

# Conditional Random Fields, Planted Constraint Satisfaction, and Entropy Concentration

Emmanuel Abbe\* and Andrea Montanari†

## Abstract

This paper studies a class of probabilistic models on graphs, where edge variables depend on incident node variables through a fixed probability kernel. The class includes planted constraint satisfaction problems (CSPs), as well as more general structures motivated by coding and community clustering problems. It is shown that under mild assumptions on the kernel and for sparse random graphs, the conditional entropy of the node variables given the edge variables concentrates around a deterministic threshold. This implies in particular the concentration of the number of solutions in a broad class of planted CSPs, the existence of a threshold function for the disassortative stochastic block model, and the proof of a conjecture on parity check codes. It also establishes new connections among coding, clustering and satisfiability.

---

\* Department of Electrical Engineering and Program in Applied and Computational Mathematics, Princeton University, Email: eabbe@princeton.edu

† Departments of Electrical Engineering and Statistics, Stanford University, Email: montanari@stanford.edu

# 1 Introduction

This paper studies a class of probabilistic models on graphs encompassing models of statistical learning theory, coding theory, and random combinatorial optimization. Depending on the framework, the class may be described as a family of conditional random fields, memory channels, or planted constrained satisfaction problems. We start by providing motivations in the latter framework.

Constrained satisfaction problems (CSPs) are key components in the theory of computational complexity as well as important mathematical models in various applications of computer science, engineering and physics. In CSPs, a set of variables  $x_1, \dots, x_n$  is required to satisfy a collection of constraints involving each a subset of the variables. In many cases of interest, the variables are Boolean and the constraints are all of a common type: e.g., in  $k$ -SAT, the constraints require the OR of  $k$  Boolean variables or their negations to be TRUE, whereas in  $k$ -XORSAT, the XOR of the variables or their negations must equal to zero. Given a set of constraints and a number of variables, the problem is to decide whether there exists a satisfying assignment. In random CSPs, the constraints are drawn at random from a given ensemble, keeping the constraint density<sup>1</sup> constant. In this setting, it is of interest to estimate the *probability* that a random instance is satisfiable. One of the fascinating phenomenon occurring for random instances is the phase transition, which makes the task of estimating this probability much easier in the limit of large  $n$ . For a large class of CSPs, and as  $n$  tends to infinity, the probability of being satisfiable tends to a step function, jumping from 1 to 0 when the constraint density crosses a critical threshold. For random  $k$ -XORSAT the existence of such a critical threshold is proved [DR08, DM02, DGM<sup>+</sup>10, PS12]. For random  $k$ -SAT,  $k \geq 3$ , the existence of a  $n$ -dependent threshold is proved in [Fri99]. However it remains open to show that this threshold converges when  $n$  tends to infinity. Upper and lower bounds are known to match up to a term that is of relative order  $k 2^{-k}$  as  $k$  increases [ANP05]. Phase transition phenomena in other types of CSPs are also investigated in [AKKT02, MRT09, ANP05]

In planted random CSPs, a “planted assignment” is first drawn, and the constraints are then drawn at random so as to keep that planted assignment a satisfying one. Planted ensembles were investigated in [BHL<sup>+</sup>02, HJKN05, AKG, AJM04, JMS05, ACO08], and at high density in [AMZ06, ACOV07, FMV06]. In the planted setting, the probability of being SAT is always one by construction, and a more relevant question is to determine the actual *number* of satisfying assignments. One would expect that this problem becomes easier in the limit of large  $n$  due to an asymptotic phenomenon. This paper shows that, indeed, a concentration phenomenon occurs: for a large class of planted CSPs (including SAT, NAE-SAT and XOR-SAT) the normalized logarithm of the number of satisfying assignment concentrates around a deterministic number. Moreover, this deterministic threshold is  $n$ -independent.

It is worth comparing the result obtained in this paper for planted CSPs, with the one obtained in [AM] for non planted CSPs. In that case, the number of solution is zero with positive probability and therefore the logarithm of the number of solution does not have a finite expectation. Technically, standard martingale methods does not allow to prove concentration, even around an  $n$ -dependent threshold. In [AM] an interpolation method [GT02] is used to prove the existence of the limit of a ‘regularized’ quantity, namely the logarithm of the number of solutions plus one, divided by the number of variables. A technical consequence of this approach is that the concentration of this quantity around a value that is independent of  $n$  can only be proved when the UNSAT probability

---

<sup>1</sup>The ratio of the expected number of constraints per variables.

is known to be  $O(1/\log(n)^{1+\varepsilon})$ .

This paper shows that –in the planted case– the concentration around an  $n$ -independent value holds unconditionally and is exponentially fast. We use again the interpolation technique [GT02, FL03, FLT03, PT04, BGT10, AM] but with an interesting twist. While in all the cited references, the entropy (or log-partition function) is shown to be superadditive, in the present setting it turns out to be subadditive.

Let us also mention that a fruitful line of work has addressed the relation between planted random CSPs and their non planted counterparts in the satisfiable phase [ACO08], and in [KZ09, ZK11]. These papers show that, when the number of solutions is sufficiently concentrated, planting does not play a critical role in the model. It would be interesting to use these ideas to ‘export’ the concentration result obtained here to non planted models.

In this paper, we pursue a different type of approach. Motivated by applications<sup>2</sup>, in particular in coding theory and community clustering, we consider extensions of the standard planted CSPs to a setting allowing soft probabilistic constraints. Within this setting, the planted solution is an unknown vector to be reconstructed, and the constraints are regarded as noisy observations of this unknown vector. For instance one can recover the case of planted random  $k$ -SAT as follows. Each clause is generated by selecting first  $k$  variable indices  $i_1, \dots, i_k$  uniformly at random, representing the hyperedge of a random graph. Then a clause is drawn uniformly among the ones that are satisfied by the variables  $x_{i_1}, \dots, x_{i_k}$  appearing in the planted assignment. The clause can hence be regarded as a noisy observation of  $x_{i_1}, \dots, x_{i_k}$ . More generally the formula can be seen as a noisy observation of the planted assignment.

Our framework extends the above to include numerous examples from coding theory and statistics. Within LDPC or LDGM codes [RU08], encoding is performed by evaluating the sum of a random subset of information bits and transmitting it through a noisy communication channel. The selection of the information bits is described by a graphs, drawn at random for the code construction, and the transmission of these bits leads to a noisy observation of the graph variables. Similarly, a community clustering block model [GZFA10] can be seen as a random graph model, whereby each edge is a noisy observation of the community assignments of the adjacent nodes. Definitions will be made precise in the next section.

The conditional probability of the unknown vector given the noisy observations takes the form of a graphical model, i.e. factorizes according to an hypergraph whose nodes correspond to variables and hyperedges correspond to noisy observations. Such graphical models have been studied by many authors in machine learning [Laf01] under the name of ‘conditional random fields’, and in [Mon08] in the context of LDPC and LDGM codes. The conditional entropy of the unknown vector given the observations is used here to quantify the residual uncertainty of the vector. This is equivalent to considering the mutual information between the node and edge variables. In such a general setting, we prove that the conditional entropy per variable concentrates around a well defined deterministic limit. This framework allows a unified treatment of a large class of interesting random combinatorial optimization problems, raises new connections among them, and opens up to new models. We obtain in particular a proof of a conjecture posed in [RKPSS10] on low-density parity-check codes, and the existence of a threshold function for the disassortative stochastic block model [DKMZ11].

---

<sup>2</sup>Planted models are also appealing to cryptographic application, as hard instances with known solutions provide good one-way functions.

## 2 The model

Let  $k$  and  $n$  be two positive integers with  $n \geq k$ .

- Let  $V = [n]$  and  $g = (V, E(g))$  be a hypergraph with vertex set  $V$  and edge set  $E(g) \subseteq E_k(V)$ , where  $E_k(V)$  denotes the set of all possible  $\binom{n}{k}$  hyperedges of order  $k$  on the vertex set  $V$ . We will often drop the term “hyper”.
- Let  $\mathcal{X}$  and  $\mathcal{Y}$  be two finite sets called respectively the input and output alphabets. Let  $Q(\cdot|\cdot)$  be a probability transition function (or channel) from  $\mathcal{X}^k$  to  $\mathcal{Y}$ , i.e., for each  $u \in \mathcal{X}^k$ ,  $Q(\cdot|u)$  is a probability distribution on  $\mathcal{Y}$ .
- To each vertex in  $V$ , we assign a node-variable in  $\mathcal{X}$ , and to each edge in  $E(g)$ , we assign an edge-variable in  $\mathcal{Y}$ . We define

$$P_g(y|x) \equiv \prod_{I \in E(g)} Q(y_I|x[I]), \quad x \in \mathcal{X}^V, y \in \mathcal{Y}^{E(g)}, \quad (1)$$

where  $y_I$  denotes the edge-variable attached to edge  $I$ , and  $x[I]$  denotes the  $k$  node-variables attached to the vertices adjacent to edge  $I$ . This defines for a given hypergraph  $g$  the probability of the edge-variables given the node-variables.

The above is a type of factor or graphical model, or a planted constraint satisfaction problem with soft probabilistic constraints. For each  $x \in \mathcal{X}^V$ ,  $P_g(\cdot|x)$  is a product measure on the set of edge-variables. We call  $P_g$  a **graphical channel with graph  $g$  and kernel  $Q$** . We next put the uniform probability distribution on the set of node-variables  $\mathcal{X}^V$ , and define the a posteriori probability distribution (or reverse channel) by

$$R_g(x|y) \equiv \frac{1}{S_g(y)} P_g(y|x) 2^{-n}, \quad x \in \mathcal{X}^V, y \in \mathcal{Y}^{E(g)}, \quad (2)$$

where

$$S_g(y) \equiv \sum_{x \in \mathcal{X}^V} P_g(y|x) 2^{-n} \quad (3)$$

is the output marginal distribution.

We now define two probability distributions on the hypergraph  $g$ , which are equivalent for the purpose of this paper:

- A sparse Erdős-Rényi distribution, where each edge is drawn independently with probability  $p = \frac{\alpha n}{\binom{n}{k}}$ , where  $\alpha > 0$  is the edge density.
- A sparse Poisson distribution, where for each  $I \in E_k(V)$ , a number of edges  $m_I$  is drawn independently from a Poisson distribution of parameter  $p = \frac{\alpha n}{\binom{n}{k}}$ . Note that  $m_I$  takes value in  $\mathbb{Z}$ , hence  $G$  is now a multi-edge hypergraph. To cope with this more general setting, we allow

the edge-variable  $y_I$  to take value in  $\mathcal{Y}^{m_I}$ , i.e.,  $y_I = (y_I(1), \dots, y_I(m_I))$ , and define (with a slight abuse of notation)

$$Q(y_I|x[I]) = \prod_{i=1}^{m_I} Q(y_I(i)|x[I]). \quad (4)$$

This means that for each  $I$ ,  $m_I$  i.i.d. outputs are drawn from the kernel  $Q$ . If  $m_I = 0$ , no edge is drawn. We denote by  $\mathcal{P}_k(\alpha, n)$  the above distribution on (multi-edge) hypergraphs.

Since  $p = \frac{\alpha n}{\binom{n}{k}}$ , the number of edges concentrates around its expectation given by  $\alpha n$  and the two models are equivalent in the limit of large  $n$  — at least they are equivalent for the subsequent results.

### 3 Main Results

We now define the conditional entropy between the node and edge variables. This is equivalent, up to a constant shift, to the mutual information between the node and edge variables.

**Definition 3.1.** Let  $X$  be uniformly drawn in  $\mathcal{X}^n$ ,  $G$  be a random sparse hypergraph drawn from the  $\mathcal{P}_k(\alpha, n)$  ensemble independently of  $X$ , and  $Y$  be the output of  $X$  through the graphical channel  $P_G$  defined in (1) for a kernel  $Q$ . We define

$$H_G^{(n)}(X|Y) \equiv -2^{-n} \sum_{x \in \mathcal{X}^V} \sum_{y \in \mathcal{Y}^{E(G)}} P_G(y|x) \log R_G(x|y), \quad (5)$$

$$H^{(n)}(X|Y) \equiv \mathbb{E}_G H_G^{(n)}(X|Y), \quad (6)$$

where  $P_G$  and  $R_G$  are defined in (1) and (2) respectively. Note that  $H_G^{(n)}(X|Y)$  is a random variable since  $G$  is random, and for a realization  $G = g$ ,  $H_g^{(n)}(X|Y)$  is the conditional entropy of  $X$  given  $Y$ , which can be expressed as  $H_g^{(n)}(X|Y) = \mathbb{E}_y H_g^{(n)}(X|Y = y)$ . Note that the mutual information between the node and edge variables is also obtained as  $I_g^{(n)}(X|Y) = n - H_g^{(n)}(X|Y)$ .

**Definition 3.2.** We denote by  $M_1(\mathcal{X}^l)$  the set of probability measures on  $\mathcal{X}^l$ . For a kernel  $Q$  from  $\mathcal{X}^k$  to  $\mathcal{Y}$ , we define

$$\Gamma_l : M_1(\mathcal{X}^l) \rightarrow \mathbb{R} \quad (7)$$

$$\nu \mapsto \Gamma_l(\nu) = \frac{1}{|\mathcal{Y}|} \sum_{u^{(1)}, \dots, u^{(l)} \in \mathcal{X}^k} \left[ \sum_{z \in \mathcal{Y}} \prod_{r=1}^l (1 - Q(z|u^{(r)})) \right] \prod_{i=1}^k \nu(u_i^{(1)}, \dots, u_i^{(l)}). \quad (8)$$

**Hypothesis H.** A kernel  $Q$  is said to satisfy hypothesis H if  $\Gamma_l$  is convex for any  $l \geq 1$ .

Despite the lengthy expression, it is important to note that the definition of  $\Gamma_l$  depends solely on the kernel  $Q$ . We will see in Section 4 that a large variety of kernels satisfy this hypothesis, including kernels corresponding to parity-check encoded channels, planted SAT, NAE-SAT, XORSAT, and disassortative stochastic block models.

We first show a sub-additivity property for the expected conditional entropy of graphical channels.

**Theorem 3.3.** *Let  $Q$  be a kernel satisfying hypothesis  $H$  and  $n = n_1 + n_2$ , with  $n_1, n_2 \geq k$ . Then*

$$H^{(n)}(X|Y) \leq H^{(n_1)}(X|Y) + H^{(n_2)}(X|Y). \quad (9)$$

The proof of this theorem is outlined in Section 5.

**Corollary 3.4.** *Let  $Q$  be a kernel satisfying hypothesis  $H$ . There exists  $C_k(\alpha, Q)$  such that*

$$\frac{1}{n}H^{(n)}(X|Y) \rightarrow C_k(\alpha, Q), \quad \text{as } n \rightarrow \infty. \quad (10)$$

The following is obtained using previous corollary and a concentration argument.

**Theorem 3.5.** *Let  $Q$  be a kernel satisfying hypothesis  $H$ , then, almost surely,*

$$\lim_{n \rightarrow \infty} \frac{1}{n}H_G^{(n)}(X|Y) = C_k(\alpha, Q), \quad (11)$$

with  $C_k(\alpha, Q)$  as in Corollary 3.4.

The proof is given in Section A.

## 4 Applications

We next present three applications of the general model described in previous section. While planted CSPs and parity-check codes are directly derived as particular cases of our model, the stochastic block model is obtained with a limiting argument. One of the advantages of relying on a general model class, is that it allows to consider new hybrid structures. For example, one may consider codes which are not linear but which rely on OR gates as in SAT, or on community models whose connectivity rely on collections of  $k$  nodes.

### 4.1 Planted constraint satisfaction problems

**Definition 4.1.** *A CSP kernel is given by*

$$Q(z|u) = \frac{1}{|A(u)|} \mathbb{1}(z \in A(u)), \quad u \in \mathcal{X}^k, z \in \mathcal{Y}, \quad (12)$$

where  $A(u)$  is a subset of  $\mathcal{Y}$  containing the “authorized constraints”, with the property that  $|A(u)|$  is constant (it may depend on  $k$  but not on  $u$ ).

We next show that a graphical channel with a CSP kernel corresponds to a planted CSP. We derive first a few known examples from this model.

- For planted  $k$ -SAT,  $\mathcal{Y} = \{0, 1\}^k$  and  $A(u) = \{0, 1\}^k \setminus \bar{u}$ , where  $\bar{u}$  is the vector obtained by flipping each component in  $u$ . Using this kernel for the graphical channel means that for any selected edge  $I \in E_k(V)$ , the edge variable  $y_I$  is a vector in  $\{0, 1\}^k \setminus \bar{x}[I]$  uniformly drawn, representing the negation pattern of the constraint  $I$ . Note that using  $u$  rather than  $\bar{u}$  leads to an equivalent probabilistic model,  $\bar{u}$  is simply used here to represent  $u$  as a “satisfying assignment”. Note that  $|A(u)| = 2^k - 1$ .

- For planted  $k$ -NAE-SAT,  $\mathcal{Y} = \{0, 1\}^k$  and  $A(u) = \{0, 1\}^k \setminus \{u, \bar{u}\}$ , with  $|A(u)| = 2^k - 2$ .
- For  $k$ -XOR-SAT,  $\mathcal{Y} = \{0, 1\}$  and  $A(u) = \bigoplus_{i=1}^k u_i$  and  $|A(u)| = 1$ .

In general, a graphical channel with graph  $g$  and kernel  $Q$  as in (12) leads to a planted CSP where the constraints are given by  $A(x[I]) \ni y_I$  for any  $I \in E(g)$ . For example, for planted  $k$ -SAT, the constraints are  $\bar{x}[I] \neq y_I$ , whereas for planted  $k$ -NAE-SAT, the constraints are  $\bar{x}[I] \notin (y_I, \bar{y}_I)$ . If  $y$  is drawn from the output marginal distribution  $S_g$  (cf. (3)), then there exists a satisfying assignment by construction.

**Lemma 4.2.** *For a graphical channel with graph  $g$  and CSP kernel  $Q$  as in (12), and for  $y$  in the support of  $S_g$ ,*

$$H_g(X|Y = y) = \log Z_g(y) \quad (13)$$

where  $Z_g(y)$  is the number of satisfying assignments of the corresponding planted CSP.

**Corollary 4.3.** *For a graphical channel with CSP kernel  $Q$  as in (12), and for a graph drawn from the ensemble  $\mathcal{P}(\alpha, n)$ ,*

$$H^{(n)}(X|Y) = \mathbb{E}_{G,Y} \log Z_G(Y), \quad (14)$$

where  $Z_G(Y)$  is the number of satisfying assignments of the corresponding random planted CSP.

**Lemma 4.4.** *For any  $k \geq 1$ , and for the CSP kernel corresponding to planted  $k$ -SAT, the operator  $\Gamma_l$  is convex for any  $l \geq 1$ .*

**Lemma 4.5.** *For any  $k \geq 1$ , and for the CSP kernel corresponding to planted  $k$ -NAE-SAT, the operator  $\Gamma_l$  is convex for any  $l \geq 1$ .*

**Lemma 4.6.** *For any  $k$  even, and for the CSP kernel corresponding to planted  $k$ -XOR-SAT, the operator  $\Gamma_l$  is convex for any  $l \geq 1$ .*

Using Theorem 3.5 and previous lemmas, the following is obtained.

**Corollary 4.7.** *For random planted  $k$ -SAT,  $k$ -NAE-SAT, and  $k$ -XOR-SAT ( $k$  even), the normalized logarithm of the number of solutions concentrates in probability.*

## 4.2 Stochastic block model

The problem of community clustering is to divide a set of vertices in a network (graph) into groups having a higher connectivity within the groups and lower connectivity across the groups (assortative case), or the other way around (disassortative case). This is a fundamental problem in many modern statistics, machine learning, and data mining problems with a broad range of applications in population genetics, image processing, biology and social science. A large variety of models have been proposed for community detection problems, we refer to [New11, For10, GZFA10] for a survey on the subject.

At an algorithmic level, the problem of finding the smallest cut in a graph with two equally sized groups, i.e., the min-bisection problem, is well-known to be NP-hard [DF89]. Concerning average-case complexity, various random graphs models have been proposed for community clustering. The

Erdős-Rényi random graph is typically a very bad model for community structures, since each node is equally connected to any other nodes and no communities are typically formed. The stochastic block model is a natural extension of an Erdős-Rényi model with a community structure. Although the model is fairly simple (communities emerge but the average degree is still constant<sup>3</sup>), it is a fascinating model with several fundamental questions open.

We now describe the stochastic block model (SBM), also called planted bisection model, with two groups and symmetric parameters. Let  $V = [n]$  be the vertex set and  $a, b$  be two positive real numbers. For a uniformly drawn assignment  $X \in \{0, 1\}^V$  on the vertices, an edge is drawn between vertex  $i$  and  $j$  with probability  $a/n$  if  $X_i = X_j$  and with probability  $b/n$  if  $X_i \neq X_j$ , and each edge is drawn independently. We denote this model by  $\mathcal{G}(n, a, b)$ . Note that the average degree of an edge is  $(a + b)/2$ , however, a 0-labelled node is connected in expectation with  $a/2$  0-labeled nodes and with  $b/2$  1-labeled nodes.

This type of model was introduced in [DF89], in the dense regime. The attention to the sparse regime described above is more recent, with [Co10] and [KN11, DKMZ11, MNS12]. In particular, [DKMZ11] conjectured a phase transition phenomenon, with the detection of clusters<sup>4</sup> being possible if  $(a - b)^2 > 2(a + b)$  and impossible otherwise. In [MNS12], a remarkable proof of the impossibility part is obtained, leaving the achievability part open.

We next define a parametrized kernel which will allow us to approximate the above SBM model with a graphical channel.

**Definition 4.8.** *An SBM kernel is given by*

$$Q(z|u_1, u_2) = \begin{cases} a/\gamma & \text{if } u_1 = u_2, \\ b/\gamma & \text{if } u_1 \neq u_2, \end{cases} \quad (15)$$

where  $u_1, u_2, z \in \{0, 1\}$ .

**Lemma 4.9.** *There exists  $n_0 = n_0(\gamma, a, b)$  and  $C = C(a, b)$  such that the following holds true. Let  $X$  be uniformly drawn on  $\{0, 1\}^V$ ,  $Y$  be the output (the graph) of a sparse stochastic block model of parameters  $a, b$ , and  $Y_\gamma$  be the output of a graphical channel with graph ensemble  $\mathcal{P}(\gamma, n)$  and kernel (15), then, for all  $n \geq n_0$*

$$|H^{(n)}(X|Y) - H^{(n)}(X|Y_\gamma)| \leq \frac{Cn}{\gamma}. \quad (16)$$

**Lemma 4.10.** *For the SBM kernel given by (15),  $a \leq b$  (disassortative case) and  $\gamma$  large enough, the operator  $\Gamma_l$  is convex for any  $l \geq 1$ .*

**Corollary 4.11.** *For the disassortative SBM, the limit of  $H(X^{(n)}|Y)/n$  exists and satisfies*

$$\lim_{n \rightarrow \infty} \frac{1}{n} H^{(n)}(X|Y) = \lim_{\gamma \rightarrow \infty} \lim_{n \rightarrow \infty} \frac{1}{n} H^{(n)}(X|Y_\gamma). \quad (17)$$

In a work in progress, the assortative case is investigated with a different proof technique. The computation of the above limit is also expected to reflect a phase transition for the SBM [DKMZ11, MNS12].

---

<sup>3</sup>Models with corrected degrees have been proposed in [KN11]

<sup>4</sup>Obtaining a reconstruction positively correlated with the true assignment



### 4.3 Parity-check encoded channels

The Shannon celebrated coding theorem states that for a discrete memoryless channel  $W$  from  $\mathcal{X}$  to  $\mathcal{Y}$ , the largest rate at which reliable communication can take place is given by the capacity  $C(W) = \max_X I(X; Y)$ , where  $I(X; Y)$  is the mutual information of the channel  $W$  with a random input  $X$ . To show that rates up to capacity are achievable, Shannon used random code books, relying on a probabilistic argument. Shortly after, Elias [Eli55] showed that random linear codes allow to achieve capacity, reducing the encoding complexity from exponential to quadratic in the code dimension. However, Berlekamp, McEliece, and Van Tilborg showed in [BMVT78] that the maximum likelihood decoding of unstructured linear codes is NP-complete.

In order to reduce the complexity of the decoder, Gallager proposed the use sparse linear codes [Gal63], giving birth to the LDPC codes, with sparse parity-check matrices, and LDGM codes, with sparse generator matrices. Various types of LDPC/LDGM codes depend on various types of row and column degree distributions. Perhaps one of the most basic class of such codes is the LDGM code with constant right degree, which corresponds to a generator matrix with column having a fixed number  $k$  of one's. This means that each codeword is the XOR of  $k$  uniformly selected information bits. In other words, this is a graph based code drawn from an Erdős-Rényi or Poisson ensemble  $\mathcal{P}_k(\alpha, n)$ . The dimension of the code is  $m = \alpha n$  and the rate is  $r = 1/\alpha$ . The code can also be seen as a planted  $k$ -XOR-SAT formula.

Despite the long history of research on the LDPC and LDGM codes, and their success in practical applications of communications, there are still many open questions concerning the behaviour of these codes. In particular, even for the simple code described above, it is still open to show that the mutual information  $\frac{1}{n}I(X^n; Y^m)$  concentrates, with the exception of the binary erasure channel for which much more is known [LMSS01, LMS<sup>+</sup>97]. In the case of dense random codes, standard probability arguments show that concentration occurs with a transition at capacity for any discrete memoryless channels. But for sparse codes, the traditional arguments fail. Recently, the following was conjectured in [RKPSS10] for constant right degree LDGM codes and binary input symmetric output channels <sup>5</sup>,

$$\mathbb{P}\left\{\frac{1}{m}I(X; Y) < C(W)\right\} \rightarrow \begin{cases} 0 & \text{if } \alpha < C_k(W) \\ 1 & \text{if } \alpha > C_k(W) \end{cases} \quad (18)$$

where  $C_k(W)$  is a constant depending on  $k$  and  $W$ .

We provide next a concentration result for this model, which implies the above conjecture for even degrees.

**Definition 4.12.** *An encoded symmetric kernel is given by*

$$Q(z|u) = W(z|\oplus_{i=1}^k u_i), \quad (19)$$

where  $W$  is a binary input symmetric output (BISO) channel from  $\mathcal{X}$  to  $\mathcal{Y}$ .

Note that this corresponds to the output of a BISO  $W$  when the input to the channel is the XOR of  $k$  information bits. This corresponds also to the constant right-degree LDGM codes considered in the conjecture of [RKPSS10].

---

<sup>5</sup>This means that the channel is a weighted sum of binary symmetric channels

**Lemma 4.13.** *For an encoded symmetric kernel with  $k$  even, the operator  $\Gamma_l$  is convex for any  $l \geq 1$ .*

**Corollary 4.14.** *Let  $X$  be uniformly drawn in  $GF(2)^n$ ,  $U = XG$  be the output of a  $k$ -degree LDGM code of dimension  $\alpha n$ , and  $Y$  be the output of  $U$  on a BISO channel  $W$ . Then  $\frac{1}{n}I(X; Y)$  converges in probability to a constant  $C_k(\alpha, W)$ .*

Note that  $\frac{1}{m}I(X; Y) = \frac{1}{m}H(Y) - H(W)$ , where  $H(W)$  denotes the conditional entropy of the channel  $W$ . Hence  $\frac{1}{m}I(X; Y) < 1 - H(W) \equiv \frac{1}{m}H(Y) < 1$ . Since  $\frac{1}{m}H(Y)$  converges from previous corollary, and since the limit must be decreasing in  $\alpha$  (increasing in  $r$ ), the conjecture (18) follows.

## 5 Proof outline for Theorem 3.3: Interpolation method for graphical channels

We now show the sub-additivity of  $H^{(n)}(X|Y)$ ,

$$H^{(n)}(X|Y) \leq H^{(n_1)}(X|Y) + H^{(n_2)}(X|Y). \quad (20)$$

Note that if we partition the set of vertices  $[n]$  into two disjoint sets of size  $n_1$  and  $n_2$  with  $n_1 + n_2 = n$ , and denote by  $g_1$  and  $g_2$  the restriction of  $g$  onto these subsets obtained by **removing** all the crossing hyperedges, then the following is obtained by basic properties of the entropy

$$H_g^{(n)}(X|Y) \leq H_{g_1}^{(n)}(X|Y) + H_{g_2}^{(n)}(X|Y). \quad (21)$$

Hence the above is true for a random graph  $G$  drawn from the ensemble  $\mathcal{P}_k(\alpha, n)$ . However, the terms  $H_{G_i}^{(n)}(X|Y)$ ,  $i = 1, 2$ , do not correspond to  $H_{G_i}^{(n_i)}(X|Y)$ , since the edge probability is  $\frac{\alpha n}{\binom{n}{k}}$  and not  $\frac{\alpha n_i}{\binom{n_i}{k}}$ . Consequently, the above does not imply  $H^{(n)}(X|Y) \leq H^{(n_1)}(X|Y) + H^{(n_2)}(X|Y)$ . To obtain the proper term on the right hand side, one should add the edges lost in the splitting of the vertices (e.g., via a coupling argument), but this gives a lower bound on the right hand side of (21), conflicting with the upper bound. The interpolation method provides a way to compare the right quantities.

The interpolation method was first introduced in [GT02] for the Sherrington-Kirkpatrick model. This is a model for a spin-glass (i.e. a spin model with random couplings) on a complete graph. It was subsequently shown in [FL03, FLT03, PT04] that the same ideas can be generalized to models on random sparse graphs, and applications in coding theory and random combinatorial optimization were proposed in [Mon05, KM09] and [BGT10, AM]. We next develop an interpolation method to estimate the conditional entropy of general graphical channels for different values of  $n$ . Interestingly, the planting flips the behaviour of the entropy from super to sub-additive.

**Definition 5.1.** *We define a more general Poisson model for the random graph, where a parameter  $\varepsilon_I \geq 0$  is attached to each  $I \in E_k(V)$ , and the number of edges  $m_I(\varepsilon_I)$  is drawn from a Poisson distribution of parameter  $\varepsilon_I$ . This defines a random hypergraph whose edge probability is not homogenous but depends on the parameters  $\varepsilon_I$ . Denoting by  $\underline{\varepsilon}$  the collection of all  $\binom{n}{k}$  parameters  $\varepsilon_I$ , we denote this ensemble as  $\mathcal{P}_k(\underline{\varepsilon}, n)$ . If for any  $I$ ,  $\varepsilon_I = \frac{\alpha n}{\binom{n}{k}}$ ,  $\mathcal{P}_k(\underline{\varepsilon}, n)$  reduces to  $\mathcal{P}_k(\alpha, n)$  as previously defined.*

**Lemma 5.2.** *Let  $X$  be uniformly drawn over  $\mathcal{X}^n$ ,  $G$  be a random hypergraph drawn from the ensemble  $\mathcal{P}_k(\underline{\varepsilon}, n)$  independently of  $X$ , and  $Y(\underline{\varepsilon})$  be the output of  $X$  through  $P_G$  defined in (1) for a kernel  $Q$ . Then*

$$\frac{\partial}{\partial \varepsilon_I} H^{(n)}(X|Y(\underline{\varepsilon})) = -I(Y_I; X_I|Y(\underline{\varepsilon})), \quad (22)$$

where  $Y_I$  and  $Y(\underline{\varepsilon})$  are independent conditionally on  $X$  (i.e.,  $Y_I$  is drawn under  $Q(\cdot|X[I])$  and  $Y(\underline{\varepsilon})$  is drawn independently under  $R_G(\cdot|X)$ ).

We define a *path* as a differentiable map  $t \mapsto \underline{\varepsilon}(t)$ , with  $t \in [0, T]$  for some  $T \geq 0$ . We say that a path is balanced if

$$\sum_{I \in E_k(V)} \frac{d\varepsilon_I}{dt}(t) = 0. \quad (23)$$

We will write  $\dot{\varepsilon}_I(t)$  for the derivative of  $\varepsilon_I(t)$  along the path and  $Y(t)$  for  $Y(\underline{\varepsilon}(t))$ .

**Corollary 5.3.** *For a balanced path*

$$\frac{d}{dt} H(X|Y(t)) = - \sum_{I \in E_k(V)} H(Y_I|Y(t)) \dot{\varepsilon}_I(t). \quad (24)$$

Given a partition  $V = V_1 \sqcup V_2$ , we define the associated *canonical path*  $\underline{\varepsilon} : t \in [0, 1] \rightarrow \underline{\varepsilon}(t) \in [0, 1]^{E_k(V)}$  as follows. Let  $n_i = |V_i|$ ,  $m_i = |E_k(V_i)|$ ,  $i \in \{1, 2\}$ , and  $m = |E_k(V)|$ . We define

$$\varepsilon_I(0) \equiv \frac{\alpha n}{m}, \quad \forall I \in E_k(V), \quad (25)$$

$$\varepsilon_I(1) \equiv \begin{cases} \frac{\alpha n_1}{m_1} & \text{if } I \in E_k(V_1) \\ \frac{\alpha n_2}{m_2} & \text{if } I \in E_k(V_2) \\ 0 & \text{otherwise.} \end{cases} \quad (26)$$

and

$$\underline{\varepsilon}(t) = (1-t)\underline{\varepsilon}(0) + t\underline{\varepsilon}(1). \quad (27)$$

Note that the canonical path is balanced. Moreover, at time  $t = 0$ ,  $\mathcal{P}_k(\underline{\varepsilon}(0), n)$  reduces to the original ensemble  $\mathcal{P}_k(\alpha, n)$ , and at time  $t = 1$ ,  $\mathcal{P}_k(\underline{\varepsilon}(1), n)$  reduces to two independent copies of the original ensemble on the subset of  $n_1$  and  $n_2$  variables:  $\mathcal{P}_k(\alpha, n_1) \times \mathcal{P}_k(\alpha, n_2)$ .

Applying Lemma 5.3, we obtain the following.

**Corollary 5.4.** *For the canonical path*

$$\frac{d}{dt} H(X|Y(t)) = \alpha n \mathbb{E}_I H(Y_I|Y(t)) - \alpha n_1 \mathbb{E}_{I_1} H(Y_{I_1}|Y(t)) - \alpha n_2 \mathbb{E}_{I_2} H(Y_{I_2}|Y(t)), \quad (28)$$

where  $I$  is drawn uniformly in  $E_k(V)$ , and  $I_i$ ,  $i \in \{1, 2\}$ , are drawn uniformly in  $E_k(V_i)$ .

We recall that

$$H(Y_I|Y(t)) = -\mathbb{E}_{Y, Y_I} \log \sum_x Q(Y_I|x[I])R_{G(t)}(x|Y) \quad (29)$$

$$= -\mathbb{E}_{Y(t), Y_I} \log \mathbb{E}_{X|Y(t)} Q(Y_I|X[I]), \quad (30)$$

where  $Y(t)$  is the output of  $P_{G(t)}$  and  $\mathbb{E}_{X|Y(t)}$  is the conditional expectation over  $R_{G(t)}$ .

**Lemma 5.5.**

$$\frac{1}{\alpha|\mathcal{Y}|} \frac{d}{dt} H(X|Y(t)) = - \sum_{l=2}^{\infty} \frac{1}{l(l-1)} \mathbb{E}_{X^{(1)}, \dots, X^{(l)}} [n\Gamma_l(V) - n_1\Gamma_l(V_1) - n_2\Gamma_l(V_2)] \quad (31)$$

where

$$\Gamma_l(V) \equiv \mathbb{E}_{I, W_I} \prod_{r=1}^l \left(1 - P(W_I|X^{(r)}[I])\right), \quad (32)$$

$I$  is uniformly drawn in  $E_k(V)$ ,  $W_I$  is uniformly drawn in  $\mathcal{Y}$ , and  $X^{(1)}, \dots, X^{(l)}$  are drawn under the probability distribution  $\sum_y \prod_{i=1}^l R_{G(t)}(x^{(i)}|y) \sum_u P_{G(t)}(y|u)2^{-n}$ .

This means that  $X^{(1)}, \dots, X^{(l)}$  are drawn i.i.d. from the channel  $R_{G(t)}$  given a hidden output  $Y$ , these are the ‘replica’ variables, which are exchangeable but not i.i.d.. Note that denoting by  $\nu$  the empirical distribution of  $X^{(1)}, \dots, X^{(l)}$ , the above definition of  $\Gamma_l(V)$  coincides with that of  $\Gamma_l(\nu)$ , hence the abuse of notation with definition (8). Hypothesis H ensures that  $\Gamma_l$  is convex for any distribution on  $\mathcal{X}^l$ , hence in particular for the empirical distribution of the replicas. Therefore, previous lemma implies Lemma 3.3 and Theorem 3.4 follows by the sub-additivity property.

## References

- [ACO08] D. Achlioptas and A. Coja-Oghlan, *Algorithmic barriers from phase transitions*, Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science (Washington, DC, USA), FOCS ’08, IEEE Computer Society, 2008, pp. 793–802.
- [ACOV07] M. Krivelevich A. Coja-Oghlan and D. Vilenchik, *Why almost all satisfiable k-cnf formulas are easy*, Proceedings of the 13th International Conference on Analysis of Algorithms, 2007, pp. 89–102.
- [AJM04] D. Achlioptas, H. Jia, and C. Moore, *Hiding satisfying assignments: two are better than one*, In Proceedings of AAAI04, 2004, pp. 131–136.
- [AKG] D. Achlioptas, H. Kautz, and C. Gomes, *Generating satisfiable problem instances*.
- [AKKT02] D. Achlioptas, J. Han Kim, M. Krivelevich, and P. Tetali, *Two-coloring random hypergraphs*, Random Structures and Algorithms **20** (2002), no. 2, 249–259.
- [AM] E. Abbe and A. Montanari, *On the concentration of the number of solutions of random satisfiability formulas*, Random Structures and Algorithm DOI 10.1002/rsa.20501, to appear., arXiv:1006.3786v1 [cs.DM], 2010.

- [AMZ06] F. Altarelli, R. Monasson, and F. Zamponi, *Can rare SAT formulas be easily recognized? On the efficiency of message passing algorithms for K-SAT at large clause-to-variable ratios*, Computing Research Repository **abs/cs/060** (2006).
- [ANP05] D. Achlioptas, A. Naor, and Y. Peres, *Rigorous Location of Phase Transitions in Hard Optimization Problems*, Nature **435** (2005), 759–764.
- [BGT10] M. Bayati, D. Gamarnik, and P. Tetali, *Combinatorial approach to the interpolation method and scaling limits in sparse random graphs*, 42nd Annual ACM Symposium on Theory of Computing (Cambridge, MA), June 2010, pp. 105–114.
- [BHL<sup>+</sup>02] W. Barthel, A. K. Hartmann, M. Leone, F. Ricci-Tersenghi, M. Weigt, and R. Zecchina, *Hiding solutions in random satisfiability problems: A statistical mechanics approach*, Phys. Rev. Lett. **88** (2002), 188701.
- [BMVT78] E. Berlekamp, R.J. McEliece, and H. C A Van Tilborg, *On the inherent intractability of certain coding problems (corresp.)*, Information Theory, IEEE Transactions on **24** (1978), no. 3, 384–386.
- [Co10] A. Coja-oghlan, *Graph partitioning via adaptive spectral techniques*, Comb. Probab. Comput. **19** (2010), no. 2, 227–284.
- [DF89] M.E Dyer and A.M Frieze, *The solution of some random np-hard problems in polynomial expected time*, Journal of Algorithms **10** (1989), no. 4, 451 – 489.
- [DGM<sup>+</sup>10] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, and M. Rink, *Tight thresholds for cuckoo hashing via xorsat*, Proceedings of the 37th international colloquium conference on Automata, languages and programming (Berlin, Heidelberg), ICALP’10, Springer-Verlag, 2010, pp. 213–225.
- [DKMZ11] A. Decelle, F. Krzakala, C. Moore, and L. Zdeborová, *Asymptotic analysis of the stochastic block model for modular networks and its algorithmic applications*, Phys. Rev. E **84**, 066106 (2011).
- [DM02] O. Dubois and J. Mandler, *The 3-xorsat threshold*, Proceedings of the 43rd Symposium on Foundations of Computer Science (Washington, DC, USA), FOCS ’02, IEEE Computer Society, 2002, pp. 769–778.
- [DR08] H. Daudé and V. Ravelomanana, *Random 2-xorsat at the satisfiability threshold*, Proceedings of the 8th Latin American conference on Theoretical informatics (Berlin, Heidelberg), LATIN’08, Springer-Verlag, 2008, pp. 12–23.
- [Eli55] P. Elias, *Coding for noisy channels*, IRE Convention Record **4** (1955), 37–46.
- [FL03] S. Franz and M. Leone, *Replica bounds for optimization problems and diluted spin systems*, J. Stat. Phys. **111** (2003), 535.
- [FLT03] S. Franz, M. Leone, and F.L. Toninelli, *Replica bounds for diluted non-Poissonian spin systems*, J. Phys. A **36** (2003), 10967.

- [FMV06] U. Feige, E. Mossel, and D. Vilenchik, *Complete convergence of message passing algorithms for some satisfiability problems*, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, Springer, 2006, pp. 339–350.
- [For10] S. Fortunato, *Community detection in graphs*, Physics Reports **486 (3-5)** (2010), 75–174.
- [Fri99] E. Friedgut, *Sharp thresholds of graph properties, and the  $k$ -sat problem*, J. Amer. Math. Soc. **12** (1999), 1017–1054, appendix by J. Bourgain.
- [Gal63] R. G. Gallager, *Low-density parity-check codes*, MIT Press, Cambridge, Massachusetts, 1963.
- [GT02] F. Guerra and F. L. Toninelli, *The thermodynamic limit in mean field spin glasses*, Commun. Math. Phys. **230** (2002), 71–79.
- [GZFA10] A. Goldenberg, A. X. Zheng, S. E. Fienberg, and E. M. Airoidi, *A survey of statistical network models*, Foundations and Trends® in Machine Learning **2** (2010), no. 2, 129–233.
- [HJKN05] H. Haanpää, M. Järvisalo, P. Kaski, and I. Niemelä, *Hard satisfiable clause sets for benchmarking equivalence reasoning techniques*, 2005.
- [JMS05] H. Jia, C. Moore, and D. Strain, *Generating hard satisfiable formulas by hiding solutions deceptively*, In AAAI, AAAI Press, 2005, pp. 384–389.
- [KM09] S. Kudekar and N. Macris, *Sharp bounds for optimal decoding of Low-Density Parity-Check codes*, IEEE Trans. on Inform. Theory **55** (2009), 4635–4650.
- [KN11] B. Karrer and M. E. J. Newman, *Stochastic blockmodels and community structure in networks*, Phys. Rev. E **83** (2011), 016107.
- [KZ09] F. Krzakala and L. Zdeborová, *Hiding quiet solutions in random constraint satisfaction problems*, Phys. Rev. Lett. **102** (2009), 238701.
- [Laf01] J. Lafferty, *Conditional random fields: Probabilistic models for segmenting and labeling sequence data*, Morgan Kaufmann, 2001, pp. 282–289.
- [LMS<sup>+</sup>97] M. Luby, Michael Mitzenmacher, A. Shokrollahi, D. A. Spielman, and V. Stemann, *Practical loss-resilient codes*, 29th annual ACM Symposium on Theory of Computing, 1997, pp. 150–159.
- [LMSS01] M. Luby, M. Mitzenmacher, A. Shokrollahi, and D. A. Spielman, *Efficient erasure correcting codes*, IEEE Trans. on Inform. Theory **47** (2001), no. 2, 569–584.
- [MNS12] E. Mossel, J. Neeman, and A. Sly, *Stochastic Block Models and Reconstruction*, arXiv:1202.1499 [math.PR].
- [Mon05] A. Montanari, *Tight bounds for LDPC and LDGM codes under MAP decoding*, IEEE Trans. on Inform. Theory **51** (2005), 3221–3246.

- [Mon08] A. Montanari, *Estimating random variables from random sparse observations*, European Transactions on Telecommunications **19** (2008), no. 4, 385–403.
- [MRT09] A. Montanari, R. Restrepo, and P. Tetali, *Reconstruction and Clustering in Random Constraint Satisfaction Problems*, CoRR abs/0904.2751, 2009.
- [New11] M. E. J. Newman, *Communities, modules and large-scale structure in networks*, Nature Physics **8** (2011), no. 1, 25–31.
- [PS12] B. Pittel and G. B. Sorkin, *The Satisfiability Threshold for  $k$ -XORSAT*, arXiv:1212.1905 (2012).
- [PT04] D. Panchenko and M. Talagrand, *Bounds for diluted mean-field spin glass models*, Prob. Theor. Rel. Fields **130** (2004), 319–336.
- [RK PSS10] K. Raj Kumar, P. Pakzad, A.H. Salavati, and A. Shokrollahi, *Phase transitions for mutual information*, Turbo Codes and Iterative Information Processing (ISTC), 2010 6th International Symposium on, 2010, pp. 137–141.
- [RU08] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, Cambridge, 2008.
- [ZK11] L. Zdeborová and F. Krzakala, *Quiet planting in the locked constraint satisfaction problems*, SIAM Journal on Discrete Mathematics **25** (2011), no. 2, 750–770.

## A Proofs of Theorems 3.4 and 3.5

We now prove the lemmas used in Section 5 to prove Theorem 3.4. We then prove Theorem 3.5. In the proofs, we may drop the upper-script  $n$  for the entropy.

*Proof of Lemma 5.2.* Note that for a random variable  $Z_\varepsilon$  which is Poisson distributed of parameter  $\varepsilon$ , and a function  $f$ ,

$$\frac{\partial}{\partial \varepsilon} \mathbb{E}f(Z_\varepsilon) = \mathbb{E}f(Z_\varepsilon + 1) - \mathbb{E}f(Z_\varepsilon). \quad (33)$$

Therefore,

$$\frac{\partial}{\partial \varepsilon_I} H^{(n)}(X|Y(\underline{\varepsilon})) = H^{(n)}(X|Y(\underline{\varepsilon}), Y_I) - H^{(n)}(X|Y(\underline{\varepsilon})), \quad (34)$$

where  $Y_I$  is an extra output drawn independently from  $Y(\underline{\varepsilon})$  but conditionally on the same  $X$ . We also recall the definition of the mutual information,  $I(A; B) = H(A) - H(A|B) = H(B) - H(B|A)$ . We have

$$\frac{\partial}{\partial \varepsilon_I} H(X|Y(\underline{\varepsilon})) = -I(Y_I; X|Y(\underline{\varepsilon})) \quad (35)$$

$$= -H(Y_I|Y(\underline{\varepsilon})) + H(Y_I|X, Y(\underline{\varepsilon})) \quad (36)$$

$$= -H(Y_I|Y(\underline{\varepsilon})) + H(Y_I|X_I, Y(\underline{\varepsilon})) \quad (37)$$

$$= -I(Y_I; X_I|Y(\underline{\varepsilon})), \quad (38)$$

where we used the fact that  $Y_I$  depends only on the components of  $X$  indexed by  $I$ .  $\square$

*Proof of Corollary 5.3.* Note that from previous proof, and using the fact that  $Y_I - X - Y(\underline{\varepsilon})$  form a Markov chain,

$$\frac{\partial}{\partial \varepsilon_I} H(X|Y(\underline{\varepsilon})) = -I(Y_I; X_I|Y(\underline{\varepsilon})) \quad (39)$$

$$= -H(Y_I|Y(\underline{\varepsilon})) + H(Y_I|X_I) \quad (40)$$

$$= -H(Y_I|Y(\underline{\varepsilon})) + H(Q) \quad (41)$$

where

$$H(Q) \equiv -2^{-k} \sum_{u \in \mathcal{X}^k, z \in \mathcal{Y}} Q(z|u) \log Q(z|u)$$

is a constant depending on  $Q$  only. Therefore, if the path is balanced, the chain rule yields the result.  $\square$

*Proof of Lemma 5.5.* By definition

$$H(Y_I|Y(t)) = -\mathbb{E}_{Y(t), Y_I} \log \mathbb{E}_{X|Y(t)} Q(Y_I|X[I]), \quad (42)$$

and expanding the logarithm in its power series,

$$\log \mathbb{E}_{X|Y(t)} Q(Y_I|X[I]) = - \sum_{l=1}^{\infty} \frac{1}{l} (\mathbb{E}_{X|Y(t)} (1 - Q(Y_I|X[I])))^l. \quad (43)$$



We now introduce the ‘replicas’  $X^{(1)}, \dots, X^{(l)}$ , which are i.i.d. under  $Q_{X|Y(t)}$ , i.e., we have the Markov relation  $X - Y(t) - (X^{(1)}, \dots, X^{(l)})$ . Denoting by  $\tilde{Q} = 1 - Q$ , we obtain

$$\log \mathbb{E}_{X|Y(t)} Q(Y_I|X[I]) = - \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}_{X^{(1)}, \dots, X^{(l)}|Y(t)} \prod_{r=1}^l \tilde{Q}(Y_I|X^{(r)}[I]). \quad (44)$$

As opposed to the non-planted case, where super-additivity is achieved by showing that terms weighted by  $1/l$  are convex in the empirical distribution of the replicas, convexity does not hold with the above expression and the following is needed. Collecting terms we have

$$H(Y_I|Y(t)) = \mathbb{E}_X \mathbb{E}_{Y(t)|X} \mathbb{E}_{Y_I|X} \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}_{X^{(1)}, \dots, X^{(l)}|Y(t)} \prod_{r=1}^l \tilde{Q}(Y_I|X^{(r)}[I]) \quad (45)$$

$$= \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}_{X, X^{(1)}, \dots, X^{(l)}} \mathbb{E}_{Y_I|X} \prod_{r=1}^l \tilde{Q}(Y_I|X^{(r)}[I]). \quad (46)$$

We next write switch measure in the expectation  $\mathbb{E}_{Y_I|X}$ , defining  $W_I$  to be uniformly distributed over  $\mathcal{Y}$ , and writing

$$H(Y_I|Y(t)) = |\mathcal{Y}| \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}_{X, X^{(1)}, \dots, X^{(l)}} \mathbb{E}_{W_I} \prod_{r=1}^l \tilde{Q}(W_I|X^{(r)}[I]) Q(W_I|X[I]). \quad (47)$$

Renaming  $X$  by  $X^{(0)}$ , and using the fact that  $X^{(0)}, X^{(1)}, \dots, X^{(l)}$  are exchangeable, we can write

$$H(Y_I|Y(t)) = |\mathcal{Y}| \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}_{X^{(0)}, X^{(1)}, \dots, X^{(l)}} \left( \mathbb{E}_{W_I} \prod_{r=1}^l \tilde{Q}(W_I|X^{(r)}[I]) - \mathbb{E}_{W_I} \prod_{r=0}^l \tilde{Q}(W_I|X^{(r)}[I]) \right) \quad (48)$$

$$= |\mathcal{Y}| \mathbb{E}_{X^{(1)}} \mathbb{E}_{W_I} \tilde{Q}(W_I|X^{(1)}[I]) - |\mathcal{Y}| \sum_{l=2}^{\infty} \frac{1}{l(l-1)} \mathbb{E}_{X^{(1)}, \dots, X^{(l)}} \mathbb{E}_{W_I} \prod_{r=1}^l \tilde{Q}(W_I|X^{(r)}[I]). \quad (49)$$

Recall that from Corollary 5.4,

$$\frac{d}{dt} H(X|Y(t)) = \alpha n \mathbb{E}_I H(Y_I|Y(t)) - \alpha n_1 \mathbb{E}_{I_1} H(Y_{I_1}|Y(t)) - \alpha n_2 \mathbb{E}_{I_2} H(Y_{I_2}|Y(t)).$$

Hence, carrying out the above expansions for each term, and since the term  $\mathbb{E}_{X^{(1)}} \mathbb{E}_{W_I} \tilde{Q}(W_I|X^{(1)}[I])$  cancels out, the lemma follows.  $\square$

*Proof of Theorem 3.5.* Since we now that  $H_G^{(n)}(X|Y)/n$  converges in expectation, it is sufficient to show that it concentrates around its expectation. Indeed we claim that there exists  $B > 0$  such that

$$\mathbb{P}\{|H_G^{(n)}(X|Y) - H^{(n)}(X|Y)| \geq n\Delta\} \leq 2e^{-nB\Delta^2}, \quad (50)$$

whence our thesis follows from Borel-Cantelli.

The proof of (50) is a direct application of Azuma-Hoeffding inequality, and we limit ourselves to sketching its main steps. We condition on the number  $m = O(n)$  of hyperedges in  $G$  and regard  $H_G^{(n)}(X|Y)$  as a function of the choice of the  $m$  hyperedges. We claim that  $|H_G^{(n)}(X|Y) - H_{G'}^{(n)}(X|Y)| \leq 2C$ , for some constant  $C$ , if  $G$  and  $G'$  differ only in one of their hyperedges, whence Eq. (50) follows by Azuma-Hoeffding.

In order to prove the last claim, let  $G' = G + a$  denote the graph  $G$  to which hyperedge  $a = (i_1, \dots, i_k)$  has been added. Then, writing explicitly the component of  $Y$  corresponding to hyperedge  $a$ , we need to prove that  $|H_{G+a}^{(n)}(X|Y, Y_a) - H_G^{(n)}(X|Y)| \leq C$ . We have, dropping the subscripts and superscript for the sake of simplicity,

$$0 \leq H(X|Y) - H(X|Y, Y_a) = H(X|Y) - H(X, Y_a|Y) + H(Y_a|Y) \quad (51)$$

$$= H(Y_a|Y) - H(Y_a|X, Y) \quad (52)$$

$$\leq \log_2 |\mathcal{Y}|, \quad (53)$$

where the last inequality follows from the fact that  $Y_a$  takes value in the finite set  $\mathcal{Y}$ .  $\square$

## B Proofs of Lemmas 4.2, 4.4, 4.5 and 4.6

*Proof of Lemma 4.2.* We have

$$P_g(y|x) = \prod_{I \in E(g)} Q(y_I|x[I]) \quad (54)$$

$$= \prod_{I \in E(g)} \frac{1}{|A|} \mathbb{1}(y_I \in A(x[I])) \quad (55)$$

$$= \begin{cases} \frac{1}{|A|^{|E(g)|}} & \text{if } x \sim y, \\ 0 & \text{otherwise,} \end{cases} \quad (56)$$

where  $x \sim y$  means that  $x$  is a satisfying assignment for  $y$ . Hence for a given  $x$ ,  $P_g(\cdot|x)$  is uniform on the set of all  $y$ 's verifying  $x$ , which has cardinality  $|A|^{|E(g)|}$ . Since  $X$  is uniform, for a given  $y$ ,  $R_g(\cdot|y)$  is a uniform measure on a set of cardinality

$$\sum_{x \in \mathcal{X}^n} \prod_{I \in E(g)} \mathbb{1}(y_I \in A(x[I])) = |\{x \in \mathcal{X}^n : y_I \in A(x[I]), \forall I \in E(g)\}| = Z_g(y) \quad (57)$$

Therefore  $H_g(X|Y = y) = \log Z_g(y)$ .  $\square$

*Proof of Lemma 4.4.* For planted  $k$ -SAT,  $\mathcal{Y} = \mathcal{X}^k = \{0, 1\}^k$ ,

$$Q(z|u) = \frac{1}{2^k - 1} \mathbb{1}(z \neq \bar{u}) \quad (58)$$

and

$$\Gamma_l(\nu) = \frac{1}{2^k} \left( \frac{1}{2^k - 1} \right)^l \sum_{u^{(1)}, \dots, u^{(l)} \in \mathcal{X}^k} \left[ \sum_{z \in \mathcal{Y}} \prod_{r=1}^l \mathbb{1}(\bar{z} = u^{(r)}) \right] \prod_{i=1}^k \nu(u_i^{(1)}, \dots, u_i^{(l)}) \quad (59)$$

$$= \frac{1}{2^k} \left( \frac{1}{2^k - 1} \right)^l \sum_{u \in \mathcal{X}^k} \prod_{i=1}^k \nu(u_i, \dots, u_i) \quad (60)$$

$$= \frac{1}{2^k} \left( \frac{1}{2^k - 1} \right)^l \sum_{u_1, \dots, u_k \in \mathcal{X}} \prod_{i=1}^k \nu(u_i, \dots, u_i) \quad (61)$$

$$= \frac{1}{2^k} \left( \frac{1}{2^k - 1} \right)^l \left( \sum_{u_1 \in \mathcal{X}} \nu(u_1, \dots, u_1) \right)^k, \quad (62)$$

which is convex in  $\nu$  for any  $k, l \geq 1$ . □

*Proof of Lemma 4.5.* For planted  $k$ -NAE-SAT,  $\mathcal{Y} = \mathcal{X}^k = \{0, 1\}^k$ ,

$$Q(z|u) = \frac{1}{2^k - 2} \mathbb{1}(z \notin (u, \bar{u})) \quad (63)$$

and

$$\Gamma_l(\nu) = \frac{1}{2^k} \left( \frac{1}{2^k - 2} \right)^l \sum_{u^{(1)}, \dots, u^{(l)} \in \mathcal{X}^k} \left[ \sum_{z \in \mathcal{Y}} \prod_{r=1}^l \mathbb{1}(u^{(r)} \in (z, \bar{z})) \right] \prod_{i=1}^k \nu(u_i^{(1)}, \dots, u_i^{(l)}) \quad (64)$$

$$= \frac{1}{2^k} \left( \frac{1}{2^k - 2} \right)^l \sum_{b_1, \dots, b_l \in \mathcal{X}} \sum_{u \in \mathcal{X}^k} \prod_{i=1}^k \nu(u_i \oplus b_1, \dots, u_i \oplus b_l) \quad (65)$$

$$= \frac{1}{2^k} \left( \frac{1}{2^k - 2} \right)^l \sum_{b_1, \dots, b_l \in \mathcal{X}} \left( \sum_{u_1 \in \mathcal{X}} \nu(u_1 \oplus b_1, \dots, u_1 \oplus b_l) \right)^k, \quad (66)$$

which is convex in  $\nu$  for any  $k, l \geq 1$ . □

*Proof of Lemma 4.6.* This is a special case of Lemma C.2 for  $s = 1, d = -1$ . □

## C Proofs of Lemmas 4.9 and 4.10

*Proof of Lemma 4.9.* We introduce a new collection of random variables  $\{Z_{ij}\}_{(ij) \in E_2(V)}$ , taking values in  $\{0, 1, *\}$ , and indexed by the  $\binom{n}{2}$  edges of the complete graph over vertex set  $V$ . These

are conditionally independent given  $X$  with distribution given as follows:

$$Z_{ij}|_{X_i=X_j} = \begin{cases} 1 & \text{with probability } a/n, \\ 0 & \text{with probability } (2\gamma - a)/n, \\ * & \text{with probability } 1 - 2\gamma/n, \end{cases} \quad (67)$$

$$Z_{ij}|_{X_i \neq X_j} = \begin{cases} 1 & \text{with probability } b/n, \\ 0 & \text{with probability } (2\gamma - b)/n, \\ * & \text{with probability } 1 - 2\gamma/n, \end{cases} \quad (68)$$

The following claim is proved below.

**Lemma C.1.** *There exists a constant  $C = C(\gamma) < \infty$  such that, uniformly in  $n$*

$$|H^{(n)}(X|Y_\gamma) - H^{(n)}(X|Z)| \leq C(\gamma). \quad (69)$$

It is therefore sufficient to bound the difference  $|H^{(n)}(X|Y) - H^{(n)}(X|Z)|$ . Notice that the variables  $X, Y, Z$  can be constructed on the same probability space in such a way that  $X - Z - Y$  form a Markov chain. Namely, it is sufficient to let the  $Y_{ij}$  be conditionally independent, and independent from  $X$  given  $Z$ , with

$$Y_{ij} = \begin{cases} 1 & \text{if } Z_{ij} = 1, \\ 0 & \text{if } Z_{ij} \in \{0, *\}. \end{cases} \quad (70)$$

We therefore have that  $H^{(n)}(X|Z) \leq H^{(n)}(X|Y)$  and we are therefore left with the task of upper bounding  $H^{(n)}(X|Y) - H^{(n)}(X|Z)$ . In the rest of this proof we will omit the superscript  $(n)$  as it is will be fixed throughout.

We have, by the Markov property and the chain rule of conditional entropy

$$H(X|Z) = H(X|Y, Z) \quad (71)$$

$$= H(X, Z|Y) - H(Z|Y) \quad (72)$$

$$= H(X|Y) + H(Z|X, Y) - H(Z|Y), \quad (73)$$

and therefore

$$H(X|Y) - H(X|Z) = H(Z|Y) - H(Z|X, Y). \quad (74)$$

Note that, by subadditivity of the entropy, and since conditioning reduces entropy, we have

$$H(Z|Y) \leq \sum_{(i,j) \in E_2(V)} H(Z_{ij}|Y) \leq \sum_{(i,j) \in E_2(V)} H(Z_{ij}|Y_{ij}). \quad (75)$$

Further, by conditional independence of the  $\{Z_{ij}\}$  given  $X, Y$ , we have

$$H(Z|X, Y) = \sum_{(i,j) \in E_2(V)} H(Z_{ij}|X, Y) = \sum_{(i,j) \in E_2(V)} H(Z_{ij}|X_i, X_j, Y_{ij}). \quad (76)$$

We therefore conclude that

$$H(X|Y) - H(X|Z) \leq \sum_{(i,j) \in E_2(V)} \{H(Z_{ij}|Y_{ij}) - H(Z_{ij}|X_i, X_j, Y_{ij})\}. \quad (77)$$

A simple calculation yields  $H(Z_{ij}|Y_{ij}) = f_n((a+b)/2)$  and  $H(Z_{ij}|X_i, X_j, Y_{ij}) = f_n(a) + f_n(b)/2$ , where

$$f_n(c) \equiv -\frac{2\gamma - c}{n} \log\left(\frac{2\gamma - c}{n}\right) - \left(1 - \frac{2\gamma}{n}\right) \log\left(1 - \frac{2\gamma}{n}\right) + \left(1 - \frac{c}{n}\right) \log\left(1 - \frac{c}{n}\right), \quad (78)$$

Subtracting an affine term, we can write

$$f_n(c) = f_{n,0} + f_{n,1}c + g_n(c), \quad (79)$$

$$g_n(c) = -\frac{2\gamma}{n} \left[ \left(1 - \frac{c}{2\gamma}\right) \log\left(1 - \frac{c}{2\gamma}\right) + \frac{c}{2\gamma} \right] + \left[ \left(1 - \frac{c}{n}\right) \log\left(1 - \frac{c}{n}\right) + \frac{c}{n} \right]. \quad (80)$$

Note that, for  $x \in [-1/2, 41/2]$ , we have  $0 \leq (1-x) \log(1-x) + x \leq x^2$ . Hence, for  $\gamma \geq c$ ,  $n \geq 2c$ ,

$$0 \geq g_n(c) \geq \frac{c^2}{n} \left[ \frac{1}{n} - \frac{1}{2\gamma} \right] \geq -\frac{c^2}{2n\gamma}, \quad (81)$$

and therefore

$$\begin{aligned} H(X|Y) - H(X|Z) &\leq \binom{n}{2} \left[ f_n\left(\frac{a+b}{2}\right) - \frac{1}{2}f_n(a) - \frac{1}{2}f_n(b) \right] \\ &= \binom{n}{2} \left[ g_n\left(\frac{a+b}{2}\right) - \frac{1}{2}g_n(a) - \frac{1}{2}g_n(b) \right] \\ &\leq \frac{n^2}{2} \frac{1}{2n\gamma} \frac{(a-b)^2}{4} = \frac{n(a-b)^2}{16\gamma}. \end{aligned}$$

This finishes the proof.  $\square$

*Proof of Lemma C.1.* We write  $Y_\gamma = \{Y_{\gamma,ij}\}_{(i,j) \in E_2(V)}$  where, for each  $(i,j) \in E_2(V)$ ,  $Y_{\gamma,ij}$  is a vector containing  $\text{Poisson}(n\gamma/\binom{n}{2})$  entries, each being an independent output of the channel  $Q$  in Eq. (15) on input  $(X_i, X_j)$ . Analogously, we can interpret  $Z_{ij}$  as a vector of length  $\text{Bernoulli}(2\gamma/n)$ , with the length 0 corresponding to the value  $*$ . When the length of the vector is equal to one, its entry is distributed as the output of the same channel  $Q$ .

Let  $\ell(Y_{\gamma,ij})$  and  $\ell(Z_{ij})$  denote the length of vectors  $Y_{\gamma,ij}$  and  $Z_{ij}$ . It follows from standard estimates on Poisson random variables that  $Y$  and  $Z$  can be coupled in such a way that  $\mathbb{E}\{|\ell(Y_{\gamma,ij}) - \ell(Z_{ij})|\} \leq C/n^2$  with  $C = C(\gamma)$  and further, whenever  $\ell(Z_{ij}) = 1$  and  $\ell(Y_{\gamma,ij}) \geq 1$ , the first entry of the vector  $Y_{\gamma,ij}$  is equal to the only entry in  $Z_{ij}$ .

Finally notice that

$$H(X|Y_\gamma, \ell(Y_{\gamma,ij}) = \ell_0 + 1) - H(X|Y_\gamma, \ell(Y_{\gamma,ij}) = \ell_0) \quad (82)$$

$$= H(Y'_{ij}|X, \ell(Y_{\gamma,ij}) = \ell_0) - H(Y'_{ij}|Y_\gamma, \ell(Y_{\gamma,ij}) = \ell_0), \quad (83)$$

with  $Y'_{ij}$  distributed as an independent output of the channel  $Q$  on input  $X_i, X_j$ . It follows that  $|H(X|Y_\gamma, \ell(Y_{\gamma,ij}) = \ell_0 + 1) - H(X|Y_\gamma, \ell(Y_{\gamma,ij}) = \ell_0)| \leq 1$  and therefore

$$|H(X|Y_\gamma) - H(X|Z)| \leq \sum_{(i,j) \in E_2(V)} \mathbb{E}\{|\ell(Y_{\gamma,ij}) - \ell(Z_{ij})|\} \leq n^2 \frac{C}{n^2} \leq C. \quad (84)$$

$\square$

*Proof of Lemma 4.10.* This is a special case of Lemma C.2 below, with  $s = (a + b)/\gamma$  and  $d = (a - b)/\gamma$ . If  $\gamma$  is large enough,  $s \leq 1$  and if  $a \leq b$ ,  $d \geq 0$ , and all the coefficients in (92) are positive.  $\square$

**Lemma C.2.** *If  $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ ,  $Q(y|x_1, \dots, x_k) = W(y | \oplus_{i=1}^k x_i)$  and  $W$  is an arbitrary binary input/output channel, then*

$$\Gamma_l(\nu) = \frac{1}{2} \sum_{w \in \mathbb{F}_2^l} d^{|w|} \left[ s^{l-|w|} + (-1)^{|w|} (2-s)^{l-|w|} \right] \mathcal{F}(\nu)^k(w) \quad (85)$$

where  $s = W(1|0) + W(1|1)$ ,  $d = W(1|0) - W(1|1)$ ,  $|w| = \sum_{i=1}^l w_i$  and  $\mathcal{F}(\nu)(w) = \sum_{x \in \mathbb{F}_2^l} (-1)^{x \cdot w} \nu(x)$  is the Fourier-Walsh transform of  $\nu$  (where  $x \cdot w$  denotes the dot product of  $x$  and  $w$ ).

Note that  $\mathcal{F}(\nu)(w)$  is linear in  $\nu$ , hence

- For  $s = 1$ , i.e., for symmetric channels,

$$\Gamma_l(\nu) = \sum_{w \in \mathbb{F}_2^k: |w| \text{ even}} d^{|w|} \mathcal{F}(\nu)^k(w) \quad (86)$$

and  $\Gamma_l$  is convex when  $k$  is even.

- If  $s \geq 1$ ,  $d \geq 0$  or  $s \leq 1$ ,  $d \leq 0$ , then  $\Gamma_l$  is convex when  $k$  is even.

*Proof of Lemma C.2.* We have

$$\Gamma_l(\nu) = \frac{1}{2} \sum_{u^{(1)}, \dots, u^{(l)} \in \mathbb{F}_2^k} \left[ \sum_{y \in \mathbb{F}_2} \prod_{r=1}^l (1 - P(y|u^{(r)})) \right] \prod_{i=1}^k \nu(u_i^{(1)}, \dots, u_i^{(l)}) \quad (87)$$

and using the fact that  $P(y|u^{(r)}) = W(y | \oplus_{i=1}^k u_i^{(r)})$ ,

$$\Gamma_l(\nu) = \frac{1}{2} \sum_{v^{(1)}, \dots, v^{(l)} \in \mathbb{F}_2} \left[ \sum_{y \in \mathbb{F}_2} \prod_{r=1}^l (1 - W(y|v^{(r)})) \right] \nu^{\star k}(v^{(1)}, \dots, v^{(l)}) \quad (88)$$

$$= \frac{1}{2} \sum_{v \in \mathbb{F}_2^l} \gamma(v) \nu^{\star k}(v) \quad (89)$$

where

$$\gamma(v) \equiv \sum_{y \in \mathbb{F}_2} \prod_{r=1}^l (1 - W(y|v^{(r)})) = (1-a)^{l-|v|} (1-b)^{|v|} + a^{l-|v|} b^{|v|} \quad (90)$$

and  $a = W(1|0)$ ,  $b = W(1|1)$ . Note that

$$a^{l-|v|} b^{|v|} \xleftrightarrow{\mathcal{F}} (a+b)^{l-|w|} (a-b)^{|w|}, \quad (91)$$

hence

$$\mathcal{F}(\gamma)(w) = (2 - (a+b))^{l-|w|} (a-b)^{|w|} (-1)^{|w|} + (a+b)^{l-|w|} (a-b)^{|w|}. \quad (92)$$

$\square$

*Proof of (91).* To show that

$$\mathbb{F}_2^l \ni v \mapsto \rho^{|v|} \xleftrightarrow{\mathcal{F}} \mathbb{F}_2^l \ni w \mapsto (1 + \rho)^{l-|w|} (1 - \rho)^{|w|} \quad (93)$$

note that the identity is true when  $l = 1$  and assume it to be true for  $l$ . Then for  $l + 1$

$$\sum_{v \in \mathbb{F}_2^{l+1}} \rho^{|v|} (-1)^{|vw|} = \sum_{v \in \mathbb{F}_2^l} \rho^{|v|} (-1)^{|vw_1^l|} + \rho^{|v|+1} (-1)^{|vw_1^l|} (-1)^{w_{l+1}} \quad (94)$$

$$= \sum_{v \in \mathbb{F}_2^l} \rho^{|v|} (-1)^{|vw_1^l|} (1 + \rho (-1)^{w_{l+1}}) \quad (95)$$

$$= (1 + \rho)^{l-|w_1^l|} (1 - \rho)^{|w_1^l|} (1 + \rho (-1)^{w_{l+1}}). \quad (96)$$

□

## D Proofs of Lemma 4.13

*Proof.* We represent the channel  $W$  as a  $2 \times |\mathcal{Y}|$  stochastic matrix. By definition of BISO channels, this matrix can be decomposed into pairs of columns which are symmetric as

$$\begin{pmatrix} c & d \\ d & c \end{pmatrix} \quad (97)$$

with  $c, d \geq 0$ , or into single columns which have constant values. Let us assume that  $W$  contains  $m$  such matrices and  $s$  such constant columns. We have

$$\Gamma_l(\nu) = \frac{1}{|\mathcal{Y}|} \sum_{u^{(1)}, \dots, u^{(l)} \in \mathbb{F}_2^k} \left[ \sum_{y \in \mathcal{Y}} \prod_{r=1}^l (1 - P(y|u^{(r)})) \right] \prod_{i=1}^k \nu(u_i^{(1)}, \dots, u_i^{(l)}) \quad (98)$$

$$= \frac{1}{|\mathcal{Y}|} \sum_{v^{(1)}, \dots, v^{(l)} \in \mathbb{F}_2} \left[ \sum_{y \in \mathcal{Y}} \prod_{r=1}^l (1 - W(y|v^{(r)})) \right] \nu^{*k}(v^{(1)}, \dots, v^{(l)}) \quad (99)$$

$$= \frac{1}{|\mathcal{Y}|} \sum_{v \in \mathbb{F}_2^l} g(v) \nu^{*k}(v) \quad (100)$$

$$= \frac{1}{|\mathcal{Y}|} \sum_{w \in \mathbb{F}_2^l} \mathcal{F}(g)(w) \mathcal{F}(\nu)^k(w) \quad (101)$$

where

$$g(v) = \sum_{i=1}^m \left( C_i^{l-|v|} D_i^{|v|} + D_i^{l-|v|} C_i^{|v|} \right) + \sum_{i=1}^s E_i^l, \quad (102)$$

for some positive constants  $C_i, D_i, i \in [m]$ ,  $E_i, i \in [s]$ . Moreover, using (91),

$$C^{l-|v|} D^{|v|} + D^{l-|v|} C^{|v|} \xleftrightarrow{\mathcal{F}} (C + D)^{l-|w|} (C - D)^{|w|} + (C + D)^{l-|w|} (D - C)^{|w|} \quad (103)$$

$$= (C + D)^{l-|w|} (C - D)^{|w|} (1 + (-1)^{|w|}), \quad (104)$$

and  $\mathcal{F}(g)(w)$  has only positive coefficients since only the terms with  $|w|$  even survive. Hence  $\Gamma_l$  is convex when  $k$  is even. □