Stat 316 Stochastic Processes on Graphs

XORSAT on random regular graphs

Andrea Montanari

Lecture 6-? - 10/10/2007

XORSAT is arguably the simplest constraint satisfaction problem. It was introduced by Nadia Creignou and Herve Daude in 1999, and studied in a number of papers since then.

1 k-XORSAT

A k-XORSAT instance is described by a factor graph $G = (V, F, E)$ where $|V| = N$, $|F| = M$ and the factor nodes have degree k. We will denote the set of variable nodes adjacent to factor node a as $\partial a = \{i_1(a), \dots, i_k(a)\}$. Further, for any $a \in F$, we need to specify $J_a \in \{+1, -1\}$.

We will consider the following distribution over $x \in \{+1, -1\}^N$

$$\mu_G(x) = \frac{1}{Z_N(\beta)} \exp\Big\{\beta \sum_{a \in F} J_a x_{i_1(a)} \cdots x_{i_k(a)}\Big\}. \tag{1}$$

In the following we shall be mostly interested in the case in which there exists at least one solution x^* with $J_a x^*_{i_1(a)} \cdots x^*_{i_k(a)} = 1$ for all $a \in F$. In this case, it can be shows that (under a change of variable) the above distribution is 'essentially equivalent' to

$$\mu_G(x) = \frac{1}{Z_N(\beta)} \exp\Big\{\beta \sum_{a \in F} x_{i_1(a)} \cdots x_{i_k(a)}\Big\}. \tag{2}$$

When it will be necessary to specify, we will refer to this as to the *unfrustrated XORSAT* model.

Exercise: What does it mean 'essentially equivalent' the above statement? Describe the change of variables we are referring to.

Basic information on XORSAT, focusing on the zero-temperature case is provided by the Chapter 17 of the book with Marc Mézard, posted online.

In this note we shall focus on ensembles of random (l, k)*-regular graphs*. Such an ensemble is defined whenever $Nl = Mk$ as follows. Attach l half-edges to each variable node $i \in V$, and k half-edges to each function node $a \in F$. Draw a uniformly random permutation over Nl elements, and connect edges on the two sides accordingly.

Throughout, the *adjacency matrix* $\mathbb{H}$ of G will be the binary matrix whose rows correspond to function nodes in F and columns to variable nodes in V. Its entry H_{ai}, $a \in F$, $i \in V$ is just the parity of the multiplicity of edge (a, i) in G.

2 Free energy

Theorem 1. *Let G be a random regular (l, k) factor graph, with $k > l \geq 2$. Then, with high probability*

$$Z_N(\beta) = 2^N (\cosh \beta)^{lN/k}. \tag{3}$$

In particular, the number of solutions is, with high probability $2^{N(1-l/k)}$.

For proving this Theorem, it is convenient to first derive an exact expression for the free energy. In order to do this, we introduce the notion of *hyperloop*. Given a factor graph $G = (V, F, E)$, an hyperloop is a subset F' of the factor node, such that the induced subgraph G' has even degree.

Lemma 2. *Let $G = (V, F, E)$ be a factor graph, $Z_N(\beta)$ the partition function of the associated unfrustrated XORSAT model, and $n_G(\ell)$ denote the number of hyperloops of size ℓ in G. Then, for any β,*

$$Z_N(\beta) = 2^N (\cosh\beta)^M \sum_{\ell=0}^{M} n_G(\ell)\, (\tanh\beta)^\ell \,. \tag{4}$$

Proof By high-temperature expansion. □

We also need a result on the solutions of of random regular linear systems.

Theorem 3. *Let G be a random regular (l, k) factor graph, with $l > k \geq 2$, and $\mathbb{H}$ denote the corresponding adjacency matrix. Then the linear system $\mathbb{H}x = 0, \mod 2$ has, with high probability, the unique solution $x = 0$.*

Proof Let $Z_{\mathbb{H}}(w)$ denote the number of solutions of $\mathbb{H}x = 0$ with w non-zero entries. Compute $\mathbb{E}\, Z_{\mathbb{H}}(w)$ and show that

$$\lim_{N\to\infty} \sum_{w=1}^{N} \mathbb{E}\, Z_{\mathbb{H}}(w) = 0 \,. \tag{5}$$

Some details of the computation are in Chapter 11 of the book online. □

Proof [Theorem 1] In view of the previous lemma, it is sufficient to show that, with high probability, $n_G(\ell) = 0$ for all $\ell \geq 1$, since $n_G(0) = 1$. Let $\mathbb{H}$ be the adjacency matrix of G (with rows corresponding to nodes in F and columns to nodes in V). Then our claim is equivalent to the following: The linear system $\mathbb{H}^T x = 0 \mod 2$ admits the unique solution $x = 0$. This follows from Theorem 3 once we notice that $\mathbb{H}^T$ is the adjacency matrix of a (k, l) regular factor graph. □

3 Phase transition

To be written.