Non-Linear Codes on Sparse Graphs

Mohamad Dia
LTHC, I&C, EPFL

Abstract—Spatial coupling has been successfully applied to various problems, ranging from error correcting codes to compressive sensing, and shown to have outstanding performance under message-passing algorithms. In particular, spatially coupled low-density parity-check (LDPC) codes were proven to universally achieve capacity under belief-propagation (BP) decoding. In this research proposal, we describe the asymptotic behaviour of spatially coupled LDPC codes, by presenting the results of threshold saturation phenomenon [1]. Then, a finite-length scaling law is presented for protograph-based spatially coupled LDPC codes under peeling decoder [2], by analysing the mean evolution of degree-one check nodes. Moreover, we show the connection between the potential functional approach used in [1] and the statistical physics’ replica method [3]. Furthermore, we introduce a class of non-linear checks for both lossy source coding and channel coding on sparse graphs.

Index Terms—Spatial coupling, replica method.

I. INTRODUCTION

In the last 20 years, a long line of research has focused on codes based on sparse graphs for both channel and source coding, mainly Low-Density Parity-Check (LDPC) codes and its counterpart Low-Density Generator-Matrix (LDGM) codes. LDPC code was originally presented as a linear error correcting code by Gallager in the early 1960’s [4]. Then, it was almost forgotten for more than 30 years. However, after the introduction of practical iterative message-passing algorithms on sparse graphs, such as Belief-Propagation (BP), the LDPC code has experienced a great comeback. Thenceforth, the design and analysis of linear codes, based on random sparse graph ensemble with iterative message-passing decoding, was coined modern coding theory [5]. A general method to determine the capacity of LDPC codes under BP algorithm, known as BP threshold, was presented in [6] under the name of density evolution (DE). Moreover, it has been observed in [7] that such codes approach the Shannon capacity when irregular ensembles are used with optimized degree distribution.

Recently, the spatially coupled LDPC codes, originally introduced as convolutional LDPC codes, have revolutionized the area of coding theory. The local coupling of several LDPC ensembles with a proper termination considerably improved the performance under iterative decoding by increasing the BP threshold. Different constructions have been proposed for spatially coupled LDPC codes. While the random construction is more suitable for analysis, the structured protograph-based construction gives practical advantages and better finite-length performance [2]. In a recent work [8], it was proven that the BP threshold of spatially coupled regular LDPC ensemble saturates to the optimal decoding MAP threshold of the underlying ensemble, over the class of binary memoryless symmetric (BMS) channels. This phenomenon was termed threshold saturation. The threshold saturation result in [8] heavily relied on the Maxwell construction to prove that BP threshold saturates to the area threshold, which is lower bounded by the MAP threshold. Another approach inspired from statistical physics was presented in [1] to provide a “simpler” proof of threshold saturation for irregular LDPC codes, using potential functional and replica method.

Over the last century, statistical physics has developed with the aim to describe and predict the dynamical behaviour of systems with large degrees of freedom using probabilistic models. This branch
of physics has interconnections with engineering problems and different fields of science [3]. In particular, the techniques developed in statistical physics can be applied to coding on sparse graphs, where the problem can be interpreted as a spin glass modeled by a certain Gibbs distribution. Furthermore, one can use these techniques to analyse and predict similar phenomena such as phase transition and nucleation. Although some techniques of statistical physics have found rigorous mathematical justification, others are used as an ansatz (educated guess) to give predictions which would be very difficult to guess. One of these techniques is the replica or cavity method. This method was conjectured to predict the free entropy of a random graphical model by looking at the average behaviour of message-passing algorithm or replica-symmetric (RS) free entropy. Thus, it is able to connect the BP threshold to the MAP threshold and helps in proving threshold saturation for spatially coupled LDPC codes. This phenomenon, in turn, is similar to the nucleation process, where the perfect side information can be seen as the seed that initiates the nucleation and transfers the system from its metastable to stable state. Recently, the replica method was proven to be exact for a large class of LDPC codes and BMS channels.

In this research proposal, we present the asymptotic and finite-length analysis for spatially coupled LDPC codes with different constructions by reviewing three different works. The potential functional, inspired from statistical physics’ replica method [3], is used to prove threshold saturation for spatially coupled irregular LDPC and LDGM codes on BMS channels under BP decoding [1]. While the random construction is used for asymptotic analysis for the ease of its mathematical tractability, the protograph-based construction exhibits a more robust performance and thus it is used for finite-length analysis on binary erasure channel (BEC) under peeling decoder [2]. We start by introducing the LDPC and LDGM codes ensembles with different constructions in Section II. The asymptotic analysis and the proof of threshold saturation of [1] are given in Section III, whereas the finite-length analysis of [2] is given in Section IV. Section V is dedicated to present the replica method [3] and show its relation with threshold saturation. We briefly present results of ours in Section VI by introducing a class of non-linear checks for both lossy source coding with the compressed word sitting on the variable-nodes with a certain degree distribution \( \lambda \), and the factor-nodes consist of the parity checks of degree distribution \( \rho \) (note that \( \lambda \) and \( \rho \) are the edge perspective degree distributions with an equivalent node perspective degree distributions \( L \) and \( H \)). The LDPC(\( \lambda, \rho \)) denotes the ensemble of such codes. A random ensemble can be created using the configuration model by matching up the sockets using random permutations over all edges. A more structured ensemble can be created based on protographs, which serve as the codes’ templates, by taking random permutations over each “edge bundle” connecting the same nodes in the protograph. The ensembles created by these methods are different, but for the asymptotic analysis they turned to be equivalent. The additional structure imposed by the protograph construction gives practical advantages and more compact way of representation in addition to a better finite-length performance (specially for spatially coupled codes as we will see later). However, this structure in the protograph ensembles leads to a multi-edge type code where the edges are not statistically equivalent and hard to analyse in contrast with the random ensembles.

2) Low-Density Generator-Matrix Codes: Low-density generator-matrix (LDGM) codes are a class of linear codes described, as a dual of LDPC codes, by a sparse generator matrix. Such codes are also represented in terms of a sparse factor graph where the information bits sit on the variable-nodes with a certain degree distribution \( \lambda \), and the factor-nodes consist of the generated codeword components of degree distribution \( \rho \). The LDGM(\( \lambda, \rho \)) denotes the ensemble of such codes. Note that these codes exhibit a non-negligible error floors compared to LDPC codes, and they are usually used in the context of lossy source coding with the compressed word sitting on the variable-nodes. The construction and asymptotic analysis of LDGM ensemble are similar to that of LDPC. However, a key difference arises due to the error floor which poses some difficulties and requires a little tweak in the analysis to reflect this difference. Therefore, we will focus more in this work on the analysis of LDPC ensemble for brevity, and then we will show how to adapt it to LDGM ensemble.

B. Coupled Systems

Spatially coupled LDPC ensembles consist of multiple LDPC ensembles placed next to each other at positions \( i = 1, 2, ..., N \) in a chain of chain length \( N \), locally coupled with a coupling window \( w \), and then terminated at the boundary with check-nodes of relatively lower degrees. This termination can be viewed as perfect information that initiates the decoding and then propagates inward to boost the performance (note that the rate-loss caused by this termination vanishes as \( N \to \infty \)). Such ensembles are denoted by
LDPC(\(\lambda, \rho, N, w\)) ensembles. Likewise single systems, spatially coupled systems can be constructed using random construction or protograph-based construction. In the sequel, we will assume a random construction, which is easier to analyse, for asymptotic analysis. The protograph-based ensemble are rather used to derive the finite-length scaling law due to its robust performance.

III. ASYMPTOTIC ANALYSIS ON BMS CHANNELS UNDER BP DECODING

Kumar et al. tackled the threshold saturation phenomenon in [1] using a simple approach inspired from statistical physics. We start by necessary preliminaries in order to present the proof of this phenomenon through Theorems 11 and 12.

Belief-propagation (BP) is an efficient low-complexity message-passing algorithm to compute the marginals of the posterior distribution on a tree, or more generally the marginals of a Gibbs measure. Therefore, such algorithm is used to estimate the marginals on a sparse factor graph, which is assumed to be locally tree, and hence it is used to perform the decoding for LDPC codes. The BP equations are the set of relations linking variable-to-check messages \(h_{i\to a}\) and check-to-variable messages \(h_{a\to i}\), in terms of half-loglikelihood ratios, in the following form

\[
h_{i\to a} = h_i + \sum_{b \in \partial_i \setminus a} \hat{h}_{b\to i}
\]

\[
\hat{h}_{a\to i} = \tanh^{-1} \left( \prod_{j \in \partial a \setminus i} \tanh h_{j\to a} \right).
\]

Density Evolution (DE) is a powerful tool used to describe the evolution of message distributions and characterize the asymptotic performance of LDPC ensemble under BP decoding. DE approach uses the concept of computation graph by first fixing the number of iterations and letting the code length tend to infinity in order to avoid loops and obtain locally optimal processing. Therefore, the incoming messages at each node can be treated as i.i.d. and the number of iterations is then taken to infinity.

Definition 1: The DE for a single ensemble under BP decoding is described by

\[
x^{(\ell+1)} = c(h) \circ \lambda^\circ (\rho^\|(x^{(\ell)})) = T_s(x^{(\ell)}; c(h)),
\]

where both \(x\) and \(c\) are symmetric probability measures. \(c(h)\) denotes the BMS channel distribution ordered by degradation and parametrized by its entropy \(h \in [0, 1]\), while \(x^{(\ell)}\) denotes the variable-node output distribution after \(\ell\) iterations of BP. The operators \(\circ\) and \(\|\) correspond to the convolution of densities at variable and check nodes respectively.

Definition 2: For a given channel distribution \(c(h)\) and under some initialization \(x^{(0)}\), if the sequence \(\{x^{(\ell)}\}\) converges we say that the DE converges to a fixed point \(x\) which satisfies

\[
x = T_s(x; c(h)) = T_s^{(\infty)}(x^{(0)}; c(h)).
\]

Definition 3: The BP threshold is therefore defined to be the largest channel parameter so that the DE initialized with \(h_0\) converges to the trivial fixed point \(\Delta_\infty\) (i.e. to the perfect decoding solution).

\[
h^\text{BP} = \sup \left\{ h \mid T_s^{(\infty)}(h) = \Delta_\infty \right\}.
\]

Definition 4: The MAP threshold characterizes the performance under optimal decoding, and it is related to the conditional entropy of the transmitted codeword given the received message.

\[
h^\text{MAP} = \inf \left\{ h \mid \lim_{n \to \infty} \frac{1}{n} \mathbb{E} [H(\mathbf{X}^n \mid Y^n(c(h)))] > 0 \right\}
\]

where the expectation is over the LDPC ensemble and \(H\) is the entropy functional.

We will now introduce the notions of potential functional and potential threshold for the single system. These tools are essential in connecting BP and MAP thresholds, and proving threshold saturation for the spatially coupled system.

Definition 5: The potential functional, \(U_s : \mathcal{X} \times \mathcal{X} \to \mathbb{R}\), of single system LDPC(\(\lambda, \rho\)) ensemble is defined as

\[
U_s(x; c) = \frac{L'(1)}{\rho^\|(x)} \mathbb{H}(\frac{R^\|(x)}{\rho^\|(x)} + L'(1) \mathbb{H}(\rho^\|(x)) - L'(1) \mathbb{H}(x^\circ \rho^\|(x)) - \mathbb{H}(c \circ L^\circ(\rho^\|(x)))
\]

where \(\mathcal{X}\) denotes the set of symmetric probability measures and the parameter \(h\) is implicit in \(c\).

We will see later the intuition behind using such functional and how it is related to the replica-asymmetric free entropy.

It turns out that fixed points of Definition 2 are also stationary points of \(U_s\). Moreover, the minimum of \(U_s\) occurs only at a fixed point.

Definition 6: For a single system LDPC(\(\lambda, \rho\)) ensemble we define the following

i) The basin of attraction to \(\Delta_\infty\)

\[
\mathcal{V}(c) \triangleq \left\{ a \in \mathcal{X} \mid T_s^{(\infty)}(a; c) = \Delta_\infty \right\}.
\]

ii) The energy gap

\[
\Delta E(c) \triangleq \inf_{x \in \mathcal{X} \setminus \mathcal{V}(c)} U_s(x; c),
\]

with the convention that the infimum over the empty set is \(\infty\) (which is the case below and up to BP threshold where the only fixed point in \(\mathcal{X}\) is the trivial \(\Delta_\infty\)).

Definition 7: The potential threshold is therefore defined to be the largest channel parameter with positive energy gap.

\[
h^* \triangleq \sup \left\{ h \mid \Delta E(h) > 0 \right\}.
\]

It is clear that \(h^*\) of a single system exceeds \(h^\text{BP}\) by including the region where other local minima,
beside the trivial one, occur with positive potential. This region eventually characterizes the additional BP performance of a spatially coupled system due to the perfect side information, and helps in connecting with \( h_{MAP} \) to prove threshold saturation.

Definition 8: One more threshold to define is the stability threshold.

\[
h_{stab} \triangleq \sup\{h \mid \mathcal{B}(c(h))\lambda'(0)\rho'(1) < 1\},
\]

with \( \mathcal{B}(c(h)) \) denotes the Battacharyya functional.

For LDPC ensembles with no degree-two variable-nodes, \( h_{stab} = 1 \). Therefore, under this assumption \( h_{stab} \) plays no necessary role.

We will now extend the DE equation and the notion of potential functional to spatially coupled system. The perfect information at the boundaries propagating inward leads to different message distributions \( x_i \) at different positions of the chain. Therefore, the same functional are applied now to vector of measures \( x \). The previous derivation of DE holds for spatially coupled system with two differences: 1) the boundary conditions that need to be reflected in the DE, 2) the variable-node output distribution and the check-node input distribution, unlike the single system, are no more the same at each position, and they are expressed as a windowed average of each other (the same holds for check-node output distribution and variable-node input distribution).

Definition 9: Accordingly, the DE for a spatially coupled ensemble under BP decoding is described by

\[
x_i^{(t+1)} = \frac{1}{w} \sum_{k=0}^{w-1} c_{i-k} \otimes \lambda \left( \frac{1}{w} \sum_{j=0}^{w-1} \rho \left( x_j^{(t)} \right) \right)
\]

\[
= T_x(c, x_i^{(t)}),
\]

for \( i \in \mathcal{N} \), \( \{1, 2, ..., N + (w - 1)\} \) with \( x_i^{(t)} \) denotes the \( i \)-th check-node input distribution after \( t \) iterations of BP. The boundary conditions are reflected by taking \( c_i = c \) for \( i \in \mathcal{N} = \{1, 2, ..., N\} \), and \( c_i = \Delta_{\infty} \) otherwise. Note that DE can be also expressed in terms of variable-node output distribution which might be a more natural representation, but we will stick with the one provided by Definition 9 for its mathematical tractability.

Definition 10: The coupled potential functional, \( U_c : X^{N+w(w-1)} \rightarrow \mathbb{R} \), is defined to be the spatial average of the single potential as given in [1]. It turns out that fixed points of the coupled DE are also stationary points of \( U_c \).

We will now prove threshold saturation for spatially coupled LDPC ensemble. First, we show using Theorems 11 and 12 that the BP threshold of the coupled system \( h_{BP}^{*} \) (defined similarly to Definition 3 but with \( T_x(c, x) \) vector operator and pointwise convergence to \( \Delta_{\infty} \)) saturates to the potential threshold \( h^{*} \) of the underlying single system. Moreover, knowing that for many LDPC ensembles \( h_{MAP} \) is upper bounded by \( h^{*} \) (Lemma 13), implies that \( h_{BP}^{*} \) saturates to \( h_{MAP}^{*} \).

Theorem 11: Fix a family of BMS channels \( c(h) \), and the LDPC(\( \lambda, \rho \)) ensemble. If \( h \leq h^{*} \), then for all \( N \) and any sufficiently large \( w \) \( (w \geq K_{h_{BP}^{*}}(h)) \), the only fixed point of DE for the spatially-coupled LDPC(\( \lambda, \rho, N, w \)) ensemble with channel \( c(h) \) is \( \Delta_{\infty} \).

Proof: A generic skeleton of the proof is given here. We define first a modified coupled system by adding saturation constraint to the original spatially coupled system. The modified system is degraded with respect to original system, and thus serves as an upper bound. Once the proof is done for the modified system, it will hold for the original spatially coupled system. The proof of uniqueness is straightforward by the monotonicity of the DE. The proof of existence of a trivial fixed point is done by contradiction. We assume a non-trivial fixed point \( x \) and take a small perturbation \( S(\lambda) \) of it. Using second order Taylor expansion of the parametrization \( \phi(t) = U_c((1- t)x + tS(\lambda); c(h)) \) about \( t_0 = 0 \) and evaluated at \( t = 1 \), we show that all variations up to second order can be made arbitrarily small (the first derivative is zero since \( x \) is a fixed point, the absolute valued second derivative is upper bounded by \( \Delta_{\infty}^{2} \) and tends to zero as \( w \rightarrow \infty \)). Knowing that the absolute change in the potential at \( x \) due to a perturbation \( S(\lambda) \) is lower bounded by a constant independent of modified system, gives a contradiction.

Theorem 12: Fix a family of BMS channels \( c(h) \), and the LDPC(\( \lambda, \rho \)) ensemble with \( h^{*} < h_{stab}^{*} \). If \( h > h^{*} \), there exists \( N_0 \) such that for any \( N > N_0 \) and a fixed coupling window \( w_0 \), the fixed point of DE for the spatially-coupled LDPC(\( \lambda, \rho, N, w_0 \)) ensemble with channel \( c(h) \) and \( \Delta_{\infty} \) initialization is degraded with respect to \( \Delta_{\infty} \).

Proof: The proof is based on the negativity of the single system potential for \( h > h^{*} \).
ii) If $h^* < h^\text{lab}$, then $h^\text{MAP} \leq h^*$.

Finally, the connection to $h^\text{MAP}$ is provided via Lemma 13 by lower bounding $h^*$. Moreover, the optimality of the MAP decoder provides an upper bound to $h_c^\text{BP}$. Hence, the saturation to MAP threshold is established

$$h_c^\text{BP} = h^* = h^\text{MAP}. \quad (4)$$

A very similar analysis can be adapted to prove threshold saturation for spatially coupled LDGM ensemble. The existence of non-trivial minimal fixed point, which is due to the non-negligible error floor of such ensembles, alters the definition of the energy gap by subtracting the value of the potential at that point from original definition. This rises some ambiguities on the monotonicity of energy gap and poses difficulties in defining potential threshold. Hence, threshold saturation can be stated here differently by showing that the minimal fixed point can be attained whenever the energy gap is positive (which is conjecture to be the region of MAP decoding).

IV. Finite-length Analysis on BEC under Peeling Decoding

In addition to its practical advantage, the protograph-based spatially coupled LDPC ensemble showed a robust finite-length performance [2]. Therefore, such ensemble is used here to derive the finite-length scaling law. However, the structure imposed by the protograph construction leads to a multi-edge type LDPC code which is harder to analyse. For this reason, we will restrict the analysis for finite-length to BEC with regular LDPC$(l, r, N, w)$ code ensemble in order to spare additional parameters in the analysis.

For BEC, the BP messages along a particular edge can only jump once (from 0 to $\pm\infty$), then stay constant thereafter. Therefore, one can do the BP decoding on BEC in a more efficient way by removing decoded variable nodes from the graph to avoid recomputing all messages. This formulation is called peeling decoding (PD), which is equivalent to BP decoding on BEC.

The PD algorithm starts by removing all non-erased variable nodes from the graph and their associated edges, in addition to resulting unconnected checks. Following this, the decoding proceeds as follows: at each iteration, one variable node connected to degree-one check (if any) is decoded and removed from the graph with the associated edge and check. The sequence of graphs resulting from this algorithm follows a typical path called expected graph evolution that characterises the graph degree distribution at any time and constitutes sufficient statistics for analysis.

**Definition 14**: The normalized multi-edge type degree distribution at time $\tau$ is defined as random process

$$v(x, \tau) = \sum_{d \in \mathcal{F}} v_d(\tau)x^d, \quad r(x, \tau) = \sum_{d \in \mathcal{F}} r_d(\tau)x^d,$$

where $v_d$ ($r_d$) represents the number of variable (check) nodes of multi-edge type $d$, and $\mathcal{F}$ is the set of all possible multi-edge types. Note that $v_d$, $r_d$ and $\tau$ are normalized by $M$, the codeword length of the underlying single LDPC code.

**Definition 15**: The BP threshold $\epsilon^{\text{BP}}$ is therefore defined to be the largest channel erasure parameter $\epsilon$ so that the mean total fraction of degree-one check nodes, given by

$$\hat{c}_1(\tau) \triangleq \frac{1}{rN} \sum_{i=1}^{rN} \hat{r}(0, r, \tau),$$

is positive for any $\tau \in [0, \epsilon N]$, where $\hat{r}(x, \tau)$ is the mean of random process in Definition 14 and $0, r, \tau$ is the zero vector except at the entry $i$. Based on this, we can say that $\hat{c}_1(\tau)$ is the mean of the random process $c_1(\tau)$.

The analytical calculation of $\hat{c}_1(\tau)$ shows two phases: 1) an initial decreasing phase of $\hat{c}_1(\tau)$ where the degree-one check nodes are removed more or less uniformly along the chain, 2) a steady-state phase, which corresponds to the decoding wave moving at a constant speed, where $\hat{c}_1(\tau) = \hat{c}_1(\tau)$. An estimate of $\hat{c}_1(\tau)$ using first-order Taylor expansion shows linear dependency on $\Delta_\epsilon = \epsilon^{\text{BP}} - \epsilon$

$$\hat{c}_1(\tau) \approx \gamma \Delta_\epsilon,$$  \quad (5)

where $\gamma$ is a constant that depends on the ensemble. The key difference between random and photograph ensembles is the value of $\hat{c}_1(\tau)$, mainly $\gamma$, that makes protograph ensemble more robust.

The finite-length scaling law is characterized by the zero-crossing probability of the process $c_1(\tau)$, and can be estimated according to [2] as follows:

$$P^* \approx 1 - \exp \left( -\frac{\epsilon N - \tau^*}{\mu_0(M, \epsilon, l, r)} \right), \quad (6)$$

where $\epsilon N - \tau^*$ is the duration of the steady-state phase and $\mu_0$ is the average survival time of the $c_1(\tau)$ process:

$$\mu_0(M, \epsilon, l, r) \approx \frac{2\pi}{\theta} \int_0^{\sqrt{\frac{\epsilon N}{\alpha}}} \Phi(z)e^{\frac{1}{2}z^2}dz \quad (7)$$

where $\Phi(z)$ is the c.d.f. of the standard Gaussian, $\alpha = \delta_1(\epsilon)\gamma^{-1}$, with $\delta_1$ is proportional to the variance of $c_1(\tau)$ at the steady-state, and $\theta(l, r)$ depends on the coupling pattern.

The performance estimated by the scaling law is compared in [2] to the actual error rate computed by Monte Carlo simulation for both random and
protograph-based ensembles. The higher mean evolution of $\bar{c}_i(\tau)$ in the steady-state, i.e., the higher $\gamma$, obtained for the protograph ensemble explains the performance gain of such ensemble. While both $\delta_1$ and $\theta$ have the same values, the higher $\gamma$ for protograph ensemble leads to an exponential increase of $\mu_0$ in (7), and thus a dramatic reduction in the error rate in (6).

V. Connection between replica method in statistical physics and threshold saturation in coding

The key tool used for proving threshold saturation in Section III is potential functional. In this section, we will provide an insight into this functional by showing its relation with the replica method used in statistical physics [3]. We will first describe the RS free entropy for a general graphical model equipped with Gibbs distribution, and then we will apply it to the LDPC ensemble. It turns out that our potential functional is nothing but the negative of the RS free entropy, or equivalently it is the RS free energy. The RS free entropy describes the average performance of the message-passing algorithm, and thus it has information about the BP, or dynamic, threshold. Furthermore, the RS free entropy tends to estimate the true free entropy of the system. This approximation was recently proven to be exact for large class of LDPC ensembles and BMS channels. The true free entropy is closely related to the conditional entropy that describes the MAP threshold in Definition 4. Therefore, the RS free entropy has also information about the MAP, or static, threshold, and hence it constitutes a powerful tool to prove threshold saturation.

For a graphical model on a factor graph $\Gamma = (V, C, E)$ with $V$, $C$ and $E$ are the sets of variable nodes, check nodes and edges respectively. Each variable node $i \in V$ is attached to a spin $\sigma_i$, belonging to a finite alphabet $\mathcal{A}$ in addition to a function $\phi_i(\sigma_i)$, and each check node $a \in C$ is attached to a constraint function $\psi_a(\{\sigma_i, i \in \partial a\}) = \psi_a(\sigma_a)$. Where $\partial(\cdot)$ denotes the set of all adjacent nodes.

The configuration space of the variables is generally equipped with a probability distribution, called “Gibbs” distribution, of the form

$$\mu(\sigma) = \frac{1}{Z} \prod_{a \in C} \psi_a(\sigma_a) \prod_{i \in V} \phi_i(\sigma_i),$$

with $Z$ denotes the normalizing factor (or partition function). The Gibbs distribution can be also represented in terms of a Hamiltonian or energy function. One is usually interested in estimating the marginals of such distribution using BP algorithm, which is exact on tree.

**Definition 16:** The free entropy is defined as

$$\frac{1}{n} \log Z,$$

with $n = |V|$.

**Definition 17:** We define the (un-normalized) Bethe free entropy $h_{\text{Bethe}}$ as a function of some set of messages $(\mu, \hat{\mu})$

$$\sum_{i \in V} F_i(\hat{\mu}_{i \rightarrow a}, b \in \partial i) + \sum_{a \in C} F_a(\mu_{j \rightarrow a}, j \in \partial a) - \sum_{(i, a) \in E} F_{i,a}(\mu_{i \rightarrow a}, \hat{\mu}_{a \rightarrow i}),$$

where the formulae of $F_i, F_a$, and $F_{i,a}$ are given in [1].

On a tree, the Bethe free entropy expressed in terms of the BP messages gives the true free entropy. But for a general graphical model the Bethe formalism itself is no more accurate, even if the BP messages are exact. However, an important observation is that the stationary points of the Bethe free entropy satisfy the BP equations. The RS free entropy describes the average behaviour of BP algorithm. Therefore, it is defined as the average of the Bethe free entropy after assuming that the set of variable-to-check messages $\mu$ is i.i.d distributed according to a fix trial distribution $m$, and the set of check-to-variable messages $\hat{\mu}$ is i.i.d distributed according to $\hat{m}$ (where $\hat{m}$ is the induced distribution that depends on $m$ through the BP equation linking $\mu$ to $\hat{\mu}$, e.g. equation (2) for the coding case).

**Definition 18:** We define the RS free entropy as a function of the trial distribution $m$

$$h_{\text{RS}}(m) \triangleq \mathbb{E}[h_{\text{Bethe}}],$$

where the expectation is over all random objects.

It turns out that the stationary points of the RS free entropy satisfy the DE equations. Moreover, it was conjectured that the maximum of the RS free entropy, over an appropriate class of trial distributions, tends to approximate the true free entropy. Recently, this approximation was proven to be exact for a large class of LDPC codes and BMS channels.

Applying the RS formalism to the LDPC ensemble, after expressing the BP messages in terms of half-loglikelihood ratios, gives the negative of our potential functional in Definition 5. The spatially coupled potential in Definition 10 can be also expressed in terms of a spatially coupled RS free entropy. In the thermodynamic limit, the statistical physics’ free entropy is equivalent to the information theoretical conditional entropy of the input in a communication channel given the output. Therefore, by the exactness of the replica method one has the following identity

$$\lim_{n \to \infty} \frac{1}{n} \mathbb{E}[H(X^n|Y^n)] = \sup_m h_{\text{RS}}(m)$$

$$= - \inf_{x \in \mathcal{X}} U_x(\kappa; c(h)).$$

Note that this equality was recently proven. Prior to this, it was used as an inequality as we saw in Lemma.
In the same spirit of replica method, the one-step replica symmetry breaking (1RSB) cavity method is introduced in [3] in order to count the number of BP solutions for a constraint satisfaction problem, mainly the XORSAT problem, with long-range correlations in the clustered phase. As the stationary points of the Bethe free entropy satisfy the BP equations, the 1RSB postulates that each BP solution message set \( \mu_\bullet \) corresponds to a Bethe measure with a probability proportional to its Bethe free entropy. This means that each BP message set \( \mu_\bullet \) has a weight \( w_\mu(y) = e^{\beta h_\mu(x, y)}, \) where \( y \) plays the role of an inverse temperature. Moreover, the 1RSB postulates that the original Gibbs distribution is written as a convex combination of all Bethe measures. Therefore, one can obtain an auxiliary constraint satisfaction problem where the BP messages are the new variables with a distribution induced by \( w_\mu(y) \). The 1RSB amounts to applying again the BP algorithm to this auxiliary problem. By computing the complexity of the auxiliary problem, one can count the number of BP solutions of the original problem.

The same formalism can be applied to other message-passing algorithms with many fixed points. Particularly, applying the 1RSB to the min-sum algorithm leads to what is termed as survey propagation.

VI. NON-LINEAR CODES ON SPARSE GRAPHS

The use of parity-check gates is a natural choice for binary linear codes based on sparse graphs, both in the context of lossy source coding and channel coding. In this section, we introduce codes based on sparse graphs with non-linear gates. First, we give an intuition behind using non-linear operators in lossy source coding. We show that such operators might improve the performance of iterative message-passing algorithm by breaking the inherent symmetry of the parity-checks. Then, we extend this approach to error correcting codes.

The lossy source coding consists of mapping a given source word \( x \in \{0, 1\}^n \) to a compressed word \( u \in \{0, 1\}^{nR} \), where \( R \in [0, 1] \) is the compression rate, such that the reconstructed word \( \hat{x}(u) \in \{0, 1\}^n \) has the minimum distortion measured by the relative Hamming distance

\[
d_n(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^{n} |x_i - \hat{x}_i|,
\]

(10)

We can formulate our lossy source coding as a constraint satisfaction problem (CSP) using LDGM code ensemble. We consider the Poisson, or check-regular, LDGM(\( k, R, n \)) ensemble which can be represented by bipartite graphs \( \Gamma = (V, C, E) \) with \( n \) check-nodes of fixed degree \( k \), and \( m = nR \) variable-nodes with i.i.d. Poisson distributed degree. Each variable-node \( i \in V \) represents a code bit \( u_i \) of the compressed word, while each check-node \( a \in C \) is attached to the source bit \( x_a \) and its reconstructed bit \( \hat{x}_a \) and having the decoding function \( f_a \in \{0, 1\} \) with

\[
\hat{x}_a = f_a(u_i \in \partial a).
\]

(11)

The optimal encoding seeks to find the configuration \( y^* \) that minimizes (10), or equivalently violates the smallest number of checks in (11), among all \( u \) in the configuration space \( \{0, 1\}^n \). Since the optimal decoder is an intractable solution that necessitates exhaustive search over the whole configuration space, we formulate the problem as a probabilistic model in order to use iterative message-passing algorithm. Hence, if we equip the configuration space with the conditional probability distribution

\[
\mu_\beta(\mathcal{y} | x) = \frac{1}{Z_\beta(x)} e^{-2\beta nd_\mu(x, \mathcal{y})}
\]

(12)

with \( \beta \) a positive real number and \( Z_\beta(x) \) the normalizing factor, we obtain a Gibbs measure similar to (8) where \( y^* \) represents its maximizer. Moreover, we can relax our problem by estimating the individual bits \( u_i \), with the help of the marginals and BP algorithm, instead of estimating the whole block \( u \).

The use of parity-checks turns our CSP to a MAX-XORSAT problem. Unlike the LDPC codes, a plain message-passing algorithm is not efficient in lossy source coding. This is due to the clustering effect, where there is an exponentially large number of solutions that are grouped into distant clusters and preventing the convergence of BP algorithm. Therefore, a heuristic decimation process is used along with the BP iterations in order to guide the algorithm to converge to one of the solutions. The decimation process requires certain convergence criterion. The BP iterates until the convergence criterion is satisfied or a maximum number of iteration is reached. Then, the code bit \( u_i \) with the highest bias is hard detected and decimated from the graph after having updating the decoding functions \( f_a \) for all \( a \in \partial i \). The decimation process continues until no more code bits remain in the graph. This process is called Belief-Propagation Guided Decimation (BPGD).

While the theoretical performance of such Poisson LDGM codes with parity-checks was proven, by the 1RSB cavity method [9], to achieve the Shannon’s rate-distortion bound under optimal encoding as the check degree \( k \) increases, the algorithmic performance using the heuristic BPGD does not. Moreover, the algorithmic performance under BPGD gets worse as \( k \) increases. We can attribute this behaviour to the full symmetry in the configuration subsets of the XOR
operator, where each bit is equally biased between 0 and 1. The inherent symmetry of the XOR operator persists after decimation, so that the decimated variable gives no hint of how to proceed with the encoding. The idea behind using non-linear checks is to break this symmetry and help the decimation process. After examining several types of non-linear checks, the random checks show to be efficient in breaking the symmetry. Furthermore, numerical simulations show that the algorithmic performance of the proposed scheme approaches the Shannon’s rate-distortion bound as the check degree increases.

We can extend this approach of using sparse graphs with non-linear checks to channel coding. However, one should note the fundamental difference between lossy source coding and channel coding. The former can be interpreted as an estimation problem, where we always tolerate a certain amount of error. Whereas the latter should exhibit a phase transition, where perfect reconstruction is required below certain noise threshold. Therefore, the targeted non-linear checks used in channel coding must reflect this property. In addition to this, using non-linear operators might impose some technical difficulties (the violation of the all-zero codeword assumption, the complexity in the encoding and rate calculation), but we will neglect these at the moment by using a planted codeword model in order to provide a general proof of concept.

Using arbitrary random checks in channel coding showed to be inefficient, since no phase transition can be observed. This can be attributed to the deficiency in the codebook, where the codewords are not well spread as in the case of parity-checks. While this is a blessing for lossy source coding, it turns out to be a curse for channel coding. An important observation that confirms this is that the BP algorithm converges w.h.p. to a wrong codeword with random checks, while this never happens with parity-checks (i.e. for parity-checks the only error occurs when BP converges outside the codebook). Therefore, the idea is to find a class of non-linear checks that behaves at least similar to the parity-checks and that experiences a phase transition with BP decoding.

It turns out that good candidates for non-linear checks are the ones used in locked occupation problem (LOP) [10]. Such checks make the CSP an extremely frozen problem, where every cluster consists of a single configuration. Therefore, they are efficient in channel coding. The LOP checks are defined as follows: the status of each check \( a \) which is connected to \( k \) binary variables \( x_1, \ldots, x_k \in \{0, 1\} \), depends on the number of ones \( r \) in these variables (or equivalently on the sum of variables \( r = \sum_{i \in \partial a} x_i \)). The check is therefore characterized by a vector \( \mathbf{a} = (a_0, \ldots, a_k) \) does not contain consecutive ones. The check \( a \) is satisfied if and only if \( a_r = 1 \). As an example, the check of degree 3 defined by \( \mathbf{a} = (1, 0, 0, 1) \) is satisfied if and only if the number of ones in the connected variables is 0 or 3. Note that the condition that \( \mathbf{a} \) does not contain consecutive ones is crucial to obtain the desired performance by imposing certain distribution on the codewords, and the violation of this condition leads to non-linear checks that do not experience any phase transition with BP decoding. One can also notice that the parity-checks are special cases of LOP checks, where \( \mathbf{a} \) is defined with alternating ones and zeros. Whenever we deviate from the parity-check definition, the LOP check loses its balance and becomes non-linear. The unbalance of LOP checks makes the rate calculation even more complicated.

An important observation about LOP checks is that they define a class of non-linear operators that experience phase transition under BP decoding and never converge element to a wrong codeword. Therefore, they can be used to design efficient non-linear error correcting codes on sparse graphs. It will be interesting to investigate in a future work the rate and the encoding strategy of such codes and provide a rigorous mathematical proof of threshold saturation using DE. Accordingly, one can compare the average performance of such codes over all codewords, by considering the general model instead of the planted one, with that of the LDPC codes of comparable rate.

REFERENCES