \sigma_A \rangle \langle \sigma_B \rangle| \leq 2 \sum_{w \in W_{AB}} \prod_{c \in w} \rho_c$$

where $\rho_c = 1$, if $c \in \mathbb{B}$ and $\rho_c = e^{4|J_c|} - 1$, if $c \notin \mathbb{B}$.

The right hand side of this bound involves a sum over all self-avoiding walks connecting the two sets A and B where each walk carries a weight depending on the softness of the check it meets. The proof proceeds by an expansion of the Gibbs weight around the point $J_c = 0$ for all c . This expansion can be organized as a sum over walks connecting nodes in A with nodes in B . It turns out that only selfavoiding walks survive, the other ones giving a zero contribution. A walk can traverse the set \mathbb{B} in which case the expansion terms are not small, hence the weight $\rho_c = 1$; and it can traverse the complement of \mathbb{B} in which case the expansion terms are small, hence the weight $\rho_c = e^{4J_c} - 1$.

III. EXACT EXPRESSION OF THE MAP-GEXIT FUNCTION FOR A CLASS OF LDPC CODES

The class of codes that we use is defined as follows. Consider a code from the standard ensemble $\text{LDPC}(n, \Lambda(x), P(x))$ with design rate $r = 1 - \frac{\Lambda'(1)}{P'(1)}$. We denote the set of variable nodes of this code by \mathcal{V} . To every check node attach a degree one variable node with probability p . Call the set of new degree one variable nodes \mathcal{V}_1 . The set of check nodes which contain a new degree one variable node is \mathcal{C}_1 and the remaining ones are denoted by \mathcal{C}_0 . On an average the resulting Tanner graph has $n + mp$ variable nodes, so that the design rate of the code is given by $R = \frac{1 - (1-r)(1-p)}{1 + p(1-r)}$. We denote a code from this resultant ensemble by G (see figure 1). We also denote averages w.r.t to a code from this ensemble by \mathbb{E}_G .

We assume communication over a binary input additive white gaussian noise (BIAWGN) channel with transition probability given by $p_{Y|X}(y|x)$ and half loglikelihood $l = \frac{1}{2} \ln \frac{p(y|0)}{p(y|1)}$ with distribution assuming all zero codeword transmission given by $\frac{1}{\sqrt{2\pi\epsilon}} e^{-(l-\epsilon)^2/2\epsilon}$. Here ϵ denotes the inverse square noise.

Under MAP decoding the posteriori probability distribution of the input to the channel X^N given the output Y^N (where

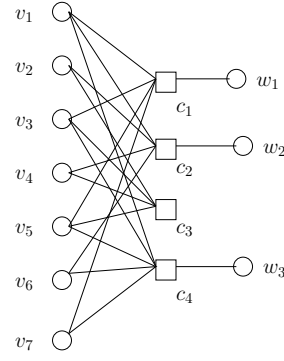


Fig. 1. A code from our ensemble is constructed from a standard LDPC graph, with 7 variable nodes and 4 check nodes denoted by v_1, v_2, \dots, v_7 and c_1, c_2, c_3, c_4 respectively, to which we attach a fraction of degree one variable nodes w_1, w_2, w_3 .

$N = |\mathcal{V} \cup \mathcal{V}_1|$ is

$$p(X^N | Y^N) = \frac{1}{Z} \prod_{c \in \mathcal{C}_0} \frac{1}{2} (1 + \sigma_{\partial c}) \prod_{c \in \mathcal{C}_1} \frac{1}{2} (1 + \sigma_{\partial c}) \prod_{i \in \mathcal{V}} e^{l_i \sigma_i} \prod_{i \in \mathcal{V}_1} e^{l_i \sigma_i}$$

with

$$Z = \sum_{\underline{\sigma}} \prod_{c \in \mathcal{C}_0} \frac{1}{2} (1 + \sigma_{\partial c}) \prod_{c \in \mathcal{C}_1} \frac{1}{2} (1 + \sigma_{\partial c}) \prod_{i \in \mathcal{V}} e^{l_i \sigma_i} \prod_{i \in \mathcal{V}_1} e^{l_i \sigma_i}$$

Let $h_N = \frac{1}{N} H(X^N | Y^N)$. We know from [3][5] that the MAP-GEXIT is given by

$$\frac{dh_N}{d\epsilon} = \frac{1}{2N} \sum_{i \in \mathcal{V}} (\mathbb{E}_L \langle \sigma_i \rangle - 1) + \frac{1}{2N} \sum_{i \in \mathcal{V}_1} (\mathbb{E}_L \langle \sigma_i \rangle - 1)$$

Taking the average w.r.t the code ensemble we get

$$\begin{aligned} \frac{d}{d\epsilon} \mathbb{E}_G[h_N] &= \frac{1}{2(1 + (1-r)p)} (\mathbb{E}_{G,\mathcal{L}} \langle \sigma_0 \rangle - 1) \\ &+ \frac{(1-r)p}{2(1 + (1-r)p)} (\mathbb{E}_{G,\mathcal{L}} \langle \sigma_1 \rangle - 1) \end{aligned} \quad (1)$$

where σ_0 denotes a spin attached to a variable node in \mathcal{V} and σ_1 denotes a spin attached to a variable node in \mathcal{V}_1 .

Our main theorem expresses the fact that both soft bit MAP estimates in equation (1) can be computed by the density evolution equations adapted to the present code ensemble. It also justifies the replica formulas in a regime of high noise. Let $\eta^{(d)}(v)$ be the density of messages from a variable node in \mathcal{V} to a check node and let $\bar{\eta}^{(d)}(u)$ be the density of messages from a check node to a variable node in \mathcal{V} . These satisfy the

following iterative equations:

$$\begin{aligned}
\bar{\eta}^{(d)}(u) &= \sum_k \rho_k \left\{ p \int dl c(l) \prod_{i=1}^{k-1} dv_i \eta^{(d-1)}(v_i) \right. \\
&\quad \times \delta\left(u - \tanh^{-1}\left(\tanh l \prod_{i=1}^{k-1} \tanh v_i\right)\right) + (1-p) \\
&\quad \times \left. \int \prod_{i=1}^{k-1} \eta^{(d-1)}(v_i) \delta\left(u - \tanh^{-1}\left(\tanh l \prod_{i=1}^{k-1} \tanh v_i\right)\right) \right\} \\
&\quad (2) \\
\eta^{(d)}(v) &= \sum_\ell \lambda_\ell \int dl c(l) \prod_{c=1}^{\ell-1} du_c \bar{\eta}^{(d)}(u_c) \delta\left(v - l - \sum_{c=1}^{\ell-1} u_c\right) \\
&\quad (3)
\end{aligned}$$

The initial condition is $\eta^{(0)}(v) = c(v)$. We will denote by the short hand \mathbb{E}_d the average w.r.t the density evolution densities given in (2), (3).

Let $1_{max}, r_{max}$ be the maximum variable and check node degrees respectively, and let $K = (r_{max} - 1)(1_{max} - 1)$

Theorem 1 (Main Result): There exist ϵ_0 and p_0 depending only on K such that for $\epsilon < \epsilon_0$ (high noise) and $p > p_0$ (high density of extra degree one nodes) the two soft bit estimates of equation (1) are given by

$$\begin{aligned}
\lim_{N \rightarrow \infty} \mathbb{E}_{G,L} \langle \sigma_0 \rangle &= \lim_{d \rightarrow \infty} \sum_\ell \Lambda_\ell \mathbb{E}_d \left[\tanh \left(l + \sum_{i=1}^\ell u_i^{(d)} \right) \right] \\
\lim_{N \rightarrow \infty} \mathbb{E}_{G,L} \langle \sigma_1 \rangle &= \lim_{d \rightarrow \infty} \sum_k P_k \mathbb{E}_d \left[\tanh \left(l + \right. \right. \\
&\quad \left. \left. \tanh^{-1} \left(\prod_{i=1}^k \tanh v_i^{(d)} \right) \right) \right]
\end{aligned}$$

As will be seen later on, our proof provides explicit expressions for the constants ϵ_0 and p_0 but we do not attempt to make theses sharp.

To prove our main theorem we utilize the following lemma. It is stated for a variable node belonging to \mathcal{V} but is also valid for a variable node belonging to \mathcal{V}_1 . We denote a neighborhood of depth D (various D 's will be needed) around the spin σ_0 by $N_D(0)$ and the check node boundary of such a neighborhood by $\partial N_D(0)$. Also define $\alpha = \ln \frac{(K-1)^{K-1}}{(1-p)p^{K-1}K^K}$.

Lemma 2 (Existence of Soft Boundary): Pick a node in \mathcal{V} and a code in the ensemble G . Take an integer $L > \frac{\ln K}{\alpha}$, a depth d and consider the two neighborhoods $N_d(0) \subset N_{(L+1)d}(0)$. The integer L is to be considered large enough but fixed while we let d go infinity when needed. With high probability $1 - o_{n,d}(1)$ these two neighborhoods are trees and there exists a check node boundary \mathcal{B} between $\partial N_d(0)$ and $\partial N_{(L+1)d}(0)$ such that all the check nodes in \mathcal{B} belong to the set \mathcal{C}_1 (are soft).

The fact that the neighborhoods are tree like with high

probability is well known for sparse graphs (see for example [1]). The existence of a boundary \mathcal{B} of soft checks follows from the standard analysis of a birth- death process and is presented in the appendix for completeness. Let us now prove theorem 1.

Proof: We prove only the first equation in the theorem, since for the other one all arguments are similar. Note that the randomness in G is two fold. One randomness comes from the choice of a code C from the LDPC($n, \Lambda(x), P(x)$) and the other one comes from the attachment of degree one variable nodes with probability p . Let us denote by $\underline{S} = \{S_1, \dots, S_m\}$ the vector of Bernoulli(p) random variables. We associate S_c to each check node c where the value $S_c = 1$ indicates that $c \in \mathcal{C}_1$ and $S_c = 0$ indicates that $c \in \mathcal{C}_0$. We will view \mathbb{E}_G as $\mathbb{E}_{C,\underline{S}}$.

Consider a spin $\sigma_0 \in \mathcal{V}$ and the neighborhoods $N_d(0), N_{(L+1)d}(0)$ around it. Let us denote Θ the event that $N_{(L+1)d}(0)$ is a tree. Since this is a high probability event for bounded degree distributions,

$$\mathbb{E}_{C,\underline{S},L} \langle \sigma_0 \rangle = \mathbb{E}_{C,\underline{S},L} [\langle \sigma_0 \rangle | \Theta] + o_n(1)$$

Let \mathcal{S} denote the set of all \underline{S} such that there exists a boundary \mathcal{B} between $\partial N_d(0)$ and $\partial N_{(L+1)d}(0)$ such that all the check nodes in \mathcal{B} belong to \mathcal{C}_1 . From the previous lemma we know that $\mathbb{P}(\mathcal{S}) \geq 1 - o_d(1)$. Thus we have

$$\mathbb{E}_{C,\underline{S},L} \langle \sigma_0 \rangle = \mathbb{E}_{C,\underline{S},L} [\langle \sigma_0 \rangle | \Theta, \mathcal{S}] + o_{d,n}(1)$$

where $o_{d,n}(1)$ is a function of d, n which goes to zero as $n, d \rightarrow \infty$. From now on we consider $\mathbb{E}_{C,\underline{S},L} [\langle \sigma_0 \rangle | \Theta, \mathcal{S}]$. For a $\underline{S} \in \mathcal{S}$, let us denote the boundary which contains only check nodes belonging to \mathcal{C}_1 by \mathcal{B}_S . Consider any check node c in the boundary \mathcal{B}_S for $S \in \mathcal{S}$ and look at the contribution $\frac{1}{2}(1 + \sigma_1 \sigma_{\partial c \setminus 1}) e^{l_1 \sigma_1}$ due to this check node and the degree one spin $\sigma_1 \in \mathcal{C}_1$ (with channel loglikelihood output given by l_1). The constraint $\frac{1}{2}(1 + \sigma_1 \sigma_{\partial c \setminus 1})$ enforces $\sigma_1 = \sigma_{\partial c \setminus 1}$. Thus the effective contribution of $\frac{1}{2}(1 + \sigma_1 \sigma_{\partial c \setminus 1}) e^{l_1 \sigma_1}$ to the Gibbs measure is given by $e^{l_1 \sigma_{\partial c \setminus 1}}$. Now assume for a moment that each variable node $i \in \mathcal{V}_1$ is transmitted through an independent channel with inverse square noise ϵ_i . Thus if $\epsilon_i = 0$ then the check node c connected to $i \in \mathcal{V}_1$ is erased from the Gibbs measure. One can interpolate between $\epsilon_i = 0$ to $\epsilon_i = \epsilon$ by using the fundamental theorem of calculus. This procedure is performed for all checks along the boundary \mathcal{B}_S according to a specified order. The details can be found in [8] and lead to

$$\begin{aligned}
\mathbb{E}_{C,\underline{S},L} [\langle \sigma_0 \rangle | \Theta, \mathcal{S}] &= \mathbb{E}_{C,\underline{S},L} [\langle \sigma_0 \rangle_{\mathcal{B}_S} | \Theta, \mathcal{S}] + \mathbb{E}_{C,\underline{S}} \left[\right. \\
&\quad \left. \sum_{b \in \mathcal{B}_S} \int_0^\epsilon dv \mathbb{E}_L (\langle \sigma_0 \sigma_{\partial b} \rangle_{l_b \sim \nu} - \langle \sigma_0 \rangle_{l_b \sim \nu} \langle \sigma_{\partial b} \rangle_{l_b \sim \nu})^2 \middle| \Theta, \mathcal{S} \right]
\end{aligned} \quad (4)$$

where $\langle \cdot \rangle_{\mathcal{B}_S}$ denotes the average w.r.t the Gibbs measure restricted to the neighborhood of σ_0 inside the boundary by \mathcal{B}_S and the sum is over check nodes in the boundary \mathcal{B}_S that are successively erased. In the average $\langle \cdot \rangle_{l_b \sim \nu}$ has the inverse

square noise of the channel loglikelihood l_b given by ν and the checks occurring before b (in the previously specified order) are erased.

The integral terms will be shown to be small thanks to the correlation bound lemma. To utilize this lemma 1 we set $J_c = \infty$ for $c \in \mathcal{C}_0$. For a check node $c \in \mathcal{C}_1$, again from the fact that the effective contribution of $\frac{1}{2}(1 + \sigma_1 \sigma_{\partial c \setminus 1})e^{l_1 \sigma_1}$ to the Gibbs measure is given by $e^{l_1 \sigma_{\partial c \setminus 1}}$, we set $J_c = l_1$ for $c \in \mathcal{C}_1$. Recall from section II that $\mathbb{B} = \{c \mid |J_c| > H\}$. Clearly all check nodes $c \in \mathcal{C}_0$ belong to the set \mathbb{B} . With this mapping we get that $\rho_c = e^{|4l_1|} - 1 \leq e^{4H} - 1$ for $c \notin \mathbb{B}$ and $\rho_c = 1$ for $c \in \mathbb{B}$. Applying the correlation decay lemma we get

$$\begin{aligned} & \mathbb{E}_l(\langle \sigma_0 \sigma_{\partial b} \rangle_{l_b \sim \nu} - \langle \sigma_0 \rangle_{l_b \sim \nu} \langle \sigma_{\partial b} \rangle_{l_b \sim \nu})^2 \\ & \leq 4 \mathbb{E}_l \sum_{w \in W_{0b}} \prod_{c \in w} ((e^{4H} - 1) \mathbb{1}_{c \notin \mathbb{B}}(c) + \mathbb{1}_{c \in \mathbb{B}}(c)) \end{aligned}$$

where $\mathbb{1}(\cdot)$ is the indicator function. We have

$$\mathbb{1}_{c \in \mathbb{B}}(c) = \mathbb{1}_{c \in \mathcal{C}_1, |J_c| > H}(c) \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)$$

Since all the walks are self-avoiding all the check nodes in a given path are independent and we can take the expectation w.r.t the noise inside the product yielding

$$\begin{aligned} & \mathbb{E}_l(\langle \sigma_0 \sigma_{\partial b} \rangle_{l_b \sim \nu} - \langle \sigma_0 \rangle_{l_b \sim \nu} \langle \sigma_{\partial b} \rangle_{l_b \sim \nu})^2 \\ & \leq 4 \sum_{w \in W_{0b}} \prod_{c \in w} \left((e^{4H} - 1) \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{P}(|l_1| > H) \mathbb{1}_{c \notin \mathcal{C}_0}(c) \right. \\ & \quad \left. + \mathbb{1}_{c \in \mathcal{C}_0}(c) \right) \\ & \leq 4 \sum_{w \in W_{0b}} \prod_{c \in w} (\delta_H \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \end{aligned}$$

where we denote $\delta_H \triangleq e^{4H} - 1 + \mathbb{P}(|l_1| > H)$ (note that finally δ_H will be some very small number). In the first inequality we used the fact that $\mathcal{C}_0 \subseteq \mathbb{B}$, thus $\mathbb{1}_{c \notin \mathbb{B}}(c) \leq \mathbb{1}_{c \notin \mathcal{C}_0}(c)$.

Now we consider the average w.r.t the randomness in \underline{S} . Since we restrict the random vector \underline{S} to lie in \mathcal{S} we lose randomness in the region between $\partial N_d(0)$ and $\partial N_{(L+1)d}(0)$. Thus for check nodes belonging to this intermediate region we can only say that $\mathbb{1}_{c \in \mathbb{B}}(c) \leq 1$. But fortunately the number of such check nodes on any self-avoiding path of any length l is upper bounded by Ld . As a result for any self-avoiding path w we have

$$\begin{aligned} & \prod_{c \in w} (\delta_H \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \leq \\ & \prod_{\substack{c \in w \\ c \notin N_{(L+1)d}(0) \setminus N_d(0)}} (\delta_H \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \end{aligned}$$

Thus taking expectation w.r.t the randomness in $\underline{S} \in \mathcal{S}$ we get

$$\begin{aligned} & 4 \mathbb{E}_{\underline{S}} \left(\sum_{w \in W_{0b}} \prod_{c \in w} (\delta_H \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \right) \leq \\ & 4 \mathbb{E}_{\underline{S}} \left(\sum_{w \in W_{0b}} \prod_{\substack{c \in w \\ c \notin N_{(L+1)d}(0) \setminus N_d(0)}} (\delta_H \mathbb{1}_{c \notin \mathcal{C}_0}(c) + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \right) \stackrel{(a)}{\leq} \\ & 4 \mathbb{E}_{\underline{S}} \left(\sum_{w \in W_{0b}} \prod_{\substack{c \in w \\ c \notin N_{(L+1)d}(0) \setminus N_d(0)}} (\delta_H + \mathbb{1}_{c \in \mathcal{C}_0}(c)) \right) \stackrel{(b)}{\leq} \\ & 4 \left(\sum_{w \in W_{0b}} \prod_{\substack{c \in w \\ c \notin N_{(L+1)d}(0) \setminus N_d(0)}} (\delta_H + \mathbb{E}_{\underline{S}}[\mathbb{1}_{c \in \mathcal{C}_0}(c)]) \right) = \\ & 4 \left(\sum_{w \in W_{0b}} \prod_{\substack{c \in w \\ c \notin N_{(L+1)d}(0) \setminus N_d(0)}} (\delta_H + 1 - p) \right) \leq 4 \mathbf{r}_{max} \times \\ & \left(\sum_{l \geq (L+1)d} K^l (\delta_H + 1 - p)^{l-Ld} + \sum_{l=d}^{Ld} K^l (\delta_H + 1 - p)^d \right) \end{aligned}$$

where in (a) we used $\mathbb{1}_{c \notin \mathcal{C}_0}(c) \leq 1$, in (b) we used the fact that all check nodes belong to \mathcal{C}_0 independent of each other with the same probability $1 - p$ and along any self-avoiding walk w we have distinct check nodes. In the last inequality we did several things. Firstly we upper bound the total number of paths of length l by K^l . Secondly, for paths with length $l \geq (L+1)d$ we do not consider the check nodes belonging to $N_{(L+1)d}(0) \setminus N_d(0)$ which gives $(\delta_H + 1 - p)^{l-Ld}$ as a contribution of such paths. Finally, for paths with length $l \leq Ld$ we do not consider check nodes outside $N_d(0)$ which results in a contribution of $(\delta_H + 1 - p)^d$ by such paths. The factor of \mathbf{r}_{max} takes into account the fact that b is a check node with maximum degree \mathbf{r}_{max} , hence the total correlation gets multiplied by a factor of \mathbf{r}_{max} .

We choose $p > 1 - \frac{1}{(2K^2)^{L+1}}$ and ϵ such that $\epsilon(1 + 2(\ln \frac{2}{1-p})^{1/2}) < \frac{1}{4} \ln(\frac{3-p}{2})$. With this choice of ϵ, p we choose H such that $\epsilon(1 + 2(\ln \frac{2}{1-p})^{1/2}) < H < \frac{1}{4} \ln(\frac{3-p}{2})$ which implies $\delta_H < (1 - p)$. Thus the correlation is upper bounded by

$$4 \frac{(2K)^{(L+1)d} (1-p)^d}{1 - (2K(1-p))^{(L+1)d}} + 4Ld(K^L 2(1-p))^d < \zeta^d$$

for some $\zeta < 1$. In the chosen regime of ϵ, p we finally bound the second term in equation (4) by γ^d for some $\gamma < 1$ (here $\gamma = \zeta K^{L+1}$).

We now evaluate the first term in equation (4). To evaluate $\mathbb{E}_{C, \underline{S}, l}[\langle \sigma_0 \rangle_{\mathcal{B}_S} | \Theta, \mathcal{S}]$ we will consider the evaluation of $\mathbb{E}_{C, \underline{S}, l}[\langle \sigma_0 \rangle_{\mathcal{B}_S} | \Theta]$ because $\mathbb{P}(\mathcal{S}^c) = o_d(1)$. For $\underline{S} \notin \mathcal{S}$ we define $\mathcal{B}_S = \partial N_{(L+1)d}(0)$. From [3], by using the Griffiths-Kelly-Sherman inequalities for random spin systems, we have

$$\begin{aligned} \mathbb{E}_{C, \underline{S}, l}[\langle \sigma_0 \rangle_{N_d(0)} | \Theta] & \leq \mathbb{E}_{C, \underline{S}, l}[\langle \sigma_0 \rangle_{\mathcal{B}_S} | \Theta] \\ & \leq \mathbb{E}_{C, \underline{S}, l}[\langle \sigma_0 \rangle_{N_{(L+1)d}(0)} | \Theta] \end{aligned} \quad (5)$$

On $N_D(0)$, the Gibbs averages can be computed exactly by

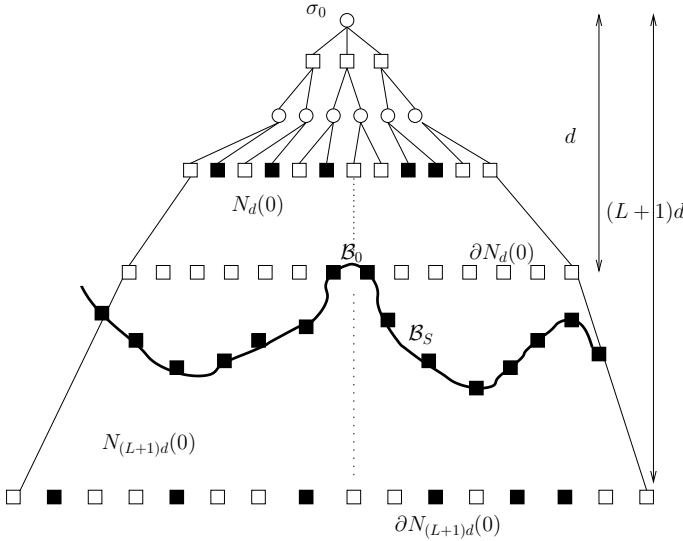


Fig. 2. On this figure we illustrate the two *tree* neighborhoods $N_d(0), N_{(L+1)d}(0)$ as well as their boundaries $\partial N_d(0), \partial N_{(L+1)d}(0)$. Check nodes belonging to \mathcal{C}_1 are shaded black and those belonging to \mathcal{C}_0 are white. We also show the irregular boundary \mathcal{B}_S consisting of only “soft” check nodes belonging to \mathcal{C}_1 and lying between the two neighborhoods. This figure is used throughout all the proofs.

the belief propagation equations,

$$\lim_{D \rightarrow \infty} \mathbb{E}_{C, \underline{S}, \underline{L}}[\langle \sigma_0 \rangle_{N_D(0)} | \Theta] = \lim_{D \rightarrow \infty} \sum_{\ell} \Lambda_{\ell} \mathbb{E}_D \left[\tanh \left(l + \sum_{i=1}^{\ell} u_i^{(D)} \right) \right]$$

where \mathbb{E}_D is the average w.r.t to the density evolution densities given by equations (2), (3). Since L is a constant which depends only on code parameters, from (5) we have

$$\lim_{d \rightarrow \infty} \mathbb{E}_{C, \underline{S}, \underline{L}}[\langle \sigma_0 \rangle_{\mathcal{B}_S} | \Theta] = \lim_{d \rightarrow \infty} \sum_{\ell} \Lambda_{\ell} \mathbb{E}_d \left[\tanh \left(l + \sum_{i=1}^{\ell} u_i^{(d)} \right) \right]$$

Putting everything together we get the theorem. \blacksquare

IV. DISCUSSION AND OPEN QUESTIONS

In this paper we have provided one example of LDPC code ensemble for which one can rigorously derive the MAP-GEXIT function for a very noisy BIAWGNC. This is the only example known to us for which such a derivation is made beyond the BEC with non-combinatorial methods. The main insight in deriving this result is the proof that correlations between distant codebits decays exponentially with their graph distance. We are not yet able to prove this for standard irregular LDPC ensembles, but hope that this work provides a step towards this goal. We have limited ourselves to the BIAWGNC, because the MAP-GEXIT formula is given by a simple expression involving the soft bit estimates (magnetizations). However, the whole analysis of this paper can be extended to other channels, notably the binary symmetric channel (BSC).

V. APPENDIX A

In this appendix we prove lemma 1. *Proof:* From standard arguments [1] the two neighborhoods $N_d(0), N_{(L+1)d}(0)$ are trees with high probability. Consider the check nodes belonging to $\partial N_d(0)$. We define the following process of finding the required boundary \mathcal{B} . Initially we set boundary $\mathcal{B} = \mathcal{B}_0 \triangleq \{c | c \in \partial N_d(0) \text{ and } c \in \mathcal{C}_1\}$. Pick a check node $c \in \partial N_d(0) \setminus \mathcal{B}_0$ we traverse down along all possible paths emanating from c till we hit a check node belonging to \mathcal{C}_1 on all the possible paths. We include all these check nodes belonging to \mathcal{C}_1 in our boundary \mathcal{B} and continue with the next check node $c \in \partial N_d(0) \setminus \mathcal{B}_0$.

Consider the following birth-death process. We call a check node “alive” if it has no degree one variable node belonging to \mathcal{V}_1 attached to it and “dead” otherwise. Clearly a check node is alive with probability $1 - p$ and dead with probability p . Initially we have a population of $\partial N_d(0) \setminus \mathcal{B}_0$ alive check nodes. From each check node generate 1_{max} variable nodes which further give rise to r_{max} check nodes, some of which are dead and some of which are alive. Continue with this process till at time T all the generated check nodes are dead. The maximum depth achieved by this boundary \mathcal{B} can be upper bounded by the extinction time T .

Let Y_{t-1} denote the number of alive check nodes at time $t-1$. Let Z_t denote the number of alive check nodes generated at time t by one alive check node at time $t-1$. Thus the number of alive check nodes at time t is given by $Y_t = Y_{t-1} + Z_t - 1$. Here Z_t is a Binomial($K, 1 - p$). For simplicity the parameter K of the Binomial has been set to its worst possible value. Thus from standard arguments [9] we have

$$\mathbb{P}(T > t) \leq \mathbb{P}(Y_t > 0) = \mathbb{P}(Z_1 + Z_2 + \dots + Z_t \geq t)$$

From the Markov inequality and the independence of $\{Z_i\}$, we have

$$\begin{aligned} \mathbb{P}(Z_1 + Z_2 + \dots + Z_t \geq t) &\leq \mathbb{E}[e^{s(Z_1 + Z_2 + \dots + Z_t)}] e^{-st} \\ &= (\mathbb{E}[e^{sZ_1}])^t e^{-st} \\ &\stackrel{(a)}{=} (p + e^s(1 - p))^{tK} e^{-st} \\ &\leq e^{-t\alpha} \end{aligned}$$

where in (a) we used the fact that Z_1 is Binomial($K, 1 - p$). For $p > 1 - \frac{1}{K}$ (condition for extinction in finite time for the birth-death process) we have $\alpha > 0$.

Since the $|\partial N_d(0) \setminus \mathcal{B}_0| \leq K^d$, and since each check node $c \in \partial N_d(0) \setminus \mathcal{B}_0$ gives rise to an independent birth-death process, because of the tree assumption, the probability that all the birth-death processes extinct within time Ld is lower bounded by

$$\begin{aligned} \mathbb{P}(\text{all birth-death processes are extinct within depth } Ld) \\ = (1 - \mathbb{P}(T > Ld))^{K^d} \geq (1 - e^{-\alpha Ld})^{K^d} \end{aligned}$$

Note that since $L > \frac{\ln K}{\alpha}$, the probability that all birth-death processes are extinct within depth Ld is lower bounded by $1 - o_d(1)$. \blacksquare

ACKNOWLEDGMENT

We gratefully acknowledge Rüdiger Urbanke for encouragement and useful discussions. We also acknowledge the support by the Swiss National Science Foundation under grant number 200020-113412.

REFERENCES

- [1] T. Richardson, R. Urbanke "Modern Coding Theory," *Cambridge University Press*, in press.
- [2] A. Montanari, "Tight Bounds for LDPC and LDGM Codes Under MAP Decoding," *IEEE Trans. Inf. Theory.*, **51**, no. 9, pp. 3221–3246, (2005).
- [3] N. Macris, "Griffith-Kelly-Sherman Correlation Inequalities: A Useful Tool in the Theory of Error Correcting Codes," *IEEE Trans. Inf. Theory.*, **53**, No. 2, pp. 664-683 (2007).
- [4] S. Kudekar, N. Macris, "Sharp Bounds for MAP Decoding of General Irregular LDPC Codes", *ISIT, Seattle*, 2006.
- [5] N. Macris, "Sharp Bounds on Generalized EXIT functions", *IEEE Trans. Inf. Theory.*, **53**, No. 7, pp. 2365-2375 (2007).
- [6] C. Measson, A. Montanari, R. Urbanke, "Asymptotic rate versus Design Rate", *Proc ISIT, Nice* (2007); see also C. Measson, "Conservation Laws for Coding", *These EPFL no 3485* (2006)
- [7] S. Kudekar, S. Korada, N. Macris, "Exact Solution for the Conditional Entropy of Poissonian LDPC Codes over the Binary Erasure Channel", *Proc ISIT, Nice* (2007)
- [8] S. Kudekar, N. Macris, "Proof of replica formulas in the high noise regime for communication using LDGM codes", *Proc. ITW Porto* (2008).
- [9] P. Erdos, J. Spencer, "The Probabilistic Method", *Wiley Interscience Series in Discrete Mathematics and Optimization* (1992)