



HAL
open science

Evidence of chaos in the Belief Propagation for LDPC codes

Jean-Christophe Sibel, Sylvain Reynal, David Declercq

► **To cite this version:**

Jean-Christophe Sibel, Sylvain Reynal, David Declercq. Evidence of chaos in the Belief Propagation for LDPC codes. Chaotic Modeling and Simulation Journal, 2013, pp 3-18, ISSN 2241-0503. <hal-00825527>

HAL Id: hal-00825527

<https://hal.science/hal-00825527v1>

Submitted on 24 May 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Evidence of chaos in the Belief Propagation for LDPC codes

J.C. Sibel, S. Reynal, and D. Declercq

ETIS / ENSEA / Univ. Cergy-Pontoise / CNRS UMR 8051
F-95000, Cergy-Pontoise, France

(E-mail: {jean-christophe.sibel,reynal,declercq}@ensea.fr)

Abstract. In this paper, we investigate the behaviors of the Belief Propagation algorithm considered as a dynamic system. In the context of LDPC (Low Density Parity-Check) codes, we use the noise power of the transmission channel as a potentiometer to evaluate the different motions that the BP can follow. The computations of dynamic quantifiers as the bifurcation diagram, the Lyapunov exponent and the reconstructed trajectory enable to bring out four main behaviors. In addition, we propose a novel measure that is the hyperspheres method, which provides the knowledge of the time evolution of the attractor size. The information collected from these different quantifiers helps to better understand the BP evolution and to focus on the noise power values for which the BP suffers from chaos.

Keywords: LDPC, iterative map, chaos, Lyapunov exponent, bifurcation diagram.

1 Introduction

The channel coding is a research field whose purpose is to protect an information to transmit from environmental disturbances. The first step is the encoding of the information, a procedure in which the information, modeled as a sequence of k bits u_1, \dots, u_k , is mapped to a larger sequence of N bits x_1, \dots, x_N . The map consists in artificial correlations called constraints or parity-check equations. In [1] are introduced the Low-Density Parity-Check (LDPC) codes which are a widespread technique to encode the information. Such a code can be represented by a Tanner graph [2], a graphical representation which turns out to be very useful in the second step, the decoding. In this part, the bits transmitted through a random noisy channel are iteratively handled by a decoding algorithm to create an associated output sequence of N bits that verify the whole set of parity-check equations and that must be as close as possible to the input sequence. One of the most famous decoding algorithm is the Belief Propagation (BP) [3], also used in statistical physics [4], extensively studied in [5,6], which is deemed to be the optimal message-passing algorithm in the case the Tanner graph of the LDPC code is loopfree. However, in most cases the Tanner graph is not loopfree [7] that involves that the BP becomes suboptimal. Moreover, the BP presents some complex behaviors in terms of the noise power of the transmitted channel, as periodic and chaotic motions [8]. Along the whole paper, we present some

measures to bring out these different behaviors. The paper is organized as follows: in the second section are presented preliminaries about the LDPC codes and the BP, in the third section we present the dynamic environment of the BP, the measures to identify the behaviors and the associated results.

2 LDPC codes and Belief Propagation

We consider a set of N binary random variables $\mathbf{X} = \{X_1, \dots, X_N\}$ whose global state is denoted by $\mathbf{x} = [x_1, \dots, x_N]$. An LDPC code is built by a set of M constraints, or parity-check equations, $\mathbf{C} = \{C_1, \dots, C_M\}$ such that for each check C_j its state is $c_j = \sum_{X_i \in \mathcal{N}_j} x_i$ where \mathcal{N}_j is a subset of \mathbf{X} called the neighborhood of C_j depending on the LDPC code, and the sum is computed over the Galois field $\text{GF}(2)$. We consider that C_j and X_i such that $X_i \in \mathcal{N}_j$, form an edge e_{ij} between two nodes inside an undirected bipartite graph called the Tanner graph $\mathbf{G} = (\mathbf{X} \cup \mathbf{C}, \{e_{ij}\})$. An example of a Tanner graph is displayed on the figure 1.

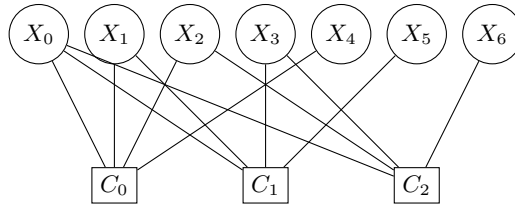


Fig. 1. Tanner graph of the Hamming code

The purpose of the BP is to estimate the joint probability distribution $p(\mathbf{X} = \mathbf{x})$, written simply $p(\mathbf{x})$, by a distribution called the belief $b(\mathbf{x})$ and to extract the most likely state $\hat{\mathbf{x}} = \arg \max_{\mathbf{x}} b(\mathbf{x})$ considered as the estimate of the input sequence. Each variable X_i has its own marginal probability distribution $p_i(x_i)$ and its own belief $\{b_i(x_i)\}_{1 \leq i \leq N}$. The BP is an iterative algorithm that consists in passing messages between the variables and the constraints on the edges of a given Tanner graph at each iteration k . For each edge e_{ij} :

- the messages $n_{ji}^{(k)}(x_i)$ from C_j to X_i are: $n_{ji}^{(k)}(x_i) = f_{ji}(\{m_{xy}^{(k-1)}\}_{(x,y)})$
- the messages $m_{ij}^{(k)}(x_i)$ from C_i to C_j are: $m_{ij}^{(k)}(x_i) = g_{ij}(\{n_{yx}^{(k)}\}_{(x,y)}, l_i(x_i))$

where the functions f_{ij} and g_{ji} are detailed in [2], and $\{l_i(x_i)\}_i$ are the likelihoods $\mathbf{L}(\mathbf{x}) = \{l_1(x_1) = p(y_1|x_1), \dots, l_N(x_N) = p(y_N|x_N)\}$ computed from the channel observations $\{y_1, \dots, y_N\}$. The noisy transmission channel that we use in all of our simulations is an additive white Gaussian noise channel whose power is σ^2 . We summarize the message-passing by a unique implicit equation $\forall e_{ij}, n_{ji}^{(k)} = G_{ij}(\{n_{nm}^{(k-1)}\}_{(m,n)}, \{l_i\}_i)$. The convergence

of the BP is: $\forall e_{ij}, n_{ji}^{(k)} = n_{ji}^{(k-1)}$. These messages provide the computation of the beliefs, whose equations are defined in [2]. All the simulations that follow are done on a commonly used example which is the Tanner code [9].

3 Dynamics

3.1 State space definition and properties

We consider $\{G_{ij}\}_{(i,j)}$ as a set of iterated maps on the state variables $\{n_{ji}^{(k)}\}_{(i,j)}$ and $T^{(k)} = \{n_{ji}^{(k)}\}_{(i,j)}$ as the points of the trajectories of the BP at iteration k in the associated state space \mathcal{E} .

3.2 Parameters and scaling

In [8] the value of σ^2 , or the corresponding Signal to Noise Ratio (SNR), is used as a parameter such that different values imply different motions of the BP. However, most of their simulations are done for particular noise realizations and scaled on the SNR, that prevents from evaluating a statistical behavior. A reason is that the noise realizations that lead the BP not to converge or to converge to a wrong estimate are rare events, essentially because the LDPC codes and the iterative algorithms are created to this end. A way to have some statistical evaluations of the behavior of the BP is:

1. finding some of these noise realizations,
2. storing the corresponding initializations on the state variables,
3. averaging the quantities to measure for a sufficient set of initializations that are close in the state space in the sense of the Euclidean distance.

By this way, we target the critical values, i.e. the SNR that correspond to a blatant change in the behavior of the algorithm, which are the bifurcations.

3.3 Bifurcation diagram

A relevant method to extract the critical values of the SNR is the use of the bifurcation diagram. It consists in evaluating the value of a function E that is computed from the state variables at their steady state for J different values of the SNR. We get a sequence $[E_{\sigma_1}, \dots, E_{\sigma_J}]$ that represents the behavior of the dynamic system in terms of the SNR. We consider the following function exposed in [8] called the mean square beliefs:

$$\forall \sigma, \quad E_\sigma = \sqrt{\frac{1}{N} \sum_{i=0}^{N-1} b_i^2(0)} \quad (1)$$

where the input sequence in the channel is the null sequence and the beliefs are computed at the last iteration K of the BP algorithm. Obviously, there is

no reason that the associated dynamic system has reached any steady state at this iteration but we need to suppose it for computation time's sake. This function presents three important values:

- $E_\sigma = 1$: all the beliefs indicate that the output sequence is the null sequence which is a good decoding,
- $E_\sigma = \frac{1}{4}$: all the beliefs are uniform thus there is no information about the state of the transmitted bits, which is a missed decoding,
- $E_\sigma = 0$: all the beliefs indicate that the output sequence is the complementary of the sent sequence, which is a completely wrong decoding.

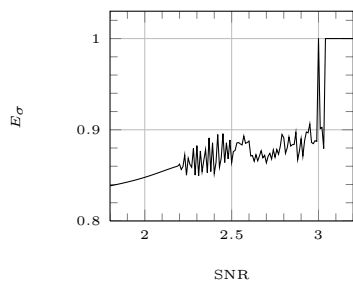


Fig. 2. Bifurcation diagrams of the BP

critical value, the algorithm follows a periodic motion. However, for values in [2.5 dB, 2.98 dB] it does not appear any known evolution which can be an indication of chaos. For values greater than 2.99 dB, the BP converges to the good decoding state.

The display of $[E_{\sigma_1}, \dots, E_{\sigma_J}]$ enables to know two properties of the used algorithm: the amplitudes provides information about the decoding performance, and the variation between successive values gives us the critical values of the SNR. We display on the figure 2 the mean bifurcation diagrams of the BP. We observe that for SNRs lower than 2.19 dB, the BP follows a regular increasing steady motion. When the SNR is greater than this critical

3.4 Reduced trajectory

Another use of the mean square beliefs function is the representation of the trajectory in a 3-dimensional state space. To this end, we use the phase space reconstruction [10]. The method is first to compute this function at each iteration to get the following sequence $\mathbf{E}_\sigma = [E_\sigma(k)]_{0 \leq k \leq K}$. After that we share this one dimensional sequence in a three dimensional sequence $\tilde{\mathbf{E}}_\sigma$. On the figures 3 and 5 are displayed some reduced trajectories of the BP for typical values of the SNR deduced from the previous bifurcation diagram.

It appears four typical behaviors that match with the four intervals exposed in the previous paragraph. We obtain a very small sized attractor for SNR = 2.10 dB that can be considered as a fixed point, whereas the reduced trajectory transforms to a limit cycle when the SNR is between 2.19 dB and 2.49 dB. A crucial point is that the thickness of the trajectory along this limit cycle increases as the SNR is getting greater up to 2.50 dB.

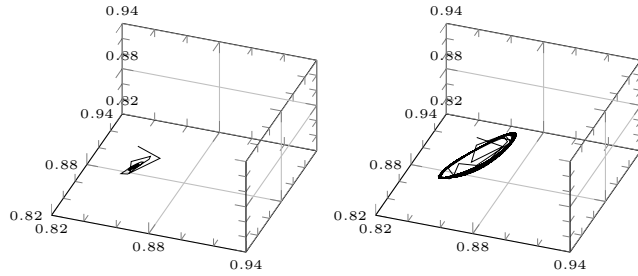


Fig. 3. Reduced trajectory for the BP on the Tanner code with SNR = 2.15 dB and 2.30 dB

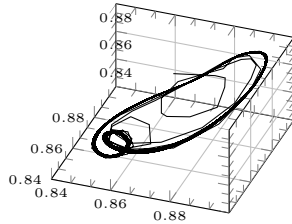


Fig. 4. Reduced trajectory for the BP on the Tanner code with SNR = 2.40 dB

At the same time this limit cycle interleaves with other limit cycles, that can be understood as a sequence of period doubling bifurcations in terms of dynamic system, as is displayed on the figure 4 with two interleft cycles. Such a phenomenon is a typical route to chaos, that is observable from 2.51 dB. A chaotic motion means that there is not any periodic motion or fixed point convergence anymore, as it is displayed for 2.70 dB. When the SNR reaches 2.99 dB the trajectory collapses to a single point that is a true fixed point.

When the SNR reaches 2.99 dB the trajectory collapses to a single point that is a true fixed point.

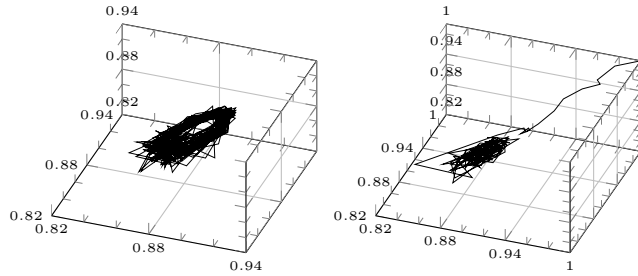


Fig. 5. Reduced trajectory for the BP on the Tanner code with SNR = 2.70 dB and 3.00 dB

We have to be cautious because $\tilde{\mathbf{E}}_\sigma$ is not a true trajectory, it does not respect the Cauchy-Lipschitz condition [10] due to the non bijection between the messages and the beliefs. Thus, this sequence only has the role of giving clues about the true behavior as the possible shape of the actual trajectory in \mathcal{E} that are: convergence to a fixed point, convergence to a limit cycle,

convergence to a chaotic attractor. To distinguish these shapes, we need a criterion that reflects the behavior by its own value.

3.5 Lyapunov exponents

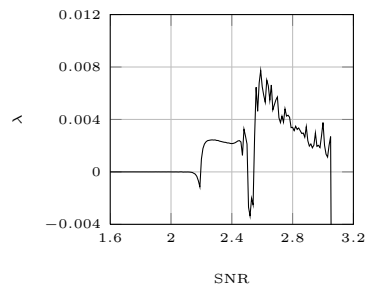


Fig. 6. Lyapunov exponents of the BP on the Tanner code scaled on the SNR

A common measure is the Lyapunov exponent λ , that consists in evaluating at each iteration $k \leq K$ the log-ratio of the Euclidean distance between two initially close trajectories. As detailed in [11,10] the sign of λ reveals the behavior of the system around the corresponding initialization of the trajectories: $\lambda \geq 0$ means the trajectories have moved away one from the other, which is an evidence of a chaotic behavior, $\lambda \leq 0$ means the trajectories have got closer, which is an evidence of a convergent behavior to a small sized volume of the state space. This volume is reduced to a fixed point if and only if $\lambda \rightarrow -\infty$. When λ crosses the x-axis the system suffers from a bifurcation meaning that the algorithm has changed of motion. The corresponding SNR are the critical values. We display on the figure 6 the Lyapunov exponents of the BP on the Tanner code. As we have observed on the bifurcation diagrams, the evolution is really different as soon as the SNR is greater than 2.09 dB. The BP curves is perfectly consistent with the associated bifurcation diagram in the sense that the critical values we extract are the same and the behaviors we could imagine by the bifurcation diagram are also revealed by the Lyapunov exponent. A relevant analyze we need to effect is the comparison with the reduced trajectory we exposed previously so as to associate accurately with each reduced motion a particular evolution of λ . For $\text{SNR} \in [0\text{dB}; 2.19\text{db}]$: the reduced trajectory converges to a very small sized volume of \mathcal{E}_{BP} that we can consider as a fixed point whereas λ is close to the null value, for $\text{SNR} \in [2.20\text{db}; 2.49\text{db}]$: the reduced trajectory is trapped into a limit cycle whereas λ has gone over a stair, for $\text{SNR} \in [2.50\text{db}; 2.98\text{db}]$: the reduced trajectory does not converge to any fixed point, limit cycle or quasi-limit cycle but to a chaotic attractor whereas λ soars to high values, for $\text{SNR} \in [2.99\text{db}; +\infty\text{db}]$: the reduced trajectory converges to a fixed point corresponding to a good decoding.

3.6 Hyperspheres method

We propose here a novel method to evaluate the unstability of the BP, based on its own trajectory in \mathcal{E} . This method is complementary to the Lyapunov exponent measure because it reveals the size of the attractor that the trajectory falls into and some other properties about the limit cycles. This method

consists in computing the rays R_k of the hyperspheres circumscribed to the trajectory inside a given temporal window centered around each point $T^{(k)}$.

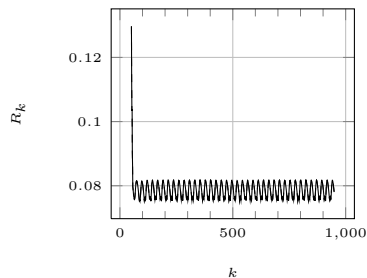


Fig. 7. Evolution of two hyperspheres rays corresponding to two initially close trajectories of the BP on the Tanner code at SNR = 2.10 dB, SNR = 2.30 dB

exponent observations. More accurately we can see that the rays has different oscillations step. This is due to the period doubling bifurcations explained previously. During 92 iterations in average for $k \leq 500$, the trajectory is trapped in a given limit cycle and for the next 92 iterations the trajectory falls into another limit cycle of different ray. For both it is possible to measure the period or pseudo-period that is the same as the period of the first limit cycle, that is 23 iterations. For $k \geq 500$ we cannot distinguish these different phases of evolution, the period doubling has led to chaos.

On the figure 7 are displayed the evolutions of two rays that correspond to two initially close trajectories in the Euclidean sense. The motion we observe for SNR = 2.30 dB is consistent with the limit cycle we observed on the reduced trajectory. The curve of the ray enables to estimate the period of the trajectory around 23 iterations. Moreover we can assert that this limit cycle is stable because the two rays cannot be distinguished. For 2.70 dB the rays moved away one from the other as it was predicted by the Lyapunov

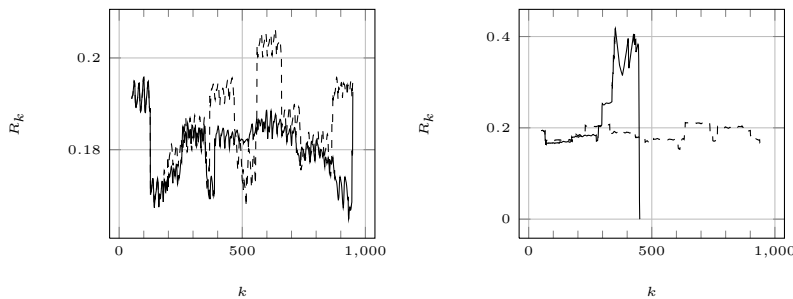


Fig. 8. Evolution of two hyperspheres rays corresponding to two initially close trajectories of the BP on the Tanner code at SNR = 2.70 dB, SNR = 3.00 dB

Such an observation makes our method relevant to bring out crucial information by a one dimensional function. Another important aspect of the hyperspheres method is the raising of the behaviors difference between two initially close trajectories: we easily observe that the evolution of the rays cannot be distinguished while $k \leq 200$ but as k is getting greater, the evo-

lution of the rays move away one from the other but they follow the same kind of motion. For both of them the hypervolumes of the state space in which they are locking in are quite of the same size. When the SNR reaches the last critical value we observe that one of the rays decreases to the null value because the BP has converged to a fixed point. The other ray has not collapsed yet because the SNR is just at the critical value, if it was increased a little we would see the two rays going to zero.

4 Conclusion

In this paper, we raised the dynamics issue of the BP by the use of known and new measures. The most important result is that the BP follows a systematic scheme when the decoding is not trivial: convergence to a small-sized attractor, locking in a limit cycle, chaos and convergence to a fixed-point. Such a property is really useful because it helps to bring out the critical values of the noise power of the channel for which the BP could present complex behaviors. Another advantage of our study is that all the measures we used can be applied on any other decoding algorithms. Therefore, we have started to create a toolbox for the dynamics study of the LDPC decoders.

References

- 1.R.G. Gallager. Low-Density Parity-Check Codes. *PhD Thesis, MIT*, 1963.
- 2.F.R. Kschischang, B. J. Frey eand H.A. Loeliger. Factor Graphs and the Sum-Product Algorithm. *IEEE Trans. on Inf. Theory*, 47.2, 2001.
- 3.J. Pearl. Probablistic Reasoning in Intelligent Systems: Networks of Plausible Inference. *Morgan Kaufmann publisher*, 1988.
- 4.H.A. Bethe. Statistical Theory of Superlattices. *Proc. Roy. Soc. London*, 1935.
- 5.T.J. Richardson. Error floors of LDPC codes. *Proc. 41st Annual Allerton Conf. on Comm. Cont. and Comp.*, 2003.
- 6.S.Y Chung, T.J. Richardson and R.L. Urbanke. Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation. *IEEE Trans. on Inf. Theory*, 47.2, 2001.
- 7.K.P. Murphy, Y. Weiss and M.I. Jordan. Loopy belef propagation for approximate inference: an empirical study. *Proc. Uncertainty in AI*, 1999.
- 8.X. Zheng, F.C.M. Lau, C.K. Tse and S.C. Wong. Study of bifurcation behavior of LDPC decoders. *Int. Journal of Bifurcation and Chaos*, 16:3435–3449, 2005.
- 9.R.M. Tanner, R. Michael, D. Sridhara and T. Fuja. A Class of Group-Structured LDPC Codes. 2001.
- 10.R. Hilborn. Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers. *Oxford University Press publisher*, 2000.
- 11.M.T. Rosenstein, J.J. Collins and C.J. De Luca. A practical method for calculating largest Lyapunov exponents from small data sets. *Physica D*, 65:117–134, 1993.