Title
Phase Transitions of Random Constraints Satisfaction Problem

Author
Zhang, Yumeng

Publication Date
2017

Peer reviewed|Thesis/dissertation

Phase Transitions of Random Constraints Satisfaction Problem

by

Yumeng Zhang

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Statistics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Allan M. Sly, Chair
Professor David J. Aldous
Professor Fraydoun Rezakhanlou

Spring 2017

Phase Transitions of Random Constraints Satisfaction Problem

Abstract

Phase Transitions of Random Constraints Satisfaction Problem

by

Yumeng Zhang

Doctor of Philosophy in Statistics

University of California, Berkeley

Professor Allan M. Sly, Chair

Constraints satisfaction problem (CSP) is a family of computation problems that are generally hard to solve in the worst case, which motivates the study of average cases by looking at random CSPs. This thesis studies problems related to random constraints satisfaction problems, in particular its different phase transitions in the large system limit as the level of constraints increases.

The first part of this thesis studies the number of solutions in a typical problem instance. It has long been observed that shortly before the satisfiability phase transition where solutions stop to exist, the number of solutions in a typical instance no longer concentrate around its expectation. Guided by the 1-step replica symmetry breaking heuristics in statistical physics, we prove the correct formula for the typical number of the solutions up to the exponent.

The second part focus on the clustering threshold around which algorithms have been observed to slow down. Different opinions exist for the reason of this algorithmic barrier. One is the shattering of solution space which is conjectured to happen at the clustering threshold. The other is the onset of frozen variables happening at a nearby rigidity threshold. Previous analysis on the clustering threshold was not strong enough to differentiate the two phase transitions. Using a detailed analysis of certain distributional recursion, we show that the reconstruction threshold on trees, which is conjectured to coincide with the clustering threshold, is strictly smaller than the rigidity threshold, laying ground for further studies.

The last part of the thesis studied the Glauber dynamics of graph colorings on d-regular trees. By comparing the Glauber dynamics to a variant of block dynamics, we show that the mixing time, and hence the speed of the related MCMC algorithm, undergoes a phase transition at the reconstruction threshold.

Contents

List of Figures

Acknowledgments

First and foremost, I express my sincere gratitude to my advisor, Allan Sly, without whom this dissertation would not exist. As a mentor, he is always patient, considerate and eager to help; when talking about research, he is never short of interesting problems and brilliant ideas to solve them. I would spend a section on his guidance and encouragement, if it's not already everywhere between the lines of this dissertation. It is one of the luckiest things to know Allan since my first year at Berkeley and become his student.

I also thank Nike Sun, with whom I started working since my fourth year. I learn a lot from her meticulous style in proofs and write-ups, as well as numerous helpful tips in both academic and daily life. In my fourth year, I spent a wonderful summer at Microsoft Research Asia with Pinyan Lu. I thank him for allowing me to join his active group for the summer, and exchanging discussions about the problems in theoretical computer science. My thanks also go to David Aldous, Elchanan Mossel and Fraydoun Rezakhanlou for their help as members of my qualifying exam committee as well as my dissertation committee.

Berkeley Statistic department has been an amazing place to live in as a PhD. I am extremely grateful to the helpful staffs, in particular La Shana, the almighty go-to person for administrative works, and Mary, who saved me every time I locked myself out of my office. I shall remember my fellow Ph.D students in the department. I thank Riddhi Basu for hours of random chatting on everything except math and those extremely handy helps in my postdoc application (and many other things). I thank Hye Soo Choi and Yuting Wei for the company and for the support. I also thank many others, in particular Jonathan Hermon, Wenpin Tang, Sourav Sarkar, Fu Shi, Lihua Lei, Cheng Ju, Jingcheng Liu, for all the math or non-math conversations and for our time together.

I shall never forget my roommate and neighbours at the Oxford Hall. Special thanks to my two roommates, Siyu Yu and Yuxu Han, whose company make a lonely apartment in a distant country home. Also I thank my friendly, fun and easy-going neighbours over the course of six years—Xinyu Cao, Yi Zhou, Anting Xu, Xiaodan Sun, Chuang Qian, Ran Chen, Dongchi Yu, Shifan Deng, Shuang Lin, Xining Zang, Yu Wang, Yuguang Tong and many others, for all those grocery lifts and hotpots, board game nights and birthday cakes, laughters and cherishing memories.

Finally, I am grateful to my parents back in China for their unconditional support. It is hardly need saying that I won't be here today if not them and for that I am forever in debt.

Chapter 1

Introduction

A *constraint satisfaction problem* (CSP) consists of n variables, each taking value from alphabet $\mathcal{X}$, subject to m constraints; a solution to a CSP instance is an assignment of values to the variables such that all constraints are satisfied. The framework of CSPs captures many interesting problems, ranging from brain teasers such as crossword and Soduku, to well-studied research problems such as the Four Coloring problem. These problems can be extremely challenging—*a priori*, finding a valid assignment of 100 binary variables by exhaustive search would require 2^{100} trials. Indeed, many models of CSPs are known to be "NP-complete" [Kar72], the polynomially-time computability of which has been the central open problem in theoretical computer science.

The fact that these problems are intractable in the *worst* case motivates people to study the *average* scenario by considering *typical* properties of *random* problem instances. The two most prominent questions are:

1. When does a CSP have solutions and how many solutions there are?
2. When does there exist an algorithm that finds solutions in polynomial times?

Since their introduction in theoretical computer science, random CSPs have also attracted the interest of physicists and mathematicians, for the rich phenomenon predicted by the theory of statistical physics and the mathematical challenges to prove them. In this thesis we address some aspects of this beautiful and complex picture.

1.1 Definition and background

To introduce the problems formally, we first define two types of constraints satisfaction problem we will be mainly working with in this thesis. Definition to more general models can be found in Section 5.2.1 or [BCO16].

Definition 1.1.1 (k-coloring)**.** Let $G = (V, E)$ be a graph with vertex set V and edge set E, and let $[k] \equiv \{1, \ldots, k\}$ be the set of k colors. We say that a configuration $\sigma \in [k]^V$ is a

k-coloring of graph G if for every edge $e = (u, v) \in E$, $\sigma_u \neq \sigma_v$. Let $\mathsf{SOL}(G) \in [k]^V$ be the set of proper colorings on graph G and define $Z(G) = |\mathsf{SOL}(G)|$ be the number of solutions, a.k.a. *partition function* in physics terms. The Gibbs measure of random colourings on G is given by the uniform measure

$$\mu(\sigma) = \frac{1}{Z}\mathbf{1}\{\sigma \in \mathsf{SOL}(G)\} = \frac{1}{Z}\prod_{e=(u,v)\in E}\mathbf{1}\{\sigma_u \neq \sigma_v\}.$$

Definition 1.1.2 (k-NAE-SAT)**.** Let $G = (V, F, E)$ be a factor graph where V is the set of variables, F the set of constraints, E the set of edges joining variables to clauses. For each $e \in E$, let $v(e) \in V$ and $a(e) \in F$ be the two ends of edge e respectively. We further equip each $e \in E$ with literal $\mathtt{L}_e \in \{\mathtt{0}, \mathtt{1}\}$ and denote the labeled graph by $\mathscr{G} = (G, \underline{\mathtt{L}})$. For each clause $a \in F$, let $\delta a \equiv \{e \in E : a(e) = a\}$ be the set of edges containing a. We say that $\sigma \in \{\mathtt{0}, \mathtt{1}\}^V$ is a solution to the *not-all-equal*-SAT (NAE-SAT) problem on $\mathscr{G}$ if

$$\text{for all } a \in F,\ (\mathtt{L}_e \oplus \sigma_{v(e)})_{e\in\delta a} \text{ is neither identically } \mathtt{0} \text{ nor identically } \mathtt{1}.$$

We further say that the problem is a k-NAE-SAT problem, if for each $a \in F$, $|\delta a| = k$, in which case $m = dn/k$. We again denote the set of NAE-SAT solutions of $\mathscr{G}$ by $\mathsf{SOL}(\mathscr{G}) \subseteq \{\mathtt{0}, \mathtt{1}\}^V$ and define $Z(\mathscr{G}) \equiv |\mathsf{SOL}(\mathscr{G})|$.

As observed in the two examples above, constraints satisfaction problems can be encoded by graphs or factor graphs. Thus the randomness of CSPs can be translated to the randomness of the underlying graph ensemble. Two common choices are the random d-regular graphs and Erdos-Renyi graphs $G(n, m = dn/2)$, or its factor graph analogue in cases where each constraint involves more than 2 variables. The aforementioned questions can be translated into the following: Given the model and the choice of graph ensemble, for what values of d and k

1. Is Z strictly larger than zero with high probability? Under those values, what is the typical value of Z?

2. Is there a polynomial-time algorithm that finds elements of SOL with high probability?

The answers to these questions are closely related to the geometric structure of the solution space SOL, defined by connecting pairs of solutions at Hamming distance one. Indeed, the complicated structure of the solution space posts major obstacles to mathematical analysis. On this front, significant advances were achieved by statistical physicists applying the theory of *spin systems*. Of particular interest is a systematic theory they developed—the so-called *1-step Replica Symmetry Breaking* (1RSB) framework—that applies to a broad family of CSP models, including the ones studied in this thesis. The main conjectural picture is that for those models the solution space $\mathsf{SOL} \subseteq \mathcal{X}^n$ undergoes several phase transitions as $n \to \infty$ and the constraints level $\alpha = m/n$ increases (See Figure 1.1.1) [ZK07; Krz+07; MRS08]. Here we briefly summarize the phenomenon:

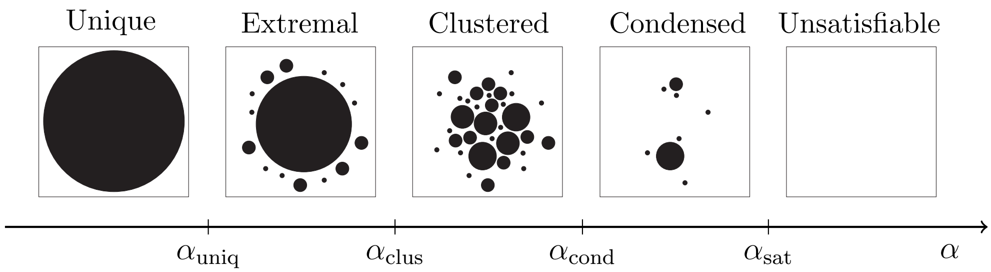


Figure 1.1.1: Phase diagram of random CSPs described by the 1RSB ansatz

For small values of α, SOL consists of a single well-connected cluster with possibly exponentially small exceptions. Upon the *clustering* threshold α_{clus}, SOL shattered into exponentially many clusters each of which is exponentially small. Both the number and the size of the clusters decrease as we increase α. At the *condensation* threshold α_{cond}, the mass condense to a bounded number of clusters. Finally, the SOL is with high probability empty after the *satisfiability* threshold α_{sat}.

While the 1RSB framework gives precise predictions of the phase diagram and has lead to significant algorithmic improvement in practice (e.g. [MZ02]), the theory itself is based on several heuristic assumptions and is hence non-rigorous. Many efforts have been made to verify these predictions and understand their algorithmic implications. In the next two sections, we briefly summarize the current status and the contribution of this thesis along the line.

1.2 Condensed phase and the number of solutions

The paper of Friedgut [Fri99] shows that for many CSP models, the satisfiability of a typical problem instance undergoes a sharp phase transition: Let $\mathbb{P}_{n,\alpha(n)}$ denote the uniform measure over all problem instances with $m = \alpha n$ constraints. There exists a sequence of thresholds $\alpha_{\text{sat}}(n)$ such that for any $\epsilon > 0$,

$$\lim_{n\to\infty} \mathbb{P}_{n,\alpha_{\text{sat}}(n)-\epsilon}(Z(\mathscr{G}) > 0) = \lim_{n\to\infty} \mathbb{P}_{n,\alpha_{\text{sat}}(n)+\epsilon}(Z(\mathscr{G}) = 0) = 1.$$

Similar results for several models on regular (factor) graphs are proved in [BGT13].

Friedgut's result does not give the exact location of $\alpha_{\text{sat}}(n)$, neither does it rule out the intuitively unlikely dependence of $\alpha_{\text{sat}}(n)$ on the number of variables n. Until recently, the exact location of satisfiability threshold has only been established for a few models: random XOR-SAT [MRTZ03], random 2-SAT [CR92; Goe96], random 1-in-k-SAT [Ach+01], all of which have a simpler phase diagram than the one in Figure 1.1.1. In the last couple of years, a sequence of works determines the exact location of α_{sat} or narrows it down for models that fall under the 1RSB framework: k-NAE-SAT [CZ12; DSS16], independent set [DSS13], k-SAT [BC15; DSS15], k-coloring [COEH16].

The time gap between the two groups of results reflects the complex nature of models following the 1RSB ansatz, which is largely due to the existence of a "condensed" phase immediately preceding the satisfiability threshold: in this regime, the solution space SOL is dominated by a few large clusters and the expected number of solutions $\mathbb{E}Z$ is blown up by "atypically-large" ones that are unlikely to be seen in a typical instance. As a result, the typical number of solutions $Z \ll \mathbb{E}Z$ with high probability [CZ12] and solving $\mathbb{E}Z = 0$ does not yield the correct α_{sat}. Non-trivial arguments are necessary to eliminate those effects, in which the physics insight again plays a crucial role.

The satisfiability threshold threshold is only one facet of the rich theory physicists have developed. There are deep conjectures for the behavior of these models inside the satisfiable regime. In Chapter 2, we continue the quest and determine the total number of solutions $Z = |\mathsf{SOL}|$ for typical instances, in particular in the condensed regime where $Z \ll \mathbb{E}Z$ with high probability. We will work with the random k-NAE-SAT model and show that for $k \geqslant k_0$ and $\alpha_{\text{cond}} \leqslant \alpha < \alpha_{\text{sat}}$, the typical value of Z is up to a sub-exponential factor given by the largest cluster exists in SOL. We further give the explicit formula $\mathsf{f}^{1\text{RSB}}(\alpha)$ such that for a typical random regular k-NAE-SAT problem as $n \to \infty$,

$$\frac{1}{n} \ln Z \xrightarrow{p.} \mathsf{f}^{1\text{RSB}}(\alpha).$$

The appeal of NAE-SAT model is that it has certain symmetries making the analysis particularly tractable, yet it is expected to share most of the interesting qualitative phenomena exhibited by other commonly studied problems, including random k-SAT and random graph colorings.

1.3 Clustering thresholds and sampling solutions

1.3.1 Algorithmic barrier

While solutions exist up to the satisfiability threshold α_{sat}, as has been observed and partially verified in many works, the actual barrier for finding and sampling solutions lies around the clustering threshold α_{clus}: simple greedy algorithms are known to find solutions for k-coloring and k-SAT instances up to $(1-\epsilon)\alpha_{\text{clus}}$, and no algorithm is known to work significantly better. In fact, the failure of certain families of algorithms has been proved for $\alpha > (1+\epsilon)\alpha_{\text{clus}}$ [RV14], or a slightly smaller region [GS14; COHH16]. This motivate people to study the clustering threshold and its algorithmic implication. Intuitively, it would be hard for algorithms to traverse the solution space when it is dominated by exponentially many well-separated clusters [ACO08; ACORT11].

Unlike the satisfiability threshold, the clustering phase transition are less well-understood. Take the k-coloring model as an example. It is conjectured that at d_{clus} (here $d = 2\alpha$) the solution space SOL shatters into exponentially many small clusters. Meanwhile, a close but different phase transition, the *rigidity* phase transition, is conjectured to happen at $d_{\text{rig}} \approx (1 + o(1))d_{\text{clus}}$, beyond which most of the clusters become "frozen", i.e. a linear fraction of variables take the same value throughout the cluster [ZK07].

The two closeby phase transitions play an important role in understanding the algorithmic barrier as different papers disagree on which one of them is more responsible for the algorithmic slow down [MZ02; ZK07; ZM08], if any of them [Bra+16]. However, it is unknown even at a heuristic level if the gap $|d_{\text{clus}} - d_{\text{rig}}|$ is indeed non-vanishing [Sly09; Mol12], let alone analyzing their impact on algorithms.

One obstacle is that the conjectural clustering threshold $d^\star_{\text{clus}}$ is characterized in physics literature by the non-trivial fixed points of certain distributional recursion. The high dimension of the recursion makes it hard to analyze without restricting the domain to distributions with large atoms—which amount to clusters with frozen variables. Thus it is hard to separate the discussion of the clustering threshold with the rigidity threshold. The other obstacle lies in proving the clustering phenomenon in the unfrozen regime, i.e. proving $d_{\text{clus}} = d^\star_{\text{clus}}$. Unlike frozen clusters, which are disconnected components of the solution space, unfrozen clusters may connect to each other as long as there are "bottlenecks" at the boundary. Thus unfrozen clusters are much harder to characterize and analyze mathematically.

In Chapter 3 and Chapter 4, we address the first obstacle by analyzing the distributional recursion used in the definition of $d^\star_{\text{clus}}$, which coincide with the *reconstruction problem* on trees [MM09, Ch.19]. With the exact definitions postponed to Chapter 3, we show that for both k-coloring model (Chapter 3) and k-NAE-SAT model (Chapter 4) with $k \geqslant k_0$, the reconstruction threshold d_{rec}, which is also the conjectural clustering threshold $d^\star_{\text{clus}}$, is strictly smaller than the rigidity threshold, and the gap is an increasing function of k.

Thus given the conjecture that $d_{\text{clus}} = d^\star_{\text{clus}}$, our results in Chapter 3 and Chapter 4 strongly suggest a non-vanishing phase where the solution space are clustered but non-frozen. We believe that analyzing algorithms in this region will be very helpful in understanding the nature of the algorithmic barrier.

1.3.2 Efficient sampling algorithms before d_{clus}

In Chapter 5, we give an example of algorithms that actually slows down at the reconstruction threshold. We consider the problem of uniformly sampling proper k-colorings on d-regular trees with n-vertices. A widely-used sampling algorithm is Markov Chain Monte Carlo (MCMC) based on the *Glauber dynamics*, which is a Markov chain that at each step updates the value of an uniformly selected vertex randomly according to its surrounding vertices. The central question is to bound the mixing time of the Markov chain, i.e. the time until the Markov chain is "close" to its stationary distribution. More precisely, let $P^t(\sigma, \cdot)$ be the distribution of the Markov chain starting from σ after t steps, and π be the stationary distribution, the mixing time is defined as

$$t_{\text{mix}} \equiv \min\{t \geqslant 0 : |P^t(\sigma, A) - \pi(A)| \leqslant 1/4, \text{ for all initial state } \sigma \text{ and event } A\},$$

If the mixing time grows polynomially in the number of variables, then the corresponding MCMC algorithm samples solutions efficiently.

In Chapter 5, we show that the mixing time is $O(n \ln n)$ for $k \geqslant k_0, d \leqslant d_{\text{rec}} \approx (1 + o(1))k \ln k$ (cf. (3.1.3)), improving the previous results of $d \leqslant k + 2$ [MSW07; Bha+11]. In particular combining our result with [Tet+12] implies a sharp transition of the mixing time at the exact reconstruction threshold $d = d_{\text{rec}}$.

1.4 Note on prior publication and collaboration

The results presented in this dissertation are obtained in collaboration with other researchers and some have already been published elsewhere. Chapter 2 is based on a joint work with Allan Sly and Nike Sun [SSZ16]. The remaining chapters are based on joint works with Allan Sly: Chapter 3 is based on [SZ16], Chapter 4 is based on unpublished note, and Chapter 5 is based on [SZ14]. All three papers mentioned are available on ArXiv. I express my sincere thanks towards my co-authors for allowing the inclusion of joints works with them in this dissertation.

Chapter 2

The number of solutions for random regular NAE-SAT

2.1 Introduction

2.1.1 Main result

In this chapter, we study the number of solutions to a *random k-NAE-SAT problem.* (The formal definition is given in Section 2.2.) More specifically, we work on *d-regular* instances where each variable appears in exactly d clauses. See [AM06] for important early work on the closely related model of random (Erdős–Rényi) NAE-SAT.

Following convention, we fix k and then parametrize the model by its clause-to-variable ratio, $\alpha = d/k$. The *partition function* of the model, denoted $Z \equiv Z_n$, is simply the number of valid NAE-SAT assignments for an instance on n variables. It is conjectured that for each $k \geqslant 3$, the model has an exact satisfiability threshold $\alpha_{\text{sat}}(k)$: for $\alpha < \alpha_{\text{sat}}$ it is satisfiable ($Z > 0$) with high probability, but for $\alpha > \alpha_{\text{sat}}$ it is unsatisfiable ($Z = 0$) with high probability (as $n \to \infty$, with k fixed). This has been proved [DSS16] for all k exceeding an absolute constant k_0, together with an explicit formula for α_{sat} which matches the physics prediction. The exact formula is rather intricate so we omit it here, and note only its approximate value

$$\alpha_{\text{sat}} = \left(2^{k-1} - \frac{1}{2} - \frac{1}{4\ln 2}\right)\ln 2 + \epsilon_k \tag{2.1.1}$$

where ϵ_k denotes an error tending to zero as $k \to \infty$.

We say the model has *free energy* $\mathsf{f}(\alpha)$ if $Z^{1/n}$ converges to $\mathsf{f}(\alpha)$ in probability as $n \to \infty$. *A priori*, the limit may not be well-defined. If it exists, however, Markov's inequality and Jensen's inequality imply that it must be upper bounded by the *replica symmetric free energy*

$$\mathsf{f}^{\text{RS}}(\alpha) \equiv (\mathbb{E}Z)^{1/n} = 2(1 - 2/2^k)^{\alpha}. \tag{2.1.2}$$

One of the intriguing predictions from the physics analysis [ZK07; MRS08] is that there is a critical value α_{cond} strictly below α_{sat}, such that $\mathsf{f}(\alpha)$ and $\mathsf{f}^{\text{RS}}(\alpha)$ agree up to $\alpha =$

α_{cond} and diverge thereafter. Since f^{RS} is analytic, f must be non-analytic at α_{cond}. This is the *condensation* or *Kauzmann transition*, and will be further described below. For $\alpha \in (\alpha_{\text{cond}}, \alpha_{\text{sat}})$ it is conjectured that $\mathsf{f}(\alpha)$ takes a value $\mathsf{f}^{1\text{RSB}}(\alpha)$ strictly below $\mathsf{f}^{\text{RS}}(\alpha)$. The function $\mathsf{f}^{1\text{RSB}}(\alpha)$ is explicit, although not extremely simple: it is derived via the heuristic of *one-step replica symmetry breaking* (1RSB), and is presented below in Definition 2.1.3. Our main result is to prove this prediction for large k.

Theorem 1. *In random regular k-NAE-SAT with $k \geqslant k_0$, for all $\alpha < \alpha_{\text{sat}}(k)$ the free energy $\mathsf{f}(\alpha)$ exists and equals the predicted value $\mathsf{f}^{1\text{RSB}}(\alpha)$.*

Remark 2.1.1. We allow for k_0 to be adjusted as long as it remains an absolute constant (so it need not equal the k_0 from [DSS16]). The result of Theorem 1 is already proved [DSS16] for $\alpha \leqslant \alpha_{\text{lbd}} \equiv (2^{k-1}-2)\ln 2$, so we restrict our attention to $\alpha \in (\alpha_{\text{lbd}}, \alpha_{\text{sat}})$, which is a strict superset of the condensation regime $(\alpha_{\text{cond}}, \alpha_{\text{sat}})$. Of course, for $\alpha > \alpha_{\text{sat}}$, we already know $\mathsf{f}(\alpha) = 0$. The case $\alpha = \alpha_{\text{sat}}$ can arise only if $d_{\text{sat}}(k) \equiv k\alpha_{\text{sat}}(k)$ is integer-valued for some k. We have no reason to believe that this ever occurs; if however it does miraculously occur then the probability for $Z > 0$ is bounded away from both zero and one. In this case, our methods would show that $Z^{1/n}$ does not concentrate around a single value but rather on two values, zero and $\lim_{\alpha\uparrow\alpha_{\text{sat}}} \mathsf{f}^{1\text{RSB}}(\alpha)$.

The condensation transition has been actively studied in recent work. The existence of a condensation phenomenon was first established for random NAE-SAT [CP12], and has since been found in random regular NAE-SAT and independent set [DSS16; DSS13]. It has been demonstrated to occur even at positive temperature in the problem of hypergraph bicoloring (which is very similar to NAE-SAT) [BCORm16]. However, determining the precise location of α_{cond} is challenging, and was first achieved for the random graph coloring model [Bap+16] by an impressive and technically challenging analysis. Subsequent work pinpoints α_{cond} for random regular k-SAT (which again is very similar to NAE-SAT) [BC15]. The main contribution of this paper is to determine for the first time the free energy throughout the condensation regime $(\alpha_{\text{cond}}, \alpha_{\text{sat}})$.

2.1.2 Statistical physics predictions

As mentioned in the introduction chapter, the random regular NAE-SAT model has a single level of replica symmetry breaking (1RSB) and undergoes similar phase transitions as pictured in Figure 1.1.1. We now summarize the key predictions leading to the condensation phase transition and refer the details to [MM09, Ch. 19]. While part of the following discussion remains conjectural, much of it is rigorously established by the present paper. For this discussion we focus on the leading exponential terms and ignore $\exp\{o(n)\}$ corrections.

Fix k and set $\alpha = d/k$. Recall that for α well above α_{clus} (which is true for α_{cond} when k is large), the solution space breaks up into well-separated clusters. It is predicted that the number of clusters of size $\exp\{ns\}$ has mean value $\exp\{n\Sigma(s;\alpha)\}$, and further is concentrated about this mean; Σ is the "cluster complexity function." It is common to abbreviate $\Sigma(s) \equiv \Sigma(s;\alpha)$. Summing this prediction over cluster sizes s gives that the total number Z of NAE-SAT solutions has mean

$$\mathbb{E}Z \doteq \sum_s \exp\{n[s+\Sigma(s)]\} \doteq \exp\{n[s_1+\Sigma(s_1)]\},$$

where $s_1 = \arg\max[s+\Sigma(s)]$, and we write $\doteq$ to indicate equality up to $\exp\{o(n)\}$ factors. It is predicted that Σ is continuous and strictly concave in s, and also that $s+\Sigma(s)$ has a unique maximizer s_1 with $\Sigma'(s_1) = -1$. Note that we have the dependence $s_1 = s_1(\alpha)$, and $\Sigma(s_1) = \Sigma(s_1(\alpha);\alpha)$.

Under the 1RSB framework, physicists propose an explicit (conjectural) formula for Σ. For NAE-SAT and related models, this explicit calculation reveals another critical value $\alpha_{\text{cond}} \in (\alpha_{\text{clus}}, \alpha_{\text{sat}})$, characterized as

$$\alpha_{\text{cond}} = \inf\{\alpha \geqslant \alpha_{\text{clus}} : \Sigma(s_1(\alpha);\alpha) < 0\}.$$

For $\alpha > \alpha_{\text{cond}}$, $\mathbb{E}Z$ is dominated by clusters of size $\exp\{ns_1\}$, whose mean number $\exp\{n\Sigma(s_1)\}$ is exponentially small, meaning they are highly unlikely to appear in a typical realization. Instead, a typical realization is dominated by clusters of size $s_{\max}$ where

$$s_{\max} \equiv s_{\max}(\alpha) \equiv \arg\max\{s+\Sigma(s) : \Sigma(s) \geqslant 0\}.$$

Since $\Sigma(s_{\max}) = 0$, it follows that with high probability

$$Z \doteq \exp\{n[s_{\max}+\Sigma(s_{\max})]\} = \exp\{ns_{\max}\}.$$

According to this picture, we will have (with high probability) $Z \doteq \mathbb{E}Z$ for $\alpha \leqslant \alpha_{\text{cond}}$, and $Z \ll \mathbb{E}Z$ for $\alpha > \alpha_{\text{cond}}$. Thus, for $\alpha > \alpha_{\text{cond}}$, the first moment $\mathbb{E}Z$ fails to capture the typical behavior of Z. This difficulty persists up to and beyond the satisfiability threshold

$$\alpha_{\text{sat}} = \inf\{\alpha \geqslant \alpha_{\text{cond}} : \max_s \Sigma(s;\alpha) < 0\}$$

— indeed, it is well known that there is a non-trivial interval $(\alpha_{\text{sat}}, \alpha_1)$ in which $\mathbb{E}Z \gg 1$ even though $Z = 0$ with high probability.

2.1.3 The tilted cluster partition function

Once the function $\Sigma(s;\alpha)$ is determined, it becomes straightforward to derive α_{cond}, α_{sat}, and $\mathsf{f}(\alpha)$. However, prior works have not taken the approach of actually computing Σ. Indeed, α_{sat} was determined [DSS16] by an analysis involving only $\max_s \Sigma(s;\alpha)$, which contains less information than the full curve Σ. In related models, the determination of α_{cond} [Bap+16; BC15] also avoids Σ, going instead through the so-called "planted model." In order to obtain Σ, consider the λ-tilted partition function

$$\boldsymbol{Z}_\lambda \equiv \sum_{\boldsymbol{\gamma}} |\boldsymbol{\gamma}|^\lambda \tag{2.1.3}$$

where the sum is taken over all clusters $\boldsymbol{\gamma}$. According to the physics heuristic as described above, $\mathbb{E}\boldsymbol{Z}_\lambda \doteq \exp\{n\mathfrak{F}(\lambda)\}$ where $\mathfrak{F}$ is the Legendre dual of $-\Sigma$:

$$\mathfrak{F}(\lambda) \equiv (-\Sigma)^\star(\lambda) \equiv \max_s[\lambda s + \Sigma(s)].$$

The physics approach to computing Σ is to first compute $\mathfrak{F}$, and then set $\Sigma = -\mathfrak{F}^\star$. Note that by differentiating $\mathfrak{F}(\lambda) = n^{-1}\ln\mathbb{E}\boldsymbol{Z}_\lambda$ we find that $\mathfrak{F}$ is convex in λ, so the resulting Σ will indeed be concave.

The computation of $\mathfrak{F}(\lambda)$ may seem at first glance quite intractable. Indeed, the reason for NAE-SAT solutions to occur in clusters is that a typical solution has a positive density of variables which are *free*, meaning their value can be changed without violating any clause. Each cluster (connected component of NAE-SAT solutions) may be a complicated subset of $\{\mathtt{0},\mathtt{1}\}^n$ — changing the value at one free variable may affect whether its neighbors are free, so a cluster need not be a simple subcube of $\{\mathtt{0},\mathtt{1}\}^n$. We then wish to sum over the cluster sizes raised to non-integer powers.

However, in the regime of interest $\alpha \geqslant \alpha_{\mathrm{lbd}}$ (see Remark 2.1.1), the analysis of NAE-SAT solution clusters is greatly simplified by the fact that in a typical satisfying assignment the vast majority of variables are *frozen* rather than free. The result of this, roughly speaking, is that a cluster can be encoded by a configuration $\underline{x} \in \{\mathtt{0},\mathtt{1},\mathtt{f}\}^n$ (representing its circumscribed subcube, so $x_v = \mathtt{f}$ indicates a free variable) with no essential loss of information. We call $\underline{x}$ the *frozen configuration* representing the cluster. It turns out that the frozen configurations can be regarded as the solutions of a certain CSP lifted from the original NAE-SAT problem — so the physics heuristics can be applied again to the new CSP. Variations on this idea appear in several places in the physics literature; in the specific context of random CSPs we refer to [Par02; BMZ05; MMW07].

Analyzing the *number* of frozen configurations — corresponding to (2.1.3) with $\lambda = 0$ — leads to the sharp satisfiability threshold for this model [DSS16]. To analyze (2.1.3) for general λ requires a deeper investigation of the arrangement of free and frozen variables in the frozen configurations $\underline{x}$. In fact, the majority of free variables are simply isolated vertices. A smaller fraction occur in linked pairs, and a yet smaller fraction occur in components of size three or more. Each free component $\boldsymbol{T}$ is surrounded by frozen variables, and we let $z(\boldsymbol{T})$ count the number of NAE-SAT assignments on $\boldsymbol{T}$ which are consistent with the frozen boundary. Then the total size of the cluster represented by $\underline{x}$ is simply the product of $z(\boldsymbol{T})$ over all the free components $\boldsymbol{T}$ of $\underline{x}$.

The random NAE-SAT graph has few short cycles, so almost all of the free components are *trees*, and so their weights $z(\boldsymbol{T})$ can be evaluated recursively by the method of *belief propagation* (BP). To implement this, we must replace variable spins by "messages," which are indexed by the directed edges of the graph and so are more natural for tree recursions. The message $\mathtt{m}_{v\to a}$ from variable v to clause a represents the state of v "in absence of a." It is also necessary to introduce a richer alphabet of symbols for these messages, replacing $\{\mathtt{0},\mathtt{1},\mathtt{f}\}$ with probability measures on $\{\mathtt{0},\mathtt{1}\}$ (where any non-degenerate measure will project to $\mathtt{f}$). Thus the message $\mathtt{m}_{v\to a}$ represents the distribution at v (within the cluster) in absence of clause a. The messages are related to one another via local consistency equations, which are precisely the BP equations. The configuration $\underline{\mathtt{m}}$ encodes the same cluster as $\underline{x}$, with the key advantage that *the cluster size can be readily deduced from* $\underline{\mathtt{m}}$*, as a certain product of local functions.* For the cluster size raised to power λ, simply raise each local function to power λ. Thus the configurations $\underline{\mathtt{m}}$ with λ-tilted weights form a *spin system* (Markov random field), whose partition function is the quantity of interest (2.1.3). The new spin system is sometimes termed the "auxiliary model" [MM09, Ch. 19].

2.1.4 One-step replica symmetry breaking

Above, we asserted informally that each BP solution $\underline{\mathtt{m}}$ encodes a cluster of NAE-SAT solutions. An important caveat is that this is only rigorous if the free variables in $\underline{\mathtt{m}}$ occur in trees, separated by frozen regions where we must have messages $\mathtt{m}_{v\to a}$ that are degenerate (supported on either on $\mathtt{0}$ or on $\mathtt{1}$). Otherwise, one always has the trivial "replica symmetric" BP solution where every $\mathtt{m}_{v\to a}$ is $\mathrm{unif}(\{\mathtt{0},\mathtt{1}\})$, and this is not a "meaningful" solution for large α. One way to understand this is via the physics calculation of $\mathsf{f}^{\mathrm{RS}}(\alpha)$, which we now describe by way of motivating the more complicated expression for $\mathsf{f}^{\mathrm{1RSB}}(\alpha)$.

Given a random regular NAE-SAT instance $\mathscr{G}$ on n variables, choose k uniformly random variables $v_1,\ldots,v_k$, and assume for simplicity that no two of these share a clause. Then (1) remove the k variables along with their kd incident clauses, producing an instance $\mathscr{G}''$, and (2) add $d(k-1)$ new clauses to $\mathscr{G}''$, producing $\mathscr{G}'$. Then $\mathscr{G}'$ is distributed as a random regular NAE-SAT instance on $n-k$ variables. If the free energy exists, then

$$\mathsf{f}(\alpha)^n \doteq Z \doteq [Z(\mathscr{G})/Z(\mathscr{G}')]^{n/k}. \tag{2.1.4}$$

Suppose u is a variable in $\mathscr{G}'$ of degree $d-1$, meaning it was a neighbor of a clause a which was deleted from $\mathscr{G}$. The interpretation of $\underline{\mathtt{m}}$ is that in $\mathscr{G}''$, the spin at u has law $\mathtt{m}_{u\to a}$, and the different $u's$ are independent. If every $\mathtt{m}_{u\to a}$ is $\mathrm{unif}(\{\mathtt{0},\mathtt{1}\})$, then

$$\left(\frac{Z(\mathscr{G})}{Z(\mathscr{G}'')}\right)^{1/k} = 2(1-2/2^k)^d, \quad \left(\frac{Z(\mathscr{G}')}{Z(\mathscr{G}'')}\right)^{1/k} = (1-2/2^k)^{\alpha(k-1)}, \tag{2.1.5}$$

Taking the ratio of these and substituting into (2.1.4) gives the prediction $\mathsf{f}(\alpha) \doteq \mathsf{f}^{\mathrm{RS}}(\alpha)$, which we know to be false for large α. Thus the replica symmetric $\underline{\mathtt{m}}$ gives the incorrect prediction. The reason for this failure is that in reality the u's are *not* independent in $\mathscr{G}''$, but rather are significantly correlated even though they are typically far apart in $\mathscr{G}''$. This phenomenon of long-range dependence may be taken as a definition of replica symmetry breaking, and it is expected to occur precisely for $\alpha > \alpha_{\mathrm{cond}}$.

The idea of 1RSB is that, in passing from the original NAE-SAT model to the (seemingly far more complicated) "auxiliary model" of weighted BP solutions, we in fact return to replica symmetry, provided

$$\Sigma(s_\lambda) > 0 \quad \text{for} \quad s_\lambda \equiv \arg\max_s\{\lambda s + \Sigma(s)\}. \tag{2.1.6}$$

That is, for such λ, the auxiliary model is predicted to have correlation decay, in contrast with the long-range correlations of the original model. The implication is that in this context, the above heuristic ((2.1.4) and (2.1.5)) *is* expected to yield the correct answer. The replica symmetric BP solution for the auxiliary model will be a certain measure $\dot{q}_\lambda$ over messages $\mathtt{m}$. Taking $\dot{q}_{v\to a} \equiv \dot{q}_\lambda$ is the precise analogue, in the auxiliary model, of taking $\mathtt{m}_{v\to a} \equiv \mathrm{unif}(\{\mathtt{0},\mathtt{1}\})$ on every $v \to a$ in the original model. Under the assumption that the auxiliary model has strong correlation decay, (2.1.4) and (2.1.5) give an expression for $\mathfrak{F}(\lambda)$ in terms of $\dot{q}_\lambda$.

2.1.5 The 1RSB free energy prediction

Having described the heuristic reasoning, we now proceed to formally state the 1RSB free energy prediction. We first describe $\dot{q}_\lambda$ is a certain discrete probability measure over $\mathtt{m}$. Since $\mathtt{m}$ is a probability measure over $\{\mathtt{0},\mathtt{1}\}$, we encode it by $x \equiv \mathtt{m}(\mathtt{1}) \in [0,1]$. A measure q on $\mathtt{m}$ can thus be encoded by an element $\mu \in \mathscr{P}$ where $\mathscr{P}$ denotes the set of discrete probability measures on $[0,1]$. For measurable $B \subseteq [0,1]$, define

$$\begin{aligned}
\hat{\mathscr{R}}_\lambda\mu(B) &\equiv \hat{\mathscr{Z}}(\mu)^{-1}\int\Big(2-\prod_{i=1}^{k-1}x_i-\prod_{i=1}^{k-1}(1-x_i)\Big)^\lambda \mathbf{1}\Big\{\frac{1-\prod_{i=1}^{k-1}x_i}{2-\prod_{i=1}^{k-1}x_i-\prod_{i=1}^{k-1}(1-x_i)}\in B\Big\}\prod_{i=1}^{k-1}\mu(dx_i),\\
\dot{\mathscr{R}}_\lambda\mu(B) &\equiv \dot{\mathscr{Z}}(\mu)^{-1}\int\Big(\prod_{i=1}^{d-1}y_i+\prod_{i=1}^{d-1}(1-y_i)\Big)^\lambda \mathbf{1}\Big\{\frac{\prod_{i=1}^{d-1}y_i}{\prod_{i=1}^{d-1}y_i+\prod_{i=1}^{d-1}(1-y_i)}\in B\Big\}\prod_{i=1}^{d-1}\mu(dy_i),
\end{aligned} \tag{2.1.7}$$

where $\hat{\mathscr{Z}}(\mu)$ and $\dot{\mathscr{Z}}(\mu)$ are the normalizing constants such that $\hat{\mathscr{R}}_\lambda\mu$ and $\dot{\mathscr{R}}_\lambda\mu$ are also probability measures on $[0,1]$. (In the context of $\lambda = 0$ we take the convention that $0^0 = 0$.) Denote $\mathscr{R}_\lambda \equiv \dot{\mathscr{R}}_\lambda \circ \hat{\mathscr{R}}_\lambda$. The map $\mathscr{R}_\lambda : \mathscr{P} \to \mathscr{P}$ represents the BP recursion for the auxiliary model. The following presents a solution in the regime

$$(2^{k-1}-2)\ln 2 \equiv \alpha_{\mathrm{lbd}} \leqslant \alpha \leqslant \alpha_{\mathrm{ubd}} \equiv 2^{k-1}\ln 2,$$

which we recall is a superset of $(\alpha_{\mathrm{cond}}, \alpha_{\mathrm{sat}})$.

Proposition 2.1.2. *For any $\lambda \in [0,1]$, let $\dot{\mu}_{\lambda,l} \in \mathscr{P}$ be the sequence of probability measures defined by $\dot{\mu}_{\lambda,0} \equiv \frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$ and $\dot{\mu}_{\lambda,l+1} = \mathscr{R}_\lambda\dot{\mu}_{\lambda,l}$ for all $l \geqslant 1$. Let*

$$S_l \equiv (\operatorname{supp}\dot{\mu}_{\lambda,l})\backslash(\operatorname{supp}(\dot{\mu}_{\lambda,0}+\ldots+\dot{\mu}_{\lambda,l-1})),$$

so S_l is a finite subset of $[0,1]$. Regard $\dot{\mu}_{\lambda,l}$ as an infinite sequence indexed by the elements of S_1 in increasing order, followed by the elements of S_2 in increasing order, and so on. For $k \geqslant k_0$ and $\alpha_{\mathrm{lbd}} \leqslant \alpha \leqslant \alpha_{\mathrm{ubd}}$, in the limit $l \to \infty$, $\dot{\mu}_{\lambda,l}$ converges in the ℓ^1 sequence space to a limit $\dot{\mu}_\lambda \in \mathscr{P}$ satisfying $\dot{\mu}_\lambda = \mathscr{R}_\lambda\dot{\mu}_\lambda$ and

$$\dot{\mu}_\lambda((0,1)) \leqslant 7/2^k, \quad \dot{\mu}_\lambda(dx) = \dot{\mu}_\lambda(d(1-x)).$$

The limit $\dot{\mu}_\lambda$ of Proposition 2.1.2 encodes the desired replica symmetric solution $\dot{q}_\lambda$ for the auxiliary model. We can then express $\mathfrak{F}(\lambda)$ in terms of $\dot{\mu}_\lambda$ as follows. Writing $\hat{\mu}_\lambda \equiv \mathscr{R}_\lambda \dot{\mu}_\lambda$, let $\dot{w}_\lambda, \hat{w}_\lambda, \bar{w}_\lambda \in \mathscr{P}$ be defined by

$$\begin{aligned}
\dot{w}_\lambda(B) &= (\dot{\mathfrak{Z}}_\lambda)^{-1} \int \bigg(\prod_{i=1}^d y_i + \prod_{i=1}^d (1-y_i) \bigg)^\lambda \mathbf{1}\bigg\{ \prod_{i=1}^d y_i + \prod_{i=1}^d (1-y_i) \in B \bigg\} \prod_{i=1}^d \hat{\mu}_\lambda(dy_i), \\
\hat{w}_\lambda(B) &= (\hat{\mathfrak{Z}}_\lambda)^{-1} \int \bigg(1 - \prod_{i=1}^k x_i - \prod_{i=1}^k (1-x_i) \bigg)^\lambda \mathbf{1}\bigg\{ 1 - \prod_{i=1}^k x_i - \prod_{i=1}^k (1-x_i) \in B \bigg\} \prod_{i=1}^k \dot{\mu}_\lambda(dx_i), \\
\bar{w}_\lambda(B) &= (\bar{\mathfrak{Z}}_\lambda)^{-1} \iint \Big(xy + (1-x)(1-y) \Big)^\lambda \mathbf{1}\Big\{ xy + (1-x)(1-y) \in B \Big\} \dot{\mu}_\lambda(dx) \hat{\mu}_\lambda(dy),
\end{aligned} \tag{2.1.8}$$

with $\dot{\mathfrak{Z}}_\lambda, \hat{\mathfrak{Z}}_\lambda, \bar{\mathfrak{Z}}_\lambda$ the normalizing constants. The analogue of (2.1.5) for this model is

$$\left(\frac{\boldsymbol{Z}_\lambda(\mathscr{G})}{\boldsymbol{Z}_\lambda(\mathscr{G}'')} \right)^{1/k} = \dot{\mathfrak{Z}}_\lambda (\hat{\mathfrak{Z}}_\lambda / \bar{\mathfrak{Z}}_\lambda)^d, \quad \left(\frac{\boldsymbol{Z}_\lambda(\mathscr{G}')}{\boldsymbol{Z}_\lambda(\mathscr{G}'')} \right)^{1/k} = (\hat{\mathfrak{Z}}_\lambda)^{\alpha(k-1)},$$

and substituting into (2.1.4) gives the 1RSB prediction $\boldsymbol{Z}_\lambda \doteq \exp\{\mathfrak{F}(\lambda)\}$ where

$$\mathfrak{F}(\lambda) \equiv \mathfrak{F}(\lambda; \alpha) \equiv \ln \dot{\mathfrak{Z}}_\lambda + \alpha \ln \hat{\mathfrak{Z}}_\lambda - k\alpha \ln \bar{\mathfrak{Z}}_\lambda. \tag{2.1.9}$$

Further, the maximizer of (2.1.6) is predicted to be given by

$$s_\lambda \equiv s_\lambda(\alpha) \equiv \int \ln(x) \dot{w}_\lambda(dx) + \alpha \int \ln(x) \hat{w}_\lambda(dx) - k\alpha \int \ln(x) \bar{w}_\lambda(dx). \tag{2.1.10}$$

If $s = s_\lambda$ for $\lambda \in [0,1]$ we define

$$\Sigma(s) \equiv \Sigma(s; \alpha) \equiv \mathfrak{F}(\lambda; \alpha) - \lambda s_\lambda(\alpha).$$

This yields the predicted thresholds

$$\begin{aligned}
\alpha_{\text{cond}} &\equiv \sup\{\alpha : \Sigma(s_1; \alpha) > 0\}, \\
\alpha_{\text{sat}} &\equiv \sup\{\alpha : \Sigma(s_0; \alpha) > 0\},
\end{aligned}$$

and we can now formally state the predicted free energy of the original NAE-SAT model:

Definition 2.1.3. For $\alpha \in k^{-1}\mathbb{Z}$, 1RSB free energy prediction $\mathsf{f}^{\text{1RSB}}(\alpha)$ is defined as

$$\mathsf{f}^{\text{1RSB}}(\alpha) = \begin{cases} \mathsf{f}^{\text{RS}}(\alpha) = 2(1-2/2^k)^\alpha & \alpha \leqslant \alpha_{\text{cond}}, \\ \exp[\sup\{s : \Sigma(s) \geqslant 0\}] & \alpha_{\text{cond}} \leqslant \alpha < \alpha_{\text{sat}}, \\ 0 & \alpha > \alpha_{\text{sat}}. \end{cases} \tag{2.1.11}$$

(In regular k-NAE-SAT we must have integer $d = k\alpha$, so we need not consider $\alpha \notin k^{-1}\mathbb{Z}$.)

Proposition 2.1.4. *Consider $\alpha \in A \equiv [\alpha_{\text{lbd}}, \alpha_{\text{ubd}}] \cap (k^{-1}\mathbb{Z})$. For $k \geqslant k_0$ and $\alpha \in A$, the function $\Sigma(s) \equiv \Sigma(s; \alpha)$ is well-defined, continuous, and strictly decreasing in s, so that $\mathsf{f}^{\text{RS}}(\alpha)$ is well-defined.*

Proposition 2.1.5. *For $k \geqslant k_0$ and $\lambda \in [0,1]$, $\Sigma(s_\lambda;\alpha) \equiv \mathfrak{F}(\lambda) - \lambda s_\lambda$ is strictly decreasing as a function of $\alpha \in A$. There is a unique $\alpha_\lambda \in A$ such that $\Sigma(s_\lambda;\alpha)$ is non-negative for all $\alpha \leqslant \alpha_\lambda$, and is negative for all $\alpha > \alpha_\lambda$. In particular*

$$\alpha_{\text{cond}} = \alpha_1 = (2^{k-1} - 1)\ln 2 + \mathsf{err}, \quad \alpha_{\text{sat}} = \alpha_0 = \Big(2^{k-1} - \frac{1}{2} - \frac{1}{4\ln 2}\Big)\ln 2 + \mathsf{err}.$$

We remark that the asymptotic expansion of α_{sat} matches the previously mentioned result (2.1.1) from [DSS16]. The asymptotic expansion of α_{cond} matches an earlier result of [CZ12], which was obtained for a slightly different but closely related model.

2.1.6 Proof approach

Since $\mathsf{f} = \mathsf{f}(\alpha)$ is *a priori* not well-defined, the statement $\mathsf{f} \leqslant \mathsf{g}$ means formally that for all $\epsilon > 0$,

$$\lim_{n\to\infty} \mathbb{P}(Z^{1/n} \geqslant \mathsf{g} + \epsilon) = 0.$$

With this notation in mind, we will prove separately the upper bound $\mathsf{f}(\alpha) \leqslant \mathsf{f}^{\text{1RSB}}(\alpha)$ and the matching lower bound $\mathsf{f}(\alpha) \geqslant \mathsf{f}^{\text{1RSB}}(\alpha)$. This implies the main result Theorem 1: the free energy $\mathsf{f}(\alpha)$ is indeed well-defined, and equals $\mathsf{f}^{\text{1RSB}}(\alpha)$.

The upper bound is proved in Section 2.8 by an interpolation argument. This builds on similar bounds for spin glasses on Erdős–Rényi graphs [FL03; PT04], together with ideas from [BGT13] for interpolation in random regular models. Write $Z_n(\beta)$ for the partition function of NAE-SAT at inverse temperature $\beta > 0$. The interpolation method yields an upper bound on $\mathbb{E}\ln Z_n(\beta)$ which is expressed as the infimum of a certain function $\mathcal{P}(\mu;\beta)$, with μ ranging over probability measures on $[0,1]$. We then choose μ according to Proposition 2.1.2, and take $\beta \to \infty$ to obtain the desired bound $\mathsf{f}(\alpha) \leqslant \mathsf{f}^{\text{1RSB}}(\alpha)$.

Most of the paper is devoted to establishing the matching lower bound. The proof is inspired by the physics picture described above, and at a high level proceeds as follows. Take any λ for which the (predicted) value of $\Sigma(s_\lambda)$ is non-negative, and let $\boldsymbol{Y}_\lambda$ be the number of clusters of size $\doteq \exp\{ns_\lambda\}$. The informal statement of what we show is that

$$\boldsymbol{Y}_\lambda \doteq \exp\{n[\lambda s_\lambda + \Sigma(s_\lambda)]\}. \tag{2.1.12}$$

Adjusting λ as indicated by (2.1.11) then proves the desired bound $\mathsf{f}(\alpha) \geqslant \mathsf{f}^{\text{1RSB}}(\alpha)$.

Proving a formalized version of (2.1.12) occupies a significant part of the present paper. We introduce a slightly modified version of the messages $\mathtt{m}$ which record the topologies of the free trees $\boldsymbol{T}$. We then restrict to free trees with fewer than T variables, which limits the distance that information can propagate between free variables. We prove a version of (2.1.12) for every fixed T, and show that this yields the sharp lower bound in the limit $T \to \infty$. The proof of (2.1.12) for fixed T is via the moment method for the auxiliary model, which boils down to a complicated optimization problem over many dimensions. It is known (see e.g. [DSS16, Lem. 3.6]) that stationary points of the optimization problem correspond to "generalized" BP fixed points — these are measures $Q_{v\to a}(\mathtt{m}_{v\to a}, \mathtt{m}_{a\to v})$, rather than the simpler "one-sided" measures $q_{v\to a}(\mathtt{m}_{v\to a})$ considered in the 1RSB heuristic.

The one-sided property is a crucial simplification, but is challenging to prove in general. One contribution of this work that we wish to highlight is a novel resampling argument which yields a reduction to one-sided messages, and allows us to solve the moment optimization problem. (We are helped here by the truncation on the sizes of free trees.) Furthermore, the approach allows us to bring in methods from large deviations theory. With these we can show that the objective function has negative-definite Hessian at the optimizer, which is necessary for the second moment method. This resampling approach is quite general and should apply in a broad range of models.

2.1.7 Open problems

Beyond the free energy, it remains a challenge to establish the full picture predicted by statistical physicists for $\alpha \leqslant \alpha_{\text{sat}}$. Several recent works targeted at a broad class of models in the regime $\alpha \leqslant \alpha_{\text{cond}}$ [BCO16; CPS15; CP16b]. In the condensation regime $(\alpha_{\text{cond}}, \alpha_{\text{sat}})$, an initial step would be to show that most solutions lie within a bounded number of clusters. A much more refined prediction is that the mass distribution among the largest clusters forms a Poisson–Dirichlet process. Another question is to show that on a typical problem instance over n variables, if $\underline{\boldsymbol{x}}^1, \underline{\boldsymbol{x}}^2$ are sampled independently and uniformly at random from the solutions of that instance, then the normalized overlap $R_{1,2} \equiv n^{-1}\{v : \boldsymbol{x}^1_v = \boldsymbol{x}^2_v\}$ concentrates on two values (corresponding roughly to the two cases that $\underline{\boldsymbol{x}}^1, \underline{\boldsymbol{x}}^2$ come from the same cluster, or from different clusters). This criterion is sometimes taken as the precise definition of 1RSB, and so would be interesting to prove for models in the condensation regime.

Beyond the immediate context of random CSPs, understanding the condensation transition may deepen our understanding of the stochastic block model, a model for random networks with underlying community structure. Here again ideas from statistical physics have played an important role [Dec+11]. A great deal is now known rigorously for the case of two blocks [Mas14; MNS15], where there is no condensation regime. For models with more than two blocks, however, it is predicted that the condensation can occur, and may define a regime where detection is information-theoretically possible but computationally intractable. Part of this conjecture is verified in [CO+16].

2.2 Combinatorial model

Here we give the formal definition of the model. A *not-all-equal*-SAT (NAE-SAT) problem instance is naturally encoded by a bipartite graph $\mathscr{G}$, as follows. The vertex set of $\mathscr{G}$ is divided into a set $V = \{v_1, \ldots, v_n\}$ of variables and a set $F = \{a_1, \ldots, a_m\}$ of clauses. All vertices are labelled, and the edge set E joins variables to clauses. For each $e \in E$ we let $v(e)$ denote the incident variable, and $a(e)$ the incident clause. The edge e comes with a literal

$\mathtt{L}_e \in \{\mathtt{0}, \mathtt{1}\}$, indicating that $v(e)$ participates affirmatively ($\mathtt{L}_e = \mathtt{0}$) or negatively ($\mathtt{L}_e = \mathtt{1}$) in $a(e)$. We permit $\mathscr{G}$ to have multi-edges; in particular it is possible that a is joined to v by two edges $e', e'' \in E$, whose literals may or may not agree. We assume the graph is (d,k)-regular: each variable has d incident edges, and each clause has k incident edges, so $|E| = nd = mk$. Formally, we regard the edge set E as a permutation $\mathfrak{m}$ of $[nd]$, as follows. The i-th variable v_i has d incident half-edges, labelled

$$\dot{e}_{d(i-1)+1}, \ldots, \dot{e}_{di}.$$

The i-th clause a_i has k incident half-edges, labelled

$$\hat{e}_{k(i-1)+1}, \ldots, \hat{e}_{ki}.$$

An edge then consists of a pair of half-edges $(\dot{e}, \hat{e})$, and we take $E = \{(\dot{e}_i, \dot{e}_{\mathfrak{m}(i)}) : i \in [nd]\}$. For $v \in V$ we write δv for the ordered d-tuple of edges incident to v:

$$\delta v_i = ((\dot{e}_{d(i-1)+1}, \hat{e}_{\mathfrak{m}(d(i-1)+1)}), \ldots, (\dot{e}_{di}, \hat{e}_{\mathfrak{m}(di)})).$$

For $a \in F$ we write δa for the ordered k-tuple of edges incident to a:

$$\delta a_i = ((\dot{e}_{\mathfrak{m}^{-1}(k(i-1)+1)}, \hat{e}_{k(i-1)+1}), \ldots, (\dot{e}_{\mathfrak{m}^{-1}(ki)}, \hat{e}_{ki})).$$

Throughout this paper we denote $\mathscr{G} = (V, F, E)$ where it is understood that E corresponds to a permutation $\mathfrak{m}$ of $[nd]$, and includes the literals $\underline{\mathtt{L}}$. We also write

$$\mathscr{G} \equiv (G, \underline{\mathtt{L}}) \tag{2.2.1}$$

where G denotes the graph forgetting the edge labels $\underline{\mathtt{L}}$. We define all edges to have length $\frac{1}{2}$, so two variables $v \neq v'$ lie at unit distance if and only if they appear in the same clause.

Definition 2.2.1. An NAE-SAT solution for $\mathscr{G} = (V, F, E)$ is any $\underline{\boldsymbol{x}} \in \{\mathtt{0}, \mathtt{1}\}^V$ such that

$$\text{for all } a \in F,\ (\mathtt{L}_e \oplus \boldsymbol{x}_{v(e)})_{e \in \delta a} \text{ is neither identically } \mathtt{0} \text{ nor identically } \mathtt{1}.$$

Let $\mathsf{SOL}(\mathscr{G}) \subseteq \{\mathtt{0}, \mathtt{1}\}^V$ denote the set of all NAE-SAT solutions of $\mathscr{G}$, and define a graph on $\mathsf{SOL}(\mathscr{G})$ by connecting any pair of solutions at Hamming distance one. The connected components of this graph are the *clusters* of NAE-SAT solutions.

2.2.1 Frozen and warning configurations

We begin by reviewing two standard encodings (see [Par02; BMZ05; MMW07; MM09; DSS16]) of NAE-SAT solution clusters, via frozen configurations and warning configurations.

Definition 2.2.2. On $\mathscr{G} = (V, F, E)$, we say that $\underline{x} \in \{\mathtt{0}, \mathtt{1}, \mathtt{f}\}^V$ is a valid *frozen configuration* if (with the convention $\mathtt{1} \oplus \mathtt{f} = \mathtt{0} \oplus \mathtt{f} = \mathtt{f}$)

1. For all $a \in F$, $(\mathtt{L}_e \oplus x_{v(e)})_{e\in\delta a}$ is neither identically $\mathtt{0}$ nor identically $\mathtt{1}$; and

2. For all $v \in V$, $x_v \in \{\mathtt{0},\mathtt{1}\}$ if and only if there exists some $e \in \delta v$ such that

$$(\mathtt{L}_{e'} \oplus x_{v(e')})_{e'\in\delta a(e)\setminus e} \text{ is identically equal to } \mathtt{L}_e \oplus x_v \oplus \mathtt{1}. \tag{2.2.2}$$

If no such $e \in \delta v$ exists then $x_v = \mathtt{f}$.

It is well known that on any given problem instance $\mathscr{G} = (V, F, E)$, every NAE-SAT solution $\underline{\boldsymbol{x}}$ can be mapped to a frozen configuration $\underline{x} = \underline{x}(\underline{\boldsymbol{x}})$ via a "coarsening" or "whitening" procedure [Par02], as follows. Start by setting $\underline{x} = \underline{\boldsymbol{x}}$. Then, whenever $x_v \in \{\mathtt{0},\mathtt{1}\}$ but there exists no $e \in \delta v$ such that (2.2.2) holds, update x_v to $\mathtt{f}$. Iterate until no further updates can be made; the result is then a valid frozen configuration. Two NAE-SAT solutions $\underline{\boldsymbol{x}}$, $\underline{\boldsymbol{x}}'$ map to the same frozen configuration $\underline{x}$ if and only if they lie in the same cluster (Definition 2.2.1).

We say that an NAE-SAT solution $\underline{\boldsymbol{x}}$ *extends* a frozen configuration $\underline{x}$ if $\boldsymbol{x}_v = x_v$ whenever $x_v \in \{\mathtt{0},\mathtt{1}\}$. Let $\mathsf{size}(\underline{x})$ count the number of such extensions. The purpose of this section is to define (under a certain restriction) an alternative combinatorial representation $\underline{\sigma}$ of $\underline{x}$ — which we call a *coloring* — from which $\mathsf{size}(\underline{x})$ can be easily calculated. We will explain the correspondence between $\underline{x}$ and $\underline{\sigma}$ in a few stages:

$$\begin{aligned} &\text{frozen configurations } \underline{x} \\ &\leftrightarrow \text{warning configurations } \underline{y} \\ &\leftrightarrow \text{message configurations } \underline{\tau} \\ &\leftrightarrow \text{colorings } \underline{\sigma}. \end{aligned} \tag{2.2.3}$$

The first step $\underline{x} \leftrightarrow \underline{y}$ is quite standard: $\underline{y}$ takes values in M^E where $M = \{\mathtt{0},\mathtt{1},\mathtt{f}\}^2$. Each $e \in E$ has a pair of warnings $y_e \equiv (\dot{y}_e, \hat{y}_e)$ where $\dot{y}_e$ represents the variable-to-clause warning along e, and $\hat{y}_e$ represents the clause-to-variable warning along e. The warnings must satisfy some local equations, as follows:

Definition 2.2.3. On $\mathscr{G} = (V, F, E)$, $\underline{y} \in M^E$ is a valid *warning configuration* if for all $e \in E$,

$$\begin{aligned} \dot{y}_e &= \dot{\mathtt{Y}}((\hat{y}_{e'})_{e'\in\delta v(e)\setminus e}) \text{ and} \\ \hat{y}_e &= \mathtt{L}_e \oplus \hat{\mathtt{Y}}((\mathtt{L}_{e'} \oplus \dot{y}_{e'})_{e'\in\delta a(e)\setminus e}) \end{aligned}$$

where $\dot{\mathtt{Y}} : \{\mathtt{0},\mathtt{1},\mathtt{f}\}^{d-1} \to \{\mathtt{0},\mathtt{1},\mathtt{f},\varnothing\}$ and $\hat{\mathtt{Y}} : \{\mathtt{0},\mathtt{1},\mathtt{f}\}^{k-1} \to \{\mathtt{0},\mathtt{1},\mathtt{f}\}$ are defined by

$$\dot{\mathtt{Y}}(\underline{\hat{y}}) = \begin{cases} \mathtt{0} & \mathtt{0} \in \{\hat{y}_i\} \subseteq \{\mathtt{0},\mathtt{f}\}; \\ \mathtt{1} & \mathtt{1} \in \{\hat{y}_i\} \subseteq \{\mathtt{1},\mathtt{f}\}; \\ \mathtt{f} & \{\hat{y}_i\} = \mathtt{f}; \\ \varnothing & \text{otherwise.} \end{cases} \qquad \hat{\mathtt{Y}}(\underline{\dot{y}}) = \begin{cases} \mathtt{0} & \{\dot{y}_i\} = \{\mathtt{1}\}; \\ \mathtt{1} & \{\dot{y}_i\} = \{\mathtt{0}\}; \\ \mathtt{f} & \text{otherwise.} \end{cases}$$

(For $\underline{y}$ to be valid, we require that no edge e has $\dot{y}_e = \varnothing$.)

It is well known that there is a bijection

$$\left\{\begin{array}{c}\text{frozen configurations}\\ \underline{x}\in\{\mathtt{0},\mathtt{1},\mathtt{f}\}^V\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{warning configurations}\\ \underline{y}\in M^E\end{array}\right\}.$$

The mapping from $\underline{x}$ to $\underline{y}$ is as follows: for any v and any $e\in\delta v$ such that (2.2.2) holds, set $\hat{y}_e = x_v \in \{\mathtt{0},\mathtt{1}\}$. In all other cases set $\hat{y}_e = \mathtt{f}$. If any entry of $(\hat{y}_{e'})_{e'\in\delta v(e)\setminus e}$ is not $\mathtt{f}$, then it must equal $x_{v(e)}$, and in this case set $\dot{y}_e = x_{v(e)}$. Otherwise, set $\dot{y}_e = \mathtt{f}$.

2.2.2 Message configurations

We shall now restrict consideration to frozen configurations without "free cycles" (defined below), and decompose $\mathtt{f}$ into a more refined set of "messages."

Definition 2.2.4. Let $\underline{x}\in\{\mathtt{0},\mathtt{1},\mathtt{f}\}^V$ be a valid frozen configuration on $\mathscr{G}=(V,F,E)$. We say that a clause $a\in F$ is *separating* (with respect to $\underline{x}$) if there exist $e',e''\in\delta a$ such that

$$\mathtt{L}_{e'}\oplus x_{v(e')} = \mathtt{L}_{e''}\oplus x_{v(e'')}\oplus 1 \neq \mathtt{f}.$$

In particular, a forcing clause is also separating. A cycle is a sequence of edges

$$e_1 e_2 \ldots e_{2\ell-1} e_{2\ell} e_1,$$

where, taking indices modulo 2ℓ, it holds for each integer i that e_{2i-1} and e_{2i} are distinct but share a clause, while e_{2i} and e_{2i+1} are distinct but share a variable. (In particular, if v is joined to a by two edges $e'\neq e''$, then $e'e''$ forms a cycle.) We say the cycle is *free* if all its variables are free and all its clauses are non-separating.

Definition 2.2.5. Let $\underline{x}$ be a frozen configuration on $\mathscr{G}=(V,F,E)$. Let H be the subgraph of $\mathscr{G}$ induced by the free variables and non-separating clauses of $\underline{x}$. If $\underline{x}$ has no free cycles, then H is a disjoint union of tree components $\boldsymbol{t}$, which we term the *free trees* of $\underline{x}$. For each $\boldsymbol{t}$, let $\boldsymbol{T}$ be the subgraph of $\mathscr{G}$ induced by the depth-one neighborhood of $\boldsymbol{t}$, which may contain cycles. The subgraphs $\boldsymbol{T}$ will be termed the *free pieces* of $\underline{x}$. Each free variable is covered by exactly one free piece. In the simplest case, a free piece consists of a single free variable surrounded by d separating clauses.

In the message configuration $\underline{\tau}\in\mathscr{M}^E$, each edge $e\in E$ has a pair of messages $\tau_e\equiv(\dot{\tau}_e,\hat{\tau}_e)$, where each message is a rooted tree. To motivate the formal definition, consider the situation that e belongs to a free piece $\boldsymbol{T}$ which is a tree. We define one-sided versions $\dot{\boldsymbol{T}}_e$ and $\hat{\boldsymbol{T}}_e$: delete from $\boldsymbol{T}$ the edges $\delta a(e)\setminus e$, and let $\dot{\boldsymbol{T}}_e$ denote the component containing e in what remains. Likewise, delete from $\boldsymbol{T}$ the edges $\delta v(e)\setminus e$, and let $\hat{\boldsymbol{T}}_e$ denote the component containing e in what remains. We regard $\dot{\boldsymbol{T}}_e$ and $\hat{\boldsymbol{T}}_e$ as being rooted at $a(e)$ and $v(e)$ respectively. Informally, $\dot{\tau}_e$ encodes the isomorphism class of $\dot{\boldsymbol{T}}_e$ while $\hat{\tau}_e$ encodes the isomorphism class of $\hat{\boldsymbol{T}}_e$. However the situation is more subtle if the edge has warning $\mathtt{f}$ in one direction but $\mathtt{0}/\mathtt{1}$ in the reverse direction; minor complications also arise relating to the edge literals and the presence of cycles. We now make a formal definition which takes these issues into account.

It will be convenient to let $\mathtt{E}$ indicate a directed edge, pointing from tail vertex $t(\mathtt{E})$ to head vertex $h(\mathtt{E})$. If e is the undirected version of $\mathtt{E}$, then we let

$$(y_{\mathtt{E}}, \tau_{\mathtt{E}}) = \begin{cases} (\dot{y}_e, \dot{\tau}_e) & \text{if } t(\mathtt{E}) \text{ is a variable;} \\ (\hat{y}_e, \hat{\tau}_e) & \text{if } t(\mathtt{E}) \text{ is a clause.} \end{cases}$$

We will make a definition such that either $\tau_{\mathtt{E}}$ is a bipartite factor tree, or $\tau_{\mathtt{E}} = \star$. The tree is *unlabelled* except that one vertex is distinguished as the root, and some edges are assigned $\mathtt{0}$ or $\mathtt{1}$ values as explained below. The root vertex of the tree is required to have degree one, and should be thought of as corresponding to $h(\mathtt{E})$.

In the context of message configurations $\underline{\tau}$, we use "$\mathtt{0}$" or "$\mathtt{1}$" to stand for the tree consisting of a single edge which is labelled $\mathtt{0}$ or $\mathtt{1}$ and rooted at one of its endpoints — the root is the incident clause in the case of $\dot{\tau}$, the incident variable in the case of $\hat{\tau}$. We use $\square$ to stand for the tree consisting of a single unlabelled edge, rooted at the incident variable. Given a collection of rooted trees $t_1, \ldots, t_\ell$ whose roots $o_1, \ldots, o_\ell$ are all of the same type (either all variable or all clauses), we define $t = \mathsf{join}(t_1, \ldots, t_\ell)$ by identifying all the o_i as a single vertex o, then adding an edge which joins o to a new vertex o'. The vertex o has the same type as the o_i, and o' is given the opposite type, so the resulting tree t is a bipartite factor graph rooted at a vertex of degree one. Let $\dot{\mathscr{M}}$ and $\hat{\mathscr{M}}$ denote the possible values of $\dot{\tau}_e$ and $\hat{\tau}_e$ respectively. Write

$$\dot{\Omega}_{\mathtt{f}} \equiv \dot{\mathscr{M}} \backslash \{\mathtt{0}, \mathtt{1}, \star\}, \quad \hat{\Omega}_{\mathtt{f}} \equiv \hat{\mathscr{M}} \backslash \{\mathtt{0}, \mathtt{1}, \star\}.$$

In particular, $\square \in \hat{\Omega}_{\mathtt{f}}$. We will see below what other elements belong to $\dot{\Omega}_{\mathtt{f}}$ and $\hat{\Omega}_{\mathtt{f}}$.

Definition 2.2.6. On $\mathscr{G} = (V, F, E)$, $\underline{\tau} \in \mathscr{M}^E$ is a valid *message configuration* if for all $e \in E$,

$$\begin{aligned} \dot{\tau}_e &= \dot{\mathtt{T}}\big((\hat{\tau}_{e'})_{e' \in \delta v(e) \backslash e}\big) \text{ and} \\ \hat{\tau}_e &= \mathsf{L}_e \oplus \hat{\mathtt{T}}\big((\mathsf{L}_{e'} \oplus \dot{\tau}_{e'})_{e' \in \delta a(e) \backslash e}\big) \end{aligned}$$

where $\dot{\mathtt{T}} : \hat{\mathscr{M}}^{d-1} \to \dot{\mathscr{M}}$ and $\hat{\mathtt{T}} : \dot{\mathscr{M}}^{k-1} \to \hat{\mathscr{M}}$ are defined by

$$\dot{\mathtt{T}}(\underline{\hat{\tau}}) = \begin{cases} \mathtt{0} & \mathtt{0} \in \{\hat{\tau}_i\} \subseteq \dot{\mathscr{M}} \backslash \{\mathtt{1}\}; \\ \mathtt{1} & \mathtt{1} \in \{\hat{\tau}_i\} \subseteq \dot{\mathscr{M}} \backslash \{\mathtt{0}\}; \\ \mathsf{join}\{\hat{\tau}_i\} & \{\hat{\tau}_i\} \subseteq \hat{\Omega}_{\mathtt{f}}; \\ \star & \star \in \{\hat{\tau}_i\} \subseteq \{\star\} \cup \hat{\Omega}_{\mathtt{f}}; \\ \varnothing & \text{otherwise;} \end{cases} \qquad \hat{\mathtt{T}}(\underline{\dot{\tau}}) = \begin{cases} \mathtt{0} & \{\dot{\tau}_i\} = \{\mathtt{1}\}; \\ \mathtt{1} & \{\dot{\tau}_i\} = \{\mathtt{0}\}; \\ \square & \{\mathtt{0}, \mathtt{1}\} \subseteq \{\dot{\tau}_i\}; \\ \mathsf{join}\{\dot{\tau}_i\} & \{\mathtt{0}\} \neq \{\dot{\tau}_i\} \subseteq \{\mathtt{0}\} \cup \dot{\Omega}_{\mathtt{f}} \\ & \text{or } \{\mathtt{1}\} \neq \{\dot{\tau}_i\} \subseteq \{\mathtt{1}\} \cup \dot{\Omega}_{\mathtt{f}}; \\ \star & \text{otherwise.} \end{cases}$$

For $\underline{\tau}$ to be valid, we require for all $e \in E$ that $\dot{\tau}_e \neq \varnothing$, and further if one of $\dot{\tau}_e, \hat{\tau}_e$ equals $\star$ then the other must be in $\{\mathtt{0}, \mathtt{1}\}$.

Given a frozen configuration $\underline{x}$ we define the message configuration $\underline{\tau}$ in a recursive manner. If $y_{\mathtt{E}} \in \{\mathtt{0},\mathtt{1}\}$ then set $\tau_{\mathtt{E}} = y_{\mathtt{E}}$. If

$$\{\mathtt{0},\mathtt{1}\} \subseteq \{\mathtt{L}_{e'} \oplus \dot{y}_{e'}\}_{e'\in\delta a(e)\backslash e}$$

then set $\hat{\tau}_e = \square$. Let $\mathtt{F}$ denote the reversal of $\mathtt{E}$, and let $\delta\mathtt{E}$ denote the set of directed edges $\mathtt{E}'$ pointing towards $t(\mathtt{E})$ (including $\mathtt{F}$). Then, whenever $\tau_{\mathtt{E}}$ is undefined but $\tau_{\mathtt{E}'}$ is defined for all $\mathtt{E}' \in \delta\mathtt{E}\backslash\mathtt{F}$, set

$$\tau_{\mathtt{E}} \equiv \begin{cases} \dot{\mathtt{T}}((\hat{\tau}_{e'})_{e'\in\delta v(e)\backslash e}) & \text{if } t(\mathtt{E}) \text{ is a variable;} \\ \mathtt{L}_e \oplus \hat{\mathtt{T}}((\mathtt{L}_{e'} \oplus \dot{\tau}_{e'})_{e'\in\delta a(e)\backslash e}) & \text{if } t(\mathtt{E}) \text{ is a clause;} \end{cases}$$

Repeat until no further updates are possible. At the end of this procedure, if any $\tau_{\mathtt{E}}$ remains undefined then set it to $\star$.

Lemma 2.2.7. *Let $\underline{x} \in \{\mathtt{0},\mathtt{1},\mathtt{f}\}^V$ be a valid frozen configuration on $\mathscr{G} = (V,F,E)$ which has no free cycles. Then $\underline{x}$ maps under the above procedure to a valid message configuration $\underline{\tau}$.*

Proof. Suppose $\tau_{\mathtt{E}} = \star$, and let $\mathtt{F}$ denote the reversal of $\mathtt{E}$. From the above construction, it must be that $y_{\mathtt{E}} = \mathtt{f}$ and $\tau_{\mathtt{E}'} = \star$ for some $\mathtt{E}' \in \delta\mathtt{E}\backslash\mathtt{F}$. Consequently $\mathtt{E}$ must belong to a cycle of directed edges

$$\mathtt{E}_1\mathtt{E}_2\ldots\mathtt{E}_{2k}\mathtt{E}_1$$

with all the $\tau_{\mathtt{E}_i}$ equal to $\star$. Whenever $\mathtt{E}$ points from a separating clause a to free variable v, we must have $\tau_{\mathtt{E}} = \square$. As a result, if all the variables along the cycle are free, then none of the clauses can be separating, contradicting the assumption that $\underline{x}$ has no free cycles. Therefore some variable v on the cycle must take value $x_v \in \{\mathtt{0},\mathtt{1}\}$, and by relabelling we may assume $v = t(\mathtt{E}_1)$. Let $\mathtt{F}_i$ denote the reversal of $\mathtt{E}_i$: since $x_v \neq \mathtt{f}$ but $y_{\mathtt{E}_1} = \mathtt{f}$, it must be that $y_{\mathtt{F}_1} = x_v$. This means that the clause $a = h(\mathtt{E}_1) = t(\mathtt{F}_1)$ is forcing to v, so in particular $y_{\mathtt{F}_2} \in \{\mathtt{0},\mathtt{1}\}$. Continuing in this way we see that $y_{\mathtt{F}_i} \in \{\mathtt{0},\mathtt{1}\}$ for all i, and it follows that $\underline{\tau}$ is a valid message configuration. □

Lemma 2.2.8. *There is a bijection*

$$\left\{\begin{matrix}\textit{frozen configurations } \underline{x} \in \{\mathtt{0},\mathtt{1},\mathtt{f}\}^V \\ \textit{without free cycles}\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\textit{message configurations} \\ \underline{\tau} \in \mathscr{M}^E\end{matrix}\right\}.$$

Proof. Given $\underline{x}$, let $\underline{y}$ and $\underline{\tau}$ be the corresponding warning and message configurations. The mapping from $\underline{y}$ to $\underline{\tau}$ is clearly injective. Since $\underline{x} \leftrightarrow \underline{y}$, the mapping from $\underline{x}$ to $\underline{\tau}$ is also injective. To see that it is surjective, let $\underline{\tau}$ be any message configuration. Projecting $\{\star\} \cup \dot{\Omega}_{\mathtt{f}} \mapsto \mathtt{f}$ and $\{\star\} \cup \hat{\Omega}_{\mathtt{f}} \mapsto \mathtt{f}$ yields a valid warning configuration $\underline{y}$, which in turn maps to a valid frozen configuration $\underline{x}$. It remains then to check that $\underline{x}$ has no free cycles. Suppose for the sake of contradiction that there exists a cycle of directed edges

$$\mathtt{E}_1\mathtt{E}_2\ldots\mathtt{E}_{2k}\mathtt{E}_1$$

where all the variables are free and all the clauses are non-separating. Writing $\mathtt{F}_i$ for the reversal of $\mathtt{E}_i$, we see that all the messages $\tau_{\mathtt{E}_i}, \tau_{\mathtt{F}_i}$ must lie in $\{\star\} \cup \dot{\Omega}_{\mathtt{f}} \cup \hat{\Omega}_{\mathtt{f}}$. In fact, none of the messages can be $\star$, since in that case we require the message in the reverse direction to be in $\{\mathtt{0},\mathtt{1}\}$. Therefore all the messages are in $\dot{\Omega}_{\mathtt{f}} \cup \hat{\Omega}_{\mathtt{f}}$. By definition of $\dot{\mathtt{T}}$ and $\hat{\mathtt{T}}$, $\tau_{\mathtt{E}_i}$ must be a proper subtree of $\tau_{\mathtt{E}_{i+1}}$ for all i, with indices modulo $2k$. Going around the cycle we find that $\tau_{\mathtt{E}_1}$ is a proper subtree of $\tau_{\mathtt{E}_{2k+1}} = \tau_{\mathtt{E}_1}$, which gives the required contradiction. □

2.2.3 Bethe formula

The messages $\dot{\tau}_e, \hat{\tau}_e$ can be used to define probability measures $\dot{\boldsymbol{m}}_e, \hat{\boldsymbol{m}}_e$ on $\{\mathtt{0},\mathtt{1}\}$ where

$$\begin{aligned}&\dot{\boldsymbol{m}}_e \equiv \dot{\boldsymbol{m}}(\dot{\tau}_e) \text{ represents the law of } v(e) \text{ in absence of } a(e);\\ &\hat{\boldsymbol{m}}_e \equiv \hat{\boldsymbol{m}}(\hat{\tau}_e) \text{ represents the law of } v(e) \text{ in absence of } \delta v(e)\backslash e.\end{aligned}$$

If $\dot{\tau}_e \neq \star$, then there will be a normalizing constant $\dot{z}_e$ such that

$$\dot{\boldsymbol{m}}_e(x) = \frac{1}{\dot{z}_e} \prod_{e' \in \delta v(e)\backslash e} \hat{\boldsymbol{m}}_{e'}(x) \quad \text{ for } x \in \{\mathtt{0},\mathtt{1}\}.$$

Similarly, let $I^{\text{NAE}}(\underline{x})$ be the indicator that the entries of $\underline{x}$ are not all equal: if $\hat{\tau}_e \neq \star$ then there will be a normalizing constant $\hat{z}_e$ such that

$$\hat{\boldsymbol{m}}_e(x) = \frac{1}{\hat{z}_e} \sum_{\underline{x}_{\delta a(e)\backslash e}} I^{\text{NAE}}(x \oplus \mathtt{L}_e, (\underline{x} \oplus \mathtt{L})_{\delta a(e)\backslash e}) \prod_{e' \in \delta a(e)\backslash e} \dot{\boldsymbol{m}}(x_{e'}) \quad \text{ for } x \in \{\mathtt{0},\mathtt{1}\}.$$

In what follows we usually represent a probability measure on $\{\mathtt{0},\mathtt{1}\}$ by the probability assigned to $\mathtt{1}$, writing $\dot{m} \equiv \dot{\boldsymbol{m}}(\mathtt{1})$ and $\hat{m} \equiv \hat{\boldsymbol{m}}(\mathtt{1})$. Explicitly, $\dot{m}(\dot{\tau})$ and $\hat{m}(\hat{\tau})$ can be defined recursively, starting from the base cases

$$\dot{m}(\mathtt{1}) = \hat{m}(\mathtt{1}) = 1, \quad \dot{m}(\mathtt{0}) = \hat{m}(\mathtt{0}) = 0.$$

If $\dot{\tau} \in \dot{\Omega}_{\mathtt{f}}$ equals $\dot{\mathtt{T}}(\hat{\tau}_1, \ldots, \hat{\tau}_{d-1})$ where none of the $\hat{\tau}_i$ are $\star$, then set

$$\dot{m}(\dot{\tau}) = \frac{1}{\dot{z}(\dot{\tau})} \prod_{i=1}^{d-1} \hat{m}(\hat{\tau}_i), \quad \dot{z}(\dot{\tau}) = \prod_{i=1}^{d-1} \hat{m}(\hat{\tau}_i) + \prod_{i=1}^{d-1} (1 - \hat{m}(\hat{\tau}_i)), \tag{2.2.4}$$

where we note that $(\hat{\tau}_1, \ldots, \hat{\tau}_{d-1})$ can be recovered from $\dot{\tau}$ modulo permutation of the indices, so $\dot{z}(\dot{\tau})$ is well-defined. Similarly, if $\hat{\tau} \in \hat{\Omega}_{\mathtt{f}}$ equals $\hat{\mathtt{T}}(\dot{\tau}_1, \ldots, \dot{\tau}_{k-1})$ where none of the $\dot{\tau}_i$ are $\star$, then set

$$\hat{m}(\hat{\tau}) = \frac{1}{\hat{z}(\hat{\tau})} \left(1 - \prod_{i=1}^{k-1} \dot{m}(\dot{\tau}_i)\right), \quad \hat{z}(\hat{\tau}) = 2 - \prod_{i=1}^{k-1} \dot{m}(\dot{\tau}_i) - \prod_{i=1}^{k-1} (1 - \dot{m}(\dot{\tau}_i)). \tag{2.2.5}$$

Finally, we will see below that for our purposes we can take $\dot{m}(\star), \hat{m}(\star)$ to be any fixed values in $(0, 1)$. We arbitrarily set $\dot{m}(\star) = \frac{1}{2} = \hat{m}(\star)$.

Lemma 2.2.9. *Suppose on $\mathscr{G} = (V, F, E)$ that $\underline{\tau}$ is a valid message configuration, and let $\underline{x}$ be the corresponding frozen configuration (which has no free cycles). Suppose $\boldsymbol{T}$ is a free piece of $\underline{x}$, and let $\boldsymbol{t}$ be the free tree inside $\boldsymbol{T}$. Let $\mathsf{size}(\underline{x}; \boldsymbol{T})$ count the number of valid* NAE-SAT *assignments which extend $\underline{x}$ on $\boldsymbol{T}$. Then*

$$\mathsf{size}(\underline{x}; \boldsymbol{T}) = \prod_{v \in \boldsymbol{t} \cap V} \dot{\varphi}(\hat{\underline{\tau}}_{\boldsymbol{t} \cap \delta v}) \prod_{a \in \boldsymbol{t} \cap F} \hat{\varphi}^{\mathrm{lit}}((\dot{\underline{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}) \prod_{e \in \boldsymbol{t} \cap E} \bar{\varphi}(\tau_e) \tag{2.2.6}$$

where $\bar{\varphi}(\dot{\tau}, \hat{\tau}) \equiv [\dot{m}(\dot{\tau})\hat{m}(\hat{\tau}) + (1 - \dot{m}(\dot{\tau}))(1 - \hat{m}(\hat{\tau}))]^{-1}$,

$$\hat{\varphi}^{\mathrm{lit}}(\dot{\tau}_1, \ldots, \dot{\tau}_k) = 1 - \prod_{i=1}^{k} \dot{m}(\dot{\tau}_i) - \prod_{i=1}^{k}(1 - \dot{m}(\dot{\tau}_i)),$$

and for any $\ell \geqslant 0$ we define

$$\dot{\varphi}(\hat{\tau}_1, \ldots, \hat{\tau}_\ell) = \prod_{i=1}^{\ell} \hat{m}(\hat{\tau}_i) + \prod_{i=1}^{\ell}(1 - \hat{m}(\hat{\tau}_i)).$$

We take the convention that the empty product equals one, so if $\ell = 0$ then $\dot{\varphi} = 2$. The number of valid NAE-SAT *assignments extending $\underline{x}$ is given by*

$$\mathsf{size}(\underline{x}) = \prod_{\boldsymbol{T} \in \underline{x}} \mathsf{size}(\underline{x}; \boldsymbol{T}) \tag{2.2.7}$$

where the product is taken over all free pieces (Definition 2.2.5) $\boldsymbol{T}$ of $\underline{x}$.

Proof. The first claim (2.2.6) is a well-known calculation; see e.g. [MM09, Ch. 14]. The product formula (2.2.7) then follows from the fact that different free trees are disjoint. □

Corollary 2.2.10. *Suppose on $\mathscr{G} = (V, F, E)$ that $\underline{\tau}$ is a valid message configuration, and let $\underline{x}$ be the corresponding frozen configuration. Then*

$$\mathsf{size}(\underline{x}) = \prod_{v \in V} \dot{\varphi}(\hat{\underline{\tau}}_{\delta v}) \prod_{a \in F} \hat{\varphi}^{\mathrm{lit}}((\dot{\underline{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}) \prod_{e \in \boldsymbol{t} \cap E} \bar{\varphi}(\tau_e);$$

and this identity holds for any choices of $\dot{m}(\star), \hat{m}(\star) \in (0, 1)$.

Proof. Let V' denote the set of free variables, and F' the set of non-separating clauses. For each $v \in V'$ let $\boldsymbol{t}(v)$ denote the (unique) free tree containing v. Rearranging the product formula (2.2.7) gives

$$\mathsf{size}(\underline{x}) = \prod_{v \in V'} \left\{ \dot{\varphi}(\hat{\underline{\tau}}_{\boldsymbol{t}(v) \cap \delta v}) \prod_{e \in \boldsymbol{t}(v) \cap \delta v} \bar{\varphi}(\tau_e) \right\} \prod_{a \in F'} \hat{\varphi}^{\mathrm{lit}}((\dot{\underline{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}).$$

If e joins a free variable v to a separating clause a, then $\hat{m}(\hat{\tau}_e) = \frac{1}{2} = \bar{\varphi}(\tau_e)^{-1}$, so

$$\dot{\varphi}(\hat{\underline{\tau}}_{\boldsymbol{t}(v) \cap \delta v}) = \dot{\varphi}(\hat{\underline{\tau}}_{\delta v}) 2^{|\delta v \setminus \boldsymbol{t}|} = \dot{\varphi}(\hat{\underline{\tau}}_{\delta v}) \prod_{e \in \delta v \setminus \boldsymbol{t}(v)} \bar{\varphi}(\tau_e).$$

Substituting into the above proves that

$$\mathsf{size}(\underline{x}) = \prod_{v \in V'} \left\{ \dot{\varphi}(\underline{\hat{\tau}}_{\delta v}) \prod_{e \in \delta v} \bar{\varphi}(\tau_e) \right\} \prod_{a \in F'} \hat{\varphi}^{\text{lit}}((\underline{\dot{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}). \tag{2.2.8}$$

For $v \notin V'$ (meaning $x_v \in \{\mathtt{0}, \mathtt{1}\}$), partition δv into

$$\delta v(\mathtt{r}) = \{e \in \delta v : \hat{y}_e = x_v\}, \quad \delta v(\mathtt{b}) = \{e \in \delta v : \hat{y}_e = \mathtt{f}\}.$$

Say without loss that $x_v = \mathtt{1}$: since $\hat{m}(\hat{\tau}_e) = 1$ for all $e \in \delta v(\mathtt{r})$, we have

$$\dot{\varphi}(\underline{\hat{\tau}}_{\delta v}) = \prod_{e \in \delta v} \hat{m}(\hat{\tau}_e) + \prod_{e \in \delta v} (1 - \hat{m}(\hat{\tau}_e)) = \prod_{e \in \delta v(\mathtt{b})} \hat{m}(\hat{\tau}_e) = \prod_{e \in \delta v(\mathtt{b})} \bar{\varphi}(\tau_e)^{-1}. \tag{2.2.9}$$

Some of the messages $\hat{\tau}_e$ incoming to v may equal $\star$, but the above identity holds for any choice of $\hat{m}(\star) \in (0,1)$. Likewise, if a is a separating clause which is non-forcing, then some of the messages $\dot{\tau}_e$ incoming to a may equal $\star$, but

$$\hat{\varphi}^{\text{lit}}((\underline{\dot{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}) = 1 \tag{2.2.10}$$

for any choice of $\dot{m}(\star) \in (0,1)$. Finally, if a is forcing in the direction of edge e, then

$$\hat{\varphi}^{\text{lit}}((\underline{\dot{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}) = \bar{\varphi}(\tau_e)^{-1} = \begin{cases} \dot{m}(\dot{\tau}_e) & \text{if } x_{v(e)} = \mathtt{1}; \\ 1 - \dot{m}(\dot{\tau}_e) & \text{if } x_{v(e)} = \mathtt{0}; \end{cases} \tag{2.2.11}$$

including in the case that $\dot{\tau}_e = \star$. It follows from (2.2.9), (2.2.10), and (2.2.11) that

$$\prod_{v \in V \setminus V'} \left\{ \dot{\varphi}(\underline{\hat{\tau}}_v) \prod_{e \in \delta v} \bar{\varphi}(\tau_e) \right\} \prod_{a \in F \setminus F'} \hat{\varphi}^{\text{lit}}((\underline{\dot{\tau}} \oplus \underline{\mathtt{L}})_{\delta a}) = 1,$$

and multiplying with (2.2.8) proves the claim. □

2.2.4 Colorings

We now define the last step of (2.2.3). Recall $\underline{\tau} \in \mathscr{M}^E$, and let $\Omega_{\mathtt{f}} \subseteq \mathscr{M}$ denote the subset of values $\tau = (\dot{\tau}, \hat{\tau}) \in \mathscr{M}$ for which $\dot{\tau} \in \dot{\Omega}_{\mathtt{f}}$ and $\hat{\tau} \in \hat{\Omega}_{\mathtt{f}}$. Then the colorings will be configurations $\underline{\sigma} \in \Omega^E$ where

$$\Omega \equiv \{\mathtt{r}_0, \mathtt{r}_1, \mathtt{b}_0, \mathtt{b}_1\} \cup \Omega_{\mathtt{f}}.$$

We define a mapping $\mathsf{s} : \mathscr{M} \to \Omega$ by

$$\mathsf{s}(\tau) = \begin{cases} \mathtt{r}_0 & \hat{\tau} = \mathtt{0}; \\ \mathtt{r}_1 & \hat{\tau} = \mathtt{1}; \\ \mathtt{b}_0 & \hat{\tau} \neq \mathtt{0} \text{ and } \dot{\tau} = \mathtt{0}; \\ \mathtt{b}_1 & \hat{\tau} \neq \mathtt{1} \text{ and } \dot{\tau} = \mathtt{1}; \\ \tau & \text{otherwise.} \end{cases} \tag{2.2.12}$$

Note that if $\tau = (\dot\tau, \hat\tau)$ with $\dot\tau = \star$, then $\hat\tau$ must equal some $x \in \{\mathtt{0}, \mathtt{1}\}$, and so we set $\sigma(\tau) = \mathtt{r}_x$. Likewise if $\hat\tau = \star$ then $\dot\tau$ must equal some $x \in \{\mathtt{0}, \mathtt{1}\}$ and so we set $\sigma(\tau) = \mathtt{b}_x$. If $\sigma = \tau \in \Omega_{\mathtt{f}}$ we write $(\dot\sigma, \hat\sigma) \equiv (\dot\tau, \hat\tau)$; otherwise we write $(\dot\sigma, \hat\sigma) \equiv (\sigma, \sigma)$. We write $\dot\Omega, \hat\Omega$ for the possible values of $\dot\sigma, \hat\sigma$. The map $\mathtt{s}$ is not one-to-one, and we shall denote

$$\begin{aligned}
\dot\tau^{\mathrm{pos}}(\dot\sigma) &= \{\dot\tau \in \dot{\mathscr{M}} : (\dot\tau, \hat\tau) \in \mathtt{s}^{-1}(\dot\sigma, \hat\sigma) \text{ for some } \hat\tau \in \hat{\mathscr{M}}, \hat\sigma \in \hat\Omega\},\\
\hat\tau^{\mathrm{pos}}(\hat\sigma) &= \{\hat\tau \in \hat{\mathscr{M}} : (\dot\tau, \hat\tau) \in \mathtt{s}^{-1}(\dot\sigma, \hat\sigma) \text{ for some } \dot\tau \in \dot{\mathscr{M}}, \dot\sigma \in \dot\Omega\},\\
\dot\sigma^{\mathrm{pos}}(\dot\tau) &= \{\dot\sigma \in \dot\Omega : (\dot\sigma, \hat\sigma) = \mathtt{s}(\dot\tau, \hat\tau) \text{ for some } \hat\tau \in \hat{\mathscr{M}}, \hat\sigma \in \hat\Omega\},\\
\hat\sigma^{\mathrm{pos}}(\hat\tau) &= \{\hat\sigma \in \hat\Omega : (\dot\sigma, \hat\sigma) = \mathtt{s}(\dot\tau, \hat\tau) \text{ for some } \dot\tau \in \dot{\mathscr{M}}, \dot\sigma \in \dot\Omega\}.
\end{aligned}$$

The following definition is derived from Definition 2.2.6.

Definition 2.2.11. On $\mathscr{G} = (V, F, E)$, $\underline{\sigma} \in \Omega^E$ is a valid *coloring* if for all $e \in E$,

$$\begin{aligned}
\dot\sigma_e &\in \dot{\mathtt{S}}((\hat\sigma_{e'})_{e' \in \delta v(e) \setminus e}) \text{ and}\\
\hat\sigma_e &\in \mathtt{L}_e \oplus \hat{\mathtt{S}}((\mathtt{L}_{e'} \oplus \dot\sigma_{e'})_{e' \in \delta a(e) \setminus e})
\end{aligned}$$

where $\dot{\mathtt{S}} : \hat\Omega^{d-1} \to 2^{\dot\Omega}$ and $\hat{\mathtt{S}} : \dot\Omega^{k-1} \to 2^{\hat\Omega}$ are defined by

$$\begin{aligned}
\dot{\mathtt{S}}(\underline{\hat\sigma}) &= \dot\sigma^{\mathrm{pos}} \circ \dot{\mathtt{T}} \circ \hat\tau^{\mathrm{pos}}(\underline{\hat\sigma}) = \{\dot\sigma : \dot\sigma \in \dot\sigma^{\mathrm{pos}}(\dot{\mathtt{T}}(\underline{\hat\tau})) \text{ for any } \underline{\hat\tau} \text{ with } \hat\tau_i \in \hat\tau^{\mathrm{pos}}(\hat\sigma_i)\ \forall i\},\\
\hat{\mathtt{S}}(\underline{\dot\sigma}) &= \hat\sigma^{\mathrm{pos}} \circ \hat{\mathtt{T}} \circ \dot\tau^{\mathrm{pos}}(\underline{\dot\sigma}) = \{\hat\sigma : \hat\sigma \in \hat\sigma^{\mathrm{pos}}(\hat{\mathtt{T}}(\underline{\dot\tau})) \text{ for any } \underline{\dot\tau} \text{ with } \dot\tau_i \in \dot\tau^{\mathrm{pos}}(\dot\sigma_i)\ \forall i\}.
\end{aligned}$$

An equivalent characterization is that $\underline{\sigma}$ is a valid coloring if and only if

$$\prod_{v \in V} \dot I(\underline{\sigma}_{\delta v}) \prod_{a \in F} \hat I^{\mathrm{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a}) = 1 \tag{2.2.13}$$

where $\dot I : \Omega^d \to \{0,1\}$ and $\hat I^{\mathrm{lit}} : \Omega^k \to \{0,1\}$ are given by

$$\dot I(\underline{\sigma}) \equiv \prod_{i=1}^{d-1} \mathbf{1}\{\dot\sigma_i \in \dot{\mathtt{S}}((\hat\sigma_j)_{j \neq i})\}, \quad \hat I^{\mathrm{lit}}(\underline{\sigma}) \equiv \prod_{i=1}^{k-1} \mathbf{1}\{\hat\sigma_i \in \hat{\mathtt{S}}((\dot\sigma_j)_{j \neq i})\}.$$

This builds on a related encoding introduced by [CP16a]. More explicitly, we have

$$\dot I(\underline{\sigma}) = \begin{cases} 1 & \mathtt{r_0} \in \{\sigma_i\} \subseteq \{\mathtt{r_0}, \mathtt{b_0}\},\\ 1 & \mathtt{r_1} \in \{\sigma_i\} \subseteq \{\mathtt{r_1}, \mathtt{b_1}\},\\ 1 & \{\sigma_i\} \subseteq \Omega_{\mathtt{f}} \text{ and}\\ & \qquad \dot\sigma_i = \dot{\mathtt{T}}((\hat\sigma_j)_{j \neq i})\ \forall i,\\ 0 & \text{otherwise;} \end{cases} \qquad \hat I^{\mathrm{lit}}(\underline{\sigma}) = \begin{cases} 1 & \exists i : \sigma_i = \mathtt{r_0} \text{ and } \{\sigma_j\}_{j \neq i} = \{\mathtt{b_1}\},\\ 1 & \exists i : \sigma_i = \mathtt{r_1} \text{ and } \{\sigma_j\}_{j \neq i} = \{\mathtt{b_0}\},\\ 1 & \{\sigma_i\} \cap \{\mathtt{r_0}, \mathtt{r_1}\} = \varnothing,\\ & \qquad \nexists i : \{\sigma_j\}_{j \neq i} = \{\mathtt{b_0}\} \text{ or } \{\mathtt{b_1}\}, \text{ and}\\ & \qquad \hat\sigma_i \in \{\mathtt{b_0}, \mathtt{b_1}, \hat{\mathtt{T}}((\dot\tau^{\mathrm{pos}}(\dot\sigma_j))_{j \neq i})\}\ \forall i,\\ 0 & \text{otherwise.} \end{cases}$$

In the definition of $\hat I^{\mathrm{lit}}$, we note that if $\{\sigma_i\} \cap \{\mathtt{r_0}, \mathtt{r_1}\} = \varnothing$, then $\dot\tau^{\mathrm{pos}}(\dot\sigma_i)$ is a singleton for each i. If $\{\sigma_j\}_{j \neq i}$ is neither $\{\mathtt{b_0}\}$ nor $\{\mathtt{b_1}\}$, then we have $\hat{\mathtt{T}}((\dot\tau^{\mathrm{pos}}(\dot\sigma_j))_{j \neq i}) \in \hat\Omega_{\mathtt{f}}$.

One purpose of this encoding is to take advantage of some of the cancellations seen in the proof of Corollary 2.2.10. It follows easily from the definition that we have a bijection

$$\left\{\begin{array}{c}\text{message configurations}\\ \underline{\tau} \in \mathscr{M}^E\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{colorings}\\ \underline{\sigma} \in \Omega^E\end{array}\right\},$$

The following is a straightforward consequence of Lemma 2.2.9:

Lemma 2.2.12. *Suppose $\underline{\sigma}$ be a valid coloring on $\mathscr{G} = (V, F, E)$. Let $\underline{\tau}$ be the corresponding message configuration, and $\underline{x}$ the corresponding frozen configuration. Then $\mathsf{size}(\underline{x}) \equiv \mathsf{size}(\underline{\sigma})$ is given by the formula*

$$\mathsf{size}(\underline{\sigma}) = \boldsymbol{w}_{\mathscr{G}}^{\mathrm{lit}}(\underline{\sigma}) \equiv \prod_{v\in V} \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a\in F} \hat{\Phi}^{\mathrm{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a}) \prod_{e\in E} \bar{\Phi}(\sigma_e)$$

where Φ agrees with φ for v, a, e belonging to free trees, and is one otherwise. More precisely, $\dot{\Phi} : \Omega^d \to \mathbb{R}_{\geqslant 0}$ is given by

$$\dot{\Phi}(\underline{\sigma}) = \begin{cases} 0 & \dot{I}(\underline{\sigma}) = 0; \\ 1 & \dot{I}(\underline{\sigma}) = 1 \textit{ and } \{\sigma_i\} \textit{ contains } \mathtt{r}_0 \textit{ or } \mathtt{r}_1; \\ \dot{\varphi}(\hat{\underline{\tau}}) & \textit{otherwise, meaning } v \in V'; \end{cases}$$

note in the last case that each σ_i can be mapped to a unique $\hat{\tau}_i$, so the value of $\dot{\varphi}(\hat{\underline{\tau}})$ is well-defined. Similarly, $\hat{\Phi}^{\mathrm{lit}} : \Omega^k \to \mathbb{R}_{\geqslant 0}$ is given by

$$\hat{\Phi}^{\mathrm{lit}}(\underline{\sigma}) = \begin{cases} 0 & \hat{I}^{\mathrm{lit}}(\underline{\sigma}) = 0; \\ 1 & \hat{I}^{\mathrm{lit}}(\underline{\sigma}) = 1 \textit{ and } \{\sigma_i\} \textit{ contains } \mathtt{r}_0 \textit{ or } \mathtt{r}_1; \\ 1 & \hat{I}^{\mathrm{lit}}(\underline{\sigma}) = 1 \textit{ and } \{\mathtt{b}_0, \mathtt{b}_1\} \subseteq \{\sigma_i\}; \\ \hat{\varphi}^{\mathrm{lit}}(\dot{\underline{\tau}}) & \textit{otherwise, meaning } a \in F'; \end{cases}$$

note again in the last case that each σ_i can be mapped to a unique $\dot{\tau}_i$, so the value of $\hat{\varphi}^{\mathrm{lit}}(\dot{\underline{\tau}})$ is well-defined. Finally, $\bar{\Phi} : \Omega \to \mathbb{R}_{\geqslant 0}$ is given by

$$\bar{\Phi}(\sigma) = \begin{cases} 1 & \sigma \in \{\mathtt{r}_0, \mathtt{r}_1, \mathtt{b}_0, \mathtt{b}_1\}; \\ \bar{\varphi}(\sigma) & \textit{otherwise.} \end{cases}$$

Proof. This is essentially a rewriting of (2.2.8). □

According to the above definitions, if $\underline{\sigma}$ is not a valid coloring, then $\boldsymbol{w}_{\mathscr{G}}^{\mathrm{lit}}(\underline{\sigma}) \equiv 0$. For $\sigma \in \Omega$ let $|\sigma|$ count the number of free variables encoded by σ. Thus $|\sigma| = 0$ if and only if $\sigma \notin \Omega_{\mathtt{f}}$. On $\mathscr{G} = (V, F, E)$ we say that $\underline{\sigma}$ is a valid T-*coloring* if $|\sigma_e| \leqslant T$ for all $e \in E$. We write $\boldsymbol{I}_{\mathscr{G},T}(\underline{\sigma})$ for the indicator that $\underline{\sigma}$ is a valid T-coloring of $\mathscr{G}$, and let

$$\boldsymbol{w}_{\mathscr{G},T}^{\mathrm{lit}}(\underline{\sigma}) \equiv \boldsymbol{w}_{\mathscr{G}}^{\mathrm{lit}}(\underline{\sigma}) \boldsymbol{I}_{\mathscr{G},T}(\underline{\sigma}).$$

Recall from Lemma 2.2.12 the product formula for $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G}}(\underline{\sigma})$, and note that an analogous formula for $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ is obtained by simply replacing $\bar{\Phi}$ with the modified factor $\bar{\Phi}_T$, where

$$\bar{\Phi}_T(\sigma) \equiv \bar{\Phi}(\sigma)\mathbf{1}\{|\sigma| \leqslant T\}.$$

We then define $\boldsymbol{Z}_{\lambda,T}$ to be the partition function of λ-tilted T-colorings,

$$\boldsymbol{Z}_{\lambda,T} = \sum_{\underline{\sigma}\in\Omega^E} \boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})^{\lambda}. \tag{2.2.14}$$

Thus $\boldsymbol{Z}_{\lambda,T}$ is a function of the NAE-SAT problem instance $\mathscr{G} = (V,F,E)$. Clearly $\boldsymbol{Z}_{\lambda,T}$ is nondecreasing in T, and we write $\boldsymbol{Z}_{\lambda,\infty} \equiv \boldsymbol{Z}_{\lambda}$ for the sum over all valid colorings with no size truncation. The following gives the formal version of (2.1.3) which we will work with in the proof of the free energy lower bound.

Proposition 2.2.13. *On $\mathscr{G} = (V,F,E)$ let $\mathscr{C}(\mathscr{G})$ denote the collection of* NAE-SAT *clusters, so each $\boldsymbol{\gamma} \in \mathscr{C}(\mathscr{G})$ is a subset of $\{0,1\}^V$. Then, for all $0 \leqslant T \leqslant \infty$,*

$$\boldsymbol{Z}_{\lambda,T} \leqslant \sum_{\boldsymbol{\gamma}\in\mathscr{C}(\mathscr{G})} |\boldsymbol{\gamma}|^{\lambda}.$$

Proof. This is a direct consequence of Lemma 2.2.12. □

2.3 Proof outline

Having formally set up our combinatorial model encoding the clusters of NAE-SAT solutions (Proposition 2.2.13), we now proceed to outline the proof of Theorem 1. The basic approach will be to show concentration for $\boldsymbol{Z}_{\lambda,T}$ via the second moment method.

2.3.1 Averaging over edge literals

In the setting of NAE-SAT, we can take advantage of the following simplification:

Remark 2.3.1. For any function $g : \{0,1\}^t \to \mathbb{R}$, let $\mathbb{E}^{\mathrm{lit}} g$ denote the average value of $g(\underline{\mathtt{L}})$ over all $\underline{\mathtt{L}} \in \{0,1\}^t$. Recalling from (2.2.1) the notation $\mathscr{G} = (G, \underline{\mathtt{L}})$, if $\underline{\sigma}$ is any coloring of the edges of G, then the average of $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ over all $\underline{\mathtt{L}}$ is given by

$$\mathbb{E}^{\mathrm{lit}}[\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})^{\lambda}] = \boldsymbol{w}_{G,T}(\underline{\sigma})^{\lambda} \equiv \left\{ \prod_{v\in V} \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a\in F} \hat{\Phi}(\underline{\sigma}_{\delta a}) \prod_{e\in E} \bar{\Phi}_T(\sigma_e) \right\}^{\lambda}, \tag{2.3.1}$$

with $\hat{\Phi}(\underline{\sigma}) \equiv (\mathbb{E}^{\mathrm{lit}}[\hat{\Phi}(\underline{\sigma}\oplus\underline{\mathtt{L}})^{\lambda}])^{1/\lambda}$. A similar simplification holds in the second moment, where we consider pairs $\underline{\sigma} \equiv (\underline{\sigma}^1, \underline{\sigma}^2)$ with weights $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma}) \equiv \boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma}^1)\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma}^2)$:

$$\mathbb{E}^{\mathrm{lit}}[\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})^{\lambda}] = \boldsymbol{w}_{G,T}(\underline{\sigma})^{\lambda} \equiv \left\{ \prod_{v\in V} \dot{\Phi}_2(\underline{\sigma}_{\delta v}) \prod_{a\in F} \hat{\Phi}_2(\underline{\sigma}_{\delta a}) \prod_{e\in E} \bar{\Phi}_{T,2}(\sigma_e) \right\}^{\lambda} \tag{2.3.2}$$

where $\dot{\Phi}_2(\underline{\sigma}) \equiv \dot{\Phi}(\underline{\sigma}^1)\dot{\Phi}(\underline{\sigma}^2)$, $\bar{\Phi}_{T,2}(\sigma) \equiv \bar{\Phi}_T(\sigma^1)\bar{\Phi}_T(\sigma^2)$, and

$$\hat{\Phi}_2(\underline{\sigma}) = \Big(\mathbb{E}^{\mathrm{lit}}[\hat{\Phi}(\underline{\sigma}^1 \oplus \underline{\mathtt{L}})^\lambda \hat{\Phi}(\underline{\sigma}^2 \oplus \underline{\mathtt{L}})^\lambda]\Big)^{1/\lambda}.$$

Let us emphasize that $\hat{\Phi}$ and $\hat{\Phi}_2$ depend on λ, although we suppress it from the notation.

Clearly the weight $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ depends on $\underline{\mathtt{L}}$, since $\underline{\sigma}$ need not even be a valid coloring for all choices of $\underline{\mathtt{L}}$. However, the following lemma shows that, as long as $\underline{\sigma}$ remains valid, the size of its encoded cluster remains the same:

Lemma 2.3.2. *Given G, let $\boldsymbol{w}^{\max}_{G,T}(\underline{\sigma})$ denote the maximum of $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ over all $\mathscr{G} = (G, \underline{\mathtt{L}})$. For any $\mathscr{G} = (G, \underline{\mathtt{L}})$, $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ is either zero or equal to $\boldsymbol{w}^{\max}_{G,T}(\underline{\sigma})$.*

Proof. We claim that for all $\underline{\sigma}, \underline{\mathtt{L}}$ we have the factorization

$$\begin{aligned} \hat{\Phi}^{\mathrm{lit}}(\underline{\sigma} \oplus \underline{\mathtt{L}}) &= \hat{I}^{\mathrm{lit}}(\underline{\sigma} \oplus \underline{\mathtt{L}})\hat{\Phi}^{\max}(\underline{\sigma}), \text{ where} \\ \hat{\Phi}^{\max}(\underline{\sigma}) &\equiv \max\{\hat{\Phi}^{\mathrm{lit}}(\underline{\sigma} \oplus \underline{\mathtt{L}}) : \underline{\mathtt{L}} \in \{\mathtt{0},\mathtt{1}\}^k\}. \end{aligned}$$

To see this, note that for $\underline{\zeta} \in \Omega^{d-1}$ and $\underline{\xi} \in \Omega^{k-1}$, if $\dot{I}(\sigma, \underline{\zeta}) = 1$ and $\hat{I}^{\mathrm{lit}}(\sigma, \underline{\xi}) = 1$, then

$$\begin{aligned} \dot{\Phi}(\sigma, \underline{\zeta})\bar{\Phi}_T(\sigma) &= \dot{z}(\dot{\sigma}) \equiv \begin{cases} \dot{z}(\dot{\tau}) & \text{if } \dot{\sigma} = \dot{\tau}, \\ 1 & \text{otherwise;} \end{cases} \\ \hat{\Phi}^{\mathrm{lit}}(\sigma, \underline{\xi})\bar{\Phi}_T(\sigma) &= \hat{z}(\hat{\sigma}) \equiv \begin{cases} \hat{z}(\hat{\tau}) & \text{if } \hat{\sigma} = \hat{\tau}, \\ 1 & \text{otherwise.} \end{cases} \end{aligned} \tag{2.3.3}$$

In particular, since $\hat{z}(\hat{\sigma}) = \hat{z}(\hat{\sigma} \oplus \mathtt{1})$, we see that the claim holds with $\hat{\Phi}^{\max}(\underline{\sigma}) = \hat{z}(\hat{\sigma}_i)/\bar{\Phi}_T(\sigma_i)$ for any $1 \leqslant i \leqslant k$. The lemma then follows: either $\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})$ is zero, or it equals

$$\prod_v \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_a \hat{\Phi}^{\max}(\underline{\sigma}_{\delta a}) \prod_e \bar{\Phi}_T(\sigma_e) = \boldsymbol{w}^{\max}_{G,T}(\underline{\sigma}),$$

as claimed. ∎

Lemma 2.3.2 says that, in averaging over the literals, we do not lose any essential information on the cluster size. For $\underline{\sigma} \in \Omega^k$, let

$$\hat{v}(\underline{\sigma}) \equiv \mathbb{E}^{\mathrm{lit}}[\hat{I}^{\mathrm{lit}}(\underline{\sigma} \oplus \underline{\mathtt{L}})] \tag{2.3.4}$$

denote the fraction of $\underline{\mathtt{L}} \in \{\mathtt{0},\mathtt{1}\}^k$ which are compatible with $\underline{\sigma}$. Then Lemma 2.3.2 gives

$$\boldsymbol{w}_{G,T}(\underline{\sigma})^\lambda = \boldsymbol{w}^{\max}_{G,T}(\underline{\sigma})^\lambda \boldsymbol{p}_G(\underline{\sigma}), \quad \boldsymbol{p}_G(\underline{\sigma}) \equiv \prod_{a \in F} \hat{v}(\underline{\sigma}). \tag{2.3.5}$$

We will see below that, thanks to this simplification, we can extract the desired information from the averaged weights $\boldsymbol{w}_{G,T}(\underline{\sigma})$, without referring to the edge literals $\underline{\mathtt{L}}$.

Definition 2.3.3. On a bipartite factor graph G (without edge literals), the *factor model* with specification $g \equiv (\dot{g}, \hat{g}, \bar{g})$ is the probability measure ν_G on configurations $\underline{\xi} \in \mathscr{X}^E$ defined by

$$\nu_G(\underline{\xi}) = \frac{1}{Z} \prod_{v \in V} \dot{g}(\underline{\xi}_{\delta v}) \prod_{a \in F} \hat{g}(\underline{\xi}_{\delta a}) \prod_{e \in E} \bar{g}(\xi_e), \tag{2.3.6}$$

with Z the normalizing constant.

The measure (2.3.1) on T-colorings is a factor model with specification $(\dot{\Phi}, \hat{\Phi}, \bar{\Phi}_T)^\lambda$. The measure (2.3.2) on pairs of T-colorings is a factor model with specification $(\dot{\Phi}_2, \hat{\Phi}_2, \bar{\Phi}_{T,2})^\lambda$. To distinguish between the two cases, we sometimes refer to (2.3.1) as the "first-moment" or "single-copy" model, and refer to (2.3.2) as the "second-moment" or "pair" model. In much of what follows, we treat these two in a unified manner under the general framework (2.3.6).

2.3.2 Empirical measures and moments

We will decompose colorings $\underline{\sigma}$ according to their empirical measure H, defined as follows:

Definition 2.3.4. Given a coloring $\underline{\sigma}$ on $\mathscr{G} = (G, \underline{\mathtt{L}})$, let

$$\begin{aligned} \dot{H}(\underline{\zeta}) &= |\{v \in V : \underline{\sigma}_{\delta v} = \underline{\zeta}\}|/|V| \quad \text{for } \underline{\zeta} \in \Omega^d, \\ \hat{H}(\underline{\xi}) &= |\{a \in F : \underline{\sigma}_{\delta a} = \underline{\xi}\}|/|F| \quad \text{for } \underline{\xi} \in \Omega^k, \\ \bar{H}(\sigma) &= |\{e \in E : \sigma_e = \sigma\}|/|E| \quad \text{for } \sigma \in \Omega. \end{aligned}$$

Note that the validity of $\underline{\sigma}$ on $\mathscr{G}$ clearly depends on $\underline{\mathtt{L}}$, but we can regard H as a function of $(G, \underline{\sigma})$ only. We therefore write

$$H \equiv H(\mathscr{G}, \underline{\sigma}) \equiv H(G, \underline{\sigma}) \equiv (\dot{H}, \hat{H}, \bar{H}),$$

and we term this the *empirical measure* of $\underline{\sigma}$ on G.

If $\mathbf{H}$ is any subset of empirical measures H, we write $\underline{\sigma} \in \mathbf{H}$ to indicate that $H(G, \underline{\sigma}) \in \mathbf{H}$, and let $\boldsymbol{Z}_{\lambda,T}(\mathbf{H})$ denote the contribution to $\boldsymbol{Z}_{\lambda,T}$ from (valid) colorings $\underline{\sigma} \in \mathbf{H}$. If $\mathbf{H}$ is a singleton $\{H\}$, then we write $\underline{\sigma} \in H$ to indicate $H(G, \underline{\sigma}) = H$, and let $\boldsymbol{Z}_{\lambda,T}(H)$ denote the contribution from all colorings $\underline{\sigma} \in H$. Much of the paper concerns the calculation of first and second moments for $\boldsymbol{Z}_{\lambda,T}(H)$.

First note that for any pair $(G, \underline{\sigma})$ with $H(G, \underline{\sigma}) = H$, the weight $\boldsymbol{w}_{G,T}(\underline{\sigma})$ is the same and depends only on T, G, and H. In fact, the weight equals $\boldsymbol{w}_G(\underline{\sigma}) \equiv \boldsymbol{w}_{G,\infty}(\underline{\sigma})$ if the support of $\bar{H}$ is contained in Ω_T, and equals zero otherwise. From now on we assume $\bar{H}$ is supported within Ω_T, so $\boldsymbol{w}_{G,T}(\underline{\sigma}) = \boldsymbol{w}_G(\underline{\sigma})$ depends only on (G, H), and can be denoted $\boldsymbol{w}_G(H)$. Further, we see in (2.3.5) that, as long as $\operatorname{supp} \bar{H} \subseteq \Omega_T$, the weights $\boldsymbol{w}^{\max}_{G,T}(\underline{\sigma})$ and $\boldsymbol{p}_G(\underline{\sigma})$ also depend only on (G, H), so we can rewrite (2.3.5) as

$$\boldsymbol{w}_G(H)^\lambda = \boldsymbol{w}^{\max}_G(H)^\lambda \boldsymbol{p}(H). \tag{2.3.7}$$

In what follows, for ease of notation we will often suppress the dependence on λ and T, and write simply $\boldsymbol{Z} \equiv \boldsymbol{Z}_{\lambda,T}$.

In fact we have a quite explicit expression for $\mathbb{E}\boldsymbol{Z}(H)$, as follows. We will use the usual multi-index notations, in particular, if π is a probability measure on a space X, we write

$$\binom{n}{n\pi} \equiv n! \Big/ \prod_{x \in X} (n\pi(x))!.$$

It follows straightforwardly from the definition of the random regular NAE-SAT graph that

$$\mathbb{E}\boldsymbol{Z}(H) = \left\{ \binom{n}{n\dot{H}} \binom{m}{m\hat{H}} \Big/ \binom{nd}{nd\bar{H}} \right\} \boldsymbol{w}_G(H)^\lambda. \tag{2.3.8}$$

We write $\mathcal{H}(\pi) = -\langle \pi, \ln \pi \rangle$ for the Shannon entropy of π. Applying Stirling's formula gives the following:

Lemma 2.3.5. *For any fixed $H \equiv (\dot{H}, \hat{H}, \bar{H})$, we have in the limit of large n that*

$$\mathbb{E}\boldsymbol{Z}(H) \asymp n^{-\wp(H)/2} \exp\{n\boldsymbol{F}(H)\}$$

where for an empirical measure $H = (\dot{H}, \hat{H}, \bar{H})$ we define

$$\begin{aligned}
\boldsymbol{v}(H) &\equiv (d/k)\langle \ln \hat{v}, \hat{H} \rangle = n^{-1} \ln \boldsymbol{p}(H), \\
\boldsymbol{s}(H) &\equiv \langle \ln \dot{\Phi}, \dot{H} \rangle + (d/k)\langle \ln \hat{\Phi}^{\max}, \hat{H} \rangle + d\langle \ln \bar{\Phi}, \bar{H} \rangle = n^{-1} \ln \boldsymbol{w}^{\max}(H), \\
\boldsymbol{\Sigma}(H) &\equiv \mathcal{H}(\dot{H}) + (d/k)\mathcal{H}(\hat{H}) - d\mathcal{H}(\bar{H}) + \boldsymbol{v}(H), \\
\boldsymbol{F}(H) &\equiv \boldsymbol{\Sigma}(H) + \boldsymbol{s}(H)\lambda, \\
\wp(H) &\equiv |\operatorname{supp} \dot{H}| + |\operatorname{supp} \hat{H}| - |\operatorname{supp} \bar{H}| - 1.
\end{aligned} \tag{2.3.9}$$

2.3.3 Outline of first moment

The function $\boldsymbol{F}(H)$ is difficult to optimize directly, and we combine a few techniques in order to analyze it. In view of the result of [DSS16] (see Remark 2.1.1), we restrict consideration to the regime

$$(2^{k-1} - 2) \ln 2 \equiv \alpha_{\text{lbd}} \leqslant d \leqslant \alpha_{\text{ubd}} \equiv 2^{k-1} \ln 2. \tag{2.3.10}$$

In this regime, we use *a priori* estimates to show that the optimal H must lie in a certain restricted set $\mathbf{N}_\circ$. We then show that in the restricted set, a certain block optimization procedure converges to a unique, and explicit, optimizer $H_\star$. The convergence of the block optimization is based on a certain contraction estimate for the belief propagation recursion, which we describe below.

First, to describe the set $\mathbf{N}_\circ$, let us abbreviate $\bar{H}(\texttt{r})$ and $\bar{H}(\texttt{f})$ for the mass assigned by $\bar{H}$ to the sets $\{\texttt{r}\} \equiv \{\texttt{r}_0, \texttt{r}_1\}$ and $\{\texttt{f}\} \equiv \Omega_{\texttt{f}}$; and let $\mathbf{N}_\circ$ denote the set of H such that

$$\max\{\bar{H}(\texttt{f}), \bar{H}(\texttt{r})\} \leqslant 7/2^k. \tag{2.3.11}$$

The following *a priori* estimate shows that in the regime (2.3.10), the measures $H \notin \mathbf{N}_\circ$ give a negligible contribution to the first moment.

Lemma 2.3.6. *Let $\boldsymbol{Z}((\mathbf{N}_\circ)^c)$ be the contribution to $\boldsymbol{Z} = \boldsymbol{Z}_{\lambda,T}$ from empirical measures $H \notin \mathbf{N}_\circ$. For $k \geqslant k_0$, α satisfying (2.3.10), and $0 \leqslant \lambda \leqslant 1$, $\mathbb{E}\boldsymbol{Z}((\mathbf{N}_\circ)^c)$ is exponentially small in n.*

Proof. In view of Proposition 2.2.13, for $0 \leqslant \lambda \leqslant 1$ we have

$$\boldsymbol{Z}((\mathbf{N}_\circ)^c) \leqslant Z^{\texttt{free}} + Z^{\texttt{red}}$$

where $Z^{\texttt{free}}$ (resp. $Z^{\texttt{red}}$) counts NAE-SAT solutions $\underline{\boldsymbol{x}} \in \{\texttt{0},\texttt{1}\}^V$ which map — via coarsening and the bijection (2.2.3) — to warning configurations $\underline{y}$ with density of $\texttt{free}$ (resp. $\texttt{red}$) edges $\geqslant 7/2^k$. For α satisfying (2.3.10), $\mathbb{E}Z^{\texttt{f}}$ is exponentially small in n by [DSS16, Propn. 2.2]. As for $Z^{\texttt{red}}$, let us say that an edge $e \in E$ is *blocked* under $\underline{\boldsymbol{x}} \in \{\texttt{0},\texttt{1}\}^V$ if

$$\texttt{L}_e \oplus x_{v(e)} = \texttt{1} \oplus \texttt{L}_{e'} \oplus x_{v(e')} \quad \text{for all } e' \in \delta a(e) \backslash e.$$

Note that if $\underline{\boldsymbol{x}}$ maps to $\underline{y}$, the only possibility for $y_e \in \{\texttt{r}_0, \texttt{r}_1\}$ is that e was blocked under $\underline{\boldsymbol{x}}$. (The converse need not hold.) If we condition on $\underline{\boldsymbol{x}}$ being a valid NAE-SAT solution, then each clause contains a blocking edge independently with chance $\theta = 2k/(2^k - 2)$; note also that a clause can contain at most one blocking edge. It follows that

$$\mathbb{E}Z^{\texttt{red}} \leqslant (\mathbb{E}Z)\mathbb{P}\Big(\text{Bin}(m,\theta) \geqslant 7nd/2^k\Big),$$

which is exponentially small in n by a standard Chernoff bound, in combination with the trivial bound $\mathbb{E}Z \leqslant 2^n$. □

Lemma 2.3.6 tells us that $\max\{\boldsymbol{F}(H) : H \notin \mathbf{N}_\circ\}$ is negative. On the other hand, we shall assume that the global maximum of $\boldsymbol{F}$ is non-negative, since otherwise $\mathbb{E}\boldsymbol{Z}$ is exponentially small in n and there is nothing to prove. From this we conclude that any maximizer H of $\boldsymbol{F}$ must lie in $\mathbf{N}_\circ$. By a block optimization procedure in $\mathbf{N}_\circ$, we prove

Proposition 2.3.7 (*proved in Section 2.6*)**.** *Assuming the global maximum of $\boldsymbol{F}$ is non-negative, the unique maximizer of $\boldsymbol{F}$ is a point $H_\star$ in the interior of $\mathbf{N}_\circ$. Further, there is a positive constant $\epsilon = \epsilon(k,\lambda,T)$ so that for $\|H - H_\star\| \leqslant \epsilon$, $\boldsymbol{F}(H) \leqslant \boldsymbol{F}(H_\star) - \epsilon\|H - H_\star\|^2$. Explicitly,*

$$\dot{H}_\star(\zeta) = \frac{\dot{\Phi}(\zeta)^\lambda}{\dot{\mathfrak{Z}}_\star} \prod_{i=1}^d \hat{q}_\star(\dot{\zeta}_i), \quad \hat{H}_\star(\xi) = \frac{\hat{\Phi}(\xi)^\lambda}{\hat{\mathfrak{Z}}_\star} \prod_{i=1}^d \dot{q}_\star(\hat{\xi}_i), \quad \bar{H}_\star(\sigma) = \frac{\bar{\Phi}(\sigma)^{-\lambda}}{\bar{\mathfrak{Z}}_\star} \dot{q}_\star(\dot{\sigma})\hat{q}_\star(\hat{\sigma}), \tag{2.3.12}$$

where $\dot{q}_\star$ is the fixed point of $\texttt{BP}_{\lambda,T}$ given by Proposition 2.4.2, $\hat{q}_\star = \hat{\texttt{BP}}_{\lambda,T}(\dot{q}_\star)$, and $\dot{\mathfrak{Z}}_\star$, $\hat{\mathfrak{Z}}_\star$, $\bar{\mathfrak{Z}}_\star$ are the normalizing constants such that $\dot{H}_\star, \hat{H}_\star, \bar{H}_\star$ are probability measures.

A straightforward consequence of the above is that we can compute the first moment of $\boldsymbol{Z}$ up to constant factors. More formally, define the neighborhood

$$\mathbf{N} = \{H : \|H - H_\star\| \leqslant n^{-1/3}\} \subseteq \mathbf{N}_\circ.$$

We say $\underline{\sigma} \in \mathbf{N}$ if $H(G, \underline{\sigma}) \in \mathbf{N}$, and let $\boldsymbol{Z}(\mathbf{N})$ be the contribution to $\boldsymbol{Z}$ from colorings $\underline{\sigma} \in \mathbf{N}$. In the following, let $\dot{s} \equiv \dot{s}(T)$ count the number of d-tuples $\underline{\sigma} \in (\Omega_T)^d$ for which $\dot{\Phi}(\underline{\sigma}) > 0$. Let $\hat{s} \equiv \hat{s}(T)$ count the number of k-tuples $\underline{\sigma} \in (\Omega_T)^k$ for which $\hat{\Phi}(\underline{\sigma}) > 0$. Let $\bar{s} \equiv |\Omega_T|$, and denote $\wp \equiv \dot{s} + \hat{s} - \bar{s} - 1$.

Corollary 2.3.8. *In the setting of Proposition 2.3.7,*

$$\mathbb{E}\boldsymbol{Z}(\mathbf{N}) \asymp \mathbb{E}\boldsymbol{Z} \asymp \exp\{\boldsymbol{F}(H_\star)\}.$$

Proof. In an pair empirical measure $H = (\dot{H}, \hat{H}, \bar{H})$, the edge marginal $\bar{H}$ can be determined from either the variable or the clause measure:

$$nd\bar{H}(\sigma) = \sum_{\zeta} n\dot{H}(\zeta)\dot{M}(\sigma, \zeta) = \sum_{\xi} m\hat{H}(\xi)\hat{M}(\sigma, \xi) \tag{2.3.13}$$

where $\dot{M} \in \mathbb{R}^{\bar{s} \times \dot{s}}$ and $\hat{M} \in \mathbb{R}^{\bar{s} \times \hat{s}}$ are defined by

$$\dot{M}(\sigma, \zeta) = \sum_{i=1}^{d} \mathbf{1}\{\zeta_i = \sigma\}, \quad \hat{M}(\sigma, \xi) = \sum_{i=1}^{k} \mathbf{1}\{\xi_i = \sigma\}.$$

The $(\dot{s} + \hat{s})$-dimensional vector $(\dot{H}, \hat{H})$ gives rise to a valid empirical measure on the graph G if and only if

(i) $\langle \mathbf{1}, \dot{H} \rangle = 1$;

(ii) $(n\dot{H}, m\hat{H})$ lies in the kernel of the $\bar{s} \times (\dot{s} + \hat{s})$ matrix $M \equiv \begin{pmatrix} \dot{M} & -\hat{M} \end{pmatrix}$;

(iii) $(n\dot{H}, m\hat{H})$ is integer-valued;

(iv) $\dot{H}, \hat{H} \geqslant 0$.

One can verify that the matrix M is of full rank, from which it follows that the space of $(\dot{H}, \hat{H})$ satisfying (i) and (ii) has dimension $\wp$. In Lemma 2.5.6 we will show that M satisfies a stronger condition, which implies that the space of $(\dot{H}, \hat{H})$ satisfying (i), (ii), and (iii) is an affine translation of $(n^{-1}\mathbb{Z})^{\wp}$, where the coefficients of the transformation are bounded. It then follows by combining Lemma 2.3.5 and Proposition 2.3.7 that

$$\frac{\mathbb{E}\boldsymbol{Z}}{\exp\{n\boldsymbol{F}(H_\star)\}} \asymp \sum_{z \in (n^{-1}\mathbb{Z})^{\wp}} \frac{1}{n^{\wp/2} \exp\{\Theta(1) n \|z\|^2\}} \asymp 1$$

The contribution to $\mathbb{E}\boldsymbol{Z}$ from $H \notin \mathbf{N}$ is negligible, so the above estimate holds as well with $\mathbb{E}\boldsymbol{Z}(\mathbf{N})$ in place of $\mathbb{E}\boldsymbol{Z}$. $\square$

2.3.4 Second moment of correlated pairs

We will show in Section 2.10 that for fixed $\lambda \in [0,1]$, the pair $(\boldsymbol{s}(H_\star), \boldsymbol{\Sigma}(H_\star))$ converges as $T \to \infty$ to a limit $(s_\lambda, \Sigma(s_\lambda))$, which matches the physics 1RSB prediction. We then consider the second moment only for colorings in $\mathbf{N}$, beginning with the following definition (following [CP16a]) which is intended to address the contribution from pairs of colorings with large correlation.

Definition 2.3.9. Given a coloring $\underline{\sigma}$ of G, write $\underline{x}(\underline{\sigma}) \equiv (x_v(\underline{\sigma}))_{v\in V}$ for the corresponding frozen configuration. For two colorings $\underline{\sigma}, \underline{\sigma}'$ of G, let

$$\delta(\underline{\sigma}, \underline{\sigma}') \equiv |\{v \in V : x_v(\underline{\sigma}) \neq x_v(\underline{\sigma}')\}|/|V|.$$

Let $I_{\mathrm{sep}} \equiv [(1 - k^4/2^{k/2})/2, (1 + k^4/2^{k/2})/2]$. Write $\underline{\sigma}' \succcurlyeq \underline{\sigma}$ if the number of free variables in $\underline{x}(\underline{\sigma}')$ upper bounds the number in $\underline{x}(\underline{\sigma})$. We say that a coloring $\underline{\sigma} \in \mathbf{N}$ is *separable* if

$$|\{\underline{\sigma}' \in \mathbf{N} : \underline{\sigma}' \succcurlyeq \underline{\sigma} \text{ and } \delta(\underline{\sigma}, \underline{\sigma}') \notin I_{\mathrm{sep}}\}| \leqslant \exp\{(\ln n)^4\},$$

where it is understood that both $\underline{\sigma}, \underline{\sigma}'$ must be valid colorings.

Proposition 2.3.10 (*proved in Section 2.7*)**.** *If $\boldsymbol{S}(\mathbf{N})$ is the contribution to $\boldsymbol{Z}(\mathbf{N})$ from separable colorings, then $\mathbb{E}\boldsymbol{S}(\mathbf{N}) = (1 - o(1))\mathbb{E}\boldsymbol{Z}(\mathbf{N})$.*

In the second moment, we continue to write $H \equiv (\dot{H}, \hat{H}, \bar{H})$ for the empirical measure, with the understanding that it now refers to pair colorings $\underline{\sigma} = (\underline{\sigma}^1, \underline{\sigma}^2)$. Thus $\dot{H}$ is in this context a measure on $(\dot{\Omega}^d)^2$, and so on. If we wish to emphasize that we are in the second moment setting, we will refer to H as the *pair* empirical measure. The single-copy marginals of H are defined as $H^j = (\dot{H}^j, \hat{H}^j, \bar{H}^j)$ for $j = 1, 2$ where

$$\dot{H}^j(\underline{\zeta}) = \sum_{\underline{\sigma}^1, \underline{\sigma}^2} \dot{H}(\underline{\sigma}^1, \underline{\sigma}^2)\mathbf{1}\{\underline{\sigma}^j = \underline{\zeta}\},$$

and similarly for $\hat{H}^j, \bar{H}^j$. To calculate the second moment of $\boldsymbol{Z}(\mathbf{N})$, we must understand all pair empirical measures H in the set

$$\mathbf{N}_2 \equiv \{H : H^1, H^2 \in \mathbf{N}\}.$$

The purpose of Definition 2.3.9 is to allow us to make a further restriction: we compute the second moment of $\boldsymbol{S}(\mathbf{N})$ rather than of $\boldsymbol{Z}(\mathbf{N})$. Any $\underline{\sigma} = (\underline{\sigma}^1, \underline{\sigma}^2)$ with pair empirical measure H will have the same value $\delta(\underline{\sigma}^1, \underline{\sigma}^2) = \delta$, so we can define $\delta(H) = \delta$. Let

$$\mathbf{N}_{\mathrm{sep}} \equiv \{H \in \mathbf{N}_2 : \delta(H) \in I_{\mathrm{sep}}\}, \quad \mathbf{N}_{\mathrm{ns}} \equiv \mathbf{N}_2 \backslash \mathbf{N}_{\mathrm{sep}}.$$

Lemma 2.3.11. *If $\boldsymbol{S}^2(\mathbf{N}_{\mathrm{ns}})$ is the contribution to $\boldsymbol{S}(\mathbf{N})^2$ from pair empirical measures $H \in \mathbf{N}_{\mathrm{ns}}$, then $\mathbb{E}[\boldsymbol{S}^2(\mathbf{N}_{\mathrm{ns}})] \leqslant \exp\{n\boldsymbol{s}(H_\star)\lambda + o(n)\}\,\mathbb{E}\boldsymbol{Z}$.*

Proof. Denote $\underline{\sigma} \in \boldsymbol{S}(\mathbf{N})$ if $\underline{\sigma}$ contributes to $\boldsymbol{S}(\mathbf{N})$, meaning that $\underline{\sigma}$ is separable and has empirical measure in $\mathbf{N}$. Then, by symmetry,

$$\begin{aligned}\boldsymbol{S}^2(\mathbf{N}_{\mathrm{ns}}) &= \sum_{(\underline{\sigma},\underline{\sigma}')\in\mathbf{N}_{\mathrm{ns}}} \mathbf{1}\{\underline{\sigma},\underline{\sigma}' \text{ separable}\}\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})^{\lambda}\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma}')^{\lambda}\\ &\leqslant 2\sum_{(\underline{\sigma},\underline{\sigma}')\in\mathbf{N}_{\mathrm{ns}}} \mathbf{1}\{\underline{\sigma} \text{ separable}\}\mathbf{1}\{\underline{\sigma}' \geqslant \underline{\sigma}\}\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma})^{\lambda}\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G},T}(\underline{\sigma}')^{\lambda}\\ &\leqslant \exp\{n\boldsymbol{s}(H_\star)\lambda + o(n)\}\boldsymbol{S}(\mathbf{N}),\end{aligned}$$

where the last step is by the definition of separability. The result follows easily by noting that $\boldsymbol{S}(\mathbf{N}) \leqslant \boldsymbol{Z}$. □

Corollary 2.3.12. *For any $\lambda \in [0,1]$ with $\Sigma(s_\lambda) > 0$, there exists $T(\lambda)$ large enough such that for all $T \geqslant T(\lambda)$, the ratio*

$$\frac{\mathbb{E}[\boldsymbol{S}^2(\mathbf{N}_{\mathrm{ns}})]}{(\mathbb{E}\boldsymbol{Z}(\mathbf{N}))^2}$$

decays exponentially with n.

Proof. By Lemma 2.3.11 and and Proposition 2.3.7,

$$\frac{\mathbb{E}[\boldsymbol{S}^2(\mathbf{N}_{\mathrm{ns}})]}{(\mathbb{E}\boldsymbol{Z}(\mathbf{N}))^2} \leqslant \frac{\exp\{n\boldsymbol{s}(H_\star)\lambda + o(n)\}}{\mathbb{E}\boldsymbol{Z}(\mathbf{N})} = \exp\{-n\boldsymbol{\Sigma}(H_\star) + o(n)\}.$$

Since for fixed λ the pair $(\boldsymbol{s}(H_\star), \boldsymbol{\Sigma}(H_\star))$ converges in the limit $T \to \infty$ to $(s_\lambda, \Sigma(s_\lambda))$, for $T \geqslant T(\lambda)$ the above ratio decays exponentially with n, concluding the proof. □

2.3.5 Second moment of uncorrelated pairs

The derivation of Lemma 2.3.5 applies equally well to the second moment, giving the expansion

$$\mathbb{E}[\boldsymbol{Z}^2(H)] \asymp n^{-\wp(H)}\exp\{n\boldsymbol{F}_2(H)\}$$

where H is the empirical measure for pair colorings, and $\wp(H), \boldsymbol{F}_2(H)$ are defined explicitly as follows. Recalling (2.3.4), for $\underline{\sigma} \in \Omega^{2k}$ let

$$\hat{v}_2(\underline{\sigma}) \equiv \mathbb{E}^{\mathrm{lit}}[\hat{I}^{\mathrm{lit}}(\underline{\sigma}^1 \oplus \underline{\mathtt{L}})\hat{I}^{\mathrm{lit}}(\underline{\sigma}^2 \oplus \underline{\mathtt{L}})].$$

For a pair empirical measure H with single-copy marginals H^1, H^2 we have (cf. (2.3.9))

$$\begin{aligned}\boldsymbol{v}_2(H) &\equiv (d/k)\langle \ln\hat{v}_2, \hat{H}\rangle,\\ \boldsymbol{s}_2(H) &\equiv \boldsymbol{s}(H^1) + \boldsymbol{s}(H^2),\\ \boldsymbol{\Sigma}_2(H) &\equiv \mathcal{H}(\dot{H}) + (d/k)\mathcal{H}(\hat{H}) - d\mathcal{H}(\bar{H}) + \boldsymbol{v}_2(H),\\ \boldsymbol{F}_2(H) &\equiv \boldsymbol{\Sigma}_2(H) + \boldsymbol{s}_2(H)\lambda,\\ \wp(H) &\equiv |\operatorname{supp}\dot{H}| + |\operatorname{supp}\hat{H}| - |\operatorname{supp}\bar{H}| - 1.\end{aligned} \tag{2.3.14}$$

We will show that the maximizer for $\boldsymbol{F}_2$ can be described in terms of the maximizer $H_\star$ of $\boldsymbol{F}$. To this end, we will say that a measure $\hat{K}$ on pairs $(\underline{\xi}, \underline{\mathtt{L}})$ is *factorized* if

(i) the marginal $\hat{K}$ on $\underline{\mathtt{L}}$ is uniform over $\{\mathtt{0},\mathtt{1}\}^k$, and

(ii) for each $\underline{\xi}$ the conditional measure $\hat{K}(\underline{\mathtt{L}}|\underline{\xi})$ is uniform on $\{\underline{\mathtt{L}} : \hat{I}^{\mathrm{lit}}(\underline{\xi} \oplus \underline{\mathtt{L}}) = 1\}$.

From (2.3.12) and Lemma 2.3.2, $\hat{H}_\star$ is the marginal on $\underline{\xi}$ of the probability measure $\hat{K}_\star$ on pairs $(\underline{\xi}, \underline{\mathtt{L}}) \in \Omega^k \times \{\mathtt{0},\mathtt{1}\}^k$ defined by

$$\hat{K}_\star(\underline{\xi}, \underline{\mathtt{L}}) \cong \hat{I}^{\mathrm{lit}}(\underline{\xi} \oplus \underline{\mathtt{L}})\hat{g}(\underline{\xi}), \quad \text{where } \hat{g}(\underline{\xi}) = \hat{\Phi}^{\max}(\underline{\xi}) \prod_{i=1}^{k} \dot{q}_\star(\xi_i).$$

We will characterize $\dot{q}_\star$ in detail below, but for now we note that it has the symmetry $\dot{q}_\star(\dot{\sigma}) = \dot{q}_\star(\dot{\sigma} \oplus \mathtt{1})$, which implies $\hat{g}(\underline{\xi}) = \hat{g}(\underline{\xi} \oplus \underline{\mathtt{L}})$ for any $\underline{\mathtt{L}} \in \{\mathtt{0},\mathtt{1}\}^k$. It follows from this that the measure $\hat{K}_\star$ is indeed factorized.

Lemma 2.3.13. *Assume we have empirical measures $H^j = (\dot{H}^j, \hat{H}^j, \bar{H}^j)$ $(j = 1, 2)$, such that $\hat{H}^j$ is the marginal on $\underline{\xi}$ of an $\underline{\mathtt{L}}$-factorized measure $\hat{K}^j$. Suppose $H = (\dot{H}, \hat{H}, \bar{H})$ where $\dot{H}, \bar{H}$ are the product measures $\dot{H}^1 \otimes \dot{H}^2$ and $\bar{H}^1 \otimes \bar{H}^2$, and*

$$\hat{H}(\underline{\xi}) = \mathbb{E}^{\mathrm{lit}}[\hat{K}^1(\underline{\xi}^1|\underline{\mathtt{L}})\hat{K}^2(\underline{\xi}^2|\underline{\mathtt{L}})].$$

Then $\boldsymbol{F}_2(H) = \boldsymbol{F}(H^1) + \boldsymbol{F}(H^2)$.

Proof. From the definitions we have

$$(k/d)[\boldsymbol{F}_2(H) - \boldsymbol{F}(H^1) - \boldsymbol{F}(H^2)] = \mathcal{H}(\hat{H}) + \langle \ln \hat{v}_2, \hat{H} \rangle - \sum_{j=1,2} [\mathcal{H}(\hat{H}^j) + \langle \ln \hat{v}, \hat{H}^j \rangle].$$

From the assumption, $\hat{H}$ is the marginal on $\underline{\xi}$ of the measure $\hat{K}(\underline{\xi}, \underline{\mathtt{L}}) = 2^{-k}\hat{K}^1(\underline{\xi}^1|\underline{\mathtt{L}})\hat{K}^2(\underline{\xi}^2|\underline{\mathtt{L}})$. Note that the marginal of $\hat{K}$ on $\underline{\mathtt{L}}$ is uniform, and $\hat{K}(\underline{\mathtt{L}}|\underline{\xi}^1, \underline{\xi}^2)$ is uniform on $\underline{\mathtt{L}}$ compatible with both $\underline{\xi}^1, \underline{\xi}^2$. Therefore, letting $(\underline{\xi}^1, \underline{\xi}^2, \underline{\mathtt{L}})$ denote a random sample from $\hat{K}$,

$$\mathcal{H}(\hat{H}) + \langle \ln \hat{v}_2, \hat{H} \rangle = \mathcal{H}(\underline{\xi}^1, \underline{\xi}^2|\underline{\mathtt{L}}) + \mathcal{H}(\underline{\mathtt{L}}) - \mathcal{H}(\underline{\mathtt{L}}|\underline{\xi}^1, \underline{\xi}^2) + \langle \ln \hat{v}_2, \hat{H} \rangle = \mathcal{H}(\underline{\xi}^1, \underline{\xi}^2|\underline{\mathtt{L}}).$$

Applying conditional independence gives

$$\mathcal{H}(\underline{\xi}^1, \underline{\xi}^2|\underline{\mathtt{L}}) = \sum_{j=1,2} [\mathcal{H}(\underline{\xi}^j) + \mathcal{H}(\underline{\mathtt{L}}|\underline{\xi}^j) - \mathcal{H}(\underline{\mathtt{L}})] = \sum_{j=1,2} [\mathcal{H}(\hat{H}^j) + \langle \ln \hat{v}, \hat{H}^j \rangle],$$

which proves $\boldsymbol{F}_2(H) = \boldsymbol{F}(H^1) + \boldsymbol{F}(H^2)$. □

Proposition 2.3.14 (*proved in Section 2.6*)**.** *The unique maximizer of $\boldsymbol{F}_2$ in $\mathbf{N}_{\mathrm{sep}}$ is the pair empirical measure $H_\otimes = (\dot{H}_\otimes, \hat{H}_\otimes, \bar{H}_\otimes)$ given by $\dot{H}_\otimes = \dot{H}_\star \otimes \dot{H}_\star$, $\bar{H}_\otimes = \bar{H}_\star \otimes \bar{H}_\star$, and*

$$\hat{H}_\otimes = \mathbb{E}^{\mathrm{lit}}[\hat{K}_\star(\cdot|\underline{\mathtt{L}}) \otimes \hat{K}_\star(\cdot|\underline{\mathtt{L}})].$$

Further, there is a positive constant $\epsilon = \epsilon(k, \lambda, T)$ so that for $\|H - H_\otimes\| \leqslant \epsilon$,

$$\boldsymbol{F}_2(H) \leqslant \boldsymbol{F}_2(H_\otimes) - \epsilon\|H - H_\otimes\|^2.$$

Corollary 2.3.15. *There exists a constant $C = C(k, \lambda, T)$ such that*

$$\mathbb{E}[\boldsymbol{Z}^2(\mathbf{N}_{\text{sep}})] \leqslant C(\mathbb{E}\boldsymbol{Z}(\mathbf{N}))^2$$

Proof. Recall from Corollary 2.3.8 the definition of $(\dot{s}, \hat{s}, \bar{s})$ for the single-copy model, and define $(\dot{s}_2, \hat{s}_2, \bar{s}_2)$ analogously for the pair model. Let $\wp_2 \equiv \dot{s}_2 + \hat{s}_2 - \bar{s}_2 - 1$. For any fixed $H^1, H^2 \in \mathbf{N}$, the set of pair empirical measures H with single-copy marginals (H^1, H^2) spans a space of dimension $\wp_2 - 2\wp$. Thus, writing $\mathbb{E}[\boldsymbol{Z}^2(H^1, H^2)]$ for the second-moment contribution from such measures, it follows from Proposition 2.3.14 and Lemma 2.5.6 that

$$\mathbb{E}[\boldsymbol{Z}^2(H^1, H^2)] \asymp n^{-\wp} \exp\{n\boldsymbol{F}_2(H_\otimes)\}.$$

Summing over $(H^1, H^2) \in \mathbf{N}_{\text{sep}}$ then gives

$$\mathbb{E}[\boldsymbol{Z}^2(\mathbf{N}_{\text{sep}})] \asymp n^{-\wp} \exp\{n\boldsymbol{F}_2(H_\otimes)\},$$

which in turn is $\asymp (\mathbb{E}\boldsymbol{Z}(\mathbf{N}))^2$ by Proposition 2.3.7 and Lemma 2.3.13. □

2.3.6 Conclusion of main result

We now explain that the main theorem follows from the preceding assertions.

Corollary 2.3.16. *For any $\lambda \in [0, 1]$ with $\Sigma(s_\lambda) > 0$, there exists $T(\lambda)$ large enough such that for all $T \geqslant T(\lambda)$, and for n sufficiently large,*

$$\mathbb{E}[\boldsymbol{S}(\mathbf{N})^2] \leqslant C(\mathbb{E}\boldsymbol{S}(\mathbf{N}))^2$$

for a constant $C = C(k, \lambda, T)$.

Proof. Since $\boldsymbol{S} \leqslant \boldsymbol{Z}$, we can bound

$$\mathbb{E}[\boldsymbol{S}(\mathbf{N})^2] \leqslant \mathbb{E}[\boldsymbol{Z}^2(\mathbf{N}_{\text{sep}})] + \mathbb{E}[\boldsymbol{Z}^2(\mathbf{N}_{\text{ns}})].$$

By Corollaries 2.3.12 and 2.3.15, the above is bounded by a constant times $(\mathbb{E}\boldsymbol{Z}(\mathbf{N}))^2$, which in turn is bounded by a constant times $(\mathbb{E}\boldsymbol{S}(\mathbf{N}))^2$ by Proposition 2.3.10. □

Corollary 2.3.16 implies $\mathbb{P}(\boldsymbol{S}(\mathbf{N}) \geqslant \delta\mathbb{E}\boldsymbol{S}(\mathbf{N})) \geqslant \delta$ for some positive constant δ. By adapting methods of [DSS16] we can strengthen this to

Proposition 2.3.17. *In the setting of Corollary 2.3.16, $\boldsymbol{S}(\mathbf{N})$ concentrates around its mean in the sense that $\lim_{\epsilon \downarrow 0} \liminf \mathbb{P}(\epsilon \leqslant \boldsymbol{S}(\mathbf{N})/\mathbb{E}\boldsymbol{S}(\mathbf{N}) \leqslant \epsilon^{-1}) = 1.$*[1]

Proof. This is a straightforward consequence of the method described in [DSS16, §6]. □

Corollary 2.3.18. *For $k \geqslant k_0$, $\mathsf{f}(\alpha) \geqslant \mathsf{f}^{1\text{RSB}}(\alpha)$ for all $\alpha_{\text{lbd}} \leqslant \alpha < \alpha_{\text{sat}}$.*

[1] The upper bound follows trivially from Markov's inequality, so the task is to show the lower bound.

Proof. Follows by combining Corollary 2.3.16 and Proposition 2.3.17. □

The proofs of the above propositions occupies Sections 2.4 through 2.7, with the contraction estimates deferred to Section 2.9. In Section 2.8 we will show

Proposition 2.3.19. *For $k \geqslant k_0$, it holds for all $\alpha < \alpha_{\text{sat}}$ that $\mathsf{f}(\alpha) \leqslant \mathsf{f}^{1\text{RSB}}(\alpha)$.*

Proof of Theorem 1. Follows by combining Corollary 2.3.18 and Proposition 2.3.19. □

2.4 Tree recursions

2.4.1 Belief propagation

We now describe the *belief propagation* (BP) recursions for this model. In the standard formulation (see e.g. [MM09, Ch. 14]), this is a pair of relations for two probability measures $\dot{\boldsymbol{q}}, \hat{\boldsymbol{q}}$ over Ω:

$$\dot{\boldsymbol{q}}(\sigma) = [\dot{\boldsymbol{B}}(\hat{\boldsymbol{q}})](\sigma) = \frac{1}{\dot{\boldsymbol{z}}} \bar{\Phi}_T(\sigma)^\lambda \sum_{\sigma_2,\ldots,\sigma_d} \dot{\Phi}(\sigma, \sigma_2, \ldots, \sigma_d)^\lambda \prod_{i=2}^{d} \hat{\boldsymbol{q}}(\sigma_i)$$

$$\hat{\boldsymbol{q}}(\sigma) = [\hat{\boldsymbol{B}}(\dot{\boldsymbol{q}})](\sigma) = \frac{1}{\hat{\boldsymbol{z}}} \bar{\Phi}_T(\sigma)^\lambda \sum_{\sigma_2,\ldots,\sigma_k} \hat{\Phi}(\sigma, \sigma_2, \ldots, \sigma_k)^\lambda \prod_{i=2}^{k} \dot{\boldsymbol{q}}(\sigma_i)$$

where $\dot{\boldsymbol{z}}, \hat{\boldsymbol{z}}$ are the normalizing constants ensuring that the outputs are probability measures. The first equation above is the *variable recursion*, and the second is the *clause recursion*. A standard simplification (see e.g. [MM09, Ch. 19]) is to assume a one-sided dependence:

$$\dot{\boldsymbol{q}}(\sigma) \cong \dot{q}(\dot{\sigma}) \text{ and } \hat{\boldsymbol{q}}(\sigma) \cong \hat{q}(\hat{\sigma}). \tag{2.4.1}$$

where $\dot{q}, \hat{q}$ are probability measures on $\dot{\Omega}, \hat{\Omega}$, and $\cong$ denotes equivalence up to normalization. To see that this restriction makes sense, we note the following lemma which confirms that the restriction is preserved under the BP mapping:

Lemma 2.4.1. *The restriction (2.4.1) is preserved under the* BP *mapping, that is, if $\dot{\boldsymbol{q}}$ depends only on $\dot{\sigma}$ then $\hat{\boldsymbol{B}}(\dot{\boldsymbol{q}})$ depends only on $\hat{\sigma}$; and if $\hat{\boldsymbol{q}}$ depends only on $\hat{\sigma}$ then $\dot{\boldsymbol{B}}(\hat{\boldsymbol{q}})$ depends only on $\dot{\sigma}$.*

Proof. Suppose $\hat{\boldsymbol{q}}$ depends only on $\hat{\sigma}$, so $\hat{\boldsymbol{q}}(\sigma) \cong \hat{q}(\hat{\sigma})$, and consider the variable BP mapping $\dot{\boldsymbol{B}}$. If $\sigma \notin \Omega_{\mathtt{f}}$ then $\hat{\sigma}$ is uniquely determined by $\dot{\sigma}$, so there is nothing to prove. Therefore we need only consider the case that $\sigma \in \Omega_{\mathtt{f}}$. In order for $\dot{I}(\sigma, \sigma_2, \ldots, \sigma_d) = 1$, we must have

$$\dot{\sigma} = \dot{\mathtt{T}}(\hat{\sigma}_2, \ldots, \hat{\sigma}_d); \tag{2.4.2}$$

note that this condition does not depend on $\hat{\sigma}$. Further, given $(\sigma, \hat{\sigma}_2, \ldots, \hat{\sigma}_d)$ satisfying (2.4.2), there is a unique choice of $(\dot{\sigma}_2, \ldots, \dot{\sigma}_d)$ for which $\dot{I}(\sigma, \sigma_2, \ldots, \sigma_d) = 1$; it is determined by the relation $\dot{\sigma}_i = \dot{\mathtt{T}}((\hat{\sigma}_j)_{j \neq i})$. In this case, applying (2.3.3) gives

$$\dot{\Phi}(\sigma, \sigma_2, \ldots, \sigma_d)\bar{\Phi}(\sigma) = \dot{z}(\dot{\sigma}),$$

which also does not depend on $\hat{\sigma}$. It follows that

$$[\dot{\boldsymbol{B}}(\hat{\boldsymbol{q}})](\sigma) \cong \dot{z}(\dot{\sigma})^{\lambda} \sum_{\hat{\sigma}_2, \ldots, \hat{\sigma}_d} \mathbf{1}\{\dot{\sigma} = \dot{\mathtt{T}}((\hat{\sigma}_i)_{i \geqslant 2})\} \prod_{i=2}^{d} \hat{q}(\hat{\sigma}_i).$$

The right-hand side does not depend on $\hat{\sigma}$, which proves the claim concerning $\dot{\boldsymbol{B}}$.

Similarly, suppose $\dot{\boldsymbol{q}}$ depends only on $\dot{\sigma}$, so $\dot{\boldsymbol{q}}(\sigma) \cong \dot{q}(\dot{\sigma})$, and consider the clause mapping $\hat{\boldsymbol{B}}$. Again, if $\sigma \notin \Omega_{\mathtt{f}}$ then there is nothing to prove, so suppose $\sigma \in \Omega_{\mathtt{f}}$. Then, in order for $\hat{I}^{\text{lit}}((\sigma, \sigma_2, \ldots, \sigma_k) \oplus \underline{\mathtt{L}}) = 1$, we must have

$$\hat{\sigma} = \mathtt{L}_1 \oplus \hat{\mathtt{T}}((\dot{\sigma}_i \oplus \mathtt{L}_i)_{i \geqslant 2}); \tag{2.4.3}$$

note that this condition does not depend on $\dot{\sigma}$. Further, given $(\sigma, \dot{\sigma}_2, \ldots, \dot{\sigma}_k, \underline{\mathtt{L}})$ satisfying (2.4.3), there is a unique choice of $(\hat{\sigma}_2, \ldots, \hat{\sigma}_k)$ for which $\hat{I}^{\text{lit}}((\sigma, \sigma_2, \ldots, \sigma_k) \oplus \underline{\mathtt{L}}) = 1$; it is determined by the mapping $\hat{\mathtt{T}}$. In this case, applying (2.3.3) gives

$$\hat{\Phi}((\sigma, \sigma_2, \ldots, \sigma_k) \oplus \underline{\mathtt{L}})\bar{\Phi}(\sigma) = \hat{z}(\hat{\sigma}),$$

which also does not depend on $\dot{\sigma}$. It follows that

$$[\hat{\boldsymbol{B}}(\dot{\boldsymbol{q}})](\sigma) \cong \hat{z}(\hat{\sigma})^{\lambda} \sum_{\underline{\mathtt{L}}} \sum_{\dot{\sigma}_2, \ldots, \dot{\sigma}_d} \mathbf{1}\{\hat{\sigma} = \mathtt{L}_1 \oplus \hat{\mathtt{T}}((\dot{\sigma}_i \oplus \mathtt{L}_i)_{i \geqslant 2})\} \prod_{i=2}^{k} \dot{q}(\dot{\sigma}_i).$$

The right-hand side does not depend on $\dot{\sigma}$, which proves the claim concerning $\hat{\boldsymbol{B}}$. □

Lemma 2.4.1 verifies that the one-sided dependence is preserved under the BP recursion, and from now on we always assume (2.4.1). In this setting, $\dot{\boldsymbol{B}}$ and $\hat{\boldsymbol{B}}$ reduce to mappings

$$\dot{\mathtt{BP}} \equiv \dot{\mathtt{BP}}_{\lambda,T} : \mathscr{P}(\hat{\Omega}) \to \mathscr{P}(\dot{\Omega}),$$
$$\hat{\mathtt{BP}} \equiv \hat{\mathtt{BP}}_{\lambda,T} : \mathscr{P}(\dot{\Omega}) \to \mathscr{P}(\hat{\Omega}).$$

(Generally we will fix λ, T and suppress them from the notation.) We also denote

$$\mathtt{BP} \equiv \dot{\mathtt{BP}} \circ \hat{\mathtt{BP}} \equiv \mathtt{BP}_{\lambda,T}. \tag{2.4.4}$$

Note that $\dot{q}$ is a measure on spins $\dot{\sigma} \in \dot{\Omega}$. In the introduction we discussed probability measures over messages $\dot{\mathtt{m}}$; this can be recovered by taking $\dot{q}(\{\dot{\sigma} : \dot{m}(\dot{\sigma}) = \dot{\mathtt{m}}\})$. As in Proposition 2.1.2 we consider $\mathscr{P}(\dot{\Omega})$ and $\mathscr{P}(\hat{\Omega})$ as ℓ^1 sequence spaces.

In the context of NAE-SAT, a useful observation is that the BP recursion has an averaging property, as follows. Since in the clause recursion we average over the clause literals $\underline{\mathtt{L}}$, we can make the change of variables $\tau_i = \mathtt{L}_1 \oplus \sigma_i \oplus \mathtt{L}_i$ for $i \geqslant 2$, which yields

$$\begin{aligned}\hat{\boldsymbol{B}}(\dot{\boldsymbol{q}}) &\cong \bar{\Phi}_T(\sigma)^\lambda \sum_{\tau_2,\ldots,\tau_k} \tfrac{1}{2}\sum_{\mathtt{L}_1} \hat{\Phi}^{\mathrm{lit}}((\sigma,\tau_2,\ldots,\tau_k)\oplus\mathtt{L}_1)^\lambda \prod_{i=2}^{k}\left\{\tfrac{1}{2}\sum_{\mathtt{L}_i}\dot{\boldsymbol{q}}(\tau_i\oplus\mathtt{L}_i\oplus\mathtt{L}_1)\right\}\\ &= \bar{\Phi}_T(\sigma)^\lambda \sum_{\tau_2,\ldots,\tau_k} \hat{\Phi}^{\mathrm{lit}}(\sigma,\tau_2,\ldots,\tau_k)^\lambda \prod_{i=2}^{k} \dot{\boldsymbol{q}}^{\mathrm{avg}}(\tau_i) = \hat{\boldsymbol{B}}(\dot{\boldsymbol{q}}^{\mathrm{avg}})\end{aligned}$$

where $\dot{\boldsymbol{q}}^{\mathrm{avg}}(\sigma) \equiv \frac{1}{2}[\dot{\boldsymbol{q}}(\sigma)+\dot{\boldsymbol{q}}(\sigma\oplus\mathtt{1})]$. Therefore, under assumption (2.4.1),

$$\hat{\mathtt{BP}}\dot{q} = \hat{\mathtt{BP}}\dot{q}^{\mathrm{avg}}, \quad \text{and consequently} \quad \mathtt{BP}\dot{q} = \mathtt{BP}\dot{q}^{\mathrm{avg}}.$$

We are primarily interested in fixed points of the mapping $\mathtt{BP}$, in which case we can restrict attention to measures satisfying $\dot{q} = \dot{q}^{\mathrm{avg}}$.

The BP recursions for the pair model are completely analogous to those of the single-copy model. They can be simplified to a pair of mappings

$$\begin{aligned}\dot{\mathtt{BP}}_2 &: \mathscr{P}(\hat{\Omega}^2) \to \mathscr{P}(\dot{\Omega}^2),\\ \hat{\mathtt{BP}}_2 &: \mathscr{P}(\dot{\Omega}^2) \to \mathscr{P}(\hat{\Omega}^2);\end{aligned}$$

and once again $\mathtt{BP}_2 \equiv \dot{\mathtt{BP}}_2 \circ \hat{\mathtt{BP}}_2$ satisfies the averaging property $\mathtt{BP}_2(\dot{q}) = \mathtt{BP}_2(\dot{q}^{\mathrm{avg}})$ where

$$\dot{q}^{\mathrm{avg}}(\dot{\sigma}^1,\dot{\sigma}^2) = \tfrac{1}{2}\dot{q}(\dot{\sigma}^1,\dot{\sigma}^2) + \tfrac{1}{2}\dot{q}(\dot{\sigma}^1\oplus\mathtt{1},\dot{\sigma}^2\oplus\mathtt{1}).$$

In what follows we will drop the subscript and write simply $\dot{\mathtt{BP}}, \hat{\mathtt{BP}}, \mathtt{BP}$; it will be clear from context whether we are in the single-copy or pair setting.

2.4.2 Contraction estimate

A key step in the proof is to (explicitly) define a subset $\boldsymbol{\Gamma} \subseteq \mathscr{P}(\dot{\Omega})$ on which we have a contraction estimate of the form $\|\mathtt{BP}\dot{q} - \dot{q}_\star\|_1 \leqslant c\|\dot{q}-\dot{q}_\star\|_1$ for a constant $c < 1$, in both first- and second-moment settings. We remark that it suffices to prove such an estimate for measures $\dot{q} = \dot{q}^{\mathrm{avg}}$, since for general $\dot{q}$ it implies

$$\|\mathtt{BP}\dot{q} - \dot{q}_\star\|_1 = \|\mathtt{BP}\dot{q}^{\mathrm{avg}} - \dot{q}_\star\|_1 \leqslant c\|\dot{q}^{\mathrm{avg}} - \dot{q}_\star\|_1 \leqslant c\|\dot{q}-\dot{q}_\star\|_1.$$

Thus it will be sufficient to define $\boldsymbol{\Gamma}$ as a subset of measures satisfying $\dot{q} = \dot{q}^{\mathrm{avg}}$. Let us abbreviate $\{\mathtt{r}\} \equiv \{\mathtt{r}_0,\mathtt{r}_1\}$ and $\{\mathtt{b}\} \equiv \{\mathtt{b}_0,\mathtt{b}_1\}$. We also abbreviate $\{\mathtt{f}\} \equiv \dot{\Omega}_{\mathtt{f}}$ in the context of $\dot{q}$, and $\{\mathtt{f}\} \equiv \hat{\Omega}_{\mathtt{f}}$ in the context of $\hat{q}$. For the first moment analysis, we define $\boldsymbol{\Gamma}$ to be the set of measures $\dot{q}$ supported on $\dot{\Omega}_T$, satisfying $\dot{q} = \dot{q}^{\mathrm{avg}}$, such that

$$\begin{aligned}\dot{q}(\mathtt{r}) + 2^k\dot{q}(\mathtt{f}) &= O(1)\dot{q}(\mathtt{b}),\\ \dot{q}(\mathtt{b})[1-O(2^{-k})] &\leqslant \dot{q}(\mathtt{r}).\end{aligned} \tag{2.4.5}$$

For the second moment analysis, we define $\mathbf{\Gamma} = \mathbf{\Gamma}(c, \kappa)$ to be the set of $\dot{q}$ supported on $(\dot{\Omega}_T)^2$, satisfying $\dot{q} = \dot{q}^{\text{avg}}$, such that

$$\begin{aligned}
&\text{(A)}\quad \textstyle\sum_{\dot{\sigma}\notin\{\texttt{bb}\}}(2^{-k})^{\texttt{r}[\dot{\sigma}]}p(\dot{\sigma}) = O(2^{-k})p(\texttt{bb}), \quad |p(\texttt{b}_0\texttt{b}_0) - p(\texttt{b}_0\texttt{b}_1)| \leqslant (k^9/2^{ck})p(\texttt{bb}),\\
&\text{(B)}\quad p(\{\texttt{rf},\texttt{fr}\}) = O(2^{-\kappa k})p(\texttt{bb}), \quad p(\texttt{rr}) = O(2^{(1-\kappa)k})p(\texttt{bb}),\\
&\text{(C)}\quad p(\texttt{r}_x\dot{\sigma}) \geqslant [1-O(2^{-k})]p(\texttt{b}_x\dot{\sigma}) \text{ and}\\
&\qquad\ \ p(\dot{\sigma}\texttt{r}_x) \geqslant [1-O(2^{-k})]p(\dot{\sigma}\texttt{b}_x) \text{ for all } x \in \{\texttt{0},\texttt{1}\} \text{ and } \dot{\sigma} \in \dot{\Omega}.
\end{aligned} \tag{2.4.6}$$

Proposition 2.4.2. *In the first moment, let* $\texttt{BP} \equiv \texttt{BP}_{\lambda,T}$ *for* $\lambda \in [0,1]$ *and* $1 \leqslant T \leqslant \infty$. *There is a unique* $\dot{q}_\star \equiv \dot{q}_{\lambda,T} \in \mathbf{\Gamma}$ *satisfying* $\dot{q}_\star = \texttt{BP}\dot{q}_\star$. *If* $\dot{q}$ *is any element of* $\mathbf{\Gamma}$, *then* $\texttt{BP}\dot{q} \in \mathbf{\Gamma}$ *also, with* $\|\texttt{BP}\dot{q} - \dot{q}_\star\|_1 = O(k^2/2^k)\|\dot{q} - \dot{q}_\star\|_1$.

Proposition 2.4.3 (second moment contraction)**.** *In the second moment, let* $\texttt{BP} \equiv \texttt{BP}_{\lambda,T}$ *for* $\lambda \in [0,1]$ *and* $1 \leqslant T \leqslant \infty$. *There is a unique* $\dot{q}_\star \equiv \dot{q}_{\lambda,T} \in \mathbf{\Gamma}(1,1)$ *satisfying* $\dot{q}_\star = \texttt{BP}\dot{q}_\star$. *Further, for* $c \in (0,1]$ *and* $k \geqslant k_0(c)$, *there is no other fixed point of* $\texttt{BP}$ *in* $\mathbf{\Gamma}(c,1)$*: if* $\dot{q} \in \mathbf{\Gamma}(c,1)$ *then* $\texttt{BP}\dot{q} \in \mathbf{\Gamma}(1,1)$, *with* $\|\texttt{BP}\dot{q} - \dot{q}_\star\|_1 = O(k^4/2^k)\|\dot{q} - \dot{q}_\star\|_1$.

We will also make use of the following lemma which says that if $\dot{q}$ is a BP fixed point, then showing (2.4.6) with $\kappa = 0$ implies the stronger bound with $\kappa = 1$:

Lemma 2.4.4. *In the second moment, if for some* $c \in (0,1]$ *we have* $\dot{q} \in \mathbf{\Gamma}(c,0)$ *and* $\dot{q} = \texttt{BP}(\dot{q})$, *then in fact* $\dot{q} \in \mathbf{\Gamma}(c,1)$.

The proofs of Proposition 2.4.2 and 2.4.3 and of Lemma 2.4.4 are deferred to Section 2.9. In the next sections we apply them to compute the first and second moments of $\boldsymbol{Z}_{\lambda,T}(H)$.

2.5 Reduction to tree optimization

In this section we prove a key reduction for the proofs of Propositions 2.3.7 and 2.3.14, concerning the optimization of $\boldsymbol{F}$ and its second-moment analogue $\boldsymbol{F}_2$. As we have already commented, direct analysis of these functions is in general quite challenging. Instead, we first rely on other means to restrict the set of empirical measures — the set $\mathbf{N}_\circ$ in the first moment, and the set $\mathbf{N}_{\text{sep}}$ in the second moment. With this restriction, we can successfully optimize $\boldsymbol{F}$ and $\boldsymbol{F}_2$ through a related, but simpler, optimization problem on trees. In this section we explain this reduction.

Definition 2.5.1. The tree analogues of $\mathbf{\Sigma}, \mathbf{\Sigma}_2$ (from (2.3.9) and (2.3.14)) are defined as

$$\begin{aligned}
\mathbf{\Theta}(H) &\equiv \mathcal{H}(\dot{H}) + d\mathcal{H}(\hat{H}) - d\mathcal{H}(\bar{H}) + \boldsymbol{v}(H)\\
\mathbf{\Theta}_2(H) &\equiv \mathcal{H}(\dot{H}) + d\mathcal{H}(\hat{H}) - d\mathcal{H}(\bar{H}) + \boldsymbol{v}_2(H)
\end{aligned}$$

(where H denotes a single-copy empirical measure in the first line, and a pair empirical measure in the second). The tree analogues of $\boldsymbol{F}, \boldsymbol{F}_2$ are defined as

$$\begin{aligned}
\mathbf{\Lambda}(H) &\equiv \mathbf{\Theta}(H) + \lambda\boldsymbol{s}(H),\\
\mathbf{\Lambda}_2(H) &\equiv \mathbf{\Theta}_2(H) + \lambda\boldsymbol{s}_2(H).
\end{aligned}$$

Given H, let $\dot{h}^{\text{tree}}(H)$ be the measure on $\dot{\sigma}$ defined by

$$[\dot{h}^{\text{tree}}(H)](\dot{\sigma}) \equiv (k-1)^{-1} \sum_{\xi \in \Omega^k} \sum_{j=2}^{k} \hat{H}(\underline{\sigma}) \mathbf{1}\{\xi_j = \dot{\sigma}\}.$$

We then let

$$\begin{aligned} \mathbf{\Lambda}^{\text{opt}}(\dot{h}) &\equiv \sup\{\mathbf{\Lambda}(H) : \dot{h}^{\text{tree}}(H) = \dot{h}\}, & \Xi(H) &\equiv \mathbf{\Lambda}^{\text{opt}}(\dot{h}^{\text{tree}}(H)) - \mathbf{\Lambda}(H); \\ \mathbf{\Lambda}_2^{\text{opt}}(\dot{h}) &\equiv \sup\{\mathbf{\Lambda}_2(H) : \dot{h}^{\text{tree}}(H) = \dot{h}\}, & \Xi_2(H) &\equiv \mathbf{\Lambda}_2^{\text{opt}}(\dot{h}^{\text{tree}}(H)) - \mathbf{\Lambda}_2(H). \end{aligned}$$

Note that Ξ, Ξ_2 are non-negative functions.

Definition 2.5.2. For $\underline{\sigma} \in \Omega^k$ and $j \in [k]$ define the rotation

$$\underline{\sigma}^{(j)} \equiv (\sigma_j, \ldots, \sigma_k, \sigma_1, \ldots, \sigma_{j-1}).$$

We let $\hat{H}^{\text{sym}}(\underline{\sigma})$ denote the average of $\hat{H}(\underline{\sigma}^{(j)})$ over $j \in [k]$, and write $H^{\text{sym}} \equiv (\dot{H}, \hat{H}^{\text{sym}}, \bar{H})$.

Theorem 2.5.3. *For ϵ small enough, and with H^{sym} as in Definition 2.5.2,*

$$\begin{aligned} \boldsymbol{F}(H) &\leqslant \max\{\boldsymbol{F}(H') : \|H' - H\|_1 \leqslant \epsilon (dk)^{2T}\} - \epsilon \cdot \Xi(H^{\text{sym}}), \\ \boldsymbol{F}_2(H) &\leqslant \max\{\boldsymbol{F}_2(H') : \|H' - H\|_1 \leqslant \epsilon (dk)^{2T}\} - \epsilon \cdot \Xi_2(H^{\text{sym}}). \end{aligned}$$

For the sake of exposition, we will give the proof of Theorem 2.5.3 for $\boldsymbol{F}$ only; the assertion for $\boldsymbol{F}_2$ follows from the same argument with essentially no modifications. The interpretation of $\mathbf{\Lambda}$ will emerge during the proof, which occupies the remainder of this section. Informally, while $\boldsymbol{F}$ refers to a graph optimization problem which need not be concave, $\mathbf{\Lambda}$ refers to an entropy maximization problem on colorings of a finite tree, which becomes a tractable problem. Once we have proved Theorem 2.5.3 it remains to analyze the functions $\mathbf{\Lambda}, \mathbf{\Lambda}_2$, which will be done in Section 2.6.

2.5.1 Tree updates

We prove Theorem 2.5.3 by analyzing one step of a certain Markov chain. To define the chain we require a certain update function for colorings on trees, which we now describe.

Definition 2.5.4. A *directed tree* is a bipartite tree $\boldsymbol{n}$ rooted at an edge $e_\circ$ which has a single incident vertex $x_\circ$. All edges e of $\boldsymbol{n}$ are labelled with literals $\mathtt{L}_e \in \{\mathtt{0}, \mathtt{1}\}$. We let $\mathcal{L}(\boldsymbol{n})$ denote the boundary edges of $\boldsymbol{n}$ other than $e_\circ$. We call $\boldsymbol{n}$ a *variable-to-clause tree* if $x_\circ$ is a variable; otherwise we call it a *clause-to-variable tree*. We say that $\underline{\sigma} \in \Omega^{E(\boldsymbol{n})}$ is a valid T-coloring of the tree $\boldsymbol{n}$ if the weight

$$\boldsymbol{w}^{\text{lit}}_{\boldsymbol{n},T}(\underline{\sigma}) \equiv \prod_{v \in V(\boldsymbol{n})} \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a \in F(\boldsymbol{n})} \hat{\Phi}^{\text{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a}) \prod_{e \in E(\boldsymbol{n})} \bar{\Phi}_T(\sigma_e)$$

is positive.

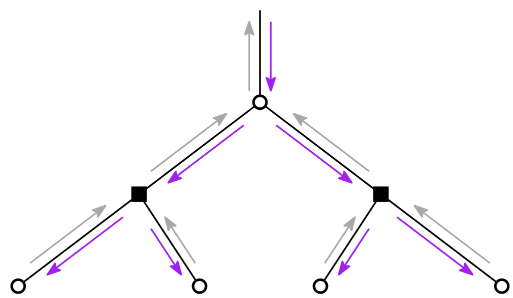


Figure 2.5.1: A variable-to-clause tree $\boldsymbol{n}$ (Definition 2.5.4).

We always visualize the tree $\boldsymbol{n}$ as in Figure 2.5.1, with the root edge at the top, so that paths leaving the root travel downwards. On an edge $e = (av)$, the *upward color* is $\dot{\sigma}_{av}$ if a lies above v, and $\hat{\sigma}_{av}$ if v lies above a. Now suppose $\underline{\sigma}$ is a valid T-coloring of a directed tree $\boldsymbol{n}$ with root spin $\sigma_{e_\circ} = \sigma$, and consider updating to a new root spin $\zeta \in \Omega_T$. If σ and ζ agree in the upward direction of $e_\circ$, then there is a unique valid coloring

$$\underline{\zeta} = \mathsf{update}(\underline{\sigma}, \zeta; \boldsymbol{n}) \in \Omega^{E(\boldsymbol{n})}$$

which has root spin ζ, and agrees with $\underline{\sigma}$ in all the upward colors. Indeed, the only possibility for $\sigma \neq \zeta$ is that both $\sigma, \zeta \in \Omega_{\mathtt{f}}$. It is then clear that $\mathsf{update}(\underline{\sigma}, \zeta; \boldsymbol{n})$ is uniquely defined by recursively applying the mappings $\dot{\mathtt{T}}$ and $\hat{\mathtt{T}}$, starting from the root and continuing downwards.

Since we assumed that $\underline{\sigma}$ was a valid T-coloring and $\zeta \in \Omega_T$, it is easy to verify that the resulting $\underline{\zeta}$ is also a valid T-coloring, so the update procedure respects the restriction to Ω_T. From now on we assume all edge colors belong to Ω_T, and for the most part we drop T from the notation.

Lemma 2.5.5. *If $\underline{\sigma}$ is a valid coloring of the directed tree $\boldsymbol{n}$, and $\underline{\zeta} = \mathsf{update}(\underline{\sigma}, \zeta; \boldsymbol{n})$ agrees with $\underline{\sigma}$ on the boundary edges $\mathcal{L}(\boldsymbol{n})$, then*

$$\boldsymbol{w}_{\boldsymbol{n}}^{\text{lit}}(\underline{\sigma}) = \boldsymbol{w}_{\boldsymbol{n}}^{\text{lit}}(\underline{\zeta}).$$

Proof. For each vertex $x \in \boldsymbol{n}$, let $e(x)$ denote the parent edge of x (the unique edge of $\boldsymbol{n}$ which lies above x). We then have

$$\boldsymbol{w}_{\boldsymbol{n}}^{\text{lit}}(\underline{\sigma}) = \prod_{e \in \mathcal{L}(\boldsymbol{n})} \bar{\Phi}(\sigma_e) \prod_{v \in V(\boldsymbol{n})} \Big\{ \dot{\Phi}(\underline{\sigma}_{\delta v}) \bar{\Phi}(\sigma_{e(v)}) \Big\} \prod_{a \in F(\boldsymbol{n})} \Big\{ \hat{\Phi}^{\text{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a}) \bar{\Phi}(\sigma_{e(a)}) \Big\}.$$

For a variable v in $\boldsymbol{n}$ with $e(v) = e$, it follows from (2.3.3) that

$$\dot{\Phi}(\underline{\sigma}_{\delta v}) \bar{\Phi}(\sigma_e) = \dot{z}(\dot{\sigma}_e) = \dot{z}(\dot{\zeta}_e) = \dot{\Phi}(\underline{\zeta}_{\delta v}) \bar{\Phi}(\zeta_e).$$

Likewise, at a clause a in $\boldsymbol{n}$ with $e(a) = e$, it follows from (2.3.3) that

$$\hat{\Phi}^{\text{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a}) \bar{\Phi}(\underline{\sigma}_e) = \hat{z}(\hat{\sigma}_e) = \hat{z}(\hat{\zeta}_e) = \hat{\Phi}^{\text{lit}}((\underline{\zeta} \oplus \underline{\mathtt{L}})_{\delta a}) \bar{\Phi}(\zeta_e).$$

Recalling that $\underline{\sigma}$ and $\underline{\zeta}$ agree on $\mathcal{L}(\boldsymbol{n})$, we have $\boldsymbol{w}_{\boldsymbol{n}}^{\text{lit}}(\underline{\sigma}) = \boldsymbol{w}_{\boldsymbol{n}}^{\text{lit}}(\underline{\zeta})$ as claimed. $\square$

Lemma 2.5.6. *Let $\dot{M}, \hat{M}$ be as defined in Corollary 2.3.8, and let $\dot{M}_2, \hat{M}_2$ be their analogues in the pair model. For any $\sigma, \sigma' \in \Omega$ there exists an integer-valued vector $(\dot{H}, \hat{H})$ so that*

$$\langle \mathbf{1}, \dot{H} \rangle = 0 = \langle \mathbf{1}, \hat{H} \rangle \quad \text{and} \quad \dot{M}\dot{H} - \hat{M}\hat{H} = \mathbf{1}_\sigma - \mathbf{1}_{\sigma'},$$

where $\mathbf{1}$ denotes the all-ones vector, and $\mathbf{1}_\sigma$ denotes the vector which is one in the σ coordinate and zero elsewhere. The analogous statement holds for $(\dot{M}_2, \hat{M}_2)$.

Proof. We define a graph on Ω by putting an edge between σ and σ' if there exist valid colorings $\underline{\sigma}, \underline{\sigma}'$ on some directed tree $\boldsymbol{n}$ which take values σ, σ' on the root edge $e_\circ$, but agree on the boundary edges $\mathcal{L}(\boldsymbol{n})$. If σ, σ' are connected in this way, then taking

$$\dot{H}(\zeta) = \sum_{v \in V(\boldsymbol{n})} \mathbf{1}\{\underline{\sigma}_{\delta v} = \zeta\} - \sum_{v \in V(\boldsymbol{n})} \mathbf{1}\{(\underline{\sigma}')_{\delta v} = \zeta\},$$
$$\hat{H}(\xi) = \sum_{a \in F(\boldsymbol{n})} \mathbf{1}\{\underline{\sigma}_{\delta a} = \xi\} - \sum_{a \in F(\boldsymbol{n})} \mathbf{1}\{(\underline{\sigma}')_{\delta a} = \xi\}.$$

gives $\dot{M}\dot{H} - \hat{M}\hat{H} = \mathbf{1}_\sigma - \mathbf{1}_{\sigma'}$ as required. It therefore suffices to show that the graph we have defined on Ω is connected (hence complete).

If $\dot{\sigma} = \dot{\sigma}'$, it is clear that σ and σ' can be connected via colorings $\underline{\sigma}, \underline{\sigma}'$ of some variable-to-clause tree $\boldsymbol{n}$, with $\underline{\sigma}' = \mathtt{update}(\underline{\sigma}, \zeta; \boldsymbol{n})$. Similarly, if $\hat{\sigma} = \hat{\sigma}'$, then σ and σ' can be connected using a clause-to-variable tree. This implies that $\Omega_{\mathtt{f}}$ is connected.

Next, it is also easy to see that if $\sigma = \mathtt{r}_x$ and $\sigma' = \mathtt{b}_x$, then they can be connected via a depth-one variable-to-clause tree. Similarly, if $\sigma = \mathtt{b}_x$ and $\sigma' = (\dot{\tau}, \square)$ for any $\dot{\tau} \in \dot{\Omega}_{\mathtt{f}}$, then they can be connected via a depth-one clause-to-variable tree. It follows that Ω is indeed connected, which proves the assertion concerning $(\dot{M}, \hat{M})$. The proof for $(\dot{M}_2, \hat{M}_2)$ is very similar. ☐

2.5.2 Markov chain

We now define a Markov chain on tuples $(\mathscr{G}, \underline{\sigma}, Y)$ where $\mathscr{G} = (V, F, E)$ is a (d,k)-regular NAE-SAT instance, $\underline{\sigma}$ is a valid T-coloring on $\mathscr{G}$, and $Y \subseteq V$ is a subset of variables such that

(i) for all $v \in Y$, the neighborhood $B_{2T}(v)$ is a tree, and
(ii) each pair of variables $v \neq v'$ in Y lies at graph distance at least $4T$. (2.5.1)

(Recall that each variable-clause edge is defined to have length $\frac{1}{2}$.) For $v \in Y$ let $\mathscr{N}(v)$ denote the depth-one neighborhood of v, excluding the variables at unit distance from v. Let $\mathscr{N} \equiv \mathscr{N}(Y)$ denote the (disjoint) union of the graphs $\mathscr{N}(v)$, $v \in Y$:

$$\mathscr{N} = (\mathcal{N}, \underline{\mathtt{L}}_{\mathcal{N}})$$

where $\mathcal{N}$ denotes the graph without the edge literals, and $\underline{\mathtt{L}}_{\mathcal{N}}$ denotes the vector of $|Y|dk$ edge literals. Let $\underline{\sigma}_{\mathcal{N}}$ be the restriction of $\underline{\sigma}$ to the edges incident to vertices of $\mathcal{N}$, and define

$$\boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\sigma}_{\mathcal{N}} | \underline{\mathtt{L}}_{\mathcal{N}}) \equiv \boldsymbol{w}^{\mathrm{lit}}_{\mathscr{N}}(\underline{\sigma}_{\mathcal{N}}) \equiv \prod_{v \in Y} \left\{ \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{e \in \delta v} \left\{ \hat{\Phi}^{\mathrm{lit}}((\underline{\sigma} \oplus \underline{\mathtt{L}})_{\delta a(e)}) \bar{\Phi}(\sigma_e) \right\} \right\}.$$

Let V_∂ denote the vertices of $G\backslash\mathcal{N}$ (including the variables at unit distance from Y), and let F_∂ denote the clauses of $G\backslash\mathcal{N}$. Let E_∂ denote the set of all edges incident to $V_\partial \cup F_\partial$, and let $\underline{\sigma}_\partial$ denote the restriction of $\underline{\sigma}$ to E_∂. Define

$$\boldsymbol{w}_\partial^{\text{lit}}(\underline{\sigma}_\partial) \equiv \prod_{v\in V_\partial} \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a\in F_\partial} \hat{\Phi}^{\text{lit}}((\underline{\sigma} \oplus \underline{\mathsf{L}})_{\delta a}) \prod_{e\in E_\partial} \bar{\Phi}(\sigma_e).$$

Then the overall weight $\boldsymbol{w}_{\mathscr{G}}^{\text{lit}}(\underline{\sigma})$ of $\underline{\sigma}$ factorizes as

$$\boldsymbol{w}_{\mathscr{G}}^{\text{lit}}(\underline{\sigma}) = \boldsymbol{w}_\partial^{\text{lit}}(\underline{\sigma}_\partial)\boldsymbol{w}_{\mathcal{N}}^{\text{lit}}(\underline{\sigma}_{\mathcal{N}}|\underline{\mathsf{L}}_{\mathcal{N}}). \tag{2.5.2}$$

Let $\delta\mathcal{N}$ denote the boundary edges of $\mathcal{N}$, and let $\dot{h}^{\text{tree}}(\underline{\sigma}_{\delta\mathcal{N}})$ be the empirical measure of the spins $(\dot{\sigma}_e)_{e\in\delta\mathcal{N}}$. Given initial state $(\mathscr{G}, \underline{\sigma}, Y)$, we take one step of the Markov chain as follows:

1. Sample a new pair $(\underline{\mathsf{L}}'_{\mathcal{N}}, \underline{\zeta}_{\mathcal{N}})$ from the probability measure

$$p((\underline{\mathsf{L}}'_{\mathcal{N}}, \underline{\zeta}_{\mathcal{N}}) \,|\, (\underline{\mathsf{L}}_{\mathcal{N}}, \underline{\sigma}_{\mathcal{N}})) = \frac{1}{z}\mathbf{1}\{\dot{h}^{\text{tree}}(\underline{\sigma}_{\delta\mathcal{N}}) = \dot{h}^{\text{tree}}(\underline{\zeta}_{\delta\mathcal{N}})\}\boldsymbol{w}_{\mathcal{N}}^{\text{lit}}(\underline{\zeta}_{\mathcal{N}}|\underline{\mathsf{L}}'_{\mathcal{N}})^\lambda$$

   where z denotes the normalizing constant, which depends on $|\mathcal{N}|$ and $\dot{h}^{\text{tree}}(\underline{\sigma}_{\delta\mathcal{N}})$.

2. If $e = (\dot{e}, \hat{e})$ then denote

$$\dot{\sigma}_e \equiv \dot{\sigma}(\dot{e}) \equiv \dot{\sigma}(\hat{e}).$$

   Each edge $e \in E$ pairs some $\dot{e}_i$ with some $\hat{e}_{\mathfrak{m}(i)}$, for some permutation $\mathfrak{m} : [nd] \to [nd]$. Let B denote the subset of indices $i \in [nd]$ such that $(\dot{e}_i, \hat{e}_{\mathfrak{m}(i)}) \in \delta\mathcal{N}$. Now consider the set $\mathcal{M} = \mathcal{M}(\mathscr{G}, Y, \underline{\sigma}, \underline{\zeta})$ of permutations $\mathfrak{m}' : [nd] \to [nd]$ such that

$$\mathfrak{m}'(i) = \mathfrak{m}(i) \text{ for all } i \in [nd]\backslash B, \quad \dot{\sigma}(\dot{e}_i) = \dot{\zeta}(\hat{e}_{\mathfrak{m}'(i)}) \text{ for all } i \in B. \tag{2.5.3}$$

   Sample $\mathfrak{M}$ uniformly at random from $\mathcal{M}$. Let $\mathscr{G}'$ be the new graph formed from $\mathscr{G}$ by replacing $\underline{\mathsf{L}}_{\mathcal{N}}$ with $\underline{\mathsf{L}}'_{\mathcal{N}}$, and replacing $\mathfrak{m}$ with $\mathfrak{M}$.

3. For each $e \in \delta\mathcal{N}$, let $\boldsymbol{n}(e)$ denote the depth-$2T$ neighborhood of $v(e)$ in the graph $\mathscr{G}\backslash\{a(e)\}$, including the edge e which we regard as the root of $\boldsymbol{n}(e)$. Let

$$\underline{\zeta}_{\boldsymbol{n}(e)} \equiv \mathsf{update}(\underline{\sigma}_{\boldsymbol{n}(e)}, \zeta_e; \boldsymbol{n}(e));$$

   note that, since $\underline{\sigma}$ is a valid T-coloring, $\underline{\zeta}_{\boldsymbol{n}(e)}$ and $\underline{\sigma}_{\boldsymbol{n}(e)}$ must agree at the boundary of $\boldsymbol{n}(e)$. For any edge e' which does not appear in $\mathcal{N}$ or any of the trees $\boldsymbol{n}(e)$, define $\zeta_{e'} = \sigma_{e'}$.

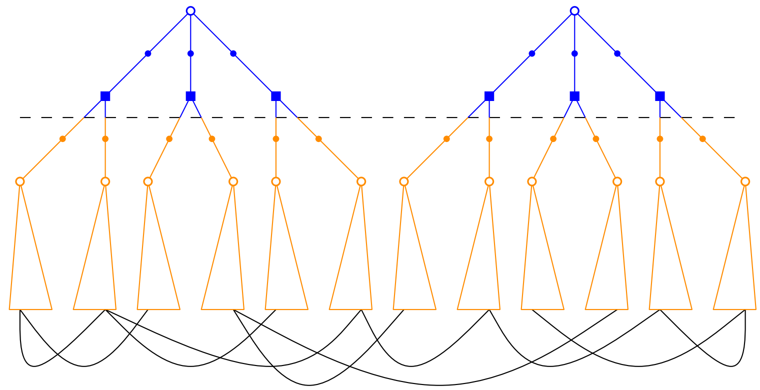
The state of the Markov chain after one step is $(\mathscr{G}', \underline{\zeta}, Y)$. See Figure 2.5.2.

Lemma 2.5.7. *Suppose we have a measure $\mathbb{P}(Y|\mathscr{G})$ such that, whenever the tuples $(\mathscr{G}, Y, \underline{\sigma})$ and $(\mathscr{G}', Y, \underline{\zeta})$ belong to the same orbit of the Markov chain, it holds that*

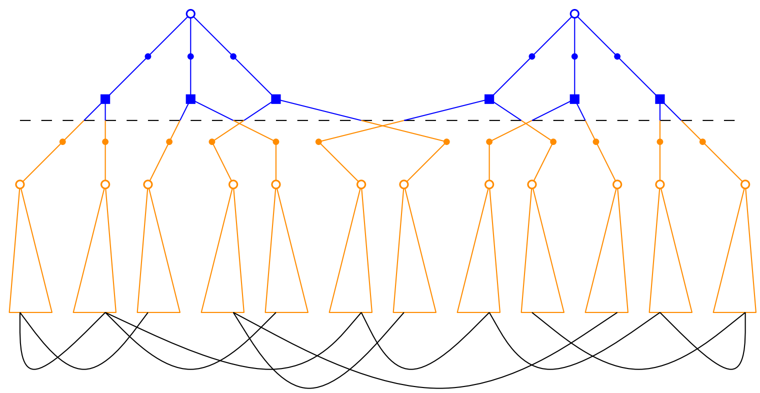
$$\mathbb{P}(Y|\mathscr{G}) = \mathbb{P}(Y|\mathscr{G}'). \tag{2.5.4}$$

A reversing measure for the Markov chain is then given by

$$\mu(\mathscr{G}, \underline{\sigma}, Y) = \mathbb{P}(\mathscr{G})\mathbb{P}(Y|\mathscr{G})\boldsymbol{w}_{\mathscr{G}}^{\text{lit}}(\underline{\sigma})^\lambda$$



(a) $(\mathscr{G}, Y, \underline{\sigma})$



(b) $(\mathscr{G}', Y, \underline{\sigma}')$

Figure 2.5.2: $(\mathscr{G}, Y, \underline{\sigma})$ to $(\mathscr{G}', Y, \underline{\sigma}')$.

Proof. Started from $\mathrm{A} = (\mathscr{G}, \underline{\sigma}, Y)$, let $\pi(\mathrm{A}, \mathrm{B})$ denote the chance to reach state $\mathrm{B} = (\mathscr{G}', \underline{\zeta}, Y)$ in one step of the Markov chain:

$$\pi(\mathrm{A}, \mathrm{B}) = \frac{p((\underline{\mathrm{L}}'_{\mathcal{N}}, \underline{\zeta}_{\mathcal{N}}) \,|\, (\underline{\mathrm{L}}_{\mathcal{N}}, \underline{\sigma}_{\mathcal{N}}))}{|} \mathcal{M}(\mathrm{A}, \mathrm{B})|$$

for $\mathcal{M}$ as defined in (2.5.3). The size of $\mathcal{M}$ can be expressed as a function of $(|Y|, \dot{h})$ only, so $|\mathcal{M}(\mathrm{A}, \mathrm{B})| = |\mathcal{M}(\mathrm{B}, \mathrm{A})|$. It follows that

$$\begin{aligned} \frac{\mu(\mathrm{A})\pi(\mathrm{A}, \mathrm{B})}{\mu(\mathrm{B})\pi(\mathrm{B}, \mathrm{A})} &= \frac{\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G}}(\underline{\sigma})^{\lambda}}{\boldsymbol{w}^{\mathrm{lit}}_{\mathscr{G}}(\underline{\zeta})^{\lambda}} \frac{p((\underline{\mathrm{L}}'_{\mathcal{N}}, \underline{\zeta}_{\mathcal{N}}) \,|\, (\underline{\mathrm{L}}_{\mathcal{N}}, \underline{\sigma}_{\mathcal{N}}))}{p((\underline{\mathrm{L}}_{\mathcal{N}}, \underline{\sigma}_{\mathcal{N}}) \,|\, (\underline{\mathrm{L}}'_{\mathcal{N}}, \underline{\zeta}_{\mathcal{N}}))} \\ &= \frac{\boldsymbol{w}^{\mathrm{lit}}_{\partial}(\underline{\sigma}_{\partial})^{\lambda} \boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\sigma}_{\mathcal{N}} | \underline{\mathrm{L}}_{\mathcal{N}})^{\lambda} \boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\zeta}_{\mathcal{N}} | \underline{\mathrm{L}}'_{\mathcal{N}})^{\lambda}}{\boldsymbol{w}^{\mathrm{lit}}_{\partial}(\underline{\zeta}_{\partial})^{\lambda} \boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\zeta}_{\mathcal{N}} | \underline{\mathrm{L}}'_{\mathcal{N}})^{\lambda} \boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\sigma}_{\mathcal{N}} | \underline{\mathrm{L}}_{\mathcal{N}})^{\lambda}} = \frac{\boldsymbol{w}^{\mathrm{lit}}_{\partial}(\underline{\sigma}_{\partial})^{\lambda}}{\boldsymbol{w}^{\mathrm{lit}}_{\partial}(\underline{\zeta}_{\partial})^{\lambda}}, \end{aligned}$$

using (2.5.2). It follows from Lemma 2.5.5 that this ratio equals one, which proves reversibility. (We remark that since the Markov chain breaks up into many disjoint orbits, the reversing measure is not unique.) $\square$

Let A be any subset of the state space, and let B denote the set of states reachable from A in one step of the chain. Then reversibility implies

$$\mu(A) = \sum_{\mathrm{A}\in A}\sum_{\mathrm{B}\in B}\mu(\mathrm{A})\pi(\mathrm{A},\mathrm{B}) = \sum_{\mathrm{A}\in A}\sum_{\mathrm{B}\in B}\mu(\mathrm{B})\pi(\mathrm{B},\mathrm{A}) \leqslant \mu(B)\max_{\mathrm{B}\in B}\pi(\mathrm{B},A). \tag{2.5.5}$$

2.5.3 From graph to tree optimizations

Given $\mathscr{G} = (V, F, E)$, a valid coloring $\underline{\sigma}$ on $\mathscr{G}$, and a nonempty subset of variables $Y \subseteq V$, we define

$$H^{\mathrm{samp}} \equiv H^{\mathrm{samp}}(\mathscr{G}, \underline{\sigma}, Y) \equiv H^{\mathrm{samp}}(G, \underline{\sigma}, Y) \equiv (\dot{H}^{\mathrm{samp}}, \hat{H}^{\mathrm{samp}}, \bar{H}^{\mathrm{samp}})$$

which records the empirical distribution of $\underline{\sigma}$ near Y, as follows. For $v \in Y$ and $e \in \delta v$, let $1 \leqslant j(e) \leqslant k$ denote the index of e in $\delta a(e)$. Let

$$\begin{array}{lll} \dot{H}^{\mathrm{samp}}(\underline{\zeta}) & = |\{v \in Y : \underline{\sigma}_{\delta v} = \underline{\zeta}\}|/|Y|, & \underline{\zeta} \in \Omega^d, \\ \hat{H}^{\mathrm{samp}}(\underline{\xi}) & = |\{(v,e) : v \in Y, e \in \delta v, (\underline{\sigma}_{\delta a(e)})^{(j(e))} = \underline{\xi}\}|/(d|Y|), & \underline{\xi} \in \Omega^k, \\ \bar{H}^{\mathrm{samp}}(\zeta) & = |\{(v,e) : v \in Y, e \in \delta v, \sigma_e = \sigma\}|/(d|Y|), & \sigma \in \Omega, \end{array} \tag{2.5.6}$$

where $(\underline{\sigma}_{\delta a})^{(j)}$ is the rotation of $\underline{\sigma}_{\delta a}$ in which the j-th entry appears first (Definition 2.5.2). We then define $\dot{h} = \dot{h}^{\mathrm{tree}}(H^{\mathrm{samp}})$ as the empirical measure of $\dot{\sigma}$ on the edges $\delta a(e)\backslash e$, for $e \in \delta v$:

$$\dot{h}^{\mathrm{tree}}(\dot{\sigma}) = (k-1)^{-1}\sum_{\underline{\zeta}\in\Omega^k}\hat{H}(\underline{\zeta})\sum_{i=2}^{k}\mathbf{1}\{\dot{\zeta}_i = \dot{\sigma}\}, \quad \dot{\sigma} \in \dot{\Omega}.$$

It is clear that $H^{\mathrm{samp}}(\mathscr{G}, \underline{\sigma}, Y)$ can be expressed as a function of $\underline{\sigma}_{\mathcal{N}}$, and from now on we indicate this relation by

$$H^{\mathrm{samp}}(\mathscr{G}, \underline{\sigma}, Y) = H(\underline{\sigma}_{\mathcal{N}}).$$

Let $\mathbb{E}Z_{\mathcal{N}}(H^{\mathrm{samp}})$ denote the total weight of pairs $(\underline{\mathrm{L}}_{\mathcal{N}}, \underline{\sigma}_{\mathcal{N}})$ which are consistent with H^{samp}, normalized by the number of literal assignments:

$$\mathbb{E}Z_{\mathcal{N}}(H^{\mathrm{samp}}) \equiv \frac{1}{2^{|\mathcal{N}|dk}}\sum_{\underline{\sigma}_{\mathcal{N}}}\mathbf{1}\{H(\underline{\sigma}_{\mathcal{N}}) = H^{\mathrm{samp}}\}\sum_{\underline{\mathrm{L}}_{\mathcal{N}}}\boldsymbol{w}^{\mathrm{lit}}_{\mathcal{N}}(\underline{\sigma}_{\mathcal{N}}|\underline{\mathrm{L}}_{\mathcal{N}})^{\lambda}.$$

Clearly, this depends on $\mathcal{N}$ only through $s = |\mathcal{N}|$, so we denote $\mathbb{E}Z_s(H^{\mathrm{samp}}) \equiv \mathbb{E}Z_{\mathcal{N}}(H^{\mathrm{samp}})$. The following lemma gives an explicit calculation of $\mathbb{E}Z_s(H^{\mathrm{samp}})$.

Lemma 2.5.8. *With $\hat{\Phi}$ as in Remark 2.3.1,*

$$\mathbb{E}Z_s(H^{\mathrm{samp}}) = \frac{\binom{s}{s\dot{H}^{\mathrm{samp}}}\binom{ds}{ds\hat{H}^{\mathrm{samp}}}}{\binom{ds}{ds\bar{H}^{\mathrm{samp}}}}\dot{\Phi}^{\lambda s\dot{H}^{\mathrm{samp}}}\hat{\Phi}^{\lambda ds\hat{H}^{\mathrm{samp}}}\bar{\Phi}^{\lambda ds\bar{H}^{\mathrm{samp}}}.$$

This equals $s^{O(1)}\exp\{s\boldsymbol{\Lambda}(H^{\mathrm{samp}})\}$ where $\boldsymbol{\Lambda}$ is given by Definition 2.5.1, and is concave in H.

Proof. The first assertion follows by a straightforward combinatorial calculation (cf. (2.3.8)). Stirling's formula yields the asymptotic expansion $\mathbb{E}Z_s(H^{\mathrm{samp}}) = s^{O(1)}\exp\{s\mathbf{\Lambda}(H^{\mathrm{samp}})\}$. The function $\mathbf{\Lambda}(H)$ is the sum of $\mathbf{\Theta}(H)$ and the linear function $\boldsymbol{s}(H)\lambda$, and we claim that $\mathbf{\Theta}$ is concave. To see this, recall that $H = H^{\mathrm{samp}}$ must satisfy

$$\bar{H}(\sigma) = \sum_{\zeta\in\Omega^k} \hat{H}(\zeta)\mathbf{1}\{\zeta_1 = \sigma\}.$$

Let $\hat{H}_\sigma(\zeta)$ denote the probability of ζ under $\hat{H}$, conditioned on $\zeta_1 = \sigma$. Then

$$\mathbf{\Theta}(H) = \mathcal{H}(\dot{H}) + d\sum_{\sigma}\bar{H}(\sigma)\mathcal{H}(\hat{H}_\sigma) + \boldsymbol{v}(H).$$

The entropy function $\mathcal{H}$ is concave, so this proves that $\mathbf{\Theta}$ is indeed concave. ☐

Remark 2.5.9. An equivalent characterization of $\mathbf{\Lambda}$ is as follows. Recall that $\mathcal{N}$ consists of s disjoint trees $\mathcal{N}(v_1),\ldots,\mathcal{N}(v_s)$ where each $\mathcal{N}(v_s)$ is a copy of the depth-one tree $\mathcal{D}$ depicted in Figure 2.5.3. We use $\mathcal{L}(\mathcal{D})$ to denote the set of boundary edges $e \in \delta a\backslash(av)$, $a \in \partial v$, so $|\mathcal{L}(\mathcal{D})| = d(k-1)$. Both $\mathcal{N}$ and $\mathcal{D}$ do not include edge literals. The natural weight function on colorings of $\mathcal{D}$ is defined by

$$\boldsymbol{w}_{\mathcal{D}}(\underline{\sigma}_{\mathcal{D}}) = \dot{\Phi}(\underline{\sigma}_{\delta v})\prod_{e\in\delta v}\left\{\bar{\Phi}(\sigma_e)\hat{\Phi}(\underline{\sigma}_{\delta a(e)})\right\},$$

where $\hat{\Phi}$ is as in Remark 2.3.1. If ν is a probability measure over colorings $\underline{\sigma}_{\mathcal{D}}$, then we denote $H(\nu) = (\dot{H},\hat{H},\bar{H})$ where (cf. (2.5.6))

$$\dot{H}(\zeta) = \nu(\underline{\sigma}_{\delta v} = \zeta),\ \ \hat{H}(\xi) = d^{-1}\sum_{e\in\delta v}\nu((\underline{\sigma}_{\delta a(e)})^{j(e)} = \xi),\ \ \bar{H}(\sigma) = d^{-1}\sum_{e\in\delta v}\nu(\sigma_e = \sigma).$$

Let $Z_s(\nu)$ be the contribution to $Z_s(H^{\mathrm{samp}})$ from colorings $\underline{\sigma}_{\mathcal{N}}$ with empirical measure ν — that is, colorings $\underline{\sigma}_{\mathcal{N}}$ satisfying $s\nu(\underline{\sigma}_{\mathcal{D}}) = |\{i\in[s] : \underline{\sigma}_{\mathcal{N}(v_i)} = \underline{\sigma}_{\mathcal{D}}\}|$ for all $\underline{\sigma}_{\mathcal{D}}$. Using multi-index notation as before, we have

$$\mathbb{E}Z_s(\nu) = \binom{s}{s\nu}(\boldsymbol{w}_{\mathcal{D}})^{\lambda\nu} = s^{O(1)}\exp\{\mathcal{H}(\nu) + \lambda\langle\ln\boldsymbol{w}_{\mathcal{D}},\nu\rangle\}.$$

Summing over all ν such that $s\nu$ is integer-valued and $H(\nu) = H^{\mathrm{samp}}$ gives

$$\mathbb{E}Z_s(H^{\mathrm{samp}}) = \sum_{\nu}\mathbb{E}Z_s(\nu) = s^{O(1)}\exp\{n\mathbf{\Lambda}(H^{\mathrm{samp}})\}$$

for the following alternative equivalent of $\mathbf{\Lambda}$:

$$\mathbf{\Lambda}(H^{\mathrm{samp}}) = \sup\{\mathcal{H}(\nu) + \lambda\langle\ln\boldsymbol{w}_{\mathcal{D}},\nu\rangle : H(\nu) = H^{\mathrm{samp}}\}.$$

This representation also explains clearly why $\mathbf{\Lambda}$ is concave. Lastly, note we can express $\mathbf{\Lambda}^{\mathrm{opt}}$ similarly as $\mathbf{\Lambda}^{\mathrm{opt}}(\dot{h}) = \sup\{\mathcal{H}(\nu) + \lambda\langle\ln\boldsymbol{w}_{\mathcal{D}},\nu\rangle : \dot{h}^{\mathrm{tree}}(H(\nu)) = H^{\mathrm{samp}}\}$.

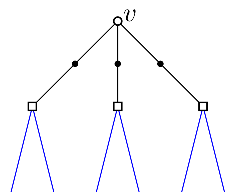


Figure 2.5.3: The depth-one tree $\mathcal{D}$, rooted at variable v.

Proposition 2.5.10. *Let $A(H)$ be the set of tuples $(\mathscr{G}, \underline{\sigma}, Y)$ such that $\underline{\sigma}$ is a valid T-coloring on $\mathscr{G}$ with empirical measure H, and Y is a subset of V satisfying (2.5.1) as well as*

$$n\epsilon \leqslant |Y| \leqslant 6n\epsilon \text{ and } \|H^{\text{samp}}(\mathscr{G}, \underline{\sigma}, Y) - H^{\text{sym}}\| \leqslant (\ln\ln n)^{-1/2}.$$

Suppose we define an exceptional set of graphs $\mathscr{B}$ with $\mathbb{P}(\mathscr{B}) \leqslant \exp\{-n(\ln n)^{1/2}\}$, and a law $\mathbb{P}(Y|\mathscr{G})$ such that for all $\mathscr{G} \notin \mathscr{B}$ and all $\underline{\sigma}$ with $H(\mathscr{G}, \underline{\sigma}) = H$, we have

$$\mathbb{P}(A(H) \,|\, (\mathscr{G}, \underline{\sigma})) = \sum_Y \mathbb{P}(Y|\mathscr{G}) \mathbf{1}\{(\mathscr{G}, \underline{\sigma}, Y) \in A(H)\} \geqslant \tfrac{1}{2}. \tag{2.5.7}$$

Then the expected weight of colorings with empirical measure H satisfies

$$\mathbb{E}\boldsymbol{Z}(H) \leqslant \frac{e^{o_n(1)} \max\{\mathbb{E}\boldsymbol{Z}(H') : \|H' - H\|_1 \leqslant \epsilon(dk)^{2T}\}}{\exp\{n\epsilon \min\{\boldsymbol{\Xi}(H'') : \|H'' - H^{\text{sym}}\|_1 \leqslant (\ln\ln n)^{-1/2}\}\}}.$$

Proof. Since $\boldsymbol{Z}(H) \leqslant 2^n$,

$$\mathbb{E}\boldsymbol{Z}(H) \leqslant \mathbb{E}[\boldsymbol{Z}(H); \mathscr{G} \notin \mathscr{B}] + \exp\{-\Omega(n(\ln n)^{1/2})\}.$$

Since we only consider measures H for which $\boldsymbol{F}(H) > -\infty$, the right-hand side above is dominated by the contribution from $\mathscr{G} \notin \mathscr{B}$. Next recall from Lemma 2.5.7 the reversing measure $\mu(\mathscr{G}, \underline{\sigma}, Y)$. Applying assumption (2.5.7),

$$\mathbb{E}\boldsymbol{Z}(H) \leqslant 2\mathbb{E}[\boldsymbol{Z}(H); \mathscr{G} \notin \mathscr{B}] = 2 \sum_{\mathscr{G} \notin \mathscr{B}} \mathbb{P}(\mathscr{G}) \sum_{\underline{\sigma}} \boldsymbol{w}^{\text{lit}}_{\mathscr{G}}(\underline{\sigma})^{\lambda} \leqslant 4\mu(A(H)).$$

We now apply (2.5.5), writing $B(H)$ for the set of states $\text{B} = (\mathscr{G}', \underline{\sigma}', Y')$ reachable from $A(H)$ in one step of the Markov chain. First note that if $\text{B} \in B(H)$ then $H' = H(\mathscr{G}', \underline{\sigma}', Y')$ must satisfy (crudely) $\|H' - H\| \leqslant \epsilon(dk)^{2T}$, so summing over the $\epsilon(dk)^{2T}$-neighborhood of H,

$$\mu(B(H)) \leqslant s^{O(1)} \max\{\mathbb{E}\boldsymbol{Z}(H') : \|H' - H\| \leqslant \epsilon(dk)^{2T}\}.$$

Next, writing $s = |Y'|$, we have

$$\pi(\text{B}, A(H)) = \frac{Z_s(H^{\text{samp}})}{\sum_{H''} Z_s(H'')\mathbf{1}\{\dot{h}^{\text{tree}}(H'') = \dot{h}^{\text{tree}}(H^{\text{samp}})\}},$$

where H'' represents $H^{\text{samp}}(\mathscr{G}', \underline{\sigma}', Y')$. Applying Lemma 2.5.8 gives

$$\pi(\text{B}, A(H)) \leqslant s^{O(1)} \exp\{s[\boldsymbol{\Lambda}(H^{\text{samp}}) - \boldsymbol{\Lambda}^{\text{opt}}(\dot{h}^{\text{tree}}(H^{\text{samp}}))]\}.$$

Recalling $\|H^{\text{samp}} - H^{\text{sym}}\| \leqslant (\ln\ln n)^{-1/2}$ and $n\epsilon \leqslant s \leqslant 6n\epsilon$, the result follows. $\square$

2.5.4 Sampling

We now define the law $\mathbb{P}(Y|\mathscr{G})$ and verify condition (2.5.7). To this end, given $\mathscr{G} = (V, F, E)$, let $V_t \subseteq V$ be the subset of variables $v \in V$ such that the t-neighborhood $B_t(v)$ around v is a tree. Recall the following form of the Chernoff bound: if X is a binomial random variable with mean μ, then for all $t \geqslant 1$ we have

$$\mathbb{P}(X \geqslant t\mu) \leqslant \exp\{-t\mu \ln(t/e)\}. \tag{2.5.8}$$

Lemma 2.5.11. *If $\mathscr{G} = (V, F, E)$ is sampled from the (d, k)-regular configuration model, then for any fixed t it holds for $n \geqslant n_\circ(t)$ that*

$$\mathbb{P}(|V\backslash V_t| \geqslant n(\ln\ln n)^{-1}) \leqslant \exp\{-n(\ln n)^{1/2}\}.$$

Proof. Let γ count the total number of cycles in $\mathscr{G}$ of length at most $2t$. If $v \notin V_t$ then v must certainly lie within distance t of one of these cycles, so crudely we have

$$|V\backslash V_t| \leqslant 2t(dk)^t\gamma. \tag{2.5.9}$$

Consider breadth-first search exploration in $\mathscr{G}$ started from an arbitrary variable, say $v = 1$. At each step of the exploration we reveal one edge, so the exploration takes nd steps total. Conditioned on everything revealed in the first t steps, the chance that the edge revealed at step $t + 1$ will form a new cycle of length $\leqslant 2t$ is upper bounded by

$$\frac{(dk)^{2t}}{nd - t}.$$

It follows that the total number of cycles revealed up to time $nd(1 - \delta)$ is stochastically dominated by a binomial random variable

$$\gamma' \sim \mathrm{Bin}\Big(nd(1-\delta), \frac{(dk)^{2t}}{nd\delta}\Big).$$

The final $nd\delta$ exploration steps can form at most $nd\delta$ new cycles, so $\gamma \leqslant \gamma' + nd\delta$. Applying (2.5.8) with $\delta = (\ln\ln n)^{-2}$,

$$\mathbb{P}(\gamma \geqslant 2nd\delta) \leqslant \mathbb{P}(\gamma' \geqslant nd\delta) \leqslant \exp\Big\{-nd\delta \ln \frac{nd\delta^2}{e(dk)^{2t}}\Big\} \leqslant \exp\{-n(\ln n)^{1/2}\}$$

for large enough n. Recalling (2.5.9) gives the claimed bound. □

Recalling Proposition 2.5.10, let $\mathscr{B}$ be the set of graphs $\mathscr{G}$ for which $|V\backslash V_t| \geqslant n/2$. For $\mathscr{G} \notin \mathscr{B}$, take i.i.d. random variables $I_v \sim \mathrm{Ber}(\epsilon')$ indexed by $v \in V_t$ for some ϵ' to be determined, and let

$$Y_v \equiv \mathbf{1}\{I_v = 1, \text{ and } I_u = 0 \text{ for all } u \in B_t(v)\backslash\{v\}\}, \quad \epsilon \equiv \tfrac{1}{2}\mathbb{E}Y_v. \tag{2.5.10}$$

We define $\mathbb{P}(Y|\mathscr{G})$ to be the law of the set $Y = \{v \in V_t : Y_v = 1\}$, with $t = 4T$. Given a valid coloring $\underline{\sigma}$ on $\mathscr{G} = (V, F, E)$, define (cf. (2.5.6))

$$\begin{array}{lll} \dot{X}_v(\zeta) & \equiv \mathbf{1}\{\underline{\sigma}_{\delta v} = \zeta\}, & \zeta \in \Omega^d, \\ \hat{X}_v(\xi) & \equiv |\{e \in \delta v : (\underline{\sigma}_{\delta a(e)})^{j(e)} = \xi\}|, & \xi \in \Omega^k, \\ \bar{X}_v(\sigma) & \equiv |\{(a, e) : a \in \partial v, e \in \delta a \backslash (av), \sigma_e = \sigma\}|, & \sigma \in \Omega. \end{array}$$

Lemma 2.5.12. *Fix $(\mathscr{G}, \underline{\sigma})$ and let $n' = |V_t| < n/2$. Then for all $x > 4|n - n'|$ we have the concentration bounds*

$$\mathbb{P}\Big(\Big| \sum_{v \in V_t} Y_v - n'\epsilon \Big| \geqslant x\Big) \leqslant \exp\Big\{ - \frac{x^2}{8n'(dk)^{2t}} \Big\}$$

$$\mathbb{P}\Big(\Big| \sum_{v \in V_t} Y_v \dot{X}_v(\zeta) - n'\epsilon \dot{H}(\zeta) \Big| \geqslant x\Big) \leqslant \exp\Big\{ - \frac{x^2}{8n'(dk)^{2t}} \Big\}$$

$$\mathbb{P}\Big(\Big| \frac{1}{d} \sum_{v \in V_t} Y_v \hat{X}_v(\xi) - n'\epsilon \hat{H}^{\mathrm{sym}}(\xi) \Big| \geqslant x\Big) \leqslant \exp\Big\{ - \frac{x^2}{8n'(dk)^{2t+1}} \Big\}$$

$$\mathbb{P}\Big(\Big| \frac{1}{d(k-1)} \sum_{v \in V_t} Y_v \bar{X}_v(\dot{\sigma}) - n'\epsilon \bar{H}(\sigma) \Big| \geqslant x\Big) \leqslant \exp\Big\{ - \frac{x^2}{8n'(dk)^{2t+1}} \Big\}$$

Proof. Assume without loss that $V_t = [n'] \equiv \{1, \ldots, n'\}$, and for $0 \leqslant s \leqslant n'$ let $\mathscr{F}_s$ denote the sigma-field generated by $Y_1, \ldots, Y_s$. Let

$$S \equiv \sum_{v \leqslant n'} A_v Y_v, \quad M_s \equiv \mathbb{E}[S|\mathscr{F}_s]$$

where we take different values of A_v for the various bounds:

$$A_v = 1,\ A_v = \dot{X}_v(\zeta),\ A_v = \hat{X}_v(\xi),\ A_v = \bar{X}_v(\sigma).$$

We emphasize that $\mathscr{G}$ and $\underline{\sigma}$ are fixed, so the only randomness is in the Y's:

$$M_s = \sum_{v \leqslant n'} A_v \mathbb{E}[Y_v|\mathscr{F}_s].$$

If v lies at distance greater than $2t$ from any variable in $[s] \equiv \{1, \ldots, s\}$, then

$$\mathbb{E}[Y_v|\mathscr{F}_s] = \mathbb{E}[Y_v] = 2\epsilon.$$

More generally, $\mathbb{E}[Y_v|\mathscr{F}_s]$ is a measurable function of all the Y_w values for $w \in [s] \cap B_{2t}(v)$. Therefore the only possibility for $\mathbb{E}[Y_v|\mathscr{F}_{s+1}] \neq \mathbb{E}[Y_v|\mathscr{F}_s]$ is that $[s+1] \cap B_{2t}(v)$ differs from $[s] \cap B_{2t}(v)$, which implies in particular that $v \in B_{2t}(s+1)$. The number of such v is at most $(dk)^t$, so we conclude

$$|M_{s+1} - M_s| \leqslant (dk)^t \|A\|_\infty.$$

It follows by the Azuma–Hoeffding martingale inequality that

$$\mathbb{P}(|S - \mathbb{E}S| \geqslant x) \leqslant \exp\Big\{ - \frac{x^2}{2n'(dk)^{2t}\|A\|_\infty}\Big\},$$

and the claimed bounds follow from the fact that removing $n - n' < n/2$ vertices from a graph can change the empirical measure by at most $2(n - n')/n$. □

Proof of Theorem 2.5.3. Take $\epsilon' > 0$ small enough such that the resulting ϵ defined by (2.5.10) satisfies $6\epsilon(dk)^{2T} < 1$. It then follows from Lemmas 2.5.11 and 2.5.12 that the conditions of Proposition 2.5.10 are satisfied by taking $\mathscr{B}$ to be the set of graphs with $|V\backslash V_t| \geqslant n(\ln\ln n)^{-1}$, and $\mathbb{P}(Y|\mathscr{G})$ to be the law of $Y = \{v \in V_t : Y_v = 1\}$, for Y_v as given by (2.5.10). □

2.6 Tree optimization problem

In this section we give the analysis of $\Xi(H)$ (Definition 2.5.1 and Theorem 2.5.3). Recall from (2.3.11) the definition of $\mathbf{N}_\circ$, and from (2.3.12) the definition of $H_\star$.

Proposition 2.6.1. *For Ξ, Ξ_2 as defined by (2.3.9) and (2.3.14), we have*

(a) On $\{H \in \mathbf{N}_\circ : H = H^{\mathrm{sym}}\}$, Ξ is uniquely minimized at $H = H_\star$, with $\Xi(H_\star) = 0$.

(b) On $\{H \in \mathbf{N}_{\mathrm{sep}} : H = H^{\mathrm{sym}}\}$, Ξ_2 is uniquely minimized at $H = H_\otimes$, with $\Xi_2(H_\otimes) = 0$.

Proposition 2.6.2. *There exists a positive constant $\epsilon = \epsilon(k)$ such that*

$$\begin{aligned} \Xi(H) &\geqslant \epsilon\|H - H_\star\|^2 \quad \text{for all } \|H - H_\star\| \leqslant \epsilon, \\ \Xi_2(H) &\geqslant \epsilon\|H - H_\otimes\|^2 \quad \text{for all } \|H - H_\otimes\| \leqslant \epsilon. \end{aligned}$$

2.6.1 Uniqueness of minimizer

We now outline the proof of Proposition 2.6.1. Let ν be any probability measure over colorings of the depth-one $\mathcal{D}$ (Figure 2.5.3). Recall from Remark 2.5.9 that

$$\begin{aligned} \mathbf{\Lambda}(H) &= \sup\{\mathcal{H}(\nu) + \lambda\langle \ln \boldsymbol{w}_\mathcal{D}, \nu\rangle : H(\nu) = H\}, \\ \mathbf{\Lambda}^{\mathrm{opt}}(\dot{h}) &= \sup\{\mathcal{H}(\nu) + \lambda\langle \ln \boldsymbol{w}_\mathcal{D}, \nu\rangle : \dot{h}^{\mathrm{tree}}(H(\nu)) = \dot{h}\}. \end{aligned}$$

The mappings $\nu \mapsto H(\nu)$ and $\nu \mapsto \dot{h}^{\mathrm{tree}}(H(\nu))$ are linear, so we are in the setting of Section 2.11. The discussion in that section (see in particular Remark 2.11.7) implies the following: there is a unique measure $\nu = \nu^{\mathrm{opt}}(\dot{h})$ achieving the maximum in $\mathbf{\Lambda}^{\mathrm{opt}}(\dot{h})$, and there exists a probability measure $\dot{q}$ on $\dot{\Omega}$ such that

$$\nu(\underline{\sigma}) = [\nu^{\mathrm{bd}}(\dot{q})](\underline{\sigma}) \equiv \frac{1}{Z}\Big\{\dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a \in \partial v}[\bar{\Phi}(\sigma_{av})\hat{\Phi}(\underline{\sigma}_{\delta a})]\Big\}^\lambda \prod_{e \in \mathcal{L}(\mathcal{D})} \dot{q}(\dot{\sigma}_e), \tag{2.6.1}$$

with Z the normalizing constant. Likewise, in the second moment there is a unique measure $\nu = \nu_2^{\mathrm{opt}}(\dot{h})$ achieving the maximum in $\mathbf{\Lambda}_2^{\mathrm{opt}}(\dot{h})$, and there exists a probability measure $\dot{q}$ on $\dot{\Omega}^2$ such that

$$\nu(\underline{\sigma}) = [\nu_2^{\mathrm{bd}}(\dot{q})](\underline{\sigma}) \equiv \frac{1}{Z}\Big\{\dot{\Phi}_2(\underline{\sigma}_{\delta v}) \prod_{a\in\partial v}[\bar{\Phi}_2(\sigma_{av})\hat{\Phi}_2(\underline{\sigma}_{\delta a})]\Big\}^{\lambda} \prod_{e\in\mathcal{L}(\mathcal{D})} \dot{q}(\dot{\sigma}_e). \tag{2.6.2}$$

In each case, although $\nu^{\mathrm{opt}}(\dot{h})$ is uniquely determined by $\dot{h}$, $\dot{q}$ need not be if the constraints are rank-deficient. Nevertheless we shall proceed simply from the existence of some $\dot{q}$.

Lemma 2.6.3. $\Xi(H_\star) = 0$ *and* $\Xi_2(H_\otimes) = 0$.

Lemma 2.6.4. *Zeroes of* Ξ, Ξ_2 *correspond to* BP *fixed points, as follows:*

(a) Suppose $\nu = \nu^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H)) = \nu^{\mathrm{bd}}(\dot{q})$, *and let* $\mu = \mu^{\mathrm{opt}}(H)$ *be the optimizer for* $\mathbf{\Lambda}(H)$. *If* $H \in \mathbf{N}_\circ$ *with* $H = H^{\mathrm{sym}}$ *and* $\Xi(H) = 0$, *then* $\mu = \nu$ *and* $\mathtt{BP}\dot{q} = \dot{q}$.

(b) Suppose $\nu = \nu_2^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H)) = \nu^{\mathrm{bd}}(\dot{q})$, *and let* $\mu = \mu_2^{\mathrm{opt}}(H)$ *be the optimizer for* $\mathbf{\Lambda}_2(H)$. *If* $H \in \mathbf{N}_{\mathrm{sep}}$ *with* $H = H^{\mathrm{sym}}$ *and* $\Xi_2(H) = 0$, *then* $\mu = \nu$ *and* $\mathtt{BP}\dot{q} = \dot{q}$.

Lemma 2.6.5. *The fixed points of Lemma 2.6.4 correpond to* $\dot{q}_\star$:

(a) If $H \in \mathbf{N}_\circ$ *and* $\nu = \nu^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H)) = \nu^{\mathrm{bd}}(\dot{q})$ *with* $\dot{q} = \mathtt{BP}\dot{q}$, *then* $\dot{q} = \dot{q}_\star$.

(b) If $H \in \mathbf{N}_{\mathrm{sep}}$ *and* $\nu = \nu_2^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H)) = \nu_2^{\mathrm{bd}}(\dot{q})$ *with* $\dot{q} = \mathtt{BP}\dot{q}$, *then* $\dot{q} = \dot{q}_\star \otimes \dot{q}_\star$.

Proof of Proposition 2.6.1. From Lemma 2.6.3, it suffices to show that if $H \in \mathbf{N}_\circ$ with $H = H^{\mathrm{sym}}$ and $\Xi(H) = 0$, then $H = H_\star$. From Lemmas 2.6.4 and 2.6.5, $\nu = \nu^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H))$ and $\mu = \mu^{\mathrm{opt}}(H)$ are equal, and can be expressed via (2.6.1) in terms of $\dot{q} = \dot{q}_\star$. It follows that $H = H(\mu) = H_\star$ as claimed. □

Proof of Lemma 2.6.3. As we noted above, $\nu^{\mathrm{opt}}(\dot{h})$ can be expressed via (2.6.1) in terms of $\dot{q}$, but $\dot{q}$ is not uniquely determined by $\dot{h}$ if the constraints are rank-deficient. However, if $\dot{h}$ is a strictly positive measure on $\dot{\Omega}$, then it is straightforward to check that the constraints are of full rank, so $\dot{q}$ is unique. Let $\nu_\star$ denote the measure given by (2.6.1) with $\dot{q} = \dot{q}_\star$. It is easy to check, from the proof of Proposition 2.4.2, that $\dot{q}_\star$ is fully supported on $\dot{\Omega}_T$. Therefore $H(\nu_\star) = H_\star$ and $\dot{h}^{\mathrm{tree}}(H(\nu_\star)) = \dot{h}^{\mathrm{tree}}(H_\star)$, and these are strictly positive. It follows that $\nu_\star$ is the (unique) optimizer for both $\mathbf{\Lambda}(H_\star)$ and $\mathbf{\Lambda}^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H_\star))$, which proves $\Xi(H_\star) = 0$. □

Proof of Lemma 2.6.4. Note that $\mathbf{\Lambda}(H)$ is an optimum over a subset of the measures ν which are considered for $\mathbf{\Lambda}^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H))$. Let $\mu = \mu^{\mathrm{opt}}(H)$ be the (unique) optimizer for $\mathbf{\Lambda}(H)$, and write $\nu = \nu^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H))$. Since ν is the unique optimizer in $\mathbf{\Lambda}^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H))$, we have $\Xi(H) = 0$ if and only if $\mu = \nu$. In this case, since $H(\mu) = H$ with $H = H^{\mathrm{sym}}$, the same must hold for

$H(\nu)$. Recall $H = H^{\mathrm{sym}}$ means that $\hat{H}$ is rotationally symmetric. We can take a marginal of (2.6.1) to obtain an expression for $\hat{H}$: in the first-moment calculation,

$$\hat{H}(\underline{\sigma}) = (\hat{\boldsymbol{z}})^{-1}\hat{\Phi}(\underline{\sigma})((\mathtt{BP}\dot{q})(\dot{\sigma}_1))\prod_{i=2}^{k}\dot{q}(\dot{\sigma}_i), \quad \underline{\sigma} \in \Omega^k.$$

The analogous expression holds in the second moment. We now claim that for the above measure $\hat{H}$ to be symmetric, we must have $\mathtt{BP}\dot{q} = \dot{q}$. Note that if $\hat{\Phi}$ were fully supported on Ω^k, and both $\dot{q}$ and $\mathtt{BP}\dot{q}$ were fully supported on $\dot{\Omega}$, the claim would be obvious. Since $\hat{\Phi}$ is certainly not fully supported, and we also do not know *a priori* whether $\dot{q}$ and $\mathtt{BP}\dot{q}$ are fully supported, the claim requires some argument, which differs slightly between the first- and second-moment cases:

1. In the first moment, Lemma 2.3.6 implies that $\dot{q}(\dot{\sigma})$ is positive for at least one $\dot{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}$. Assume without loss that $\dot{q}(\mathtt{b}_0)$ is positive; it follows that $(\mathtt{BP}\dot{q})(\dot{\sigma})$ is positive for both $\dot{\sigma} = \mathtt{b}_0, \mathtt{b}_1$. For any $\dot{\sigma} \in \dot{\Omega}$, there exists $\hat{\sigma}$ such that

$$\hat{\Phi}((\dot{\sigma}, \hat{\sigma}), \mathtt{b}_0, \ldots, \mathtt{b}_0) > 0. \tag{2.6.3}$$

   The symmetry of $\hat{H}$ then gives the relation

$$\frac{(\mathtt{BP}\dot{q})(\dot{\sigma})}{(\mathtt{BP}\dot{q})(\mathtt{b}_0)} = \frac{\dot{q}(\dot{\sigma})}{\dot{q}(\mathtt{b}_0)},$$

   so it follows that $\mathtt{BP}\dot{q} = \dot{q}$ in the first moment.

2. In the second moment, since we restrict to $H \in \mathbf{N}_{\mathrm{sep}}$, $\dot{q}(\dot{\sigma})$ is positive for at least one $\dot{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}^2$. Assume without loss that $\dot{q}(\mathtt{b}_0\mathtt{b}_0)$ is positive. For any $\dot{\sigma} \notin \{\mathtt{r}_0\mathtt{r}_1, \mathtt{r}_1\mathtt{r}_0\}$, there exists $\hat{\sigma}$ such that the second-moment analogue of (2.6.3) holds. The preceding argument gives

$$\frac{(\mathtt{BP}\dot{q})(\dot{\sigma})}{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_0)} = \frac{\dot{q}(\dot{\sigma})}{\dot{q}(\mathtt{b}_0\mathtt{b}_0)} \quad \text{for all } \dot{\sigma} \notin \{\mathtt{r}_0\mathtt{r}_1, \mathtt{r}_1\mathtt{r}_0\}.$$

   Since $(\mathtt{BP}\dot{q})(\dot{\sigma})$ is positive for all $\dot{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}^2$, it follows that the same holds for $\dot{q}$, so

$$\frac{(\mathtt{BP}\dot{q})(\dot{\sigma})}{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_1)} = \frac{\dot{q}(\dot{\sigma})}{\dot{q}(\mathtt{b}_0\mathtt{b}_1)} \quad \text{for all } \dot{\sigma} \notin \{\mathtt{r}_0\mathtt{r}_0, \mathtt{r}_1\mathtt{r}_1\}.$$

   Combining these, we have for $\dot{\sigma} \in \{\mathtt{r}_0\mathtt{r}_1, \mathtt{r}_1\mathtt{r}_0\}$ that

$$\frac{(\mathtt{BP}\dot{q})(\dot{\sigma})}{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_0)} = \frac{(\mathtt{BP}\dot{q})(\dot{\sigma})}{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_1)}\frac{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_1)}{(\mathtt{BP}\dot{q})(\mathtt{b}_0\mathtt{b}_0)} = \frac{\dot{q}(\dot{\sigma})}{\dot{q}(\mathtt{b}_0\mathtt{b}_0)},$$

   and this proves $\mathtt{BP}\dot{q} = \dot{q}$ in the second moment.

Altogether, the above proves in both the first- and second-moment settings that $\dot{q}$ is a BP fixed point. $\square$

Proof of Lemma 2.6.5. It suffices to prove that $\dot{q} \in \mathbf{\Gamma}$. Since by assumption $\dot{q} = \mathtt{BP}\dot{q}$, we must have $\dot{q} = \dot{q}^{\text{avg}}$. We then argue separately for the first and second moment:

1. For the first moment, we must verify (2.4.5). It follows directly from the relation $\dot{q} = \mathtt{BP}\dot{q}$ that $\dot{q}(\mathtt{r}) \geqslant \dot{q}(\mathtt{b})$. Since $H \in \mathbf{N}_\circ$, the majority of clauses have all `blue` edges, so

$$1/2 \leqslant \hat{H}(\mathtt{b}^k) \leqslant (\hat{\boldsymbol{z}})^{-1}\dot{q}(\mathtt{b})^k.$$

   Next, for any $\underline{\sigma} \in \Omega^k$ which has exactly one entry `free` and the remaining $k-1$ entries `blue`, we must have $\hat{\Phi}(\underline{\sigma}) \geqslant 1/2$. It follows that

$$1 \gtrsim 2^k(\bar{H}(\mathtt{r}) + \bar{H}(\mathtt{f})) \gtrsim (\hat{\boldsymbol{z}})^{-1}[\dot{q}(\mathtt{r}) + 2^k\dot{q}(\mathtt{f})]\dot{q}(\mathtt{b})^{k-1}.$$

   Comparing the two displays above gives $\dot{q}(\mathtt{r}) + 2^k\dot{q}(\mathtt{f}) \lesssim \dot{q}(\mathtt{b})$, proving $\dot{q} \in \mathbf{\Gamma}$.

2. For the second moment, we must verify (2.4.6). Condition (C) is immediate from the relation $\dot{q} = \mathtt{BP}\dot{q}$. From Lemma 2.4.4 it suffices to verify the condition with $\kappa = 0$, in which case condition (B) follows from (A). It therefore remains to verify (A). Denote

$$\mathtt{B} \equiv \{\mathtt{b}_0, \mathtt{b}_1\}^2, \quad \mathtt{B}_= \equiv \{\mathtt{b}_0\mathtt{b}_0, \mathtt{b}_1\mathtt{b}_1\} \subseteq \mathtt{B}, \quad \mathtt{B}_= \equiv \{\mathtt{b}_0\mathtt{b}_1, \mathtt{b}_1\mathtt{b}_0\} \subseteq \mathtt{B}.$$

   Since the total density of `red` and `free` edges is small, the majority of clauses must have all colors in $\mathtt{B}$: $\hat{H}(\mathtt{B}^k) = 1 - O(k/2^k)$. For any $\underline{\sigma} \in \mathtt{B}^k$, $\hat{\Phi}(\underline{\sigma}) = 1 - O(k/2^k)$. Therefore

$$1 \asymp \hat{H}(\mathtt{B}^k) \asymp \dot{q}(\mathtt{B})^k/\hat{\boldsymbol{z}}. \tag{2.6.4}$$

   For $H \in \mathbf{N}_{\text{sep}}$, we have $|\bar{H}(\mathtt{B}_=) - \bar{H}(\mathtt{B}_{\neq})| \lesssim k^4/2^{k/2}$. We can obtain $\bar{H}$ as a marginal of $\hat{H}$: using the rotational symmetry of $\hat{H}$, we can express

$$\begin{aligned}&\bar{H}(\mathtt{B}_=) - \bar{H}(\mathtt{B}_{\neq}) - \mathsf{err}(H)\\ &= \sum_{\xi=(\xi_2,\ldots,\xi_k)\in\mathtt{B}^{k-1}} \prod_{i=2}^{k} \dot{q}(\xi_i)\Big[\sum_{\sigma\in\mathtt{B}_=} \dot{q}(\sigma)\hat{\Phi}(\sigma,\xi) - \sum_{\sigma'\in\mathtt{B}_{\neq}} \dot{q}(\sigma')\hat{\Phi}(\sigma',\xi)\Big]\end{aligned}$$

   where $\mathsf{err}(H)$ is the contribution from the clauses which are not all $\mathtt{B}$, and is bounded by $O(k/2^k)$. Recalling $\hat{\Phi}(\underline{\sigma}) = 1 - O(k/2^k)$ for $\underline{\sigma} \in \mathtt{B}^k$, the right-hand side above equals

$$\frac{\dot{q}(\mathtt{B})^k}{\hat{\boldsymbol{z}}}\bigg[O(k/2^k) + \frac{\dot{q}(\mathtt{B}_=) - \dot{q}(\mathtt{B}_{\neq})}{\dot{q}(\mathtt{B})}\bigg].$$

   Applying (2.6.4) and rearranging gives

$$\frac{k^4}{2^{k/2}} \gtrsim \frac{|\dot{q}(\mathtt{B}_=) - \dot{q}(\mathtt{B}_{\neq})|}{\dot{q}(\mathtt{B})}.$$

It remains to show that $\sum_{\dot\sigma\notin\mathtt{B}}(2^{-k})^{\mathtt{r}[\dot\sigma]}\dot q(\dot\sigma) = O(2^{-k})\dot q(\mathtt{B})$. We will deduce this from the fact that the total fraction of clauses where $\sigma_i \notin \mathtt{B}$ for some $i \in [k]$ is $O(k/2^k)$. By rotational symmetry of $\hat H$, the fraction with $\sigma_1 \notin \mathtt{B}$ is $O(2^{-k})$. Take $\dot\sigma = (\dot\sigma^1, \dot\sigma^2) \in \dot\Omega^2\backslash\mathtt{B}$. For $j = 1, 2$, let

$$\sigma^j = \begin{cases} \sigma^j & \sigma^j \in \{\mathtt{r}, \mathtt{b}\}, \\ (\dot\sigma^j, \square) & \text{otherwise.} \end{cases}$$

Denote $\sigma \equiv (\sigma^1, \sigma^2)$. We now consider separately the cases $\mathtt{r}[\dot\sigma] = 0, 1, 2$:

(a) If $\mathtt{r}[\dot\sigma] = 0$, then note that for any $\underline{\xi} \in \mathtt{B}^{k-1}$ we have $\hat\Phi(\sigma, \underline{\xi}) \asymp 1$. On the other hand, using the rotational symmetry of $\hat H$, the total fraction of clauses where the first incident edge has a color in $\dot\Omega^2\backslash\mathtt{B}$ is $O(2^{-k})$. Thus

$$2^{-k} \gtrsim \frac{\dot q(\mathtt{B})^k}{\hat{\boldsymbol{z}}} \sum_{\dot\sigma\notin\mathtt{B}} \mathbf{1}\{\mathtt{r}[\dot\sigma] = 0\} \frac{\dot q(\dot\sigma)}{\dot q(\mathtt{B})} \asymp \frac{\dot q(\dot\sigma \notin \mathtt{B} : \mathtt{r}[\dot\sigma] = 0)}{\dot q(\mathtt{B})}.$$

(b) If $\mathtt{r}[\dot\sigma] = 1$, then for any $\underline{\xi} \in \mathtt{B}^{k-1}$ with at least two indices each in $\mathtt{B}_=$ and $\mathtt{B}_{\neq}$, we have $\hat\Phi(\sigma, \underline{\xi}) \asymp 2^{-k}$. Thus

$$2^{-k} \gtrsim \frac{\dot q(\mathtt{B})^k}{\hat{\boldsymbol{z}}} \sum_{\dot\sigma\notin\mathtt{B}} \mathbf{1}\{\mathtt{r}[\dot\sigma] = 1\} 2^{-k} \frac{\dot q(\dot\sigma)}{\dot q(\mathtt{B})} \asymp \frac{\dot q(\dot\sigma \notin \mathtt{B} : \mathtt{r}[\dot\sigma] = 1)}{2^k \dot q(\mathtt{B})}.$$

(c) If $\mathtt{r}[\dot\sigma] = 2$, then

$$2^{-k} \gtrsim \frac{1}{\hat{\boldsymbol{z}}} \sum_{\dot\sigma\notin\mathtt{B}} \mathbf{1}\{\mathtt{r}[\dot\sigma] = 2\} 2^{-k} \min\{\dot q(\mathtt{B}_=), \dot q(\mathtt{B}_{\neq})\}^{k-1} \asymp \frac{\dot q(\dot\sigma \notin \mathtt{B} : \mathtt{r}[\dot\sigma] = 2)}{4^k \dot q(\mathtt{B})}$$

Combining the above estimates verifies $\sum_{\dot\sigma\notin\mathtt{B}}(2^{-k})^{\mathtt{r}[\dot\sigma]}\dot q(\dot\sigma) = O(2^{-k})\dot q(\mathtt{B})$.

Altogether this verifies, in both the first and second moment, that $\dot q$ lies in the regime for BP contraction, and consequently must equal $\dot q_\star$ as claimed. $\square$

2.6.2 Non-degeneracy around minimizer

Proof of Proposition 2.6.2. Consider H near $H_\star$, and let $\nu = \nu^{\mathrm{opt}}(\dot h^{\mathrm{tree}}(H))$ and $\mu = \mu^{\mathrm{opt}}(H)$. It follows from Proposition 2.11.6 that

$$\boldsymbol{\Xi}(H) = \mathcal{H}(\mu|\nu) \gtrsim \|\mu - \nu\|^2,$$

so it suffices to show that $\|\mu - \nu\| \gtrsim \|H - H_\star\|$. To this end, recall ν can be expressed via (2.6.1) in terms of some $\dot q$, while $\nu_\star$ can be expressed in terms of $\dot q_\star$. Thus

$$\|\nu - \nu_\star\|_1 \lesssim \|\dot q - \dot q_\star\|_1.$$

For H in a small enough neighborhood of $H_\star$, the constraints are of full rank, so $\nu^{\mathrm{opt}}(\dot{h}^{\mathrm{tree}}(H))$ is expressible in terms of $\dot{q}$ for $\dot{q}$ *uniquely* determined by $\dot{h}^{\mathrm{tree}}(H)$, hereafter denoted $\dot{q} = \dot{q}^{\mathrm{opt}}(H)$. In fact, we see further from (2.11.6) that $\dot{q}^{\mathrm{opt}}$ is differentiable in a neighborhood of $H_\star$. Then, since $\dot{q}^{\mathrm{opt}}(H_\star) = \dot{q}_\star$ which lies in the interior of $\boldsymbol{\Gamma}$, we must have $\dot{q}^{\mathrm{opt}}(H) \in \boldsymbol{\Gamma}$ for H in some neighborhood of $H_\star$. It then follows by Proposition 2.4.2 in the first moment, and by Proposition 2.4.3 in the second moment, that

$$(1-c)\|\dot{q}-\dot{q}_\star\|_1 \leqslant \|\dot{q}-\dot{q}_\star\|_1 - \|\mathtt{BP}\dot{q}-\dot{q}_\star\|_1 \leqslant \|\dot{q}-\mathtt{BP}\dot{q}\|_1.$$

To compare $\dot{q}$ with $\mathtt{BP}\dot{q}$, consider

$$\sup\{\mathcal{H}(\hat{\nu}) + \lambda\langle \ln\hat{\Phi}, \hat{\nu}\rangle : \hat{\nu}(\dot{\sigma}_i = \dot{\sigma}) = \hat{H}(\dot{\sigma}_i = \dot{\sigma}) \text{ for each } i\}.$$

There is a unique optimizer $\hat{\nu} = \hat{\nu}^{\mathrm{opt}}(\hat{H})$ which can be expressed as

$$\hat{\nu}(\underline{\sigma}) \cong \hat{\Phi}(\underline{\sigma})^\lambda \prod_{i=1}^{k} \widetilde{\gamma}_i(\dot{\sigma}_i).$$

In a neighborhood of $\hat{H}_\star$, the vector $\underline{\widetilde{\gamma}} \equiv (\widetilde{\gamma}_i)_i$ is uniquely determined as a smooth function of $\hat{H}$, which we denote $\underline{\widetilde{\gamma}}^{\mathrm{opt}}(\hat{H})$. Consequently, if we denote $\hat{H}^{\mathrm{rot}}(\underline{\sigma}) = \hat{H}(\sigma_2,\ldots,\sigma_k,\sigma_1)$, then

$$\begin{aligned}
\|\dot{q}-\mathtt{BP}\dot{q}\|_1 &\leqslant \|(\mathtt{BP}\dot{q},\dot{q},\ldots,\dot{q}) - (\dot{q},\mathtt{BP}\dot{q},\dot{q},\ldots,\dot{q})\|_1 = \|\underline{\widetilde{\gamma}}^{\mathrm{opt}}(\hat{H}(\nu)) - \underline{\widetilde{\gamma}}^{\mathrm{opt}}(\hat{H}(\nu)^{\mathrm{rot}})\|_1 \\
&\lesssim \|\hat{H}(\nu) - \hat{H}(\nu)^{\mathrm{rot}}\| \leqslant \|\hat{H}(\nu)-\hat{H}(\mu)\| + \|\hat{H}(\mu) - \hat{H}(\nu)^{\mathrm{rot}}\| \\
&= 2\|\hat{H}(\nu) - \hat{H}(\mu)\| \lesssim \|\mu-\nu\|.
\end{aligned}$$

where in the last line we used that $\hat{H}(\mu) = \hat{H}(\mu)^{\mathrm{rot}}$. Combining the above inequalities gives $\|H-H_\star\| \lesssim \|\mu-\nu\|$ as claimed. ☐

Proof of Propositions 2.3.7 and 2.3.14. Follows from Proposition 2.6.1 and 2.6.2. ☐

2.7 Conclusion of lower bound

In this section we prove Propositions 2.3.10 and 2.3.17.

2.7.1 Intermediate overlap

We first show that configurations with "intermediate" overlap are negligible. This can be done with quite crude estimates, working with NAE-SAT solutions rather than colorings.

Lemma 2.7.1. *Consider random regular* NAE-SAT *at clause density $\alpha \geqslant 2^{k-1}\ln 2 - O(1)$. On $\mathscr{G} = (V,F,E)$, let $Z^2[\rho]$ count the number of pairs $\underline{x},\underline{\acute{x}} \in \{0,1\}^V$ of valid* NAE-SAT *solutions which agree on ρ fraction of variables. Then*

$$\mathbb{E}Z^2[\rho] \leqslant (\mathbb{E}Z)\exp\Big\{n\Big[H(\rho) - (\ln 2)\pi(\rho) + O(1/2^k)\Big]\Big\},$$

for $\pi(\rho) \equiv 1-\rho^k-(1-\rho)^k$.

Proof. For $\underline{u} \in \{0,1\}^V$, let $I^{\text{NAE}}_{\mathscr{G}}(\underline{u})$ be the indicator that $\underline{u}$ is a valid NAE-SAT solution on $\mathscr{G}$. Fix any pair of vectors $\underline{x}, \underline{\acute{x}} \in \{0,1\}^V$ which agree on ρ fraction of variables:

$$\mathbb{E}Z^2[\rho] = 2^n \binom{n}{n\rho} \mathbb{E}[I^{\text{NAE}}_{\mathscr{G}}(\underline{x}) I^{\text{NAE}}_{\mathscr{G}}(\underline{\acute{x}})] = (\mathbb{E}Z) \binom{n}{n\rho} \mathbb{E}[I^{\text{NAE}}_{\mathscr{G}}(\underline{\acute{x}}) \,|\, I^{\text{NAE}}_{\mathscr{G}}(\underline{x}) = 1].$$

Given $\underline{x}, \underline{\acute{x}}$, let $M \equiv M(\underline{x}, \underline{\acute{x}})$ count the number of clauses $a \in F$ where

$$|\{e \in \delta a : x_{v(e)} = \acute{x}_{v(e)}\}| \notin \{0, k\}.$$

In each of these clauses, there are $2^k - 2$ literal assignments $\underline{\mathtt{L}}_{\delta a}$ which are valid for $\underline{x}$. Out of these, exactly $2^k - 4$ are valid also for $\underline{\acute{x}}$. If we define i.i.d. binomial random variables $D_a \sim \text{Bin}(k, \rho)$, indexed by $a \in F$, then

$$\mathbb{P}(M = m\gamma) = \mathbb{P}\bigg(\sum_{a \in F} \mathbf{1}\{D_a \notin \{0,k\}\} \,\bigg|\, \sum_{a \in F} D_a = mk\rho \bigg).$$

The $(D_a)_{a \in F}$ sum to $mk\rho$ with probability which is polynomial in n, so

$$\mathbb{P}(M = m\gamma) \leqslant n^{O(1)} \mathbb{P}(\text{Bin}(m, \pi) = m\gamma)$$

with $\pi = \pi(\rho)$ as in the statement of the lemma. Therefore

$$\mathbb{E}[I^{\text{NAE}}_{\mathscr{G}}(\underline{\acute{x}}) \,|\, I^{\text{NAE}}_{\mathscr{G}}(\underline{x}) = 1] \leqslant n^{O(1)} \mathbb{E}\bigg[\bigg(\frac{2^k - 4}{2^k - 2} \bigg)^X \bigg]$$

for $X \sim \text{Bin}(m, \rho)$. It is easily seen that the above is $\leqslant \exp\{-m\pi/2^{k-1}\}$, and the claimed bound follows, using the lower bound on $\alpha = m/n$. ☐

Corollary 2.7.2. *Let $\psi(\rho) = H(\rho) - (\ln 2)\pi(\rho)$. Then $\psi(\rho) \leqslant -2k/2^k$ for all ρ in*

$$[\exp\{-k/(\ln k)\}, \tfrac{1}{2}(1 - k/2^{k/2})] \cup [\tfrac{1}{2}(1 + k/2^{k/2}), 1 - \exp\{-k/(\ln k)\}].$$

Assuming $\alpha = m/n \geqslant 2^{k-1} \ln 2 - O(1)$, $\mathbb{E}Z^2[\rho] \leqslant \exp\{-nk/2^k\}$ for all such ρ.

Proof. Note that $H(\frac{1+\epsilon}{2}) \leqslant \ln 2 - \epsilon^2/2$. If $(k \ln k)/2^k \leqslant \epsilon \leqslant 1/k$, then

$$\psi(\tfrac{1+\epsilon}{2}) \leqslant -\epsilon^2/2 + O(k\epsilon/2^k) \leqslant -\epsilon^2/3.$$

Both $H(\frac{1+\epsilon}{2})$ and $\pi(\frac{1+\epsilon}{2})$ are symmetric about $\epsilon = 0$, and decreasing on the interval $0 \leqslant \epsilon \leqslant 1$. It follows that for any $0 \leqslant a \leqslant b \leqslant 1$,

$$\max_{a \leqslant \epsilon \leqslant b} \psi(\tfrac{1+\epsilon}{2}) \leqslant H(\tfrac{1+a}{2}) - (\ln 2)\pi(\tfrac{1+b}{2}).$$

With this in mind, if $1/k \leqslant \epsilon \leqslant 1 - 5(\ln k)/k$,

$$\psi(\tfrac{1+\epsilon}{2}) \leqslant -(2k^2)^{-1} + O(k^{-5/2}) \leqslant -(4k^2)^{-1}.$$

If $1 - 5(\ln k)/k \leqslant \epsilon \leqslant 1 - (\ln k)^3/k^2$,

$$\psi(\tfrac{1+\epsilon}{2}) \leqslant O(1)(\ln k)^2/k - \Omega(1)(\ln k)^3/k \leqslant -\Omega(1)(\ln k)^3/k.$$

Finally, if $1 - (\ln k)^3/k^2 \leqslant \epsilon \leqslant 1 - \exp\{-2k/(\ln k)\}$, then

$$\psi(\tfrac{1+\epsilon}{2}) \leqslant O(1)\epsilon k/(\ln k) - \Omega(1)\epsilon k \leqslant -\Omega(1)\epsilon k.$$

Combining these estimates proves the claimed bound on $\psi(\rho)$. The assertion for $\mathbb{E}[Z^2(\rho)]$ then follows by substituting into Lemma 2.7.1, and noting that $\mathbb{E}Z \leqslant \exp\{O(n/2^k)\}$. □

2.7.2 Large overlap

In what follows, we restrict consideration to a small neighborhood $\mathbf{N}$ of $H_\star$. We abbreviate $\underline{\sigma} \in H$ if $H(\mathscr{G}, \underline{\sigma}) = H$, and $\underline{\sigma} \in \mathbf{N}$ if $H(\mathscr{G}, \underline{\sigma}) \in \mathbf{N}$. Recall that we write $\underline{\sigma}' \succcurlyeq \underline{\sigma}$ if the number of free variables in $\underline{x}(\underline{\sigma}')$ upper bounds the number in $\underline{x}(\underline{\sigma})$. We also write $H' \succcurlyeq H$ if $\underline{\sigma}' \succcurlyeq \underline{\sigma}$ for any (all) $\underline{\sigma} \in H$ and $\underline{\sigma}' \in H'$. Let $\boldsymbol{Z}^{\mathrm{ns}}(H, H')$ count the colorings $\underline{\sigma} \in H$ such that

$$\Big|\Big\{\underline{\sigma}' \in H' : \delta(\underline{\sigma}, \underline{\sigma}') \leqslant \exp\{-k/(\ln k)\}\Big\}\Big| \geqslant \omega(n),$$

for $\omega(n) = \exp\{(\ln n)^4\}$. (Although we will not write it explicitly, it should be understood that $\boldsymbol{Z}^{\mathrm{ns}}(H, H')$ depends on $\mathscr{G}$, since both $\underline{\sigma}, \underline{\sigma}'$ are required to be valid colorings of $\mathscr{G}$.) Let $\boldsymbol{Z}^{\mathrm{ns}}(\mathbf{N})$ denote the sum of $\boldsymbol{Z}^{\mathrm{ns}}(H; H')$ over all pairs $H, H' \in \mathbf{N}$ with $H' \succcurlyeq H$. Let $\boldsymbol{Z}(\mathbf{N})$ denote the sum of $\boldsymbol{Z}(H)$ over all $H \in \mathbf{N}$.

Proposition 2.7.3. *There exists a small enough positive constant $\epsilon_{\max}(k)$ such that, if $\mathbf{N}$ is the ϵ-neighborhood of $H_\star$ for any $\epsilon \leqslant \epsilon_{\max}$, then*

$$\mathbb{E}\boldsymbol{Z}^{\mathrm{ns}}(\mathbf{N}) \leqslant \mathbb{E}\boldsymbol{Z}(\mathbf{N}) \exp\{-(\ln n)^2\}.$$

Proof. By definition,

$$\boldsymbol{Z}^{\mathrm{ns}}(\mathbf{N}) = \sum_{H \in \mathbf{N}} \boldsymbol{Z}^{\succcurlyeq}(H), \quad \boldsymbol{Z}^{\succcurlyeq}(H) \equiv \sum_{H' \in \mathbf{N}} \mathbf{1}\{H' \succcurlyeq H\} \boldsymbol{Z}^{\mathrm{ns}}(H, H').$$

It suffices to show that for every $H \in \mathbf{N}$, $\mathbb{E}\boldsymbol{Z}^{\succcurlyeq}(H) \leqslant \mathbb{E}\boldsymbol{Z}(H) \exp\{-2(\ln n)^2\}$. Note that the total number of empirical measures H' is at most n^c for some constant $c(k, T)$. Let $\boldsymbol{E}$ denote the set of pairs $(\mathscr{G}, \underline{\sigma})$ for which

$$\Big|\Big\{\underline{\sigma}' \in \mathbf{N} : \underline{\sigma}' \succcurlyeq \underline{\sigma} \text{ and } \delta(\underline{\sigma}, \underline{\sigma}') \leqslant \exp\{-k/(\ln k)\}\Big\}\Big| \geqslant \omega(n).$$

(Again, it is understood that both $\underline{\sigma}, \underline{\sigma}'$ must be valid colorings of $\mathscr{G}$.) Then

$$\boldsymbol{Z}^{\succcurlyeq}(H) \leqslant n^c \sum_{\underline{\sigma} \in H} \mathbf{1}\{(\mathscr{G}, \underline{\sigma}) \in \boldsymbol{E}\}.$$

Consequently, in order to show the required bound on $\mathbb{E}\boldsymbol{Z}^{\geqslant}(H)$, it suffices to show

$$\mathbb{P}^H(\boldsymbol{E}) \leqslant n^{-c}\exp\{-2(\ln n)^2\}, \tag{2.7.1}$$

where $\mathbb{P}^H$ is a "planted" measure on pairs $(\mathscr{G}, \underline{\sigma})$: to sample from $\mathbb{P}^H$, we start with a set V of n isolated variables each with d incident half-edges, and a set F of m isolated clauses each with k incident half-edges. Assign colorings of the half-edges,

$$\underline{\sigma}_\delta \equiv (\underline{\sigma}_{\delta V}, \underline{\sigma}_{\delta F}) \quad \text{where } \underline{\sigma}_{\delta V} \equiv (\underline{\sigma}_{\delta v})_{v\in V},\ \underline{\sigma}_{\delta F} \equiv (\underline{\sigma}_{\delta a})_{a\in F},$$

which are uniformly random subject to the empirical measure H. Then $\underline{\sigma}_\delta$ is the "planted" coloring: conditioned on it, we sample uniformly at random a graph $\mathscr{G}$ such that $\underline{\sigma}_\delta$ becomes a valid coloring $\underline{\sigma}$ on $\mathscr{G}$. The resulting pair $(\mathscr{G}, \underline{\sigma})$ is a sample from $\mathbb{P}^H$.

Suppose $(\mathscr{G}, \underline{\sigma}) \in \boldsymbol{E}$. The total number of configurations $\underline{\sigma}'$ with $\delta(\underline{\sigma}, \underline{\sigma}') \leqslant \delta$ is at most $(cn)^{n\delta}$, which is $\ll \omega(n)$ if $\delta \leqslant n^{-1}(\ln n)^2$. This implies that there must exist $\underline{\sigma}' \in \mathbf{N}$ such that $\underline{\sigma}' \geqslant \underline{\sigma}$ and $n^{-1}(\ln n)^2 \leqslant \delta(\underline{\sigma}, \underline{\sigma}') \leqslant \exp\{-k/(\ln k)\}$. It follows that

$$S \equiv \{v \in V : x_v(\underline{\sigma}) \in \{\mathtt{0},\mathtt{1}\} \text{ and } x_v(\underline{\sigma}') \neq x_v(\underline{\sigma})\}$$

has size $|S| \equiv ns$ for $s \in [(2n)^{-1}(\ln n)^2, \exp\{-k/(\ln k)\}]$. The set S is *internally forced* in $\underline{\sigma}$: for every $v \in S$, any clause forcing to v must have another edge connecting to S. Formally, let $\mathtt{R}_U$ (resp. $\mathtt{B}_U$) count the number of `red` (resp. `blue`) edges incident to a subset of vertices U. Let I_S be the indicator that all variables in S are forced. For any fixed $S \subseteq V$,

$$\mathbb{P}^H(S \text{ internally forced}) \leqslant \mathbb{E}_{\mathbb{P}^H}\left[I_S k^{\mathtt{R}_S}\frac{(\mathtt{B}_S)_{\mathtt{R}_S}}{(\mathtt{B}_F)_{\mathtt{R}_S}}\right] \leqslant \mathbb{E}_{\mathbb{P}^H}[I_S(4ks)^{\mathtt{R}_S}].$$

In the first inequality, the factor $k^{\mathtt{R}_S}$ accounts for the choice, for each S-incident `red` edge e, of another edge e' sharing the same clause. The factor $(\mathtt{B}_S)_{\mathtt{R}_S}/(\mathtt{B}_F)_{\mathtt{R}_S}$ then accounts for the chance that the chosen edge e' (which must be `blue`) will also be S-incident. The second inequality follows by noting that we certainly have $\mathtt{B}_S \leqslant nsd$, and for H near $H_\star$ we also clearly have $\mathtt{B}_F \geqslant nd/4$.

To bound the above, we can work with a slightly different measure $\mathbb{Q}^H$: instead of sampling $\underline{\sigma}_\delta$ subject to H, we can simply sample variable-incident colorings $\underline{\sigma}_{\delta v}$ i.i.d. from $\dot{H}$, and clause-incident colorings $\underline{\sigma}_{\delta a}$ i.i.d. from $\hat{H}$. On the event MARG that the resulting $\underline{\sigma}_\delta$ has empirical measure H, we sample the graph $\mathscr{G}$ according to $\mathbb{P}^H(\mathscr{G}|\underline{\sigma}_\delta)$, and otherwise we set $\mathscr{G} = \varnothing$. Then, since $\mathbb{Q}^H(\mathsf{MARG}) \geqslant n^{-c}$ (adjusting c as needed), we have

$$\mathbb{P}^H((\mathscr{G}, \underline{\sigma})) = \mathbb{Q}^H((\mathscr{G}, \underline{\sigma}) \,|\, \mathsf{MARG}) \leqslant n^c\,\mathbb{Q}^H((\mathscr{G}, \underline{\sigma}); \mathsf{MARG}).$$

Let us abbreviate $\dot{H}(\ell)$ for the probability under $\dot{H}$ that $\underline{\sigma}$ has ℓ `red` entries: then

$$\mathbb{E}_{\mathbb{P}^H}[I_S(4ks)^{\mathtt{R}_S}] \leqslant n^c\,\mathbb{E}_{\mathbb{Q}^H}[I_S(4ks)^{\mathtt{R}_S}; \mathsf{MARG}] \leqslant n^c\left(\sum_{\ell\geqslant 1}\dot{H}(\ell)(4ks)^\ell\right)^{ns}. \tag{2.7.2}$$

For H sufficiently close to $H_\star$, we will have

$$\dot{H}(\ell) \leqslant 2\dot{H}_\star(\ell) \leqslant 2\binom{d}{\ell}\frac{\hat{q}_\star(\mathtt{r}_1)^\ell \hat{q}_\star(\mathtt{b}_1)^{d-\ell}}{[\hat{q}_\star(\mathtt{r}_1)+\hat{q}_\star(\mathtt{b}_1)]^d - \hat{q}_\star(\mathtt{b}_1)^d}.$$

It follows that the right-hand side of (2.7.2) is (for some absolute constant δ)

$$\leqslant n^c\, 2^{ns}\left(\frac{[\hat{q}_\star(\mathtt{r}_1)\cdot 4ks+\hat{q}_\star(\mathtt{b}_1)]^d - \hat{q}_\star(\mathtt{b}_1)^d}{[\hat{q}_\star(\mathtt{r}_1)+\hat{q}_\star(\mathtt{b}_1)]^d - \hat{q}_\star(\mathtt{b}_1)^d}\right)^{ns} \leqslant n^c s^{ns} 2^{-\delta kns},$$

where the last inequality uses that $s \leqslant \exp\{-k/(\ln k)\}$. Summing over S gives

$$\mathbb{P}^H(\boldsymbol{E}) \leqslant \max_{s \geqslant (2n)^{-1}(\ln n)^2} n^c 2^{-\delta kns/2} \leqslant \exp\{-\Omega(1)k(\ln n)^2\}.$$

This implies (2.7.1); and the claimed result follows as previously explained. □

Proof of Proposition 2.3.10. Follows by combining Corollary 2.7.2 and Proposition 2.7.3. □

2.8 Upper bound

In this section we prove the upper bound, Proposition 2.3.19.

2.8.1 Interpolation bound for regular graphs

For a certain family of spin systems that includes NAE-SAT, an interpolative calculation gives an upper bound for the free energy on Erdős-Rényi graphs ([FL03; PT04], cf. [Gue03]). These bounds build on earlier work [GT03] concerning the subadditivity of the free energy in the Sherrington–Kirkpatrick model, which was later generalized to a broad class of models [BGT13; Gam14]. (Although these results are closely related, we remark that interpolation gives quantitative bounds whereas subadditivity does not.) To prove our main result, we establish the analogue of [FL03; PT04] for random *regular* graphs. Although the main concern of this paper is the NAE-SAT model, we give the bound for a more general class of models, which may be of independent interest.

Recall $G = (V, F, E)$ denotes a (d, k)-regular bipartite graph (without edge literals). We consider measures defined on vectors $\underline{x} \in \mathcal{X}^V$ where $\mathcal{X}$ is some fixed alphabet of finite size. Fix also a finite index set S. Suppose we have (random) vectors $b \in \mathbb{R}^S$ and $f \in \mathcal{F}(\mathcal{X})^S$, where $\mathcal{F}(\mathcal{X})$ denotes the space of functions $\mathcal{X} \to \mathbb{R}_{\geqslant 0}$. Independently of b, let $f_1, \ldots, f_k$ be i.i.d. copies of f, and define the random function

$$\theta(\underline{x}) \equiv \sum_{s \in S} b_s \prod_{j=1}^{k} f_{s,j}(x_j). \tag{2.8.1}$$

Let h be another (random) element of $\mathcal{F}(\mathcal{X})$. Assume there is a constant $\epsilon > 0$ so that

$$\epsilon \leqslant \{h, 1-\theta\} \leqslant 1/\epsilon \quad \text{almost surely.} \tag{2.8.2}$$

Note we do not require the b_s to be non-negative; however, we assume that

$$b^p(\underline{s}) \equiv \mathbb{E}\Big[\prod_{\ell=1}^{p} b_{s_\ell}\Big] \geqslant 0 \quad \text{for any } p \geqslant 1,\ \underline{s} \equiv (s_1, \ldots, s_p) \in S^p. \tag{2.8.3}$$

Let $\mathscr{G}$ denote the graph G labelled by a vector $((h_v)_{v\in V}, (\theta_a)_{a\in F})$ of independent functions, where the h_v are i.i.d. copies of h and the θ_a are i.i.d. copies of θ. For $a \in F$ we abbreviate $\underline{x}_{\delta a} \equiv (x_{v(e)})_{e\in\delta a} \in \mathcal{X}^k$, and we consider the (random) Gibbs measure

$$\mu_{\mathscr{G}}(\underline{x}) \equiv \frac{1}{Z(\mathscr{G})} \prod_{v\in V} h_v(x_v) \prod_{a\in F} [1 - \theta_a(\underline{x}_{\delta a})] \tag{2.8.4}$$

where $Z(\mathscr{G})$ is the normalizing constant. Now let $\mathscr{G}$ be the random (d,k)-regular graph on n variables, together with the random function labels. We write $\mathbb{E}_n$ for expectation over the law of $\mathscr{G}$, and define the (logarithmic) free energy of the model to be

$$F_n \equiv n^{-1} \mathbb{E}_n \ln Z(\mathscr{G}).$$

Example 2.8.1 (positive temperature NAE-SAT)**.** Let $\mathcal{X} = \{\mathtt{0}, \mathtt{1}\}$, and let $\underline{\mathtt{L}} \equiv (\mathtt{L}_i)_{i\leqslant k}$ be a sequence of i.i.d. Bernoulli(1/2) random variables. The positive-temperature NAE-SAT model corresponds to taking $h \equiv 1$ and

$$\theta(\underline{x}) \equiv (1 - e^{-\beta}) \bigg(\prod_{i=1}^{k} \frac{\mathtt{L}_1 \oplus x_i}{2} + \prod_{i=1}^{k} \frac{\mathtt{1} \oplus \mathtt{L}_i \oplus x_i}{2} \bigg)$$

where $\beta \in (0, \infty)$ is the inverse temperature. In this model, each violated clause incurs a multiplicative penalty $e^{-\beta}$.

Example 2.8.2 (positive-temperature coloring)**.** Let $\mathcal{X} = [q]$. The positive-temperature coloring (anti-ferromagnetic Potts) model on a k-uniform hypergraph corresponds to $h \equiv 1$ and

$$\theta(\underline{x}) \equiv (1 - e^{-\beta}) \sum_{s=1}^{q} \mathbf{1}\{x_1 = \cdots = x_k = s\}$$

where $\beta \in (0, \infty)$ is the inverse temperature. In this model, each monochromatic (hyper)edge incurs a multiplicative penalty $e^{-\beta}$.

The following bound is a random regular graph analog of [PT04, Thm. 3]. (We have stated our result for a more general class of models than considered in [PT04]; however the main result of [PT04] extends to these models with minor modifications.)

Theorem 2.8.3. *Consider a (random) Gibbs measure* (2.8.4) *satisfying assumptions* (2.8.1)-(2.8.3)*, and let* $F_n \equiv n^{-1}\mathbb{E}_n \ln Z(\mathscr{G})$*. Let*

$$\begin{aligned}
\mathcal{M}_0 &\equiv \text{space of probability measures over } \mathcal{X},\\
\mathcal{M}_1 &\equiv \text{space of probability measures over } \mathcal{M}_0,\\
\mathcal{M}_2 &\equiv \text{space of probability measures over } \mathcal{M}_1.
\end{aligned}$$

For $\zeta \in \mathcal{M}_2$*, let* $\underline{\eta} \equiv (\eta_{a,j})_{a\geqslant 0,j\geqslant 0}$ *be an array of i.i.d. samples from* ζ*. For each index* (a,j) *let* $\rho_{a,j}$ *be a conditionally independent sample from* $\eta_{a,j}$*, and denote* $\underline{\rho} \equiv (\rho_{a,j})_{a\geqslant 0,j\geqslant 0}$*. Let* $(h\rho)_{a,j}(x) \equiv h_{a,j}(x)\rho_{a,j}(x)$*, define random variables*

$$\boldsymbol{u}_a(x) \equiv \sum_{\underline{x}\in\mathcal{X}^k} \mathbf{1}\{x_1 = x\}[1-\theta_a(\underline{x})]\prod_{j=2}^{k}(h\rho)_{a,j}(x_j),$$

$$\boldsymbol{u}_a \equiv \sum_{\underline{x}\in\mathcal{X}^k} [1-\theta_a(\underline{x})]\prod_{j=1}^{k}(h\rho)_{a,j}(x_j).$$

For any $\lambda \in (0,1)$ *and any* $\zeta \in \mathcal{M}_2$*,*

$$F_n \leqslant \lambda^{-1}\mathbb{E}\ln\mathbb{E}'\Big[\Big(\sum_{x\in\mathcal{X}} h(x)\prod_{a=1}^{d}\boldsymbol{u}_a(x)\Big)^{\lambda}\Big] - (k-1)\alpha\lambda^{-1}\mathbb{E}\ln\mathbb{E}'[(\boldsymbol{u}_0)^{\lambda}] + O_\epsilon(n^{-1/3})$$

where $\mathbb{E}'$ *denotes the expectation over* $\underline{\rho}$ *conditioned on all else, and* $\mathbb{E}$ *denotes the overall expectation.*

Remark 2.8.4. In the statistical physics framework, elements $\rho \in \mathcal{M}_0$ correspond to belief propagation messages for the underlying model, which has state space $\mathcal{X}$. Elements $\eta \in \mathcal{M}_1$ correspond to belief propagation messages for the 1RSB model (termed "auxiliary model" in [MM09, Ch. 19]), which has state space $\mathcal{M}_0$. The informal picture is that the η associated to variable x is determined by the geometry of the local neighborhood of x — that is to say, the randomness of ζ reflects the randomness in the geometry of the R-neighborhood of a uniformly randomly variable in the graph. In random regular graphs this randomness is degenerate — the R-neighborhood of (almost) every vertex is simply a regular tree. It is therefore expected that the best upper bound in Theorem 2.8.3 can be achieved with ζ a point mass.

2.8.2 Replica symmetric bound

Along the lines of [PT04], we first prove a weaker "replica symmetric" version of Theorem 2.8.3. Afterwards we will apply it to obtain the full result.

Theorem 2.8.5. *In the setting of Theorem 2.8.3, define*

$$\Phi_V \equiv \mathbb{E}\ln\Big(\sum_{x\in\mathcal{X}} h(x)\prod_{a=1}^{d}\boldsymbol{u}_a(x)\Big), \quad \Phi_F \equiv (k-1)\alpha\mathbb{E}\ln(\boldsymbol{u}_0).$$

Then $F_n \leqslant \Phi_V - \Phi_F - O_\epsilon(n^{-1/3})$.

Inspired by the proof of [BGT13], we prove Theorem 2.8.5 by a combinatorial interpolation between two graphs, $\mathscr{G}_{-1}$ and $\mathscr{G}_{nd+1}$. The initial graph $\mathscr{G}_{-1}$ will have free energy Φ_V, and the final graph $\mathscr{G}_{nd+1}$ will have free energy $F_n + \Phi_F$. We will show that, up to $O_\epsilon(n^{1/3})$ error, the free energy of $\mathscr{G}_{-1}$ will be larger than that of $\mathscr{G}_{nd+1}$, from which the bound of Theorem 2.8.5 follows.

To begin, we take $\mathscr{G}_{-1}$ to be a factor graph consisting of n disjoint trees (Figure 2.8.1a). Each tree is rooted at a variable v which joins to d clauses. Each of these clauses then joins to $k-1$ more variables, which form the leaves of the tree. We write V for the root variables, A for the clauses, and U for the leaf variables. Note $|V| = n$, $|A| = nd$, and $|U| = nd(k-1)$.

Independently of all else, take a vector of i.i.d. samples $(\eta_u, \rho_u)_{u \in U}$ where η_u is a sample from ζ, and ρ_u is a sample from η_u.[2] As before, the variables and clauses in $\mathscr{G}_{-1}$ are labelled independently with functions h_v and θ_a. We now additionally assign to each $u \in U$ the label (η_u, ρ_u). Let $(h\rho)_u(x) \equiv h_u(x)\rho_u(x)$. We consider the factor model on $\mathscr{G}_{-1}$ defined by

$$\mu_{\mathscr{G}_{-1}}(\underline{x}) = \frac{1}{Z(\mathscr{G}_{-1})} \prod_{v \in V} h_v(x_v) \prod_{a \in A} [1 - \theta_a(\underline{x}_{\delta a})] \prod_{u \in U} (h\rho)_u(x_u).$$

We now define the interpolating sequence of graphs $\mathscr{G}_{-1}, \mathscr{G}_0, \ldots, \mathscr{G}_{nd+1}$. Fix $m' \equiv 2n^{2/3}$. The construction proceeds by adding and removing clauses. Whenever we remove a clause a, the edges δa are left behind as k unmatched edges in the remaining graph. Whenever we add a new clause b, we label it with a fresh sample θ_b of θ. The graph $\mathscr{G}_r$ has clauses F_r which can be partitioned into $A_{U,r}$ (clauses involving U only), $A_{V,r}$ (clauses involving V only), and A_r (clauses involving both U and V). We will define below a certain sequence of events COUP_r. Let $\mathsf{COUP}_{\leqslant r}$ be the event that COUP_s occurs for all $0 \leqslant s \leqslant r$. The event $\mathsf{COUP}_{\leqslant -1}$ occurs vacuously, so $\mathbb{P}(\mathsf{COUP}_{\leqslant -1}) = 1$. With this notation in mind, the construction goes as follows:

1. Starting from $\mathscr{G}_{-1}$, choose a uniformly random subset of m' clauses from $F_{-1} = A_{-1} = A$, and remove them to form the new graph $\mathscr{G}_0$.

2. For $0 \leqslant r \leqslant nd - m' - 1$, we start from $\mathscr{G}_r$ and form $\mathscr{G}_{r+1}$ as follows.

   a. If $\mathsf{COUP}_{\leqslant r-1}$ succeeds, choose a uniformly random clause a from A_r, and remove it to form the new graph $\mathscr{G}_{r,\circ}$. Let $\delta' U_{r,\circ}$ and $\delta' V_{r,\circ}$ denote the unmatched half-edges incident to U and V respectively in $\mathscr{G}_{r,\circ}$, and define the event

   $$\mathsf{COUP}_r \equiv \{\min\{\delta' U_{r,\circ}, \delta' V_{r,\circ}\} \geqslant k\}.$$

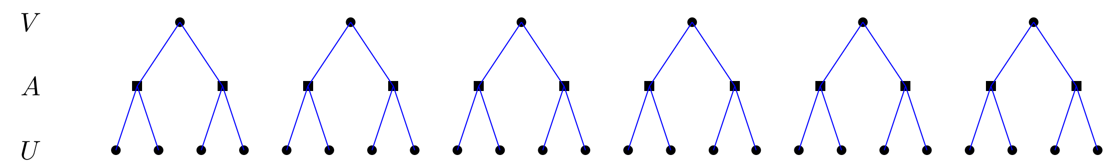
   If instead $\mathsf{COUP}_{\leqslant r-1}$ fails, then $\mathsf{COUP}_{\leqslant r}$ fails by definition.

   b. If $\mathsf{COUP}_{\leqslant r}$ fails, let $\mathscr{G}_{r+1} = \mathscr{G}_r$. If $\mathsf{COUP}_{\leqslant r}$ succeeds, then with probability $1/k$ take k half-edges from $\delta' V_{r,\circ}$ and join them into a new clause c. With the remaining probability $(k-1)/k$ take k half-edges from $\delta' U_{r,\circ}$ and join them into a new clause c.

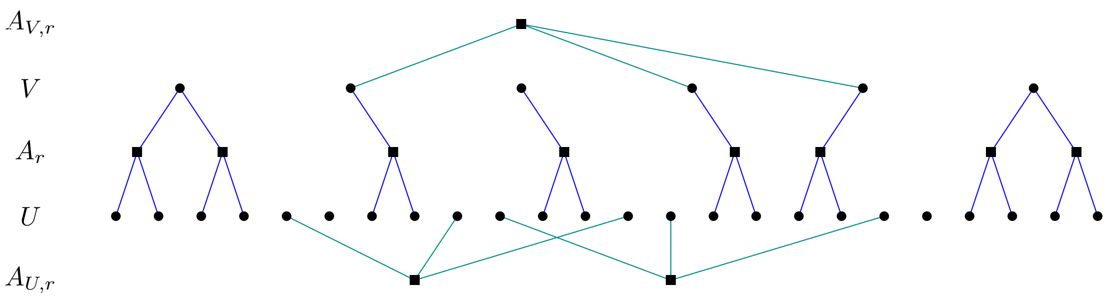
[2] For the proof of Theorem 2.8.5 it is equivalent to sample ρ from $\eta^{\text{avg}} \equiv \int \eta \, d\zeta$.

3. For $nd - m' \leqslant r \leqslant nd-1$ let $\mathscr{G}_{r+1} = \mathscr{G}_r$. Starting from $\mathscr{G}_{nd}$, remove all the clauses in A_{nd}. Then connect (uniformly at random) all remaining unmatched V-incident edges into clauses. Likewise, connect all remaining unmatched U-incident edges into clauses. Denote the resulting graph $\mathscr{G}_{nd+1}$.

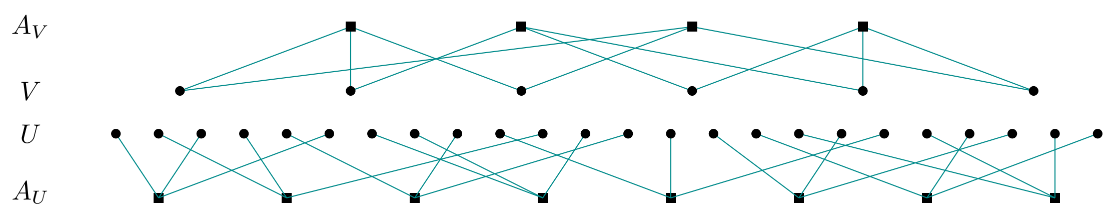
By construction, $\mathscr{G}_{nd+1}$ consists of two disjoint subgraphs, which are the induced subgraphs $\mathscr{G}_U, \mathscr{G}_V$ of U, V respectively. Note that $\mathscr{G}_V$ is distributed as the random graph $\mathscr{G}$ of interest, while $\mathscr{G}_U$ consists of a collection of $nd(k-1)/k = n\alpha(k-1)$ disjoint trees.



(a) $\mathscr{G}_{-1}$



(b) $\mathscr{G}_r$ with $m' = 1, r = 3$



(c) $\mathscr{G}_{nd+1}$

Figure 2.8.1: Interpolation with $d = 2, k = 3$, $n = 6$.

Lemma 2.8.6. *Under the construction above,*

$$\mathbb{E} \ln Z(\mathscr{G}_0) \geqslant \mathbb{E} \ln Z(\mathscr{G}_{nd}) - O_\epsilon(n^{1/3}), \tag{2.8.5}$$

where the expectation $\mathbb{E}$ *is over the sequence of random graphs* $(\mathscr{G}_r)_{-1 \leqslant r \leqslant nd+1}$.

Proof. Let $\mathscr{F}_{r,\circ}$ be the σ-field generated by $\mathscr{G}_{r,\circ}$, and write $\mathbb{E}_{r,\circ}$ for expectation conditioned on $\mathscr{F}_{r,\circ}$. One can rewrite (2.8.5) as

$$\mathbb{E} \ln \frac{Z(\mathscr{G}_0)}{Z(\mathscr{G}_{nd})} = \sum_{r=0}^{nd-1} \mathbb{E}\Delta_r, \quad \Delta_r \equiv \mathbb{E}_{r,\circ} \ln \frac{Z(\mathscr{G}_r)}{Z(\mathscr{G}_{r,\circ})} - \mathbb{E}_{r,\circ} \ln \frac{Z(\mathscr{G}_{r+1})}{Z(\mathscr{G}_{r,\circ})}. \tag{2.8.6}$$

In particular, $\Delta_r = 0$ if the coupling fails. Therefore it suffices to show that Δ_r is positive conditioned on $\mathsf{COUP}_{\leqslant r}$.[3] First we compare $\mathscr{G}_r$ and $\mathscr{G}_{r,\circ}$. Conditioned on $\mathscr{F}_{r,\circ}$, we know $\mathscr{G}_{r,\circ}$. From $\mathscr{G}_{r,\circ}$ we can obtain $\mathscr{G}_r$ by adding a single clause $a \equiv a_r$, together with a random label θ_a which is a fresh copy of θ. To choose the unmatched edges $\delta a = (e_1, \ldots, e_k)$ which are combined into the clause a, we take e_1 uniformly at random from $\delta' V_{r,\circ}$, then take $\{e_2, \ldots, e_k\}$ a uniformly random subset of $\delta' U_{r,\circ}$. Let $\mu_{r,\circ}$ be the Gibbs measure on $\mathscr{G}_{r,\circ}$ (ignoring unmatched half-edges). Let $\underline{\underline{x}} \equiv (\underline{x}, \underline{x}^1, \underline{x}^2, \ldots)$ be an infinite sequence of i.i.d. samples from $\mu_{r,\circ}$, and write $\langle \cdot \rangle_{r,\circ}$ for the expectation with respect to their joint law. Then

$$\mathbb{E}_{r,\circ} \ln \frac{Z(\mathscr{G}_r)}{Z(\mathscr{G}_{r,\circ})} = \mathbb{E}_{r,\circ} \ln(1 - \langle \theta(\underline{x}_{\delta a}) \rangle_{r,\circ}) = \sum_{p \geqslant 1} \frac{1}{p} \mathscr{A}_p, \quad \mathscr{A}_p \equiv \mathbb{E}_{r,\circ} \bigg[\Big\langle \prod_{\ell=1}^{p} \theta(\underline{x}^\ell_{\delta a}) \Big\rangle_{r,\circ} \bigg].$$

We have $\mathbb{E}_{r,\circ} = \mathbb{E}_a \mathbb{E}_\theta$ where $\mathbb{E}_a$ is expectation over the choice of δa, and $\mathbb{E}_\theta$ is expectation over the choice of θ. Under $\mathbb{E}_a$, the edges $(e_2, \ldots, e_k)$ are weakly dependent, since they are required to be distinct elements of $\delta' U_{r,\circ}$. We can consider instead sampling $e_2, \ldots, e_k$ uniformly *with replacement* from $\delta' U_{r,\circ}$, so that $e_1, \ldots, e_k$ are independent conditional on $\mathscr{F}_{r,\circ}$; let $\mathbb{E}_{a,\mathrm{ind}}$ denote expectation with respect to this choice of δa. Under $\mathbb{E}_{a,\mathrm{ind}}$ the chance of a collision $e_i = e_j$ $(i \leqslant j)$ is $O(k^2/|\delta' U_{r,\circ}|)$. Recalling $1 - \theta \geqslant \epsilon$ almost surely, we have

$$\mathscr{A}_{p,\mathrm{ind}} \equiv \mathbb{E}_{a,\mathrm{ind}} \mathbb{E}_\theta \bigg[\Big\langle \prod_{\ell=1}^{p} \theta(\underline{x}^\ell_{\delta a}) \Big\rangle_{r,\circ} \bigg] = \mathscr{A}_p + O(1)(1-\epsilon)^p \min\bigg\{ \frac{k^2}{|\delta' U_{r,\circ}|}, 1 \bigg\}.$$

Recall from (2.8.1) the product form of θ, and let $\mathbb{E}_f$ denote expectation over the law of $f \equiv (f_s)_{s \in S}$. Then, with $b^p(\underline{s})$ as defined in (2.8.3), we have

$$\begin{aligned} \mathscr{A}_{p,\mathrm{ind}} &= \sum_{\underline{s} \in S^p} b^p(\underline{s}) \Big\langle \mathbb{E}_{a,\mathrm{ind}} \Big\{ \prod_{j=1}^{k} \mathbb{E}_f \Big[\prod_{\ell=1}^{p} f_{s_\ell}(x^\ell_{e_j}) \Big] \Big\} \Big\rangle_{r,\circ} \\ &= \sum_{\underline{s} \in S^p} b^p(\underline{s}) \langle I_{V,\underline{s}}(\underline{\underline{x}}) I_{U,\underline{s}}(\underline{\underline{x}})^{k-1} \rangle_{r,\circ}, \end{aligned}$$

where, for $W = U$ or $W = V$, we define

$$I_{W,\underline{s}}(\underline{\underline{x}}) \equiv \frac{1}{|\delta' W_{r,\circ}|} \sum_{e \in \delta' W_{r,\circ}} \mathbb{E}_f \Big[\prod_{\ell=1}^{p} f_{s_\ell}(x^\ell_e) \Big].$$

Summing over $p \geqslant 1$ gives that, on the event $\mathsf{COUP}_{\leqslant r}$,

$$\mathbb{E}_{r,\circ} \ln \frac{Z(\mathscr{G}_r)}{Z(\mathscr{G}_{r,\circ})} = \sum_{p \geqslant 1} \frac{1}{p} \sum_{\underline{s} \in S^p} b^p(\underline{s}) \mathbb{E}_{r,\circ} \langle I_{V,\underline{s}}(\underline{\underline{x}}) I_{U,\underline{s}}(\underline{\underline{x}})^{k-1} \rangle_{r,\circ} + \mathsf{err}_{r,1},$$
$$\text{where } |\mathsf{err}_{r,1}| \leqslant O_\epsilon(1) \min\bigg\{ \frac{k^2}{|\delta' U_{r,\circ}|}, 1 \bigg\}.$$

[3]The event $\mathsf{COUP}_{\leqslant r}$ is measurable with respect to $\mathscr{F}_{r,\circ}$, since $\delta' V_{r,\circ}, \delta' U_{r,\circ}$ would remain less than k if the coupling fails at an earlier iteration.

A similar comparison between $\mathscr{G}_{r+1}$ and $\mathscr{G}_{r,\circ}$ gives

$$\mathbb{E}_{r,\circ} \ln \frac{Z(\mathscr{G}_r)}{Z(\mathscr{G}_{r,\circ})} = \sum_{p\geqslant 1} \frac{1}{p} \mathbb{E}_{r,\circ} \bigg[\sum_{\underline{s}\in S^p} b^p(\underline{s}) \Big\langle \frac{k-1}{k} I_{U,\underline{s}}(\underline{\underline{x}})^k + \frac{1}{k} I_{V,\underline{s}}(\underline{\underline{x}})^k \Big\rangle_{r,\circ} \bigg] + \mathsf{err}_{r,2},$$

$$|\mathsf{err}_{r,2}| \leqslant O_\epsilon(1) \min \left\{ \frac{k^2}{\min\{|\delta' U_{r,\circ}|, |\delta' V_{r,\circ}|\}}, 1 \right\}.$$

We now argue that the sum of the error terms $\mathsf{err}_{r,1}, \mathsf{err}_{r,2}$, over $0 \leqslant r \leqslant nd-1$, is small in expectation. First note that for a constant $C = C(k,\epsilon)$,

$$\sum_{r=0}^{nd-1} \mathbb{E}[\mathsf{err}_{r,1} + \mathsf{err}_{r,2}] \leqslant Cn \Big[n^{-2/3} + \mathbb{P}\Big(\min\{|\delta' V_{r,\circ}|, |\delta' V_{r,\circ}|\} \leqslant n^{2/3} \text{ for some } r \leqslant nd \Big) \Big].$$

The process $(|\delta' V_{r,\circ}|)_{r\geqslant 0}$ is an unbiased random walk started from $m'+1 = 2n^{2/3}+1$. In each step it goes up by 1 with chance $(k-1)/k$, and down by $k-1$ with chance $1/k$; it is absorbed if it hits k before time $nd-m'$. Similarly, $(|\delta' U|_{r,\circ})_{r\geqslant 0}$ is an unbiased random walk started from $(m'+1)(k-1)$ with an absorbing barrier at k. By the Azuma–Hoeffding bound, there is a constant $c = c(k)$ such that

$$\mathbb{P}(|\delta' V_{r,\circ}| \leqslant |\delta' V_{0,\circ}| - n^{2/3}) + \mathbb{P}(|\delta' U_{r,\circ}| \leqslant |\delta' U_{0,\circ}| - n^{2/3}) \leqslant \exp\{-cn^{1/3}\}$$

Taking a union bound over r shows that with very high probability, neither of the walks $|\delta' V_{r,\circ}|, |\delta' U_{r,\circ}|$ is absorbed before time $nd-m'$, and (adjusting the constant C as needed)

$$\sum_{r=0}^{nd-1} \mathbb{E}[\mathsf{err}_{r,1} + \mathsf{err}_{r,2}] \leqslant Cn^{1/3}.$$

Altogether this gives

$$\begin{aligned} &\mathbb{E} \ln \frac{Z(\mathscr{G}_0)}{Z(\mathscr{G}_{nd})} - O_\epsilon(n^{1/3}) \\ &= \sum_{r=0}^{nd-1} \sum_{p\geqslant 1} \frac{1}{p} \sum_{\underline{s}} b^p(\underline{s}) \mathbb{E}_{r,\circ} \Big\langle I_{V,\underline{s}}(\underline{\underline{x}}) I_{U,\underline{s}}(\underline{\underline{x}})^{k-1} - \frac{k-1}{k} I_{U,\underline{s}}(\underline{\underline{x}})^{k-1} - \frac{1}{k} I_{V,\underline{s}}(\underline{\underline{x}})^{k-1} \Big\rangle_{r,\circ}. \end{aligned}$$

Using the fact that $x^k - kxy^{k-1} + (k-1)y^k \geqslant 0$ for all $x, y \in \mathbb{R}$ and even $k \geqslant 2$, or $x, y \geqslant 0$ and odd $k \geqslant 3$ finishes the proof. ☐

Corollary 2.8.7. *In the setting of Lemma 2.8.6,*

$$\mathbb{E} \ln Z(\mathscr{G}_{-1}) \geqslant \mathbb{E} \ln Z(\mathscr{G}_{nd+1}) - O_\epsilon(n^{2/3}),$$

where the expectation $\mathbb{E}$ is over the sequence of random graphs $(\mathscr{G}_r)_{-1\leqslant r\leqslant nd+1}$.

Proof. Adding or removing a clause can change the partition function by at most a multiplicative constant (depending on ϵ). On the event that the coupling succeeds for all r,

$$\left|\ln \frac{Z(\mathscr{G}_0)}{Z(\mathscr{G}_{-1})}\right| + \left|\ln \frac{Z(\mathscr{G}_{nd+1})}{Z(\mathscr{G}_{nd})}\right| = O_\epsilon(m') = O_\epsilon(n^{2/3}).$$

On the event that the coupling fails, the difference is crudely $O_\epsilon(n)$. We saw in the proof of Lemma 2.8.6 that the coupling fails with probability exponentially small in n, so altogether we conclude

$$\mathbb{E}\left|\ln \frac{Z(\mathscr{G}_0)}{Z(\mathscr{G}_{-1})}\right| + \mathbb{E}\left|\ln \frac{Z(\mathscr{G}_{nd+1})}{Z(\mathscr{G}_{nd})}\right| = O_\epsilon(n^{2/3}).$$

Combining with the result of Lemma 2.8.6 proves the claim. □

Proof of Theorem 2.8.5. In the interpolation, the initial graph $\mathscr{G}_{-1}$ consists of n disjoint trees T_v, each rooted at a variable $v \in V$. Thus

$$n^{-1}\mathbb{E}\ln Z(\mathscr{G}_{-1}) = \mathbb{E}\ln Z(T_v) = \mathbb{E}\ln\bigg(\sum_{x\in\mathcal{X}} h_v(x)\prod_{a=1}^{d}\boldsymbol{u}_a(x)\bigg).$$

The final graph $\mathscr{G}_{nd+1}$ is comprised of two disjoint subgraphs — one subgraph $\mathscr{G}_V$ has the same law as the graph $\mathscr{G}$ of interest, while the other subgraph $\mathscr{G}_U = (U, F_U, E_U)$ consists of $n\alpha(k-1)$ disjoint trees S_c, each rooted at a clause $c \in A_U$. Thus

$$n^{-1}\mathbb{E}\ln Z(\mathscr{G}_{nd+1}) = \alpha(k-1)\mathbb{E}\ln Z(S_c) + n^{-1}\mathbb{E}\ln Z(\mathscr{G}) = \alpha(k-1)\mathbb{E}\ln \boldsymbol{u}_0 + F_n.$$

The theorem follows by substituting these into the bound of Corollary 2.8.7. □

2.8.3 1RSB bound

For the proof of Theorem 2.8.3, we take $\mathscr{G}_{-1}$ as before and modify it as follows. Where previously each $u \in U$ had spin value $x_u \in \mathcal{X}$, it now has the augmented spin (x_u, γ_u) where γ goes over the positive integers. Let $\underline{\gamma} \equiv (\gamma_u)_u$. Next, instead of labeling u with (h_u, η_u, ρ_u) as before, we now label it with $(h_u, \eta_u, (\rho_u^\gamma)_{\gamma\geqslant 1})$ where $(\rho_u^\gamma)_{\gamma\geqslant 1}$ is an infinite sequence of i.i.d. samples from η_u. Lastly, we join all variables in U to a new clause a_* (Figure 2.8.2), which is labelled with the function

$$\varphi_{a_*}(\underline{\gamma}) = \sum_{\gamma\geqslant 1} z_\gamma \prod_{u\in U}\mathbf{1}\{\gamma_u = \gamma\}$$

for some sequence of (random) weights $(z_\gamma)_{\gamma\geqslant 1}$. Let $\mathscr{H}_{-1}$ denote the resulting graph.

Given $\mathscr{H}_{-1}$, let $\mu_{\mathscr{H}_{-1}}$ be the associated Gibbs measure on configurations $(\underline{\gamma}, \underline{x})$. Due to the definition of φ_{a_*}, the support of $\mu_{\mathscr{H}_{-1}}$ contains only those configurations where all the γ_u share a common value γ, in which case we denote $(\underline{\gamma}, \underline{x}) \equiv (\gamma, \underline{x})$. Explicitly,

$$\mu_{\mathscr{H}_{-1}}(\gamma, \underline{x}) = \frac{1}{Z(\mathscr{H}_{-1})} z_\gamma \prod_{v\in V} h_v(x_v) \prod_{a\in A}[1 - \theta_a(\underline{x}_{\delta a})] \prod_{u\in U}(\rho^\gamma h)_u(x_u).$$

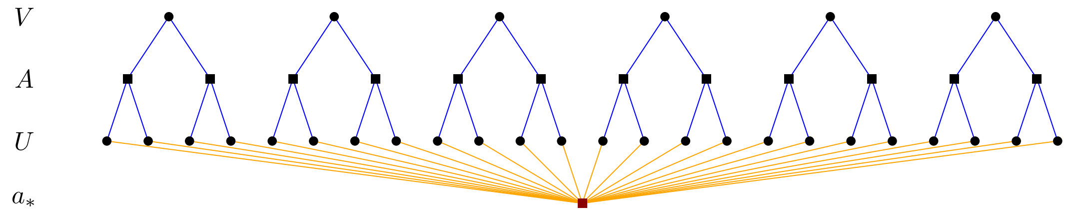


Figure 2.8.2: $\mathscr{H}_{-1}$

We can then define an interpolating sequence $\mathscr{H}_{-1}, \ldots, \mathscr{H}_{nd+1}$ precisely as in the proof of Theorem 2.8.5, leaving a_* untouched. Let $\mathscr{G}_r$ denote the graph $\mathscr{H}_r$ without the clause a_*, and let $Z_\gamma(\mathscr{G}_r)$ denote the partition function on $\mathscr{G}_r$ restricted to configurations where $\gamma_u = \gamma$ for all u. Then, for each $0 \leqslant r \leqslant nd + 1$,

$$Z(\mathscr{H}_r) = \sum_\gamma z_\gamma Z_\gamma(\mathscr{G}_r).$$

The proofs of Lemma 2.8.6 and Corollary 2.8.7 carry over to this setting with essentially no changes, giving

Corollary 2.8.8. *Under the assumptions above,*

$$\mathbb{E} \ln Z(\mathscr{H}_{-1}) \geqslant \mathbb{E} \ln Z(\mathscr{H}_{nd+1}) - O_\epsilon(n^{2/3}),$$

where the expectation $\mathbb{E}$ *is over the sequence of random graphs* $(\mathscr{H}_r)_{-1 \leqslant r \leqslant nd+1}$.

The result of Corollary 2.8.8 applies for any choice of $(z_\gamma)_{\gamma \geqslant 1}$. Let us now take $(z_\gamma)_{\gamma \geqslant 1}$ to be a Poisson–Dirichlet process with parameter $\lambda \in (0,1)$.[4] The process has the following invariance property (see e.g. [Pan13, Ch. 2]):

Proposition 2.8.9. *Let* $(z_\gamma)_{\gamma \geqslant 1}$ *be a Poisson–Dirichlet process with parameter* $\lambda \in (0,1)$. *Independently, let* $(\xi_\gamma)_{\gamma \geqslant 1}$ *be a sequence of i.i.d. positive random variables with finite second moment. Then the two sequences* $(z_\gamma \xi_\gamma)_{\gamma \geqslant 1}$ *and* $(z_\gamma (\mathbb{E}\xi_1^\lambda)^{1/\lambda})_{\gamma \geqslant 1}$ *have the same distribution, and consequently*

$$\mathbb{E} \ln \sum_{\gamma \geqslant 1} z_\gamma \xi_\gamma = \frac{1}{\lambda} \ln \mathbb{E} \xi^\lambda.$$

Proof of Theorem 2.8.3. Consider

$$\underline{Z}(\gamma) \equiv (Z_\gamma(\mathscr{G}_r))_{-1 \leqslant r \leqslant nd+1}.$$

[4]That is to say, let $(w_\gamma)_{\gamma \geqslant 1}$ be a Poisson point process on $\mathbb{R}_{>0}$ with intensity measure $w^{-(1+\lambda)}\,dw$. Let W denote their sum, which is finite almost surely. Assume the points of w_γ are arranged in decreasing order, and write $z_\gamma \equiv w_\gamma / W$. Then $(z_\gamma)_{\gamma \geqslant 1}$ is distributed as a Poisson–Dirichlet process with parameter λ.

If we condition on everything else except for the ρ's, then $(\underline{Z}(\gamma))_{\gamma\geqslant 1}$ is an i.i.d. sequence indexed by γ. Let $\mathbb{E}_{z,\rho}$ denote expectation over the z's and ρ's, conditioned on all else: then applying Proposition 2.8.9 gives

$$\begin{aligned} n^{-1}\mathbb{E}\ln Z(\mathscr{H}_{-1}) &= (n\lambda)^{-1}\mathbb{E}\ln\mathbb{E}_{z,\rho}[Z(\mathscr{G}_{-1})^\lambda] = \lambda^{-1}\mathbb{E}\ln\mathbb{E}_{z,\rho}\bigg[\bigg(\sum_{x\in\mathcal{X}} h(x)\prod_{a=1}^d \boldsymbol{u}_a(x)\bigg)^\lambda\bigg], \\ n^{-1}\mathbb{E}\ln Z(\mathscr{H}_{nd+1}) &= F_n + \lambda^{-1}\mathbb{E}\ln\mathbb{E}_{z,\rho}[(\boldsymbol{u}_0)^\lambda]. \end{aligned}$$

Combining with Corollary 2.8.8 proves the result. □

2.8.4 Conclusion of upper bound

We now apply Theorem 2.8.3 to prove the upper bound for the NAE-SAT model, Proposition 2.3.19. Following Example 2.8.1, let $F_n(\beta) \equiv n^{-1}\mathbb{E}\ln Z_n(\beta)$ be the expected free energy for NAE-SAT at inverse temperature β. (The expectation is with respect to the law of the random (d,k)-regular graph.)

Let $\dot{\mu}_\lambda$ be the fixed point specified by Proposition 2.1.2, and let $(\rho_{aj})_{a,j\geqslant 0}$ be an array of i.i.d. samples from $\dot{\mu}_\lambda$. For each $\rho = \rho_{aj}$ we can define a (random) measure on $\mathcal{X} = \{\mathtt{0},\mathtt{1}\}$ by giving mass ρ to $\mathtt{1}$, and giving the remaining mass $1-\rho$ to $\mathtt{0}$. Let $\eta \equiv \eta_\lambda$ be the law of this measure, and let $\zeta \equiv \zeta_\lambda$ denote the Dirac mass at η (cf. Remark 2.8.4). Recall from Proposition 2.1.2 that ρ has the same distribution as $1-\rho$. Using this symmetry, the quantities $\boldsymbol{u}_0$ and $\boldsymbol{u}_a(x)$ in Theorem 2.8.3 are equidistributed with $\boldsymbol{v}_0$ and $\boldsymbol{v}_a(x)$ where

$$\begin{aligned} \boldsymbol{v}_0 &\equiv 1-(1-e^{-\beta})\bigg\{\prod_{j=1}^k \rho_{0j} + \prod_{j=1}^k (1-\rho_{0j})\bigg\}, \\ (\boldsymbol{v}_a(\mathtt{0}),\boldsymbol{v}_a(\mathtt{1})) &\equiv \bigg(1-(1-e^{-\beta})\prod_{j=1}^{k-1}\rho_{0j}, 1-(1-e^{-\beta})\prod_{j=1}^{k-1}(1-\rho_{0j})\bigg). \end{aligned}$$

In the following calculation we will accumulate some error terms of size $O(e^{-\beta})$, which we will eventually take care of by sending $\beta\to\infty$. It is useful to recall that for any $a,b\geqslant 0$ and $\lambda\in[0,1]$ we have $(a+b)^\lambda \leqslant a^\lambda + b^\lambda$. It follows that for any $x\geqslant 0$ and any $\epsilon\in[-x,\infty)$,

$$|(x+\epsilon)^\lambda - x^\lambda| \leqslant |\epsilon|^\lambda. \tag{2.8.7}$$

(Note this bound is not useful for $\lambda = 0$, but in that case $(x+\epsilon)^\lambda = 1 = x^\lambda$.)

Lemma 2.8.10. *Let $\dot{\mu}_\lambda$ be the fixed point of Proposition 2.1.2. With $\dot{\mathfrak{Z}}_\lambda$ and $\hat{\mathfrak{Z}}_\lambda$ as in (2.1.8),*

$$\begin{aligned} \mathbb{E}[(\boldsymbol{u}_0)^\lambda] &= \hat{\mathfrak{Z}}_\lambda + O(e^{-\lambda\beta}), \\ \mathbb{E}\bigg[\bigg(\sum_{x\in\{\mathtt{0},\mathtt{1}\}^k}\prod_{a=1}^d \boldsymbol{u}_a(x)\bigg)^\lambda\bigg] &= (\hat{\mathfrak{Z}}_\lambda/\bar{\mathfrak{Z}}_\lambda)^d\,\dot{\mathfrak{Z}}_\lambda + O(e^{-\lambda\beta}). \end{aligned}$$

Proof. We assume $\lambda \in (0,1]$, since for $\lambda = 0$ there is nothing to prove. It follows straightforwardly from the above definitions that

$$\mathbb{E}[(\boldsymbol{u}_0)^\lambda] = \mathbb{E}[(\boldsymbol{v}_0)^\lambda] = \hat{\mathfrak{Z}}_\lambda + O(e^{-\lambda\beta}),$$

where the $O(e^{-\lambda\beta})$ error is by an application of (2.8.7). Next, let

$$\boldsymbol{z}_a \equiv \boldsymbol{v}_a(0) + \boldsymbol{v}_a(1), \quad \boldsymbol{r}_a \equiv \boldsymbol{v}_a(1)/\boldsymbol{z}_a.$$

Recall from (2.1.7) the definition of the distributional recursion $\hat{\mathscr{R}}_\lambda : \dot{\mu}_\lambda \mapsto \hat{\mu}_\lambda$, and the associated normalizing constant $\hat{\mathscr{Z}}(\dot{\mu}_\lambda)$. For any continuous bounded function $f : [0,1]^d \to \mathbb{R}$,

$$\begin{aligned}
&\int f(\boldsymbol{r}_1, \ldots, \boldsymbol{r}_d)\Big(\prod_{a=1}^d \boldsymbol{z}_a\Big)^\lambda \prod_{a=1}^d \Big\{\prod_{j=1}^{k-1} \dot{\mu}_\lambda(d\rho_{aj})\Big\} \\
&= \hat{\mathscr{Z}}(\dot{\mu}_\lambda)^d \int f(\hat{\rho}_1, \ldots, \hat{\rho}_d) \prod_{a=1}^d \hat{\mu}_\lambda(d\hat{\rho}_a) + O(e^{-\lambda\beta}).
\end{aligned}$$

It follows from this that

$$\begin{aligned}
&\mathbb{E}\Big[\Big(\sum_{x \in \{0,1\}^k} \prod_{a=1}^d \boldsymbol{u}_a(x)\Big)^\lambda\Big] + O(e^{-\lambda\beta}) \\
&= \hat{\mathscr{Z}}(\dot{\mu}_\lambda)^d \int \Big(\prod_{a=1}^d \hat{\rho}_a + \prod_{a=1}^d (1-\hat{\rho}_a)\Big)^\lambda \prod_{a=1}^d \hat{\mu}_\lambda(d\hat{\rho}_a) = \hat{\mathscr{Z}}(\dot{\mu}_\lambda)^d \dot{\mathfrak{Z}}_\lambda.
\end{aligned}$$

Finally, it is straightforward to check that for the fixed point $\dot{\mu}_\lambda$ we have

$$\hat{\mathscr{Z}}(\dot{\mu}_\lambda)\bar{\mathfrak{Z}}_\lambda = \hat{\mathfrak{Z}}_\lambda, \tag{2.8.8}$$

so the lemma follows. □

Proof of Proposition 2.3.19. Applying Lemma 2.8.10 to the bound of Theorem 2.8.3, we have

$$F_n(\beta) \leqslant \lambda^{-1}\Big(\ln \dot{\mathfrak{Z}}_\lambda + \alpha \ln \hat{\mathfrak{Z}}_\lambda - d \ln \bar{\mathfrak{Z}}_\lambda + O(e^{-\lambda\beta})\Big) = \lambda^{-1}\Big(\mathfrak{F}(\lambda) + O(e^{-\lambda\beta})\Big).$$

A standard argument gives that for any finite β, $n^{-1} \ln Z_n(\beta)$ is well-concentrated around its expected value $F_n(\beta)$.[5] Thus, for any fixed $\lambda \in (0,1]$ and $\epsilon > 0$, we can choose $\beta = \beta(\lambda, \epsilon)$ sufficiently large so that

$$\limsup_{n\to\infty} \mathbb{P}\Big((Z_n(\beta))^{1/n} \geqslant \exp\{(1+\epsilon)\lambda^{-1}\mathfrak{F}(\lambda)\}\Big) = 0.$$

Since $Z_n \leqslant Z_n(\beta)$ for any finite β, we conclude

$$\mathsf{f}(\alpha) \leqslant \inf\{\lambda^{-1}\mathfrak{F}(\lambda) : \lambda \in (0,1]\}.$$

For $\alpha < \alpha_{\text{sat}}$, if $\lambda = \lambda_\star \in (0,1)$ then $\lambda^{-1}\mathfrak{F}(\lambda) \leqslant s_\star = \mathsf{f}^{1\text{RSB}}(\alpha)$. If instead $\lambda = \lambda_\star = 1$ then again $\lambda^{-1}\mathfrak{F}(\lambda) = s_\star + \Sigma(s_\star) = \mathsf{f}^{1\text{RSB}}(\alpha)$. In any case this proves $\mathsf{f}(\alpha) \leqslant \mathsf{f}^{1\text{RSB}}(\alpha)$. □

[5] Take the Doob martingale of $\ln Z_n(\beta)$ with respect to the clause-revealing filtration for the random NAE-SAT instance, then apply the Azuma–Hoeffding concentration bound.

2.9 Contraction estimates

In this section we prove Propositions 2.4.2 and 2.4.3, as well as Lemma 2.4.4.

2.9.1 Single-copy coloring recursions

We first analyze the BP recursions for the single-copy coloring model, and prove Proposition 2.4.2. We first consider the BP recursion with fixed parameters $\lambda \in [0,1]$ and $1 \leqslant T \leqslant \infty$. Recall that we have restricted our attention to measures $\dot{Q}, \hat{Q}$ such that

$$\begin{aligned} \dot{Q}(\sigma) &\cong \dot{q}(\dot{\sigma})\mathbf{1}\{|\sigma| \leqslant T\}, \\ \hat{Q}(\sigma) &\cong \hat{q}(\hat{\sigma})\mathbf{1}\{|\sigma| \leqslant T\} \end{aligned}$$

for some probability measures $\dot{q}, \hat{q}$ defined on $\dot{\Omega}_T, \hat{\Omega}_T$. Recall further that we can assume $\dot{q} = \dot{q}^{\mathrm{avg}}$ and $\hat{q} = \hat{q}^{\mathrm{avg}}$. For measures of this type we can give a fairly explicit description of the BP recursion. In what follows it will be convenient to take the convention

$$\dot{m}(\mathtt{r}_1) = \hat{m}(\mathtt{b}_1) = 1, \quad \dot{m}(\mathtt{r}_0) = \hat{m}(\mathtt{b}_0) = 0. \tag{2.9.1}$$

For $x \in \{\mathtt{0}, \mathtt{1}\}$ we abbreviate

$$\mathtt{g} \equiv \mathtt{b} \cup \mathtt{f},\ \mathtt{g}_x \equiv \mathtt{b}_x \cup \mathtt{f},\ \mathtt{y} \equiv \mathtt{r} \cup \mathtt{f},\ \mathtt{p}_x \equiv \mathtt{b}_x \cup \mathtt{r}_x.$$

The variable recursion $\dot{\mathtt{BP}} \equiv \dot{\mathtt{BP}}_{\lambda,T}$ is given by

$$(\dot{\mathtt{BP}}\hat{q})(\dot{\sigma}) \cong \begin{cases} \hat{q}(\mathtt{p}_1)^{d-1} & \dot{\sigma} \in \{\mathtt{r}_0, \mathtt{r}_1\}, \\ \hat{q}(\mathtt{p}_1)^{d-1} - \hat{q}(\mathtt{b}_1)^{d-1} & \dot{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}, \\ \dot{z}(\dot{\sigma})^{\lambda} \displaystyle\sum_{\hat{\sigma}_2,\ldots,\hat{\sigma}_d} \mathbf{1}\{\dot{\sigma} = \dot{\mathtt{T}}((\hat{\sigma}_i)_{i\geqslant 2})\} \prod_{i=2}^{d} \hat{q}(\hat{\sigma}_i) & \dot{\sigma} \in \dot{\Omega}_{\mathtt{f}} \cap \dot{\Omega}_T, \end{cases}$$

where $\cong$ indicates the normalization which makes $\dot{\mathtt{BP}}\hat{q}$ a probability measure on $\dot{\Omega}_T$.

For the clause BP recursion, by symmetry it suffices to consider a clause a with all incident edge literals $\mathtt{L}_{aj} = \mathtt{0}$. We write $\underline{\dot{\sigma}} \sim \hat{\sigma}$ if $\underline{\dot{\sigma}} \equiv (\dot{\sigma}_2, \ldots, \dot{\sigma}_k) \in (\dot{\Omega}_T)^{k-1}$ is compatible with $\hat{\sigma}$, in the sense that there is a valid coloring $\underline{\sigma}$ of δa with

$$\underline{\sigma} = ((\dot{\sigma}, \hat{\sigma}), (\dot{\sigma}_2, \hat{\sigma}_2), \ldots (\dot{\sigma}_k, \hat{\sigma}_k)) \in (\Omega_T)^k. \tag{2.9.2}$$

The clause recursion $\hat{\mathtt{BP}} \equiv \hat{\mathtt{BP}}_{\lambda,T}$ is given by

$$(\hat{\mathtt{BP}}\dot{q})(\hat{\sigma}) \cong \begin{cases} \dot{q}(\mathtt{b}_0)^{k-1} & \hat{\sigma} \in \{\mathtt{r}_0, \mathtt{r}_1\}, \\ \hat{z}(\hat{\sigma})^{\lambda} \displaystyle\sum_{\underline{\dot{\sigma}}} \mathbf{1}\{\hat{\sigma} = \hat{\mathtt{T}}((\dot{\sigma}_i)_{i\geqslant 2})\} \prod_{i=2}^{k} \dot{q}(\dot{\sigma}_i) & \hat{\sigma} \in \hat{\Omega}_{\mathtt{f}} \cap \hat{\Omega}_T, \\ \displaystyle\sum_{\underline{\dot{\sigma}} \sim \mathtt{b}_1} \Big(1 - \prod_{i=2}^{k} \dot{m}(\dot{\sigma}_i)\Big)^{\lambda} \prod_{i=2}^{k} \dot{q}(\dot{\sigma}_i) & \hat{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}, \end{cases}$$

where the last line uses the convention (2.9.1). Recall that $\mathtt{BP} \equiv \dot{\mathtt{BP}} \circ \hat{\mathtt{BP}} \equiv \mathtt{BP}_{\lambda,T}$. We will show the following contraction result.

Proposition 2.9.1. *Suppose $\dot{q}_1, \dot{q}_2$ belong to $\mathbf{\Gamma}$, as defined by (2.4.5). Let $\mathtt{BP} \equiv \mathtt{BP}_{\lambda,T}$ for $\lambda \in [0,1]$ and $1 \leqslant T \leqslant \infty$. Then $\mathtt{BP}\dot{q}_1, \mathtt{BP}\dot{q}_2 \in \mathbf{\Gamma}$ and $\|\mathtt{BP}\dot{q}_1 - \mathtt{BP}\dot{q}_2\|_1 = O(k^2/2^k)\|\dot{q}_1 - \dot{q}_2\|_1$.*

Before the proof of Proposition 2.9.1 we deduce the following consequences:

Proof of Proposition 2.4.2. Let $\dot{q}^{(0)}$ be the uniform measure on $\{\mathtt{b}_0, \mathtt{b}_1, \mathtt{r}_1, \mathtt{r}_0\}$, and recursively define $\dot{q}^{(l)} \equiv \mathtt{BP}(\dot{q}^{(l-1)})$. It is clear that $\dot{q}^{(0)} \in \mathbf{\Gamma}$, so Proposition 2.9.1 implies $\dot{q}^{(l)} \in \mathbf{\Gamma}$ for all $l \geqslant 1$, and furthermore that $(\dot{q}^{(l)})_{l \geqslant 1}$ forms an ℓ^1 Cauchy sequence. By completeness of ℓ^1 we conclude that there exists $\dot{q}^{(\infty)} = \dot{q}_\star \in \mathbf{\Gamma}$ satisfying

$$\lim_{l \to \infty} \|\dot{q}^{(l)} - \dot{q}_\star\|_1 = 0, \quad \mathtt{BP}\dot{q}_\star = \dot{q}_\star.$$

Applying Proposition 2.9.1 again gives $\|\mathtt{BP}\dot{q} - \dot{q}_\star\|_1 = O(k^2/2^k)\|\dot{q} - \dot{q}_\star\|_1$ for any $\dot{q} \in \mathbf{\Gamma}$, from which it follows that $\dot{q}_\star$ is the unique fixed point of $\mathtt{BP}$ in $\mathbf{\Gamma}$. ☐

Corollary 2.9.2. *For $\lambda \in [0,1]$ and $1 \leqslant T \leqslant \infty$, let $\dot{q}_{\lambda,T}$ be the fixed point of $\mathtt{BP}_{\lambda,T}$ given by Proposition 2.4.2. Then $\|\dot{q}_{\lambda,T} - \dot{q}_{\lambda,\infty}\|_1 \to 0$ in the limit $T \to \infty$.*

Proof. For each $1 \leqslant T \leqslant \infty$, let $(\dot{q}_{\lambda,T})^{(l)}$ $(l \geqslant 0)$ be defined in the same way as $\dot{q}^{(l)}$ in the proof of Proposition 2.9.1. It follows from the definition that $(\dot{q}_{\lambda,T})^{(l)} = (\dot{q}_{\lambda,\infty})^{(l)}$ for all $l \leqslant l_T$, where $l_T \equiv \ln T / \ln(dk)$. By the triangle inequality and Proposition 2.4.2,

$$\|\dot{q}_{\lambda,T} - \dot{q}_{\lambda,\infty}\|_1 \leqslant \|\dot{q}_{\lambda,T} - (\dot{q}_{\lambda,\infty})^{(l_T)}\|_1 + \|(\dot{q}_{\lambda,\infty})^{(l_T)} - \dot{q}_{\lambda,\infty}\|_1 \leqslant (C/2^k)^{l_T}$$

for some absolute constant k. The result follows assuming $k \geqslant k_0$. ☐

We now turn to the proof of Proposition 2.9.1. We work with the non-normalized BP recursions $\mathtt{N}\dot{\mathtt{BP}} \equiv \mathtt{N}\dot{\mathtt{BP}}_{\lambda,T}$ and $\mathtt{N}\hat{\mathtt{BP}} \equiv \mathtt{N}\hat{\mathtt{BP}}_{\lambda,T}$, defined by substituting "$\cong$" with "$=$" in the definitions of $\dot{\mathtt{BP}}$ and $\hat{\mathtt{BP}}$ respectively. One can then recover $\dot{\mathtt{BP}}, \hat{\mathtt{BP}}$ from $\mathtt{N}\dot{\mathtt{BP}}, \mathtt{N}\hat{\mathtt{BP}}$ via

$$(\dot{\mathtt{BP}}\hat{p})(\dot{\sigma}) = \frac{(\mathtt{N}\dot{\mathtt{BP}}\hat{p})(\dot{\sigma})}{\sum_{\dot{\sigma}' \in \dot{\Omega}} (\mathtt{N}\dot{\mathtt{BP}}\hat{p})(\dot{\sigma}')}, \quad (\hat{\mathtt{BP}}\dot{p})(\hat{\sigma}) = \frac{(\mathtt{N}\hat{\mathtt{BP}}\dot{p})(\hat{\sigma})}{\sum_{\hat{\sigma}' \in \hat{\Omega}} (\mathtt{N}\hat{\mathtt{BP}}\dot{p})(\hat{\sigma}')}.$$

Let $\dot{p}$ be the reweighted measure defined by

$$\dot{p}(\dot{\sigma}) \equiv [\dot{p}(\dot{q})](\dot{\sigma}) \equiv \frac{\dot{q}(\dot{\sigma})}{1 - \dot{q}(\mathtt{r})}. \tag{2.9.3}$$

In the above we have assumed that the inputs to $\dot{\mathtt{BP}}, \hat{\mathtt{BP}}, \mathtt{N}\dot{\mathtt{BP}}, \mathtt{N}\hat{\mathtt{BP}}$ are probability measures; we now extend them in the obvious manner to non-negative measures with strictly positive total mass.

Given two measures r_1, r_2 defined on any space $\mathcal{X}$, we denote $\Delta r(x) \equiv |r_1(x) - r_2(x)|$. We regard Δr as a non-negative measure on $\mathcal{X}$: for any subset $S \subseteq \mathcal{X}$,

$$\Delta r(S) = \sum_{x \in S} |r_1(x) - r_2(x)| \geqslant |r_1(S) - r_2(S)|,$$

where the inequality may be strict. For any non-negative measure $\hat{r}$ on $\hat{\Omega}$, we abbreviate

$$\begin{aligned} \hat{m}^\lambda \hat{r}(\hat{\sigma}) &\equiv \hat{m}(\hat{\sigma})^\lambda \hat{r}(\hat{\sigma}), \\ (1-\hat{m})^\lambda \hat{r}(\hat{\sigma}) &\equiv (1-\hat{m}(\hat{\sigma}))^\lambda \hat{r}(\hat{\sigma}). \end{aligned}$$

In what follows we will begin with two measures in $\mathbf{\Gamma}$, and show that they contract under one step of the BP recursion. Let $\mathtt{N}\hat{\mathtt{BP}}$ and $\mathtt{N}\dot{\mathtt{BP}}$ be the non-normalized single-copy BP recursions at parameters λ, T. Starting from $\dot{q}_i \in \mathbf{\Gamma}$ $(i = 1, 2)$, denote

$$\begin{aligned} \dot{p}_i &\equiv \dot{p}(\dot{q}_i) \text{ (as defined by (2.9.3))}, \\ \hat{p}_i &\equiv \mathtt{N}\hat{\mathtt{BP}}(\dot{p}_i) \text{ and } \hat{p}_{i,\infty} \equiv \mathtt{N}\hat{\mathtt{BP}}_{\lambda,\infty}(\dot{p}_i), \\ \dot{p}_i^{\mathrm{u}} &\equiv \mathtt{N}\dot{\mathtt{BP}}(\hat{p}_i) \text{ and } \tilde{q}_i \equiv \dot{\mathtt{BP}}\hat{p}_i = \mathtt{BP}\dot{q}_i. \end{aligned}$$

With this notation in mind, the proof of Proposition 2.9.1 is divided into four lemmas.

Lemma 2.9.3 (effect of reweighting)**.** *Assuming $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}$, $\|\Delta \dot{p}\|_1 = O(1)\|\dot{q}_1 - \dot{q}_2\|_1$, where $O(1)$ indicates a constant depending on the constant appearing in (2.4.5).*

Lemma 2.9.4 (clause BP)**.** *Assuming $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}$,*

$$\begin{aligned} \hat{m}^\lambda \hat{p}_i(\square) &= 1 - 4/2^k + O(k/4^k), \\ \hat{m}^\lambda \hat{p}_i(\mathtt{f}) &= \hat{m}^\lambda \hat{p}_i(\square) + O(k/4^k), \\ \hat{m}^\lambda \hat{p}_i(\mathtt{b}_1) &= 1 + O(k/2^k), \\ \hat{m}^\lambda \hat{p}_i(\mathtt{r}_1) &= (2/2^k)[1 + O(k/2^k)]. \end{aligned} \tag{2.9.4}$$

Further, writing $\Delta \hat{m}^\lambda \hat{p}(\cdot) \equiv \hat{m}^\lambda(\cdot)|\hat{p}_1(\cdot) - \hat{p}_2(\cdot)|$,

$$\begin{aligned} \Delta \hat{m}^\lambda \hat{p}(\mathtt{f}) + \Delta \hat{m}^\lambda \hat{p}(\mathtt{r}) &= O(k/2^k)\Delta \dot{p}(\mathtt{f}), \\ \|\Delta \hat{m}^\lambda \hat{p}\|_1 &= O(k^2/2^k)\|\Delta \dot{p}\|_1. \end{aligned} \tag{2.9.5}$$

(Recall that $\hat{p}(\hat{\sigma} \oplus \mathtt{1}) = \hat{p}(\hat{\sigma})$ and $\hat{m}(\hat{\sigma} \oplus \mathtt{1}) = 1 - \hat{m}(\hat{\sigma})$, so $(1-\hat{m})^\lambda \hat{p}(\hat{\sigma}) = \hat{m}^\lambda \hat{p}(\hat{\sigma} \oplus \mathtt{1})$. As a result, the bounds for $\Delta \hat{m}^\lambda \hat{p}$ imply analogous bounds for $\Delta(1-\hat{m})^\lambda \hat{p}$.)

Lemma 2.9.5 (variable BP, non-normalized)**.** *Assuming $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}$,*

$$\begin{bmatrix} \dot{p}_i^{\mathrm{u}}(\mathtt{f}) \\ \dot{p}_i^{\mathrm{u}}(\mathtt{r}) \end{bmatrix} = \begin{bmatrix} O(2^{-k}) \\ 1 + O(2^{-k}) \end{bmatrix} \dot{p}_i^{\mathrm{u}}(\mathtt{b}), \quad \begin{bmatrix} \Delta \dot{p}^{\mathrm{u}}(\mathtt{f}) \\ \Delta \dot{p}^{\mathrm{u}}(\mathtt{b}) \\ \Delta \dot{p}^{\mathrm{u}}(\mathtt{r}) \end{bmatrix} = \begin{bmatrix} O(k) \\ O(k2^k) \\ O(k2^k) \end{bmatrix} \|\Delta \hat{m}^\lambda \hat{p}\|_1 \max_{i=1,2} \left\{ \dot{p}_i^{\mathrm{u}}(\mathtt{b}) \right\}. \tag{2.9.6}$$

Lemma 2.9.6 (variable BP, normalized)**.** *Assuming $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}$, we have $\tilde{q}_1, \tilde{q}_2 \in \mathbf{\Gamma}$ as well, with $\|\tilde{q}_1 - \tilde{q}_2\|_1 \lesssim k\|\Delta \hat{m}^\lambda \hat{p}\|_1$.*

Proof of Proposition 2.9.1. Follows by combining the four preceding lemmas 2.9.3–2.9.6. □

We now prove the four lemmas.

Proof of Lemma 2.9.3. This follows from the elementary identity

$$\frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{1}{b_1}(a_1 - a_2) + \frac{b_2 - b_1}{b_1 b_2} a_2. \tag{2.9.7}$$

together with (2.4.5). □

In the proof of the next two lemmas, the following elementary fact will be used repeatedly: suppose for $1 \leqslant l \leqslant m$ that we have non-negative measures a^l, b^l over a finite set $\mathcal{X}^l$. Then, denoting $\underline{\mathcal{X}} = \mathcal{X}^1 \times \cdots \times \mathcal{X}^m$, we have

$$\begin{aligned}\sum_{\underline{x} \in \underline{\mathcal{X}}} \bigg| \prod_{l=1}^m a^l(x^l) - \prod_{l=1}^m b^l(x^l) \bigg| &\leqslant \sum_{l=1}^m \sum_{\underline{x} \in \underline{\mathcal{X}}} \bigg\{ \prod_{1 \leqslant j < l} b^j(x^j) \bigg\} \bigg\{ \prod_{l < j \leqslant m} a^j(x^j) \bigg\} \Big| a^l(x^l) - b^l(x^l) \Big| \\ &\leqslant \sum_{l=1}^m \|a^l - b^l\|_1 \prod_{j \neq l} \Big(\|a^j\|_1 + \|a^j - b^j\|_1 \Big). \end{aligned} \tag{2.9.8}$$

If all the $(\mathcal{X}^l, a^l, b^l)$ are the same $(\mathcal{X}, a, b)$, this reduces to the bound

$$\sum_{x_1, \ldots, x_m \in \mathcal{X}} \bigg| \prod_{i=1}^m a(x_i) - \prod_{i=1}^m b(x_i) \bigg| \leqslant m \|a - b\|_1 \Big(\|a\|_1 + \|a - b\|_1 \Big)^{m-1}. \tag{2.9.9}$$

In what follows we will abbreviate (for $x \in \{\mathtt{0}, \mathtt{1}\}$)

$$\mathsf{a}_x \equiv \Big\{ \hat{\sigma} \in \hat{\Omega}_T : \underline{\dot{\sigma}} \in (\mathsf{g}_x)^{k-1} \text{ for all } \underline{\dot{\sigma}} \sim \hat{\sigma} \Big\}. \tag{2.9.10}$$

Proof of Lemma 2.9.4. From the definition, if $\dot{p} = \dot{p}(\dot{q})$ then

$$\dot{p}(\mathtt{b}) = \frac{\dot{q}(\mathtt{b})}{1 - \dot{q}(\mathtt{r})} = \frac{\dot{q}(\mathtt{b})}{\dot{q}(\mathtt{g})} = 1 - \dot{p}(\mathtt{f}).$$

It follows that for any $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}$ we have

$$\Delta \dot{p}(\mathtt{b}) \leqslant \Delta \dot{p}(\mathtt{f}) \leqslant \dot{p}_1(\mathtt{f}) + \dot{p}_2(\mathtt{f}) = O(2^{-k}).$$

Another consequence of the definition of $\mathbf{\Gamma}$ is that $\|\Delta \dot{p}\|_1 = O(1)$. We now control $\Delta \hat{m}^\lambda \hat{p}(\hat{\sigma})$, distinguishing a few cases:

1. We first consider $\hat{\sigma} \in \hat{\Omega} \backslash \{\mathtt{b}, \square\}$. For such $\hat{\sigma}$ we have

$$\Delta \hat{m}^\lambda \hat{p}(\hat{\sigma}) = \bigg| [\hat{m}(\hat{\sigma}) \hat{z}(\hat{\sigma})]^\lambda \sum_{\underline{\dot{\sigma}} \sim \hat{\sigma}} \bigg(\prod_{j=2}^k \dot{p}_1(\dot{\sigma}_j) - \prod_{j=2}^k \dot{p}_2(\dot{\sigma}_j) \bigg) \bigg|,$$

and it is easy to check that

$$\hat{m}(\hat{\sigma})\hat{z}(\hat{\sigma}) = 1 - \prod_{j=2}^{k} \dot{m}(\dot{\sigma}_j) \in [0,1].$$

Note moreover that any such $\hat{\sigma}$ must belong to $\mathtt{a}_0$ or $\mathtt{a}_1$. By summing over $\hat{\sigma} \in \mathtt{a}_0$ and applying (2.9.9) we have

$$\Delta\hat{m}^\lambda\hat{p}(\mathtt{a}_0) \leqslant (k-1)\Delta\dot{p}(\mathtt{g}_0)\Big(\dot{p}_1(\mathtt{g}_0) + \Delta\dot{p}(\mathtt{f})\Big)^{k-2}.$$

Recalling that $\dot{p}_1, \dot{p}_2 \in \mathbf{\Gamma}$, in the above we have $\dot{p}_1(\mathtt{g}_0) + \Delta\dot{p}(\mathtt{f}) \leqslant [1 + O(2^{-k})]/2$, as well as $\Delta\dot{p}(\mathtt{g}_0) = O(1)\Delta\dot{p}(\mathtt{f})$. Combining these gives

$$\Delta\hat{m}^\lambda\hat{p}(\mathtt{a}_0) = O(k/2^k)\Delta\dot{p}(\mathtt{f}),$$

and the same bound holds for $\Delta\hat{m}^\lambda\hat{p}(\mathtt{a}_1)$.

2. Next consider $\hat{\sigma} = \square$, for which we have $\hat{m}(\hat{\sigma}) = 1/2$ and $\hat{z}(\hat{\sigma}) = 2$. Thus

$$\hat{m}^\lambda\hat{p}(\square) = 1 - \dot{p}(\mathtt{g}_0)^{k-1} - \dot{p}(\mathtt{g}_1)^{k-1} + \dot{p}(\mathtt{f})^{k-1}. \tag{2.9.11}$$

Arguing as above gives $\Delta\hat{m}^\lambda\hat{p}(\square) = O(k/2^k)\Delta\dot{p}(\mathtt{f})$, proving the first half of (2.9.5).

3. Lastly consider $\hat{\sigma} \in \{\mathtt{b}_0, \mathtt{b}_1\}$. Recalling (2.9.1) we have $\Delta\hat{m}^\lambda\hat{p}(\mathtt{b}_0) = 0$, so let us take $\hat{\sigma} = \mathtt{b}_1$, and consider $\underline{\dot{\sigma}} \sim \mathtt{b}_1$. Note that if $\underline{\dot{\sigma}} \sim \mathtt{b}_1$ has no $\mathtt{red}$ spin, then there must exist some $\hat{\sigma} \in \hat{\Omega}_{\mathtt{f}}$ such that $\underline{\dot{\sigma}} \sim \hat{\sigma}$ as well. Conversely, if $\hat{\sigma} \in \hat{\Omega}_{\mathtt{f}} \cap \hat{\Omega}_T$ and $\underline{\dot{\sigma}} \sim \hat{\sigma}$, then $\underline{\dot{\sigma}} \sim \mathtt{b}_1$, unless $\underline{\dot{\sigma}}$ has exactly one spin $\dot{\sigma}_i \in \{\mathtt{b}_0, \mathtt{f}\}$ with the remaining $k-2$ spins equal to $\mathtt{b}_1$.[6] Again making use of (2.9.1), this $\underline{\dot{\sigma}}$ gives the same contribution to $\hat{m}^\lambda\hat{p}_\infty(\hat{\sigma}')$ as to $\hat{m}^\lambda\hat{p}(\mathtt{b}_1)$. It follows that

$$\Delta\hat{m}^\lambda\hat{p}(\mathtt{b}_1) \leqslant \Delta\hat{m}^\lambda\hat{p}_\infty(\mathtt{y}) + k\Big|\dot{p}_1(\mathtt{r}_0)\dot{p}_1(\mathtt{b}_1)^{k-2} - \dot{p}_2(\mathtt{r}_0)\dot{p}_2(\mathtt{b}_1)^{k-2}\Big|.$$

The first term on the right-hand side captures the contribution from those $\underline{\dot{\sigma}}$ with no $\mathtt{red}$ spin, and by the preceding arguments it is $O(k/2^k)\Delta\dot{p}(\mathtt{f})$. It is easy to check that the second term is $O(k^2/2^k)\|\Delta\dot{p}\|_1$, which finishes the second part of (2.9.5).

Combining the above estimates proves (2.9.5). We next prove (2.9.4). Denote $\mathtt{f}_{\geqslant 1} \equiv \{\mathtt{f}\}\backslash\{\square\}$. Since $\dot{q}_i \in \mathbf{\Gamma}$, we must have from (2.4.5) that

$$\hat{m}^\lambda\hat{p}_i(\mathtt{f}_{\geqslant 1}) \leqslant 2\sum_{l=1}^{k-1}\binom{k-1}{l}\dot{p}_i(\mathtt{f})^l\dot{p}_i(\mathtt{b}_0)^{k-1-l} \leqslant 2\dot{p}_i(\mathtt{b}_0)^{k-1}\sum_{l=1}^{k-1}\left(\frac{k\dot{p}_i(\mathtt{f})}{\dot{p}_i(\mathtt{b}_0)}\right)^l = O(k/4^k). \tag{2.9.12}$$

[6] The converse is not needed for the final bound, but we mention it for the sake of concreteness.

On the other hand, we see from (2.9.11) that

$$\hat{m}^\lambda \hat{p}_i(\square) = 1 - 4/2^k + O(k/4^k).$$

It follows that

$$\begin{aligned}\hat{m}^\lambda \hat{p}_i(\mathtt{b}_1) = \hat{p}_i(\mathtt{b}_1) &= \hat{m}^\lambda \hat{p}_{i,\infty}(\mathtt{f}) + (k-1)\Big[\dot{p}_i(\mathtt{r}_0) - \dot{p}_i(\mathtt{g}_0)\Big]\dot{p}_i(\mathtt{b}_1)^{k-2} \\ &\leqslant \hat{m}^\lambda \hat{p}_{i,\infty}(\mathtt{f}) + (k-1)\dot{p}_i(\mathtt{r}_0)\dot{p}_i(\mathtt{b}_1)^{k-2} = 1 + O(k/2^k).\end{aligned} \tag{2.9.13}$$

For a lower bound it suffices to consider the contribution from clauses with all k incident edges colored `blue`:

$$\hat{m}^\lambda \hat{p}_i(\mathtt{b}_1) = \hat{p}_i(\mathtt{b}_1) \geqslant \dot{p}_i(\mathtt{b})^{k-1}[1 - O(k/2^k)] = 1 - O(k/2^k). \tag{2.9.14}$$

Lastly, note by symmetry that

$$\hat{m}^\lambda \hat{p}_i(\mathtt{r}_1) = \hat{p}_i(\mathtt{r}_1) = \dot{p}_i(\mathtt{b}_0)^{k-1} = (2/2^k)\dot{p}_i(\mathtt{b})^{k-1}.$$

Combining these estimates proves (2.9.4). $\square$

Proof of Lemma 2.9.5. We control $\dot{p}^{\mathrm{u}}$ and $\Delta\dot{p}^{\mathrm{u}}$ in two cases.

1. First consider $\dot{\sigma} \in \dot{\Omega}_{\mathtt{f}}$. Up to permutation there is a unique $\underline{\hat{\sigma}} \in (\hat{\Omega}_{\mathtt{f}})^{d-1}$ such that $\dot{\sigma} = \hat{\mathtt{T}}(\underline{\hat{\sigma}})$. Let $\mathsf{comb}(\dot{\sigma})$ denote the number of distinct tuples $\underline{\hat{\sigma}}'$ that can be obtained by permuting the coordinates of $\underline{\hat{\sigma}}$. For this $\underline{\hat{\sigma}}$ we have

$$\prod_{j=2}^{d} \hat{m}(\hat{\sigma}_j)^\lambda \leqslant \dot{z}(\dot{\sigma})^\lambda \leqslant \prod_{j=2}^{d} \hat{m}(\hat{\sigma}_j)^\lambda + \prod_{j=2}^{d}(1 - \hat{m}(\hat{\sigma}_j))^\lambda, \tag{2.9.15}$$

where the rightmost inequality uses that $(a+b)^\lambda \leqslant a^\lambda + b^\lambda$ for $a, b \geqslant 0$ and $\lambda \in [0,1]$. It follows that for $i = 1, 2$ we have

$$\mathsf{comb}(\dot{\sigma}) \prod_{j=2}^{d} \hat{m}\hat{p}_i(\hat{\sigma}_j) \leqslant \dot{p}_i^{\mathrm{u}}(\dot{\sigma}) \leqslant \mathsf{comb}(\dot{\sigma}) \bigg\{ \prod_{j=2}^{d} \hat{m}^\lambda \hat{p}_i(\hat{\sigma}_j) + \prod_{j=2}^{d}(1-\hat{m})^\lambda \hat{p}_i(\hat{\sigma}_j) \bigg\}.$$

It follows by symmetry that $\hat{m}^\lambda \hat{p}_i(\mathtt{f}) = (1-\hat{m})^\lambda \hat{p}_i(\mathtt{f})$, so

$$[\hat{m}^\lambda \hat{p}_i(\square)]^{d-1} \leqslant \dot{p}_i^{\mathrm{u}}(\mathtt{f}) \leqslant [\hat{m}^\lambda \hat{p}_i(\mathtt{f})]^{d-1} + [(1-\hat{m})^\lambda \hat{p}_i(\mathtt{f})]^{d-1} = 2[\hat{m}^\lambda \hat{p}_i(\mathtt{f})]^{d-1}. \tag{2.9.16}$$

Making use of the symmetry together with (2.9.15) gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{f}) \leqslant 2 \sum_{\underline{\hat{\sigma}} \in (\hat{\Omega}_{\mathtt{f}})^{d-1}} \bigg| \prod_{j=2}^{d-1} \hat{m}^\lambda \hat{p}_1(\hat{\sigma}_j) - \prod_{j=2}^{d-1} \hat{m}^\lambda \hat{p}_2(\hat{\sigma}_j) \bigg|,$$

and applying (2.9.9) gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{f}) \lesssim d\|\Delta\hat{m}^\lambda\hat{p}\|_1\Big(\hat{m}^\lambda\hat{p}_1(\mathtt{f}) + \Delta\hat{m}^\lambda\hat{p}_1(\mathtt{f})\Big)^{d-2}.$$

Combining (2.9.4) with the lower bound from (2.9.15) then gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{f}) \lesssim d\|\Delta\hat{m}^\lambda\hat{p}\|_1 \max_{i=1,2}\Big\{\dot{p}^{\mathrm{u}}_i(\mathtt{f})\Big\}.$$

2. Next consider $\dot{\sigma} \in \{\mathtt{red}, \mathtt{blue}\}$: note that $\dot{p}^{\mathrm{u}}_i(\mathtt{r}_x) = \hat{p}_i(\mathtt{p}_x)^{d-1}$, and

$$\frac{\dot{p}^{\mathrm{u}}_i(\mathtt{r}_x) - \dot{p}^{\mathrm{u}}_i(\mathtt{b}_x)}{\dot{p}^{\mathrm{u}}_i(\mathtt{r}_x)} = \frac{\hat{p}_i(\mathtt{b}_x)^{d-1}}{\hat{p}_i(\mathtt{p}_x)^{d-1}} = \bigg(1 - \frac{\hat{p}_i(\mathtt{r}_x)}{\hat{p}_i(\mathtt{p}_x)}\bigg)^{d-1} = O(2^{-k}), \tag{2.9.17}$$

where the last estimate uses (2.9.4) and $d/k = 2^{k-1}\ln 2 + O(1)$. Applying (2.9.9) gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{p}_1) \lesssim d\|\hat{m}^\lambda\hat{p}\|_1\Big(\min_{i=1,2}\Big\{\hat{m}^\lambda\hat{p}_i(\mathtt{p}_1)\Big\} + \Delta\hat{m}^\lambda\hat{p}(\mathtt{p}_1)\Big)^{d-2}.$$

Suppose without loss that $\hat{m}^\lambda\hat{p}_1(\mathtt{b}_1) \leqslant \hat{m}^\lambda\hat{p}_2(\mathtt{b}_1)$: then

$$\begin{aligned}\hat{m}^\lambda\hat{p}_1(\mathtt{p}_1) + \Delta\hat{m}^\lambda\hat{p}(\mathtt{p}_1) &= \hat{m}^\lambda\hat{p}_2(\mathtt{b}_1) + \hat{m}^\lambda\hat{p}_1(\mathtt{r}_1) + \Delta\hat{m}^\lambda\hat{p}(\mathtt{r}_1)\\ &\leqslant \hat{m}^\lambda\hat{p}_2(\mathtt{p}_1) + 2\Delta\hat{m}^\lambda\hat{p}(\mathtt{r}_1),\end{aligned}$$

and substituting into the above gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{p}_1) \lesssim d\|\hat{m}^\lambda\hat{p}\|_1\Big(\max_{i=1,2}\Big\{\hat{m}^\lambda\hat{p}_i(\mathtt{p}_1)\Big\} + \Delta\hat{m}^\lambda\hat{p}(\mathtt{r}_1)\Big)^{d-2}.$$

From (2.9.5) and the definition (2.4.5) of $\mathbf{\Gamma}$ we have $\Delta\hat{m}^\lambda\hat{p}(\mathtt{r}_1) = O(k/2^k)\Delta\dot{p}(\mathtt{f}) = O(k/4^k)$. It follows from (2.9.17) that

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{p}_1) \lesssim d\|\Delta\hat{m}^\lambda\hat{p}\|_1 \max_{i=1,2}\Big\{\dot{p}^{\mathrm{u}}_i(\mathtt{b}_1)\Big\}. \tag{2.9.18}$$

It remains to show $\dot{p}^{\mathrm{u}}(\mathtt{f})/\dot{p}^{\mathrm{u}}(\mathtt{b}) = O(2^{-k})$. From (2.9.13),

$$\hat{m}^\lambda\hat{p}_i(\mathtt{f}) - \hat{m}^\lambda\hat{p}_i(\mathtt{b}_1) \leqslant \hat{m}^\lambda\hat{p}_{i,\infty}(\mathtt{f}) - \hat{m}^\lambda\hat{p}_i(\mathtt{b}_1) \leqslant (k-1)\Big[\dot{p}_i(\mathtt{g}_0) - \dot{p}_i(\mathtt{r}_0)\Big]\dot{p}_i(\mathtt{b}_1)^{k-2},$$

and from the definition of $\mathbf{\Gamma}$ the right-hand side is $O(k/4^k)\dot{p}_i(\mathtt{b})^{k-1}$. Now recall from (2.9.14) that $\hat{m}^\lambda\hat{p}_i(\mathtt{b}_1) \gtrsim \dot{p}_i(\mathtt{b})^{k-1}$. Combining these gives

$$\hat{m}^\lambda\hat{p}_i(\mathtt{f}) \leqslant [1 + O(k/4^k)]\hat{m}^\lambda\hat{p}_i(\mathtt{b}_1). \tag{2.9.19}$$

Recalling (2.9.15), it follows that

$$\frac{\dot{p}^{\mathrm{u}}_i(\mathtt{f})}{\dot{p}^{\mathrm{u}}_i(\mathtt{b}_1)} \lesssim \bigg(\frac{\hat{m}^\lambda\hat{p}_i(\mathtt{f})}{\hat{m}^\lambda\hat{p}_i(\mathtt{p}_1)}\bigg)^{d-1} \lesssim \bigg(\frac{\hat{m}^\lambda\hat{p}_i(\mathtt{b}_1)}{\hat{m}^\lambda\hat{p}_i(\mathtt{p}_1)}\bigg)^{d-1} \lesssim 2^{-k},$$

where the last step uses (2.9.4). This concludes the proof. $\square$

Proof of Lemma 2.9.6. Denote $\tilde{q}_i \equiv \dot{\mathtt{BP}}\dot{q}_i$ and $\Delta\tilde{q} \equiv |\tilde{q}_1 - \tilde{q}_2|$. We first check that $\tilde{q}_i$ lies in $\mathbf{\Gamma}$: the first condition of (2.4.5) follows from (2.9.6), and the second is automatically satisfied from the definition of $\dot{\mathtt{BP}}$. Next we bound $\Delta\tilde{q}$. With some abuse of notation, we shall write $\tilde{q}_i(\mathtt{R}) \equiv \tilde{q}_i(\mathtt{r}) - \tilde{q}_i(\mathtt{b})$ and

$$\Delta\tilde{q}(\mathtt{R}) \equiv |(\tilde{q}_1(\mathtt{r}) - \tilde{q}_1(\mathtt{b})) - (\tilde{q}_2(\mathtt{r}) - \tilde{q}_2(\mathtt{b}))|.$$

Let $\dot{p}^{\mathrm{u}}_i(\mathtt{R})$ and $\Delta\dot{p}^{\mathrm{u}}(\mathtt{R})$ be similarly defined. Arguing similarly as in the derivation of (2.9.18),

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{R}) = 2|\hat{p}_1(\mathtt{b}_1)^{d-1} - \hat{p}_2(\mathtt{b}_1)^{d-1}| \lesssim k\|\Delta\hat{m}^\lambda\hat{p}\|_1 \max_{i=1,2}\left\{\dot{p}^{\mathrm{u}}_i(\mathtt{b})\right\} \tag{2.9.20}$$

Recalling $\|\tilde{q}_i\|_1 = 1$, we have

$$\begin{aligned} 2\tilde{q}_i(\mathtt{r}) &= [1 - \tilde{q}_i(\mathtt{f})] + [\tilde{q}_i(\mathtt{r}) - \tilde{q}_i(\mathtt{b})] \text{ and} \\ 2\tilde{q}_i(\mathtt{b}) &= [1 - \tilde{q}_i(\mathtt{f})] - [\tilde{q}_i(\mathtt{r}) - \tilde{q}_i(\mathtt{b})], \text{ so} \\ \|\Delta\tilde{q}\|_1 &\lesssim \Delta\tilde{q}(\mathtt{f}) + \Delta\tilde{q}(\mathtt{R}). \end{aligned}$$

If we take $a \in \{1,2\}$ and $b = 2 - a$, and write $\dot{Z}_i \equiv \|\dot{p}^{\mathrm{u}}_i\|_1$, then

$$\Delta\tilde{q}(\mathtt{f}) + \Delta\tilde{q}(\mathtt{R}) \leqslant \frac{\Delta\dot{p}^{\mathrm{u}}(\mathtt{f}) + \Delta\dot{p}^{\mathrm{u}}(\mathtt{R})}{\dot{Z}_a} + \frac{|\dot{Z}_a - \dot{Z}_b|}{\dot{Z}_a}\frac{[\dot{p}^{\mathrm{u}}_b(\mathtt{f}) + \dot{p}^{\mathrm{u}}_b(\mathtt{r}) - \dot{p}^{\mathrm{u}}_b(\mathtt{b})]}{\dot{Z}_b}.$$

If we take $a \in \arg\max_i \dot{p}^{\mathrm{u}}_i(\mathtt{b})$, then, by (2.9.6) and (2.9.20), the first term on the right-hand side is

$$\lesssim \frac{k\|\Delta\hat{m}^\lambda\hat{p}\|_1\dot{p}^{\mathrm{u}}_a(\mathtt{b})}{\dot{Z}_a} \lesssim k\|\Delta\hat{m}^\lambda\hat{p}\|_1,$$

where the rightmost inequality uses $\dot{Z}_i \geqslant \dot{p}^{\mathrm{u}}_i(\mathtt{b})$. As for the second term, (2.9.6) gives

$$\frac{|\dot{Z}_a - \dot{Z}_b|}{\dot{Z}_a} \lesssim d\|\Delta\hat{m}^\lambda\hat{p}\|_1 \quad \text{and} \quad \frac{[\dot{p}^{\mathrm{u}}_b(\mathtt{f}) + \dot{p}^{\mathrm{u}}_b(\mathtt{r}) - \dot{p}^{\mathrm{u}}_b(\mathtt{b})]}{\dot{Z}_b} \lesssim 2^{-k}.$$

Combining these estimates yields the claimed bound. □

2.9.2 Pair coloring recursions

In this section we analyze the BP recursions for the pair coloring model and prove Proposition 2.4.3 and Lemma 2.4.4. Recall that we have restricted our attention to measures $\dot{Q}, \hat{Q}$ such that

$$\begin{aligned} \dot{Q}(\sigma^1, \sigma^2) &\cong \dot{q}(\dot{\sigma}^1, \dot{\sigma}^2)\mathbf{1}\{|\sigma^1|, |\sigma^2| \leqslant T\}, \\ \hat{Q}(\sigma^1, \sigma^2) &\cong \hat{q}(\hat{\sigma}^1, \hat{\sigma}^2)\mathbf{1}\{|\sigma^1|, |\sigma^2| \leqslant T\} \end{aligned}$$

for probability measures $\dot{q}, \hat{q}$ defined on $(\dot{\Omega}_T)^2, (\hat{\Omega}_T)^2$. Recall further that we assume $\dot{q} = \dot{q}^{\mathrm{avg}}$ and $\hat{q} = \hat{q}^{\mathrm{avg}}$. For any measure $p(x)$ defined on $x \equiv (x^1, x^2)$ in $(\dot{\Omega}_T)^2$ or $(\hat{\Omega}_T)^2$, define

$$(\mathtt{F}p)(x) \equiv p(\mathtt{F}x) \quad \text{where } \mathtt{F}x \equiv x \oplus (\mathtt{0},\mathtt{1}) \equiv (x^1, x^2 \oplus \mathtt{1}).$$

Recall the definition (2.4.6) of $\mathbf{\Gamma}(c, \kappa)$. We will prove that

Proposition 2.9.7. *For any constant $c \in (0,1]$ and probability measures $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}(c,1)$, we have $\mathtt{BP}\dot{q}_1, \mathtt{BP}\dot{q}_2 \in \mathbf{\Gamma}(1,1)$ and*

$$\|\mathtt{BP}\dot{q}_1 - \mathtt{BP}\dot{q}_2\|_1 = O(k^4/2^k)\|\dot{q}_1 - \dot{q}_2\|_1 + O(k^4/2^k)\sum_{i=1,2}\|\dot{q}_i - \mathtt{F}\dot{q}_i\|_1. \tag{2.9.21}$$

Assuming this result, it is straightforward to deduce Proposition 2.4.3:

Proof of Proposition 2.4.3. Let $\dot{q}^{(0)}$ be the uniform probability measure on $\{\mathtt{b_0}, \mathtt{b_1}, \mathtt{r_1}, \mathtt{r_0}\}^2$, and define recursively $\dot{q}^{(l)} = \mathtt{BP}(\dot{q}^{(l-1)})$ for $l \geqslant 1$. It is clear that $\dot{q}^{(0)} \in \mathbf{\Gamma}(1,1)$ and $\dot{q}^{(0)} = \mathtt{F}\dot{q}^{(0)}$. Since $\dot{q}^{(l)} = \mathtt{F}\dot{q}^{(l)}$ for all $l \geqslant 1$, it follows from (2.9.21) that $(\dot{q}^{(l)})_{l\geqslant 1}$ forms an ℓ^1 Cauchy sequence. It follows by completeness of ℓ^1 that $\dot{q}^{(l)}$ converges to a limit $\dot{q}^{(\infty)} = \dot{q}_\star \in \mathbf{\Gamma}(1,1)$, satisfying $\dot{q}_\star = \mathtt{F}\dot{q}_\star = \mathtt{BP}\dot{q}_\star$. This implies that for any probability measure $\dot{q}$,

$$\|\dot{q} - \mathtt{F}\dot{q}\|_1 \leqslant \|\dot{q} - \dot{q}_\star\|_1 + \|\dot{q}_\star - \mathtt{F}\dot{q}\|_1 = 2\|\dot{q} - \dot{q}_\star\|_1.$$

Applying (2.9.21) again gives

$$\|\mathtt{BP}\dot{q} - \dot{q}_\star\|_1 = O(k^4/2^k)\|\dot{q} - \dot{q}_\star\|_1 + O(k^4/2^k)\|\dot{q} - \mathtt{F}\dot{q}\|_1 = O(k^4/2^k)\|\dot{q} - \dot{q}_\star\|_1,$$

proving the claimed contraction estimate. Uniqueness of $\dot{q}_\star$ can be deduced from this contraction. □

We now turn to the proof of Proposition 2.9.7. The proof of Lemma 2.4.4 is given after the proof of Proposition 2.9.7. Let $\mathtt{N\dot{B}P}, \mathtt{N\hat{B}P}$ now denote the non-normalized BP recursions for the pair model. Let $\dot{p} \equiv \dot{p}(\dot{q})$ be the reweighted measure

$$\dot{p}(\dot{\sigma}) \equiv \frac{\dot{q}(\dot{\sigma})}{1 - \dot{q}(\mathtt{r}[\dot{\sigma}] > 0)}. \tag{2.9.22}$$

Recalling convention (2.9.1), we will denote

$$\hat{m}^\lambda \hat{r}(\hat{\sigma}^1, \hat{\sigma}^2) \equiv [\hat{m}(\hat{\sigma}^1)\hat{m}(\hat{\sigma}^2)]^\lambda \hat{r}(\hat{\sigma}^1, \hat{\sigma}^2).$$

Let $\mathtt{N\hat{B}P}$ and $\mathtt{N\dot{B}P}$ be the non-normalized pair BP recursions at parameters λ, T. Starting from $\dot{q}_i \in \mathbf{\Gamma}(c,\kappa)$ $(i = 1,2)$, we denote

$$\begin{aligned} \dot{p}_i \quad &\equiv \dot{p}(\dot{q}_i) \text{ (as defined by (2.9.22))}, \\ \hat{p}_i \quad &\equiv \mathtt{N\hat{B}P}(\dot{p}_i) \text{ and } \hat{p}_{i,\infty} \equiv \mathtt{N\hat{B}P}_{\lambda,\infty}(\dot{p}_i), \\ \dot{p}_i^{\mathrm{u}} \quad &\equiv \mathtt{N\dot{B}P}(\hat{p}_i) \text{ and } \tilde{q}_i \equiv \mathtt{\dot{B}P}\hat{p}_i = \mathtt{BP}\dot{q}_i. \end{aligned}$$

With this notation in mind, the proof of Proposition 2.9.7 is divided into the following lemmas.

Lemma 2.9.8 (effect of reweighting)**.** *Suppose $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}(c,\kappa)$ for $c \in (0,1]$ and $\kappa \in [0,1]$: then*

$$\begin{aligned} \|\Delta\dot{p}\|_1 \quad &\equiv O(2^{2(1-\kappa)k})\|\Delta\dot{q}\|_1, \\ \|\dot{p}_i - \mathtt{F}\dot{p}_i\|_1 \quad &\equiv O(2^{(1-\kappa)k})\|\dot{q}_i - \mathtt{F}\dot{q}_i\|_1. \end{aligned}$$

Lemma 2.9.9 (clause BP contraction). *Suppose $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}(c,\kappa)$ for $c \in (0,1]$ and $\kappa \in [0,1]$: then*

$$\begin{aligned} \Delta\hat{m}^\lambda\hat{p}(\texttt{yy}) &= O(k^3/2^k)\Delta\dot{p}(\texttt{gg}) = O(k^3/2^{(1+c)k}), \\ \Delta\hat{m}^\lambda\hat{p}(\{\texttt{br},\texttt{bf}_{\geqslant 1}\}) &= O(k^2/2^k)[\Delta\dot{p}(\texttt{gg}) + 2^{-k}\Delta\dot{p}(\dot{\Omega}^2\backslash\{\texttt{rr}\})] = O(k^3/2^{(1+c)k}), \\ \|\Delta\hat{m}^\lambda\hat{p}\|_1 &= O(k^3/2^k)\|\Delta\dot{p}\|_1 = O(k^3 2^{(1-2\kappa)k}), \end{aligned} \tag{2.9.23}$$

and the same estimates hold with $\texttt{F}\hat{p}$ in place of $\hat{p}$. For both $i = 1,2$,

$$\|\hat{m}^\lambda\hat{p}_i - \hat{m}^\lambda\texttt{F}\hat{p}_i\|_1 = O(k^3/2^{(1+\kappa)k})\|\dot{p}_i - \texttt{F}\dot{p}_i\|_1 = O(k^3/2^{2\kappa k})\|\dot{q}_i - \texttt{F}\dot{q}_i\|_1. \tag{2.9.24}$$

Lemma 2.9.10 (clause BP output values). *Suppose $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}(c,\kappa)$ for $c \in (0,1]$ and $\kappa \in [0,1]$. For $s,t \subseteq \hat{\Omega}$ let $st \equiv s \times t$. Then it holds for all $s,t \in \{\texttt{r}_1,\texttt{b}_1,\texttt{f},\square\}$ that*

$$\frac{\hat{m}^\lambda\hat{p}_i(s,t)}{(2/2^k)^{\texttt{r}[s]+\texttt{r}[t]}} = \begin{cases} 1 + O(k^2/2^k) & \texttt{r}[s]+\texttt{r}[t] \leqslant 1, \\ 1 + O(k^2/2^{ck}) & \texttt{r}[s]+\texttt{r}[t] = 2. \end{cases} \tag{2.9.25}$$

Furthermore we have the bounds

$$\begin{aligned} \hat{m}^\lambda\hat{p}_i(\texttt{f}_{\geqslant 1}t) + \hat{m}^\lambda\hat{p}_i(t\texttt{f}_{\geqslant 1}) &\leqslant O(k/4^k) \text{ for all } t \in \{\texttt{r}_1,\texttt{b}_1,\texttt{f},\square\}, \\ \hat{m}^\lambda\hat{p}_i(\{\texttt{f}\}\times\hat{\Omega}) - \hat{m}^\lambda\hat{p}_i(\{\texttt{b}_1\}\times\hat{\Omega}) &\leqslant O(k/4^k). \end{aligned} \tag{2.9.26}$$

The same estimates hold with $\texttt{F}\hat{p}_i$ in place of $\hat{p}_i$.

Lemma 2.9.11 (variable BP). *Suppose $\dot{q}_1, \dot{q}_2 \in \mathbf{\Gamma}(c,\kappa)$ for $c \in (0,1]$ and $\kappa \in [0,1]$. Then we have $\texttt{BP}\dot{q}_1, \texttt{BP}\dot{q}_2 \in \mathbf{\Gamma}(c',1)$ with $c' = \max\{0, 2\kappa-1\}$, and*

$$\|\texttt{BP}\dot{q}_1 - \texttt{BP}\dot{q}_2\|_1 = O(k)\big(\|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\texttt{F}\hat{p}\|_1\big) + O(k2^k)\sum_{i=1,2}\|\hat{m}^\lambda\hat{p}_i - \hat{m}^\lambda\texttt{F}\hat{p}_i\|_1.$$

Proof of Proposition 2.9.7. Follows by combining the preceding lemmas 2.9.8–2.9.11. □

Proof of Lemma 2.4.4. If $\dot{q} \in \mathbf{\Gamma}(c,0)$ is a fixed point of $\texttt{BP}$, then it follows from the preceeding lemmas 2.9.9–2.9.11 that $\dot{q} \in \mathbf{\Gamma}(c,0) \cap \mathbf{\Gamma}(0,1) = \mathbf{\Gamma}(c,1)$. □

We now prove the three lemmas leading to Proposition 2.9.7.

Proof of Lemma 2.9.8. Applying (2.9.7) we have

$$|\dot{p}_1(\dot{\sigma}) - \dot{p}_2(\dot{\sigma})| \leqslant \frac{|\dot{q}_1(\dot{\sigma}) - \dot{q}_2(\dot{\sigma})|}{\dot{q}_1(\texttt{gg})} + \frac{|\dot{q}_1(\texttt{gg}) - \dot{q}_2(\texttt{gg})|}{\dot{q}_1(\texttt{gg})\dot{q}_2(\texttt{gg})}\dot{q}_2(\dot{\sigma}),$$

and summing over $\dot{\sigma} \in \dot{\Omega}^2$ gives

$$\|\Delta\dot{p}\|_1 \leqslant \frac{\|\dot{q}_1 - \dot{q}_2\|_1}{\dot{q}_1(\texttt{gg})} + \frac{|\dot{q}_1(\texttt{gg}) - \dot{q}_2(\texttt{gg})|}{\dot{q}_1(\texttt{gg})\dot{q}_2(\texttt{gg})} \leqslant \frac{2\|\dot{q}_1 - \dot{q}_2\|_1}{\dot{q}_1(\texttt{gg})\dot{q}_2(\texttt{gg})}.$$

Since $\dot{q}_i \in \mathbf{\Gamma}$, we have

$$\begin{aligned} \dot{p}_i(\dot{\Omega}^2 \backslash \{\texttt{rr}\}) &= O(1) && \text{by part (A) of (2.4.6)}, \\ \text{and } \dot{p}_i(\texttt{rr}) &= O(2^{(1-\kappa)k}) && \text{by part (B) of (2.4.6)}. \end{aligned} \tag{2.9.27}$$

Consequently $\dot{q}_i(\texttt{gg})^{-1} \leqslant O(1)2^{(1-\kappa)k}$, and the claimed bound on $\|\Delta\dot{p}\|_1$ follows. The bound on $\|\dot{p}_i - \texttt{F}\dot{p}_i\|_1$ follows by noting that if $\dot{q}_2 = \texttt{F}\dot{q}_1$, then $\dot{q}_1(\texttt{gg}) = \dot{q}_2(\texttt{gg})$. □

Proof of Lemma 2.9.9. We will prove (2.9.23) for $\hat{p}_i$; the proof for $\texttt{F}\hat{p}_i$ is entirely similar. It follows from the symmetry $\dot{p}_i = (\dot{p}_i)^{\mathrm{avg}}$ that for any $x, y \in \{\texttt{0}, \texttt{1}\}$,

$$\Big|\dot{p}_i(\texttt{bb}) - 4\dot{p}_i(\texttt{b}_x\texttt{b}_y)\Big| = 2\Big|\dot{p}_i(\texttt{b}_x\texttt{b}_{y\oplus 1}) - \dot{p}_i(\texttt{b}_x\texttt{b}_y)\Big| = 2\Big|\dot{p}_i(\texttt{b}_0\texttt{b}_0) - \dot{p}_i(\texttt{b}_0\texttt{b}_1)\Big|,$$

from which we obtain that

$$\Delta\dot{p}(\texttt{bb}) = |\dot{p}_1(\texttt{bb}) - \dot{p}_2(\texttt{bb})| + O(1)\max_{i=1,2}\Big|\dot{p}_i(\texttt{b}_0\texttt{b}_0) - \dot{p}_i(\texttt{b}_0\texttt{b}_1)\Big|.$$

Recall $\texttt{g} = \{\texttt{b}, \texttt{f}\}$ and $\dot{p}_i(\texttt{gg}) = 1$. Combining the above with (2.4.6) gives

$$\begin{aligned} \Delta\dot{p}(\texttt{gg}) &\leqslant \Delta\dot{p}(\texttt{bb}) + \Delta\dot{p}(\texttt{gf}) + \Delta\dot{p}(\texttt{fg}) \\ &\lesssim \sum_{i=1,2}\bigg\{\Big|\dot{p}_i(\texttt{b}_0\texttt{b}_0) - \dot{p}_i(\texttt{b}_0\texttt{b}_1)\Big| + \dot{p}_i(\texttt{gf}) + \dot{p}(\texttt{fg})\bigg\} = O(2^{-ck}). \end{aligned} \tag{2.9.28}$$

Step I. We first control $\Delta\hat{m}^\lambda\hat{p}(\hat{\sigma})$. As before, by symmetry it suffices to analyze the BP recursion at a clause with all literals $\texttt{L}_j = \texttt{0}$. We distinguish the following cases of $\hat{\sigma} \in \hat{\Omega}^2$:

1. Recall $\texttt{y} \equiv \texttt{r} \cup \texttt{f}$, and note $\{\texttt{y}\}\backslash\{\square\} \subseteq \texttt{a}_0 \cup \texttt{a}_1$ (as defined by (2.9.10)). Thus

$$\Delta\hat{m}^\lambda\hat{p}(\{\texttt{yy}\}\backslash\{\square\square\}) \leqslant \sum_{x\in\{\texttt{0},\texttt{1}\}}\big[\Delta\hat{m}^\lambda\hat{p}(\texttt{a}_x\texttt{y}) + \Delta\hat{m}^\lambda\hat{p}(\texttt{y}\texttt{a}_x)\big]. \tag{2.9.29}$$

   Consider $\hat{\sigma} \in \{\texttt{a}_x\texttt{y}\}$: in order for $\underline{\dot{\sigma}} \in (\dot{\Omega}^2)^{k-1}$ to be compatible with $\hat{\sigma}$, it is necessary that $\dot{\sigma}_j \in \{\texttt{g}_x\texttt{g}\}$ for all $2 \leqslant j \leqslant k$. Combining with (2.9.9) gives

$$\Delta\hat{m}^\lambda\hat{p}(\texttt{a}_x\texttt{y}) \leqslant \sum_{\underline{\dot{\sigma}}\in\{\texttt{g}_x\texttt{g}\}^{k-1}}\bigg|\prod_{j=2}^k\dot{p}_1(\dot{\sigma}_j) - \prod_{j=2}^k\dot{p}_2(\dot{\sigma}_j)\bigg| \leqslant k\Delta\dot{p}(\texttt{gg})\Big(\dot{p}_1(\texttt{g}_x\texttt{g}) + \Delta\dot{p}(\texttt{gg})\Big)^{k-2}.$$

   It follows from (2.4.6) that $\dot{p}_1(A) + \Delta\dot{p}(\texttt{gg}) = \frac{1}{2} + O(2^{-ck})$, so we conclude

$$\Delta\hat{m}^\lambda\hat{p}(\{\texttt{yy}\}\backslash\{\square\square\}) = O(k/2^k)\Delta\dot{p}(\texttt{gg}). \tag{2.9.30}$$

2. Now take $\hat{\sigma} = \square\square$: for $\underline{\dot{\sigma}} \in (\dot{\Omega}^2)^{k-1}$ to be compatible with $\hat{\sigma}$, it is necessary that $\underline{\dot{\sigma}} \in \{\mathtt{gg}\}^{k-1}$. On the other hand, it is sufficient that $\underline{\dot{\sigma}} \in \{\mathtt{gg}\}^{k-1}$ does not belong to any of the sets $\{\mathtt{g}_x\mathtt{g}\}^{k-1}, \{\mathtt{gg}_x\}^{k-1}, x \in \{\mathtt{0},\mathtt{1}\}$. Therefore

$$\Delta\hat{m}^\lambda\hat{p}(\square\square) \leqslant \sum_{x\in\{\mathtt{0},\mathtt{1}\}} \sum_{\underline{\dot{\sigma}}\in\{\mathtt{g}_x\mathtt{g}\}^{k-1}\cup\{\mathtt{gg}_x\}^{k-1}} \left| \prod_{j=2}^k \dot{p}_1(\dot{\sigma}_j) - \prod_{j=2}^k \dot{p}_2(\dot{\sigma}_j) \right| = O(k/2^k)\Delta\dot{p}(\mathtt{gg}),$$

where the last estimate follows by the same argument that led to (2.9.30). This concludes the proof of the first line of (2.9.23).

3. Now consider $\hat{\sigma}$ with exactly one coordinate in $\{\mathtt{b}\}$, meaning the other must be in $\{\mathtt{y}\}$. Recalling convention (2.9.1), we assume without loss that $\hat{\sigma} \in \{\mathtt{b_1y}\}$ and proceed to bound $\Delta\hat{m}^\lambda\hat{p}(\hat{\sigma})$. Let $\underline{\dot{\sigma}} \in (\dot{\Omega}^2)^{k-1}$ be compatible with $\hat{\sigma}$. There are two cases:

   a. If $\underline{\dot{\sigma}}$ contains no **red** spin, it must also be compatible with some $\hat{\sigma}' \in \{\mathtt{yy}\}$, as long as we permit the possibility that $|(\hat{\sigma}')^1| > T$. Such $\underline{\dot{\sigma}}$ gives the same contribution to $\hat{m}^\lambda\hat{p}(\hat{\sigma})$ as to $\hat{m}^\lambda\hat{p}_\infty(\mathtt{yy})$. It follows from the preceding estimates that the contribution to $\Delta\hat{m}^\lambda\hat{p}(\mathtt{b_1y})$ from all such $\underline{\dot{\sigma}}$ is upper bounded by

$$\Delta\hat{m}^\lambda\hat{p}_\infty(\mathtt{yy}) = O(k/2^k)\Delta\dot{p}(\mathtt{gg}) \tag{2.9.31}$$

   b. The only remaining possibility is that some permutation of $\underline{\dot{\sigma}}$ belongs to $A \times B^{k-2}$ for $A = \{\mathtt{r_0g}\}$ and $B = \{\mathtt{b_1g}\}$: the contribution to $\Delta\hat{m}^\lambda\hat{p}(\mathtt{b_1y})$ from all such $\underline{\dot{\sigma}}$ is

$$\leqslant (k-1) \sum_{\underline{\dot{\sigma}}\in A\times B^{k-2}} \left| \prod_{j=2}^k \dot{p}_1(\dot{\sigma}_j) - \prod_{j=2}^k \dot{p}_2(\dot{\sigma}_j) \right| = O(k^2/2^k)\|\Delta\dot{p}\|_1, \tag{2.9.32}$$

   where the last estimate follows using (2.9.8) and (2.9.27).

   Combining the above estimates (and using the symmetry between $\mathtt{b_1y}$ and $\mathtt{yb_1}$) gives

$$\Delta\hat{m}^\lambda\hat{p}(\mathtt{b_1y}) + \Delta\hat{m}^\lambda\hat{p}(\mathtt{yb_1}) = O(k^2/2^k)\|\Delta\dot{p}\|_1. \tag{2.9.33}$$

   If we further assume $\hat{\sigma} \in \{\mathtt{b_1}\} \times \{\mathtt{r}, \mathtt{f}_{\geqslant 1}\}$, then, arguing as above, $\underline{\dot{\sigma}}$ either contributes to $\Delta\hat{m}^\lambda\hat{p}_\infty(\mathtt{y} \times \{\mathtt{r}, \mathtt{f}_{\geqslant 1}\})$, or else belongs to $A_x \times B_x^{k-2}$ for $A_x = \{\mathtt{r_0g}_x\}$, $B_x = \{\mathtt{b_1g}_x\}$ and $x \in \{\mathtt{0},\mathtt{1}\}$. The contribution from first case is bounded by (2.9.30). The contribution from the second case, using (2.9.8) and (2.9.27), is

$$\lesssim k\Delta\dot{p}(\dot{\Omega}^2\backslash\{\mathtt{rr}\})\Big(\max_{x\in\{\mathtt{0},\mathtt{1}\}} \dot{p}_1(B_x) + \Delta\dot{p}(\mathtt{gg})\Big)^{k-2} = O(k^2/4^k)\Delta\dot{p}(\dot{\Omega}^2\backslash\{\mathtt{rr}\}).$$

   The second claim of (2.9.23) follows by combining these estimates and recalling (2.9.28).

4. Lastly we consider $\hat{\sigma} \in \{\mathtt{bb}\}$. Without loss of generality, we take $\hat{\sigma} = \mathtt{b_1b_1}$ and proceed to bound $\Delta\hat{m}^\lambda\hat{p}(\mathtt{b_1b_1})$. Let $\underline{\dot{\sigma}} \in (\dot{\Omega}^2)^{k-1}$ be compatible with $\hat{\sigma}$. We distinguish three cases:

a. For at least one $i \in \{1,2\}$, $\underline{\dot{\sigma}}^i$ contains no $\texttt{red}$ spin. In this case $\underline{\dot{\sigma}}$ is also compatible with some $\hat{\sigma}' \in \{\texttt{b}_1\texttt{y}\} \cup \{\texttt{y}\texttt{b}_1\}$, as long as we permit the possibility that $|(\hat{\sigma}')^i| > T$. The contribution of all such $\underline{\dot{\sigma}}$ to $\Delta\hat{m}^\lambda\hat{p}(\texttt{b}_1\texttt{b}_1)$ is therefore upper bounded by

$$\Delta\hat{m}^\lambda\hat{p}_\infty(\texttt{b}_1\texttt{y}) + \Delta\hat{m}^\lambda\hat{p}_\infty(\texttt{y}\texttt{b}_1) = O(k^2/2^k)\|\Delta\dot{p}\|_1, \tag{2.9.34}$$

where the last step is by the same argument as for (2.9.33).

b. The next case is that $\underline{\dot{\sigma}}$ is a permutation of $(\texttt{r}_0\texttt{r}_0, (\texttt{b}_1\texttt{b}_1)^{k-2})$. The contribution to $\Delta\hat{m}^\lambda\hat{p}(\texttt{b}_1\texttt{b}_1)$ from this case is at most

$$(k-1)\Big|\dot{p}_1(\texttt{r}_0\texttt{r}_0)\dot{p}_1(\texttt{b}_1\texttt{b}_1)^{k-2} - \dot{p}_2(\texttt{r}_0\texttt{r}_0)\dot{p}_2(\texttt{b}_1\texttt{b}_1)^{k-2}\Big|.$$

Using (2.9.8) and (2.4.6), this is at most

$$\begin{aligned} &O(k^2/4^k)\Big(\Delta\dot{p}(\texttt{r}_0\texttt{r}_0) + \dot{p}(\texttt{r}_0\texttt{r}_0)\cdot\Delta\dot{p}(\texttt{b}_1\texttt{b}_1)\Big) \\ &= O(k^2/4^k)\|\dot{p}\|_1\|\Delta\dot{p}\|_1 = O(k^2/2^{(1+\kappa)k})\|\Delta\dot{p}\|_1. \end{aligned} \tag{2.9.35}$$

c. The last case is that $\underline{\dot{\sigma}}$ is a permutation of $(\texttt{r}_0\texttt{b}_1, \texttt{b}_1\texttt{r}_0, (\texttt{b}_1\texttt{b}_1)^{k-3})$. The contribution to $\Delta\hat{m}^\lambda\hat{p}(\texttt{b}_1\texttt{b}_1)$ from this case is at most

$$k^2\Big|\dot{p}_1(\texttt{r}_0\texttt{b}_1)\dot{p}_1(\texttt{b}_1\texttt{r}_0)\dot{p}_1(\texttt{b}_1\texttt{b}_1)^{k-3} - \dot{p}_2(\texttt{r}_0\texttt{b}_1)\dot{p}_2(\texttt{b}_1\texttt{r}_0)\dot{p}_2(\texttt{b}_1\texttt{b}_1)^{k-3}\Big|.$$

This is at most $O(k^2/4^k)\|\Delta\dot{p}\|_1$ by another application of (2.9.8) and (2.4.6).

The above estimates together give

$$\Delta\hat{m}^\lambda\hat{p}(\texttt{b}_1\texttt{b}_1) = O(k^2/2^k)\|\Delta\dot{p}\|_1, \tag{2.9.36}$$

where the main contribution comes from (2.9.34). Combining with the previous bound (2.9.33) yields the last part of (2.9.23).

Step II. Next we prove (2.9.24) by improving the preceding bounds in the special case that $\dot{p}_1 = \dot{p}$ and $\dot{p}_2 \equiv \texttt{F}\dot{p}$. Recall $\hat{p}_i \equiv \texttt{N}\hat{\texttt{B}}\texttt{P}(\dot{p}_i)$; it follows that $\hat{p}_2 = \texttt{F}\hat{p}_1$. Thus, for any $\hat{\sigma} \in \hat{\Omega}^2$ with $\hat{\sigma}^2 = \square$, we have $\hat{\sigma} = \texttt{F}\hat{\sigma}$, so $\hat{p}_2(\hat{\sigma}) = \hat{p}_1(\texttt{F}\hat{\sigma}) = \hat{p}_1(\hat{\sigma})$. For $\hat{\sigma} \in \hat{\Omega}^2$ with $\hat{\sigma}^1 = \square$, we have $\hat{\sigma} = (\texttt{F}\hat{\sigma}) \oplus \texttt{1}$, so $\hat{p}_2(\hat{\sigma}) = \hat{p}_1(\texttt{F}\hat{\sigma}) = \hat{p}_1(\hat{\sigma})$, where the last step uses that $\hat{p}_1 = (\hat{p}_1)^{\mathrm{avg}}$. It follows that instead of (2.9.29) and (2.9.31) we have the improved bound

$$\begin{aligned} \Delta\hat{m}^\lambda\hat{p}_\infty(\texttt{yy}) &= \Delta\hat{m}^\lambda\hat{p}_\infty(\{\texttt{yy}\}\backslash(\{\square\texttt{y}\} \cup \{\texttt{y}\square\})) \leqslant \sum_{x\in\{0,1\}} \Delta\hat{m}^\lambda\hat{p}_\infty(\texttt{a}_x\texttt{a}_y) \\ &= O(k)\|\Delta\dot{p}\|_1 \sum_{x,y\in\{0,1\}} \Big(\dot{p}_1(\texttt{g}_x\texttt{g}_y) + \Delta\dot{p}(\texttt{gg})\Big)^{k-2} = O(k/4^k)\|\dot{p} - \texttt{F}\dot{p}\|_1. \end{aligned}$$

Similarly, instead of (2.9.32) we would only have a contribution from $\underline{\dot{\sigma}}$ belonging to either $A_0 \times (B_0)^{k-2}$ or $A_1 \times (B_1)^{k-2}$, where $A_x = \{\mathtt{r}_0\mathtt{g}_x\}$ and $B_x = \{\mathtt{b}_1\mathtt{g}_x\}$. It follows that instead of (2.9.33) and (2.9.34) we have the improved bound

$$\Delta\hat{m}^\lambda\hat{p}_\infty(\mathtt{b}_1\mathtt{y}) + \Delta\hat{m}^\lambda\hat{p}_\infty(\mathtt{y}\mathtt{b}_1) = O(k^4/4^k)\|\Delta\dot{p}\|_1.$$

Previously the main contribution in (2.9.36) came from (2.9.34), but now it comes instead from (2.9.35). This gives the improved bound $\Delta\hat{m}^\lambda\hat{p}(\mathtt{b}_1\mathtt{b}_1) = O(k^2/2^{(1+\kappa)k})$, which proves the first part of (2.9.24). The second part follows by applying Lemma 2.9.8. □

Proof of Lemma 2.9.10. We first prove (2.9.25). Assume $s, t \in \{\mathtt{b}_1, \mathtt{f}, \square\}$, and write $st \equiv s \times t \subseteq \hat{\Omega}^2$. Then for a lower bound we have

$$\hat{m}^\lambda\hat{p}_i(st) \geqslant [1 - O(k/2^k)]\dot{p}_i(\mathtt{bb})^{k-1} = 1 - O(k/2^k).$$

for an upper bound we have

$$\begin{aligned}\hat{m}^\lambda\hat{p}_i(st) \leqslant \dot{p}_i(\mathtt{gg})^{k-1} + k\dot{p}_i(\mathtt{r}_0\mathtt{g})\dot{p}_i(\mathtt{b}_1\mathtt{g})^{k-2} + k\dot{p}_i(\mathtt{g}\mathtt{r}_0)\dot{p}_i(\mathtt{g}\mathtt{b}_1)^{k-2} \\ + k\dot{p}_i(\mathtt{r}_0\mathtt{r}_0)\dot{p}_i(\mathtt{b}_1\mathtt{b}_1)^{k-2} + k^2\dot{p}_i(\mathtt{r}_0\mathtt{b}_1)\dot{p}_i(\mathtt{b}_1\mathtt{r}_0)\dot{p}_i(\mathtt{b}_1\mathtt{b}_1)^{k-3} = 1 + O(k^2/2^k).\end{aligned}$$

Writing $\mathtt{r}_1 t \equiv \mathtt{r}_1 \times t$ for $t \in \{\mathtt{b}_1, \mathtt{f}, \square\}$, a similar argument gives

$$\begin{aligned}\hat{m}^\lambda\hat{p}_i(\mathtt{r}_1 t) &\geqslant [1 - O(k/2^k)]\dot{p}_i(\mathtt{b}_0\mathtt{b})^{k-1} = [1 - O(k/2^k)] \cdot (2/2^k), \\ \hat{m}^\lambda\hat{p}_i(\mathtt{r}_1 t) &\leqslant \dot{p}_i(\mathtt{b}_0\mathtt{g})^{k-1} + k\dot{p}_i(\mathtt{b}_0\mathtt{r}_0)\dot{p}_i(\mathtt{b}_0\mathtt{b}_1)^{k-2} = [1 + O(k/2^k)] \cdot (2/2^k).\end{aligned}$$

Lastly, it is easily seen that

$$\hat{m}\hat{p}_i(\mathtt{r}_1\mathtt{r}_1) = \dot{p}_i(\mathtt{b}_0\mathtt{b}_0)^{k-1} = [1 - O(k/2^{ck})] \cdot (2/2^k)^2.$$

This concludes the proof of (2.9.25), and we turn next to the proof of (2.9.26). Arguing similarly as for (2.9.12) gives

$$\hat{m}^\lambda\hat{p}_i(\{\mathtt{ff}\}\backslash\{\square\square\}) \leqslant \hat{m}^\lambda\hat{p}_i(\mathtt{f}_{\geqslant 1}\mathtt{f}) + \hat{m}^\lambda\hat{p}_i(\mathtt{f}\mathtt{f}_{\geqslant 1}) = O(k/4^k).$$

Next, suppose $\underline{\dot{\sigma}}$ is compatible with $\hat{\sigma} \in \mathtt{b}_1\mathtt{f}_{\geqslant 1}$: if $\underline{\dot{\sigma}}$ has no $\mathtt{red}$ spin, then it is also compatible with some $\hat{\sigma}' \in \mathtt{f}\mathtt{f}_{\geqslant 1}$, provided we allow $|(\hat{\sigma}')^1| > T$. Therefore

$$\begin{aligned}&\hat{m}^\lambda\hat{p}_i(\mathtt{b}_1\mathtt{f}_{\geqslant 1}) - \hat{m}^\lambda\hat{p}_{i,\infty}(\mathtt{f}\mathtt{f}_{\geqslant 1}) \\ &\qquad \leqslant \sum_{y\in\{0,1\}} \Big[k\dot{p}_i(\mathtt{r}_0\mathtt{f})\dot{p}_i(\mathtt{b}_1\mathtt{g}_y)^{k-2} + k^2\dot{p}_i(\mathtt{r}_0\mathtt{b}_y)\dot{p}_i(\mathtt{b}_1\mathtt{f})\dot{p}_i(\mathtt{b}_1\mathtt{g}_y)^{k-3} \Big],\end{aligned}$$

and applying (2.4.6) this is $O(k/4^k)$. Finally,

$$\hat{m}^\lambda\hat{p}_i(\mathtt{r}_1\mathtt{f}_{\geqslant 1}) \leqslant \sum_{y\in\{0,1\}} k\dot{p}_i(\mathtt{b}_0\mathtt{f})\dot{p}_i(\mathtt{b}_0\mathtt{g}_y)^{k-2} = O(k/8^k),$$

which proves the first part of (2.9.26). For the second part, arguing similarly as for (2.9.19), we have for any $\xi \in \hat{\Omega}$ that

$$\hat{m}^\lambda \hat{p}_i(\mathtt{f}\xi) - \hat{m}^\lambda \hat{p}_i(\mathtt{b}_1\xi) \leqslant (k-1) \sum_{\underline{\dot{\sigma}} \sim \xi} [\dot{p}_i(\mathtt{g}_0\dot{\sigma}_2) - \dot{p}_i(\mathtt{r}_0\dot{\sigma}_2)] \prod_{j=3}^{k} \dot{p}_i(\mathtt{b}_1\dot{\sigma}_j).$$

Note that $\underline{\dot{\sigma}}$ has at most one $\mathtt{red}$ spin. If $\dot{\sigma}_2 = \mathtt{r}_0$, then $\dot{\sigma}_j = \mathtt{b}_1$ for all $j \geqslant 3$. Since $\dot{q}_i \in \mathbf{\Gamma}(c,\kappa)$ (which means also that $\dot{q}_i = (\dot{q}_i)^{\mathrm{avg}}$), we have

$$\sum_{\underline{\dot{\sigma}} \sim \xi} \mathbf{1}\{\dot{\sigma}_2 = \zeta\} \prod_{j=3}^{k} \dot{p}_i(\mathtt{b}_1\dot{\sigma}_j) \leqslant \begin{cases} \dot{p}_i(\mathtt{b}_1\mathtt{b}_1)^{k-2} & \leqslant O(4^{-k}) \quad \text{if } \zeta = \mathtt{r}_0, \\ \dot{p}_i(\mathtt{b}_1\mathtt{g})^{k-3} & \leqslant O(2^{-k}) \quad \text{if } \zeta \in \dot{\Omega}\backslash\{\mathtt{r}_0\}. \end{cases}$$

On the other hand, $\dot{q}_i \in \mathbf{\Gamma}(c,\kappa)$ also implies

$$\dot{p}_i(\mathtt{g}_0\zeta) - \dot{p}_i(\mathtt{r}_0\zeta) \leqslant O(2^{-k})\dot{p}_i(\mathtt{b}_0\zeta) + \dot{p}_i(\mathtt{f}\zeta) \leqslant \begin{cases} O(1) & \zeta = \mathtt{r}_0, \\ O(2^{-k}) & \text{if } \zeta \in \dot{\Omega}\backslash\{\mathtt{r}_0\}. \end{cases}$$

Combining these estimates and summing over ξ proves the second part of (2.9.26). □

An immediate application of (2.9.25), which will be useful in the next proof, is that

$$\frac{\hat{m}^\lambda \hat{p}_i(\mathtt{r}_x t)}{\hat{m}^\lambda \hat{p}_i(\mathtt{b}_x t)} \geqslant [1 + O(k^2/2^k)] \cdot (2/2^k). \tag{2.9.37}$$

for all $t \in \{\mathtt{b}_0, \mathtt{b}_1, \mathtt{f}, \square\}$.

Proof of Lemma 2.9.11. We divide the proof in two parts.
Step I. Non-normalized messages.

1. First consider $\dot{\sigma} \in \{\mathtt{ff}\}$. Recalling $(a+b)^\lambda \leqslant a^\lambda + b^\lambda$ for $a, b \geqslant 0$ and $\lambda \in [0,1]$,

$$\Delta \dot{p}^{\mathrm{u}}(\mathtt{ff}) \leqslant 2 \sum_{\hat{r} \in \{\hat{p}, \mathtt{F}\hat{p}\}} \sum_{\underline{\hat{\sigma}} \in \{\mathtt{ff}\}^{k-1}} \left| \prod_{j=2}^{d} \hat{m}^\lambda \hat{r}_1(\hat{\sigma}_j) - \prod_{j=2}^{d} \hat{m}^\lambda \hat{r}_2(\hat{\sigma}_j) \right|$$

where the $\hat{r} = \mathtt{F}\hat{p}$ term arises from the fact that

$$\hat{m}(\hat{\sigma}^1)^\lambda [1 - \hat{m}(\hat{\sigma}^2)]^\lambda \hat{p}(\hat{\sigma}) = \hat{m}(\hat{\sigma}^1)^\lambda \hat{m}(\hat{\sigma}^2 \oplus 1)^\lambda (\mathtt{F}\hat{p})(\mathtt{F}\hat{\sigma}) = \hat{m}^\lambda \mathtt{F}\hat{p}(\mathtt{F}\hat{\sigma}).$$

Applying (2.9.9) gives

$$\Delta \dot{p}^{\mathrm{u}}(\mathtt{ff}) = O(d) \sum_{\hat{r} \in \{\hat{p}, \mathtt{F}\hat{p}\}} \Delta \hat{m}^\lambda \hat{r}(\mathtt{ff}) \Big(\hat{m}^\lambda \hat{r}_1(\mathtt{ff}) + \Delta \hat{m}^\lambda \hat{r}(\mathtt{ff}) \Big)^{d-2}.$$

We have from (2.9.23) and (2.9.25) that $\hat{m}^\lambda \hat{p}_1(\mathtt{ff}) \asymp 1$ and $\Delta \hat{m}^\lambda \hat{p}(\mathtt{ff}) = O(k^3/2^{(1+c)k})$, so

$$\Delta \dot{p}^{\mathrm{u}}(\mathtt{ff}) = O(d) \|\Delta \hat{m}^\lambda \hat{p} + \Delta \hat{m}^\lambda \mathtt{F}\hat{p}\|_1 \cdot \dot{p}_1^{\mathrm{u}}(\mathtt{ff}). \tag{2.9.38}$$

2. Next consider $\dot\sigma \in \{\texttt{p}_1\texttt{f}\}$. Let $\hat r_{\max}(\hat\sigma) \equiv \max_{i=1,2} \hat r_i(\hat\sigma)$ — in this notation,

$$\hat r_{\max}(\hat\Omega) = \sum_{\hat\sigma\in\hat\Omega} \max_{i=1,2} \hat r_i(\hat\sigma) \geqslant \max_{i=1,2} \sum_{\hat\sigma\in\hat\Omega} \hat r_i(\hat\sigma) = \max_{i=1,2} \hat r_i(\hat\Omega)$$

where the inequality may be strict. Then

$$\Delta\dot p^{\mathrm{u}}(\texttt{p}_1\texttt{f}) = O(d) \sum_{\hat r\in\{\hat p,\texttt{F}\hat p\}} \Delta\hat m^\lambda \hat r(\texttt{p}_1\texttt{f})[\hat m^\lambda \hat r_{\max}(\texttt{p}_1\texttt{f})]^{d-2}.$$

Let $a \in \arg\max_i \hat r_i(\texttt{b}_1\square)$, so that

$$0 \leqslant \hat m^\lambda \hat r_{\max}(\texttt{p}_1\texttt{f}) - \hat m^\lambda \hat r_a(\texttt{p}_1\texttt{f}) \leqslant \Delta\hat m^\lambda \hat r(\texttt{r}_1\texttt{f}) + \Delta\hat m^\lambda \hat r(\texttt{b}_1\texttt{f}_{\geqslant 1}) = O(2^{-(1+c)k}),$$

where the last estimate is by (2.9.23) and (2.9.26). On the other hand, we have from (2.9.25) that $\hat m^\lambda \hat p(\texttt{p}_1\texttt{f}) \geqslant \hat m^\lambda \hat p(\texttt{b}_1\texttt{f}) \asymp 1$, and it follows that

$$[\hat m^\lambda \hat r_{\max}(\texttt{p}_1\texttt{f})]^{d-2} \asymp [\hat m^\lambda \hat r_a(\texttt{p}_1\texttt{f})]^{d-1}. \tag{2.9.39}$$

Applying (2.9.25) and (2.9.26) again, we have (for $i = 1, 2$)

$$[\hat m^\lambda \hat r_i(\texttt{p}_1\texttt{f})]^{d-1} \asymp [\hat m^\lambda \hat r_i(\texttt{p}_1\square)]^{d-1}.$$

On the other hand, assuming $T \geqslant 1$, we have

$$\dot p_i^{\mathrm{u}}(\texttt{r}_1\texttt{f}) \geqslant [\hat m^\lambda \hat r_i(\texttt{p}_1\square)]^{d-1} - [\hat m^\lambda \hat r_i(\texttt{b}_1\square)]^{d-1} \asymp [\hat m^\lambda \hat r_i(\texttt{p}_1\square)]^{d-1}$$

where the last step follows by (2.9.37). Similarly,

$$\begin{aligned}\dot p_i^{\mathrm{u}}(\texttt{r}_1\texttt{f}) - \dot p_i^{\mathrm{u}}(\texttt{b}_1\texttt{f}) &= O(1) \sum_{\hat r\in\{\hat p,\texttt{F}\hat p\}} \hat m^\lambda \hat r_i(\texttt{b}_1\texttt{f})^{d-1} = O(2^{-k}) \sum_{\hat r\in\{\hat p,\texttt{F}\hat p\}} \hat m^\lambda \hat r_i(\texttt{p}_1\texttt{f})^{d-1}\\ &= O(2^{-k})\dot p_i^{\mathrm{u}}(\texttt{r}_1\texttt{f}) = O(2^{-k})\dot p_i^{\mathrm{u}}(\texttt{b}_1\texttt{f}),\end{aligned} \tag{2.9.40}$$

where the last step follows by rearranging the terms. Combining the above gives

$$\Delta\dot p^{\mathrm{u}}(\texttt{p}_1\texttt{f}) \leqslant O(d)\|\Delta\hat m^\lambda \hat p + \Delta\hat m^\lambda \texttt{F}\hat p\|_1 \max_{i=1,2} \dot p_i^{\mathrm{u}}(\texttt{b}_1\texttt{f}). \tag{2.9.41}$$

Clearly, similar bounds hold if we replace $\texttt{p}_1\texttt{f}$ with any of $\texttt{p}_0\texttt{f}$, $\texttt{f}\texttt{p}_1$, or $\texttt{f}\texttt{p}_0$.

3. Lastly we bound $\Delta\dot p^{\mathrm{u}}(\texttt{p}_x\texttt{p}_y)$. As in the single-copy recursion, for $x, y \in \{\texttt{0}, \texttt{1}\}$ we denote

$$\begin{aligned}\dot r(\texttt{R}_x\dot\sigma) &\equiv \dot r(\texttt{r}_x\dot\sigma) - \dot r(\texttt{b}_x\dot\sigma),\\ \dot r(\dot\sigma\texttt{R}_x) &\equiv \dot r(\dot\sigma\texttt{r}_x) - \dot r(\dot\sigma\texttt{b}_x),\\ \dot r(\texttt{R}_x\texttt{R}_y) &\equiv \dot r(\texttt{r}_x\texttt{r}_y) - \dot r(\texttt{r}_x\texttt{b}_y) - \dot r(\texttt{b}_x\texttt{r}_y) + \dot r(\texttt{b}_x\texttt{b}_y).\end{aligned}$$

Applying (2.9.37) gives

$$\begin{aligned}\dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{r}_y) &= [\hat{p}_i(\mathtt{b}_x\mathtt{p}_y)]^{d-1} = O(2^{-k})[\hat{p}_i(\mathtt{p}_x\mathtt{p}_y)]^{d-1} = O(2^{-k})\dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y),\\ \dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{R}_y) &= [\hat{p}_i(\mathtt{b}_x\mathtt{b}_y)]^{d-1} = O(2^{-k})\dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y).\end{aligned}$$

Combining the above estimates gives

$$\dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y) - \dot{p}_i^{\mathrm{u}}(\mathtt{b}_x\mathtt{b}_y) = \dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{r}_y) + \dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{R}_y) - \dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{R}_y) = O(2^{-k})\dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y).$$

Further, it follows from the BP equations that

$$\begin{aligned}&\max\{\dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{R}_y), \dot{p}_i^{\mathrm{u}}(\mathtt{b}_x\mathtt{R}_y), \dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{r}_y), \dot{p}_i^{\mathrm{u}}(\mathtt{R}_x\mathtt{b}_y)\} \leqslant \dot{p}_i^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y) - \dot{p}_i^{\mathrm{u}}(\mathtt{b}_x\mathtt{b}_y),\\ &\text{so } \dot{p}_i^{\mathrm{u}}(st) = [1+O(2^{-k})]\dot{p}_i^{\mathrm{u}}(\mathtt{b}_x\mathtt{b}_y) \text{ for all } s \in \{\mathtt{r}_x, \mathtt{b}_x\},\ t \in \{\mathtt{r}_y, \mathtt{b}_y\}.\end{aligned} \tag{2.9.42}$$

Similarly, we can upper bound

$$\begin{aligned}\Delta\dot{p}^{\mathrm{u}}(\mathtt{p}_x\mathtt{p}_y) &\leqslant 4[\Delta\dot{p}^{\mathrm{u}}(\mathtt{r}_x\mathtt{r}_y) + \Delta\dot{p}^{\mathrm{u}}(\mathtt{R}_x\mathtt{r}_y) + \Delta\dot{p}^{\mathrm{u}}(\mathtt{r}_x\mathtt{R}_y) + \Delta\dot{p}^{\mathrm{u}}(\mathtt{R}_x\mathtt{R}_y)].\\ &\leqslant O(d)\sum_{\hat{r}\in\{\hat{p},\mathtt{F}\hat{p}\}}\ \sum_{\substack{s\in\{\mathtt{p}_x,\mathtt{b}_x\}\\ t\in\{\mathtt{p}_y,\mathtt{b}_y\}}} \|\Delta\hat{m}^\lambda\hat{r}\|_1[\hat{m}^\lambda\hat{r}_{\max}(st)]^{d-2}.\end{aligned} \tag{2.9.43}$$

For $\hat{r} \in \{\hat{p}, \mathtt{F}\hat{p}\}$, let $a = \arg\max_{i=1,2}\hat{m}^\lambda\hat{r}_i(\mathtt{b}_1\mathtt{b}_1)$: then, for any $s \in \{\mathtt{p}_x, \mathtt{b}_x\}$, $t \in \{\mathtt{p}_y, \mathtt{b}_y\}$,

$$\begin{aligned}0 &\leqslant \hat{m}^\lambda\hat{r}_{\max}(st) - \max_{i=1,2}\hat{m}^\lambda\hat{r}_i(st) \leqslant \hat{m}^\lambda\hat{r}_{\max}(st) - \hat{m}^\lambda\hat{r}_a(st)\\ &\leqslant O(1)\Delta\hat{m}^\lambda\hat{r}(\{\mathtt{pp}\}\backslash\{\mathtt{bb}\}) \leqslant O(1/2^{(1+c)k}),\end{aligned}$$

where the last estimate is by (2.9.23). Combining with (2.9.4) and (2.9.42) gives

$$\sum_{\substack{s\in\{\mathtt{p}_x,\mathtt{b}_x\}\\ t\in\{\mathtt{p}_y,\mathtt{b}_y\}}} [\hat{m}^\lambda\hat{r}_{\max}(st)]^{d-2} = O(1)\Big[\max_{i=1,2}\hat{r}_i(\mathtt{p}_x\mathtt{p}_y)\Big]^{d-1} = O(1)\max_{i=1,2}\dot{p}_i^{\mathrm{u}}(\mathtt{bb}).$$

Substituting into (2.9.43) gives

$$\Delta\dot{p}^{\mathrm{u}}(\mathtt{p}_x\mathtt{p}_y) \leqslant O(d)\|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\mathtt{F}\hat{p}\|_1\max_{i=1,2}\dot{p}_i^{\mathrm{u}}(\mathtt{bb}). \tag{2.9.44}$$

Further, for any $st \in \{\mathtt{r}_x\mathtt{R}_y, \mathtt{R}_x\mathtt{r}_y, \mathtt{R}_x\mathtt{R}_y\}$, we have

$$\Delta\dot{p}^{\mathrm{u}}(st) \leqslant O(k)\|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\mathtt{F}\hat{p}\|_1\max_{i=1,2}\dot{p}_i^{\mathrm{u}}(\mathtt{bb}). \tag{2.9.45}$$

Lastly, in the special case $\hat{p}_2 = \mathtt{F}\hat{p}_1$, (2.9.44) reduces to

$$\begin{aligned}|\dot{p}_1^{\mathrm{u}}(\mathtt{b}_0\mathtt{b}_0) - \dot{p}_1^{\mathrm{u}}(\mathtt{b}_0\mathtt{b}_1)| &\leqslant O(d)\|\hat{m}^\lambda\hat{p}_1 - \hat{m}^\lambda\mathtt{F}\hat{p}_1\|_1\dot{p}_1^{\mathrm{u}}(\mathtt{bb})\\ &\leqslant k^5 2^{(1-2\kappa)k}\|\dot{p}_i - \mathtt{F}\dot{p}_i\|_1.\end{aligned} \tag{2.9.46}$$

where the last estimate is by (2.9.24).

Step II. Normalized messages. Recall $\tilde{q}_i \equiv \texttt{BP}\dot{q}_i$. It remains to verify that $\tilde{q}_i \in \mathbf{\Gamma}(c', 1)$ with $c' = \max\{0, 2\kappa - 1\}$: recalling (2.4.6), this means

$$\begin{aligned}
&(\text{A}) \quad \textstyle\sum_{\dot{\sigma}\notin\{\texttt{bb}\}}(2^{-k})^{\texttt{r}[\dot{\sigma}]}p(\dot{\sigma}) = O(2^{-k})p(\texttt{bb}), \quad |p(\texttt{b}_0\texttt{b}_0) - p(\texttt{b}_0\texttt{b}_1)| \leqslant (k^9/2^{c'k})p(\texttt{bb}),\\
&(\text{B}) \quad p(\texttt{fr}) = O(2^{-k})p(\texttt{bb}), \quad p(\texttt{rr}) = O(1)p(\texttt{bb}),\\
&(\text{C}) \quad p(\texttt{r}_x\dot{\sigma}) \geqslant [1 - O(2^{-k})]p(\texttt{b}_x\dot{\sigma}) \text{ for all } x \in \{\texttt{0},\texttt{1}\} \text{ and } \dot{\sigma} \in \dot{\Omega}.
\end{aligned} \tag{2.9.47}$$

Condition (C) is automatically satisfied due to the BP equations. The second part of (B) follows from (2.9.42). The second part of (A) holds trivially in the case $c' = 0$, and otherwise follows from (2.9.46). We claim that

$$\tilde{q}_i(\{\texttt{rf}, \texttt{fr}, \texttt{ff}\}) = O(2^{-k})\tilde{q}_i(\texttt{bb}). \tag{2.9.48}$$

This immediately implies the first part of (B). Further, the BP equations give $\tilde{q}_i(\texttt{bf}) \leqslant \tilde{q}_i(\texttt{rf})$ and $\tilde{q}_i(\texttt{fb}) \leqslant \tilde{q}_i(\texttt{fr})$, so the first part of (A) also follows. To see that (2.9.48) holds, note that the second part of (2.9.26) gives

$$\begin{aligned}
\dot{p}_i^{\mathrm{u}}(\texttt{ff}) &\leqslant O(1)\sum_{\hat{r}\in\{\hat{p},\mathrm{F}\hat{p}\}}[\hat{m}^\lambda\hat{r}_i(\texttt{ff})]^{d-1} \leqslant O(1)\sum_{\hat{r}\in\{\hat{p},\mathrm{F}\hat{p}\}}[\hat{m}^\lambda\hat{r}_i(\texttt{b}_1\texttt{b}_1)]^{d-1},\\
\dot{p}_i^{\mathrm{u}}(\texttt{r}_1\texttt{f}) &\leqslant O(1)\sum_{\hat{r}\in\{\hat{p},\mathrm{F}\hat{p}\}}[\hat{m}^\lambda\hat{r}_i(\texttt{p}_1\texttt{f})]^{d-1} \leqslant O(1)\sum_{\hat{r}\in\{\hat{p},\mathrm{F}\hat{p}\}}[\hat{m}^\lambda\hat{r}_i(\texttt{p}_1\texttt{b}_1)]^{d-1}.
\end{aligned}$$

Combining with (2.9.37) gives $\dot{p}_i^{\mathrm{u}}(\{\texttt{r}_1\texttt{f}, \texttt{ff}\}) = O(2^{-k})\dot{p}_i^{\mathrm{u}}(\texttt{r}_1\texttt{r}_1)$. Recalling (2.9.42) (and making use of symmetry) gives (2.9.48). Finally, we conclude the proof of the lemma by bounding the difference $\Delta\tilde{q} \equiv |\tilde{q}_1 - \tilde{q}_2|$. Recalling the definition of $\texttt{R}_x$, we have

$$\begin{aligned}
\Delta\tilde{q}(\texttt{pp}) &\leqslant O(1)\Delta\tilde{q}(\{\texttt{bb}, \texttt{rR}, \texttt{Rr}, \texttt{RR}\}),\\
\Delta\tilde{q}(\dot{\Omega}^2\backslash\{\texttt{pp}\}) &\leqslant O(1)\Delta\tilde{q}(\{\texttt{bf}, \texttt{fb}, \texttt{ff}, \texttt{fR}, \texttt{Rf}\}).
\end{aligned}$$

We next bound $\Delta\tilde{q}(\texttt{bb})$, which is the sum of $\Delta\tilde{q}(\texttt{b}_x\texttt{b}_y)$ over $x, y \in \{\texttt{0},\texttt{1}\}$. By symmetry let us take $x = y = \texttt{0}$. Since $\tilde{q}_i = (\tilde{q}_i)^{\mathrm{avg}}$, $\tilde{q}_i(\texttt{b}_0\texttt{b}_0) = \frac{1}{4}\tilde{q}_i(\texttt{bb}) + \frac{1}{2}[\tilde{q}_i(\texttt{b}_0\texttt{b}_0) - \tilde{q}_i(\texttt{b}_0\texttt{b}_1)]$, so

$$\Delta\tilde{q}(\texttt{b}_0\texttt{b}_0) \lesssim |\tilde{q}_1(\texttt{bb}) - \tilde{q}_2(\texttt{bb})| + \sum_{i=1,2}|\tilde{q}_i(\texttt{b}_0\texttt{b}_0) - \tilde{q}_i(\texttt{b}_0\texttt{b}_1)|.$$

Since the $\tilde{q}_i$ are normalized to be probability measures,

$$1 - \tilde{q}_i(\dot{\Omega}^2\backslash\{\texttt{pp}\}) = \tilde{q}_i(\texttt{pp}) = 2\tilde{q}_i(\texttt{rR}) + 2\tilde{q}_i(\texttt{Rr}) - 3\tilde{q}_i(\texttt{RR}) + 4\tilde{q}_i(\texttt{bb}),$$

from which it follows that

$$|\tilde{q}_1(\texttt{bb}) - \tilde{q}_2(\texttt{bb})| \lesssim |\tilde{q}_1(\dot{\Omega}^2\backslash\{\texttt{pp}\}) - \tilde{q}_2(\dot{\Omega}^2\backslash\{\texttt{pp}\})| + \Delta\tilde{q}(\{\texttt{rR}, \texttt{Rr}, \texttt{RR}\}).$$

Combining the above estimates gives

$$\|\Delta\tilde{q}\|_1 \lesssim \Delta\tilde{q}(\texttt{A}) + \sum_{i=1,2}|\tilde{q}_i(\texttt{b}_0\texttt{b}_0) - \tilde{q}_i(\texttt{b}_0\texttt{b}_1)|, \quad \texttt{A} \equiv \{\texttt{bf}, \texttt{fb}, \texttt{ff}, \texttt{fR}, \texttt{Rf}, \texttt{rR}, \texttt{Rr}, \texttt{RR}\}.$$

Write $\dot{Z}_i \equiv \|\dot{p}_i^{\mathrm{u}}\|_1$. Taking $a \in \{1,2\}$ and $b = 2-a$,

$$\|\Delta\tilde{q}\|_1 \leqslant e_1 + e_2 e_3 + e_4 \quad \text{with } e_1 \equiv \frac{\Delta\dot{p}^{\mathrm{u}}(\mathtt{A})}{\dot{Z}_a},\ e_2 \equiv \frac{|\dot{Z}_1 - \dot{Z}_2|}{\dot{Z}_a} \leqslant \frac{\|\Delta\dot{p}^{\mathrm{u}}\|_1}{\dot{Z}_a},$$
$$e_3 \equiv \frac{\dot{p}_b^{\mathrm{u}}(\mathtt{A})}{\dot{Z}_b},\ e_4 \equiv \sum_{i=1,2} \frac{|\dot{p}_i^{\mathrm{u}}(\mathtt{b}_0\mathtt{b}_0) - \dot{p}_i^{\mathrm{u}}(\mathtt{b}_0\mathtt{b}_1)|}{\dot{Z}_i}.$$

It follows from (2.9.38), (2.9.41), (2.9.45) and (2.9.48), and taking $a = \arg\max_i \dot{p}_i^{\mathrm{u}}(\mathtt{bb})$, that

$$e_1 \lesssim \|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\mathtt{F}\hat{p}\|_1 (d/2^k) \max_{i=1,2} \dot{p}_i^{\mathrm{u}}(\mathtt{bb})/\dot{Z}_a \lesssim k\|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\mathtt{F}\hat{p}\|_1.$$

Further, recalling (2.9.44) gives

$$e_2 \lesssim k2^k \|\Delta\hat{m}^\lambda\hat{p} + \Delta\hat{m}^\lambda\mathtt{F}\hat{p}\|_1.$$

Combining (2.9.40), (2.9.42), and (2.9.48) gives $e_3 = O(2^{-k})$. Finally, (2.9.46) gives

$$e_4 \lesssim k2^k \|\hat{m}^\lambda\hat{p}_i - \hat{m}^\lambda\mathtt{F}\hat{p}_i\|_1.$$

Combining the pieces together finishes the proof. □

2.10 The 1RSB free energy

2.10.1 Equivalence of recursions

In this section, we relate the coloring recursion (2.4.4) to the distributional recursion (2.1.7). The main task of this section is to show the following

Proposition 2.10.1. *Let $\dot{q}_\lambda$ be the fixed point given by Proposition 2.4.2 for parameters $\lambda \in [0,1]$ and $T = \infty$. Let $H_\lambda \equiv (\dot{H}_\lambda, \hat{H}_\lambda, \bar{H}_\lambda)$ be the associated triple of measures defined by Proposition 2.3.7. Then $(\boldsymbol{s}(H_\lambda), \boldsymbol{\Sigma}(H_\lambda), \boldsymbol{F}(H_\lambda)) = (s_\lambda, \Sigma(s_\lambda), \mathfrak{F}(\lambda))$.*

In the course of proving Proposition 2.10.1, we will obtain Proposition 2.1.2 as a corollary. Throughout the section we take $T = \infty$ unless explicitly indicated otherwise. We begin with some notations. Recall that $\mathscr{P}(\mathfrak{X})$ is the space of probability measures on $\mathfrak{X}$. Given $\dot{q} \in \mathscr{P}(\dot{\Omega})$, we define two associated measures $\dot{m}^\lambda\dot{q}, (1-\dot{m})^\lambda\dot{q}$ on $\dot{\Omega}$ by

$$(\dot{m}^\lambda\dot{q})(\dot{\sigma}) \equiv \dot{m}(\dot{\sigma})^\lambda\dot{q}(\dot{\sigma}), \quad ((1-\dot{m})^\lambda\dot{q})(\dot{\sigma}) \equiv (1-\dot{m}(\dot{\sigma}))^\lambda\dot{q}(\dot{\sigma}),$$

We let $\dot{\pi} \equiv \dot{\pi}(\dot{q})$ be the probability measure on $\dot{\mathscr{M}}\backslash\{\star\}$ given by

$$\dot{\pi}(\dot{\tau}) = \begin{cases} [1-\dot{q}(\mathtt{r})]^{-1}\dot{q}(\dot{\tau}) & \text{if } \dot{\tau} \in \dot{\Omega}_{\mathtt{f}}, \\ [1-\dot{q}(\mathtt{r})]^{-1}\dot{q}(\mathtt{b}_x) & \text{if } \dot{\tau} = x \in \{\mathtt{0},\mathtt{1}\}. \end{cases}$$

Recalling the definition (2.2.4) of the mapping $\dot{m} : \dot{\Omega} \to [0,1]$, we denote the pushforward measure $\dot{u} \equiv \dot{u}(\dot{q}) \equiv \dot{\pi} \circ \dot{m}^{-1}$, so that $\dot{u}$ belongs to the space $\mathscr{P}$ of discrete probability measures on $[0,1]$. Analogously, given $\hat{q} \in \mathscr{P}(\hat{\Omega})$, we define two associated measures $\hat{m}^\lambda \hat{q}, (1-\hat{m})^\lambda \hat{q}$ on $\hat{\Omega}$. We let $\hat{\pi} \equiv \hat{\pi}(\hat{q})$ be the probability measure on $\hat{\mathscr{M}} \backslash \{\star\}$ given by

$$\hat{\pi}(\hat{\tau}) \equiv \begin{cases} [1-\hat{q}(\mathtt{b})]^{-1}\hat{q}(\hat{\tau}) & \text{if } \hat{\tau} \in \hat{\Omega}_{\mathtt{f}}, \\ [1-\hat{q}(\mathtt{b})]^{-1}\hat{q}(\mathtt{r}_x) & \text{if } \hat{\tau} = x \in \{\mathtt{0},\mathtt{1}\}. \end{cases}$$

Recalling the definition (2.2.5) of the mapping $\hat{m} : \hat{\Omega} \to [0,1]$, we denote the pushforward measure $\hat{u} \equiv \hat{u}(\hat{q}) \equiv \hat{\pi} \circ \hat{m}^{-1}$, so that $\hat{u} \in \mathscr{P}$ also. The next two lemmas follow straightforwardly from the above definitions, and we omit their proofs:

Lemma 2.10.2. *Suppose $\dot{q} \in \mathscr{P}(\dot{\Omega})$ satisfies $\dot{q} = \dot{q}^{\text{avg}}$ and*

$$\dot{m}^\lambda \dot{q}(\mathtt{f}) = \dot{q}(\mathtt{r}_1) - \dot{q}(\mathtt{b}_1) = \dot{q}(\mathtt{r}_0) - \dot{q}(\mathtt{b}_0) = (1-\dot{m})^\lambda \dot{q}(\mathtt{f}) \tag{2.10.1}$$

Then $\hat{q} \equiv \hat{\mathtt{BP}}\dot{q} \in \mathscr{P}(\hat{\Omega})$ must satisfy $\hat{q} = \hat{q}^{\text{avg}}$ and

$$\hat{m}^\lambda \hat{q}(\mathtt{f}) = \hat{q}(\mathtt{b}_1) = \hat{q}(\mathtt{b}_0) = (1-\hat{m})^\lambda \hat{q}(\mathtt{f}), \tag{2.10.2}$$

Let $\hat{\boldsymbol{z}} \equiv (\mathtt{N}\hat{\mathtt{BP}}\dot{q})/(\hat{\mathtt{BP}}\dot{q})$ be the normalizing constant. Then $\dot{u} \equiv \dot{u}(\dot{q})$ and $\hat{u} \equiv \hat{u}(\hat{q})$ satisfy

$$\hat{u} = \hat{\mathscr{R}}_\lambda(\dot{u}), \quad \hat{\mathscr{Z}}_\lambda(\dot{u}) = \frac{\hat{\boldsymbol{z}}(1-\hat{q}(\mathtt{b}))}{(1-\dot{q}(\mathtt{r}))^{k-1}}. \tag{2.10.3}$$

Lemma 2.10.3. *Suppose $\hat{q} \in \mathscr{P}(\hat{\Omega})$ satisfies $\hat{q} = \hat{q}^{\text{avg}}$ and (2.10.2). Then $\dot{q} \equiv \dot{\mathtt{BP}}\hat{q} \in \mathscr{P}(\dot{\Omega})$ must satisfy $\dot{q} = \dot{q}^{\text{avg}}$ and (2.10.1). Let $\dot{\boldsymbol{z}} \equiv (\mathtt{N}\dot{\mathtt{BP}}\hat{q})/(\dot{\mathtt{BP}}\hat{q})$ be the normalizing constant: then*

$$\dot{u} = \dot{\mathscr{R}}_\lambda(\hat{u}), \quad \dot{\mathscr{Z}}_\lambda(\hat{u}) = \frac{\dot{\boldsymbol{z}}(1-\dot{q}(\mathtt{r}))}{(1-\hat{q}(\mathtt{b}))^{d-1}}. \tag{2.10.4}$$

Proof of Proposition 2.1.2. This is simply a rephrasing of the proof of Proposition 2.4.2, using Lemma 2.10.2 and Lemma 2.10.3. □

We next prove Proposition 2.10.1. In the remainder of this section, fix $\lambda \in [0,1]$ and $T = \infty$. Let $\dot{q} \equiv \dot{q}_\lambda$ be the fixed point of $\mathtt{BP} \equiv \mathtt{BP}_{\lambda,\infty}$ given by Proposition 2.4.2. Let $\hat{q} \equiv \hat{q}_\lambda$ denote the image of $\dot{q}$ under the mapping $\hat{\mathtt{BP}} \equiv \hat{\mathtt{BP}}_{\lambda,\infty}$. Denote the associated normalizing constants

$$\hat{\boldsymbol{z}} \equiv \hat{\boldsymbol{z}}_\lambda \equiv (\mathtt{N}\hat{\mathtt{BP}}\dot{q})/(\hat{\mathtt{BP}}\dot{q}), \quad \dot{\boldsymbol{z}} \equiv \dot{\boldsymbol{z}}_\lambda \equiv (\mathtt{N}\dot{\mathtt{BP}}\hat{q})/(\dot{\mathtt{BP}}\hat{q}).$$

Let $H_\lambda \equiv (\dot{H}_\lambda, \hat{H}_\lambda, \bar{H}_\lambda)$ be the triple of associated measures defined as in Proposition 2.3.7, with normalizing constants $(\dot{\mathfrak{Z}}_\lambda, \hat{\mathfrak{Z}}_\lambda, \bar{\mathfrak{Z}}_\lambda)$. Recall from (2.1.9) that $\mathfrak{F}(\lambda) = \ln \dot{\mathfrak{Z}}_\lambda + \alpha \ln \hat{\mathfrak{Z}}_\lambda - d \ln \bar{\mathfrak{Z}}_\lambda$. We now show that it coincides with $\boldsymbol{F}(H_\lambda)$:

Lemma 2.10.4. *Under the above notations, $\boldsymbol{F}(H_\lambda) = \ln \dot{\mathscr{Z}}_\lambda + \alpha \ln \hat{\mathscr{Z}}_\lambda - d \ln \bar{\mathscr{Z}}_\lambda$, and*

$$\bar{\mathfrak{Z}}_\lambda = \frac{\bar{\mathscr{Z}}_\lambda}{(1-\dot{q}_\lambda(\mathtt{r}))(1-\hat{q}_\lambda(\mathtt{b}))}, \quad \dot{\mathfrak{Z}}_\lambda = \frac{\dot{\mathscr{Z}}_\lambda}{(1-\hat{q}_\lambda(\mathtt{b}))^d}, \quad \hat{\mathfrak{Z}}_\lambda = \frac{\hat{\mathscr{Z}}_\lambda}{(1-\dot{q}_\lambda(\mathtt{r}))^k}. \tag{2.10.5}$$

Consequently $\mathfrak{F}(\lambda) = \boldsymbol{F}(H_\lambda)$.

Proof. It follows from (2.3.9) (and recalling (2.3.5) that $\hat{\Phi}(\underline{\sigma})^\lambda = \hat{\Phi}^{\max}(\underline{\sigma})^\lambda \hat{v}(\underline{\sigma})$) that

$$\boldsymbol{F}(H_\lambda) = \langle \ln(\dot{\Phi}^\lambda/\dot{H}), \dot{H}_\lambda\rangle + \alpha\langle \ln(\hat{\Phi}^\lambda/\hat{H}_\lambda), \hat{H}_\lambda\rangle + d\langle \ln(\bar{\Phi}^\lambda \bar{H}_\lambda), \bar{H}_\lambda\rangle.$$

Substituting in (2.3.12) and rearranging gives

$$\begin{aligned} &\boldsymbol{F}(H_\lambda) - \Big(\ln \dot{\mathscr{Z}}_\lambda + \alpha \ln \hat{\mathscr{Z}}_\lambda - d \ln \bar{\mathscr{Z}}_\lambda\Big) \\ &\quad = -\Big\langle \sum_{i=1}^d \ln \hat{q}_\lambda(\hat{\sigma}_i), \dot{H}_\lambda \Big\rangle - \alpha \Big\langle \sum_{i=1}^k \ln \dot{q}_\lambda(\dot{\sigma}_i), \hat{H}_\lambda \Big\rangle + d\langle \ln[\dot{q}_\lambda(\dot{\sigma})\hat{q}_\lambda(\hat{\sigma})], \bar{H}_\lambda\rangle. \end{aligned}$$

This equals zero by (2.3.13). The proof of (2.10.5) is straightforward from the preceding definitions, and is omitted. □

Proof of Proposition 2.10.1. By similar calculations as above, it is straightforward to verify that $s_\lambda = \boldsymbol{s}(H_\lambda)$. Since by definition $\mathfrak{F}(\lambda) = \lambda s_\lambda + \Sigma(s_\lambda)$ and $\boldsymbol{F}(H_\lambda) = \lambda \boldsymbol{s}(H_\lambda) + \boldsymbol{\Sigma}(H_\lambda)$, it follows that $\Sigma(s_\lambda) = \boldsymbol{\Sigma}(H_\lambda)$, concluding the proof. □

2.10.2 Large-k asymptotics

We now evaluate the large-k asymptotics of the free energy, beginning with (2.1.9). Let $\dot{\mu}_\lambda$ be as given by Proposition 2.1.2, and write $\hat{\mu}_\lambda \equiv \hat{\mathscr{R}}_\lambda(\dot{\mu}_\lambda)$. In what follows it will be useful to denote

$$\psi_\lambda \equiv \int x^\lambda \mathbf{1}\{x \in (0,1)\}\dot{\mu}_\lambda(dx), \quad \rho_\lambda \equiv \int y^\lambda \mathbf{1}\{y \in (0,1)\backslash\{\tfrac{1}{2}\}\}\hat{\mu}_\lambda(dy).$$

Proposition 2.10.5. *For $k \geqslant k_0$, $\alpha_{\rm lbd} \leqslant \alpha = (2^{k-1}-c)\ln 2 \leqslant \alpha_{\rm ubd}$, and $\lambda \in [0,1]$,*

$$\ln \dot{\mathfrak{Z}}_\lambda = \ln 2 - (1-2^{\lambda-1})/2^k + d \ln\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + \hat{\mu}_\lambda(1) + \rho_\lambda\Big) + \mathsf{err}, \tag{2.10.6}$$

$$-d \ln \bar{\mathfrak{Z}} = -d \ln\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + \hat{\mu}_\lambda(1) + \rho_\lambda\Big) - (k\ln 2)[-\dot{\mu}_\lambda(\mathtt{f}) + 2\psi_\lambda] + \mathsf{err}, \tag{2.10.7}$$

$$\alpha \ln \hat{\mathfrak{Z}} = \alpha \ln(1-2/2^k) + (k \ln 2)(-\dot{\mu}_\lambda(\mathtt{f}) + 2\psi_\lambda) + \mathsf{err}, \tag{2.10.8}$$

where err denotes any error bounded by $k^{O(1)}/4^k$. Altogether this yields

$$\mathfrak{F}(\lambda) = \mathsf{f}^{\rm RS}(\alpha) - (1-2^{\lambda-1})/2^k + \mathsf{err} = [(2c-1)\ln 2 - (1-2^{\lambda-1})]/2^k + \mathsf{err}.$$

On the other hand $\lambda s_\lambda = \lambda(\ln 2)2^{\lambda-1}/2^k + \mathsf{err}$.

Proof of Proposition 2.1.5. Apply Proposition 2.10.5: setting $\mathfrak{F}(\lambda) = \lambda s_\lambda$ gives

$$\alpha_\lambda = (2^{k-1} - c_\lambda)\ln 2 + \mathsf{err}, \quad c_\lambda = \frac{1}{2} + \frac{1 - 2^{\lambda-1}(1-\lambda\ln 2)}{2\ln 2}.$$

Substituting the special values $\lambda = 1$ and $\lambda = 0$ gives

$$c_{\text{cond}} = c_1 = 1, \quad c_{\text{sat}} = c_0 = \frac{1}{2} + \frac{1}{4\ln 2},$$

as claimed. □

Proof of Proposition 2.10.5. Throughout the proof we abbreviate ϵ_k for a small error term which may change from one occurrence to the next, but is bounded throughout by $k^C/4^k$ for a sufficiently large absolute constant C. Note that

$$\hat{\mu}_\lambda(\tfrac{1}{2}) = 1 - 2\cdot\frac{2^{1-\lambda}}{2^k} + \epsilon_k, \quad \hat{\mu}_\lambda(1) = \hat{\mu}_\lambda(0) = \frac{2^{1-\lambda}}{2^k} + \epsilon_k, \quad \hat{\mu}_\lambda((0,1)\backslash\{\tfrac{1}{2}\}) = \epsilon_k,$$

from which it follows that $\rho_\lambda = \epsilon_k$. Meanwhile, ψ_λ is upper bounded by $\dot{\mu}_\lambda(\mathtt{f}) \equiv \dot{\mu}_\lambda((0,1))$, and we will show below that

$$\dot{\mu}_\lambda(\mathtt{f}) = \frac{2^{\lambda-1}}{2^k} + \epsilon_k. \tag{2.10.9}$$

Estimate of $\dot{\mathfrak{Z}}_\lambda$. Recall from the definition (2.1.8) that

$$\dot{\mathfrak{Z}}_\lambda = \int\bigg(\prod_{i=1}^d y_i + \prod_{i=1}^d (1-y_i)\bigg)^\lambda \prod_{i=1}^d \hat{\mu}_\lambda(dy_i).$$

Let $\dot{\mathfrak{Z}}_\lambda(\mathtt{f})$ denote the contribution to $\dot{\mathfrak{Z}}_\lambda$ from free variables, meaning $y_i \in (0,1)$ for all i. This can be decomposed further into the contribution $\dot{\mathfrak{Z}}_\lambda(\mathtt{f}_1)$ from isolated free variables (meaning $y_i = 1/2$ for all i) and the remainder $\dot{\mathfrak{Z}}_\lambda(\mathtt{f}_{\geqslant 2})$. We then calculate

$$\dot{\mathfrak{Z}}_\lambda(\mathtt{f}_1) = 2^\lambda\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2})\Big)^d.$$

This dominates the contribution from non-isolated free variables:

$$\begin{aligned}\dot{\mathfrak{Z}}_\lambda(\mathtt{f}_{\geqslant 2}) &= \sum_{j=1}^d \binom{d}{j}\bigg(\int y^\lambda \mathbf{1}\{y \in (0,1)\backslash\{\tfrac{1}{2}\}\}\hat{\mu}_\lambda(dy)\bigg)^j \Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2})\Big)^{d-j} \\ &\leqslant O(1)d\hat{\mu}_\lambda((0,1)\backslash\{\tfrac{1}{2}\})\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2})\Big)^d \leqslant \dot{\mathfrak{Z}}_\lambda(\mathtt{f}_1)k^{O(1)}/2^k.\end{aligned}$$

Next let $\dot{\mathfrak{Z}}_\lambda(\mathtt{1})$ denote the contribution from variables frozen to $\mathtt{1}$:

$$\begin{aligned}\dot{\mathfrak{Z}}_\lambda(\mathtt{1}) &= \bigg(\int y^\lambda \hat{\mu}_\lambda(dy)\bigg)^d - \bigg(\int y^\lambda \mathbf{1}\{y \in (0,1)\}\hat{\mu}_\lambda(dy)\bigg)^d \\ &= \Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + \hat{\mu}_\lambda(1) + \rho_\lambda\Big)^d - 2^{-\lambda}\dot{\mathfrak{Z}}_\lambda(\mathtt{f}_1) + \epsilon_k.\end{aligned}$$

The ratio of free to frozen variables is given by

$$\frac{\dot{\mathfrak{Z}}_\lambda(\mathtt{f})}{2[\dot{\mathfrak{Z}}_\lambda(\mathtt{1}) + 2^{-\lambda}\dot{\mathfrak{Z}}_\lambda(\mathtt{f})]} = \frac{2^\lambda}{2}\left(\frac{\hat{\mu}_\lambda(\frac{1}{2})}{\hat{\mu}_\lambda(\frac{1}{2}) + 2^\lambda \hat{\mu}_\lambda(1)}\right)^d + \epsilon_k = \frac{2^{\lambda-1}}{2^k} + \epsilon_k.$$

Combining these yields (2.10.6). The proof of (2.10.9) is very similar.
Estimate of $\bar{\mathfrak{Z}}_\lambda$. Recall from the definition (2.1.8) that

$$\bar{\mathfrak{Z}}_\lambda = \int \Big(xy + (1-x)(1-y)\Big)^\lambda \dot{\mu}_\lambda(dx)\hat{\mu}_\lambda(dy).$$

The contribution to $\bar{\mathfrak{Z}}$ from $x = 1$ is given by

$$\bar{\mathfrak{Z}}_\lambda(x = 1) = \dot{\mu}_\lambda(1)\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + \hat{\mu}_\lambda(1) + \rho_\lambda\Big).$$

There is an equal contribution from the case $x = 0$. Next, the contribution from $x \in (0,1)$ and $y = 1/2$ is given by

$$\bar{\mathfrak{Z}}_\lambda(x \in (0,1), y = 1/2) = \dot{\mu}_\lambda(\mathtt{f})2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}).$$

Lastly, the contribution from $x \in (0,1)$ and $y = 1$ is given by

$$\bar{\mathfrak{Z}}_\lambda(x \in (0,1), y = 1) = \hat{\mu}_\lambda(1)\psi_\lambda,$$

and there is an equal contribution from the case $x \in (0,1)$ and $y = 0$. The contribution from the case that both $x, y \in (0,1)$ is $\leqslant k^{O(1)}/8^k$. Combining these estimates gives

$$\begin{aligned} d\ln\bar{\mathfrak{Z}}_\lambda &= d\ln\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + 2\dot{\mu}_\lambda(1)\hat{\mu}_\lambda(1) + 2\dot{\mu}_\lambda(1)\rho_\lambda + 2\hat{\mu}_\lambda(1)\psi_\lambda\Big) + \epsilon_k \\ &= d\ln\Big(2^{-\lambda}\hat{\mu}_\lambda(\tfrac{1}{2}) + \hat{\mu}_\lambda(1) + \rho_\lambda\Big) + d\ln\left(1 + \frac{\hat{\mu}_\lambda(1)[-\dot{\mu}_\lambda(\mathtt{f}) + 2\psi_\lambda]}{2^{-\lambda}\hat{\mu}_\lambda(\frac{1}{2}) + \hat{\mu}_\lambda(\mathtt{1})}\right) + \epsilon_k. \end{aligned}$$

Recalling $\hat{\mu}_\lambda = \hat{\mathscr{R}}\dot{\mu}_\lambda$ gives

$$d\ln\left(1 + \frac{\hat{\mu}_\lambda(1)[-\dot{\mu}_\lambda(\mathtt{f}) + 2\psi_\lambda]}{2^{-\lambda}\hat{\mu}_\lambda(\frac{1}{2}) + \hat{\mu}_\lambda(\mathtt{1})}\right) = d\dot{\mu}_\lambda(0)^{k-1}[-\dot{\mu}_\lambda(\mathtt{f}) + 2\psi_\lambda] + \epsilon_k,$$

and (2.10.7) follows.
Estimate of $\hat{\mathfrak{Z}}_\lambda$. Recall from the definition (2.1.8) that

$$\hat{\mathfrak{Z}}_\lambda = \int \left(1 - \prod_{i=1}^k x_i - \prod_{i=1}^k (1-x_i)\right)\prod_{i=1}^k \dot{\mu}_\lambda(x_i).$$

The contribution to $\hat{\mathfrak{Z}}$ from separating clauses is

$$1 - 2\dot{\mu}_\lambda(\mathtt{0},\mathtt{f})^k + \dot{\mu}_\lambda(\mathtt{f})^k = 1 - (2/2^k)(1 + k\dot{\mu}(\mathtt{f})) + k^{O(1)}/8^k.$$

The contribution from clauses which are forcing to some variable that is not forced by any other clause is $2k\dot{\mu}_\lambda(0)^{k-1}\psi_\lambda$. The contribution from all other clause types is $\leqslant k^{O(1)}/8^k$, and (2.10.8) follows.

Estimate of s_λ. Recall from (2.1.10) the definition of s_λ. By similar considerations as above, it is straightforward to check that the total contribution from frozen variables, edges incident to frozen variables, and separating or forcing clauses is zero. The dominant term is the contribution of isolated free variables, and the estimate follows. □

2.10.3 Properties of the complexity function

We conclude by deducing some properties of the complexity function $\Sigma(s)$.

Lemma 2.10.6. *For fixed $1 \leqslant T < \infty$, the fixed point $\dot{q}_{\lambda,T}$ is continuously differentiable as a function of $\lambda \in [0,1]$.*

Proof. Fix $T < \infty$ and define $f_T[\dot{q},\lambda] \equiv \mathtt{BP}_{\lambda,T}[\dot{q}] - \dot{q}$ as the mapping from $\mathscr{P}(\dot{\Omega}_T) \times [0,1]$ to the set of signed measures on Ω_T. Since function $\dot{z}(\dot{\sigma})$ ($\hat{z}(\hat{\sigma})$, respectively) can take only finitely many values on $\dot{\Omega}_T$ ($\hat{\Omega}_T$, respectively) and therefore must be uniformly bounded away from 0. It is straightforward to check that for any $\lambda \in [0,1]$,

$$f_T[\dot{q}_\star(\lambda,T),\lambda](\dot{\sigma}) = 0, \quad \forall \dot{\sigma} \in \Omega_T,$$

and is uniformly differentiable in a neighborhood of $\{(\dot{q}_\star(\lambda,T),\lambda) : \lambda \in [0,1]\}$.

For any other $\dot{q}$ in the contraction region (2.4.5), Proposition 2.9.1 guarantees that

$$\begin{aligned}\|f_T[\dot{q},\lambda] - f_T[\dot{q}_\star(\lambda,T),\lambda]\|_1 &\geqslant \|\dot{q} - \dot{q}_\star(\lambda)\|_1 - \|\mathtt{BP}_{\lambda,T}[\dot{q}] - \mathtt{BP}_{\lambda,T}[\dot{q}_\star(\lambda,T)]\|_1 \\ &\geqslant (1 - O(k^2 2^{-k}))\|\dot{q} - \dot{q}_\star(\lambda,T)\|_1.\end{aligned}$$

Therefore the Jacobian matrix

$$\Big(\frac{\partial f_T(\dot{\sigma}_i)}{\partial \dot{q}(\dot{\sigma}_j)}\Big)_{\dot{\Omega}\times\dot{\Omega}}$$

is invertible at each $(\dot{q}_\star(\lambda,T),\lambda)$. By implicit function theorem, $\dot{q}_\star(\lambda,T)$, as the solution of $f_T[\dot{q},\lambda] = 0$, is uniformly differentiable in λ. □

Let us first fix $T < \infty$ and consider the clusters encoded by T-colorings. We have explicitly defined $\boldsymbol{\Sigma}(H)$ and $\boldsymbol{s}(H)$. Let

$$\mathcal{S}(s) \equiv \sup\{\boldsymbol{\Sigma}(H) : \boldsymbol{s}(H) = s\},$$

with the convention that a supremum over an empty set is $-\infty$. Thus $\mathcal{S}(s)$ is a well-defined function which captures the spirit of the function $\Sigma(s)$ discussed in the introduction. (Note $\mathcal{S}$ implicitly depends on T since the maximum is taken over empirical measures H which are supported on T-colorings.) Recall that the physics approach [Krz+07] takes $\mathcal{S}(s)$ as a conceptual starting point. However, for purposes of explicit calculation the actual starting point is the Legendre dual

$$\mathfrak{F}(\lambda) \equiv (-\mathcal{S})^\star(\lambda) = \sup_{s\in\mathbb{R}} \Big\{ \lambda s + \mathcal{S}(s) \Big\} = \sup_H \boldsymbol{F}_\lambda(H),$$

where $\boldsymbol{F}_\lambda(H) \equiv \lambda \boldsymbol{s}(H) + \boldsymbol{\Sigma}(H)$. The replica symmetry breaking heuristic gives an explicit conjecture for $\mathfrak{F}$. One then makes the assumption that $\mathcal{S}(s)$ is *concave* in s: this means it is the same as

$$\mathcal{R}(s) \equiv -\mathfrak{F}^\star(s) = -(-\mathcal{S})^{\star\star}(s),$$

so if $\mathcal{S}$ is concave then it can be recovered from $\mathfrak{F}$.

We do not have a proof that $\mathcal{S}(s)$ is concave for all s, but we will argue that this holds on the interval of s corresponding to $\lambda \in [0,1]$. Formally, for $\lambda \in [0,1]$, we proved that $\boldsymbol{F}_\lambda(H)$ has a unique maximizer $H_\star \equiv H_\lambda$. This implies that there is a unique s_λ which maximizes $\lambda s + \mathcal{S}(s)$, given by

$$s_\lambda = \boldsymbol{s}(H_\lambda).$$

Recall that H_λ and s_λ both depend implicitly on T. We also have from Lemma 2.10.6 that for any fixed $T < \infty$, s_λ is continuous in λ, so it maps $\lambda \in [0,1]$ onto some compact interval $\mathcal{I} \equiv [s_-, s_+]$. Define the modified function

$$\overline{\mathcal{S}}(s) \equiv \begin{cases} \mathcal{S}(s) & s \in \mathcal{I}, \\ -\infty & \text{otherwise.} \end{cases}$$

Lemma 2.10.7. *For all $s \in \mathbb{R}$, $\overline{\mathcal{S}}(s) = -(-\overline{\mathcal{S}})^{\star\star}(s)$. Consequently the function $\overline{\mathcal{S}}$ is concave, and s_λ is nondecreasing in λ.*

Proof. The function $-\mathcal{S}(s)$ has Legendre dual

$$\overline{\mathfrak{F}}(\lambda) = \sup_{s\in\mathbb{R}} \Big\{ \lambda s + \overline{\mathcal{S}}(s) \Big\} = \sup_{s\in\mathcal{I}} \Big\{ \lambda s + \mathcal{S}(s) \Big\} \leqslant \mathfrak{F}(\lambda).$$

For $\lambda \in [0,1]$ it is clear that $\overline{\mathfrak{F}}(\lambda) = \mathfrak{F}(\lambda)$. It is straightforward to check that if $\lambda < 0$ then

$$\overline{\mathfrak{F}}(\lambda) \leqslant \max_{s\in\mathcal{I}} \lambda s + \max_{s\in\mathcal{I}} \mathcal{S}(s) = \lambda s_{\min} + \mathcal{S}(s_0),$$

so if $s < s_{\min}$ then

$$(-\overline{\mathcal{S}})^{\star\star}(s) = (\overline{\mathfrak{F}})^\star(s) \geqslant \sup_{\lambda<0} \Big\{ \lambda s - \overline{\mathfrak{F}}(\lambda) \Big\} \geqslant \sup_{\lambda<0} \Big\{ \lambda(s - s_{\min}) - \mathcal{S}(s_0) \Big\} = +\infty.$$

A symmetric argument shows that $(-\overline{\mathcal{S}})^{\star\star}(s) = +\infty$ also for $s > s_{\max}$. If $s \in \mathcal{I}$, we must have $s = s_{\lambda_\circ}$ for some $\lambda_\circ \in [0,1]$, and so

$$(-\overline{\mathcal{S}})^{\star\star}(s) \geqslant \lambda_\circ s - \mathfrak{F}(\lambda_\circ) = -\mathcal{S}(s).$$

This proves $(-\overline{\mathcal{S}})^{\star\star}(s) \geqslant -\overline{\mathcal{S}}(s)$ for all $s \in \mathbb{R}$. On the other hand, it holds for any function f that $f^{\star\star} \leqslant f$, so we conclude $(-\overline{\mathcal{S}})^{\star\star}(s) = -\overline{\mathcal{S}}(s)$ for all $s \in \mathbb{R}$. This implies that $\overline{\mathcal{S}}$ is concave, concluding the proof. ∎

Proof of Proposition 2.1.4. We can obtain $\Sigma(s)$ as the limit of $\overline{\mathbb{S}}(s)$ in the limit $T \to \infty$. It follows from Lemma 2.10.7 together with Corollary 2.9.2 that it is strictly decreasing in s. $\square$

2.11 Constrained entropy maximization

In this section we review some general theory for entropy maximization problems under affine constraints.

2.11.1 Constraints and continuity

We will optimize a functional over non-negative measures ν on a finite space X (with $|X| = s$), subject to some affine constraints $M\nu = b$. We begin by discussing basic continuity properties. Denote

$$\mathbb{H}(b) \equiv \{\nu \geqslant 0\} \cap \{M\nu = b\} \subseteq \mathbb{R}^s.$$

Let $\Delta \equiv \{\nu \geqslant 0\} \cap \{\langle \mathbf{1}, \nu\rangle = 1\}$, and let $\boldsymbol{B}$ denote the space of $b \in \mathbb{R}^r$ for which

$$\varnothing \neq \mathbb{H}(b) \subseteq \Delta.$$

Then $\boldsymbol{B}$ is contained in the image of Δ under M, so $\boldsymbol{B}$ is a compact subset of $\mathbb{R}^r$.

Proposition 2.11.1. *If $\boldsymbol{F}$ is any continuous function on Δ and*

$$F(b) = \max\{\boldsymbol{F}(\nu) : \nu \in \mathbb{H}(b)\}, \tag{2.11.1}$$

then F is (uniformly) continuous over $b \in \boldsymbol{B}$.

Proposition 2.11.1 is a straightforward consequence of the following two lemmas.

Lemma 2.11.2. *For $b \in \boldsymbol{B}$ and any vector u in the unit sphere $\mathbb{S}^{r-1}$, let*

$$d(b, u) \equiv \inf\{t \geqslant 0 : b + tu \notin \boldsymbol{B}\}.$$

There exists $\delta = \delta(b) > 0$ such that

$$d(b, u) \in \{0\} \cup [\delta, \infty) \quad \textit{for all } b \in \boldsymbol{B}.$$

Proof. $\boldsymbol{B}$ is a polytope, so it can be expressed as the intersection of finitely many closed half-spaces $H_1, \ldots, H_k$, where $H_i = \{x \in \mathbb{R}^r : \langle a_i, x\rangle \leqslant c_i\}$. Consequently there is at least one index $1 \leqslant i \leqslant k$ such that

$$d(b, u) = \inf\{t \geqslant 0 : b + tu \notin H_i\}.$$

It follows that $\langle a_i, u\rangle > 0$ and

$$d(b,u) = \frac{c_i - \langle a_i, b\rangle}{\langle a_i, u\rangle} \geqslant \frac{c_i - \langle a_i, b\rangle}{|a_i|} = d(b, \partial H_i)$$

where $d(b, \partial H_i)$ is the distance between b and the boundary of H_i. In particular, $d(b,u) > 0$ if and only if $\langle a_i, b\rangle < c_i$, which in turn holds if and only if $d(b, \partial H_i) > 0$. It follows that for all $u \in \mathbb{S}^{r-1}$ we have $d(b,u) \in \{0\} \cup [\delta, \infty)$ with

$$\delta = \delta(b) = \min\{d(b, \partial H_i) : d(b, \partial H_i) > 0\};$$

δ is a minimum over finitely many positive numbers so it is also positive. $\square$

Lemma 2.11.3. *The set-valued function $\mathbb{H}$ is continuous on $\boldsymbol{B}$ with respect to the Hausdorff metric $d_{\mathcal{H}}$, that is to say, if $b_n \in \boldsymbol{B}$ with $\lim_{n\to\infty} b_n = b$ then*

$$\lim_{n\to\infty} d_{\mathcal{H}}(\mathbb{H}(b_n), \mathbb{H}(b)) = 0.$$

Proof. Recall that the Hausdorff distance between two subsets X and Y of a metric space is

$$d_{\mathcal{H}}(X,Y) = \inf\{\epsilon \geqslant 0 : X \subseteq Y^\epsilon \text{ and } Y \subseteq X^\epsilon\},$$

where X^ϵ, Y^ϵ are the ϵ-thickenings of X and Y. Any sequence $\nu_n \in \mathbb{H}(b_n)$ converges along subsequences to limits $\nu \in \mathbb{H}(b)$, so for all $\epsilon > 0$ there exists $n_0(\epsilon)$ large enough that

$$\mathbb{H}(b_n) \subseteq (\mathbb{H}(b))^\epsilon, \quad n \geqslant n_0(\epsilon).$$

In the other direction, we now argue that if $\nu \in \mathbb{H}(b)$ and $b' = b + tu$ for $u \in \mathbb{S}^{r-1}$ and t a small positive number, then we can find $\nu' \in \mathbb{H}(b')$ which is close to ν. For $u \in \mathbb{S}^{r-1}$ let $d(b,u)$ be as in Lemma 2.11.2, and take $\nu(b,u)$ to be any fixed element of $\mathbb{H}(b + d(b,u)u)$ (which by definition is nonempty). Since we consider $b' = b + tu$ for $t > 0$, we can assume that $d(b,u)$ is positive, hence $\geqslant \delta(b)$ by Lemma 2.11.2. We can express $b' = b + tu$ as the convex combination

$$b' = (1-\epsilon)b + \epsilon[b + d(b,u)u], \quad \epsilon = \frac{t}{d(b,u)} = \frac{|b'-b|}{d(b,u)} \leqslant \frac{|b'-b|}{\delta}.$$

Then $\nu' = (1-\epsilon)\nu + \epsilon\nu(b,u) \in \mathbb{H}(b')$, so

$$|\nu' - \nu| = \epsilon|\nu(b,u) - \nu| \leqslant \frac{(\operatorname{diam}\Delta)|b-b'|}{\delta}$$

This implies $H(b) \subseteq (H(b_n))^\epsilon$ for large enough n, and the result follows. $\square$

Proof of Proposition 2.11.1. Take $\nu \in \mathbb{H}(b)$ so that $F(b) = \boldsymbol{F}(\nu)$. If $b' = b + tu \in \boldsymbol{B}$ for $u \in \mathbb{S}^{r-1}$, then Lemma 2.11.3 implies that we can find $\nu' \in \mathbb{H}(b')$ with $|\nu' - \nu| = o_t(1)$, where $o_t(1)$ indicates a function tending to zero in the limit $t \downarrow 0$, uniformly over $u \in \mathbb{S}^{r-1}$. It follows that $\boldsymbol{F}(\nu) = \boldsymbol{F}(\nu') + o_t(1)$, since $\boldsymbol{F}$ is uniformly continuous on Δ by the Heine–Cantor theorem. Therefore

$$F(b) = \boldsymbol{F}(\nu) = \boldsymbol{F}(\nu') + o_t(1) \leqslant F(b') + o_t(1).$$

By the same argument $F(b') \leqslant F(b) + o_t(1)$, concluding the proof. $\square$

When solving (2.11.1) for a *fixed* value of $b \in \boldsymbol{B}$, it will be convenient to make the following reduction:

Remark 2.11.4. Suppose M is an $r \times s$ matrix where $s = |X|$. We can assume without loss that M has full rank r, since otherwise we can eliminate redundant constraints. We consider only $b \in \boldsymbol{B}$, meaning $\varnothing \neq \mathbb{H}(b) \subseteq \Delta$. The affine space $\{M\nu = b\}$ has dimension $s - r$; we assume this is positive since otherwise $\mathbb{H}(b)$ would be a single point. Then, if $\mathbb{H}(b)$ does not contain an interior point of $\{\nu \geqslant 0\}$, it must be that

$$X_\circ \equiv \{x \in X : \exists \nu \in \{\nu \geqslant 0\} \cap \{M\nu = b\} \text{ so that } \nu(x) > 0\}$$

is a nonempty subset of X. In this case, it is equivalent to solve the optimization problem over measures $\nu_\circ$ on the reduced alphabet $X_\circ$, subject to constraints $M'\nu_\circ = b$ where M' is the submatrix of M formed by the columns indexed by $X_\circ$. Then, by construction, the space

$$\mathbb{H}_\circ(b) = \{\nu_\circ \geqslant 0\} \cap \{M'\nu_\circ = b\}$$

contains an interior point of $\{\nu_\circ \geqslant 0\}$. The matrix M' is $r \times s_\circ$ where $s_\circ = |X_\circ|$; and if M' is not of rank r then we can again remove redundant constraints, replacing M' with an $r_\circ \times s_\circ$ submatrix $M_\circ$ which has full rank $r_\circ$. We emphasize that the final matrix $M_\circ$ depends on b. In conclusion, when solving (2.11.1) for a fixed $b \in \boldsymbol{B}$, we may assume with no essential loss of generality that the original matrix M is $r \times s$ with full rank r, and that $\mathbb{H}(b) = \{\nu \geqslant 0\} \cap \{M\nu = b\}$ contains an interior point of $\{\nu \geqslant 0\}$. It follows that this space has dimension $s - r > 0$, and its boundary is contained in the boundary of $\{\nu \geqslant 0\}$.

2.11.2 Entropy maximization

We now restrict (2.11.1) to the case of functionals $\boldsymbol{F}$ which are *concave* on the domain $\{\nu \geqslant 0\}$. It is straightforward to verify from definitions that the optimal value $F(b)$ is (weakly) concave in b. Recall that the convex conjugate of a function f on domain C is the function $f^\star$ defined by

$$f^\star(x^\star) = \sup\{\langle x^\star, x\rangle - f(x) : x \in C\}.$$

Denote $G(\gamma) \equiv (-\boldsymbol{F})^\star(M^t\gamma)$, and consider the Lagrangian functional

$$\mathcal{L}(\gamma; b) = \sup\{\boldsymbol{F}(\nu) + \langle \gamma, M\nu - b\rangle : \nu \geqslant 0\} = -\langle \gamma, b\rangle + G(\gamma).$$

It holds for any $\gamma \in \mathbb{R}^r$ that $\mathcal{L}(\gamma; b) \geqslant F(b)$, so

$$F(b) \leqslant \inf\{\mathcal{L}(\gamma; b) : \gamma \in \mathbb{R}^r\} = -G^\star(b). \tag{2.11.2}$$

Now assume ψ is a positive function on X, and consider (2.11.1) for the special case

$$\boldsymbol{F}(\nu) = \mathcal{H}(\nu) + \langle \nu, \ln \psi \rangle = \sum_{x \in X} \nu(x) \ln \frac{\psi(x)}{\nu(x)}. \tag{2.11.3}$$

We remark that the supremum in $(-\mathcal{H})^\star(\nu^\star) = \sup\{\langle \nu^\star, \nu \rangle + \mathcal{H}(\nu) : \nu \geqslant 0\}$ is uniquely attained by $\nu^{\text{opt}}(x) = \exp\{-1 + \nu^\star(x)\}$, yielding

$$(-\mathcal{H})^\star(\nu^\star) = \langle \nu^{\text{opt}}(\nu^\star), 1 \rangle = \sum_x \exp\{-1 + \nu^\star(x)\}.$$

This gives the explicit expression

$$G(\gamma) = (-\boldsymbol{F})^\star(M^t\gamma) = (-\mathcal{H})^\star(\ln \psi + M^t\gamma) = \sum_x \psi(x) \exp\{-1 + (M^t\gamma)(x)\}. \tag{2.11.4}$$

Lemma 2.11.5. *Assume ψ is a strictly positive function on a set X of size s and that M is $r \times s$ with rank r. Then the function $G(\gamma)$ of (2.11.4) is strictly convex in γ.*

Proof. Let $\nu \equiv \nu(\gamma)$ denote the measure on X defined by

$$\nu(x) = \psi(x) \exp\{-1 + (M^t\gamma)(x)\},$$

and write $\langle f(x) \rangle_\nu \equiv \langle f, \nu \rangle$. The Hessian matrix $H \equiv \operatorname{Hess} G(\gamma)$ has entries

$$H_{i,j} = \frac{\partial^2 \mathcal{L}(\gamma; b)}{\partial \gamma_i \partial \gamma_j} = \sum_{x \in X} \nu(x) M_{i,x} M_{j,x} = \langle M_{i,x} M_{j,x} \rangle_\nu.$$

Let M_x denote the vector-valued function $(M_{i,x})_{i \leqslant r}$, so

$$\alpha^t H \alpha = \langle (\alpha^t M_x)^2 \rangle_\nu.$$

This is zero if and only if $\nu(\{x \in X : \alpha^t M_x = 0\}) = 1$. Since ν is a positive measure, this can only happen if $\alpha^t M_x = 0$ for all $x \in X$, but this contradicts the assumption that M has rank r. This proves that H is positive-definite, so G is strictly convex in γ. ☐

Proposition 2.11.6. *Let $b \in \boldsymbol{B}$ such that $\mathbb{H}(b) = \{\nu \geqslant 0\} \cap \{M\nu = b\}$ contains an interior point of $\{\nu \geqslant 0\}$, and consider the optimization problem (2.11.1) for $\boldsymbol{F}$ as in (2.11.3). For this problem, the inequality (2.11.2) becomes an equality,*

$$F(b) = \inf\{\mathcal{L}(\gamma; b) : \gamma \in \mathbb{R}^r\} = -G^\star(b).$$

Further, $\mathcal{L}(\gamma; b)$ is strictly convex in γ, and its infimum is achieved by a unique $\gamma = \gamma(b)$. The optimum value of (2.11.1) is uniquely attained by the measure $\nu = \nu^{\text{opt}}(b)$ defined by

$$\nu(x) = \psi(x) \exp\{-1 + (M^t\gamma)(x)\}. \tag{2.11.5}$$

For any $\mu \in \mathbb{H}(b)$, $\boldsymbol{F}(\nu) - \boldsymbol{F}(\mu) = \mathcal{H}(\mu|\nu) \gtrsim \|\nu - \mu\|^2$. Finally, in a neighborhood of b in $\boldsymbol{B}$, $\gamma'(b)$ is defined and $F(b)$ is strictly concave in b.

Proof. Under the assumptions, the boundary of the set $\mathbb{H}(b)$ is contained in the boundary of $\{\nu \geqslant 0\}$. The entropy $\mathcal{H}$ has unbounded gradient at this boundary, so for $\boldsymbol{F}$ as in (2.11.3), the optimization problem (2.11.1) must be solved by a strictly positive measure $\nu > 0$. Since $\nu > 0$, we can differentiate in the direction of any vector δ with $M\delta = 0$ to find

$$0 = \frac{d}{dt}\bigg[\mathcal{H}(\nu + t\delta) + \langle \ln \psi, \nu + t\delta \rangle\bigg]\bigg|_{t=0} = \langle \delta, -1 - \ln \nu + \ln \psi \rangle.$$

Recalling Remark 2.11.4, we assume without loss that M is $r \times s$ with rank r, since otherwise we can eliminate redundant constraints. Then, since $M\delta = 0$, for any $\gamma \in \mathbb{R}^r$ we have

$$0 = \langle \delta, \epsilon \rangle \quad \text{where } \epsilon = -1 - \ln \nu + \ln \psi + M^t \gamma.$$

We can then solve for γ so that $M\epsilon = 0$:[7]

$$\gamma = (MM^t)^{-1} M(\ln \nu - \ln \psi + 1).$$

Setting $\delta = \epsilon$ in the above gives $0 = \|\epsilon\|^2$, therefore we must have $\epsilon = 0$. This proves the existence of $\gamma = \gamma(b) \in \mathbb{R}^r$ such that (2.11.1) is optimized by $\nu = \nu^{\mathrm{opt}}(b)$, as given by (2.11.5). The optimal value of (2.11.1) is then

$$\begin{aligned} F(b) &= \langle 1, \nu^{\mathrm{opt}}(b) \rangle - \langle M^t \gamma(b), \nu^{\mathrm{opt}}(b) \rangle \\ &= \sum_x \psi(x) \exp\{-1 + (M^t\gamma)(x)\} - \langle \gamma, b \rangle \bigg|_{\gamma = \gamma(b)} = \mathcal{L}(\gamma(b), b). \end{aligned}$$

In view of (2.11.2), this proves that in fact

$$-G^\star(b) = \inf\{\mathcal{L}(\gamma, b) : \gamma \in \mathbb{R}^r\} = \min\{\mathcal{L}(\gamma, b) : \gamma \in \mathbb{R}^r\} = \mathcal{L}(\gamma(b), b) = F(b)$$

as claimed. Now recall from Lemma 2.11.5 that $G(\gamma)$ is strictly convex, which implies that $\mathcal{L}(\gamma; b)$ is strictly convex in γ. Thus $\gamma = \gamma(b)$ is the unique stationary point of $\mathcal{L}(\gamma; b)$.

These conclusions are valid under the assumption that $\mathbb{H}(b)$ contains an interior point of $\{\nu \geqslant 0\}$, which is valid in a neighborhood of b in $\boldsymbol{B}$. Throughout this neighborhood, $\gamma(b)$ is defined by the stationarity condition $b = G'(\gamma)$. Differentiating again with respect to γ gives

$$b'(\gamma) = \operatorname{Hess} G(\gamma), \quad \gamma'(b) = [\operatorname{Hess} G(\gamma(b))]^{-1}. \tag{2.11.6}$$

We also find (in this neighborhood) that

$$F'(b) = -\gamma(b), \quad F''(b) = -\gamma'(b) = -[\operatorname{Hess} G(\gamma(b))]^{-1},$$

so F is strictly concave.

[7]The matrix MM^t is invertible: if $MM^t x = 0$ then $M^t x \in \ker M = (\operatorname{im} M^t)^\perp$. On the other hand clearly $M^t x \in \operatorname{im} M^t$, so $M^t x \in (\operatorname{im} M^t) \cap (\operatorname{im} M^t)^\perp = \{0\}$. Therefore $x \in \ker M^t$, but M^t is injective by assumption.

It remains to prove that $\boldsymbol{F}(\nu) - \boldsymbol{F}(\mu) = \mathcal{H}(\mu|\nu)$. (The estimate $\mathcal{H}(\mu|\nu) \gtrsim \|\mu-\nu\|^2$ is well known and straightforward to verify.) For any measure μ,

$$-\mathcal{H}(\mu|\nu) = \mathcal{H}(\mu) + \langle \mu, \ln(\psi \exp\{-1 + M^t\gamma\})\rangle.$$

Applying this with $\mu = \nu$ gives

$$0 = -\mathcal{H}(\nu|\nu) = \mathcal{H}(\nu) + \langle \nu, \ln(\psi \exp\{-1 + M^t\gamma\})\rangle.$$

Subtracting these two equations gives

$$-\mathcal{H}(\mu|\nu) = \mathcal{H}(\mu) - \mathcal{H}(\nu) + \langle \mu - \nu, \ln \psi\rangle + \langle \mu - \nu, \ln(\exp\{-1 + M^t\gamma\})\rangle.$$

If $M\nu = M\nu = b$ then the last term vanishes, giving $-\mathcal{H}(\mu|\nu) = \boldsymbol{F}(\mu) - \boldsymbol{F}(\nu)$. □

Remark 2.11.7. Our main application of Proposition 2.11.6 is for the depth-one tree $\mathcal{D}$ as shown in Figure 2.5.3. In the notation of the current section, X is the space of valid T-colorings $\underline{\sigma}$ of $\mathcal{D}$, and $\psi : X \to (0,\infty)$ is defined by

$$\psi(\underline{\sigma}) = \boldsymbol{w}_{\mathcal{D}}(\underline{\sigma})^\lambda = \left\{ \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a\in\partial v} [\bar{\Phi}(\sigma_{av})\hat{\Phi}(\underline{\sigma}_{\delta a})] \right\}^\lambda.$$

We then wish to solve the optimization problem (2.11.1) for $\boldsymbol{F}(\nu)$ as in (2.11.3), under the constraint that ν has marginals $\dot{h}^{\text{tree}}(\dot{\sigma})$ on the boundary edges $\mathcal{L}(\mathcal{D})$. This can be expressed as $M\nu = \dot{h}$ where M has rows indexed by the spins $\dot{\sigma} \in \dot{\Omega}$, columns indexed by valid T-colorings $\underline{\zeta}$ of $\mathcal{D}$: the $(\dot{\sigma}, \underline{\zeta})$ entry of M is given by

$$M(\dot{\sigma}, \underline{\zeta}) = |\mathcal{L}(\mathcal{D})|^{-1} \sum_{e\in\mathcal{L}(\mathcal{D})} \mathbf{1}\{\dot{\zeta}_e = \dot{\sigma}\}.$$

Recall Remark 2.11.4, let $\dot{\Omega}_+ = \{\dot{\sigma} \in \dot{\Omega} : \dot{h}^{\text{tree}}(\dot{\sigma}) > 0\}$, and $X_\circ = \{\underline{\zeta} \in X : M(\dot{\sigma}, \underline{\zeta}) = 0\ \forall \dot{\sigma} \notin \dot{\Omega}\}$. Let M_+ be the $\dot{\Omega}_+ \times X_\circ$ submatrix of M, and set $\dot{q}(\dot{\sigma}) = 0$ for all $\dot{\sigma} \notin \dot{\Omega}_+$. Next, in the matrix M_+, if the $\dot{\zeta}$ row is a linear combination of other rows, then set $\dot{q}(\dot{\zeta}) = 1$ and remove this row. Repeat until we arrive at an $\dot{\Omega}_\circ \times X_\circ$ matrix $M_\circ$ of full rank $r_\circ = |\dot{\Omega}_\circ|$. The original problem reduces to an optimization over $\{\nu_\circ \geqslant 0\} \cap \{M_\circ \nu_\circ = b_\circ\}$ where $b_\circ$ denotes the entries of b indexed by $\dot{\Omega}_\circ$. It follows from Proposition 2.11.6 that the unique maximizer of (2.11.1) is the measure $\nu = \nu^{\text{opt}}(b)$ given by

$$\nu(\underline{\sigma}) = \frac{1}{Z}\boldsymbol{w}_{\mathcal{D}}(\underline{\sigma})^\lambda = \frac{1}{Z}\left\{ \dot{\Phi}(\underline{\sigma}_{\delta v}) \prod_{a\in\partial v} [\bar{\Phi}(\sigma_{av})\hat{\Phi}(\underline{\sigma}_{\delta a})] \right\}^\lambda \prod_{e\in\mathcal{L}(\mathcal{D})} \dot{q}(\sigma_e).$$

Note however that if M_+ is not of full rank then $\dot{q}$ need not be unique.

Chapter 3

Reconstruction threshold of graph coloring

In this chapter we study the reconstruction threshold for k-coloring model on d-regular trees, the main result is Theorem 2. We first give a formal definition of reconstruction threshold using the broadcasting models on trees.

3.1 Introduction

The broadcast model on a tree is the process where information is sent from the root downward, along edges acting as noisy channels, to the leaves of the tree. Given a tree $T = (V, E)$, a finite set $[k] = \{1, \ldots, k\}$ of k values and a $[k] \times [k]$ probability matrix M as the noisy channel, the broadcast model on tree T is the probability measure on the space of configurations $[k]^V$ defined as follows: The spin σ_ρ at the root ρ is chosen according to the stationary distribution of M, denoted by π. Then for each vertex $v \in T$ with parent u, the spin σ_v is chosen according to the conditional distribution $\mathbb{P}(\sigma_v = i \mid \sigma_u = j) = M(i, j)$. For example, the coloring model has alphabet $[k]$ and probability matrix $M(i, j) = \frac{1}{k-1}\mathbf{1}\{i \neq j\}$. One can check that the measure defined by the broadcasting process is the same as the Gibbs measure defined in Definition 1.1.1 with $G = T$.

For technical convenience and independent interest, we allow randomness in the underlying trees. For any probability distribution ξ on the set of non-negative integers $\mathbb{Z}_+$, we let $\mathcal{T}_\xi$ denote the distribution of Galton-Watson tree with offspring distribution ξ. Two special cases of interest are the d-ary tree $\mathcal{T}_d$ and the Galton-Watson tree $\mathcal{T}_{\mathrm{Pois}(d)}$ with Poisson offspring distribution of average degree d, which are the local weak limit of random d-regular graphs and Erdős-Rényi random graphs respectively. The definition of broadcast model can be easily generalized to the (first finite levels of) Galton-Watson trees.

Given a (possibly random) infinite tree, the reconstruction problem asks if the distribution of the state of the root is affected by the configuration on the n'th level as n goes to infinity. More precisely, let T_n be the first n levels of tree T and L_n be its set of vertices at level n.

Write $T_n = T, L_n = \varnothing$ if T has fewer than n levels.

Definition 3.1.1 (Reconstruction)**.** Given a family of Galton-Watson trees $\mathcal{T}_\xi$, we say that the broadcast model with alphabet $[k]$ is reconstructible for $\mathcal{T}_\xi$ if there exist $i, j \in [k]$ such that,

$$\limsup_{n\to\infty} \mathbb{E}_{T\sim\mathcal{T}_\xi} d_{\mathrm{TV}}(\mathbb{P}(\sigma_{L_n} = \cdot \mid T, \sigma_\rho = i), \mathbb{P}(\sigma_{L_n} = \cdot \mid T, \sigma_\rho = j)) > 0,$$

where d_{TV} is the total-variation distance. Otherwise, we say that it is non-reconstructible.

Non-reconstruction implies that on average the spins on the distant levels have a vanishing effect on the root. Equivalently, it corresponds to the mutual information between the root and the leaves going to 0 (see e.g. [Mos04] for more equivalent definitions). Apart from the study of random CSPs, reconstruction of broadcast models also emerge in many other settings, for example in biology it determines a phase transition for the information requirements for phylogenetic reconstruction [DMR11].

Locating the exact reconstruction threshold has only been achieved in a small number of spin systems, the symmetric [Eva+00] and near-symmetric binary channels [Bor+06] and the three state symmetric channel with large degrees [Sly11]. For the k-coloring model only bounds are known which match in the first and second order asymptotic term. In one direction, the model is non-reconstructible whenever [Bha+11; Sly09; Eft15]

$$d \leqslant k(\ln k + \ln\ln k + 1 - \ln 2 + o_k(1)). \tag{3.1.1}$$

In the other direction, one need to find algorithms that reconstruct the root better than random guess. One simple algorithm is to reconstruct the root only when it is uniquely determined by the leaves. Calling the root in such case *frozen*. We define the freezing threshold as follows.

Definition 3.1.2 (Freezing)**.** Given a family of Galton-Watson tree $\mathcal{T}_\xi$, we say that the broadcast model with alphabet $[k]$ is frozen for $\mathcal{T}_\xi$ if

$$\limsup_{n\to\infty} \mathbb{P}_{T\sim\mathcal{T}_\xi}(\sigma_\rho \text{ is uniquely determined by } \sigma_{L_n}) > 0.$$

The exact location of the freezing threshold for Poisson tree $\mathcal{T}_{\mathrm{Pois}(d)}$ has been calculated in [Mol12]. Following a similar calculation for $\mathcal{T}_d$, one can show that for $k \geqslant k_0$, the k-coloring model is frozen if and only if (see also [MP03; Sem08])

$$d > d_k^f := \begin{cases} \inf_{x>0} x \ln^{-1}\left(1 - \frac{(1-e^{-x})^k}{k-1}\right) & \mathcal{T}_d \\ \inf_{x>0} \frac{(k-1)x}{(1-e^{-x})^k} & \mathcal{T}_{\mathrm{Pois}(d)} \end{cases} = k(\ln k + \ln\ln k + 1 + o_k(1)). \tag{3.1.2}$$

Moreover, [Mol12] proves that the freezing threshold for k-colorings on $\mathcal{T}_{\mathrm{Pois}(d)}$ corresponds to the rigidity threshold on Erdős-Rényi graph.

It is easy to see that the k-coloring problem is reconstructible on $\mathcal{T}_\xi$ if it is frozen. Indeed, the freezing threshold gives the best known upper bound for reconstruction threshold with the only exception of $d = 5$ and $k = 14$, in which case reconstruction is proved in [MM06] using a variational principle. The main result of this chapter is the following theorem showing that the reverse statement is not true for large k. Throughout we will assume that k exceeds a large enough absolute constant k_0, where the exact value may vary from place to place.

Theorem 2. *There exists a constant $\beta^* < 1$ such that for any $k \geqslant k_0$ the k-coloring model is reconstructible for both $\mathcal{T}_d$ and $\mathcal{T}_{\mathrm{Pois}(d)}$ for d satisfying*

$$d \geqslant k(\ln k + \ln \ln k + \beta^*). \tag{3.1.3}$$

Remark 3.1.3. The numerical result in [ZK07] suggests that the actual reconstruction threshold has a constant term roughly in the middle of $1 - \ln 2$ and 1, for technical reasons we only show reconstruction for β_* close to the freezing threshold 1.

We hope that the result of this chapter can contribute to the study of clustering phase transition of random CSPs in two directions. First, we show for the first time that the gap between reconstruction threshold and freezing threshold on trees is linear in k. This combined with the conjecture that reconstruction coincides with clustering strongly suggests a distinct phase where the solution space are clustered but non-frozen. It will be of great interest to analyze algorithms in this region. Secondly, the distributional recursion involved in the reconstruction problem (known as the averaged 1RSB equation in physics jargon [MM09]) is closely related to the BP recursion, thus in bounding the fixed point of the reconstruction recursion, we hope to provide additional information on the fixed point of the BP recursion, and shed light on the structure of the clusters.

3.1.1 Outline of the proof

Theorem 2 follows from a detailed analysis of the distributional tree recursion. We begin by specifying the distribution of the reconstruction probability $\mathbb{P}(\sigma_\rho = \cdot \mid \sigma_{L_n})$ on n-level trees as a function of the distribution on $(n-1)$-level trees $\mathbb{P}(\sigma_\rho = \cdot \mid \sigma_{L_{n-1}})$. This defines a distributional recursion on the set of probability measures on the k dimensional simplex Δ^k. For the purpose of proving reconstruction, it is enough to show that the recursion has a non-trivial fixed point, which is done in two steps: First we show that there exists a non-trivial measure μ on Δ^k such that after one step of the recursion the new measure stochastically dominates the original one. This step is done in Section 3.3. Given the result of stochastic dominance, we provide a randomized algorithm such that the distribution of the reconstruction probability equals μ on trees of any depth, which is done in Section 3.2.

3.2 Reconstruction algorithm

We begin by introducing the notations we will be using throughout the proof. In general, we will use $U, V \ldots$ for random variables and μ, ν for measures. To avoid complicated subscripts, we will use both U and μ_U for the distribution of U and use f_U for its density (using delta functions for atoms). For any function ϕ, we write $\phi \circ \mu$ for the distribution of $\phi(X)$, where X is a random sample of μ, denoted as $X \sim \mu$. We will use $B \oplus C$ to denote the (measure of) the sum of two independent copies of B and C, and $a \otimes B$ to denote the sum of a i.i.d. copies of B. One should distinguish these two operators with $+$ and $\cdot$, the usual addition and scaler multiplication of measures. By definition, we have

$$\mu_{B\oplus C} = \mu_B * \mu_C, \quad \mu_{a\otimes B} = \underbrace{\mu_B * \mu_B * \cdots * \mu_B}_{a \text{ times}}.$$

For any space Ω, we will use $\mathcal{M}(\Omega)$ to denote the space of probability measures on Ω. A substantial portion of our proof will be comparing different measures. For that sake, we define the following partial order on $\mathcal{M}(\overline{\mathbb{R}})$, where $\overline{\mathbb{R}} \equiv \mathbb{R} \cup \{-\infty, \infty\}$ is the extended real numbers.

Definition 3.2.1 (Stochastic dominance)**.** For $\mu, \nu \in \mathcal{M}(\overline{\mathbb{R}})$, we say that ν *stochastically dominates* μ, denoted by $\mu \prec \nu$, if for any $x \in \overline{\mathbb{R}}$, $\mu([-\infty, x]) \geqslant \nu([-\infty, x])$. Moreover, for any $\epsilon > 0$, we say that ν *stochastically dominates* μ *by* ϵ, denoted by $\mu \prec_\epsilon \nu$, if for any $x \in \overline{\mathbb{R}}$, we have either $\mu([-\infty, x]) = 1$ or $\nu([-\infty, x]) = 0$ or $\mu([-\infty, x]) - \epsilon \geqslant \nu([-\infty, x])$.

The following proposition gives two sufficient conditions of stochastic dominance that will be used throughout the proof. The proof of proposition should be trivial.

Proposition 3.2.2. *Let X, Y be two arbitrary independent random variables*

1. *If μ_X, μ_Y are absolutely continuous and $f_X(y) \leqslant f_Y(y)$ for all y satisfying $\mathbb{P}(Y \geqslant y) > 0$, then $X \succ Y$.*

2. *If X stochastically dominates Y by ϵ, then for any random variable X' such that $\mathbb{P}(X \neq X') \leqslant \epsilon$ and $\{x' : \mathbb{P}(X' < x') = 0\} \subseteq \{y : \mathbb{P}(Y < y) = 0\}$, X' also stochastically dominates y.*

3.2.1 k-coloring model and the tree recursion

In this section we give the distributional recursion involved in the reconstruction problem. Recall that $[k] = \{1, \ldots, k\}$ denotes the set of k-colors and let $T = (V, E) \sim \mathcal{T}_\xi$ be an instance of the Galton-Watson tree of offspring distribution ξ with root ρ. For each $n \geqslant 1$, let $T_n = (V_n, E_n)$ denote the restriction of T to its first n levels and let L_n be the leaves of T_n. For each n, the k-coloring model restricted on T_n is the uniform measure on the set of proper colorings

$$\Omega_n := \{\sigma \in [k]^{V_n} : \sigma_u \neq \sigma_v, \text{ for all } e = (u, v) \in E_n\}.$$

And we will use $\Omega(L_n)$ to denote the set of possible configurations on L_n.

For any $\eta \in \Omega(L_n)$ and $l \in [k]$, let f_n be the (deterministic) function defined as follows:

$$f_n(l, \eta; T) := \mathbb{P}(\sigma_\rho = l | T_n, \sigma_{L_n} = \eta).$$

Given tree T_n and the observed configuration $\eta \in \Omega(L_n)$, the maximum likelihood estimator of σ_ρ is the color l that achieves the maximum of $f_n(l, \eta; T)$, and this estimation is correct with probability $\max_l f_n(l, \eta; T)$. Let d_ρ be the degree of the root ρ of T, and $u_1, \ldots, u_{d_\rho}$ be the d_ρ offspring of the root ρ. For each $1 \leqslant i \leqslant d_\rho$, let T_i be the subtree rooted at u_i and $L_i^n = L_n \cap T_i$ be the subset of L_n restricted to T_i. Given the color of u_i, the configuration on T_i is independent of the configuration on $T \backslash T_i$. A standard recursive calculation gives that, for each $\eta \in \Omega(L_n)$ and $l \in [k]$,

$$f_{n+1}(l, \eta; T) = \frac{\prod_{i=1}^{d_\rho}(1 - f_n(l, \eta_i; T_i)}{\sum_{m=1}^{k} \prod_{i=1}^{d_\rho}(1 - f_n(m, \eta_i; T_i))}. \tag{3.2.1}$$

To study one step of the recursion from a vertex, one first samples the number of offspring from ξ then decides the color of each offspring accordingly. Let $\Xi^l = \Xi^l(n; \xi)$ denote the distribution of (T_n, σ_{L_n}) given $\sigma_\rho = l$ and let (T_n, η^l) be a sample from Ξ^l. Then the vector of posterior probability $\vec{X}_n := (f_n(1, \eta^1; T), \ldots, f_n(k, \eta^1; T))$ is a random vector in the k-dimensional simplex $\Delta^k := \{(x_1, \ldots, x_n) : x_i \geqslant 0, \sum_{i=1}^n x_i = 1\}$. Let (T_i, η_i^l) be the restriction of (T_n, η^l) onto T_i. By the symmetry between branches of Galton-Watson trees and the symmetry between colors, we have that

$$(f_n(m, \eta^l; T))_{m=1}^k \overset{d.}{=} (X_n^{(m-l+1)})_{m=1}^k,$$

where we uses the notation $x^{(l)}$ to denote the l-th entry of vector $\vec{x}$, modulo k when necessary. Furthermore, conditioned on the value of $\vec{X}_n^{(1)}$, $(\vec{X}_n^{(2)}, \ldots, \vec{X}_n^{(k)})$ are exchangeable. In particular $\vec{X}_n^{(l)} \overset{d.}{=} \vec{X}_n^{(2)}$ for all $l \neq 1$.

The distribution of $\vec{X}_n$ can be solved recursively using the following Δ^k-valued function Γ that takes an indefinite number of variables: Let

$$\Gamma^{(m)}(\vec{x}_{i,l}, l = 1, \ldots k, i = 1, \ldots b_l) := \frac{\prod_{l=2}^k \prod_{i=1}^{b_l}(1 - \vec{x}_{i,l}^{(m-l+1)})}{\sum_{l'=1}^k \prod_{l=2}^k \prod_{i=1}^{b_l}(1 - \vec{x}_{i,l}^{(l'-l+1)})}, \ \forall m \in [k], \tag{3.2.2}$$

where we adopt the convention of $\prod_{i \in \varnothing} a_i = 1$. Here b_l represent the number of u_i's with color l. Given d_ρ and $\sigma_\rho = 1$, the joint distribution of $(b_2, \ldots, b_k)$ follows the multinomial distribution with sum d_ρ and probability $(\frac{1}{k-1}, \ldots, \frac{1}{k-1})$ and $b_1 = 0$. Let $D_\rho, (B_1, \ldots, B_k)$ be an i.i.d. copy of $d_\rho, (b_1, \ldots, b_k)$ and $\vec{X}_{i,l}$ be i.i.d. samples of $\vec{X}_n$, (3.2.1) implies that

$$\vec{X}_{n+1} \overset{d.}{=} \left(\frac{\prod_{l=2}^k \prod_{i=1}^{B_l}(1 - \vec{X}_{i,l}^{(m-l+1)})}{\sum_{m'=1}^k \prod_{l=2}^k \prod_{i=1}^{B_l}(1 - \vec{X}_{i,l}^{(m'-l+1)})} \right)_{m=1}^k = \Gamma(\vec{X}_{i,l}, l = 1, \ldots k, i = 1, \ldots B_l). \tag{3.2.3}$$

Let $\tilde{\Xi}$ be the distribution of (T_n, σ_{L_n}) without conditioning on the value of σ_ρ and define the unconditional posterior probability $\tilde{X}_n := (f_n(1, \tilde{\eta}; T), \dots, f_n(k, \tilde{\eta}, T))$ similarly, where $\tilde{\eta}$ is sampled from $\tilde{\Xi}$. The distribution of $\vec{X}_n$ and $\tilde{X}_n$ satisfies that at each point $x \in \Delta^k$,

$$\begin{aligned}\mathbb{P}(\vec{X}_n \in dx) &= k\mathbb{P}\left(\sigma_\rho = 1, \left(\mathbb{P}(\tau_\rho = j \mid T_n, \tau_{L_n} = \sigma_{L_n})\right)_{j=1}^k \in dx\right) \\ &= k\mathbb{P}(\tilde{X}_n \in dx)\mathbb{P}(\sigma_\rho = 1 \mid \left(\mathbb{P}(\tau_\rho = j \mid T_n, \tau_{L_n} = \sigma_{L_n})\right)_{j=1}^k \in dx) \\ &= kx^{(1)}\mathbb{P}(\tilde{X}_n \in dx). \end{aligned} \tag{3.2.4}$$

Equation (3.2.3) and (3.2.4) are all we need to describe the distributional recursion. To be more concrete, we introduce some further notations. Let $\mathcal{M}_s(\Delta^k) \subset \mathcal{M}(\Delta^k)$ be the subset of measures in $\mathcal{M}(\Delta^k)$ that are invariant under permutations of the coordinates. With some abuse of notation, we will also use Γ for the transformation it induces on $\mathcal{M}(\Delta^k)$, i.e. for any $\nu \in \mathcal{M}(\Delta^k)$, we define $\Gamma\nu$ as the distribution of $\Gamma(\vec{X}_{i,l}, l = 1, \dots, k, i = 1, \dots B_l)$ where $\vec{X}_{i,l}$ are i.i.d. copies with distribution ν and B_l are defined as before. For each $\nu \in \mathcal{M}_s(\Delta^k)$, let $\Pi_l\nu$ be defined as $(\Pi_l\nu)(dx) := kx^{(l)}\nu(dx)$ and define

$$\Gamma_s\nu := \frac{1}{k}\sum_{l=1}^k (\Gamma \circ \Pi_l)\nu. \tag{3.2.5}$$

Under these notations, if $\tilde{X}_n \sim \nu$, then $\vec{X}_n \sim \Pi_1\nu$, $\vec{X}_{n+1} \sim \Gamma \circ \Pi_1\nu$ and $\tilde{X}_{n+1} \sim \Gamma_s\nu$.

It is easy to check that $\delta_{(\frac{1}{k}, \dots, \frac{1}{k})}$ is a trivial fixed point of Γ_s, which corresponds to no information about the root. To show reconstruction, it is enough to prove for $\tilde{X}_0 \sim \mu_0 := \frac{1}{k}[\delta_{(1,0,\dots,0)} + \dots + \delta_{(0,\dots,0,1)}]$ that $\Gamma_s^n\mu_0$ is weakly bounded away from $\delta_{(\frac{1}{k}, \dots, \frac{1}{k})}$. One of the main difficulties for analyzing graph colorings is that the dimension of the recursion grows linearly in k. Luckily, as it will become clear in the proof, it is sufficient to consider only the largest coordinate of $\tilde{X}_n$. All the other entries are w.h.p. negligible as $k \to \infty$. Since we are not aiming at the tightest possible bound, we shall discard this extra information reducing the recursion to $\mathbb{R}$.

Define $\lambda(\vec{x}) = (\lambda^{(0)}, \lambda^{(1)})(\vec{x}) := (\|\vec{x}\|_\infty, \arg\max \vec{x})$ and $\Lambda : \Delta^k \to \Delta^k$ to be

$$\Lambda^{(m)}(\vec{x}) = \begin{cases} \|\vec{x}\|_\infty & m = \arg\max \|\vec{x}\|_\infty \\ \frac{1-\|\vec{x}\|_\infty}{k-1} & \text{otherwise} \end{cases}. \tag{3.2.6}$$

We are mostly interested in the transformation λ and Λ induces on spaces of probability measures. With some abuse of notation, we allow extra randomness to be used to break ties in the $\arg\max$ of λ and Λ independently and uniformly randomly. For example if $X = (\frac{1}{2}, \frac{1}{2}, 0, \dots, 0)$ with probability 1, then $\lambda(X)$ equals $(\frac{1}{2}, 1)$ or $(\frac{1}{2}, 2)$ with probability $\frac{1}{2}$. Let $\Lambda^k = \Lambda(\Delta^k) \subset \Delta^k$ be the "star-shaped" image of Λ, $\lambda(\vec{x})$ gives a bijection between $\Lambda^k \backslash (\frac{1}{k}, \frac{1}{k}, \dots, \frac{1}{k})$ and $(\frac{1}{k}, 1] \times [k]$. Hence there is a bijection between $\mathcal{M}([\frac{1}{k}, 1])$ and $\mathcal{M}_s(\Lambda^k) :=$

$\mathcal{M}_s(\Delta^k) \cap \mathcal{M}(\Lambda^k)$ given by:

$$\lambda^{(0)} : \mathcal{M}_s(\Lambda^k) \to \mathcal{M}([\frac{1}{k}, 1]), \quad \mu \to \lambda^{(0)} \circ \mu = \|\mu\|_\infty;$$
$$\lambda^{-1} : \mathcal{M}([\frac{1}{k}, 1]) \to \mathcal{M}_s(\Lambda^k), \quad \mu \to \lambda^{-1} \circ \left(\mu \otimes \frac{1}{k}(\delta_1 + \cdots + \delta_k) \right).$$

Thus $\Lambda \circ \Gamma_s$ induces a transformation on $\mathcal{M}_s(\Lambda^k)$ and $\lambda^{(0)} \circ \Lambda \circ \Gamma_s \circ \lambda^{-1} = \|\Gamma_s \circ \lambda^{-1}\|_\infty$ induces a transformation on $\mathcal{M}([\frac{1}{k}, 1])$. With another abuse of notation, we will use the same notation for both $\mu \in \mathcal{M}([\frac{1}{k}, 1])$ and its unique correspondence in $\mathcal{M}_s(\Lambda_k)$ and use $\Lambda \circ \Gamma_s$ for both transformations. Also for $\mu, \nu \in \mathcal{M}_s(\Lambda_k)$, we say $\mu \prec \nu$ iff $\mu \prec \nu$ as elements of $\mathcal{M}([\frac{1}{k}, 1])$.

The main technical result of this chapter is the following theorem, which will be proved in Section 3.3.

Theorem 3.2.3. *There exist $\beta^0 < 1, c > 0$ such that for any $k > k_0$, $d \geqslant k(\ln k + \ln \ln k + \beta^0)$, and $T \sim \mathcal{T}_{\mathrm{Pois}(d)}$, one can constructs $\mu_k \in \mathcal{M}([\frac{1}{k}, 1])$ such that $(\Lambda \circ \Gamma_s)\mu_k$ stochastically dominates μ_k by $c/\ln k$.*

Using the fact that $\|\Lambda(\vec{x})\|_\infty = \|\vec{x}\|_\infty$, Theorem 3.2.3 is equivalent to the statement that $\|\Gamma_s \mu_k\|_\infty$ stochastically dominates μ_k by $c/\ln k$. It follows that if at some level we can reconstruct the root with success probability $\|\tilde{X}_n\|_\infty$ for some $\tilde{X}_n \sim \mu_k \in \mathcal{M}_s(\Lambda^k)$, then in the level above we can do strictly better with success probability $\|\tilde{X}_{n+1}\|_\infty \succ \|\tilde{X}_n\|_\infty$. However this does not directly imply reconstruction due to two reasons. First, the proof of Theorem 3.2.3 depends heavily on the low-dimensional structure of $\mu_k \in \mathcal{M}_s(\Lambda^k)$, but in general after one step $\Gamma_s \mu_k$ no longer belongs to $\mathcal{M}_s(\Lambda_k)$. Secondly, due to the non-linearity of $\Lambda \circ \Gamma_s$, it is not clear whether $(\Lambda \circ \Gamma_s)\mu_k \succ \mu_k$ would imply $(\Lambda \circ \Gamma_s)^2 \mu_k \succ (\Lambda \circ \Gamma_s)\mu_k$. We address both problems in next subsection by intentionally manipulating the observed configuration and thus manually maintaining a nontrivial fixed point for the "manipulated recursion".

3.2.2 Manipulating the tree recursions

In this section we provide a reconstruction algorithm such that its estimator of σ_ρ satisfies a modified recursion with the fixed point μ_k defined in Theorem 3.2.3. Let S_k be the symmetric group of degree k. For any $\pi \in \mathsf{S}_k$, $\eta \in \Omega(L_n)$ and $X \in \Delta^k$, define $\pi \circ \eta \in \Omega(L_n)$ to be the configuration specified by $(\pi \circ \eta)_v = \pi(\eta_v)$ and $\pi \circ X \in \Delta_k$ to be the vector with $(\pi \circ X)^{(l)} = X^{(\pi(l))}$. We first illustrate the main idea with an example:

Suppose that two people, Alice and Bob, are trying to reconstruct σ_ρ, the color of the root, from σ_{L_n}. Observing T and $\sigma_{L_n} = \eta \in \Omega(L_n)$, Bob knows that root ρ has color l with probability $f_n(l, \eta; T)$. Then Alice tells Bob that the η he observed was not the actual σ_{L_n}, but the σ_{L_n} after a randomly selected permutation π. Namely, $\eta = \pi \circ \sigma_{L_n}$ where π is sampled from some distribution $\nu \in \mathcal{M}(\mathsf{S}_k)$. Let $F(\eta) := (f_n(\ell, \eta; T))_{l=1}^k \in \Delta^k$ be the original estimator of the root with T omitted for brevity. Bob's estimation of σ_ρ after Alice's permutation becomes

$$F(\eta;\nu) := \Big(\mathbb{P}_{\pi\sim\nu}(\sigma_\rho = l \mid \pi\circ\sigma_{L_n} = \eta)\Big)_{l=1}^{k} = \sum_{\pi\in\mathsf{S}_k}\nu(\pi)F(\pi^{-1}\circ\eta) = \sum_{\pi\in\mathsf{S}_k}\nu(\pi)(\pi\circ F)(\eta).$$

Thus if Alice chooses the distribution ν carefully, she can manipulate Bob's estimation to any vector in the convex hull of $\big\{(\pi\circ F)(\eta) : \pi\in\mathsf{S}_k\big\}$. And that's essentially what we will do in this section. In particular, we consider the following two families of $\nu\in\mathcal{M}(\mathsf{S}_k)$:

1. For each $l\in[k]$, let $\nu_1(l)$ be the uniform distribution on $\mathsf{S}_{[k]\setminus l} := \{\pi\in\mathsf{S}_k : \pi_l = l\}$. For any $\eta\in\Omega(L_n)$ and $m\in[k]$,

$$F^{(m)}(\eta;\nu_1(l)) = \begin{cases} f_n(m,\eta) & m = l \\ \frac{1}{k-1}\sum_{m\neq l} f_n(m,\eta) & m\neq l \end{cases} = \begin{cases} f_n(m,\eta) & m = l \\ \frac{1}{k-1}\left(1 - f_n(m,\eta)\right) & m\neq l \end{cases}. \quad (3.2.7)$$

2. For each $p\in[0,1]$, let $\nu_2(p) := p\nu_{\mathrm{unif}} + (1-p)\delta_{\mathrm{id}}$ where ν_{unif} is the uniform distribution on S_k and δ_{id} is the point mass at the identity permutation id. For any $\eta\in\Omega(L_n)$,

$$F(\eta;\nu_2(p)) = (1-p)F(\eta) + \frac{p}{k!}\sum_{\pi\in\mathsf{S}_k}(\pi\circ F)(\eta) = (1-p)F(\eta) + p\cdot\Big(\frac{1}{k},\dots,\frac{1}{k}\Big). \quad (3.2.8)$$

In the proof, we will use $\nu_1(l)$ to simulate the transformation Λ defined in (3.2.6) and $\nu_2(p)$ to reduce the distribution $(\Lambda\circ\Gamma_s)\mu_k$ to μ_k. For the later purpose, we show the following lemma.

Lemma 3.2.4. *For any $\mu_1,\mu_2\in\mathcal{M}([\frac{1}{k},1])$ such that $\mu_1\succ\mu_2$, there exist function $q : [\frac{1}{k},1]\times[0,1]\to[\frac{1}{k},1]$, such that $q(y,u)\leqslant y$ for all $y\in[\frac{1}{k},1]$,$u\in[0,1]$ and for any independent random variables $Y\sim\mu_1$ and $U\sim\mathrm{Unif}[0,1]$, $q(Y,U)\sim\mu_2$. We say that such function q reduces μ_1 to μ_2.*

Proof. Let G_1, G_2 be the c.d.f. of μ_1,μ_2, and $G_1(x-0)$ be the left limit of G_1 at x. For $y\geqslant\frac{1}{k}$, define

$$q(y,u) := \inf\Big\{x\geqslant\frac{1}{k} : G_2(x)\geqslant G_1(y-0) + u(G_1(y) - G_1(y-0))\Big\}.$$

Note that $\mu_1\succ\mu_2$ implies that $G_2(y)\geqslant G_1(y)$ for all $y\geqslant\frac{1}{k}$. Hence $q(y,u)\in[\frac{1}{k},y]$. Let $y_x = \sup\{y : G_1(y-0)\leqslant G_2(x)\}$. A direct calculation shows that for $x\geqslant\frac{1}{k}$,

$$\begin{aligned}\mathbb{P}(q(Y,U)\leqslant x) &= \mathbb{P}(G_2(x)\geqslant G_1(Y-0) + U(G_1(Y)-G_1(Y-0)))\\ &= G_1(y_x-0) + (G_1(y_x)-G_1(y_x-0))\frac{G_2(x)-G_1(y_x-0)}{G_1(y_x)-G_1(y_x-0)} = G_2(x).\end{aligned}$$

□

Recalling the 1-to-1 correspondence between $\mathcal{M}(\Lambda^k)$ and $\mathcal{M}([\frac{1}{k}, 1])$, we define q_0 to be the function that reduces $\mu_0 = \frac{1}{k}(\delta_{(1,0,\ldots 0)} + \cdots + \delta_{(0,\ldots,0,1)})$ to μ_k and $q_\star$ to be the function that reduces $(\Lambda \circ \Gamma_s)\mu_k$ to μ_k, where the later one exists because $(\Lambda \circ \Gamma_s)\mu_k \succ \mu_k$. We further define for each $\bullet \in \{0, \star\}$ that

$$\tilde{q}_\bullet(y, u) := \frac{ky - q_\bullet(y, u)}{ky - 1} \in [0, 1] \quad \text{such that} \quad (1 - \tilde{q}_\bullet(y, u)) \cdot y + \tilde{q}_\bullet(y, u) \cdot \frac{1}{k} = q_\bullet(y, u). \tag{3.2.9}$$

Let us introduce further notations for the algorithm: Let $\mathsf{U} := (U_v)_{v \in T}$ be an array of independent Unif$[0, 1]$ random variables indexed by the vertices of T and let $\mathsf{U}_v := (U_w)_{w \in T_v}$ be the sub-array indexed over T_v, the subtree rooted at v. For each $v \in T$ and $w \in T_v$, we will encode Alice's action on T_v and Bob's information at w after Alice's actions on T_v as

$$\mathsf{a}_v := (p_v, l_v, \pi_v) \in [0, 1] \times [k] \times \mathsf{S}_k \quad \text{and} \quad \mathsf{b}_{w,v} := (p_{w,v}, \eta_{w,v}) \in [0, 1] \times [k].$$

Let A_v and B_v be arrays of a_w and $\mathsf{b}_{w,v}$ indexed over $w \in T_v$ respectively. Letting L_1^v denote the set of offspring of v, we define $\mathsf{B}_{L_1^v} := (\mathsf{b}_{w,u})_{u \in L_1^v, w \in T_u}$ as the concatenation of $(\mathsf{B}_u)_{u \in L_1^v}$ for each $v \notin L_n$ and define $\mathsf{B}_{L_1^v} := (\sigma_v)$ otherwise. With the meaning of a_v and $\mathsf{b}_{w,v}$ to be given in a moment, we formally define

$$\mathsf{P}_v^\circ := \mathsf{P}_v^\circ(\mathsf{B}_{L_1^v}) = \begin{cases} (\mathbb{P}(\sigma_v = l \mid \sigma_v))_{l=1}^k & v \in L_n. \\ (\mathbb{P}(\sigma_v = l \mid \mathsf{B}_{L_1^v}))_{l=1}^k & v \notin L_n. \end{cases}, \quad \mathsf{P}_v := \mathsf{P}_v(\mathsf{B}_v) = (\mathbb{P}(\sigma_v = l \mid \mathsf{B}_v))_{l=1}^k,$$

as Bob's belief on σ_v before and after Alice's actions on T_v (if he is given $\mathsf{B}_{L_1^v}$ or B_v respectively).

We now define the actions of Alice, namely what $\mathsf{a}_v, \mathsf{b}_v$ means and how she recursively constructs them from the leaves up to the root as a function of T_v, $\sigma_{T_v \cap L_n}$ and U_v:

1. For each leaf vertex $v \in L_n$, $T_v = \{v\}$. Bob's belief before Alice's action is simply

$$\mathsf{P}_v^\circ = (\mathbb{P}(\sigma_v = l \mid \sigma_v))_{l=1}^k = (\mathbf{1}\{\sigma_v = l\})_{l=1}^k.$$

   Alice then sets $l_v = \sigma_v$, $p_v = \tilde{q}_0(1, U_v)$ and $\pi_v = \pi_v^2 \circ \pi_v^1$, where π_v^1 is a sample of $\nu_1(l_v)$ and π_v^2 is an independent sample of $\nu_2(p_v)$. Finally, she permute σ_v by π_v (which has the same effect as using π_v^2) and prepares Bob's share of information as $\mathsf{B}_v = (\mathsf{b}_{v,v})$, where

$$\mathsf{b}_{v,v} = (q_{v,v}, \eta_{v,v}) = (p_v, \pi_v^2(l_v)) = (p_v, \pi_v^2(\sigma_v)).$$

2. Suppose that for each $w \in L_{m+1}$, Alice has recorded her actions on T_w as A_w and prepared the information for Bob as B_w, where A_w is a function of $(T_w, \sigma_{T_w \cap L_n}, \mathsf{U}_w)$ and B_w is a function of A_w. We now describe Alice's actions on T_v, namely how she constructs A_v and B_v for each $v \in L_m$ as a function of $(\mathsf{B}_u)_{u \in L_1^v}$ and U_v.

a) First, for each $u \in L_1^v$, Alice calculates P_u, namely Bob's belief of σ_u given information B_u. Given $(\mathsf{P}_u)_{u \in L_1^v}$, Alice calculates Bob's belief of σ_v before her actions on T_v. Following a similar recursion of (3.2.1),

$$\mathsf{P}_v^\circ = \left(\frac{\prod_{u \in L_1^v}(1 - \mathsf{P}_u^{(l)})}{\sum_{m=1}^k \prod_{u \in L_1^v}(1 - \mathsf{P}_u^{(m)})} \right)_{l=1}^k .$$

b) Let $U_v^i, i = 1, 2, 3$ be three independent $\mathrm{Unif}[0,1]$ random variables constructed from U_v. Let $l_v = l_v(\mathsf{P}_v^\circ, U_v^1)$ be uniformly picked from $\{l : (\mathsf{P}_v^\circ)^{(l)} = \|\mathsf{P}_v^\circ\|_\infty\}$, the set of largest coordinates of P_v°, using the randomness of U_v^1 and let $p_v = \tilde{q}_\star(\|\mathsf{P}_v^\circ\|_\infty, U_v^2)$. Alice then uses the randomness U_v^3 to sample π_v^1 from $\nu_1(l_v)$ and π_v^2 from $\nu_2(p_v)$ independently and sets $\pi_v = \pi_v^2 \circ \pi_v^1$. This gives $\mathsf{a}_v = (p_v, l_v, \pi_v)$ and completes the construction of A_v.

c) Finally, Alice "permutes" Bob's current observation of $T_v \cap L_n$ and all the previous information she prepares for Bob by π_v. This, in the language of A_v and B_v, corresponds to setting $q_{v,v} = p_v$, $\eta_{v,v} = \pi_v^2(l_v)$ and setting for each $w \in T_v \backslash \{v\}$ that $q_{w,v} = p_w$ and

$$\eta_{w,v} = \pi_v(\eta_{w,w_1}) = \pi_{w_0}(\pi_{w_1}(\cdots \pi_{w_{r-1}}(\pi_w^2(l_w)) \cdots) \cdots),$$

where $w_0 = v, w_1 \in L_1^v, \ldots, w_{r-1}, w_r = w$ is the unique path connecting v to w. This completes the definition of $\mathsf{B}_v = (\mathsf{b}_{w,v})_{w \in T_v}$.

3. As a final step, Alice tells Bob the array B_ρ as partial information of her actions, which in particular includes Bob's final observation as $(\eta_{v,\rho})_{v \in L_n}$. We emphasis that B_ρ is the only piece of information given to Bob. All the intermediate B_v's exist only in Alice's deduction and remain unknown to Bob.

The main result of the section is the following theorem.

Theorem 3.2.5. *For any $n \geqslant 1$, let T be a n-level tree sampled from $\mathcal{T}_{\mathrm{Pois}}$ and σ_{L_n} be generated by the coloring model on T. Let U be a T-indexed array of independent* $\mathrm{Unif}[0,1]$ *random variables. If Alice performs her actions as described above, then Bob's final belief of σ_ρ after all Alice's actions, represented as*

$$\mathsf{P}_\rho = \mathsf{P}_\rho(\mathsf{B}_\rho) = (\mathbb{P}(\sigma_\rho = l \mid \mathsf{B}_\rho))_{l=1}^k \in \Delta^k,$$

follows the distribution of μ_k.

Proof. For each permutation $\pi \in \mathsf{S}_k$ and T-indexed array $\mathsf{B} = (\mathsf{b}_v)_{v \in T} \in ([0,1] \times [k])^T$, let $\pi \circ \mathsf{b}_v := (p_v, \pi(\eta_v))$ and $\pi \circ \mathsf{B} := (\pi \circ \mathsf{b}_v)_{v \in T}$. We induct on the number of levels in tree T to prove the claim of Theorem 3.2.5 together with the result that

$$\mathsf{P}_\rho(\pi \circ \mathsf{B}_\rho) = \Big(\mathbb{P}(\sigma_\rho = l \mid \pi \circ \mathsf{B}_\rho)\Big)_{l=1}^k = \pi^{-1} \circ \mathsf{P}_\rho(\mathsf{B}_\rho). \tag{3.2.10}$$

For $n = 0$, $T = \{\rho\}$ is the singleton tree and $\mathsf{P}^\circ_\rho = (\mathbf{1}\{\sigma_\rho = l\})_{l=1}^k$, Bob's belief before Alice's action, follows distribution μ_0. Given $\mathsf{b}_{\rho,\rho} = (p_\rho, \eta_{\rho,\rho})$, Bob's posterior estimation of σ_ρ satisfies

$$\mathbb{P}(\sigma_\rho = \tilde{\pi}^{-1}(\eta_{\rho,\rho}) \mid \mathsf{b}_{\rho,\rho}) = \nu_2(p_\rho)(\tilde{\pi}), \quad \forall \tilde{\pi} \in \mathsf{S}_k.$$

Therefore, applying (3.2.8), Bob's belief of σ_ρ after Alice's action at ρ becomes

$$\mathsf{P}_\rho = \Big(\mathbb{P}(\sigma_\rho = l \mid \pi_\rho(\sigma_\rho) = \eta_{\rho,\rho})\Big)_{l=1}^k = (1-p_\rho)\mathsf{P}^\circ_\rho + p_\rho \cdot \Big(\frac{1}{k}, \dots, \frac{1}{k}\Big).$$

Observe that by definition $p_\rho = \tilde{q}_0(1, U_\rho) = \tilde{q}_0(\|\mathsf{P}^\circ_\rho\|_\infty, U_\rho)$. Lemma 3.2.4 and (3.2.9) then imply that P_ρ follows the distribution of μ_k. It is not hard to check that (3.2.10) also holds.

Suppose we have proved Theorem 3.2.5 and (3.2.10) for trees no greater than $n-1$ levels, we now proceed to trees of n levels. By the induction hypothesis, for each $u \in L_1$, $\mathsf{P}_u = \mathsf{P}_u(\mathsf{B}_u)$, Bob's belief of σ_u after Alice's actions on T_u, follows the distribution μ_k. Following a similar calculation of (3.2.4), we can show that conditioning on $\sigma_\rho = l$ but not T and $\sigma_{T\setminus\{\rho\}}$, $(\mathsf{P}_u)_{u\in L_1}$ has the same joint distribution as $\mathrm{Pois}(d)$ independent samples of $\Pi_l\mu_k$. Therefore

$$\mathsf{P}^\circ_\rho = \left(\frac{\prod_{u\in L_1}(1-\mathsf{P}_u^{(l)})}{\sum_{m=1}^k \prod_{u\in L_1}(1-\mathsf{P}_u^{(m)})}\right)_{l=1}^k \sim \Gamma_s\mu_k.$$

Now we turn to $\mathsf{P}_\rho = \mathsf{P}_\rho(\mathsf{B}_\rho)$. For each $u \in L_1$, let $\mathsf{B}_{\rho,u} := (\mathsf{b}_{w,\rho})_{w\in T_u}$, $\mathsf{B}_{\rho,L_1} := (\mathsf{b}_{w,\rho})_{w\in T_\rho\setminus\{\rho\}}$ be sub-arrays of B_ρ. Using the induction hypothesis on (3.2.10), for each $\pi \in \mathsf{S}_k$ we have

$$\begin{aligned}\mathsf{P}^\circ_\rho(\pi\circ\mathsf{B}_{L_1}) &= \left(\frac{\prod_{u\in L_1}(1-\mathsf{P}_u^{(l)}(\pi\circ\mathsf{B}_u))}{\sum_{m=1}^k \prod_{u\in L_1}(1-\mathsf{P}_u^{(m)}(\pi\circ\mathsf{B}_u))}\right)_{l=1}^k = \left(\frac{\prod_{u\in L_1}(1-\mathsf{P}_u^{(\pi^{-1}(l))}(\mathsf{B}_u))}{\sum_{m=1}^k \prod_{u\in L_1}(1-\mathsf{P}_u^{(m)}(\mathsf{B}_u))}\right)_{l=1}^k \\ &= \pi^{-1}\circ\mathsf{P}^\circ_\rho(\mathsf{B}_{L_1}).\end{aligned}$$

Hence set $\{l : (\mathsf{P}^\circ_\rho(\tilde{\pi}\circ\pi^1_\rho\circ\mathsf{B}_{L_1}))^{(l)} = \|\mathsf{P}^\circ_\rho(\mathsf{B}_{L_1})\|_\infty\}$ has the same size for all $\tilde{\pi} \in \mathsf{S}_k$ and contains l_ρ if $\tilde{\pi} \in \operatorname{supp}\nu_1(l_\rho)$. Furthermore, by the symmetry of σ_{L_n}, each element of $\{\pi\circ\mathsf{B}_\rho\}_{\pi\in\mathsf{S}_k}$ is equally likely to happen. Therefore by (3.2.7), the belief of Bob after the first action of Alice on T_ρ satisfies that

$$\begin{aligned}\mathsf{P}^1_\rho = \mathsf{P}^1_\rho(l_\rho, \pi^1_\rho\circ\mathsf{B}_{L_1}) &:= \Big(\mathbb{P}(\sigma_\rho = l \mid l_\rho, \pi^1_\rho\circ\mathsf{B}_{L_1})\Big)_{l=1}^k \\ &= \sum_{\tilde{\pi}\in\mathsf{S}_k} \nu_1(l_\rho)(\tilde{\pi})\mathsf{P}^\circ_\rho(\tilde{\pi}^{-1}\circ\pi^1_\rho\circ\mathsf{B}_{L_1}) = \Lambda(\mathsf{P}^\circ_\rho),\end{aligned}$$

where the same randomness U^1_ρ is used in breaking ties of Λ. It follows that $\mathsf{P}^1_\rho \sim (\Lambda\circ\Gamma_s)\mu_k$.

Next we note that for any $\tilde{\pi} \in \mathsf{S}_k$, $\|\mathsf{P}^\circ_\rho(\tilde{\pi}\circ\mathsf{B}_{L_1})\|_\infty = \|\mathsf{P}^\circ_\rho(\mathsf{B}_{L_1})\|_\infty$. Therefore p_ρ, as a function of $\|\mathsf{P}^\circ_\rho(\mathsf{B}_{L_1})\|_\infty$ and U^2_ρ, is invariant under permutations of B_{L_1}. Given $\mathsf{b}_{\rho,\rho} = (p_\rho, \eta_{\rho,\rho})$, Bob's posterior estimation of l_ρ and $\pi^1_\rho\circ\mathsf{B}_{L_1}$ satisfies that

$$\mathbb{P}(l_\rho = \tilde{\pi}_2^{-1}(\eta_{\rho,\rho}), \pi_\rho^1 \circ \mathsf{B}_{L_1} = \tilde{\pi}_2^{-1} \circ \mathsf{B}_{\rho,L_1} \mid \mathsf{B}_\rho) = \nu_2(p_\rho)(\tilde{\pi}_2).$$

Applying (3.2.8), we have that

$$\mathsf{P}_\rho(\mathsf{B}_\rho) = \sum_{\tilde{\pi}_2 \in \mathsf{S}_k} \nu_2(p_\rho)(\tilde{\pi}_2)\mathsf{P}_\rho^1(\tilde{\pi}_2^{-1}(\eta_{\rho,\rho}), \mathsf{B}_{\rho,L_1}) = (1-p_\rho)\mathsf{P}_\rho^1(\eta_{\rho,\rho}, \mathsf{B}_{\rho,L_1}) + p_\rho \cdot \left(\frac{1}{k}, \dots, \frac{1}{k}\right).$$

Recall that $p_\rho = \tilde{q}_\star(\|\mathsf{P}_\rho^\circ\|_\infty, U_\rho^2) = \tilde{q}_\star(\|\mathsf{P}_\rho^1\|_\infty, U_\rho^2)$ where $q_\star$ is the function that reduces $(\Lambda \circ \Gamma_s)\mu_k$ to μ_k and $\tilde{q}_\star$ is defined in (3.2.9). Lemma 3.2.4 then implies that P_ρ follows the distribution of μ_k.

Finally we finish the induction hypothesis of (3.2.10). Observe that for $\tilde{\pi} \sim \nu_1(l)$, $\pi \circ \tilde{\pi} \circ \pi^{-1}$ follows the distribution $\nu_1(\pi(l))$. For each $\pi \in \mathsf{S}_k$, we have

$$\begin{aligned}
\mathsf{P}_\rho^1(\pi(l_\rho), \pi(\pi_\rho^1 \circ \mathsf{B}_{L_1})) &= \sum_{\tilde{\pi} \in \mathsf{S}_k} \nu_1(\pi(l_\rho))(\tilde{\pi})\mathsf{P}_\rho^\circ(\tilde{\pi}^{-1} \circ \pi \circ \mathsf{B}_{L_1}) \\
&= \sum_{\tilde{\pi} \in \mathsf{S}_k} \nu_1(l_\rho)(\tilde{\pi})\mathsf{P}_\rho^\circ(\pi \circ \tilde{\pi}^{-1} \circ \pi^{-1} \circ \pi \circ \mathsf{B}_{L_1}) \\
&= \sum_{\tilde{\pi} \in \mathsf{S}_k} \nu_1(l_\rho)(\tilde{\pi})\mathsf{P}_\rho^\circ(\pi \circ \tilde{\pi}^{-1} \circ \mathsf{B}_{L_1}) = \pi^{-1} \circ \mathsf{P}^1(l_\rho, \pi_\rho^1 \circ \mathsf{B}_{L_1}).
\end{aligned}$$

It follows that

$$\mathsf{P}_\rho(\pi \circ \mathsf{B}_\rho) = (1-p_\rho)\mathsf{P}_\rho^1(\pi(\eta_{\rho,\rho}), \pi \circ \mathsf{B}_{\rho,L_1}) + p_\rho \cdot \left(\frac{1}{k}, \dots, \frac{1}{k}\right). = \pi^{-1} \circ \mathsf{P}_\rho(\mathsf{B}_\rho).$$

And that finishes the proof the induction hypothesis. □

Theorem 3.2.3 and Theorem 3.2.5 immediately imply the following result.

Corollary 3.2.6. *For any d, k such that Theorem 3.2.3 holds, there exist independent random array U and measurable function $\mathsf{B}_\rho(T, \sigma_{L_n}, \mathsf{U})$ such that*

$$\liminf_{n\to\infty} \mathbb{E} \sup_{l \in [k]} \left| \mathbb{P}\left(\sigma_\rho = l \mid \mathsf{B}_\rho(T_n, \sigma_{L_n}, \mathsf{U})\right) - \frac{1}{k} \right| > 0.$$

3.2.3 Regular trees

The result of Theorem 3.2.5 and Corollary 3.2.6 can be modified to regular trees by, roughly speaking, truncating $T \sim \mathcal{T}_d$ into a smaller tree: Let $\mathrm{tPois}(d', d)$ be the truncated Poisson distribution defined as the distribution of $D' \cdot \mathbf{1}\{D' \leqslant d\}$ where $D' \sim \mathrm{Pois}(d')$ and let $\mathcal{T}_{\mathrm{tPois}(d'd)}$ be the Galton-Watson tree of offspring distribution $\mathrm{tPois}(d', d)$. There exists a natural coupling between $T_1 \sim \mathcal{T}_{\mathrm{tPois}(d'd)}$, $T_2 \sim \mathcal{T}_{\mathrm{Pois}(d')}$ and $T \sim \mathcal{T}_d$ such that T_1 is a subtree of T_2 and T with probability 1.

Recall that $\mathcal{M}(\Delta^k)$-operator Γ defined in (3.2.3) depends implicitly on the offspring distribution ξ. We differentiate the two operators under $\xi = \mathcal{T}_{\mathrm{Pois}(d')}$ and $\xi = \mathcal{T}_{\mathrm{tPois}(d',d)}$ as Γ^p and Γ^t respectively. Fix $\beta^* \in (\beta^0, 1)$. For any d, k satisfying (3.1.3), let $d' := \lfloor d-(\beta^*-\beta^0)k \rfloor$. For $k \geqslant k_0(\beta^\star, c)$,

$$d_{\mathrm{TV}}(\Lambda \circ \Gamma^p_s \mu_k, \Lambda \circ \Gamma^t_s \mu_k) \leqslant \mathbb{P}(\mathrm{Pois}(d') > d) < c(k \ln k)^{-1}. \tag{3.2.11}$$

Therefore if (d', k) further satisfies Theorem 3.2.3, then $(\Lambda \circ \Gamma^t)_s \mu_k$ stochastically dominates μ_k. Thus we can find function q_t that reduces $(\Lambda \circ \Gamma^t)_s \mu_k$ to μ_k and define $\tilde{q}_t$ similarly.

Let $T \sim \mathcal{T}_d$ be the n-level d-ary tree and $\mathsf{D} := (D_v)_{v \in T}$ be a T-indexed array of independent $\mathrm{tPois}(d', d)$ random variables. We now describe the necessary modification such that $\widetilde{\mathsf{A}}_v$, $\widetilde{\mathsf{B}}_v$, $\widetilde{\mathsf{P}}^\circ_v$, $\widetilde{\mathsf{P}}_v$ can be constructed in a similar fashion as $\mathsf{A}_v, \mathsf{B}_v$, P°_v, P_v. The construction remains the same for each $v \in L_n$. For each $v \notin L_n$, we proceed with the following changes:

1. In step 2(a), instead of considering all $u \in L^v_1$, Alice now only uses the first D_v vertices and discards the rest. Namely, letting $u_1, \ldots, u_d$ be the d offspring of v, she calculates

$$\widetilde{\mathsf{P}}^\circ_v := \left(\frac{\prod_{i=1}^{D_v} (1 - \widetilde{\mathsf{P}}^{(l)}_{u_i})}{\sum_{m=1}^k \prod_{i=1}^{D_v} (1 - \widetilde{\mathsf{P}}^{(m)}_{u_i})} \right)_{l=1}^k,$$

   and sets $\tilde{\mathsf{b}}_{w,v} = (\star, \star)$ for each $w \in T_{u_i}, i > D_v$. She then continues to set $\tilde{\mathsf{a}}_v$ and the rest of $\widetilde{\mathsf{B}}_v$ using $\widetilde{\mathsf{P}}^\circ_v$ and U_v.

2. In step 2(b), instead of setting $p_v = \tilde{q}_\star(\|\mathsf{P}^\circ_v\|_\infty, U^2_v)$, Alice sets $p_v = \tilde{q}_t(\|\widetilde{\mathsf{P}}^\circ_v\|_\infty, U^2_v)$.

In short, Bob now has to reconstruct σ_ρ based only on the information $\widetilde{\mathsf{B}}_\rho$ of a truncated tree of T sampled from $\mathcal{T}_{\mathrm{tPois}(d',d)}$, as the information on the rest of the vertices are erased and set to $(\star, \star)$.

Corollary 3.2.7. *Fix $\beta^\star \in (\beta^0, 1)$. For any d, k such that $(d' := \lfloor d-(\beta^*-\beta^0)k \rfloor, k)$ satisfies Theorem 3.2.3 and (3.2.11), there exist independent random arrays U, D and measurable function $\widetilde{\mathsf{B}}_\rho(\sigma_{L_n}, \mathsf{U}, \mathsf{D})$ such that*

$$\liminf_{n \to \infty} \mathbb{E} \sup_{l \in [k]} \left| \mathbb{P}\left(\sigma_\rho = l \mid \widetilde{\mathsf{B}}_\rho(\sigma_{L_n}, \mathsf{U}, \mathsf{D}) \right) - \frac{1}{k} \right| > 0.$$

Proof. By an essentially parallel argument of Theorem 3.2.5, we can inductively show that $\widetilde{\mathsf{P}}^\circ_v$, as a function of $(T, \sigma_{T_v \cap L_n}, \mathsf{U}_v, \mathsf{D}_v)$, follows the distribution of $\Gamma^t_s \mu_k$ and hence $\widetilde{\mathsf{P}}_v \sim \mu_k$ for each $v \in T$. Corollary 3.2.7 then follows immediately. $\square$

Proof of Theorem 2. Let β^0, c be the constant in Theorem 3.2.3 and β^* be selected in Corollary 3.2.7. For any $k \geqslant k_0$ and d, k satisfying (3.1.3), they also satisfy the conditions of

Theorem 3.2.3 and Corollary 3.2.6. Therefore if the k-coloring model on $T \sim \mathcal{T}_{\mathrm{Pois}(d)}$ is not reconstructible for some d, k in the same region, then we must have

$$\limsup_{n\to\infty} \mathbb{E}_{T\sim\mathcal{T}_{\mathrm{Pois}(d)}}[\mathrm{Var}(\sigma_\rho \mid \mathsf{B}_\rho(T_n, \sigma_{L_n}, \mathsf{D}))] \leqslant \limsup_{n\to\infty} \mathbb{E}_{T\sim\mathcal{T}_{\mathrm{Pois}(d)}}[\mathrm{Var}(\sigma_\rho \mid T_n, \sigma_{L_n})] = 0,$$

where the first step follows from the fact that $\mathsf{B}_\rho = \mathsf{B}_\rho(T_n, \sigma_{L_n}, \mathsf{U})$ is independent of σ_ρ given σ_{L_n}. But that conflicts with the result of Corollary 3.2.6. The same confliction exists with $T \sim \mathcal{T}_d$, $\widetilde{\mathsf{B}}_\rho = \widetilde{\mathsf{B}}_\rho(\sigma_{L_n}, \mathsf{U}, \mathsf{D})$ and Corollary 3.2.7. Therefore both models are reconstructible.
□

3.3 Proof of Theorem 3.2.3

In this section we prove the stochastic dominance result of Theorem 3.2.3. In Section 3.3.1, we first analyse the transformation Γ induced on $\mathcal{M}(\Lambda^k)$ by (3.2.3) and give a parameterized candidate of μ_k. In the remaining sections, we verify that the candidate does indeed satisfy Theorem 3.2.3.

3.3.1 Reformulating the recursion

Recall the notations in the definition of $\Gamma\mu$ in (3.2.3), where $\mu = \Pi_1\mu_s$ for some $\mu_s \in \mathcal{M}_s(\Lambda^k)$. For each $l \in [k], 1 \leqslant i \leqslant B_l$, let $m_{i,l} := m(\vec{X}_{i,l}, l) := \arg\max_{m\in[k]} \vec{X}_{i,l}^{(m-l+1)}$ be the coordinate of $\vec{X}_{n+1}$ that contains the largest entry of $\vec{X}_{i,l}$ and draw $m_{i,l}$ from $[k]$ uniformly at random if $\vec{X}_{i,l} = (\frac{1}{k}, \ldots, \frac{1}{k})$. Since μ is tilted from some symmetric measure μ_s, similar to (3.2.4),

$$\mathbb{P}(m_{i,l} = m \mid \|\vec{X}_{i,l}\|_\infty = x) = \begin{cases} x & m = l \\ \frac{1-x}{k-1} & m \neq l \end{cases}.$$

Let $\mu^=(dx) := x\mu(dx)$ and $\mu^{\neq}(dx) := (1-x)\mu(dx)$. The joint distribution of $(\|\vec{X}_{i,l}\|_\infty, m_{i,l})$ satisfies

$$\mathbb{P}(\|\vec{X}_{i,l}\|_\infty \in dx, m_{i,l} = m) = \begin{cases} \mu^=(dx) & l = m \\ \frac{1}{k-1}\mu^{\neq}(dx) & l \neq m \end{cases}, \quad \forall x \in [0,1],\ m \in [k].$$

For each $m \in [k]$, define

$$C_m^= := \{(i,m) : m_{i,m} = m\}, \quad C_m^{\neq} := \{(i,l) : l \neq m, m_{i,l} = m\} \quad \text{and} \quad C_m := C_m^= \cup C_m^{\neq}.$$

Let $c_m^=$, $c_m^{\neq}$ be the cardinality of $C_m^=$ and $C_m^{\neq}$ respectively and set $p_{\neq} := \mu^{\neq}([\frac{1}{k}, 1]) = 1 - \mu^=([\frac{1}{k}, 1])$ to be the probability of $\{(i,l) \notin C_l^=\}$. Note that no offspring of the root has color 1. Given $d_\rho = \sum_{l=1}^k B_l$, $(c_1^=, c_2^=, \ldots, c_k^=, c_1^{\neq}, c_2^{\neq}, \ldots, c_k^{\neq})$ follows multinomial distribution of sum d_ρ and probability

$$\frac{1}{k-1}\left(0, 1-p_{\neq}, \ldots, 1-p_{\neq}, p_{\neq}, \frac{k-2}{k-1}p_{\neq}, \ldots, \frac{k-2}{k-1}p_{\neq}\right). \tag{3.3.1}$$

We now use the new notations to rewrite (3.2.3). For each $\vec{X}_{i,l} \neq (\frac{1}{k}, \ldots, \frac{1}{k})$, the entries of $\vec{X}_{i,l}$ take only two values: $\|\vec{X}_{i,l}\|_\infty$ and $(1-\|\vec{X}_{i,l}\|_\infty)/(k-1)$. And $\vec{X}_{i,l}^{(m-l+1)} = \|\vec{X}_{i,l}\|_\infty$ if and only if $m = m_{i,l}$. Let $\phi(x) := \ln\big[(1-\frac{1-x}{k-1})/(1-x)\big]$, which is an increasing function mapping $[0,1]$ to $[-\infty,\infty]$. By taking out the common factor of $\prod_{l,i}(1-\frac{1-\|\vec{X}_{i,l}\|_\infty}{k-1})$, we rewrite (3.2.3) as

$$\vec{X}_{n+1}^{(m)} \overset{d.}{=} \frac{\prod_{(i,l)\in C_m}(1-\|\vec{X}_{i,l}\|_\infty)/(1-\frac{1-\|\vec{X}_{i,l}\|_\infty}{k-1})}{\sum_{m'=1}^k \prod_{(i,l)\in C_{m'}}(1-\|\vec{X}_{i,l}\|_\infty)/(1-\frac{1-\|\vec{X}_{i,l}\|_\infty}{k-1})} = \frac{\prod_{(i,l)\in C_m} e^{-\phi(\|\vec{X}_{i,l}\|_\infty)}}{\sum_{m'=1}^k \prod_{(i,l)\in C_{m'}} e^{-\phi(\|\vec{X}_{i,l}\|_\infty)}}. \tag{3.3.2}$$

Note that the exact value of $m_{i,l}$ when $\vec{X}_{i,l} = (\frac{1}{k}, \ldots, \frac{1}{k})$ does not matter since $\phi(\frac{1}{k}) = 0$. We further rewrite (3.3.2) as

$$\vec{X}_{n+1}^{(m)} \overset{d.}{=} \frac{\left(\prod_{i=1}^{c_m^=}\exp(-\phi(Y_{i,m}^=))\prod_{i=1}^{c_m^{\neq}}\exp(-\phi(Y_{i,m}^{\neq}))\right)}{\sum_{l=1}^k\left(\prod_{i=1}^{c_l^=}\exp(-\phi(Y_{i,l}^=))\prod_{i=1}^{c_l^{\neq}}\exp(-\phi(Y_{i,l}^{\neq}))\right)} =: \frac{\exp(-Z_m)}{\sum_{m=1}^k \exp(-Z_m)}. \tag{3.3.3}$$

where $Y_{i,l}^=$ and $Y_{i,l}^{\neq}$ are i.i.d. samples of $\frac{1}{1-p_{\neq}}\mu^=$ and $\frac{1}{p_{\neq}}\mu^{\neq}$ respectively and

$$Z_m := \sum_{i=1}^{c_m^=}\phi(Y_{i,m}^=) + \sum_{i=1}^{c_m^{\neq}}\phi(Y_{i,m}^{\neq}).$$

We conclude our calculation so far in the following claim.

Proposition 3.3.1. *For any d, k, if there exists $\nu_k \in \mathcal{M}([\frac{1}{k}, 1])$ (with its unique correspondence in $\mathcal{M}(\Lambda^k)$) and $c > 0$, such that $\mu_s = \Pi_1^{-1}(\phi^{-1}\circ\nu_k) \in \mathcal{M}_s(\Lambda^k)$ and for the $(Z_m)_{m=1}^k$ defined as above using μ_s,*

$$W := \ln\left[\frac{k-2}{k-1} + \frac{1}{\sum_{m=2}^k \exp(Z_1 - Z_m)}\right] \vee 0 \succ_{c/\ln k} \nu_k, \tag{3.3.4}$$

then μ_s satisfies the requirement of Theorem 3.2.3.

Proof. Maximizing (3.3.3) over $m \in [k]$, we have that

$$\|\vec{X}_{n+1}\|_\infty = \frac{\max\{1, \exp(Z_1 - Z_m), m = 2, \ldots, k\}}{1 + \sum_{m=2}^k \exp(Z_1 - Z_m)} \geqslant \frac{1}{1 + \sum_{m=2}^k \exp(Z_1 - Z_m)} \vee \frac{1}{k}.$$

Composing ϕ to both side yields that $\phi(\|\vec{X}_{n+1}\|_\infty) \succ W$. Theorem 3.2.3 then follows from the fact that $\|\Lambda(\vec{X}_{n+1})\|_\infty = \|\vec{X}_{n+1}\|_\infty$. □

We now propose a parameterized candidate of ν_k: Let $\delta, \kappa \in (0,1)$, $M \gg 0$, $0 < \gamma, \alpha_0, \sigma, \epsilon \ll 1$ be parameters to be determined in the order of $(\delta, \kappa, \alpha_0, M, \sigma, \gamma, \epsilon)$ and write $\alpha = \phi\big(\frac{1}{2} - \alpha_0\big) = \ln 2 - O(\alpha_0) + o_k(1)$. Let $\nu_\star$ be an infinite-volume measure defined as (recalling that $\phi(\frac{1}{k}) = 0$)

$$\nu_\star(dy) := \kappa\delta_0(dy) + (1-\kappa)\delta_\alpha(dy) + \frac{\gamma}{y^2}e^{\delta y}\mathbf{1}\{y > M\}dy, \tag{3.3.5}$$

where δ_x is the Dirac measure at x, and write $\nu_r(dy) := \frac{\gamma}{y^2}e^{\delta y}\mathbf{1}\{y > M\}dy$ for the right tail of $\nu_\star$. We will use $\nu_\star$ as a "scaling limit" of ν_k and show that the assumption of Prop. 3.3.1 is satisfied with

$$\nu_k(dy) := \frac{1}{\ln k}\nu_\star(dy)\mathbf{1}\{0 \leqslant y \leqslant a_k\},$$

for some choice of $(\delta, \kappa, \alpha_0, M, \sigma, \gamma, \epsilon)$ and $k \geqslant k_0 = k_0(\delta, \kappa, \alpha_0, M, \sigma, \gamma, \epsilon)$, where a_k is the constant such that ν_k is a probability measure.

For convenience of notation, we will write $k \geqslant k_0$ where k_0 depends on all six parameters. We will use $1_{\leqslant a_k}$ or $1_{\geqslant c_k}$ to cut (part of) a measure above or below such that the total mass is 1. The exact value of a_k and c_k can be derived implicitly and may vary from line to line. Let $\nu_\star^{=}(dy) := \phi \circ \mu^{=}(dx) = \phi \circ x\mu(dx) = \phi^{-1}(y)\nu_\star(dy)$, where $\phi^{-1}(y) = 1 - (e^y + (k-1)^{-1})^{-1}$ and define $\nu_\star^{\neq}, \nu_r^{=}, \nu_r^{\neq}, \nu_k^{=}, \nu_k^{\neq}$ similarly. We define the tail weights

$$\begin{aligned}
p_r^{\neq} &:= \frac{1}{\gamma}\nu_r^{\neq}([M,\infty)) = \int_M^\infty \frac{e^{\delta y}}{y^2(e^y + \frac{1}{k-1})}dy < \infty \\
p_k^{\neq} &:= \mu_k^{\neq}([1/k, 1)) = \nu_k^{\neq}([0,\infty)) \\
&\leqslant \frac{1}{\ln k}\left[\frac{1}{k}(1-\kappa) + \Big(\frac{1}{2} - \alpha_0\Big)\kappa + \gamma p_r^{\neq}\right] = (1 - o(1))\frac{\gamma p_r^{\neq}}{\ln k}.
\end{aligned}$$

3.3.2 Distribution of Z_m

In this section we bound the distribution of Z_m in terms of $\nu_\star$. Let $D := d/(k-1) = \ln k + \ln\ln k + \beta$. For $T \sim \mathcal{T}_{\mathrm{Pois}(d)}$, (3.3.1) implies that $(c_m^{=}, c_m^{\neq})$'s are independent Poisson random variables with rate $(0, p_k^{\neq}D)$ for $m = 1$ and $((1-p_k^{\neq})D, \frac{k-2}{k-1}p_k^{\neq}D)$ for $m \geqslant 2$. Hence, for $m \geqslant 2$,

$$\begin{aligned}
Z_m &\overset{d.}{=} \left(\mathrm{Pois}((1-p_k^{\neq})D) \otimes \frac{1}{1-p_k^{\neq}}\nu_k^{=}\right) \oplus \left(\mathrm{Pois}\Big(\frac{k-2}{k-1}p_k^{\neq}D\Big) \otimes \frac{1}{p_k^{\neq}}\nu_k^{\neq}\right) \\
&= \mathrm{Pois}\left(\Big(1 - \frac{p_k^{\neq}}{k-1}\Big)D\right) \otimes \frac{\nu_k^{=} + \frac{k-2}{k-1}\nu_k^{\neq}}{(1 - \frac{1}{k-1}p_k^{\neq})} \succ \mathrm{Pois}\left(\Big(1 - \frac{p_k^{\neq}}{k-1}\Big)D\right) \otimes \frac{\nu_k}{(1 - \frac{1}{k-1}p_k^{\neq})}1_{\leqslant a_k},
\end{aligned}$$

where the last line follows from that $(\nu_k^{=} + \frac{k-2}{k-1}\nu_k^{\neq})(dy) \leqslant \nu_k(dy)$. Namely, Z_m stochastically dominates the sum of points in a Poisson point process with intensity $D\nu_k 1_{\leqslant a_k^0}$, where a_k^0 satisfies $\nu_k([0, a_k^0]) = 1 - \frac{1}{k-1}p_k^{\neq}$. We expand the summation according to the three parts of ν_k as in (3.3.5). Firstly, δ_0 does not contribute to the summation. For the second term, we define $S_1 := \mathrm{Pois}(\kappa) \otimes \delta_\alpha$ and note that $\kappa \leqslant \frac{\kappa D}{\ln k}$. Finally for $k \geqslant k_0$, the total intensity coming from the right tail of ν_k satisfies

$$D\nu_k([M, a_k^0]) = D(\nu_k([0, a_k^0]) - \ln^{-1} k) = D - 1 - O(k^{-1} \ln k) \geqslant D - 1 - \gamma.$$

and $(1 - \frac{1}{k-1} p_k^{\neq})^{-1} \nu_k(dy) \leqslant \frac{1+\gamma}{D-1-\gamma} \nu_r(dy)$. Therefore defining

$$S_0 := \mathrm{Pois}\,(D - 1 - \gamma) \otimes \frac{1+\gamma}{D-1-\gamma} \nu_r 1_{\leqslant a_k},$$

it follows that $Z_m \succ S_0 + S_1$. We first show the following bound for S_0.

Lemma 3.3.2. *For any $M > M(\alpha_0) \vee \frac{2}{\delta}$, there exists constant $C_M > 0$ such that*

$$S_0 \succ \frac{e^{\gamma+1-\beta}}{k \ln k} (\delta_0 + (1 + C_M \gamma) \nu_r 1_{\leqslant a_k^1}), \tag{3.3.6}$$

where a_k^1 satisfies $1 + (1 + C_M\gamma)\nu_r([M, a_k^1]) = k \ln k e^{-(\gamma+1-\beta)}$.

Proof. Let $B_0 \sim \mathrm{Pois}\,(D - 1 - \gamma)$ and Y_i be i.i.d. samples of distribution $\frac{1+\gamma}{D-1-\gamma} \nu_r 1_{\leqslant a_k}$. We have

$$\mathbb{P}(S_0 = 0) = \mathbb{P}(B_0 = 0) = e^{-(D-1-\gamma)} \leqslant \frac{1}{k \ln k} e^{1+\gamma-\beta}.$$

Since ν_r is supported on $[M, \infty)$ and is absolutely continuous, for $z \geqslant M$,

$$\begin{aligned}
f_{S_0}(z) = \frac{d}{dz} \mathbb{P}\Big(\sum_{i=1}^{B_0} Y_i \leqslant z\Big) &\leqslant \sum_{n=1}^{\lfloor z/M \rfloor} \mathbb{P}(B_0 = n) \frac{d}{dz} \Big[\int_{\sum y_i \leqslant z} \Big(\frac{1+\gamma}{D-1-\gamma} \Big)^n \nu_r(dy_1) \cdots \nu_r(dy_n) \Big] \\
&\leqslant \frac{e^{1+\gamma-\beta}}{k \ln k} \sum_{n=1}^{\lfloor z/M \rfloor} \frac{1}{n!} \frac{d}{dz} \Big[\int_{y_i \geqslant M, \sum_{i=1}^n y_i \leqslant z} \frac{(1+\gamma)^n \gamma^n}{y_1^2 y_2^2 \cdots y_n^2} e^{\delta(y_1 + \cdots + y_n)} dy_1 \cdots dy_n \Big] \\
&= \frac{e^{1+\gamma-\beta}}{k \ln k} \sum_{n=1}^{\lfloor z/M \rfloor} \frac{(1+\gamma)^n \gamma^n}{n!} e^{\delta z} \int_{y_i \geqslant M, \sum_{i=1}^{n-1} y_i \leqslant z - M} \frac{1}{y_1^2 \cdots y_{n-1}^2 (z - \sum_{i=1}^{n-1} y_i)^2} dy_1 \cdots dy_{n-1}.
\end{aligned}$$

Applying Fact 3.3.3 below for $n \geqslant 2$, we have that for $z \geqslant M$,

$$\begin{aligned}
f_{S_0}(z) dz &\leqslant \frac{e^{1+\gamma-\beta}}{k \ln k} \Big((1+\gamma)\gamma + \sum_{n=2}^{\infty} \frac{((1+\gamma)\gamma C_M)^n}{n!} \Big) \frac{1}{z^2} e^{\delta z} dz \\
&\leqslant \frac{e^{1+\gamma-\beta}}{k \ln k} (1 + C_M' \gamma) \frac{\gamma}{z^2} e^{\delta z} dz = \frac{e^{1+\gamma-\beta}}{k \ln k} (1 + C_M' \gamma) \nu_r(dz).
\end{aligned}$$

The desired result follows from the last equation and the fact that $\mathbb{P}(S_0 \in (0, M)) = 0$. $\square$

Fact 3.3.3. *There exist constant C_M such that for $n \geqslant 2$ and $z \geqslant nM$,*

$$\int_{y_i \geqslant M, \sum_{i=1}^{n-1} y_i \leqslant z - M} \frac{1}{y_1^2 \cdots y_{n-1}^2 (z - \sum_{i=1}^{n-1} y_i)^2} dy_1 \cdots dy_{n-1} \leqslant \frac{C_M^n}{z^2}.$$

The proof of Fact 3.3.3 is postponed to Section 3.4. Next consider the independent sum of $S_0 + S_1$.

Lemma 3.3.4. *For any $M > M(\alpha_0) \vee \frac{2}{\delta}$ and constant C_M specified in Lemma 3.3.2,*

$$Z_m \succ S_0 + S_1 \succ \frac{e^{\gamma+1-\beta}}{k\ln k}\left[\nu_{S_1} + (1+\alpha_0)(1+C_M\gamma)\exp\left(\kappa(e^{-\alpha\delta}-1)\right)\nu_r 1_{\leqslant a_k}\right]. \tag{3.3.7}$$

Proof. Letting $\nu_{S_0}^+ := \nu_r 1_{\leqslant a_k^1}$ where a_k^1 is defined in (3.3.6), we have

$$\nu_{S_0+S_1} = \frac{e^{1+\gamma-\beta}}{k\ln k}(\delta_0 * \nu_{S_1} + (1+C_M\gamma)\nu_{S_0}^+ * \nu_{S_1}) = \frac{e^{1+\gamma-\beta}}{k\ln k}(\nu_{S_1} + (1+C_M\gamma)\nu_{S_0}^+ * \nu_{S_1}). \tag{3.3.8}$$

It is left to verify that $\nu_{S_0+S_1}^+ := \nu_{S_0}^+ * \nu_{S_1} \succ (1+\alpha_0)\exp\left(\kappa(e^{-\alpha\delta}-1)\right)\nu_r 1_{\leqslant a_k}$ where a_k is chosen such that RHS of (3.3.8) has total mass 1. Recall that $S_1 \overset{d.}{=} \alpha \cdot \mathrm{Pois}(\kappa)$. $\nu_{S_0+S_1}^+$ is absolutely continuous and supported on $[M,\infty)$. For $z \geqslant M$ we have

$$f_{S_0+S_1}^+(z) = \sum_{n=0}^{\infty}\frac{\kappa^n e^{-\kappa}}{n!}f_{S_0}^+(z-n\alpha) \leqslant \sum_{n=0}^{\infty}\frac{\kappa^n e^{-\kappa}}{n!}\frac{\gamma e^{\delta(z-n\alpha)}}{(z-n\alpha)^2}\mathbf{1}\{z-n\alpha \geqslant M\}$$

To control the $(z-n\alpha)^{-2}$ term, we first choose for any $\alpha > 0$ a $N = N(\alpha_0)$ such that $\sum_{n=N+1}^{\infty}\frac{1}{n!} \leqslant \frac{1}{2e}\alpha_0$ and then choose $M(\alpha_0)$ such that for $M > M(\alpha_0)$, $n \leqslant N$ and $z \geqslant M$,

$$(1-n\alpha/z)^{-2} \leqslant (1-n\alpha/z)^{-2} \leqslant 1+\alpha_0/2. \tag{3.3.9}$$

Observe that $\frac{\gamma}{z^2}e^{\delta z}$ is monotone increasing for $z \in (\frac{2}{\delta},\infty)$. For all $M > M(\alpha_0) \vee \frac{2}{\delta}$ and $z \geqslant M$,

$$\begin{aligned} f_{S_0+S_1}^+(z)dz &\leqslant \frac{\gamma e^{\delta z}}{z^2}dz\sum_{n=0}^{N}\frac{\kappa^n e^{-\kappa}}{n!}\frac{e^{-n(\alpha\delta)}}{(1-n\alpha/z)^2} + \frac{\gamma e^{\delta z}}{z^2}dz\sum_{n=N+1}^{\infty}\frac{\kappa^n e^{-\kappa}}{n!} \\ &\leqslant (1+\alpha_0)\exp[\kappa(e^{-\alpha\delta}-1)]\nu_r(dz). \end{aligned}$$

The proof finishes by cutting ν_r at the place such that (3.3.8) has the total mass 1. $\square$

Finally, for $m = 1$ and $k \geqslant k_0$ such that $\frac{D}{\ln k} \leqslant (1+\gamma) \vee (1+\alpha_0)$, we have

$$Z_1 \overset{d.}{=} \mathrm{Pois}(p_k^{\neq}D) \otimes \frac{1}{p_k^{\neq}}\nu_k^{\neq} \prec \left(\mathrm{Pois}\left(\frac{1}{2}\kappa\right) \otimes \delta_\alpha\right) \oplus \left(\mathrm{Pois}(\gamma p_r^{\neq}) \otimes \frac{1}{\gamma p_r^{\neq}}\nu_r^{\neq}\right), \tag{3.3.10}$$

where the second term is 0 with probability $\exp(-\gamma p_r^{\neq})$.

3.3.3 Distribution of $\sum_{m=2}^{k}\exp(-Z_m)$

In this section we analysis the distribution of $\sum_{m=2}^{k}\exp(-Z_m) = (k-1)\otimes\exp(-Z_m)$. Let $\psi(x) := e^{-x}$. An easy calculation gives that

$$\psi\circ\nu_\star(dx) = (1-\kappa)\delta_1(dx) + \kappa\delta_{\psi(\alpha)}(dx) + \frac{\gamma}{(\ln x)^2}\frac{1}{x^{1+\delta}}\mathbf{1}\{0 < x < \psi(M)\}dx.$$

Define

$$C_Z := C_Z(\delta,\kappa,\alpha_0,M,\gamma) = (1+\alpha_0)(1+C_M\gamma)\exp\left(\kappa(e^{-\alpha\delta}-1)\right). \tag{3.3.11}$$

Now (3.3.7) can be rewritten as

$$\psi(Z_m) \prec \frac{1}{k\ln k}e^{\gamma+1-\beta}\Big[\psi\circ\nu_{S_1} + C_Z\frac{\gamma}{(\ln x)^2}\frac{1}{x^{1+\delta}}\mathbf{1}\{c_k < x < \psi(M)\}\Big]. \tag{3.3.12}$$

As k grows, the density of $\psi(Z_m)$ diverges quickly around 0 and the probability of seeing $Z_m \geqslant x$ for more than one $m \in [k]$ is $o(\frac{1}{k})$ for any fixed $x > 0$. Hence intuitively,

$$\nu_{k\otimes\psi(Z_m)} \approx \nu_{\max_{m\in[k]}\psi(Z_m)} \approx k\cdot\nu_{\psi(Z_m)}.$$

Lemma 3.3.5. *Fix $\delta = \frac{1}{2}$. For any $M > M(\alpha_0)\vee\frac{2}{\delta}$ such that (3.3.8) holds and $\sigma,\epsilon > 0$, $k \geqslant k_0$,*

$$(k-1)\otimes\psi(Z_m) \prec \frac{e^{\gamma+1-\beta}}{\ln k}\left[(\psi+\sigma)\circ\nu_{S_1} + (1+\epsilon)C_Z\frac{\gamma}{(\ln x)^2}\frac{1}{x^{1+\delta}}1_{x\leqslant\psi(M)}\right]1_{\geqslant c_k} + \frac{\epsilon}{\ln k}\delta_\infty,$$

where $(\psi+\sigma)(x) := \psi(x)+\sigma$ and C_Z is defined in (3.3.11).

Proof. We recall the RHS of (3.3.12) and treat its discrete part and continuous part separately. Let $p_1 := \frac{e^{\gamma+1-\beta}}{k\ln k}$, $\mu_Z^1 := \psi\circ\nu_{S_1}$ and $\mu_Z^2(dx) := \frac{p_1}{1-p_1}\frac{\gamma}{(\ln x)^2}x^{-(1+\delta)}1_{c_k<x\leqslant\psi(M)}dx$. Among the $(k-1)$ i.i.d. samples from the RHS of (3.3.12), $b \sim \text{Binom}(k-1,p_1)$ of them comes from μ_Z^1 and the rest comes from μ_Z^2. Choose $C_b > 0$ such that for any $k \geqslant k_0$, $\mathbb{P}(b \geqslant 2) \leqslant C_b\ln^{-2}k$. It follows that

$$\begin{aligned}(k-1)\otimes\psi(Z_m) &\prec \left(\text{Binom}(k,p_1)\otimes\mu_Z^1\right)\oplus\left(k\otimes\mu_Z^2\right)\\ &\prec \Big[(1-kp_1)\cdot k\otimes\mu_Z^2 + kp_1\cdot\left(\mu_Z^1\oplus(k\otimes\mu_Z^2)\right)\Big]1_{\geqslant c_k} + \frac{C_b}{\ln^2 k}\delta_\infty. \end{aligned}\tag{3.3.13}$$

We will show in Lemma 3.3.8 that for any $\epsilon > 0$ and $k \geqslant k_0$,

$$k\otimes\mu_Z^2 \prec (1+\epsilon)k\cdot\mu_Z^2 1_{\geqslant c_k^0} + \frac{\epsilon}{2\ln k}\delta_\infty. \tag{3.3.14}$$

Therefore for any $\sigma > 0$, there exists $C_\sigma > 0$ such that for $k \geqslant k_0$, $\mathbb{P}(k \otimes \mu_Z^2 \geqslant \sigma) \leqslant C_\sigma \ln^{-1} k$ and

$$\begin{aligned}
\text{RHS of (3.3.13)} &\prec \left[(1-kp_1)\cdot k\otimes \mu_Z^2 + kp_1\cdot(\mu_Z^1 * \delta_\sigma) + \frac{kp_1 C_\sigma}{\ln k}\cdot \delta_\infty\right]1_{\geqslant c_k} + \frac{C_b}{\ln^2 k}\delta_\infty \\
&\prec \left[(1+\epsilon)k(1-kp_1)\cdot \mu_Z^2 1_{\geqslant c_k^0} + kp_1\cdot(\mu_Z^1 * \delta_\sigma)\right]1_{\geqslant c_k} + \frac{\epsilon}{\ln k}\delta_\infty \\
&\prec \frac{e^{\gamma+1-\beta}}{\ln k}\left[(\psi+\sigma)\circ \nu_{S_1} + (1+\epsilon)C_Z\frac{\gamma}{(\ln x)^2}\frac{1}{x^{1+\delta}}\right]1_{\geqslant c_k} + \frac{\epsilon}{\ln k}\delta_\infty.
\end{aligned}$$

where in the last step, we observe that removing the $1_{\geqslant c_k^0}$ after μ_Z^2 will only make the measure inside the square bracket stochastically larger after cutting from below. □

In the remaining of the section, we check that (3.3.14) is true. We will henceforth omit the $O(1)$ factor $(k \ln k)\cdot \frac{p_1}{1-p_1}$ by absorbing it into γ and let

$$U \sim \mu_U := \mu_Z^2 = \frac{1}{k\ln k}\frac{\gamma}{(\ln x)^2}x^{-(1+\delta)}\mathbf{1}\{c_k < x \leqslant \psi(M)\}dx. \tag{3.3.15}$$

Measure μ_U resembles distributions that converge to stable law. However, we can not directly apply the usual proof of convergence for stable laws (cf. Section 3.7 of [Dur10], or the reference there) to $k \otimes U$, since the expression of μ_U also depends on k. With some modification, we show the following result.

Lemma 3.3.6. *For any $\delta, \gamma \in (0,1)$, $M > \frac{2}{\delta}$, let $t_k := \inf\{t : \mu_U([t,\infty)) < 1/k\}$, then $k \otimes (t_k^{-1}U)$ converges weakly to the stable law with index δ and characteristic function*

$$\exp\{-b_\star |t|^\delta (1 + i\mathrm{sgn}(t)\tan(\pi\delta/2))\},$$

where sgn *is the sign function and $b_\star = \delta\int_0^\infty (\cos x - 1)x^{-(1+\delta)}dx = -\cos(\frac{\pi}{2}\delta)\Gamma(1-\delta)$.*

In the proof we use the following calculus result, the proof of which is deferred to Section 3.4.

Fact 3.3.7. *Let t_k be defined as in Lemma 3.3.6, we have*

1. *$t_k = (1+o_k(1))(\frac{\gamma\delta}{\ln k(\ln\ln k)^2})^{1/\delta}$ and therefore*

$$\frac{\gamma}{\delta}t_k^{-\delta}\ln^{-2} t_k = (1+o_k(1))\ln k.$$

2. *For any constant $c > 0$,*

$$\begin{aligned}
\lim_{k\to\infty} k\mathbb{P}(U \geqslant ct_k) &= \lim_{k\to\infty} t_k^{-1}\int_{ct_k}^\infty \frac{1}{k\ln k}\frac{\gamma}{\ln^2 x}\frac{1}{x^{1+\delta}}dx = c^{-\delta}, \\
\lim_{k\to\infty} k\mathbb{E}(t_k^{-1}U 1_{U\leqslant ct_k}) &= \lim_{k\to\infty} t_k^{-1}k\int_0^{ct_k} \frac{1}{k\ln k}\frac{\gamma}{\ln^2 x}\frac{x}{x^{1+\delta}}dx = c^{1-\delta}\frac{\delta}{1-\delta}, \\
\lim_{k\to\infty} k\mathbb{E}(t_k^{-2}U^2 1_{U\leqslant ct_k}) &= \lim_{k\to\infty} t_k^{-2}k\int_0^{ct_k} \frac{1}{k\ln k}\frac{\gamma}{\ln^2 x}\frac{x^2}{x^{1+\delta}}dx = c^{2-\delta}\frac{\delta}{2-\delta}.
\end{aligned}$$

Proof of Lemma 3.3.6. Let $U_i, i = 1, 2, \ldots, k$ be i.i.d. copies of U and let $S_k := \sum_{i=1}^{k} U_i$. Given $\omega \in (0,1)$, let $m_{\leqslant\omega} := \mathbb{E}(U\mathbf{1}\{U \leqslant \omega t_k\})$, $S_k^\omega := \sum_{i=1}^{k} U_i \mathbf{1}\{U_i \geqslant \omega t_k\}$ and $T_k^\omega := \sum_{i=1}^{k} U_i \mathbf{1}\{U_i < \omega t_k\} - k m_{\leqslant\omega}$. We have

$$S_k = S_k^\omega + T_k^\omega + k \cdot m_{\leqslant\omega}.$$

For the first term S_k^ω, let F_k^ω and ψ_k^ω be the c.d.f. and characteristic function of $t_k^{-1} U_i$ conditioned on $\{t_k^{-1} U_i \geqslant \omega\}$. By Fact 3.3.7(2), for any $\omega > 0$ and any $x > \omega$,

$$1 - F_k^\omega(x) = (1 + o_k(1))(x/\omega)^{-\delta} \to (\omega/x)^\delta, \quad \text{as } k \to \infty.$$

Hence for any $t \in \mathbb{R}$, $\psi_k^\omega(t) \to \psi^\omega(t) := \int_\omega^\infty e^{itx} \cdot \delta\omega^\delta x^{-(\delta+1)} dx$. Meanwhile by Fact 3.3.7(2), the distribution of the number of $i \in [k]$ such that $U_i \geqslant \omega t_k$ converges weakly to $\mathrm{Pois}(\omega^{-\delta})$, hence

$$\lim_{k\to\infty} \mathbb{E}\exp(itS_k^\omega/t_k) = \exp[-\omega^{-\delta}(1 - \psi^\omega(t))] = \exp\left(\int_\omega^\infty (e^{itx} - 1)\delta x^{-(\delta+1)} dx\right).$$

For the second term T_k^ω, observe that $\mathbb{E}T_k^\omega = 0$. By Fact 3.3.7,

$$t_k^{-2}\mathbb{E}(T_k^\omega)^2 = t_k^{-2}\operatorname{Var}(T_k^\omega) \leqslant k t_k^{-2}\mathbb{E}U_i^2\mathbf{1}\{U_i < \omega t_k\} \leqslant (1 + o_k(1))\frac{\delta}{2-\delta}\omega^{2-\delta}.$$

For each $t \in \mathbb{R}$, $\exp(itx)$ is a Lipschitz function with Lipschitz constant t. By Jensen's inequality,

$$|\mathbb{E}\exp(it(t_k^{-1}S_k)) - \mathbb{E}\exp(it(t_k^{-1}S_k^\omega))| \leqslant t\left(\mathbb{E}|t_k^{-1}T_k^\omega| + t_k^{-1} k m_{\leqslant\omega}\right) \leqslant O(\omega^{1-\delta/2}).$$

Let $\omega \to 0$. By dominated convergence theorem, we have

$$\lim_{k\to\infty} \mathbb{E}(\exp(itS_k/t_k)) = \exp\left(\int_0^\infty (e^{itx} - 1)\delta x^{-(\delta+1)} dx\right).$$

The rest of the proof follows from complex analysis: Let Γ denote the gamma function (not to be confused with the recursion Γ_s defined before). For $t > 0$, (the case of $t < 0$ is parallel)

$$\begin{aligned}\int_0^\infty (e^{itx} - 1)\delta x^{-(\delta+1)} dx &= t^\delta \int_0^\infty (e^{ix} - 1)\delta x^{-(1+\delta)} dx \\ &= it^\delta \int_0^\infty x^{-\delta} e^{ix} dx = i^\delta t^\delta \int_0^\infty (ix)^{-\delta} e^{ix} d(ix) \\ &= \Gamma(1-\delta) i^\delta t^\delta = \cos(\pi\delta/2)\Gamma(1-\delta) t^\delta (1 + i\tan(\pi\delta/2)),\end{aligned}$$

where the second equality follows by integration by part and the last equality follows by doing contour integral on region $\{re^{i\theta} : \omega \leqslant r \leqslant R, \theta \in [0, \frac{\pi}{2}]\}$ and letting $\omega \to 0, R \to \infty$. $\square$

Let $\widetilde{U}$ denote the limiting stable law specified in Lemma 3.3.6. When $\delta = \frac{1}{2}$, $\widetilde{U}$ follows the Levy distribution with parameter $\frac{\pi}{2}$. Since this is the only value of δ for which we have a closed formula for $f_{\widetilde{U}}$, here and henceforth we will take $\delta = 1/2$. The result, however, should hold for all $\delta \leqslant \frac{1}{2}$ as long as (3.3.16) holds. Plugging in the formula of Levy distribution and comparing with Fact 3.3.7, we have

$$\begin{aligned} \mathbb{P}(\widetilde{U} \leqslant c) = \frac{2}{\sqrt{\pi}} \int_{\frac{1}{2}\sqrt{\pi/c}}^{\infty} e^{-t^2} dt \leqslant \frac{2}{\sqrt{\pi}} \frac{1}{2} \sqrt{\frac{\pi}{c}} e^{-\pi/2c} \leqslant c^{-1/2} e^{-\pi/2c} \\ < c^{-1/2} = (1 + o_k(1)) k \mathbb{P}(U < c t_k). \end{aligned} \tag{3.3.16}$$

Thus we can upper-bound $\mu_{k \otimes U}(dx)$ by $(1 + o_k(1))k \cdot \mu_U(dx)$ for small $x \approx O(t_k)$. In the next lemma, we bound larger values of $k \otimes U$ using the intuition of $k \otimes U \approx \max_{i=1,\ldots,k} U_i$.

Lemma 3.3.8. *Fix $\delta = 1/2$. For any $M \geqslant \frac{2}{\delta}$, $\gamma, \epsilon \in (0,1)$, and $k \geqslant k_0$,*

$$k \otimes \mu_U \prec (1 + \epsilon) k \cdot \mu_U 1_{\geqslant c_k} + \frac{\epsilon}{\ln k} \delta_\infty. \tag{3.3.17}$$

Proof. Let $U_1, \ldots, U_k$ be i.i.d. copies of U and define $U_{(1)} := \max_{i=1,\ldots,k} U_i$, $U_R := \sum_{i=1}^k U_i - U_{(1)}$. Let $c = c(\delta, M, \gamma, \epsilon) > 0$ be some small constant to be determined. We write

$$\mathbb{P}\Big(\sum_{i=1}^{k} U_i \geqslant z\Big) \leqslant \mathbb{P}(U_{(1)} \geqslant (1-c)z) + \int_0^{(1-c)z} f_{U_{(1)}}(x) \mathbb{P}(U_R \geqslant z - x \mid U_{(1)} = x) dx, \tag{3.3.18}$$

where $f_{U_{(1)}}(z) = k f_U(z) (F_U(z))^{k-1} \leqslant k f_U(z)$. Fix $\sigma = \sigma(\delta, M, \gamma, \epsilon) \in (0, \frac{1}{2})$ such that

$$\mathbb{P}(U \geqslant (1-\sigma)\psi(M)) \leqslant \frac{1}{\ln k} \int_{(1-\sigma)\psi(M)}^{\psi(M)} \frac{\gamma}{\ln^2 x} x^{-(1+\delta)} dx \leqslant \frac{\epsilon}{2 \ln k}.$$

We will split the proof into three cases: $x \in [c_k, N t_k]$, $x \in [N t_k, (1-\sigma)\psi(M)]$ and $x \geqslant (1-\sigma)\psi(M)$ where $N = N(\delta, M, \gamma, \epsilon, \sigma, c)$ is a large constant to be determined.

1. $x \in [N t_k, (1-\sigma)\psi(M)]$: To bound the first term of (3.3.18), we observe that f_U is a decreasing function and for $z \leqslant (1-\sigma)\psi(M)$, $(1+\sigma)z \leqslant \psi(M) \in \operatorname{supp} U$. Therefore

$$\frac{\mathbb{P}(U_{(1)} \in [(1-c)z, z])}{\mathbb{P}(U_{(1)} \in [z, (1+\sigma)z])} \leqslant \frac{c z f_U((1-c)z) F^{k-1}(z)}{\sigma z f_U((1+\sigma)z) F^{k-1}(z)} \leqslant \frac{c}{\sigma} \frac{f_U(z/2)}{f_U((1+\sigma)z)} \leqslant C_{\sigma,M} \cdot c,$$

for all $c \leqslant 1/2$ and $z \leqslant (1-\sigma)\psi(M)$. It follows that

$$\mathbb{P}(U_{(1)} \geqslant (1-c)z) \leqslant (1 + C_{\sigma,M} \cdot c) \mathbb{P}(U_{(1)} \geqslant z) \leqslant (1 + C_{\sigma,M} \cdot c) k \mathbb{P}(U \geqslant z). \tag{3.3.19}$$

For the second term of (3.3.18), a similar calculation of Fact 3.3.7 gives that for any $x \leqslant \psi(M)$,

$$
\begin{aligned}
k \ln k \mathbb{E}(U \mid U \leqslant x) &= \frac{k \ln k}{F_U(x)} \int_0^x z f_U(z) dz \leqslant \frac{\gamma}{1-\delta} \frac{1}{F_U(x)} \frac{1}{\ln^2 x} x^{1-\delta}, \\
k \ln k \mathbb{E}(U^2 \mid U \leqslant x) &= \frac{k \ln k}{F_U(x)} \int_0^x z^2 f_U(z) dz \leqslant \frac{\gamma}{2-\delta} \frac{1}{F_U(x)} \frac{1}{\ln^2 x} x^{2-\delta}.
\end{aligned}
$$

Recall the expression of t_k from Fact 3.3.7. For any $c > 0$ we choose $N = N(M, \gamma, \epsilon, c)$ such that for $k \geqslant k_0$ and $x \geqslant N t_k$,

$$
k \mathbb{E}(U \mid U \leqslant x) \leqslant \frac{1 + o_k(1)}{\ln k} \frac{\gamma}{1-\delta} \frac{x (N t_k)^{-\delta}}{\ln^2 t_k} = (1 + o_k(1)) N^{-\delta} \frac{\delta}{1-\delta} x \leqslant \frac{1}{2} c x. \tag{3.3.20}
$$

Given $U_{(1)} = x$, U_R is distributed as the sum of $(k-1)$ i.i.d. copies of U conditioned on $U \leqslant x$. By Chebyshev inequality, for any $z \in [2N t_k, \psi(M)]$ and $x \leqslant (1-c)z$,

$$
\mathbb{P}(U_R \geqslant z - x \mid U_{(1)} = x) \leqslant \frac{k \cdot \mathbb{E}(U^2 \mid U \leqslant x)}{(z - x - k\mathbb{E}(U \mid U \leqslant x))^2} \leqslant \frac{4}{c^2 z^2} \frac{1}{\ln k} \frac{\gamma}{2-\delta} \frac{1}{F_U(x)} \frac{x^{2-\delta}}{\ln^2 x},
$$

where in the second step, we use the fact that $\mathbb{E}(U \mid U \leqslant x)$ is monotone decreasing in x. Plugging the estimation into the RHS of (3.3.18), for $z \leqslant \psi(M)$, we have that

$$
\begin{aligned}
&\int_0^{(1-c)z} k f_U(x) F_U(x)^{k-1} \mathbb{P}(U_R \geqslant z - x \mid U_{(1)} = x) dx \\
&\qquad \leqslant \int_{c_k}^{(1-c)z} \frac{1}{\ln k} \frac{\gamma}{\ln^2 x} x^{-1-\delta} \cdot \frac{4}{c^2 z^2} \frac{1}{\ln k} \frac{\gamma}{2-\delta} \frac{x^{2-\delta}}{\ln^2 x} dx \\
&\qquad \leqslant \frac{C_{c,\gamma}}{\ln^2 k} \frac{1}{z^2} \int_{c_k}^{(1-c)z} \frac{1}{\ln^4 x} x^{1-2\delta} dx \leqslant \frac{C_{c,\gamma,M}}{\ln^2 k \cdot z^{2\delta} \ln^4 z}.
\end{aligned} \tag{3.3.21}
$$

Meanwhile, for $z \leqslant (1-\sigma)\psi(M)$,

$$
k \mathbb{P}(U \geqslant z) \geqslant k \cdot \sigma z f_U((1+\sigma)z) = \frac{C_{\gamma,\sigma,M}}{\ln k \cdot z^\delta \ln^2 z}. \tag{3.3.22}
$$

Comparing (3.3.21) and (3.3.22) and using Fact 3.3.7(1), we have for all $z \geqslant N t_k$ that

$$
\int_0^{(1-c)z} f_{U_{(1)}}(x) \mathbb{P}\left(\sum_{i=1}^n U_i \geqslant z \mid U_{(1)} = x \right) dx \leqslant C_{c,\gamma,\sigma,M} N^{-\delta} k \mathbb{P}(U \geqslant z). \tag{3.3.23}
$$

Combine (3.3.19) and (3.3.23). For each $\epsilon > 0$, we can first pick $c \leqslant \epsilon / 2C_{\sigma,M}$ and then choose $N = N(M, \gamma, \epsilon, \sigma, c)$ such that (3.3.20) is true and for all $k \geqslant k_0$, $z \in [N t_k, (1-\sigma)\psi(M)]$,

$$
\mathbb{P}\left(\sum_{i=1}^k U_i \geqslant z \right) \leqslant k \mathbb{P}(U \geqslant z) \left(1 + C_{\sigma,M} \cdot c + \frac{C_{c,\gamma,\sigma,M}}{N^\delta} \right) \leqslant (1+\epsilon) k \mathbb{P}(U \geqslant z). \tag{3.3.24}
$$

2. $z \in [c_k, Nt_k]$: Lemma 3.3.6 implies that for $z' \in (1, N]$, $\mathbb{P}(\sum_{i=0}^k U_i \geqslant z't_k)$ converges uniformly to $1 \wedge \mathbb{P}(\widetilde{U} > z')$ as $k \to \infty$ and $\widetilde{U}$ follows the Levy distribution with parameter $\frac{\pi}{2}$. Comparing the c_k in the RHS of (3.3.17) to the definition of t_k yields that $c_k \geqslant t_k$ for any $\epsilon > 0$. Therefore for $k > k_0$ and $z \in [c_k, Nt_k]$ with $z' = z/t_k \in (1, N]$,

$$\mathbb{P}\left(\sum_{i=1}^{k} U_i \geqslant z\right) \leqslant (1+\epsilon/2)\mathbb{P}\big(\tilde{U} > z'\big) \leqslant (1+\epsilon)k\mathbb{P}(U \geqslant z't_k), \tag{3.3.25}$$

where the last step uses (3.3.16).

3. Finally using (3.3.24) and recall the definition of σ, we have for all $z \geqslant (1-\sigma)\psi(M)$ that

$$\mathbb{P}\left(\sum_{i=1}^{k} U_i \geqslant z\right) \leqslant \mathbb{P}\left(\sum_{i=1}^{k} U_i \geqslant (1-\sigma)\psi(M)\right) \leqslant (1+\epsilon)k\mathbb{P}(U \geqslant (1-\sigma)\psi(M)) \leqslant \frac{\epsilon}{\ln k}. \tag{3.3.26}$$

Combining (3.3.24), (3.3.25) and (3.3.26) completes the proof. □

3.3.4 Distribution of $\ln(\sum_{m=2}^k \exp(Z_1 - Z_m))$

In this section we bound the distribution of $W_0 := -\ln(\sum_{m=2}^k e^{Z_1 - Z_m})$. First we rewrite (3.3.10) as

$$Z_1 \prec \left(\mathrm{Pois}\left(\frac{1}{2}\kappa\right) \otimes \delta_\alpha\right) \oplus \left(\mathrm{Pois}(\gamma p_r^{\neq}) \otimes \frac{1}{\gamma p_r^{\neq}}\nu_r^{\neq}\right) =: R_0 + R_r =: \widetilde{Z}_1,$$

and let $\tilde{\nu}_{-Z_1}$ be the distribution of $-\widetilde{Z}_1$. Then we define $V := -\ln(\sum_{m=2}^k e^{-Z_m})$. The conclusion of Lemma 3.3.5 can be rewritten as

$$\begin{aligned}\nu_V &\succ \frac{e^{\gamma+1-\beta}}{\ln k}\left[\psi^{-1} \circ (\psi + \sigma) \circ \nu_{S_1} + (1+\epsilon)C_Z\nu_r\right]1_{\leqslant a_k} + \frac{\epsilon}{\ln k}\delta_{-\infty} \\ &=: \tilde{\nu}_V^1 + \tilde{\nu}_V^r + \tilde{\nu}_V^\infty =: \tilde{\nu}_V.\end{aligned} \tag{3.3.27}$$

Let $\widetilde{V}$ be sampled from $\tilde{\nu}_V$. Note that Z_1 is independent of $\sum_{m=2}^k Z_m$. We finally define

$$\widetilde{W}_0 := \widetilde{V} - \widetilde{Z}_1 \prec V - Z_1 = W_0, \tag{3.3.28}$$

Lemma 3.3.9. *Assume that $(\delta, \kappa, \alpha_0, M, \sigma, \gamma, \epsilon)$ satisfies the conditions of Lemma 3.3.4 and 3.3.5.*

1. *If $\delta \leqslant \frac{1}{2}$, then there exists constant $C_{\delta,M} > 0$ such that for each $y \geqslant M$,*

$$(\nu_r * \tilde{\nu}_{-Z_1})(dy) \leqslant (1 + C_{\delta,M}\gamma)\exp(\kappa(e^{\alpha\delta} - 1)/2)\nu_r(dy).$$

2. *There exists constant* $C^\star_{\delta,\alpha,M} > 0$ *such that* $(\nu_r * \tilde{\nu}_{-Z_1})((-\infty, M]) \leqslant \gamma \cdot C^\star_{\delta,\alpha,M}$.
3. *For any fixed* κ, α_0 *and* $y_1, y_2 \geqslant M$,

$$\liminf_{\sigma,\gamma\to 0}(\tilde{\nu}_V^1 * \tilde{\nu}_{-Z_1})([y_1, y_2]) \geqslant \frac{e^{-\kappa/2}}{2\ln k}\mathbb{P}\big(\mathrm{Pois}(\kappa)\cdot\alpha \in (y_1, y_2)\big).$$

Proof. **Part 1:** By definition, for any $y \geqslant M$

$$\nu_r * \tilde{\nu}_{-Z_1}(dy) = \int_{-\infty}^{0} \frac{\gamma e^{\delta(y-z)}}{(y-z)^2}\tilde{\nu}_{-Z_1}(dz) \leqslant \frac{\gamma e^{\delta y}}{y^2}dy \cdot \int_{-\infty}^{0} e^{-\delta z}\tilde{\nu}_{-Z_1}(dz) = \nu_r(dy)\mathbb{E}e^{\delta\tilde{Z}_1}. \quad (3.3.29)$$

Hence it is enough to bound $\mathbb{E}\exp(\delta\widetilde{Z}_1) = \mathbb{E}\exp(\delta R_0)\mathbb{E}\exp(\delta R_r)$. For the first term,

$$\mathbb{E}\exp(\delta R_0) = \mathbb{E}\exp\left(\delta\alpha\cdot\mathrm{Pois}(\kappa/2)\right) = \exp\left(\kappa(e^{\alpha\delta}-1)/2\right). \quad (3.3.30)$$

For the second term, R_r has the same distribution as the sum of points from the Poisson point process with intensity $\nu_r^{\neq}(dy)$. Recall that

$$\nu_r^{\neq}(dy) = \left(e^y + (k-1)^{-1}\right)^{-1}\nu_r(dy) \leqslant \frac{\gamma}{y^2}e^{(\delta-1)y}dy$$

and $p_r^{\neq} = \frac{1}{\gamma}\nu_r^{\neq}([M,\infty))$ depends only on δ, M. By Campbell's Theorem, for any $\delta \leqslant \frac{1}{2}$ and $\gamma \leqslant 1$,

$$\mathbb{E}\exp(\delta R_r) = \exp\left(\int_M^{a_k}(e^{\delta y}-1)\nu_r^{\neq}(dz)\right) \leqslant \exp\left(\gamma\int_M^{\infty} y^{-2}e^{(2\delta-1)y}dy\right) \leqslant 1 + \gamma C_{\delta,M}, \quad (3.3.31)$$

where in the last step we use the inequality $e^x \leqslant 1 + xe^x, \forall x \geqslant 0$. Plugging (3.3.30) and (3.3.31) back into (3.3.29) yields the desired result.

Part 2: Expanding the convolution of $\nu_r * \tilde{\nu}_{-Z_1}$ yields that

$$\nu_r * \tilde{\nu}_{-Z_1}((-\infty, M]) \leqslant \int_0^{\infty}\int_M^{z+M}\frac{\gamma}{y^2}e^{\delta y}\cdot\tilde{\nu}_{Z_1}(dz)dy \leqslant \frac{\gamma e^{\delta M}}{\delta M^2}\int_0^{\infty}e^{\delta z}\tilde{\nu}_{Z_1}(dz) = \frac{\gamma e^{\delta M}}{\delta M^2}\mathbb{E}e^{\delta\tilde{Z}_1}.$$

Applying (3.3.30) and (3.3.31) to $\mathbb{E}e^{\delta\tilde{Z}_1}$ gives one possible $C^\star_{\delta,\alpha,M}$.

Part 3: Noting that $\psi^{-1}(\psi(y)+\sigma) = -\ln(e^{-y}-\sigma)$, we have that

$$\begin{aligned}\tilde{\nu}_V^1 * \tilde{\nu}_{-Z_1}([y_1, y_2]) &\geqslant \frac{e^{\gamma+1-\beta}}{\ln k}\mathbb{P}(\widetilde{Z}_1 = 0)\cdot\mathbb{P}\big(\mathrm{Pois}(\kappa)\cdot\alpha \in [\ln(e^{-y_1}-\sigma), \ln(e^{-y_2}-\sigma)]\big) \\ &\geqslant \frac{1}{\ln k}e^{-\frac{1}{2}\kappa-\gamma p_r^{\neq}}\mathbb{P}\left(\mathrm{Pois}(\kappa)\cdot\alpha \in (\ln(-e^{-y_1}-\sigma), -\ln(e^{-y_2}-\sigma))\right).\end{aligned}$$

$\mathrm{Pois}(\kappa)\cdot\alpha$ takes values from the discrete set $\alpha\mathbb{Z}_+$. For any fixed y_1, y_2, there exists $\sigma = \sigma(\alpha, y_1, y_2)$ such that there is no points of $\alpha\mathbb{Z}_+$ between $-\ln(e^{-y_i}-\sigma)$ and y_i, $i = 1, 2$. Hence in the last line we can substitute the probability by $\mathbb{P}(\mathrm{Pois}(\kappa)\cdot\alpha \in (y_1, y_2))$. Letting $\gamma \to 0$ finishes the proof. $\square$

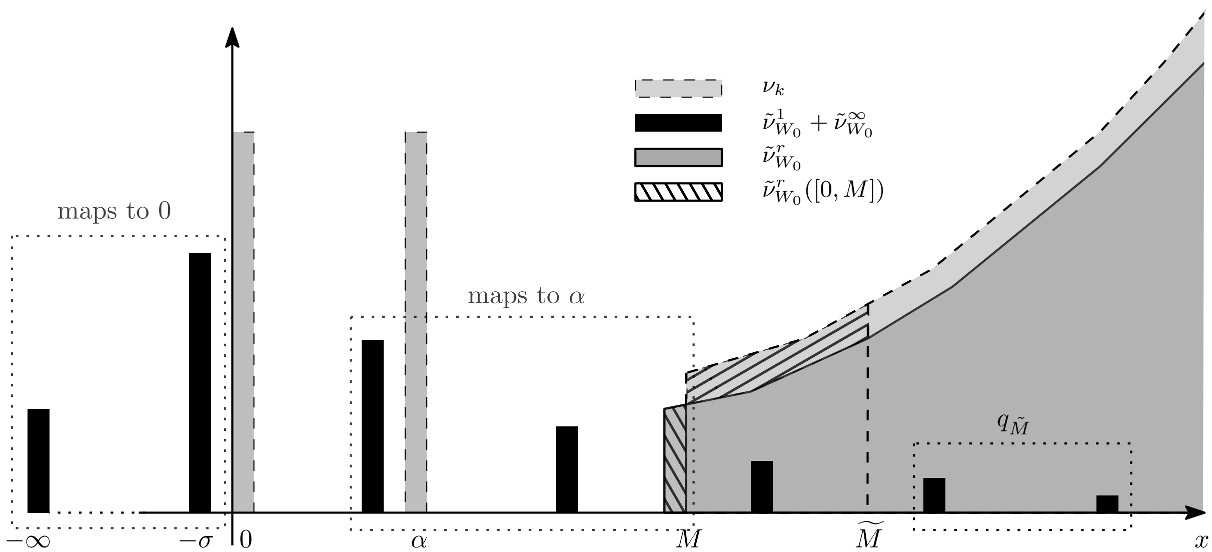


Figure 3.3.1: $\tilde{\nu}_{W_0}$ and ν_k

3.3.5 Final step

Finally we are ready to prove Theorem 3.2.3.

Proof of Theorem 3.2.3. By Proposition 3.3.1, it suffices to show that under certain choice of parameters $(\delta, \kappa, \alpha_0, M, \sigma, \gamma, \epsilon)$, the random variable W defined in (3.3.4) stochastically dominates ν_k by $c/\ln k$ for some fixed $c > 0$. For any $\alpha_0 > 0$ and $\alpha = \phi(\frac{1}{2} - \alpha_0)$, we first choose $\sigma < \sigma_1(\alpha_0)$ such that $\ln(1 + e^{-\sigma}) > \frac{1}{2}(1 - \alpha_0)$. Thus for $k \geqslant k_0$ we can write

$$W > \ln\left(\frac{k-2}{k-1} + \exp(\widetilde{W}_0)\right) \vee 0 \geqslant \begin{cases} \widetilde{W}_0 & \widetilde{W}_0 \geqslant M \\ \alpha & M > \widetilde{W}_0 \geqslant -\sigma \\ 0 & -\sigma > \widetilde{W}_0 \end{cases}. \tag{3.3.32}$$

Comparing the RHS of last equation with the definition of ν_k, it is suffices show that

$$\mathbb{P}(\widetilde{W}_0 < -\sigma) \leqslant \frac{1}{\ln k}(1-\kappa) - \frac{c}{\ln k} \quad \text{and} \tag{3.3.33}$$

$$\mathbb{P}(\widetilde{W}_0 \leqslant x) \leqslant \nu_k([0,x]) - \frac{c}{\ln k} \quad \text{for all } x \geqslant 0 \text{ such that } \nu_k([0,x]) < 1. \tag{3.3.34}$$

Recall the three parts of $\tilde{\nu}_V$ in (3.3.27) and define $\tilde{\nu}^\bullet_{W_0}(dx) := \tilde{\nu}^\bullet_V * \tilde{\nu}_{-Z_1}(dx)$ for $\bullet \in \{1, r, \infty\}$. Figure 3.3.1 gives an illustration of $\tilde{\nu}_{W_0}$ and ν_k, where bars represent the discrete parts, curves represent the continuous parts and the left two dotted boxes corresponds to last two cases of (3.3.32). Fix $\delta = \frac{1}{2}$. To show (3.3.33) is to show that the weight in the first dotted box is strictly smaller than $\nu_k(\{0\}) = \kappa$. We set $\kappa = \frac{1}{2}$ such that

$$\mathbb{P}(\text{Pois}(\kappa/2) = 0) = e^{-1/4} > \frac{3}{4} > \frac{1}{2} = \kappa.$$

Recall the definition of $C_Z = C_Z(\delta, \kappa, \alpha_0, M, \gamma)$ in (3.3.11). By Lemma 3.3.9(2), for each fixed $\delta, \kappa, \alpha_0, M$, we can choose $\epsilon_0, \gamma_0, \beta_0$ such that for all $\epsilon < \epsilon_0, \gamma < \gamma_0$, $\beta_0 < \beta < 1$ and $c_0 = \frac{1}{10}$,

$$\begin{aligned}\mathbb{P}(\widetilde{W}_0 < -\sigma) &\leqslant \frac{e^{\gamma+1-\beta}}{\ln k}\left[\mathbb{P}(\widetilde{Z}_1 \neq 0) + (1+\epsilon)C_Z\gamma \cdot C^*_{\delta,\alpha,M} + \epsilon\right] \\ &\leqslant \frac{e^{\gamma+1-\beta}}{\ln k}\left[1 - e^{-\frac{1}{2}\kappa - \gamma p^r_{\neq}} + 2C_Z C^*_{\delta,\alpha,M}\gamma + \epsilon\right] \\ &= \frac{4/3}{\ln k}\left[\frac{1}{4} + \epsilon + o_\gamma(1)\right] < \frac{2}{5}\frac{1}{\ln k} = \left(\frac{1}{2} - c_0\right)\frac{1}{\ln k}.\end{aligned}$$

The proof of (3.3.34) is roughly done in three parts. We first show that the asymptotically, $\tilde{\nu}^r_{W_0}$ is smaller than ν^r_k by a multiplicative constant factor. Then we show that the underflow of $\tilde{\nu}^r_{W_0}$ below M (the vertical stripped area in Figure 3.3.1) can be compensated by the overflow of $\tilde{\nu}^1_{W_0}$ above M (the $q_{\widetilde{M}}$ box in Figure 3.3.1). Finally we make sure that the compensation is can be absorbed into the gap of $\tilde{\nu}^r_{W_0}$ and ν^r_k (the wide stripped area in Figure 3.3.1).

We first look at sufficiently large values of x. By Lemma 3.3.9(1),

$$\tilde{\nu}^r_{W_0}(dx) \leqslant \frac{e^{\gamma+1-\beta}}{\ln k}(1+\alpha_0)(1+C_{\delta,M}(\gamma+\epsilon))\exp(\kappa(e^{\alpha\delta} + 2e^{-\alpha\delta} - 3)/2)\nu_r(dx), \quad \forall x \geqslant M. \tag{3.3.35}$$

Let α_0 be a small constant such that (note that $\phi(\frac{1}{2}) = \ln 2 - o_k(1)$ and $\exp(\sqrt{2} - 3/2) \approx 0.92 < \frac{12}{13}$)

$$(1+\alpha_0)\exp(\kappa(e^{\alpha\delta} + 2e^{-\alpha\delta} - 3)/2) = (1 + o_{\alpha_0}(1))\exp(\sqrt{2} - 3/2) < \frac{12}{13} < 1,$$

and let $M > M(\alpha_0) \vee \frac{2}{\delta}$ such that Lemma 3.3.4 is satisfied. Recall the definition of constant $C_{\delta,M}$ from the constants in Lemma 3.3.2 and Lemma 3.3.9. Given our choice of $\delta, \kappa, \alpha_0, M$ so far, we can choose $\gamma_1, \epsilon_1, \beta_1$ such that for all $\gamma \leqslant \gamma_1, \epsilon \leqslant \epsilon_1$, $1 - \beta < 1 - \beta_1$ and all $x \geqslant M$,

$$\text{RHS of (3.3.35)} \leqslant \frac{12}{13} \cdot \frac{1}{\ln k}e^{1+\gamma-\beta}\nu_r(dx) \leqslant \frac{14}{15}\frac{1}{\ln k}\nu_r(dx). \tag{3.3.36}$$

Next we consider the values of x near M. We first choose $\widetilde{M} = \widetilde{M}(\delta, \alpha, M) > M \vee 2\alpha$ such that

$$\frac{1}{15}\nu_r([M, \widetilde{M}]) = \frac{1}{15}\int_M^{\widetilde{M}} \frac{\gamma}{y^2}e^{\delta y}dy \geqslant e^{\gamma_1+1-\beta_1}(C^*_{\delta,\alpha,M} + 2e^{\gamma_1} + \epsilon_1)\gamma, \tag{3.3.37}$$

where $C^*_{\delta,\alpha,M}$ is the constant in Lemma 3.3.9(2). Let $q_{\widetilde{M}} := \frac{1}{2}\mathbb{P}(\text{Pois}(\kappa)\cdot\alpha \in (\widetilde{M}, 2\widetilde{M}))$. $q_{\widetilde{M}}$ is strictly positive since $\widetilde{M} > 2\alpha$. By Lemma 3.3.9(3), we can choose σ_2, γ_2 such that for all $\sigma < \sigma_2$, $\gamma < \gamma_2$,

$$\tilde{\nu}^1_{W_0}([\widetilde{M}, 2\widetilde{M}]) = \tilde{\nu}^1_V * \tilde{\nu}_{-Z_1}([\widetilde{M}, 2\widetilde{M}]) \geqslant q_{\widetilde{M}} > 0. \tag{3.3.38}$$

We further choose $\gamma_3, \epsilon_3, \beta_2$ such that for all $\gamma \leqslant \gamma_3$, $\epsilon \leqslant \epsilon_2 < 1$, $1-\beta \leqslant 1-\beta_2$ and some $c_1 \in (0, q_{\tilde{M}})$,

$$e^{\gamma+1-\beta}\left[(1-q_{\tilde{M}}) + \gamma C^*_{\delta,\alpha,M} + \epsilon\right] \leqslant 1 - c_1 < 1. \tag{3.3.39}$$

(3.3.36), (3.3.38) and (3.3.39) together implies for $x \leqslant \widetilde{M}$, (note that $\nu_k([0,M]) = 1/\ln k$)

$$\begin{aligned}
\tilde{\nu}_{W_0}([-\infty, x]) &:= (\tilde{\nu}^1_{W_0} + \tilde{\nu}^r_{W_0} + \tilde{\nu}^\infty_{W_0})([-\infty, x]) \\
&\leqslant \frac{e^{\gamma+1-\beta}}{\ln k}\left((1-q_{\widetilde{M}}) + \gamma C^*_{\delta,\alpha,M} + \epsilon\right) + \frac{14}{15}\frac{1}{\ln k}\nu_r([M, x \vee M]) \\
&\leqslant \frac{1-c_1}{\ln k} + \frac{14}{15}\frac{1}{\ln k}\nu_r([M, x \vee M]) \leqslant \nu_k([0,x]) - \frac{c_1}{\ln k}.
\end{aligned}$$

Finally, for $x \geqslant \widetilde{M}$ such that $\nu_k([0,x]) < 1$, we can choose c_2, β_3 such that for $\gamma = (\gamma_0 \wedge \gamma_1 \wedge \gamma_2 \wedge \gamma_3)$ and $1-\beta < 1-\beta_3$, we have $e^{\gamma+1-\beta} + c_2 < 1 + 2\gamma e^{\gamma}$. Using (3.3.37), we have

$$\begin{aligned}
\tilde{\nu}_{W_0}([-\infty, x]) &\leqslant \frac{e^{\gamma+1-\beta}}{\ln k}\left(1 + \gamma C^*_{\delta,\alpha,M} + \epsilon\right) + \frac{14}{15}\frac{1}{\ln k}\nu_r([M, \widetilde{M}]) + \frac{14}{15}\frac{1}{\ln k}\nu_r((\widetilde{M}, x]) \\
&\leqslant \frac{1}{\ln k} + \frac{1}{\ln k}\left(e^{\gamma+1-\beta}(1 + \gamma C^*_{\delta,\alpha,M} + \epsilon) - 1 - \frac{1}{15}\nu_r([M, \widetilde{M}])\right) + \frac{1}{\ln k}\nu_r([M, x]) \\
&\leqslant \frac{1-c_2}{\ln k} + \frac{1}{\ln k}\nu_r([M, x]) = \nu_k([0,x]) - \frac{c_2}{k \ln k}.
\end{aligned}$$

Combining all pieces together, we have the desired result with $\delta, \kappa, \alpha_0, M, \gamma$ set as specified before, $\sigma = \sigma_1 \wedge \sigma_2$, $\epsilon = \epsilon_0 \wedge \epsilon_1 \wedge \epsilon_2$, and $\beta^0 = \beta_0 \vee \beta_1 \vee \beta_2 \vee \beta_3$, $c = c_0 \wedge c_1 \wedge c_2$. □

3.4 Remaining Calculations

Proof of Fact 3.3.3. First fix $n = 2$ and $t' \geqslant 2M$. For each $x_1 \geqslant M$, either x_1 or $t' - x_1$ is larger than $t'/2$, hence

$$\int_M^{t'-M} \frac{1}{x_1^2(t-x_1)^2} dx_1 \leqslant \frac{2}{(t'/2)^2}\int_M^\infty \frac{1}{x_1^2} dx_1 = \frac{8}{Mt'^2}. \tag{3.4.1}$$

Recursively apply (3.4.1) with $t' = t - \sum_{i=1}^{n-j} x_i$, $j = 2, \ldots, n-1$, we have

$$\begin{aligned}
&\int_{x_i \geqslant M, \sum_{i=1}^{n-1} x_i \leqslant t-M} \frac{1}{x_1^2 \cdots x_{n-1}^2 (t - \sum_{i=1}^{n-1} x_i)^2} dx_1 \cdots dx_{n-1} \\
&= \int_{x_i \geqslant M, \sum_{i=1}^{n-2} x_i \leqslant t-2M} \frac{1}{x_1^2 \cdots x_{n-2}^2}\left(\int_M^{t-\sum_{i=1}^{n-2} x_i - M} \frac{1}{x_{n-1}^2 (t - \sum_{i=1}^{n-1} x_i)^2} dx_{n-1}\right) dx_1 \cdots dx_{n-2} \\
&\leqslant \frac{8}{M}\int_{x_i \geqslant M, \sum_{i=1}^{n-2} x_i \leqslant t-M} \frac{1}{x_1^2 \cdots x_{n-2}^2 (t - \sum_{i=1}^{n-2} x_i)^2} dx_1 \cdots dx_{n-2} \leqslant \cdots \leqslant (\frac{8}{M})^n \frac{1}{t^2}.
\end{aligned}$$

□

Proof of Fact 3.3.7. Let $s_k = (\frac{\gamma\delta}{\ln k(\ln\ln k)^2})^{1/\delta}$, it is easy to check that

$$\frac{\gamma}{\delta} s_k^{-\delta} \ln^{-2} s_k = (1 + o_k(1)) \ln k.$$

For any $\epsilon > 0$, let c be large enough such that $(1-\epsilon)^\delta - 2c^{-\delta} > 1$. It follows that

$$\begin{aligned}
\int_{(1-\epsilon)s_k}^{\infty} k \ln k \cdot \mu_U(dx) &= \int_{(1-\epsilon)s_k}^{\psi(M)} \frac{\gamma}{(\ln x)^2} x^{-(1+\delta)} dx \geqslant \frac{\gamma}{\ln^2 (1-\epsilon)s_k} \int_{(1-\epsilon)s_k}^{cs_k} x^{-(1+\delta)} dx \\
&= \frac{\gamma}{\delta \ln^2 (1-\epsilon)s_k} s_k^{-\delta} ((1-\epsilon)^{-\delta} - c^{-\delta}) > (1 + c^{-\delta} + o_k(1)) \ln k.
\end{aligned}$$

Therefore $t_k > (1-\epsilon)s_k$ for $k \geqslant k_0$. In the other direction, let $s'_k = (c' \ln k)^{-1/\delta}$ for some large constant $c' > 0$, $\ln(s'_k) = (1 + o_k(1)) \frac{1}{\delta} \ln\ln k = (1 + o_k(1)) \ln s_k$, we have

$$\begin{aligned}
\int_{(1+\epsilon)s_k}^{\infty} k \ln k \cdot \mu_U(dx) &= \int_{(1+\epsilon)s_k}^{\psi(M)} \frac{\gamma}{(\ln x)^2} \frac{1}{x^{1+\delta}} dx \\
&\leqslant \frac{\gamma}{\ln^2 \psi(M)} \int_{s'_k}^{\infty} x^{-(1+\delta)} dx + \frac{\gamma}{\ln^2 (s'_k)} \int_{(1+\epsilon)s_k}^{\infty} x^{-(1+\delta)} dx \\
&\leqslant \frac{\gamma}{\delta \ln^2 \psi(M)} c'^{-\delta} \ln k + (1 + o_k(1))(1+\epsilon)^{-\delta} \ln k.
\end{aligned}$$

Let c' be large enough such that $\frac{\gamma}{\delta \ln^2 \psi(M)} c'^{-\delta} + (1+\epsilon)^{-\delta} < 1 - c'^{-1} < 1$, we have for $k \geqslant k_0$ that $t_k < (1+\epsilon)s_k$. This completes the Part 1. Part 2 can be derived similarly. $\square$

Chapter 4

Reconstruction threshold of NAE-SAT problems

4.1 Introduction

In this chapter we show that the reconstruction threshold of the NAE-SAT problem on trees is strictly smaller than the freezing threshold. One immediate difference between k-coloring model and k-NAE-SAT is that the later is described by factor graph. Thus to describe the local weak limit of random d-regular k-factor graphs and random Erdős-Rényi k-factor graph, we define the *k-factor tree* as the tree with vertices on even levels being variables, the vertices on odd levels clauses and each clause having k children (i.e. degree $k+1$).

Since we will be working on factor trees throughout the chapter, up to recursively flipping all labels on some of the subtrees, we can ignore the literals and stay with the easier definition that every clause is adjacent to at least one $\mathtt{0}$ and one $\mathtt{1}$ (which is also known as hyper-graph 2-coloring in literature). The broadcast process on a k-factor tree that generates a uniform NAE-SAT solution can be defined as follows:

1. Choose the root uniformly randomly from $\{\mathtt{0},\mathtt{1}\}$.
2. For each clause, if we have set the value of the parent variable to be $x \in \{\mathtt{0},\mathtt{1}\}$ in previous round, we then choose the value of the rest k variables together according to the uniform distribution on $\{\mathtt{0},\mathtt{1}\}^k \backslash \{x\}^k$.

We will focus on the $(k+1)$-NAE-SAT problem on infinite d-ary k-factor trees $\mathcal{T}_{d,k}$—k-factor trees such that every vertex on even levels has d children. As in the case of Chapter 3, we also consider the Galton Watson tree $\mathcal{T}_{\mathrm{Pois}(d),k}$ where the number of offspring of each variable follows the Poisson distribution with parameter d. The definition of reconstruction and freezing (Definition 3.1.1 and Definition 3.1.2) can be generalized to factor trees in natural way.

The main result of this chapter is the following theorem. (The exact value of k_0 and $\beta^\star$ may be different than the k_0 and $\beta^\star$ in Theorem 2)

Theorem 3. *There exists a constant $\beta^\star \in (1-\ln 2, 1)$ such that for any $k \geqslant k_0$, the $(k+1)$-NAE-SAT problem on both $\mathcal{T}_{d,k}$ and $\mathcal{T}_{\mathrm{Pois}(d),k}$ is reconstructible for*

$$d \geqslant (2^k-1)(\ln k + \ln\ln k + \beta^\star + o_k(1)). \tag{4.1.1}$$

As comparison, we will show

Theorem 4.1.1. *For $(k+1)$-NAE-SAT problem on both $\mathcal{T}_{d,k}$ and $\mathcal{T}_{\mathrm{Pois}(d),k}$, there exist constants d_k^f (depending on the model) such that the root is frozen with high probability if $d > d_k^f$ and unfrozen for $d < d_k^f$. More specifically,*

$$d_k^f = \begin{cases} \inf_{x>0} x \ln^{-1}\left(1 - \frac{(1-e^{-x})^k}{2^k-1}\right) & \mathcal{T}_{d,k} \\ \inf_{x>0} \frac{(2^k-1)x}{(1-e^{-x})^k} & \mathcal{T}_{\mathrm{Pois}(d),k} \end{cases} = (2^k-1)(\ln k + \ln\ln k + 1 + o_k(1)).$$

For a complete picture, it can be shown following a similar argument of [Sly09] that the NAE-SAT problem is non-reconstructible for

$$d \leqslant (2^k-1)(\ln k + \ln\ln k + 1 - \ln 2 - o_k(1)). \tag{4.1.2}$$

We does not go into its proof here due to the limitation of space.

4.1.1 Outline of proof

The proof of Theorem 3 follows a similar argument of Chapter 3. In Section 4.2 we give the distributional recursion of reconstruction probability on trees and give the reconstruction algorithm assuming certain stochastic dominance result. We then prove the stochastic dominance result in Section 4.3. For completeness, we prove the freezing threshold in Section 4.4.

4.2 Reconstruction algorithm

4.2.1 Tree recursions

We begin by specifying the distributional recursion of the posterior probabilities. Let $T = (V, F, E) \sim \mathcal{T}_{k,\xi}$ be sampled from the Galton-Watson k-factor tree with offspring distribution ξ, $T_n = (V_n, F_n, E_n)$ its restriction onto the first $2n$ levels, and L_n the set of variables on level $2n$ (the nth level of variables). Denote the set of solutions on T_n as

$$\Omega_n := \{\sigma \in \{0,1\}^{V_n} : \text{for each } a \in F,\ \exists u, v \in \partial a, \text{ such that } \sigma_u \neq \sigma_v\}$$

and its restriction onto L_n as $\Omega(L_n)$. Define deterministic functions f_n such that for each $\eta \in \Omega(L_n)$

$$f_n(x, \eta; T) := P(\sigma_\rho = x | T, \sigma_{L_n} = \eta), x \in \{0,1\}.$$

Function $f_n(\cdot,\eta;T)$ gives the distribution of the root given boundary condition η and tree structure T. By symmetry, $f_n(\mathtt{1},\eta) = f_n(\mathtt{0}, 1\oplus\eta)$, where $\mathtt{1}\oplus\eta$ is the configuration obtained from η by flipping the value of every variable. Let d_ρ denote the degree of the root and $u_{i,j}, i = 1,\ldots,d_\rho, j = 1,\ldots,k$ be the jth variable in L_1 attached to the i'th clause. Let $T_{i,j}$ denote the subtree rooted at $u_{i,j}$ and let $L^n_{i,j} = L_n \cap T_{i,j}$ be the subset of L_n in $T_{i,j}$. Given vertex $u_{i,j}$, the configuration on $T_{i,j}$ is independent of $T\backslash T_{i,j}$. Standard recursive calculation gives that, for each $\eta \in \Omega(L_n)$ and $\eta_{i,j} = \eta_{L_{i,j}} \in \Omega(L_{n-1})$,

$$f_{n+1}(\mathtt{0},\eta;T) = \frac{\prod_{i=1}^{d_\rho}(1-\prod_{j=1}^{k} f_n(\mathtt{0},\eta_{i,j};T_{i,j}))}{\prod_{i=1}^{d_\rho}(1-\prod_{j=1}^{k} f_n(\mathtt{1},\eta_{i,j};T_{i,j})) + \prod_{i=1}^{d_\rho}(1-\prod_{j=1}^{k} f_n(\mathtt{0},\eta_{i,j};T_{i,j}))}. \tag{4.2.1}$$

For $s \in \{\mathtt{0},\mathtt{1}\}$, let $\Xi^s = \Xi^s(n;\xi)$ denote the joint distribution of (T_n, σ_{L_n}) given $\sigma_\rho = s$ and let (T_n,η^s) be sampled from Ξ^s. Write $\eta^{\mathtt{1}}_{i,j} = \eta^{\mathtt{1}}_{i,j}(n)$ for the restriction of $\eta^{\mathtt{1}}$ onto $L^n_{i,j}$. Let $\Delta := \{(x^{\mathtt{0}},x^{\mathtt{1}}) : x^{\mathtt{0}} + x^{\mathtt{1}} = 1, x^{\mathtt{0}}, x^{\mathtt{1}} \geqslant 0\}$. We consider the posterior distribution $X_{n+1} = (X^s_{n+1})_{s\in\{\mathtt{0},\mathtt{1}\}} := (f_{n+1}(s,\eta^{\mathtt{1}};T_{n+1}))_{s\in\{\mathtt{0},\mathtt{1}\}} \in \Delta$, which is a deterministic function of $\eta^{\mathtt{1}}$. By the conditional independence of Gibbs measure and the symmetry between the two states, we have

$$f_n(s,\eta^{\mathtt{1}}_{i,j};T_{i,j})\mid_{\sigma(u_{i,j})=t} \overset{d.}{=} X_n^{\mathtt{1}\oplus s\oplus t} \overset{d.}{=} \begin{cases} X_n^{\mathtt{0}} & s\neq t \\ 1-X_n^{\mathtt{0}} & s=t \end{cases}, \text{ for all } s,t \in \{\mathtt{0},\mathtt{1}\}. \tag{4.2.2}$$

Further more, $(\eta^{\mathtt{1}}_{i,1},\ldots,\eta^{\mathtt{1}}_{i,k})_{1\leqslant i\leqslant d_\rho}$ are i.i.d. with respect to i and for each i, $(\eta^{\mathtt{1}}_{i,j})_{1\leqslant j\leqslant k}$ are exchangeable with respect to j. And hence are $(X_{i,j})_{1\leqslant i\leqslant d_\rho, 1\leqslant j\leqslant k}$.

To describe the one step recursion of the law of X_n, let $\Gamma^s, s \in \{\mathtt{0},\mathtt{1}\}$ be the following functions that take an indefinite number of variables:

$$\Gamma^s(\vec{b},\vec{x}) := \frac{\Lambda^s}{\Lambda^{\mathtt{0}}+\Lambda^{\mathtt{1}}}(\vec{b},\vec{x}),$$

where $\vec{b} = (b_l)_{0\leqslant l\leqslant k-1} \in \mathbb{Z}^{k-1}_{\geqslant 0}$, $\vec{x} = (x^l_{i,j})_{i,l\geqslant 0, 1\leqslant j\leqslant k}$ such that each $x^l_{i,j} \in \Delta$, and

$$\Lambda^s(\vec{b},\vec{x}) := \prod_{l=0}^{k-1}\prod_{i=1}^{b_l}\left[1-\prod_{j=1}^{l} x^{l,s}_{i,j}\prod_{j=l+1}^{k} x^{l,\mathtt{1}\oplus s}_{i,j}\right].$$

In the formula above, b_l represents the number of clauses adjacent to the root such that l of its variable children have value s, namely $b_l := |\{i : |\{j : \sigma(u_{i,j}) = s\}| = l\}|$. Thus by the property of "not all equal", $b_k = 0$ and we omit it from the definition. Given the degree of the root d_ρ, $(b_0,\ldots,b_{k-1})$ follows multinomial distribution of sum d_ρ and probability $p_l = \binom{k}{l}(2^k-1)^{-1}$.

Let D_ρ be sampled from ξ, $\vec{B} = (B_0,\ldots,B_{k-1})$ be sampled from the conditional distribution, and $\vec{X} = (X^l_{i,j})_{i,l\geqslant 0, 1\leqslant j\leqslant k}$ be i.i.d. samples of X_n, (4.2.1) and (4.2.2) implies that

$$X_{n+1} \overset{d.}{=} \Gamma(\vec{B},\vec{X}) := (\Gamma^{\mathtt{0}}(\vec{B},\vec{X}), \Gamma^{\mathtt{1}}(\vec{B},\vec{X})). \tag{4.2.3}$$

Let $\tilde{X}_n(s) := f_n(s, \tilde{\eta}), s \in \{0, 1\}$ be the posterior probability where $\tilde{\eta}$ is the restriction of an unconditional sample (T, σ) onto L_n. The distributions of X_n and $\tilde{X}_n$ satisfies that for each $x = (x^0, x^1) \in \Delta$,

$$\begin{aligned}\mathbb{P}(X_n \in dx) &= 2\mathbb{P}(\sigma_\rho = 1, \mathbb{P}(\tau_\rho = 0 \mid \tau_{L_n} = \sigma_{L_n}) \in dx^0) \\ &= 2\mathbb{P}(X_n \in dx)\mathbb{P}(\sigma_\rho = 1 \mid \mathbb{P}(\tau_\rho = 0 \mid \tau_{L_n} = \sigma_{L_n}) \in dx^0) \\ &= 2(1 - x^0)\mathbb{P}(\tilde{X}_n^0 \in dx) = 2x^1\mathbb{P}(\tilde{X}_n^0 \in dx). \end{aligned} \tag{4.2.4}$$

Let $\mathcal{M}_s(\Delta) \subset \mathcal{M}(\Delta)$ be the subset of probability measures on $\mathcal{M}(\Delta)$ that are invariant under flip of the two coordinates. As in the definition leading to (3.2.5) in Chapter 3, we again use Γ to denote the transformation it induces on $\mathcal{M}(\Delta)$ and for each $\nu \in \mathcal{M}(\Delta)$, define $(\Pi^s\nu)(dx) := kx^s\nu(dx)$ for all $x \in \Delta$. Following (4.2.1) and (4.2.3), the distributional recursion of $\tilde{X}_n$ can then be written as

$$\tilde{\Gamma}\nu := \frac{1}{2}\Big[(\Gamma \circ \Pi^0)\nu + (\Gamma \circ \Pi^1)\nu\Big], s \in \{0, 1\}. \tag{4.2.5}$$

In particular, if $\tilde{X}_n \sim \nu$, then $X_n \sim \Pi^1\nu$, $X_{n+1} \sim \Gamma \circ \Pi^1\nu$ and $\tilde{X}_n \sim \tilde{\Gamma}\nu$.

Observe that for every $\nu \in \mathcal{M}(\Delta)$, there is a nature correspondence in $\mathcal{M}([\frac{1}{2}, 1])$ by mapping $x = (x^0, x^1)$ to $\max_s x_s$. With some abuse of notations, for any $\mu, \nu \in \mathcal{M}(\Delta)$, we say that ν stochastically dominate ν (by ϵ) if the statement is true with respect to their correspondence in $\mathcal{M}([\frac{1}{2}, 1])$. We prove the following result in Section 4.2.

Theorem 4.2.1. *There exist $\beta^0 < 1, c > 0$ such that for any $k > k_0$, $d \geqslant (2^k - 1)(\ln k + \ln\ln k + \beta^0)$, and $T \sim \mathcal{T}_{\mathrm{Pois}(d),k}$, one can constructs $\mu_k \in \mathcal{M}(\Delta)$ such that when both translated into $\mathcal{M}([\frac{1}{2}, 1])$, $\tilde{\Gamma}\mu_k$ stochastically dominates μ_k by $c/\ln k$.*

From there, repeating the arguments in Section 3.2.2 and Section 3.2.3 with $k = 2$ and modifying to factor trees when necessary, one can show the following two results.

Theorem 4.2.2. *For any d, k such that Theorem 4.2.1 holds, there exist independent random array U and measurable function $\mathsf{B}_\rho(T, \sigma_{L_n}, \mathsf{U})$ such that*

$$\liminf_{n\to\infty} \mathbb{E}\left|\mathbb{P}\left(\sigma_\rho = 0 \mid \mathsf{B}_\rho(T_n, \sigma_{L_n}, \mathsf{U})\right) - \frac{1}{2}\right| > 0.$$

Corollary 4.2.3. *Fix $\beta^\star \in (\beta^0, 1)$. For any d, k such that $(d' := \lfloor d - (\beta^* - \beta^0)2^k \rfloor, k)$ satisfies Theorem 4.2.1 and (3.2.11), there exist independent random arrays U, D and measurable function $\widetilde{\mathsf{B}}_\rho(\sigma_{L_n}, \mathsf{U}, \mathsf{D})$ such that*

$$\liminf_{n\to\infty} \mathbb{E}\left|\mathbb{P}\left(\sigma_\rho = 0 \mid \widetilde{\mathsf{B}}_\rho(\sigma_{L_n}, \mathsf{U}, \mathsf{D})\right) - \frac{1}{2}\right| > 0.$$

Proof of Theorem 3 (Reconstruction). The reconstruction part of Theorem 3 follows from Theorem 4.2.1, Theorem 4.2.2 and Corollary 4.2.3. □

4.3 Proof of Theorem 4.2.1

In this section we prove Theorem 4.2.1. We first rewrite the transformation Γ on $\mathcal{M}(\Delta)$ defined in (4.2.3) in a way easier for analyze and a give a parameterized candidate of μ_k. We then verify Theorem 4.2.1 using the candidate in the remaining sections.

4.3.1 Reformulating the recursion

To analyze (4.2.3), it is easier to work the symmetrized log-version of X_n^0. Define for each $x = (x^0, x^1) \in \Delta$ that

$$\phi(x) = \ln(x^1/x^0), \quad \phi^{-1}(y) = (1/(1+e^y), e^y/(1+e^y)).$$

$\phi(x)$ is a function mapping Δ to $\bar{\mathbb{R}} = [-\infty, \infty]$. Recall that $\phi \circ \mu$ is the distribution of $\phi(X)$ where X is sampled from μ. Let $\mathcal{M}_s(\bar{\mathbb{R}})$ denote the space of probability distributions on $\bar{\mathbb{R}}$ that are symmetric about 0. We can rewrite (4.2.3) as

$$\begin{aligned}\phi \circ \Gamma^0(\vec{B}, \vec{X}) &= \ln\left(\frac{\Gamma^1(\vec{B}, \vec{X})}{\Gamma^0(\vec{B}, \vec{X})}\right) = \ln\left(\frac{\Lambda^1(\vec{B}, \vec{X})}{\Lambda^0(\vec{B}, \vec{X})}\right) \\ &\overset{d.}{=} \sum_{l=0}^{k-1}\sum_{i=1}^{B_l}\left[\ln\left(1 - \prod_{j=1}^{l} X_{i,j}^{l,1} \prod_{j=l+1}^{k} X_{i,j}^{l,0}\right) - \ln\left(1 - \prod_{j=1}^{l} X_{i,j}^{l,0} \prod_{j=l+1}^{k} X_{i,j}^{l,1}\right)\right], \quad (4.3.1)\end{aligned}$$

We now split the construction of $\phi \circ \Gamma^0(\vec{B}, \vec{X})$ into steps.

1. For each $\nu \in \mathcal{M}_s(\bar{\mathbb{R}})$, let $\nu^1 := \phi \circ \Pi^1 \circ \phi^{-1}$. By (4.2.4), if $\phi^{-1}(\nu)$ is the distribution of $\tilde{X}_n^0$, then $\phi^{-1}(\nu^1)$ is the distribution of X_n^0. A straightforward calculation gives that
$$\frac{d\nu^1}{d\nu}(y) = 2[\phi^{-1}(y)]^1 = \frac{2e^y}{1+e^y}.$$

2. Observe that on the RHS of (4.3.1), the summand for each fixed l is i.i.d. with respect to index i. For each $l = 0, \ldots, k-1$, Define
$$Y_l = (Y_l^0, Y_l^1) := \left(-\ln\left(1 - \prod_{j=1}^{l} X_j^{l,0} \prod_{j=l+1}^{k} X_j^{l,1}\right), -\ln\left(1 - \prod_{j=1}^{l} X_j^{l,1} \prod_{j=l+1}^{k} X_j^{l,0}\right)\right), \quad (4.3.2)$$
where $\{X_j^l\}$'s are i.i.d. samples of $\phi^{-1} \circ \nu^1$. Vector Y_l evaluates the contribution from a clause with l children being `1` to the posterior distribution.

3. For each $l = 0, \ldots, k-1$, let $B_l \sim \mathrm{Pois}\left(\binom{k}{l}D\right)$ and $(Y_{i,l}^0, Y_{i,l}^1)$ be i.i.d. copies of (Y_l^0, Y_l^1). Define
$$(Z_l^0, Z_l^1) := \left(\sum_{i=1}^{B_l} Y_{i,l}^0, \sum_{i=1}^{B_l} Y_{i,l}^1\right) \quad (4.3.3)$$
to be the total contribution of clauses with l children equaling to `1`.

4. Finally we define $W := \sum_{l=0}^{k-1}(Z_l^0 - Z_l^1)$.

Claim 4.3.1. If for some measure $\nu_k \in \mathcal{M}_s(\overline{\mathbb{R}})$, the random variable W constructed following the steps above satisfies that

$$\nu_k([-t,t]) \geqslant \min\{1, \nu_W((-\infty,t]) + c/k\ln k\}, \quad \text{for all } t \geqslant 0,$$

then $\mu_k = \phi^{-1} \circ \nu_k$ satisfies the condition of Theorem 4.2.1.

Proof. This is just a rewriting of (4.2.5) and (4.3.1). □

We now propose a parameterized candidate of ν_k: Let $\delta, M \gg 0, 0 < \gamma, \sigma, \epsilon \ll 1$ be parameters to be determined in the order of $(\delta, M, \sigma, \gamma, \epsilon)$. Let $\nu_\star$ be an infinite-volume measure defined as (recalling that $\phi(\frac{1}{k}) = 0$)

$$\nu_\star(dx) := \delta_0(dx) + \frac{\gamma}{x^2}e^{\delta|x|}\mathbf{1}\{|x| > M\}dx, \tag{4.3.4}$$

where δ_x is the Dirac measure at x, and write $\nu_r(dx) := \frac{\gamma}{x^2}e^{\delta x}\mathbf{1}\{x > M\}dx$ for the right tail of $\nu_\star$. We will use $\nu_\star$ as a "scaling limit" of ν_k and show that the assumption of Claim 4.3.1 is satisfied with

$$\nu_k(dx) := \frac{1}{k\ln k}\nu_\star(dx)\mathbf{1}\{0 \leqslant x \leqslant a_k\},$$

for some choice of $(\delta, M, \gamma, \epsilon)$ and $k \geqslant k_0 = k_0(\delta, M, \gamma, \epsilon)$, where a_k is the constant such that ν_k is a probability measure.

Let $X, X_i \sim \phi \circ \nu_k^1$ through out the section. The idea is to view the recursion (4.3.1) as sum of points from some Poisson point process where the main contribution comes from Z_0^0 while Z_1^0 and Z_{k-1}^1 add a symmetric noise of $O(1)$ order. All other terms and the dependence between Z_l^1 and Z_l^0 are negligible. To taken into account of the "approximation error" between ν_k and $\nu_\star$, we will also introduce extra error terms α and ϵ in later sections. As it will be clear in the proof, we will decide these parameters in the order of $\delta, \alpha, M, \gamma, \epsilon, k$.

Recall the notations from the beginning of Section 3.2 and further define $B^{\otimes}a$ to be the product of a i.i.d. of B. We will use $1_{\leqslant a_k}$ or $1_{\geqslant c_k}$ to truncate (part of) a measure above or below such that the total mass is 1. The specific value of a_k and c_k may be different from line to line. We assume $M > 2/\delta$ so that $x^{-2}e^{\delta|x|}$ is an increasing function in $|x|$. Let

$$\nu_c(dx) = \frac{\gamma}{x^2}e^{\delta|x|}1_{M \leqslant |x|}dx, \quad \nu_r(x) = \frac{\gamma}{x^2}e^{\delta x}1_{x \geqslant M}$$

denote the continuous part of ν and its right tail. Define ν_c^1, ν_r^1 similarly. As x goes to $-\infty$, $\nu^1(dx) \approx 2\gamma x^{-2}e^{-(1-\delta)x}dx$ is integrable, hence we denote the normalized weight of left tail as

$$p_0 = p_0(\delta, M) = \nu^1((-\infty, -M])/2\gamma$$

Finally define two more functions, both of which are monotone decreasing:

$$\psi_1 : \overline{\mathbb{R}} \to [0,\infty], \ln((1-x)/x) \mapsto -\ln(1-x), y \mapsto \ln(1+e^{-y}) \tag{4.3.5}$$

$$\psi_2 : [0,\infty] \to [0,\infty], y \mapsto -\ln(1-e^{-y}), -\ln(1-x) \mapsto -\ln(x). \tag{4.3.6}$$

4.3.2 The distribution of Y_0^0

Recall that X, X_i's are i.i.d. samples of $\phi \circ \nu$. Let $U := -\ln(1-X) \sim \psi_1 \circ \nu_k^1$. By definition $Y_0^0 \overset{d.}{=} -\ln(1-(1-X)^{\otimes k})$, hence $\psi_2^{-1}(Y_0^0) \overset{d.}{=} k \otimes U$. A direct calculation gives that

$$k \ln k \cdot \nu_U(dx) = \delta_{\ln 2}(dx) + \frac{2\gamma(e^x-1)^{-1-\delta \mathrm{sgn}(\psi_1^{-1}(x))}}{\ln^2(e^x-1)} dx \cdot 1_{M \leqslant |\psi_1^{-1}(x)| \leqslant a_k} \tag{4.3.7}$$
$$\approx \begin{cases} \frac{2\gamma}{\ln^2 x} x^{-(1+\delta)} dx & x \to 0 \\ \frac{2\gamma}{x^2} e^{(\delta-1)x} dx & x \to \infty \end{cases}.$$

When k is large, ν_U is highly concentrated around 0 and the density as $x \searrow 0$ is asymptotically equal to the density in 3.3.15. Thus following a similar argument of Lemma 3.3.6, we can show the following result.

Lemma 4.3.2. *For any $\delta, \gamma \in (0,1)$, $M > \frac{2}{\delta}$, let $t_k := \inf\{t : \nu_U([t,\infty)) < 1/k\}$, then $k \otimes (t_k^{-1} U)$ converges weakly to stable law with index δ and characteristic function*

$$\exp(-b|t|^\delta (1 + i \mathrm{sgn}(t) \tan(\frac{\pi}{2}\delta)),$$

where $b = \delta \int_0^\infty (\cos x - 1) x^{-(1+\delta)} dx = -\cos(\frac{\pi}{2}\delta)\Gamma(1-\delta)$.

The proof to Lemma 4.3.2 follows exactly the same as the proof of Lemma 3.3.6 and we omit the proof from here.

Let $\tilde{U}$ the denote limiting stable law specified in Lemma 4.3.2. For $\delta = \frac{1}{2}$, $\tilde{U}$ follows Levy distribution with parameter $c = \frac{\pi}{2}$. We henceforth set $\delta = 1/2$. In particular, this implies

$$\mathbb{P}(\tilde{U} \leqslant c) = \frac{2}{\sqrt{\pi}} \int_{\frac{1}{2}\sqrt{\pi/c}}^\infty e^{-t^2} dt \leqslant \frac{2}{\sqrt{\pi}} \frac{1}{2} \sqrt{\frac{\pi}{c}} e^{-\pi/2c} \leqslant c^{-1/2} e^{-\pi/2c}$$
$$\overset{c>1}{<} c^{-1/2} = (1 + o_k(1)) k \mathbb{P}(U < c t_k).$$

This implies that $\nu_{k \otimes U}(dx)$ is upper-bounded by $(1+o_k(1))k \cdot \nu_U(dx)$ for small $x \approx O(t_k)$. On the other end of the spectrum, for any fix $x > 0$, $k \ln k \cdot \nu_U([x,\infty)) \to \psi_1(\nu)([x,\infty))$. Hence among k i.i.d. copies of U, the probability of seeing more than one of them larger than x is $O(\frac{1}{\ln^2 k})$, and we would expect

$$\nu_{k \otimes U}(dx) \approx \nu_{\min U_i, i=1,\ldots,k}(dx) \approx k \nu_U(dx) \approx \frac{1}{\ln k}(\psi_1 \circ \nu^1)(dx).$$

And indeed, that's the motivation of the following lemma.

Lemma 4.3.3. *Fix $\delta = 1/2$, for any $M \geqslant \frac{2}{\delta}$, $\gamma, \epsilon, \alpha \in (0,1)$, and $k \geqslant k_0$*

$$\psi_2^{-1}(Y_0^0) \overset{d.}{=} k \otimes U \prec \frac{1}{\ln k}(1+\epsilon)\Big[\psi_1 \circ \nu_r^1 + \delta_{\psi_1(-\alpha)} + 2\gamma p_0 \delta_\infty\Big] 1_{\geqslant c_k}$$

Proof. For each $\alpha \in (0,1)$, let M' be the chosen such that

$$\psi_1(M') + \psi_1(0) = \psi_1(M') + \ln 2 < \psi_1(\alpha). \tag{4.3.8}$$

Recall the definition of ν_U in 4.3.7. The probability that a sample of U is bigger than $\psi_1(M')$ is $O(1/k \ln k)$. Therefore out of k i.i.d. samples of U, the probability that more than one sample come is larger than $\psi_1(M')$ is $o(1/\ln k)$. Namely,

$$k \otimes (U\mathbf{1}\{U \geqslant \psi_1(M')\}) \prec \Big(1 - \frac{w_k}{\ln k}\Big)\delta_0 + \frac{1}{\ln k}[\psi_1 \circ \nu_r^1 1_{\geqslant \psi_1(M')} + \delta_{\psi_1(0)} + (2\gamma p_0 + \epsilon)\delta_\infty],$$

where w_k is chosen such that the RHS has weight 1.

For the rest of the mass, a similar argument of Lemma 3.3.8 shows that the contribution from samples smaller than $\psi_1(M')$ can be bounded as

$$k \otimes (U\mathbf{1}\{U \leqslant \psi_1(M')\}) \prec \frac{1}{\ln k}(1+\epsilon)[\psi_1 \circ \nu_r^1 1_{\leqslant \psi_1(M')} + \epsilon \delta_\infty].$$

Taking convolution of the last two equations and using (4.3.8) finishes the proof. □

Now we recover Y_0 from $\psi_2^{-1}(Y_0)$. Observe that ψ_2 is a decreasing function with

$$\psi_2 \circ \psi_1(y) = \ln(1 + e^y) \geqslant y, \quad \psi_2 \circ \psi_1(-\alpha) = \ln 2 - O(\alpha), \quad \psi_2(\infty) = 0.$$

By passing a different $\alpha', \epsilon' \in (0,1)$ into Lemma 4.3.3 when necessary, we have for $k \geqslant k_0$,

$$Y_0^0 \succ \frac{1}{\ln k}(1+\epsilon)[\psi_2 \circ \psi_1 \circ \nu_r^1 + \delta_{\ln 2 - \alpha} + 2\gamma p_0 \delta_0]1_{\leqslant a_k} =: \tilde{Y}_0^0. \tag{4.3.9}$$

4.3.3 The distribution of $Y_l^0, l \geqslant 1$

In this section, we bound the effect of Y_l^0 for $l = 1, \dots, k-1$. By definition

$$Y_l^0 \overset{d.}{=} Y_{k-l}^1 \overset{d.}{=} -\ln(1 - (1-X)^{\otimes(k-l)} X^{\otimes l}) \prec -\ln(1 - X^{\otimes l}) =: \tilde{Y}_l,$$

where the second last step corresponds to ignoring the contribution of variables with the same value as the parent variable. In particular setting $l = 1$, we have

$$\tilde{Y}_1 \overset{d.}{=} -\ln(1 - X) = \frac{1}{k \ln k}\psi_1 \circ \nu^1 1_{\geqslant c_k}.$$

The next lemma gives a crude bound of $\tilde{Y}_l$ using $\tilde{Y}_1$ and shows that it is negligible for $l \geqslant 2$.

Lemma 4.3.4. *There exist constant $C = C(\delta, \gamma, M)$ such that for all $l = 1, \dots, k$*

$$\psi_2(\tilde{Y}_l) = l \otimes (-\ln X) \succ \frac{C^{l-1}}{(k \ln k)^l}\psi_2 \circ \psi_1 \circ \nu^1 1_{\leqslant a_k},$$

and hence $\tilde{Y}_l \prec \frac{1}{k \ln k}(\frac{C}{k \ln k})^{l-1}\psi_1 \circ \nu^1 1_{\geqslant c_k}$.

Proof. For each l, we truncate $\psi_2 \circ \psi_1 \circ \nu^1$ at different places and apply different scalings. For convenience of notation, write $\tilde{\nu}_V := \psi_2 \circ \psi_1 \circ \nu^1$ (resp. $\tilde{f}_V$) for the untruncated measure (resp. density) and let $V := -\ln X \sim \frac{1}{k \ln k} \tilde{\nu}_V 1_{\leqslant a_k}$. Recall that $\psi_2 \circ \psi_1(x) = x + \ln(1 + e^{-x})$. A direct calculation gives

$$\begin{aligned} \tilde{\nu}_V(dx) &= \delta_{\ln 2}(dx) + \frac{2\gamma(e^x - 1)^\delta}{\ln^2(e^x - 1)} 1_{\psi_2 \circ \psi_1(M) \leqslant x} dx + \frac{2\gamma(e^x - 1)^{-\delta}}{\ln^2(e^x - 1)} 1_{0 < x \leqslant \psi_2 \circ \psi_1(-M)} dx \\ &\leqslant \delta_{\ln 2}(dx) + \frac{2\gamma}{x^2} e^{\delta x} 1_{\psi_2 \circ \psi_1(M) \leqslant x} dx + \frac{2\gamma}{x^\delta \ln^2 x} 1_{0 < x \leqslant \psi_2 \circ \psi_2(-M)} dx. \end{aligned} \tag{4.3.10}$$

We will prove by induction that for any $t \geqslant 0$,

$$\mathbb{P}(\psi_2(Y_l^0) \leqslant t) = \nu_{l \otimes V}([0, t]) \leqslant \frac{1}{k \ln k} \left(\frac{C}{k \ln k} \right)^{l-1} \tilde{\nu}_V([0, t]), \tag{4.3.11}$$

which together with proper truncation will imply the desired result.

The base case of $l = 1$ is trivial. Let C be a constant to be determined. Suppose (4.3.11) is true for $l - 1$ and all $t > 0$. Let $\tilde{M} = \psi_2 \circ \psi_1(M)$ and $C_1 = \tilde{\nu}_V([0, 2\tilde{M}])$. For $t \leqslant 2\tilde{M}$,

$$\begin{aligned} \mathbb{P}(l \otimes V \leqslant t) &= \int_0^t \mathbb{P}((l-1) \otimes V \leqslant t - s) \nu_V(ds) \leqslant \mathbb{P}((l-1) \otimes V \leqslant t) \int_0^{2\tilde{M}} \nu_V(ds) \\ &= \frac{C_1}{k \ln k} \mathbb{P}((l-1) \otimes V \leqslant t) \leqslant \frac{C_1 \cdot C^{l-2}}{(k \ln k)^l} \tilde{\nu}([0, t]). \end{aligned}$$

For $t \geqslant 2\tilde{M}$, by induction hypothesis,

$$\mathbb{P}(l \otimes V \leqslant t) = \int_0^t \mathbb{P}((l-1) \otimes V \leqslant t - s) \nu_V(ds) \leqslant \frac{C^{l-2}}{(k \ln k)^l} \int_0^t \tilde{\nu}_V([0, t - s]) \tilde{\nu}_V(ds).$$

Again, we have

$$\int_0^{\tilde{M}} \tilde{\nu}_V([0, t - s]) \tilde{\nu}_V(ds) \leqslant C_1 \nu_V([0, t])$$

By integrating by part, it is enough to show that

$$\int_{\tilde{M}}^t \tilde{\nu}_V([0, t - s]) \tilde{\nu}_V(ds) = \int_0^{t - \tilde{M}} \tilde{\nu}_V([\tilde{M}, t - s]) \tilde{\nu}_V(ds) \leqslant C \, \tilde{\nu}_V([0, t)).$$

Since $f_V(t)$ is well-defined for $\tilde{t} \geqslant \tilde{M}$, differentiating the last two steps of the last equation with respect to t yields

$$\int_0^{t - \tilde{M}} \tilde{f}_V(t - s) \tilde{\nu}_V(ds) \leqslant C \tilde{f}_V(t).$$

To prove the last inequality. Recall the upperbound (4.3.10) and note that $\tilde{\nu}_V((0,\psi_2\circ\psi_1(-M)]) = \nu^1((-\infty,-M]) = 2\gamma p_0$. For $t \geqslant 2\tilde{M}$,

$$\begin{aligned}
&\int_0^t \tilde{f}_V(t-s)\tilde{\nu}_V(ds) = 2\int_0^{t/2} \tilde{f}_V(t-s)\tilde{\nu}_V(ds) \\
&= 2\tilde{f}_V(t-\ln 2) + 2\int_{\tilde{M}}^{t/2} \tilde{f}_V(t-s)\tilde{f}_V(s)ds + 2\int_0^{\psi_2\circ\psi_1(-M)} \tilde{f}_V(t-s)\tilde{f}_V(s)ds \\
&\leqslant (2+4\gamma p_0)\frac{2\gamma e^{\delta t}}{t^2} + 2\int_{\tilde{M}}^{(t-\tilde{M})} \frac{8\gamma^2 e^{\delta t}}{(t-s)^2 s^2}ds \leqslant (2+4\gamma p_0 + 4\gamma C_{\tilde{M}})\frac{2\gamma e^{\delta t}}{t^2},
\end{aligned}$$

where in the last step constant $C_{\tilde{M}}$ is finite because $\int_{\tilde{M}}^{\infty} 1/t^2 dt < \infty$. □

In particular, for $Y_0^1 \overset{d.}{=} Y_k^0 \overset{d.}{=} \psi_2(k\otimes V)$, a crude application of Lemma (4.3.4) yields

$$\mathbb{P}(Y_0^1 > k^{-3}) \leqslant k^{-3}. \tag{4.3.12}$$

We will use this to give a bound for $Y_0^0 - Y_0^1$ regardless of their dependency.

Corollary 4.3.5. *For fixed $\delta = \frac{1}{2}, M, \gamma > 0$ and any $\alpha, \epsilon > 0$, for $k > k(\delta,\alpha,M,\gamma,\epsilon)$, $Y_0^0 - Y_0^1$ satisfies that*

$$Y_0^0 - Y_0^1 \succ \frac{1}{\ln k}[(1+\epsilon)(\nu_r^1 + 2\gamma p_0\delta_0) + \delta_{\ln 2-\alpha})]1_{\leqslant a_k} + \frac{1}{k^3}\delta_{-\infty} =: \tilde{Y}_0. \tag{4.3.13}$$

Proof. By (4.3.9) and (4.3.12), for all $y > 0$ and $k \geqslant k_0$,

$$\begin{aligned}
\mathbb{P}(Y_0^0 - Y_0^1 \leqslant y) &\leqslant \mathbb{P}(Y_0^0 \leqslant y+\alpha) + \mathbb{P}(Y_0^1 > \alpha) \\
&\leqslant (1+\epsilon)\mathbb{P}(\tilde{Y}_0^0 \leqslant y) + \frac{1}{\ln k}1_{y\in[\ln 2-2\alpha,\ln 2-\alpha)} + \frac{1}{k^3}.
\end{aligned}$$

Hence passing a different ϵ, α onto Lemma 4.3.3 if necessary, it is enough to show that $\mathbb{P}(Y_0^0 - Y_0^1 < 0) < \frac{1}{k^3}$, which is equivalent to $\mathbb{P}(k\otimes\ln((1-X)/X) < 0) < \frac{1}{k^3}$. Recall by definition $\ln(1-X)/X = \phi(X) \sim \nu_k^1$, there exist constant $C_{\gamma,M}$ such that

$$\mathbb{E}e^{-\frac{1}{2}\ln((1-X)/X)} \leqslant \frac{1}{k\ln k}\int_{-\infty}^{\infty} e^{-\frac{1}{2}s}\nu^1(ds) = \frac{1}{k\ln k}C_{\gamma,M}.$$

Applying Markov inequality yields

$$P\big(k\otimes\ln\frac{1-X}{X} < 0\big) < \mathbb{E}e^{-\frac{1}{2}k\otimes\ln((1-X)/X)} < \left(\frac{C_{\gamma,M}}{k\ln k}\right)^k < \frac{1}{k^3}.$$

□

4.3.4 The distribution of $Z_0^0 - Z_0^1$

Let $D := d/(2^k - 1) = \ln k + \ln\ln k + \beta$. Recall from definitions (4.3.3) and (4.3.13) that

$$Z_0^0 - Z_0^1 \overset{d.}{=} \mathrm{Pois}(D) \otimes (Y_0^0 - Y_0^1) \succ \mathrm{Pois}(D) \otimes \tilde{Y}_0,$$

where $\tilde{Y}_0$ is a mixture of Dirac measure $\delta_{\ln 2-\alpha}, \delta_0, \delta_{-\infty}$ and a continuous part $(1+\epsilon)\nu_r^1 1_{\leqslant a_k}$ with mass $\frac{1}{\ln k}, \frac{(1+\epsilon)2\gamma p_0}{\ln k}$, $\frac{1}{k^3}$ and $1 - \frac{(1+\epsilon)2\gamma p_0+1}{\ln k}$. Define $p_- := (1+\epsilon)2\gamma p_0 + 1$ and

$$S_1 := \mathrm{Pois}(1) \otimes \delta_{\ln 2-\alpha},\ S_0 := \mathrm{Pois}\left(\left(1 - \frac{p_-}{\ln k}\right) D\right) \otimes \frac{(1+\epsilon)}{1 - \frac{p_-}{\ln k}} \nu_r^1 1_{\leqslant a_k},\ S_\infty := \mathrm{Pois}(k^{-2}) \otimes \delta_{-\infty}$$

By Poisson thinning and the fact that $\ln k \leqslant D \leqslant k$, S_1, S_0 and S_∞ give lower-bounds to the contribution of $\tilde{Y}_0$ samples supported on $\delta_{\ln 2-\alpha}$, ν_r^1 and $\delta_{-\infty}$ and

$$\mathrm{Pois}(D) \otimes \tilde{Y}_0 \succ S_1 + S_0 + S_{-\infty}. \tag{4.3.14}$$

In particular, $S_{-\infty}$ take two values 0 and $-\infty$ with

$$\mathbb{P}(S_{-\infty} \neq 0) = O(k^{-2}). \tag{4.3.15}$$

The next two lemmas follows from a similar argument to Lemma 3.3.2 and Lemma 3.3.4, the proofs of which are omitted to avoid redundancy. Note that the key term $e^{(2e^{-\alpha})^{-\delta}-1}$ in Lemma 3.3.4 comes from shifting ν_r by Pois(1) number of $(\ln 2 - \alpha)$'s.

Lemma 4.3.6. *There exists constant C_M such that for any parameter $(\delta, \alpha, M, \gamma, \epsilon)$ and $k \geqslant k_0$ satisfying the condition of Corollary 4.3.5 holds, we have*

$$S_0 \succ \frac{1}{k \ln k} e^{\gamma + p_- - \beta}[\delta_0 + (1 + C_M(\gamma+\epsilon))2\nu_r 1_{\leqslant a_k}]. \tag{4.3.16}$$

Lemma 4.3.7. *For any $\alpha > 0$, there exist constant $M(\alpha)$ such that for all $M > M(\alpha) \vee 4$ and $(\delta, \alpha, M, \gamma, \epsilon)$ satisfying Lemma 4.3.6, we have*

$$S_0 + S_1 \succ \frac{e^{p_- + \gamma - \beta}}{k \ln k}[\nu_{S_1} + (1+\alpha)(1 + C_M(\gamma+\epsilon))e^{(2e^{-\alpha})^{-\delta}-1}(2\nu_r)1_{\leqslant a_k}]. \tag{4.3.17}$$

Corollary 4.3.5, (4.3.14) and (4.3.17) together complete the picture of $Z_0^0 - Z_0^1$.

Corollary 4.3.8. *Fix $\delta = \frac{1}{2}$, for any $\alpha, \gamma, \epsilon \in (0, 1)$, and all $M > M(\alpha) \vee 4$, there exist constant C_M such that for large enough k,*

$$Z_0^0 - Z_0^r \succ \frac{e^{p_- + \gamma - \beta}}{k \ln k}(\nu_{S_1} + \nu_{S_0+S_1}^1) + \frac{1}{k^2}\delta_{-\infty} \tag{4.3.18}$$

where $\nu_{S_0+S_1}^r = (1+\alpha)(1 + C_M(\gamma+\epsilon))e^{(2e^{-\alpha})^{-\delta}-1}(2\nu_r)1_{\leqslant a_k}$ is the continuous part of $S_0 + S_1$.

4.3.5 The effect of $R = \sum_{l=1}^{k-1}(Z_l^0 - Z_l^1)$

Recall from definition that $W = (Z_0^0 - Z_0^1) + \sum_{l=1}^{k-1}(Z_l^0 - Z_l^1)$. Define $R := \sum_{l=1}^{k-1}(Z_l^0 - Z_l^1)$. R acts as a symmetric perturbation on the leading term $(Z_0^0 - Z_0^1)$. From Corollary 4.3.8,

$$W \succ (S_0 + S_1) + R + S_{-\infty} \succ \frac{e^{p_- + \gamma - \beta}}{k \ln k}(\nu_{S_1} * \nu_R + \nu^1_{S_0+S_1} * \nu_R) + \frac{1}{k^2}\delta_{-\infty}. \tag{4.3.19}$$

Let $\tilde{\nu}_W^0 := \nu_{S_1} * \nu_R$, $\tilde{\nu}_W^r := \nu^r_{S_0+S_1} * \nu_R$ where $\nu^r_{S_1+S_0}$ is defined in Corollary 4.3.8.

Lemma 4.3.9. *For any $\delta \in (0, \frac{1}{2}]$, $M > M_\star(\delta)$, $(\delta, \alpha, M\gamma, \epsilon)$ satisfying the conditions of Corollary 4.3.8 and Lemma 4.3.4, and $k > k_0$,*

1. *There exists some constant $C_{\delta,M}$ such that for $x \geqslant M$,*
$$\tilde{\nu}_W^r(dt) \leqslant (1 + C_{\delta,M}\gamma)\exp(2^\delta + 2^{-\delta} - 2)\nu^r_{S_0+S_1}(dt).$$
2. *There is constant $C^\star_{\delta,\alpha,M}$ such that $\tilde{\nu}_W^r((-\infty, M]) \leqslant \gamma \cdot C^\star_{\delta,\alpha,M}$.*
3. *For every integer $m \geqslant 1$ and $\tilde{M} = (m + 1/2) \cdot (\ln 2 - \alpha)$, we have*
$$\tilde{\nu}_W^0([\tilde{M}, \infty)) \geqslant \nu_{S_1}([\tilde{M}, 2\tilde{M})) = \mathbb{P}(\mathrm{Pois}(1) \in [m+1, 2m+1]).$$

The $M_\star(\delta)$ in the proof comes from the following calculus fact, the proof of which is postponed,which will be proved in Secion 4.5.

Fact 4.3.10. *There exist $M_\star(\delta)$ such that for $M > M_\star(\delta)$ and $t > t - s > M$*

$$\frac{1}{(t-s)^2}e^{-\delta s} + \frac{1}{(t+s)^2}e^{\delta s} \leqslant \frac{1}{t^2}(e^{-\delta s} + e^{\delta s}). \tag{4.3.20}$$

Proof of Lemma 4.3.9. **Part 1:** Let f_r denote the density of ν_r. Since ν_R is symmetric about 0, using Fact 4.3.10 we have

$$\begin{aligned}
(2\nu_r) * \nu_R(dt) &\leqslant \int_{-\infty}^{t-M} 2f_r(t-s)d(t-s)\nu_R(ds) \leqslant \int_{-\infty}^{t-M} \frac{2\gamma e^{\delta(t-s)}}{(t-s)^2}\nu_R(ds)dt \\
&\leqslant 2\gamma e^{\delta t}\left(\int_0^{t-M}\left(\frac{1}{(t-s)^2}e^{-\delta s} + \frac{1}{(t+s)^2}e^{\delta s}\right)\nu_R(ds) + \int_{t-M}^{\infty}\frac{1}{(t+s)^2}e^{\delta s}\nu_R(ds)\right) \\
&\leqslant \frac{2\gamma e^{\delta t}}{t^2}dt \cdot \int_{-\infty}^{\infty} e^{-\delta s}\nu_R(ds) = \nu^1(dt)\mathbb{E}e^{-\delta R}
\end{aligned}$$

It is enough to show that $\mathbb{E}e^{-\delta R} \leqslant (1+O(\gamma))\exp(2^\delta + 2^{-\delta} - 2)$ for large k. Since $\{(Z_l^1, Z_l^0)\}_{\ell=1}^k$ are independent random variables with respect to l, by Campbell theorem,

$$\begin{aligned}
\mathbb{E}e^{-\delta R} &= \mathbb{E}e^{-\delta\sum_{l=1}^{k-1}(Z_l^0 - Z_l^1)} = \prod_{l=1}^{k-1}\mathbb{E}e^{-\delta(Z_l^0 - Z_l^1)} \\
&= \prod_{l=1}^{k-1}\mathbb{E}e^{-\delta\left[\mathrm{Pois}\left(\binom{k}{l}D\right)\otimes\left(Y_l^0 - Y_l^1\right)\right]} = \exp\left(\sum_{l=1}^{k-1}\binom{k}{l}D \cdot \mathbb{E}(e^{\delta(Y_l^1 - Y_l^0)} - 1)\right).
\end{aligned}$$

For arbitrary $a, b > 0$, we have $e^{a-b} - 1 \leqslant e^a(e^{-b} - 1) + e^a - 1 \leqslant (e^{-b} - 1) + (e^a - 1)$. Applying this inequality to $\delta Y_l^1, \delta Y_l^0$ and exchanging the order of summation, the last equation satisfies

$$\begin{aligned}\mathbb{E}e^{-\delta R} &\leqslant \exp\left(\sum_{l=1}^{k-1}\binom{k}{l}D[\mathbb{E}(e^{-\delta Y_l^0} - 1) + \mathbb{E}(e^{\delta Y_l^1} - 1)]\right) \\ &= \exp\left(\sum_{l=1}^{k-1}\binom{k}{l}D[\mathbb{E}(e^{-\delta Y_l^0} - 1) + \mathbb{E}(e^{\delta Y_{k-l}^1} - 1)]\right). \end{aligned} \tag{4.3.21}$$

Note that by definition $Y_l^1 \overset{d}{=} Y_{k-l}^0$. Since $e^{-\delta s} + e^{\delta s} - 2$ is increasing in s for $s > 0$, by properties of stochastic dominance and Lemma 4.3.4, we have

$$\begin{aligned}&\mathbb{E}(e^{-\delta Y_l^0} - 1) + \mathbb{E}(e^{\delta Y_{k-l}^1} - 1) = \mathbb{E}(e^{-\delta Y_l^0} + e^{\delta Y_l^0} - 2) \leqslant \mathbb{E}(e^{-\delta \tilde{Y}_l^0} + e^{\delta \tilde{Y}_l^0} - 2) \\ &\leqslant \frac{C^{l-1}}{(k\ln k)^l}\int_0^\infty (e^{-\delta s} + e^{\delta s} - 2)(\psi_1 \circ \nu^1)(ds). \end{aligned} \tag{4.3.22}$$

Recall the density of $\psi \circ \nu^1$ calculated in (4.3.7), we have

$$\int_0^\infty (e^{-\delta s} + e^{\delta s} - 2)\psi_1 \circ \nu^1(ds) = (2^{-\delta} + 2^\delta - 2) + \int_0^\infty (e^{-\delta s} + e^{\delta s} - 2)\psi_1 \circ \nu_c^1(ds)$$

Since $\gamma^{-1}\nu_c^1$ is independent of γ, for $\delta \leqslant \frac{1}{2}$, we define

$$C_{\delta,M} := \frac{1}{\gamma}\int_0^\infty (e^{-\delta s} + e^{\delta s} - 2)\psi_1 \circ \nu_c^1(ds) < \infty.$$

Plugging the last two equations back into (4.3.22) and then (4.3.21), we have

$$\begin{aligned}\mathbb{E}e^{-\delta R} &\leqslant \exp\left(((2^{-\delta} + 2^\delta - 2) + 2\gamma C_{\delta,M}) \cdot \sum_{l=1}^{k-1}\binom{k}{l}D\frac{C^{l-1}}{(k\ln k)^l}\right) \\ &= \left(1 + O(\gamma) + O\left(\frac{\ln\ln k}{\ln k}\right)\right)\exp(2^{-\delta} + 2^\delta - 2). \end{aligned} \tag{4.3.23}$$

Part 2: Again, writing out the integration form of $(2\nu_r) * \nu_R$ and applying (4.3.23), we have

$$\begin{aligned}(2\nu_r) * \nu_R((-\infty, M]) &\leqslant \int_M^\infty \int_{t-M}^\infty \nu_R(ds)\cdot(2\nu_r)(dt) \leqslant \int_0^\infty \left(\int_M^{s+M}\frac{2\gamma}{t^2}e^{\delta t}dt\right)\nu_R(ds) \\ &\leqslant \frac{2\gamma e^{\delta M}}{\delta M^2}\int_0^\infty e^{\delta s}\nu_R(ds) = \gamma C'_{\delta,M}.\end{aligned}$$

Therefore by the definition of $\nu^1_{S_0+S_1}$ in Corollary 4.3.8, there exists $C^\star_{\alpha,\delta,M}$ depending on the choice of α, δ and M such that $\tilde{\nu}_W^1((-\infty, M]) \leqslant \gamma C^\star_{\alpha,\delta,M}$.

Part 3: Finally we bound $\tilde{\nu}_W^0 = \nu_{S_1} * \nu_R$ and show that $\mathbb{P}(S_1 + R \geqslant \tilde{M}) \geqslant \mathbb{P}(S_1 \in [\tilde{M}, 2\tilde{M}])$. Write $\alpha' = (\ln 2 - \alpha)$ so that $\tilde{M} = (m + 1/2)\alpha'$. Note that S_1 only takes values in $\alpha'\mathbb{Z}_+$.

$$\begin{aligned}\mathbb{P}(S_1 + R \geqslant \tilde{M}, S_1 < \tilde{M}) &= \mathbb{P}(S_1 + R \geqslant \tilde{M}, S_1 \leqslant \tilde{M} - \alpha'/2) \\ &= \sum_{l=0}^{m} \mathbb{P}(S_1 = l\alpha')\mathbb{P}(R \geqslant \tilde{M} - l\alpha')\end{aligned}$$

Since $\mathbb{P}(\text{Pois}(1) = m)$ is decreasing in $m \geqslant 1$ and R is symmetric about 0, it follows that

$$\begin{aligned}\sum_{l=0}^{m} \mathbb{P}(S_1 = l\alpha')\mathbb{P}(R \geqslant \tilde{M} - l\alpha') &\geqslant \sum_{l=0}^{m} \mathbb{P}(S_1 = 2\tilde{M} - l\alpha')\mathbb{P}(R \leqslant -\tilde{M} + l\alpha') \\ &= \mathbb{P}(S_1 \in [\tilde{M}, 2\tilde{M}], S_1 + R \leqslant \tilde{M}).\end{aligned}$$

Comparing the last two equations yields the proof. □

4.3.6 Final step

Now we have all the ingredients to nail down the parameters and prove Theorem 4.2.1.

Proof of Theorem 4.2.1. Recall from Claim 4.3.1 that it is enough to show that

$$\nu_W((-\infty, t]) \leqslant \nu_k([-t, t]) - c/k\ln k, \qquad \text{whenever } \nu_k([-t, t]) < 1. \tag{4.3.24}$$

for some choice of parameter $(\delta, \alpha, M, \gamma, \epsilon)$, constant $c > 0$ and all $k \geqslant k_0$. Recall (4.3.19), on the right hand side we can absorb the $\frac{1}{k^2}\delta_{-\infty}$ term into $c/k\ln k$. Thus it is enough to consider the rest two terms:

$$\nu_W^0 := \frac{e^{p_- + \gamma - \beta}}{k\ln k}\tilde{\nu}_W^0 = \frac{e^{p_- + \gamma - \beta}}{k\ln k}\nu_{S_1} * \nu_R, \quad \nu_W^r := \frac{e^{p_- + \gamma - \beta}}{k\ln k}\tilde{\nu}_W^r = \frac{e^{p_- + \gamma - \beta}}{k\ln k}\nu_{S_0+S_1}^r * \nu_R.$$

We first consider the right tail of ν_W^r. Combining Lemma 4.3.9 Part 1 and Corollary 4.3.8 and recalling that $|p_- - 1| = (1+\epsilon)\gamma p_0$, for all $t \geqslant M$ we have

$$\nu_W^r(dt) \leqslant \frac{e^{1-\beta}}{k\ln k}(1+\alpha)e^{(2e^{-\alpha})^{-\delta} + 2^{\delta} + 2^{-\delta} - 3}(1 + C_{\delta,M}(\gamma + \epsilon))(2\nu_r)(dt). \tag{4.3.25}$$

Fix $\delta = 1/2$ and α small enough such that (note $\exp(2\sqrt{2} - 3) \approx 0.8423$)

$$(1+\alpha)\exp((2e^{-\alpha})^{-\delta} + 2^{\delta} + 2^{-\delta} - 3) = (1 + O(\alpha))\exp(2\sqrt{2} - 3) \leqslant \frac{17}{20} < 1.$$

Let $M = (m + 1/2)(\ln 2 - \alpha)$ where m is the smallest integer such that the condition in Fact 4.3.10 and Lemma 4.3.7 is satisfied. Finally for constant $C_{\delta,M}$ depending on $p_0 = p_0(\delta, M)$

and the constants in Corollary 4.3.8 and Lemma 4.3.9, let $\gamma \leqslant \gamma_1 < 1, \epsilon \leqslant \epsilon_1 < 1$ and $0 < 1-\beta < 1-\beta_1$ such that for all $t \geqslant M$,

$$\text{RHS of (4.3.25)} \leqslant \frac{9}{10}\frac{e^{1-\beta}}{k\ln k}(2\nu_r)(dt) \leqslant \frac{19}{20}\frac{1}{k\ln k}(2\nu_r)(dt). \tag{4.3.26}$$

Next we prove (4.3.24) for t around M. The key idea is to show that the mass of ν_W^0 escaping $[-M,M]$ is smalle than the mass of ν_W^r dropping below M, and those mass can be absorbed by the mulipilicative improvement of ν_W^r in (4.3.26). Let $\tilde{M} = \tilde{M}(\delta,\alpha,M) = (\tilde{m}+1/2)(\ln 2-\alpha)$ such that for the $C^\star_{\delta,\alpha,M}$ in Lemma 4.3.9 Part 2,

$$\frac{1}{20}(2\nu_r)([M,\tilde{M}]) = \frac{1}{20}\int_M^{\tilde{M}}\frac{2\gamma}{t^2}e^{\delta t}dt \geqslant e^{1-\beta_1}(C^\star_{\delta,\alpha,M}+1)\gamma. \tag{4.3.27}$$

Write $q_{\tilde{M}} := \mathbb{P}((\ln 2-\alpha)\mathrm{Pois}(1) \in [\tilde{M},2\tilde{M}]) > 0$. Given α and $\tilde{M}$, let $\gamma \leqslant \gamma_2$ and $1-\beta \leqslant 1-\beta_2$ such that for some $c_1 \in (0, q_{\tilde{M}})$,

$$e^{1-\beta}\left((1-q_{\tilde{M}}) + \gamma C^\star_{\delta,\alpha,M}\right) \leqslant 1-c_1 < 1. \tag{4.3.28}$$

Note for any $t < M$, $\nu_k([-t,t]) = \nu_k(\{0\}) = 1/k\ln k$. By Lemma 4.3.9 Part 3, $\mathbb{P}(S_1+R \geqslant \tilde{M}) \geqslant q_{\tilde{M}}$. By (4.3.26) and (4.3.28), we have for $t \leqslant \tilde{M}$

$$\begin{aligned}\nu_W((-\infty,t]) &\leqslant \nu_W^0((-\infty,\tilde{M})) + \nu_W^r((-\infty,M]) + \nu_W^r((M,t\vee M])\\ &\leqslant \frac{e^{1-\beta}}{k\ln k}((1-q_{\tilde{M}})+\gamma C^\star_{\delta,\alpha,M}) + \frac{19}{20}\frac{1}{k\ln k}(2\nu_r)([M,t\vee M])\\ &\leqslant \frac{1-c_1}{k\ln k} + \frac{19}{20}\frac{1}{k\ln k}(2\nu_r)([M,t\vee M]) \leqslant \nu_k([-t,t]) - \frac{c_1}{k\ln k}.\end{aligned}$$

Finally we prove (4.3.24) for $t \geqslant \tilde{M}$ and $\nu_k([-t,t]) < 1$. Choose $c_2 > 0$ such that for $\gamma = \gamma_1 \wedge \gamma_2$ and $1-\beta < 1-\beta_3$, $e^{1-\beta}+c_2 < 1+\gamma$. By (4.3.27), we have

$$\begin{aligned}\nu_W((-\infty,t]) &\leqslant \frac{e^{1-\beta}}{k\ln k}(1+\gamma C^\star_{\delta,\alpha,M}) + \frac{19}{20}\frac{1}{k\ln k}(2\nu_r)([M,\tilde{M}]) + \frac{19}{20}\frac{1}{k\ln k}(2\nu_r)((\tilde{M},t])\\ &\leqslant \frac{e^{1-\beta}-\gamma}{k\ln k} + \frac{1}{k\ln k}(2\nu_r)([M,t]) + \frac{1}{k\ln k}\left[e^{1-\beta}(1+C^\star_{\delta,\alpha,M})\gamma - \frac{1}{20}(2\nu_r)([M,\tilde{M}])\right]\\ &\leqslant 1-\frac{c_2}{k\ln k} + \frac{1}{k\ln k}(2\nu_r)([M,t]) = \nu_k([-t,t]) - \frac{c_2}{k\ln k}.\end{aligned}$$

Combine all pieces together, we have the desired result with $\beta_\star = \beta_1 \vee \beta_2 \vee \beta_3$, $c = c_1 \wedge c_2$ and $k > k_0$. □

4.4 Freezing threshold

Proof of Theorem 4.1.1. Let p_n denote the probability that the root is uniquely fixed by the configuration on L_n. This will happen if and only if there is at least one clause i attached to ρ such that $\{u_{i,j}\}_{j=1}^{l}$ has the same value under σ and each of them is fixed by the sub-configuration L_{ij}. Hence $p_0 = 1$ and

$$\begin{aligned} p_n &= 1 - \mathbb{P}(\text{no such } i) = 1 - \mathbb{E}\left(1 - \frac{1}{2^k - 1} p_{n-1}^k\right)^{d_\rho} \\ &= \begin{cases} 1 - (1 - \frac{1}{2^k-1} p_{n-1}^k)^d & \mathcal{T}_{d,k} \\ 1 - e^{-(2^k-1)^{-1} p_{n-1}^k d} & \mathcal{T}_{\mathrm{Pois}(d),k} \end{cases} =: f(p_{n-1}). \end{aligned}$$

Recall the definition of d_k^f in Theorem 4.1.1, we first prove the correctness of d_k^f. For $T \sim \mathcal{T}_{\mathrm{Pois}(d),k}$ and $d > d_k^f$, let x_d be the largest solution of $\frac{(2^k-1)x}{(1-e^{-x})^k} = d$. $f(p)$ is an increasing function of p and $p_d := 1 - e^{-x_d}$ is a fix point of f. Hence by induction we have $p_n = f(p_{n-1}) \geqslant f(p_d) = p_d$ and $\liminf p_n \geqslant p_d > 0$, i.e. the model freezes on infinite tree with positive probability.

For each $d < d_k^f$, the definition of d_k^f ensures the existence of $\delta > 0$ such that for every $x > 0$, $\frac{(2^k-1)x}{(1-e^{-x})^k} > d(1+\delta)$. For every $p = 1 - e^{-x} < 1$,

$$1 - f(p) = e^{-(2^k-1)^{-1} p^k d} \geqslant e^{-x/(1+\delta)} = (1-p)^{1/(1+\delta)}.$$

Note that $1 - p_1 = 1 - f(1) = (\frac{2^k-2}{2^k-1})^d > 0$. By induction we have $1 - p_n \geqslant (1-p_1)^{1/(1+\delta)^n} \to 1$, i.e. with high probability the model will not freeze as the size of the tree tends to infinity. The proof for $T \sim \mathcal{T}_{d,k}$ is exactly parallel.

To determine the asymptotic of d_k^f, we first work with $\mathcal{T}_{\mathrm{Pois}(d),k}$. Split the infimum over $x > 0$ into three cases: $x \in (0, \ln 2]$, $x \in [\ln 2, \ln k]$ and $x \geqslant \ln k$. For $x \geqslant \ln k$, let $y = k \ln k \cdot e^{-x} \in (0, \ln k]$. Using the fact that $(1-a)^{-k} \geqslant (1+a)^k \geqslant 1 + ka$, we have

$$\begin{aligned} x(1-e^{-x})^{-k} &= (\ln k + \ln\ln k - \ln y)(1 - \frac{y}{k \ln k})^{-k} \geqslant (\ln k + \ln\ln k - \ln y)(1 + \frac{y}{\ln k}) \\ &\geqslant \ln k + \ln\ln k + y - \ln y \geqslant \ln k + \ln\ln k + 1, \end{aligned}$$

where in the last step equality is achieved by $y = 1$. Plugging $y = 1$ back to the LHS yields that indeed $\inf_{x \geqslant \ln k} x(1-e^{-x})^{-k} = \ln k + \ln\ln k + 1 + o_k(1)$. For $x \in [\ln 2, \ln k]$, let $z = ke^{-x} \in [1, \frac{1}{2}k]$. Inequality $e^{-a} > (1-a)$ implies that $(1 - \frac{z}{k})^{-k} \geqslant e^z$ and

$$\inf_{x \in [\ln 2, \ln k]} x(1-e^{-x})^{-k} = \inf_{z \in [1, \frac{1}{2}k]} (\ln k - \ln z)(1 - \frac{z}{k})^{-k} \geqslant \inf_{z \in [1, \frac{1}{2}k]} (\ln k - \ln z) e^z = e \ln k.$$

where the last step uses that $\frac{d}{dz}((\ln k - \ln z)e^z) = (\ln k - \ln z - \frac{1}{z})e^z > 0$, for all $z \leqslant \frac{1}{2}k$. Finally for $x \in (0, \ln 2]$,

$$\inf_{x \in (0, \ln 2]} x(1-e^{-x})^{-k} \geqslant \inf_{x \in (0, \ln 2]} x^{1-k} = (\ln 2)^{1-k}.$$

Combining all pieces together we have $d_k^f = \ln k + \ln\ln k + 1 + o_k(1)$ for $\mathcal{T}_{\mathrm{Pois}(d),k}$.

For regular trees, we note that since $x \ln^{-1}\left(1 - \frac{(1-e^{-x})^k}{2^k-1}\right) \geqslant \frac{(2^k-1)x}{(1-e^{-x})^k}$, the d_k^f of $\mathcal{T}_{d,k}$ can not be smaller than that of $\mathcal{T}_{\mathrm{Pois}(d),k}$. Plugging in $x = \frac{1}{k \ln k}$ gives the same asymptotic order. $\square$

4.5 Remaining calculation

Proof of Fact 4.3.10. Let $h(s) = \frac{(1-s)^{-2}-1}{1-(1+s)^{-2}} = \frac{2-s}{2+s} \cdot \frac{(1+s)^2}{(1-s)^2}$. We have $h(0) = 1$ and $h'(s)$ is uniformly bounded on $[0, \frac{1}{2}]$. Let $m = \sup_{s \in [0,\frac{1}{2}]} h'(s) \vee 1$. Rearranging the terms, (4.3.20) is equivalent to

$$e^{2\delta s} \geqslant \frac{(1-\frac{s}{t})^{-2}-1}{1-(1+\frac{s}{t})^{-2}} = h(\frac{s}{t}). \tag{4.5.1}$$

Both sides of equation (4.5.1) equals to 1 at $s = 0$. Differentiate both sides with respect to s and let $M > M_1 := m/2\delta$, we have for all $t > M$ and $0 < s \leqslant t/2$,

$$\frac{d}{ds}(\text{RHS of (4.5.1)}) = \frac{1}{t}h'(\frac{s}{t}) \leqslant \frac{m}{M_1} \leqslant 2\delta \leqslant 2\delta e^{2\delta s} = \frac{d}{ds}(\text{LHS of (4.5.1)}).$$

Hence (4.5.1) is true for all $t > M$ and $0 < s \leqslant t/2$. For any s, t such that $t - s > M$ and $s > t/2$, we must have $t > 2M, s > M$. Therefore for $M > M_2 := \frac{2}{\delta} \vee \frac{1}{2\delta}\ln(36/5) = \frac{2}{\delta}$

$$\begin{aligned}
\text{(LHS-RHS) of (4.3.20)} &\leqslant \frac{1}{M^2}e^{-\delta s} + (\frac{1}{(3/2)^2} - 1)\frac{1}{t^2}e^{\delta s} \leqslant e^{-\delta s}(\frac{1}{M^2} - \frac{5}{9t^2}e^{2\delta(t/2)}) \\
&\leqslant e^{-\delta s}(\frac{1}{M^2} - \frac{5}{36M^2}e^{2\delta M}) = e^{-\delta s}\frac{1}{M^2}(1 - \frac{5}{36}e^{2\delta M}) < 0.
\end{aligned}$$

Letting $M_\star(\delta) = M_1 \vee M_2$ finishes the proof. □

Chapter 5

Rapid mixing of graph colorings on trees

In this chapter we show that the mixing time of the Glauber dynamics of graph colorings (defined in Section 5.2.1) on trees undergoes a phase transition at $d = d_{\mathrm{rec}}$. The main result is following.

Theorem 4. *There exists absolute constant k_0 such that for $k \geqslant k_0$, $\beta < 1$ and*

$$d \leqslant k[\ln k + \ln \ln k + \beta],$$

if the k-coloring model is non-reconstructible on d-regular trees, then the mixing time of the Glauber dynamics of the k-coloring model on n-vertex d-ary tree is $O(n \ln n)$.

Theorem 4 and Theorem 2 together implies that for sufficiently large k (the exact value of k_0 in the two theorems might be different), the Glauber dynamics has $O(n \ln n)$ mixing time whenever the model is non-reconstructible. The other direction is shown in [Tet+12].

5.1 Introduction

There have been intensive studies on the mixing times of Markov chains for sampling spin systems in both theoretical computer science and statistical physics. Many results have shown that the mixing time of the Glauber dynamics, both for the k-coloring model and general spin systems, are related to the spatial properties of the Gibbs measure. Two properties of primary interest are the uniqueness of the infintie-volume Gibbs measure and the reconstructability as defined in Definition 3.1.1.

In a sequence of results by Martinelli, Sinclair and Weitz [MSW04; MSW07; Wei04], it was shown under quite general settings that the Glauber dynamics exhibits rapid mixing on d-regular trees regardless of the boundary condition, when the corresponding spin system admits an unique infinite-volume Gibbs measure. Their method uses the decay of correlation between the root and the leaves to bound the log-Soblev constant of the block dynamics.

Less general results are known beyond the uniqueness threshold. The main obstacle, as in the case of graph colorings, is that the chain might be reducible under certain boundary conditions. Thus one can not hope to get a meaningful bound for all boundary conditions.

Notwithstanding this, it is still interesting to consider the mixing time under the free boundary condition. The correlation between the roots and leaves in the absence of boundary conditions is closely related to the problem of reconstructions on trees, as both properties concerns about to influences of an *average* boundary configurations on the root. It is natural to hope that the rapid mixing of the Glauber dynamics holds throughout the non-reconstruction regime.

Restrict our attention to the k-coloring problem on d-ary trees for the moment. The uniqueness of the Gibbs measure is shown to hold for $k \geqslant d+2$ by Jonasson [Jon02] and the results of [MSW04; MSW07] imply an $O(n \ln n)$ mixing time in the same region. Recall the reconstruction threshold $d_{\text{rec}} = (1 + O(1))k \ln k$ from Section 3.1. Bhatnagar et al. [Bha+11] show that the block dynamics for k-coloring model mixes in $O(n \ln n)$ time in the same region using non-reconstruction and following the methods of [MSW04]. However their result can not be easily extended to the Glauber dynamics due to the failure of Markov chain comparison between the two dynamics. Namely, one step in the block dynamics might not be replaced by bounded number of steps in the Glauber dynamics.

For more results in the non-uniqueness regime, Berger et.al. [Ber+05] showed for general models that the mixing time on trees is at most polynomial whenever the dynamics is ergodic, which in the case of coloring corresponds to $k \geqslant 3$ and $d \geqslant 2$. Goldberg et.al. [GJK10] proved an upper bound of $n^{O(d/\ln d)}$ for the complete tree with branching factor d. Lucier et.al. [LMP09] showed $n^{O(1+d/k \ln d)}$ mixing time for all d and $k \geqslant 3$. [Tet+12] proved that the mixing time undergoes a phase transition at the reconstruction threshold $k = (1+o(1))d/\ln d$, where their upper bound for the mixing time when $k \geqslant (1+o(1))d/\ln d$ is $O(n^{1+o_k(1)})$. They also showed that the mixing time is $\Omega(n^{d/k \ln d - o_k(1)})$ for $k \leqslant (1-o(1))d/\ln d$, i.e. rapid mixing does not hold in the reconstruction regime.

The main purpose of this chapter is to reduce the mixing time in the non-reconstruction regime from the polynomial upper-bound of $n^{1+o(1)}$ to the sharp bound of $O(n \ln n)$. Our proof is based on a modification of the techniques used in [MSW04]. The main obstacle, as hinted above, is the reducibility of the Glauber dynamics on subtrees under fixed boundary condition. Heuristically, in the non-uniqueness regime, vertices may be "freezed" by their neighbors. While the block dynamics can update "frozen" vertices together with their neighbors in one single move, extra efforts are needed for the Glauber dynamics to pass around the barrier and "defreeze" the vertices, leading to the failure of the standard Markov chain comparison result between the two dynamics. With that in mind, we introduce a new variant of the block dynamics that focuses on the connected component on the state space of the usual block dynamics induced by valid moves of the Glauber dynamics. By carefully examining the portion of "frozen" vertices and their influences on nearby sites, we will show rapid mixing of our new version of the block dynamics which implies the final result.

We conclude this section by discribing the literature on the mixing times on general graphs. For k-colorings on graphs with n vertices and maximal degree d, the Glauber dynamics is not in general irreducible if $k \leqslant d+1$. A long-standing conjectured is that the chain exhibits rapid mixing whenever $k \geqslant d+2$. So far the best result on general graphs is given by Vigoda in [Vig00], where he showed $O(n^2 \ln n)$ mixing time for $k \geqslant \frac{11}{6}d$. A series of improvements on the constant $\frac{11}{6}$ for rapid mixing have been made with extra conditions on the degree or the girth. See the survey [FV07] for more results toward this direction.

5.1.1 General spin system

The correspondence between rapid mixing and spatial correlation decay is not restricted to the coloring model alone, but is a common phenomenon that extends to general spin systems. For instance, Weitz conjectured in [Wei04] that for any k-state spin system on regular trees, the system mixes in $O(n \ln n)$ time whenever it admits an unique Gibbs measure and the Glauber dynamics is connected under given boundary condition. He proved the statement for $k = 2$ and for the ferromagnetic Potts model and colorings as two special cases of $k > 2$. He also provided a sufficient condition that applies to a wide range of other models.

As suggested by the case of the coloring model, the mixing time under free boundary condition is more closely related to the reconstruction threshold. In fact, Berger et al. [Ber+05] showed that for general spin systems on trees, $O(n)$ relaxation time under free-boundary condition implies non-reconstruction. Our methods for the coloring model can also be extended to general k-state spin systems provided that the spin system satisfies certain mild connectivity conditions. Therefore as an intermediate result, we provide a sufficient condition for spin systems to exhibit rapid mixing in the non-reconstruction region.

In Section 5.2.1, we specify a spin system by its Markov chain kernel M, where $M(c, c') = \mu(\sigma_y = c' | \sigma_x = c)$ for any $(x, y) \in E$, and restrict our discussion to kernels that are ergodic and reversible (see also [Geo11] for more details). Let λ be the second largest eigenvalue of M. We show that the Glauber dynamics is rapidly mixing for spin systems M assuming a certain *connectivity condition* $\mathcal{C}$ that will be specified in Section 5.2.3.

Theorem 5.1.1. *Let M be a k-state spin system on the n-vertex d-ary tree T with second eigenvalue λ. If M satisfies the connectivity condition $\mathcal{C}$, is non-reconstructible on T, and $d\lambda^2 < 1$ then the mixing time of Glauber dynamics on T under free boundary condition is $O(n \ln n)$.*

In the statement of Theorem 5.1.1, the connectivity condition C mainly concerns about the hard constraints. Roughly speaking, it requires the root to be able to "change freely" between all k states with high probability as the size of the tree grows. In particular, it includes all models without hard constraints or models with a permissive state, a state that can occur next to all other states (e.g. the hardcore model).

The requirement of $d\lambda^2 < 1$ comes from the Kesten-Stigum bound $d\lambda^2 = 1$ in reconstruction problems: Whenever $d\lambda^2 > 1$, the system is reconstructible by simply counting the number of leaves in each state [Mos04]. Hence non-reconstruction implies $d\lambda^2 \leqslant 1$. The Kestin-Stigum bound is known to be tight for models including the Ising model (symmetric binary channel) and near-symmetric binary channels [Bor+06]. For other models such as hardcore model and graph colorings, it is strictly larger than the true threshold. Nonetheless it has been suggested that the speed of decay of correlation undergoes a phase transition at the critical value $d\lambda^2 = 1$ with different scalings for $d\lambda^2 = 1$ and $d\lambda^2 < 1$. Indeed, a recent work of Ding, Lubetzky and Peres [DLP10] showed that the mixing time for the Ising model is at least of order $n \ln^3 n$ when $d\lambda^2 = 1$. Therefore we can only hope to prove Theorem 5.1.1 for $d\lambda^2$ strictly smaller than 1.

5.2 Preliminaries

5.2.1 Definition of model

General spin systems: Throughout the chapter, we will write $T = (V, E)$ for the d-ary tree with root ρ and $|V| = n$ vertices. Denote the l-th level of T by L_l starting with $L_0 = \{\rho\}$. Given vertex $x \in T$, we will use T_x to represent the subtree rooted at x and let $B_{x,l}$, $L_{x,l}$ denote the first l levels and the l-th level of T_x respectively.

Let $[k] = \{1, \ldots, k\}$ denote the set of possible spin values. We are interested in general k-state spin systems specified by potentials U and W, where U is a symmetric function from $[k] \times [k] \to \mathbb{R} \cup \{\infty\}$ and W is a function from $[k] \to \mathbb{R}$. Given U and W, the (free-boundary) Gibbs measure on T is the probability measure on configurations $\sigma \in [k]^V$ defined as

$$\mu(\sigma) = \frac{1}{Z} \exp\left[-\Big(\sum_{(x,y) \in E} U(\sigma_x, \sigma_y) + \sum_{x \in V} W(\sigma_x) \Big) \right],$$

where Z, also known as the partition function, is the normalizing constant such that

$$\sum_{\sigma \in [k]^V} \mu(\sigma) = 1.$$

We say that a configuration σ is *proper* if $\mu(\sigma) > 0$ and denote the set of proper configurations on T by $\Omega_T = \{\sigma : \mu(\sigma) > 0\}$. For each pair of states $(i,j) \in [k]^2$, we say that (i,j) is a hard constraint if $U(i,j) = \infty$, otherwise we say that i and j are *compatible*. For each subset of vertices $A \subseteq T$, we will write σ_A for the restriction of σ to A and use superscript for boundary conditions. In particular, $\Omega_A^\eta = \{\sigma : \sigma \in \Omega_T, \sigma_{T \setminus A} = \eta_{T \setminus A}\}$ is the set of configurations compatible with boundary condition η and we denote the conditional law on $\Omega^\eta(A)$ as $\mu_A^\eta(\sigma) = \mu(\sigma \mid \sigma \in \Omega_A^\eta)$.

For the reconstruction problem, it is easy to work with the Markov chain construction of the Gibbs measure on trees, which is just the broadcast model on trees. Recall from Section 3.1. For each probability kernel M with stationary π, the law of a random configuration generated by the broadcast model on T is given by

$$\mu(\sigma) = \pi(\sigma_\rho) \prod_{(x,y) \in E} M(\sigma_x, \sigma_y).$$

It is easy to check that for any reversible M, the aformentioned probablity measure corresponds to the spin system with potentials U, W given by

$$U(c_1, c_2) = -\ln\left(\frac{M(c_1, c_2)}{\pi(c_2)}\right), W(c) = -\ln \pi(c). \tag{5.2.1}$$

Note that not all potential pairs U, W can be expressed this way. A necessary condition for (5.2.1) is that

$$\sum_{c' \in [k]} \exp[-(U(c, c') + W(c'))] \equiv C, \quad \forall c \in [k]$$

for some constant C. We will henceforth restrict our attention to spin systems that can be expressed as (5.2.1) and refer such systems by their probability kernel M. We will also assume that M is ergodic and reversible.

The principal example of spin systems for this chapter is the graph coloring model, where for each $c, c \in [k]$ $W(c) \equiv 0, U(c, c') = \infty \cdot 1(c = c')$, or equivalently $M(c, c') = \frac{1}{k-1} 1(c = c'), \pi(c) \equiv \frac{1}{k}$.

Uniqueness and reconstruction: Two key notions of spatial decay of correlation for spin systems on trees are the uniqueness and reconstruction thresholds. Recall the definition of reconstruction from Section 3.1.

Definition (Reconstruction)**.** For $k \geqslant 2$, we say that a k-state system M is reconstructible on tree T if there exist two states $c, c' \in [k]$ such that

$$\limsup_{l \to \infty} d_{\mathrm{TV}}(\mu(\sigma_{L_l} = \cdot \mid \sigma_\rho = c), \mu(\sigma_{L_l} = \cdot \mid \sigma_\rho = c')) > 0.$$

Otherwise we say that the system has non-reconstruction on T.

Non-reconstruction corresponds to the vanishing influence of an *average* boundary condition. A strictly stronger condition is the uniqueness property, which corresponds to the vanishing influence of the *worst* boundary condition.

Definition (Uniqueness)**.** For $k \geqslant 2$, we say that a k-state system M has uniqueness on tree T if

$$\limsup_{l \to \infty} \sup_{\eta, \eta' \in \Omega_{L_l}} d_{\mathrm{TV}}(\mu(\sigma_\rho = \cdot \mid \sigma_{L_l} = \eta), \mu(\sigma_\rho = \cdot \mid \sigma_{L_l} = \eta')) > 0,$$

where Ω_{L_l} is the set of configurations restricted to level l.

Glauber dynamics and mixing time: The Glauber dynamics of a k-state spin system M is a Markov chain X_t on state space Ω_T. A step of the Markov chain from X_t to X_{t+1} is defined as follows:

1. Pick a vertex x uniformly at random from T;

2. Pick a state $c \in [k]$ according to the conditional distribution of the spin value of x given the rest of configuration, i.e. state c is picked with probability $\mu^{\sigma}_{\{x\}}(c) = \mu(\sigma'_x = c \mid \sigma'_y = \sigma_y, \forall y \neq x)$;

3. Set $X_{t+1}(x) = c$ and $X_{t+1}(y) = X_t(y)$, for all $y \neq x$.

In the case of graph coloring, the second step corresponds to picking uniformly at random colors that do not appear in the neighborhood of x.

To justify our study of the Glauber dynamics under free boundary condition, we first show that the Markov chain is irreducible and hence ergodic on the set of all proper configurations. For the sake of recursive analysis on subtrees later, we also prove irreducibility in a related case where the root of T is connected to one more vertex, namely its "parent", and the value of its parent is fixed. For each $c \in [k]$, let Ω^c_T denote the set of configurations with the parent of root ρ fixed to state c and let μ^c_T be the corresponding conditional Gibbs measure.

Lemma 5.2.1. *For any k-state system M on d-ary tree T, if M is reversible and ergodic, then Ω_T is irreducible under the Glauber dynamics and so is Ω^c_T for each $c \in [k]$.*

Proof. We first prove the irreducibility of Ω^c_T by induction on the number of levels l in T. For $l = 0$, it is trivially true since Ω^c_T is simply the set of states compatible of c. Suppose that the Glauber dynamics is irreducible on the $(l-1)$-level tree. For the l-level tree T, we need to show that for any two configurations $\sigma, \sigma' \in \Omega^c_T$, there exists a path of valid moves of the dynamics connecting σ to σ'. To construct such a path, one can first change every vertex $x \in L_1$ to state c by a sequence of moves in the tree T_x. This is possible since alternating layers of states c and σ_ρ is a proper configuration in $\Omega^{\sigma_\rho}_{T_x}$ and any two configurations in $\Omega^{\sigma_\rho}_{T_x}$ are connected by the inductive hypothesis. One may then change the spin of the root from σ_ρ to σ'_ρ, since both states are compatible with c. Finally we may change the configuration of every subtree T_x to σ'_{T_x} using the inductive hypothesis, ending in the configuration σ'.

To show the irreducibility of Ω_T, we choose $\sigma, \sigma' \in \Omega_T$. By the ergodicity of M, there exists a sequence of states $c_0, \ldots, c_{2m} \in [k]$ such that $c_0 = \sigma_\rho$, $c_{2m} = \sigma'_\rho$ and for each $0 \leqslant i \leqslant 2m-1$, c_i is compatible with c_{i+1}. For each $0 \leqslant i \leqslant m$, let $\tau_i \in \Omega_T$ be the configuration with alternating layers of c_{2i} and c_{2i+1}(let c_{2m+1} be an arbitrary state compatible with $c_{2m} = \sigma'_\rho$). One can first change σ to τ_0 using the irreducibility of the Glauber dynamics on $\Omega^{\sigma_\rho}_{T_x}$ for each $x \in L_1$, then for each $1 \leqslant i \leqslant m$ change from τ_{i-1} to τ_i by first changing all vertices on even levels to c_{2i} then vertices on odd levels to c_{2i+1}, and finally change each $(\tau_m)_{T_x}$ to σ'_{T_x}. $\square$

Lemma 5.2.1 implies that the Glauber dynamics with free boundary conditions will always converges to the Gibbs measure μ. The *mixing time* of the Glauber dynamics is defined as

$$t_{\text{mix}} = \max_{\sigma \in \Omega_T} \min\{t : d_{\text{TV}}(P^t(\sigma, \cdot), \mu) \leqslant 1/4\},$$

where P is the probability kernel of X_t and $d_{\text{TV}}(\eta, \mu) = \frac{1}{2}\sum_\sigma |\eta(\sigma) - \mu(\sigma)|$ is the total variance distance. To bound the mixing time we will make use of the *log-Sobolev constant*.

For a non-negative function $f : \Omega_T \to \mathbb{R}$, let $\mu(f) = \sum_\sigma \mu(\sigma)f(\sigma)$ be the expectation of f and $\mathrm{Ent}(f) = \mu(f \ln f) - \mu(f)\ln\mu(f)$ be its entropy. The Dirichlet form of f is defined as

$$\mathcal{D}(f) = \frac{1}{2}\sum_{\sigma,\sigma'\in\Omega_T} \mu(\sigma)P(\sigma,\sigma')(f(\sigma) - f(\sigma'))^2.$$

And the log-Sobolev constant is defined as $\gamma = \inf_{f\geqslant 0} \frac{\mathcal{D}(\sqrt{f})}{\mathrm{Ent}(f)}$. Applying results in functional analysis to the Glauber dynamics yields the following bound (see e.g. [SC97, Thm 2.2.5]):

Theorem. *For k-state system M on n-vertex d-ary tree T, there exists a constant $C > 0$ such that $t_{\mathrm{mix}} \leqslant \frac{1}{\gamma} \cdot Cn\ln n$.*

Therefore to show rapid mixing it is enough to show that γ is uniformly bounded away from zero as $n \to \infty$.

5.2.2 Component Dynamics

Next we define a new variant of block dynamics on T, which we call the "component dynamics". Each step of the new dynamics updates a block of vertices each step, but only chooses configurations within the connected component of the Glauber dynamic. In this way we can utilize the techniques in [MSW04] while bypassing the problem that one step of the block dynamics may not be connected in the Glauber dynamics when $k \leqslant d + 1$. To give a formal definition, for $A \subset T$, we say that $\sigma' \sim_A \sigma$ if ${\sigma'}_{T\setminus A} = \sigma_{T\setminus A}$ and σ'_A, σ_A are connected by valid moves of the Glauber dynamics on A with fixed boundary condition $\sigma_{T\setminus A}$. We will omit the A in $\sigma \sim_A \sigma'$ when it is clear from context. Let $\Omega^{*,\sigma}_A = \{\sigma' \in \Omega^\sigma_A, \sigma' \sim_A \sigma\}$ denote the connected component of σ in Ω^σ_A, and $\mu^{*,\sigma}_A(\sigma') = \mu(\sigma'|\Omega^{*,\sigma}_A)$ be the Gibbs distribution conditioned on both configuration outside A and the connected component within A.

For $l \geqslant 1$, recall $B_{x,l}$ is the block of l levels rooted at x and $L_{x,l}$ be the l-th level of $B_{x,l}$. If x is within distance l of the leaves, let $B_{x,l} = T_x$. We define the *component dynamics* to be the Markov chain on Ω_T with the following update rule: In each step,

1. Pick a vertex x uniformly randomly from T,
2. Replace σ by σ' drawn from conditional distribution $\mu^{*,\sigma}_{B_{x,l}}$.

The dynamics is reversible with respect to the Gibbs distribution. For test functions $f : \Omega_T \to \mathbb{R}$, let $\mu^{*,\sigma}_A(f) = \sum_{\sigma'\in\Omega^{*,\sigma}_A} f(\sigma')\mu^{*,\sigma}_A(\sigma')$ be the conditional expectation of f on $\Omega^{*,\sigma}_A$ and for $f \geqslant 0$, let

$$\mathrm{Ent}^{*,\sigma}_A(f) = \mathrm{Ent}(f \mid \Omega^{*,\sigma}_A) = \mu^{*,\sigma}_A(f\ln f) - \mu^{*,\sigma}_A(f)\ln\mu^{*,\sigma}_A(f)$$

be the conditional entropy of f. We write the sum of local entropies of block size l as $\mathcal{E}^*_l = \sum_{x\in T} \mu_T(\mathrm{Ent}^{*,\sigma}_{B_{x,l}}(f))$. With minor modification, the comparison result of block dynamics also works for component dynamics: (see e.g. Prop 3.4 of [Mar99], in the proof substitute $\mathcal{E}_D(f, f)$ by $\mathcal{E}_l^*$ and note $\sum_{\sigma'} \mu_T^\tau(\sigma')\mu_{B_{x,l}}^{*,\sigma'}(\sigma) = \mu_T^\tau(\sigma)$.)

$$\gamma \geqslant \frac{1}{l} \cdot \inf_{f \geqslant 0} \frac{\mathcal{E}_l^*}{\mathrm{Ent}(f)} \cdot \min_{\sigma,x} \gamma_{B_{x,l}}^{*,\sigma}$$

where $\gamma_{B_{x,l}}^{*,\sigma}$ is the log-Soblev constant of the Glauber dynamics on $\Omega_{B_{x,l}}^{*,\sigma}$ with the boundary condition on $\partial B_{x,l}$ given by σ. From our definition of $\Omega_{B_{x,l}}^{*,\sigma}$, it is easy to see that $\min_{\sigma,x} \gamma_{B_{x,l}}^{*,\sigma}$ is a constant only depending on the branching number d, block size l and M itself and is strictly greater than 0 independent of T. Thus to show $O(n \ln n)$ mixing time for the Glauber dynamics, it is enough to show $\mathcal{E}_l^* \geqslant \text{const} \times \mathrm{Ent}(f)$ for all $f \geqslant 0$ and some choice of block size l independent of tree size $|T| = n$.

5.2.3 Connectivity condition

In this section we specify the connectivity condition $\mathcal{C}$ mentioned in Theorem 5.1.1. First we will define the notion of free vertices. Let T be a tree of l levels. Given configuration $\sigma \in \Omega_T$ with $\sigma_\rho = c$, $\sigma_{L_l} = \eta$, we say that the root can change (from c) to state c' in one step if and only if there exists a path $\sigma = \sigma^0, \sigma^1, \ldots, \sigma^n \in \Omega_T$ such that

1. $\sigma_{L_l}^i \equiv \eta$ for each $0 \leqslant i \leqslant n$. $\sigma_\rho^i = c$, for each $0 \leqslant i \leqslant n-1$ and $\sigma_\rho^n = c'$.

2. For each $0 \leqslant i \leqslant n-1$, configuration σ^i differs from σ^{i+1} at exactly one vertex.

Put another way, the path is a valid trajectory of the Glauber dynamics with fixed boundary condition which changes the state of ρ only once in the final step. For $x \in T$, we say x is *free* (in σ) if, considered as the root of T_x, x can change to all the other $(k-1)$-states in one step. We are interested in the probability that the root of an l-level tree is free and we denote it by $p_l^{\text{free}} = \mu(\sigma : \rho \text{ is free in } \sigma)$.

Definition. We say that a k-state system M on the d-ary tree satisfies the connectivity condition $\mathcal{C}$ if M is ergodic, reversible and satisfies the following conditions:

1. If $k \geqslant 3$, then for any $c_1, c_2, c_3 \in [k]$, there exists $c \in [k]$ such that c is compatible with c_1, c_2, c_3.

2. The probability of being free tends to 1 as l tends to infinity, i.e. $\lim_{l\to\infty} p_l^{\text{free}} = 1$.

Roughly speaking, the connectivity condition controls the behavior of "frozen" vertices in a typical configuration. As will be shown in Section 5.4, under the connectivity condition the probability that a vertex is "frozen" by the boundary condition is extremely small and the extra restriction of the component dynamics is negligible for vertices faraway from the bottom (see the remark after Claim 5.4.2 for more discussions).

5.2.4 Outline of Proof

A key ingredient in [MSW04] is that a certain strong concentration property implies "entropy mixing" in space which in turn implies the fast mixing of the block dynamics. The following Theorem 5.2.2 can be seen as the combination of Theorems 3.4 and 5.3 of [MSW04] adapted to the component dynamics (the notation here is closer to Theorem 5.1 of [Bha+11]). For completeness, we include an outline of the proof in Section 5.5, highlighting the differences from [MSW04].

Theorem 5.2.2. *There exists some constant $\alpha > 0$ such that for every $\delta > 0$ and $l \geqslant 1$ the following statement holds: If for all $x \in T$ that is at least l levels from the leaves and all compatible pairs of states $c, c' \in [k]$, the conditional measure $\mu^c = \mu^c_{T_x}$ satisfies*

$$\mathbb{P}_{\tau\sim\mu^c}\left(\left|\frac{\mu^c(\sigma_x = c' \mid \sigma \sim_{B_{x,l}} \tau)}{\mu^c(\sigma_x = c')} - 1\right| \geqslant \frac{(1-\delta)^2}{\alpha(l+1-\delta)^2}\right) \leqslant e^{-2\alpha(l+1-\delta)^2/(1-\delta)^2}, \tag{5.2.2}$$

then for every function $f \geqslant 0$, $\mathrm{Ent}(f) \leqslant \frac{2}{\delta}\mathcal{E}^*_l$.

To prove Theorem 5.1.1, it suffices to verify (5.2.2) for some choice of l and δ. We first show a weaker inequality (5.2.3) in the following theorem. Note that the same inequality is proved in Theorem 5.3 of [MSW04] or Theorem 5.1 of [Bha+11] for specific models such as the coloring model. Here we provide a different proof that works for general models using only non-reconstruction.

Theorem 5.2.3. *For a k-state system M, if M is non-reconstructible and $d\lambda^2 < 1$, then for any $\alpha > 0, 0 < \delta < 1$, there exist $l_0 \geqslant 1$ such that for all $l \geqslant l_0$, every $x \in T$ that is at least l levels from the leaves, and any pair of compatible states $c, c' \in [k]$, $\mu^c = \mu^c_{T_x}$ satisfies*

$$\mathbb{P}_{\tau\sim\mu^c}\left(\left|\frac{\mu^c(\sigma_x = c' \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}})}{\mu^c(\sigma_x = c')} - 1\right| \geqslant \frac{(1-\delta)^2}{\alpha(l+1-\delta)^2}\right) \leqslant e^{-2\alpha(l+1-\delta)^2/(1-\delta)^2} \tag{5.2.3}$$

The difference between (5.2.2) and (5.2.3) is that in equation (5.2.2), the inner measure μ^c conditions not only on the boundary condition $\sigma_{L_{x,l}} = \tau_{L_{x,l}}$, but also the connected component of τ. We will show that under connectivity condition $\mathcal{C}$, the difference between $\sigma \sim_{B_{x,l}} \tau$ and $\sigma_{L_{x,l}} = \tau_{L_{x,l}}$ is negligible in the upper half of a large block, hence (5.2.2) holds.

Lemma 5.2.4. *Let M be a k-state system satisfying $\mathcal{C}$ such that (5.2.3) holds for $l \geqslant l_0$ and $\delta = \delta_0$. Then there exist constants $l_1 \geqslant 2l_0$ and $\delta_1 \geqslant \delta_0$ such that for all $l \geqslant l_1$, equation (5.2.2) holds with $\delta = \delta_1$.*

Theorems 5.2.2 and 5.2.3 and Lemma 5.2.4 together imply Theorem 5.1.1. The rest of the chapter is structured as follows: We will prove Theorem 5.2.3 in Section 5.3 and Lemma 5.2.4 in Section 5.4, and we will include a sketch of Theorem 5.2.2 in Section 5.5. After that we will apply the result to the k-coloring model and prove Theorem 4 in Section 5.6.

5.3 Proof of Theorem 5.2.3

In this section we prove Theorem 5.2.3. The result for the k-coloring model was proved in [Bha+11], which used the specific structure of coloring model. Here we will give a different proof for general systems M using only non-reconstruction and $d\lambda^2 < 1$. We first introduce some notations. Recall that the stationary distribution of M is π. For $x \in T$, let

$$\tilde{R}_{x,l}(\tau)(c) = \frac{1}{\pi(c)}\mu_{T_x}(\sigma_x = c \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}})$$

denote the ratio of conditional and unconditional distribution at x and write $R_{x,l}(\tau) = \|\tilde{R}_{x,l}(\tau) - 1\|_\infty = \max_{c\in[k]} |\tilde{R}_{x,l}(\tau)(c) - 1|$. We will omit τ when it is clear from context. In the proof we will work with the unconditional Gibbs measure $\mu = \mu_{T_x}$ and π instead of $\mu^c_{T_x}$ and $\mu^c_{T_x}(\sigma_x = c')$ and show the following stronger inequality.

Theorem 5.3.1. *Under the assumptions of Theorem 5.2.3, there exists constant $\xi > 0$ and $l_0 > 0$, such that for all $l \geqslant l_0$, every $x \in T$ that is at least l levels from the leaves, $\mu = \mu_{T_x}$ satisfies*

$$\mathbb{P}_{\tau\sim\mu}\left(R_{x,l}(\tau) \geqslant e^{-\xi l}\right) \leqslant \exp(-e^{\xi l}). \tag{5.3.1}$$

Proof of Theorem 5.2.3. To see that (5.3.1) implies (5.2.3), consider the Markov chain construction of σ. Let E_x be the edge set of T_x, we have

$$\mu(\sigma) = \pi(\sigma_x)\prod_{(y,z)\in E_x} M(\sigma_y, \sigma_z),\ \mu^c(\sigma) = M(c, \sigma_x)\prod_{(y,z)\in E_x} M(\sigma_y, \sigma_z).$$

Hence for any event $A \subseteq \Omega_{T_x}$,

$$\mathbb{P}_{\tau\sim\mu^c}(A) = \sum_{\tau\in A}\mu^c(\tau) = \sum_{\tau\in A}\frac{M(c,\tau_x)}{\pi(\tau_x)}\mu(\tau) \leqslant \pi_{\min}^{-1}\mu(A) = \pi_{\min}^{-1}\mathbb{P}_{\tau\sim\mu}(A),$$

where $\pi_{\min} = \min_{c\in[k]}\pi(c) > 0$. Note that

$$\left|\frac{\mu^c(\sigma_x = c' \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}})}{\mu^c(\sigma_x = c')} - 1\right| = \left|\frac{1}{\pi(c')}\mu(\sigma_x = c' \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}}) - 1\right| \leqslant R_{x,l}(\tau).$$

It follows that

$$\mathbb{P}_{\tau\sim\mu^c}\left(\left|\frac{\mu^c(\sigma_x = c' \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}})}{\mu^c(\sigma_x = c')} - 1\right| \geqslant e^{-\xi l}\right) \leqslant \pi_{\min}^{-1}\exp(-e^{\xi l}).$$

Theorem 5.2.3 then follows by taking l_0 large enough such that $\exp(-\xi l_0) \leqslant (1-\delta)^2/\alpha(l_0 - 1 + \delta)^2$. $\square$

In the rest of the section we assume that M satisfies the assumptions of Theorem 5.3.1. The following lemma gives the recursive relation of $\tilde{R}_{x,l}(c)$.

Lemma 5.3.2. *Fix $\tau \in \Omega_T$ and $x \in T$ and let $x_1, \dots, x_d$ denote the d children of x. $\tilde{R}_{x,l}$ can be written as a rational function of $\tilde{R}_{x_i,l-1}$:*

$$\tilde{R}_{x,l}(c) = \frac{\prod_{i=1}^d M\tilde{R}_{x_i,l-1}}{\pi \prod_{i=1}^d M\tilde{R}_{x_i,l-1}}(c) = \frac{\prod_{i=1}^d \sum_{c_i \in [k]} M(c,c_i)\tilde{R}_{x_i,l-1}(c_i)}{\sum_{c' \in [k]} \pi(c') \prod_{i=1}^d \sum_{c_i \in [k]} M(c',c_i)\tilde{R}_{x_i,l-1}(c_i)}. \tag{5.3.2}$$

Proof. Let E_x and E_{x_i} denote the edge set of T_x and T_{x_i}, they satisfy that

$$E_x = \cup_i \left(E_{x_i} \cup \{(x, x_i)\}\right).$$

Let $\Omega_x(c) = \{\sigma : \sigma_x = c, \sigma_{L_{x,l}} = \tau_{L_{x,l}}\}$ and $\Omega_{x_i}(c) = \{\sigma : \sigma_{x_i} = c, \sigma_{L_{x_i,l-1}} = \tau_{L_{x_i,l-1}}\}$ be the set of configurations on T_x and T_{x_i} with boundary condition τ. By the Markov chain construction, we have

$$\begin{aligned}
\mu(\Omega_x(c)) &= \mu(\sigma_x = c, \sigma_{L_{x,l}} = \tau_{L_{x,l}}) \\
&= \sum_{\sigma \in \Omega_x(c)} \pi(c) \prod_{(y,z)\in E} M(\sigma_y, \sigma_z) = \sum_{c_1,\cdots,c_d \in [k]} \pi(c) \prod_{i=1}^d M(c, c_i) \sum_{\sigma^i \in \Omega_i(c_i)} \prod_{(y,z)\in E_i} M(\sigma^i_y, \sigma^i_z) \\
&= \sum_{c_1,\cdots,c_d \in [k]} \pi(c) \prod_{i=1}^d \frac{M(c,c_i)}{\pi_{c_i}} \mu(\Omega_i(c_i)) = \pi(c) \prod_{i=1}^d \sum_{c_i \in [k]} \frac{M(c,c_i)}{\pi_{c_i}} \mu(\Omega_i(c_i)).
\end{aligned}$$

Therefore by Bayes formula,

$$\begin{aligned}
\tilde{R}_{x,l}(c) &= \frac{1}{\pi(c)} \mu(\sigma_x = c \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}}) = \frac{1}{\pi(c)} \frac{\mu(\Omega_x(c))}{\sum_{c' \in [k]} \mu(\Omega(c'))} \\
&= \frac{\prod_{i=1}^d \sum_{c_i \in [k]} \frac{M(c,c_i)}{\pi_{c_i}} \mu(\Omega_i(c_i))}{\sum_{c' \in [k]} \pi(c') \prod_{i=1}^d \sum_{c_i \in [k]} \frac{M(c',c_i)}{\pi_{c_i}} \mu(\Omega_i(c_i))} \\
&= \frac{\prod_{i=1}^d \sum_{c_i \in [k]} M(c,c_i)\tilde{R}_{x_i,l-1}(c_i)}{\sum_{c' \in [k]} \pi(c') \prod_{i=1}^d \sum_{c_i \in [k]} M(c',c_i)\tilde{R}_{x_i,l-1}(c_i)}.
\end{aligned}$$

where the last step followed by dividing $\prod_{i=1}^d \sum_{c_i' \in [k]} \mu(\Omega_i(c_i'))$ from the numerator and the denominator. □

Observe that in the recursive relationship of (5.3.2), $\tilde{R}_{x,l}(c)$ is a rational function of $\tilde{R}_{x_i,l-1}, i = 1, \dots, d$, where $\tilde{R}_{x,l}$ takes values from the k dimensional simplex $\Delta_{[k]} = \{R \in \mathbb{R}^k : \pi R = 1, R_i \geqslant 0, i = 1, \dots, k\}$. The next lemma establishes a contraction property of $R_{x,l}$, using the continuity of (5.3.2) and the ergodicity of M.

Lemma 5.3.3. *There exist an integer $m \geqslant 1$ and constant $\epsilon > 0$ such that for all d^m vertices $y_1, \dots, y_{d^m} \in L_{x,m}$, if at most one y_i has $R_{y_i,l-m} > \epsilon$ then*

$$R_{x,l} \leqslant \frac{1}{2} \sum_{i=1}^{d^m} R_{y_i,l-m}. \tag{5.3.3}$$

Proof. Let $f : \Delta_{[k]}^d \to \Delta_{[k]}$ be the function on the RHS of (5.3.2) such that $\tilde{R}_{x,l} = f(\tilde{R}_{x_1,l-1}, \ldots, \tilde{R}_{x_d,l-1})$. Observe from (5.3.2) that f is a rational function with $f(1,\ldots,1) = 1$. When $\tilde{R}_{x_2,l-1} = \cdots = \tilde{R}_{x_d,l-1} = 1$, f can be simplified as

$$\tilde{R}_{x,l} = f(\tilde{R}_{x_1,l-1}, 1, \ldots, 1) = \frac{M\tilde{R}_{x_1,l-1}}{\pi M \tilde{R}_{x_1,l-1}} = M\tilde{R}_{x_1,l-1}.$$

Iterating the function m times, we can write $\tilde{R}_{x,l} = f^{(m)}(\tilde{R}_{y_1,l-m}, \ldots, \tilde{R}_{y_{d^m},l-m})$ where $f^{(m)} : \Delta_{[k]}^{d^m} \to \Delta_{[k]}$ is another rational function. A similar calculation shows when $\tilde{R}_{y_2,l-m} = \cdots = \tilde{R}_{y_{d^m},l-m} = 1$,

$$\tilde{R}_{x,l} = f^{(m)}(\tilde{R}_{y_1,l-m}, 1, \ldots, 1) = M^m \tilde{R}_{y_1,l-m}.$$

Since $f^{(m)}$ is a smooth function in any regions without poles, there exists constant $C_1 = C_1(d,m,M)$ such that in the local neighborhood of $(1,\ldots,1)$

$$\|\tilde{R}_{x,l} - 1 - \sum_{i=1}^{d^m}(M^m\tilde{R}_{y_i,l-m} - 1)\| \leqslant C_1 \sum_{i=1}^{d^m} \|\tilde{R}_{y_i,l-m} - 1\|^2 \leqslant C_1 k \sum_{i=1}^{d^m} \|\tilde{R}_{y_i,l-m} - 1\|_\infty^2.$$

By the ergodicity of M, for sufficiently large m and all $\tilde{R} \in \Delta_{[k]}$ we have $\|M^m\tilde{R} - 1\|_\infty \leqslant \frac{1}{4}\|\tilde{R} - 1\|_\infty$. Therefore there exists $\epsilon_1 = \epsilon_1(C_1, k)$ such that if $R_{y_i,l-m} \leqslant \epsilon_1$ for all vertices $y_i \in L_{x,m}$ then

$$\|\tilde{R}_{x,l} - 1\|_\infty \leqslant (\frac{1}{4} + C_1 k\epsilon_1) \sum_{i=1}^{d^m} \|\tilde{R}_{y_i,l-m} - 1\|_\infty \leqslant \frac{1}{2}\sum_{i=1}^{d^m} R_{y_i,l-m}. \tag{5.3.4}$$

This suffices provided that there are no large $R_{y_i,l-m}$.

We now consider the case when there is one large $R_{y_i,l-m}$, which we can without loss of generality assume is $i = 1$. Again since $f^{(m)}$ is smooth, there exists $C_2, \epsilon_2 > 0$ such that for all $\tilde{R}_{y_1,l-m} > \epsilon_1$, if $\sup_{i\geqslant 2} R_{y_i,l-m} \leqslant \epsilon_2$ then

$$\|\tilde{R}_{x,l} - M^m\tilde{R}_{y_1,l-m}\| \leqslant C_2 \sum_{i=2}^{d^m} \|\tilde{R}_{y_i,l-m} - 1\|.$$

Let $\epsilon = \epsilon_2 \wedge (4C_2 d^m k)^{-1}\epsilon_1$, if we moreover have $\sup_{i\geqslant 2} R_{y_i,l-m} \leqslant \epsilon$, then

$$\|\tilde{R}_{x,l} - 1\|_\infty \leqslant \frac{1}{4}\|\tilde{R}_{y_1,l-m} - 1\|_\infty + C_2 d^m k\epsilon \leqslant \frac{1}{4}R_{y_1,l-m} + \frac{1}{4}\epsilon_1 \leqslant \frac{1}{2}R_{y_1,l-m}. \tag{5.3.5}$$

Combining equations (5.3.4) and (5.3.5) and noting that $\epsilon < \epsilon_1$ completes the proof. □

So far we have not used the assumption of non-reconstruction and $d\lambda^2 < 1$. In [JM04], Janson and Mossel introduced the notion of "robust reconstruction" and showed the following result: (rephrased to the notations here)

Theorem 5.3.4 (Lemma 2.7 and Lemma 2.8 of [JM04]). *If M is ergodic and $d\lambda^2 < 1$, then there exist constants $C_1 = C_1(d) > 0$ and $\delta = \delta(d) > 0$ such that for any $l \geqslant 1$ if $d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}) \leqslant \delta$ for all $c \in [k]$, then*

$$d_{\mathrm{TV}}(\mu^c_{L_{l+1}}, \mu_{L_{l+1}}) \leqslant e^{-C_1} d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}), \quad \text{for all } c \in [k].$$

Theorem 5.3.4 combined with non-reconstruction implies the following weaker concentration inequality.

Corollary 5.3.5. *Under the assumptions of Theorem 5.3.1, there exists constant $C_1, C_2 > 0$ such that*

$$\mathbb{P}_{\tau\sim\mu}(R_{x,l} > z) \leqslant \frac{C_2}{z} e^{-C_1 l}. \tag{5.3.6}$$

Proof. By the definition of non-reconstruction, $\lim_{l\to\infty} d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}) = 0$. Hence for sufficiently large l, $d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}) \leqslant \delta$ and by induction there exists constant $C_2 > 0$ that

$$d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}) \leqslant C_2 e^{-C_1 l}.$$

A duality argument then shows that

$$\begin{aligned}\mathbb{E}_{\tau\sim\mu}|\tilde{R}_{x,l}(c) - 1| &= \mathbb{E}_{\tau\sim\mu}\left|\frac{1}{\pi(c)}\mu(\sigma_x = c \mid \sigma_{L_{x,l}} = \tau_{L_{x,l}}) - 1\right| = \mathbb{E}_{\tau\sim\mu}\left|\frac{\mu^c(\sigma_{L_{x,l}} = \tau_{L_{x,l}})}{\mu(\sigma_{L_{x,l}} = \tau_{L_{x,l}})} - 1\right| \\ &= \sum_{\tau}\left|\mu^c(\sigma_{L_{x,l}} = \tau_{L_{x,l}}) - \mu(\sigma_{L_{x,l}} = \tau_{L_{x,l}})\right| = 2d_{\mathrm{TV}}(\mu^c_{L_l}, \mu_{L_l}) \leqslant 2C_2 e^{-C_1 l}.\end{aligned}$$

Maximizing over $c \in [k]$ we get $\mathbb{E}_{\tau\sim\mu} R_{x,l} \leqslant C_2 e^{-C_1 l}$ for some (different) constant $C_1, C_2 > 0$ and (5.3.6) follows by Markov's inequality. □

Finally we improve the concentration bound of (5.3.6) using Lemma 5.3.3.

Proof of Theorem 5.3.1. By Lemma 5.3.3, the event $R_{x,l} > z$ implies that either there exist two $i \in [d^m]$ such that $R_{y_i,l-m} > \epsilon$ or $\sum_{i=1}^{d^m} R_{y_i,l-m} > 2z$. In the second case if the event $\sum_{i=1}^{d^m} R_{y_i,l-m} > 2z$ holds and for every y_i, $R_{y_i,l-m} \leqslant \frac{3}{2}z$, then there must exist at least two i such that $R_{y_i,l-m} > \frac{1}{2d^m}z$, otherwise $\sum_{i=1}^{d^m} R_{y_i,l-m} \leqslant \frac{3}{2}z + \frac{d^m-1}{2d^m}z < 2z$. Therefore we can write

$$\begin{aligned}\mathbb{P}_{\tau\sim\mu}(R_{x,l} > z) \leqslant\ & \mathbb{P}_{\tau\sim\mu}(\exists \text{ two } y_i \in L_{x,m}, R_{y_i,l-m} > \epsilon) + \mathbb{P}_{\tau\sim\mu}(\exists y_i \in L_{x,m}, R_{y_i,l-m} > \frac{3}{2}z) \\ &+ \mathbb{P}_{\tau\sim\mu}(\exists \text{ two } y_i \in L_{x,m}, R_{y_i,l-m} > \frac{1}{2d^m}z).\end{aligned}$$

Let $g(z,l) = \mathbb{P}_{\tau\sim\mu}(R_{x,l} > z)$ and $C = \max\{2d^m, \frac{1}{\epsilon\pi_{\min}}\}$, note $g(z,l)$ is a decreasing function in z, the equation above become

$$\begin{aligned}g(z,l) &\leqslant d^{2m} g^2(\epsilon, l-m) + d^m g(\frac{3}{2}z, l-m) + d^{2m} g^2(\frac{1}{2d^m}z, l-m) \\ &\leqslant d^m g(\frac{3}{2}z, l-m) + 2d^{2m} g^2(\frac{1}{C}z, l-m).\end{aligned}$$

Iterating this estimation h times, we have

$$g(z,l) \leqslant \sum_{i=0}^{h} (2d^{2m})^{2^{h-i}(1+i)} g^{2^{h-i}} \left((\frac{3}{2})^i (\frac{1}{C})^{h-i} z, l - hm \right). \tag{5.3.7}$$

where the coefficient can be shown by induction on h using inequality $(a+b)^2 \leqslant 2(a^2+b^2)$.

Since for all $z > \pi_{\min}^{-1}$ we have $g(z,l) = 0$, the summand on the RHS of (5.3.7) is zero for large i. Fix $\kappa = \ln \frac{4}{3}C / \ln \frac{3}{2}C < 1$, for $h \geqslant \ln(\frac{1}{z\pi_{\min}})/\ln(\frac{4}{3})$ and $i > \kappa h$, we have $(\frac{3}{2})^i(\frac{1}{C})^{h-i}z > \pi_{\min}^{-1}$. Therefore

$$g(z,l) \leqslant \sum_{i=0}^{\kappa h} (2d^{2m})^{2^{h-i}(1+i)} g^{2^{h-i}} \left((\frac{3}{2})^i (\frac{1}{C})^{h-i} z, l - hm \right) \leqslant \kappa h \left[(2d^{2m})^h g \left(C^{-h} z, l - hm \right) \right]^{2^{(1-\kappa)h}}$$

Now apply (5.3.6) and let $h = rl/m$ for small $r > 0$ such that $(1-r)C_1 - r \cdot \frac{1}{m} \ln(2Cd^{2m}) > \frac{1}{2}C_1 > 0$. For large enough l such that $\ln l \leqslant 2^{\frac{(1-\kappa)r}{m} l}$, we have

$$\begin{aligned} g(z,l) &\leqslant \kappa h \left((2d^{2m})^h \frac{C_2 C^h}{z} e^{-C_1(l-hm)} \right)^{2^{(1-\kappa)h}} \\ &\leqslant \frac{\kappa r}{m} l \left(\frac{C_2}{z} (2Cd^{2m})^{\frac{r}{m} l} e^{-C_1(1-r)l} \right)^{2^{\frac{(1-\kappa)r}{m} l}} \leqslant \frac{\kappa r}{m} \left(\frac{2C_2}{z} e^{-\frac{1}{2}C_1 l} \right)^{2^{\frac{(1-\kappa)r}{m} l}}. \end{aligned}$$

Let $C_3 = \frac{2}{C_1}, C_4 = \frac{\kappa r}{m}$, $C_5 = \frac{(1-\kappa)r}{m} \ln 2$. For $l > C_3(1 + \ln 2C_2 - \ln z)$, we have $g(z,l) \leqslant C_4 \exp\{-\exp(C_5 l)\}$.

Finally define $\xi = \frac{1}{2}\min\{C_3^{-1}, C_5\}$, plug in $z_l = \exp(-\xi l)$. When l is large enough, we have $C_3(1 + \ln 2C_2 - \ln z) \leqslant C_3(1 + \ln 2C_2) + \frac{1}{2}l < l$ and $\exp(\exp(\frac{1}{2}C_5 l)) > C_4$, therefore

$$\mathbb{P}_{\tau\sim\mu}\left(R_{x,l}(\tau) \geqslant e^{-\xi l} \right) = g(z_l, l) \leqslant C_4 \exp(-e^{C_5 l}) \leqslant \exp(-e^{\xi l}),$$

completing the proof. □

5.4 Proof of Lemma 5.2.4

The proof of Lemma 5.2.4 contains two steps. First for block $B_{x,l}$ with sufficiently large l, we study the measure $\mu^{*,\tau}_{B_{x,l}}$ induced on the upper half of block $B_{x,l/2}$ (here and throughout the section, we choose l to be even) and consider the following subset of $\Omega^\tau_{B_{x,l}}$,

$$A_\tau = \{\sigma \in \Omega^\tau_{B_{x,l}} : \forall x \in L_{x,l/2+2},\ x \text{ is free w.r.t. } \sigma\}.$$

A_τ can be considered as the set of "good" configurations with boundary condition τ. As we will show later, under connectivity condition $\mathcal{C}$, $\mu^{*,\tau}_{B_{x,l}}(A_\tau)$ is close to 1 with high probability. And as the following lemma claims, conditioning on A_τ and the configuration on $L_{x,l/2}$, the boundary of $B_{x,l/2}$, the marginal of x induced by $\mu^{*,\tau}_{B_{x,l}}$ equals to the marginal induced by μ^c. Therefore, as a second step we can apply the result of Theorem 5.2.3 to $B_{x,l/2}$. Let $\Omega_{L_{x,l/2}}$ be the set of configuration on $L_{x,l/2}$. Throughout the section, we assume that M satisfies the connectivity condition $\mathcal{C}$.

Lemma 5.4.1. *For arbitrary $\tau \in \Omega^c_{T_x}$, $\eta \in \Omega_{L_{x,l/2}}$ and state $c' \in [k]$ that is compatible with c,*

$$\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta, \sigma \in A_\tau) = \mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta). \tag{5.4.1}$$

Proof. For convenience of notation, abbreviate $\sigma_{(1)} = \sigma_{B_{x,l/2-1}}$, $\sigma_{(2)} = \sigma_{B_{x,l}\backslash B_{x,l/2}}$, so every configuration $\sigma \in \Omega_{B_{x,l}}$ can be written as a three tuple $(\sigma_{(1)}, \eta, \sigma_{(2)})$. We of course have that $\sigma_{(1)}, \sigma_{(2)}$ are conditionally independent given $\sigma_{L_{x,l/2}} = \eta$. By the definition of A_τ, $\{\sigma \in A_\tau\}$ only depends on $\sigma_{(2)}$. Therefore to show (5.4.1), it is enough to show that conditioned on $\sigma_{L_{x,l/2}}$ and $\sigma \in A_\tau$, $\sigma \sim \tau$ is independent of $\sigma_{(1)}$. From there we have

$$\begin{aligned}\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta, \sigma \in A_\tau) &= \mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta, \sigma \sim \tau, \sigma \in A_\tau)\\ &= \mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta, \sigma \in A_\tau) = \mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta).\end{aligned}$$

Since "$\sim$" is a transitive relation, the conditional independence of $\sigma \sim \tau$ and $\sigma_{(1)}$ follows from the following claim. □

Claim 5.4.2. For each $\tau \in \Omega^c_{T_x}$, $\eta \in \Omega_{L_{x,l/2}}$ and for all $\sigma = (\sigma_{(1)}, \eta, \sigma_{(2)})$, $\sigma' = (\sigma'_{(1)}, \eta, \sigma_{(2)}) \in \Omega^\tau_{B_{x,l}}$ if $\sigma, \sigma' \in A_\tau$, then $\sigma \sim \sigma'$.

Proof. For each $x \in T$, let $p(x)$ denote the parent of x. By Lemma 5.2.1, there exists a path Γ connecting $\sigma_{(1)}$ to $\sigma'_{(1)}$ in $\Omega^c_{B_{x,l/2}}$ via valid moves of the Glauber dynamics on $B_{x,l/2}$ with $\sigma_{p(x)} = c$ and free boundary condition on $L_{x,l/2}$. We will construct a path Γ' in $\Omega^\tau_{B_{x,l}}$ connecting σ to σ' by adding steps between steps of Γ which only changes the configuration on $B_{x,l}\backslash B_{x,l/2}$, such that vertices in $L_{x,l/2+1}$ won't block the moves in Γ and after finishing Γ, we can change the configuration on $B_{x,l}\backslash B_{x,l/2}$ back to the original $\sigma_{(2)}$. The construction of Γ' is specified below:

(1) **Before starting Γ.** For each $y \in L_{x,l/2+2}$, $\sigma \in A_\tau$ implies that there exists a path Γ_y in T_y changing y from σ_y to $\sigma_{p(p(y))} = \eta_{p(p(y))}$ in one step. To see Γ_y is also a connected path in $B_{x,l}$, we have to show that the parent of y won't block Γ_y. The only neighbor of $p(y)$ in T_y is y and the only move involving y in Γ_y is the last step changing y from σ_y to $\sigma_{p(p(y))}$. The value of $p(y)$ won't block this last step because $\sigma_{p(y)}$ is compatible with both σ_y and $\sigma_{p(p(y))}$ (they are states of neighboring vertices in σ). Now we will concatenate the Γ_y's for each $y \in L_{x+l/2+2}$ and change σ_y to $\sigma_{p(p(y))}$. After that, for each $w \in L_{x,l/2}$, all vertices in $L_{w,2}$ are in state $\sigma_w = \eta_w$. The configuration on and below $L_{x,l/2+2}$ will henceforth remain fixed until we finish Γ.

(2) **Performing Γ.** For each step in Γ, the existence of $B_{x,l-1}\backslash B_{x,l/2}$ might block this move only if it changes the state of some vertex $w \in L_{x,l/2}$. Suppose it changes w from c_1 to c_2. Remember in the construction above, all vertices in $L_{w,2}$ have states η_w. By part 1 of $\mathcal{C}$,

we can find $c_3 \in [k]$ which is compatible with c_1, c_2 and η_w. Now in order to change w from c_1 to c_2, it suffices to first change the state of every vertex $z \in L_{w,1}$ to c_3, and then change w from c_1 to c_2. This construction keeps the configuration on and below $L_{x,l/2+2}$ unchanged.

(3) **After Γ.** After the moves in Γ, the configuration in $B_{x,l/2}$ is $(\sigma'_{(1)}, \eta)$. We can change every vertex $z \in L_{x,l/2+1}$ back to $\sigma'_z = \sigma_z$ because at this moment its parent $p(z) \in L_{x,l/2}$ and all children of z in $L_{z,1}$ have state $\eta_{p(z)} = \sigma_{p(z)}$, which is compatible with σ_z. From there, we can reverse the path Γ_y for each $y \in L_{x,l/2+2}$ and change the configuration on and below $L_{x,l/2+2}$ back to the original configuration $\sigma_{(2)}$. This completes the construction achieving $\sigma'_{(2)} = \sigma_{(2)}$. $\square$

Lemma 5.4.3. *There exist constants $C_1 > 1$, $C_2 > 0$ such that for all $l \geqslant 1$,*

$$1 - p_l^{\text{free}} \leqslant C_2 \exp(-C_1^l). \tag{5.4.2}$$

Proof. Fix $x \in T$ and $\sigma \in \Omega_{T_x}$. First if for all $1 \leqslant i \leqslant d$, $z_i \in L_{x,1}$ is free, then x is also free. To see that, for any $c \in [k]$, by connectivity condition there exists $c' \in [k]$ such that c' is compatible with both c and σ_x, we can first change all z_i to c' in one step and then change x from σ_x to c as the final step.

Now consider the set of y_{ij}'s where $y_{ij} \in L_{z_i,1} \subset L_{x,2}$ for $1 \leqslant i, j \leqslant d$. If at most one of the y_{ij}'s is not free, say $y_{11} \in L_{z_1,1}$, then for each $i \neq 1$, z_i is free and z_1 can change in one step to all states compatible with $\sigma_{y_{11}}$. Again by $\mathcal{C}$, for all $c \in [k]$ there exists $c' \in [k]$ such that c' is compatible with c, σ_x and $\sigma_{y_{11}}$. By the construction above, we can change x from σ_x to c in one step, hence x is also free.

This implies if x is not free, then there exist at least two $y_{ij} \in L_{x,2}$ that are not free. By part 2 of $\mathcal{C}$, there exists $l_0 > 0$, such that for all $l > l_0$ we have $1 - p_l^{\text{free}} < 1/d^8$ and hence

$$1 - p_l^{\text{free}} \leqslant \binom{d^2}{2}(1 - p_{l-2}^{\text{free}})^2 \leqslant d^4(1 - p_{l-2}^{\text{free}})^2 \leqslant (1 - p_{l-2}^{\text{free}})^{1.5}.$$

By induction, $1 - p_l^{\text{free}} \leqslant (1 - p_{l_0}^{\text{free}})^{(1.5)^{(l-l_0)/2}}$ which completes the proof. $\square$

Remark 5.4.4. Claim 5.4.2 and Lemma 5.4.3 are the two main places where connectivity conditions are used: The first part of condition $\mathcal{C}$ is used in the construction of Γ'. It might be possible circumvented the assumption by using more carefully constructed paths. However this would be purely technical and not the main interest of this chapter. The second part of condition $\mathcal{C}$ is used to show that A_τ happens with high probability.

Note that Claim 5.4.2 implies that when restricted to A_τ, the fixed boundary Glauber dynamics on $B_{x,l/2}$ is irreducible as a subgraph of the Glauber dynamic on the larger block $B_{x,l}$. It is possible to replace the current connectivity condition by general assumptions bounding the probability of the later events directly.

Now we can finish the proof of Lemma 5.2.4, from which Theorem 5.1.1 follows immediately.

Proof of Lemma 5.2.4. Let $C = \alpha(l/2+1-\delta)^2/[(1-\delta)^2\mu^c(\sigma_x = c')]$ be the quantity on the left hand side of (5.2.3). It is enough to show that there exist constants $l_1 \geqslant 2l_0$, $K \geqslant 1$ such that for all $l \geqslant l_1$

$$\mathbb{P}_{\tau\sim\mu^c}\left(|\mu^c(\sigma_x = c' \mid \sigma \sim \tau) - \mu^c(\sigma_x = c')| \geqslant \frac{K}{C}\right) \leqslant e^{-2C/K}.$$

To see the sufficiency, note that this is just equation (5.2.2) with δ_1 satisfying $1-\delta_1 = \frac{1}{4K}(1-\delta)$.

Recall $A_\tau = \{\sigma \in \Omega^\tau_{B_{x,l}} : \forall x \in L_{x,l/2+2}, x \text{ is free in } \sigma\}$. Lemma 5.4.3 implies that for some constant $C_1 > 1$, $C_2 > 0$, and $l \geqslant 1$

$$\begin{aligned}\mathbb{E}_{\tau\sim\mu^c}(\mu^{*,\tau}_{B_{x,l}}(A^c_\tau)) &= \mathbb{E}_{\tau\sim\mu^c}(\mu^c(\sigma \notin A_\tau \mid \sigma\sim\tau)) \\ &= \mathbb{P}_{\sigma\sim\mu^c}(\exists y \in L_{x,l/2+2}, y \text{ is not free }) \\ &\leqslant d^{l/2+2}(1-p^{\text{free}}_{l/2-2}) \leqslant C_2 d^{l/2+2}\exp(-C_1^{l/2-2}).\end{aligned}$$

By Markov inequality,

$$\mathbb{P}_{\tau\sim\mu^c}\left(\mu^{*,\tau}_{B_{x,l}}(A^c_\tau) > \frac{1}{2C}\right) \leqslant 2C\mathbb{E}_{\tau\sim\mu^c}(\mu^{*,\tau}_{B_{x,l}}(A^c_\tau)) \leqslant Cd^{l/2+2}C_2\exp(-C_1^{l/2-2}) \to 0, \quad (5.4.3)$$

as $l\to\infty$. On the event $\{\tau : \mu^{*,\tau}_{B_{x,l}}(A^c_\tau) \leqslant \frac{1}{2C}\}$,

$$\begin{aligned}&\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau) \leqslant \frac{\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c')}{\mu^{*,\tau}_{B_{x,l}}(\sigma\in A_\tau)} \leqslant \mu^{*,\tau}_{B_{x,l}}(\sigma_x = c') + \frac{1}{C}, \\ &\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau) \geqslant \mu^{*,\tau}_{B_{x,l}}(\sigma_x = c', \sigma\in A_\tau) \geqslant \mu^{*,\tau}_{B_{x,l}}(\sigma_x = c') - \frac{1}{C}. \end{aligned} \quad (5.4.4)$$

Combining the two results together we have

$$\left|\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c') - \mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau)\right| \leqslant \frac{1}{C}. \quad (5.4.5)$$

Now splitting $\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau)$ according to $\sigma_{L_{x,l/2}}$ and applying Lemma 5.4.1, we have

$$\begin{aligned}\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau) &= \sum_\eta \mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma\in A_\tau, \sigma_{L_{x,l/2}} = \eta)\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{x,l/2}} = \eta \mid \sigma\in A_\tau) \\ &= \sum_\eta \mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta)\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{x,l/2}} = \eta \mid \sigma\in A_\tau). \end{aligned} \quad (5.4.6)$$

We would like to estimate the set of η such that $\mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta)$ has a large bias. Let

$$B = \{\eta : \left|\mu^c(\sigma_x = c' \mid \sigma_{L_{x,l/2}} = \eta) - \mu^c(\sigma_x = c')\right| \geqslant \frac{1}{C}\}.$$

Theorem 5.2.3 implies that for $l/2 \geqslant l_0$ and some $\delta > 0$, we have $\mathbb{P}_{\eta\sim\mu^c}(B) \leqslant e^{-2C}$, where $\eta \sim \mu^c$ denotes the measure μ^c induced on $L_{x,l/2}$. Again by Markov's inequality,

$$\mathbb{P}_{\tau\sim\mu^c}(\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{x,l/2}} \in B) > \frac{1}{C}) \leqslant C\mathbb{E}_{\tau\sim\mu^c}\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{x,l/2}} \in B) = C\mu^c(B) \leqslant Ce^{-2C}. \tag{5.4.7}$$

On the event $\{\tau : \mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} \in B) \leqslant \frac{1}{C}\} \cap \{\tau : \mu^{*,\tau}_{B_{x,l}}(A^c_\tau) \leqslant \frac{1}{2C}\}$, from (5.4.6) we have

$$\begin{aligned}\left|\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c' \mid \sigma \in A_\tau) - \mu^c(\sigma_x = c')\right| &\leqslant \sum_\eta \left|\mu^c(\sigma_x = c' \mid \sigma_{L_{l/2}} = \eta) - \mu^c(\sigma_x = c')\right| \mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} = \eta \mid \sigma \in A_\tau) \\ &\leqslant \sum_{\eta\in B^c} \frac{1}{C}\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} = \eta \mid \sigma \in A_\tau) + \mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} \in B \mid \sigma \in A_\tau) \\ &\leqslant \frac{1}{C}\cdot 1 + \frac{1}{C} + \frac{1}{C} = \frac{3}{C} \end{aligned} \tag{5.4.8}$$

where the last inequality follows from similar argument to (5.4.4).

Combining the result of equations (5.4.5) and (5.4.8), on the event $\{\tau : \mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} \in B) \leqslant \frac{1}{C}\} \cap \{\tau : \mu^{*,\tau}_{B_{x,l}}(A^c_\tau) \leqslant \frac{1}{2C}\}$, we have

$$\left|\mu^{*,\tau}_{B_{x,l}}(\sigma_x = c') - \mu^c(\sigma_x = c')\right| \leqslant \frac{3}{C} + \frac{3}{C} = \frac{6}{C}.$$

Therefore using the bounds from (5.4.3) and (5.4.7), for all $l \geqslant 2l_0$,

$$\begin{aligned}\mathbb{P}_{\tau\sim\mu^c}\left(|\mu^c(\sigma_x = c' \mid \sigma \sim \tau) - \mu^c(\sigma_x = c')| > \frac{6}{C}\right) &\leqslant \mathbb{P}(\mu^{*,\tau}_{B_{x,l}}(\sigma_{L_{l/2}} \in B) \leqslant \frac{1}{C}) + \mathbb{P}(\mu^{*,\tau}_{B_{x,l}}(A^c_\tau) \leqslant \frac{1}{2C}) \\ &\leqslant Cd^{l/2+2}C_2\exp(-C_1^{l/2-2}) + Ce^{-2C} \leqslant e^{-16C},\end{aligned}$$

where the last step is true for large enough constant $\tilde{l}$ depending on d, C_1, C_2 and C'. This means that the strong concentration inequality (5.2.2) holds for $K = 6$, $\delta_1 = 1 - \frac{1}{4K}(1-\delta)$ and $l_1 = \max\{2l_0, \tilde{l}\}$. Moreover, by taking l large enough and changing the constant C to $6C$ in (5.4.5) and (5.4.8), we can make K arbitrarily close to 1. □

5.5 Component dynamics version of fast mixing results

In this section we prove Theorem 5.2.2. The theorem was originally proved for block dynamics in [MSW04]. Here we give a modification of their theorem adapted to the component dynamics by roughly "adding stars" at all occurrence of $B_{x,l}$. We will only state the key steps and refer the details to [MSW04]. For the remainder of this section, we let $\mu = \mu^c_T, \Omega = \Omega^c_T$. Recall that $\tilde{T}_x = T_x \backslash \{x\}$. First we define the entropy mixing condition for Gibbs measure to be the following:

Definition (Entropy Mixing)**.** We say that μ satisfies $\mathrm{EM}^*(l, \epsilon)$ if for every $x \in T$, $\eta \in \Omega$ and any $f \geqslant 0$ that does not depend on the connected component of $B_{x,l}$, i.e. $f(\sigma) = \mu^{*,\sigma}_{B_{x,l}}(f), \forall \sigma \in \Omega$, we have $\mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(f)] \leqslant \epsilon \cdot \mathrm{Ent}^{\eta}_{T_x}(f)$ where $\mathrm{Ent}^{\eta}_{T_x}$ means the entropy w.r.t $\mu^{\eta}_{T_x}$.

Let $p_{\min} = \min_{c,c' \in [k]}\{M(c,c') : M(c,c') > 0\}$. By the Markov chain construction of configurations, it satisfies that $p_{\min} = \min_{x,c,c'}\{\mu^{c}_{T_x}(\sigma_x = c') : c, c' \text{ are compatible}\}$. The following theorem relates the entropy mixing condition to the log-Soblev constant.

Theorem 5.5.1. *For any l and $\delta > 0$, if μ satisfies $\mathrm{EM}^*(l, [(1-\delta)p_{\min}/(l+1-\delta)]^2)$ then $\mathrm{Ent}(f) \leqslant \frac{2}{\delta} \cdot \mathcal{E}^*_l(f)$.*

To prove Theorem 5.5.1, we need the following modification of Lemma 3.5 (ii) of [MSW04]. The proof follows from its analog in [MSW04] immediately once we replace $\nu_A, \mathrm{Ent}_A, \nu_B, \mathrm{Ent}_B$ there with $\nu_{\tilde{T}_x}, \mathrm{Ent}_{\tilde{T}_x}, \nu^*_{B_{x,l}}, \mathrm{Ent}^*_{B_{x,l}}$ respectively.

Lemma 5.5.2. *For any $\epsilon < p^2_{\min}$, if μ satisfies $\mathrm{EM}^*(l, \epsilon)$ then for every $x \in T$, any $\eta \in \Omega$ and any $f \geqslant 0$ we have $\mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(f)] \leqslant \frac{1}{1-\epsilon'} \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}^*_{B_{x,l}}(f)] + \frac{\epsilon'}{1-\epsilon'} \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}_{\tilde{T}_x}(f)]$ with $\epsilon' = \sqrt{\epsilon}/p_{\min}$.*

Now plugging $\epsilon = [(1-\delta)p_{\min}/(l+1-\delta)]^2$ into Lemma 5.5.2 verifies the hypothesis of the following claim, which then implies Theorem 5.5.1:

Claim 5.5.3. If for every $x \in T$, $\eta \in \Omega$ and any $f \geqslant 0$,

$$\mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(f)] \leqslant c \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}^*_{B_{x,l}}(f)] + \frac{1-\delta}{l} \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}_{\tilde{T}_x}(f)], \tag{5.5.1}$$

then $\mathrm{Ent}(f) \leqslant \frac{c}{\delta} \cdot \mathcal{E}^*_l(f)$ for all $f \geqslant 0$.

Proof. First we decompose $\mathrm{Ent}(f)$ as a sum of $\mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(f)]$. Suppose T have m levels, consider $\varnothing = F_0 \subset F_1 \subset \cdots \subset F_{m+1} = T$, where F_i is the lowest i levels of T. By basic properties of conditional entropy (equation (3), (4), (5) of [MSW04]) and Markov property of Gibbs measure, we have

$$\mathrm{Ent}(f) = \cdots = \sum_{i=1}^{m+1} \mu[\mathrm{Ent}_{F_i}(\mu_{F_{i-1}}(f))] \leqslant \sum_{i=1}^{m+1} \sum_{x \in F_i \setminus F_{i-1}} \mu[\mathrm{Ent}_{T_x}(\mu_{F_{i-1}}(f))] \leqslant \sum_{x \in T} \mu[\mathrm{Ent}_{T_x}(\mu_{\tilde{T}_x}(f))]. \tag{5.5.2}$$

Denote the final sum by $\mathrm{PEnt}(f)$. For each term in the sum of $\mathrm{PEnt}(f)$, apply (5.5.1) to $g = \mu_{T_x \setminus B_{x,l} \cup \partial B_{x,l}}(f)$ and perform the decomposition trick of (5.5.2) again, we have for every $x \in T$ and $\eta \in \Omega$

$$\begin{aligned} \mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(f)] = \mathrm{Ent}^{\eta}_{T_x}[\mu_{\tilde{T}_x}(g)] &\leqslant c \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}^*_{B_{x,l}}(g)] + \frac{1-\delta}{l} \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}_{\tilde{T}_x}(g)] \\ &\leqslant c \cdot \mu^{\eta}_{T_x}[\mathrm{Ent}^*_{B_{x,l}}(f)] + \frac{1-\delta}{l} \cdot \sum_{y \in B_{x,l} \cup \partial B_{x,l}, y \neq x} \mu^{\eta}_{T_x}[\mathrm{Ent}_{T_y}(\mu_{\tilde{T}_y}(f))]. \end{aligned}$$

Now sum over $x \in T$ and take expectation w.r.t. μ for $\eta \in \Omega$. Note that the first term of the last line sums up to $\mathcal{E}_l^* = \sum_{x\in T} \mu(\mathrm{Ent}^*_{B_{x,l}}(f))$ and each y in second term appears in at most l blocks, we have

$$\begin{aligned}\mathrm{PEnt}(f) &\leqslant c\cdot \mathcal{E}_l^*(f) + \frac{1-\delta}{l}\cdot \sum_{x\in T}\sum_{y\in B_{x,l}\cup\partial B_{x,l}, y\neq x} \mu[\mathrm{Ent}_{T_y}(\mu_{\tilde{T}_y}(f))] \\ &\leqslant c\cdot \mathcal{E}_l^*(f) + \frac{1-\delta}{l}\cdot l\cdot \sum_{y\in T}\mu[\mathrm{Ent}_{T_y}(\mu_{\tilde{T}_y}(f))] = c\cdot\mathcal{E}_l^*(f) + (1-\delta)\cdot \mathrm{PEnt}(f),\end{aligned}$$

and hence $\mathrm{Ent}(f) \leqslant \mathrm{PEnt}(f) \leqslant \frac{c}{\delta}\cdot \mathcal{E}_l^*$. □

Given the result of Theorem 5.5.1, it is enough to show that for some constant α, concentration inequality of (5.2.2) implies $\mathrm{EM}^*(l, [(1-\delta)p_{\min}/(l+1-\delta)]^2)$. For convenience of notation, we define the two following functions for each $c' \in [k]$:

$$g_{c'}(\sigma) = \frac{\mu(\sigma|\sigma_\rho = c')}{\mu(\sigma)} = \frac{1}{\mu(\sigma_\rho = c')}\cdot 1\{\sigma_\rho = c'\}, \quad g_{c'}^{*(l)} = \mu^*_{B_{\rho,l}}(g_{c'}).$$

Letting $\delta' = (1-\delta)^2/\alpha(l+1-\delta)^2$, we can rewrite (5.2.2) as

$$\mu\left(\left|g_{c'}^{*(l)} - 1\right| > \delta'\right) \leqslant e^{-2/\delta'}. \tag{5.5.3}$$

Theorem 5.5.4. *There exists a constant C such that if (5.5.3) holds for some $\delta' \geqslant 0$ and all pairs of states $c, c' \in [k]$, we have $\mathrm{Ent}[\mu_{\tilde{T}}(f)] \leqslant C\delta'\mathrm{Ent}(f)$ for any $f \geqslant 0$ satisfying $f(\sigma) = \mu^{*,\sigma}_{B_{\rho,l}}(f), \forall \sigma \in \Omega^c$, i.e. $\mathrm{EM}^*(l, C\delta')$ holds.*

Proof. Since for any $f' \geqslant 0$, $\mathrm{Ent}(f') \leqslant \mathrm{Var}(f')/\mu(f)$, we can write

$$\begin{aligned}\mathrm{Ent}[\mu_{\tilde{T}}(f)] &\leqslant \frac{\mathrm{Var}[\mu_{\tilde{T}}(f)]}{\mu(\mu_{\tilde{T}}(f))} = \frac{1}{\mu(f)}\sum_{c'\in[k]}\mu(\sigma_\rho = c')\left(\mu(f|\sigma_\rho = c') - \mu(f)\right)^2 \\ &= \frac{1}{\mu(f)}\sum_{c'\in[k]}\mu(\sigma_\rho = c')\mathrm{Cov}(g_{c'}, f)^2 \leqslant \max_{c'\in[k]}\frac{\mathrm{Cov}(g_{c'}, f)^2}{\mu(f)} = \max_{c'\in[k]}\frac{\mathrm{Cov}(g_{c'}^{*(l)}, f)^2}{\mu(f)}.\end{aligned} \tag{5.5.4}$$

where covariance is taken w.r.t. μ and the last step is because $f(\sigma) = \mu^{*,\sigma}_{B_{\rho,l}}(f)$. Now using Lemma 5.4 of [MSW04] (cited below) with

$$f_1 = \frac{g_{c'}^{*(l)} - 1}{\left\|g_{c'}^{*(l)}\right\|_\infty}, f_2 = \frac{f}{\mu(f)}$$

and noting that $\left\|g_{c'}^{*(l)}\right\|_\infty \leqslant \|g_{c'}\|_\infty \leqslant p_{\min}$, we have $\mathrm{Cov}(g_{c'}^{*(l)}, f)^2 \leqslant C\delta'\mu(f)\mathrm{Ent}(f)$ for some constant $C = C'/p^2_{\min}$. Plug it into (5.5.4), we get $\mathrm{Ent}[\mu_{\tilde{T}}(f)] \leqslant C\delta'\mathrm{Ent}(f)$. □

Lemma 5.5.5 (Lemma 5.4 of [MSW04]). *Let $\{\Omega, \mathcal{F}, \nu\}$ be a probability space and let f_1 be a mean-zero random variable such that $\|f\|_\infty \leqslant 1$ and $\nu[|f_1| > \delta] \leqslant e^{-2/\delta}$ for some $\delta \in (0,1)$. Let f_2 be a probability density w.r.t ν, i.e. $f_2 \geqslant 0$ and $\nu(f_2) = 1$. Then there exists a numerical constant $C' > 0$ independent of ν, f_1, f_2 and δ, such that $\nu(f_1 f_2) \leqslant C'\delta \mathrm{Ent}_\nu(f_2)$.*

Proof of Theorem 5.2.2. Fix $\alpha = C/p_{\min}^2$ where C is the constant in Theorem 5.5.4. The desired result follows the combination of Theorem 5.5.1 and 5.5.4. □

5.6 Results for k-coloring

In this section we prove Theorem 4, for which it is enough to verify the connectivity condition $\mathcal{C}$, in particular to show that $p_l^{\text{free}} \to 1$, as $l \to \infty$. In fact for the coloring model, as we will show in a moment, a vertex can change to all k states in one step if all its children can change to 2 or 3 states in one step. We will first formalize this idea by defining the "types" of vertices and then analyze the recursion of this new definition.

Recall the definition that for given configuration $\sigma \in \Omega_T$ with $\sigma_\rho = c$, we say that the root can change to color c' in one step if and only if there exists a path $\sigma = \sigma^0, \sigma^1, \ldots, \sigma^n \in \Omega_T^\sigma$ such that for each $i, \sigma^i, \sigma^{i+1}$ differs by only one vertex and

$$\sigma_\rho^i = \begin{cases} c & 0 \leqslant i \leqslant n-1 \\ c' & i = n \end{cases}.$$

Let $C(\rho)$ denote the set of colors the root can change to in one step (including its original color). We define the type of root to be *rigid* (*type 2, type 3*, resp.) if $|C(\rho)| = 1$ ($= 2, \geqslant 3$, resp.). For general vertex $x \in T$, not necessarily the root, we can similarly define $C(x)$ and rigid, type 2, type 3 by treating x as the root of subtree T_x and considering $\sigma|_{T_x}$. Set $C(x)$ is a function of σ_{T_x} and is independent of the rest of the tree.

Let $p_l^r = \mu_l$(the root is rigid), where μ_l is the Gibbs measure on l-level tree with free boundary condition. Define $p_l^{(2)}, p_l^{(3)}$ similarly, we have $p_l^r + p_l^{(2)} + p_l^{(3)} = 1$. For tree T with $l' > l$ levels and vertex $x \in T$ that is l levels above the bottom boundary, noting that $\mu_{l'}|_{T_x} = \mu_l$, we also have

$$\mu_{l'}(x \text{ is rigid/type 2/type 3}) = \mu_{l'}|_{T_x}(x \text{ is rigid/type 2/type 3}) = p_l^r/p_l^{(2)}/p_l^{(3)}.$$

The definition above is independent of the parent of x. In order to analyze these probabilities recursively, we introduce one further definition describing how the type of one vertex affects the type of its parent. Recall that $p(x)$ denotes the parent of x. Fix a configuration $\sigma \in \Omega_T$. For any $x \in \tilde{T} = T \backslash \{\rho\}$, we say x is *bad* if $C(x) \backslash \{\sigma_{p(x)}\} = \{\sigma_x\}$ and *good* other wise. Observe that σ_x is always an element of $C(x)$. If x is good, then $|C(x) \backslash \{\sigma_{p(x)}\}| \geqslant 2$, i.e. x has at least one more choice other than $\sigma_{p(x)}$. Note that the event that x is bad depends only on $\sigma|_{T_{p(x)}}$ and given σ_x, for $x_i \in L_{x,1}$, events $\{x_i \text{ is bad}\}$ are conditionally i.i.d. and independent of the configurations outside T_x. Hence, by similar argument, we can define $p_l^b = 1 - p_l^g =$

$\mu_{l'}(x \text{ is bad})$. The relation between the type of a vertex and its goodness/badness is given in the following lemma.

Lemma 5.6.1. *For $l' > l > 0$ and $x \in T$ l levels above the bottom boundary,*

$$\mu_{l'}(x \text{ is bad} \mid x \text{ is rigid})=1, \mu_{l'}(x \text{ is bad} \mid x \text{ is type 2})=\frac{1}{k-1}, \mu_{l'}(x \text{ is bad} \mid x \text{ is type 3})=0, \tag{5.6.1}$$

Hence $p_l^b = p_l^r + \frac{1}{k-1}p_l^{(2)}, p_l^g = p_l^{(3)} + \frac{k-2}{k-1}p_l^{(2)}$.

Proof. The first and third equation of (5.6.1) is obvious as $|C(x)|$ and $|C(x)\backslash\{\sigma_{p(x)}\}|$ differs at most by one, and the equality about p_l^b and p_l^g follows immediately from (5.6.1). Hence it lefts to show the second equation. Given $|C(x)| = 2$, x is bad if and only if $\sigma_{p(x)} \in C(x)$. Therefore the conditional probability on the left hand side of the second equation equals to $\mathbb{P}(C(x) = \{\sigma_{p(x)}, \sigma_x\} \mid |C(x)| = 2)$.

Note that $C(x)$ is a function of σ_{T_x}, in particular it is conditionally independent of $\sigma_{p(x)}$ given σ_x. By symmetry, the distribution of $C(x)\backslash\{\sigma_x\}$ given $|C(x)|$ and σ_x is the uniformly distribution on the $\binom{k-1}{|C(x)|-1}$ ways of choosing $|C(x)|-1$ elements from $[k]\backslash\{\sigma_x\}$. Hence

$$\mathbb{P}(C(x) = \{\sigma_{p(x)}, \sigma_x\} \mid |C(x)| = 2) = \frac{1}{\binom{k-1}{1}} = \frac{1}{k-1}.$$

□

The next lemma follows a similar argument to Claim 5.4.2 and Lemma 5.4.3, and shows that in order to bound the probability of a vertex being free, it is enough to bound the probability of being bad.

Lemma 5.6.2. *Suppose $k \geqslant 4$. For any $\sigma \in \Omega_T$ and $x \in T$, if every child of x is good, then x is free.*

Proof. Fix $c \in [k]$. Since all children of x are god, for each child y_i there exists $c_i \in C(y_i)\backslash\{c, \sigma_x\}$. Therefore to change x from σ_x to c in one step, we can first change the color of every y_i to c_i in one step and then in the final step change x from σ_x to c. Since this is true for all $c \in [l]$, we conclude that x is free. □

Now we will show that for large enough k, in the region of non-reconstruction, the probability of seeing a bad vertex l levels above bottom decays double exponentially fast in l. In fact we will prove the result for a region slightly larger than the known non-reconstruction region , which is $d \leqslant k[\ln k + \ln\ln k + \beta]$, for any $\beta < 1 - \ln 2$ (see [Sly09]).

Theorem 5.6.3. *Suppose $\beta < 1$, For sufficiently large k and $d \leqslant k[\ln k + \ln\ln k + \beta]$, there exists a constant l_0 depending only on k and d, such that for $l \geqslant l_0$,*

$$p_l^b \leqslant \exp(-(k/2)^{l-l_0}). \tag{5.6.2}$$

We first finish the proof of Theorem 4 using Lemma 5.6.2 and Theorem 5.6.3.

Proof of Theorem 4. It has been shown in [Sly09] that for any $\beta < 1 - \ln 2$, there exist $k_0 = k_0(\beta)$ such that for any $k \geqslant k_0$ and $d \leqslant k(\ln k + \ln\ln k + \beta)$, the k-coloring model is non-reconstructible on d-ary trees. Therefore by Theorem 5.1.1, it is enough to show that the connectivity condition holds. The first part of the condition is obviously true for $k \geqslant 4$. For the second condition,

$$1 - p_l^{\text{free}} = \mathbb{P}_{\sigma\sim\mu_l}(\text{root is not free}) \leqslant \mathbb{P}(\exists x \in L_1, x \text{ is bad}) \leqslant dp_{l-1}^b \leqslant d\exp(-(\frac{1}{2}k)^{l-l_0}).$$

The last term in the equation above tends to 0 as l tends to infinity, which completes the proof. □

The proof of Theorem 5.6.3 is split into two phases: when p_l^b is close to 1 and when p_l^b is smaller than $\frac{1}{ed}$.

Lemma 5.6.4. *Under the assumption of Theorem 5.6.3, there exist a constant l_0 depending only on k and d such that $p_{l_0}^b < \frac{1}{ed}$.*

Proof. This proof is similar to Lemma 2 and Lemma 4 of [Sly09]. We recursively analyze the probabilities as a function of the depth of the tree l. For $l = 0$, T consist only the bottom boundary and hence $p_0^r = 1, p_0^{(2)} = p_0^{(3)} = 0, p_0^b = p_0^r + \frac{1}{k-1}p_0^{(2)} = 1$.

For $l \geqslant 1$, suppose without loss of generality that the color of the root is 1 and its children are $x_1, \ldots, x_d \in L_1$. Let $\mathcal{F}$ denote the sigma-field generated by $(\sigma_{x_i})_{i=1}^d$ and let $d_c = |\{i, \sigma_{x_i} = c\}|$ be the number of children with color c for $2 \leqslant c \leqslant k$. By definition, the sizes of $C(x_i)$'s and hence the types of x_i's are independent of $\mathcal{F}$ and i.i.d. distributed. Conditioning on $\mathcal{F}$ and $(|C(x_i)|)_{i=1}^k$, set $C(x_i)\backslash\{\sigma_{x_i}\}$ is uniformly randomly chosen among all subsets of $[k]\backslash\{\sigma_{x_i}\}$ with $(|C(x_i)| - 1)$ elements. Therefore the number of bad vertices of color c given $\mathcal{F}$ is follows the binomial distribution with parameter $\text{Bin}(d_c, p_{l-1}^b)$.

Following similar argument of Lemma 5.6.2, the root can change to color c in one step if and only if none of the x_i's with color c is bad, which happens with probability $(1 - p_{l-1}^b)^{d_c}$. Therefore we have

$$p_l^b = p_l^r + \frac{1}{k-1}p_l^{(2)} = \prod_{c=2}^{k}\mathbb{E}\left[1 - (1 - p_{l-1}^b)^{d_c}\right] + \frac{1}{k-1}\sum_{c'=2}^{k}\mathbb{E}\left[(1-p_{l-1}^b)^{d_{c'}}\prod_{c\neq c'}\left(1 - (1 - p_{l-1}^b)^{d_c}\right)\right].$$

Viewing the right hand side as a function of $(d_2, \ldots, d_k)$, increasing d_c means adding more vertices of color c, which increases the probability of blocking the move of the root. Therefore p_l^b is an increasing function w.r.t every d_c. By symmetry, $(d_2, \ldots, d_k)$ follows a multi-nominal distribution. Fix $\beta < \beta^* < 1$ and let $\tilde{d}_c$ be i.i.d. Poisson(D) random variables where $D = \ln k + \ln\ln k + \beta^*$. We can couple $(d_2, \ldots, d_k)$ and $(\tilde{d}_2, \ldots, \tilde{d}_k)$ such that $(d_2, \ldots, d_k) \leqslant$

$(\tilde{d}_2, \ldots, \tilde{d}_k)$ whenever $\sum_{c=2}^k \tilde{d}_c \geqslant d$. Letting $p = \mathbb{P}(\text{Poisson}((k-1)D) < d)$, the recursion relationship satisfies

$$\begin{aligned}
p_l^b &= p_l^r + \frac{1}{k-1} p_l^{(2)} = \prod_{c=2}^k \mathbb{E}\left[1 - (1-p_{l-1}^b)^{d_c}\right] + \frac{1}{k-1} \sum_{c'=2}^k \mathbb{E}\left[(1-p_{l-1}^b)^{d_{c'}} \prod_{c \neq c'} \left(1 - (1-p_{l-1}^b)^{d_c}\right)\right] \\
&\leqslant \prod_{c=2}^k \mathbb{E}\left[1 - (1-p_{l-1}^b)^{\tilde{d}_c}\right] + \frac{1}{k-1} \sum_{c'=2}^k \mathbb{E}(1-p_{l-1}^b)^{\tilde{d}_{c'}} \prod_{c \neq c'} \mathbb{E}\left[1 - (1-p_{l-1}^b)^{\tilde{d}_c}\right] + p \\
&= \left(1 - \exp(-p_{l-1}^b D)\right)^{k-1} + \frac{k-1}{k-1} \exp(-p_{l-1}^b D) \left(1 - \exp(-p_{l-1}^b D)\right)^{k-2} + p \\
&= \left(1 - \exp(-p_{l-1}^b D)\right)^{k-2} + p \leqslant \exp\left(-(k-2)\exp(-p_{l-1}^b D)\right) + p
\end{aligned}$$

where the last step follows from the fact that $(1-r)^k \leqslant e^{-kr}$ for $0 < r < 1$.

The rest of the proof resembles the argument of Lemma 3 of [Sly09]. Let $f(x) = \exp\left(-(k-2)\exp(-xD)\right) + p$, $y_0 = p_0^b = 1$ and recursively define $y_l = f(y_{l-1})$. Since $f(x)$ is an increasing function of x, we have that $p_l^b \leqslant y_l$ for any $l \geqslant 0$. Hence it is enough to show the existence of l_0 such that $y_{l_0} \leqslant \frac{1}{ed}$.

Note that $\frac{d}{dx}\exp(-x) \mid_{x=0} = -1$. For any sufficiently small $\epsilon > 0$, there exists $\delta > 0$ such that for any $0 < x < \delta$, $e^{-x} \leqslant 1 - (1-\epsilon)x$. Let k be large enough such that $(k-2)\exp(-D) = \frac{k-2}{k \ln k} e^{-\beta^*} < \delta$. We have

$$y_1 = f(1) \leqslant 1 - (1-\epsilon)\frac{k-2}{k \ln k} e^{-\beta^*} + p.$$

Recall our choice of $\beta < \beta^* < 1$ and $(k-1)D - d \geqslant (\beta^* - \beta)k + o(k)$, by Hoeffding's inequality, the error term p satisfies that $p = \exp(-\Omega(\frac{k}{\sqrt{d}})) = o(k^{-2}) = o(d^{-1})$. Therefore, for large enough k,

$$y_1 \leqslant 1 - \frac{1-\epsilon}{2e \ln k} + o(k^{-1}) \leqslant 1 = y_0.$$

Repeating the arguments above shows that y_l is decreasing in l as long as $(k-2)\exp(-y_l D) < \delta$. Pick ϵ small enough such that $(1-\epsilon)e^{-\beta^*} > e^{-1}$ and choose $r' > r > 0$ such that $(1-\epsilon)e^{-\beta^*} > e^{-1}(1+r')$. It follows that

$$\begin{aligned}
1 - y_{l+1} &\geqslant 1 - \left(p + 1 - (1-\epsilon)(k-2)\exp(-y_l D)\right) \\
&\geqslant (1-\epsilon)\frac{(k-2)e^{-\beta^*}}{k \ln k} \exp((1-y_l)\ln k) - p \\
&\geqslant \frac{k-2}{k}(1-\epsilon)e^{1-\beta^*}(1-y_l) - p \\
&\geqslant (1+r')(1-y_l) - p \geqslant (1+r)(1-y_l)
\end{aligned}$$

where the second last inequality follows from inequality $e^x > ex$, and the last inequality follows from that $1 - y_l \geqslant 1 - y_1 = O(\frac{1}{\ln k})$ while $p = o(k^{-2})$. Therefore after a constant number of steps, there must exist some l such that $(k-2)\exp(-y_l D) \geqslant \delta$. Now choose α, α' such that $e^{-\delta} < \alpha' < \alpha < 1$. When k is large enough, $y_{l+1} \leqslant p + e^{-\delta} < \alpha' < 1$. Then again for k large enough, $\exp(-y_{l+1}D) \geqslant \exp(-\alpha' D) \geqslant \exp(-\alpha \ln k) = k^{-\alpha}$. Therefore for k large enough

$$y_{l+2} \leqslant p + \exp(-(k-2)\exp(-y_{l+1}D)) \leqslant p + \exp(-\frac{1}{2}k^{1-\alpha}) \leqslant \frac{1}{ed}.$$

□

After first l_0 levels, we cannot use the same method because the error of Poisson coupling becomes non-negligible; but meanwhile, p_l^b is small enough such that bounding the total number of bad children is enough to finish the proof.

Proof of Theorem 5.6.3. In order for a vertex to be bad, there must be at least $k-2$ of its children which are bad. Therefore,

$$p_l^b \leqslant \binom{d}{k-2} (p_{l-1}^b)^{k-2} \leqslant (dp_{l-1}^b)^{k-2}.$$

Let l_0 be the constant in Lemma 5.6.4. We complete the proof by inducting on l for $l \geqslant l_0$: If $l = l_0$, then $p_{l_0}^b \leqslant \frac{1}{ed} \leqslant \frac{1}{e}$. If for $l > l_0$, p_l^b satisfies (5.6.2), then for k large enough such that $\ln(2k\ln k) \leqslant \frac{1}{6}k$ and $k-2 \geqslant \frac{3}{4}k$,

$$\begin{aligned} p_{l+1}^b &\leqslant (dp_l^b)^{k-2} \leqslant \left(2k\ln k \exp\left(-(k/2)^{l-l_0}\right)\right)^{k-2} = \exp(k-2)\left(-(k/2)^{l-l_0} + \ln(2k\ln k)\right) \\ &\leqslant \exp\left(-\frac{3}{4}k \cdot \frac{2}{3}(k/2)^{l-l_0}\right) = \exp\left(-(k/2)^{l+1-l_0}\right). \end{aligned}$$

Therefore (5.6.2) holds for all $l \geqslant l_0$. □

Bibliography

[Ach+01] Dimitris Achlioptas et al. "The phase transition in 1-in-k SAT and NAE 3-SAT". In: *Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics. 2001, pp. 721–722.

[ACO08] Dimitris Achlioptas and Amin Coja-Oghlan. "Algorithmic barriers from phase transitions". In: *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*. IEEE. 2008, pp. 793–802.

[ACORT11] Dimitris Achlioptas, Amin Coja-Oghlan, and Federico Ricci-Tersenghi. "On the solution-space geometry of random constraint satisfaction problems". In: *Random Structures Algorithms* 38.3 (2011), pp. 251–268. ISSN: 1042-9832. DOI: 10.1002/rsa.20323. URL: http://dx.doi.org/10.1002/rsa.20323.

[AM06] Dimitris Achlioptas and Cristopher Moore. "Random k-SAT: two moments suffice to cross a sharp threshold". In: *SIAM J. Comput.* 36.3 (2006), 740–762 (electronic). ISSN: 0097-5397. DOI: 10.1137/S0097539703434231. URL: http://dx.doi.org/10.1137/S0097539703434231.

[Bap+16] Victor Bapst et al. "The condensation phase transition in random graph coloring". In: *Comm. Math. Phys.* 341.2 (2016), pp. 543–606. ISSN: 0010-3616. DOI: 10.1007/s00220-015-2464-z. URL: http://dx.doi.org/10.1007/s00220-015-2464-z.

[BC15] Victor Bapst and Amin Coja-Oghlan. *The condensation phase transition in the regular k-SAT model*. arXiv:1507.03512. 2015.

[BCO16] Victor Bapst and Amin Coja-Oghlan. "Harnessing the Bethe free energy". In: *Random Structures Algorithms* 49.4 (2016), pp. 694–741. ISSN: 1042-9832. DOI: 10.1002/rsa.20692. URL: http://dx.doi.org/10.1002/rsa.20692.

[BCORm16] Victor Bapst, Amin Coja-Oghlan, and Felicia Raß mann. "A positive temperature phase transition in random hypergraph 2-coloring". In: *Ann. Appl. Probab.* 26.3 (2016), pp. 1362–1406. ISSN: 1050-5164. DOI: 10.1214/15-AAP1119. URL: http://dx.doi.org/10.1214/15-AAP1119.

[Ber+05] Noam Berger et al. “Glauber dynamics on trees and hyperbolic graphs”. In: *Probab. Theory Related Fields* 131.3 (2005), pp. 311–340. ISSN: 0178-8051. DOI: 10.1007/s00440-004-0369-4. URL: http://dx.doi.org/10.1007/s00440-004-0369-4.

[BGT13] Mohsen Bayati, David Gamarnik, and Prasad Tetali. “Combinatorial approach to the interpolation method and scaling limits in sparse random graphs”. In: *Ann. Probab.* 41.6 (2013), pp. 4080–4115. ISSN: 0091-1798. DOI: 10.1214/12-AOP816. URL: http://dx.doi.org/10.1214/12-AOP816.

[Bha+11] Nayantara Bhatnagar et al. “Reconstruction for colorings on trees”. In: *SIAM J. Discrete Math.* 25.2 (2011), pp. 809–826. ISSN: 0895-4801. DOI: 10.1137/090755783. URL: http://dx.doi.org/10.1137/090755783.

[BMZ05] A. Braunstein, M. Mézard, and R. Zecchina. “Survey propagation: an algorithm for satisfiability”. In: *Random Structures Algorithms* 27.2 (2005), pp. 201–226. ISSN: 1042-9832. DOI: 10.1002/rsa.20057. URL: http://dx.doi.org/10.1002/rsa.20057.

[Bor+06] Christian Borgs et al. “The Kesten-Stigum reconstruction bound is tight for roughly symmetric binary channels”. In: *Foundations of Computer Science, 2006. FOCS'06. 47th Annual IEEE Symposium on*. IEEE. 2006, pp. 518–530.

[Bra+16] Alfredo Braunstein et al. “The large deviations of the whitening process in random constraint satisfaction problems”. In: *J. Stat. Mech. Theory Exp.* 5 (2016), pp. 053401, 79. ISSN: 1742-5468.

[CO+16] Amin Coja-Oghlan et al. “Information-theoretic thresholds from the cavity method”. In: *arXiv preprint arXiv:1611.00814* (2016).

[COEH16] Amin Coja-Oghlan, Charilaos Efthymiou, and Samuel Hetterich. “On the chromatic number of random regular graphs”. In: *J. Combin. Theory Ser. B* 116 (2016), pp. 367–439. ISSN: 0095-8956. DOI: 10.1016/j.jctb.2015.09.006. URL: http://dx.doi.org/10.1016/j.jctb.2015.09.006.

[COHH16] Amin Coja-Oghlan, Amir Haqshenas, and Samuel Hetterich. “Walksat stalls well below the satisfiability threshold”. In: *arXiv preprint arXiv:1608.00346* (2016).

[CP12] Amin Coja-Oghlan and Konstantinos Panagiotou. “Catching the k-NAE-SAT threshold”. In: *Proc. 44th STOC*. New York: ACM, 2012, pp. 899–907. DOI: 10.1145/2213977.2214058. URL: http://dx.doi.org/10.1145/2213977.2214058.

[CP16a] Amin Coja-Oghlan and Konstantinos Panagiotou. “The asymptotic k-SAT threshold”. In: *Adv. Math.* 288 (2016), pp. 985–1068. ISSN: 0001-8708. DOI: 10.1016/j.aim.2015.11.007. URL: http://dx.doi.org/10.1016/j.aim.2015.11.007.

[CP16b] Amin Coja-Oghlan and Will Perkins. *Belief propagation on replica symmetric random factor graph models*. arXiv:1603.08191. 2016.

[CPS15] Amin Coja-Oghlan, Will Perkins, and Kathrin Skubch. *Limits of discrete distributions and Gibbs measures on random graphs*. arXiv:1512.06798. 2015.

[CR92] Vašek Chvátal and Bruce Reed. "Mick gets some (the odds are on his side)(satisfiability)". In: *Foundations of Computer Science, 1992. Proceedings., 33rd Annual Symposium on*. IEEE. 1992, pp. 620–627.

[CZ12] Amin Coja-Oghlan and Lenka Zdeborová. "The condensation transition in random hypergraph 2-coloring". In: *Proc. 23rd SODA*. ACM, New York, 2012, pp. 241–250.

[Dec+11] Aurelien Decelle et al. "Asymptotic analysis of the stochastic block model for modular networks and its algorithmic applications". In: *Phys. Rev. E* 84.6 (2011), p. 066106.

[DLP10] Jian Ding, Eyal Lubetzky, and Yuval Peres. "Mixing time of critical Ising model on trees is polynomial in the height". In: *Comm. Math. Phys.* 295.1 (2010), pp. 161–207. ISSN: 0010-3616. DOI: 10.1007/s00220-009-0978-y. URL: http://dx.doi.org/10.1007/s00220-009-0978-y.

[DMR11] Constantinos Daskalakis, Elchanan Mossel, and Sébastien Roch. "Evolutionary trees and the Ising model on the Bethe lattice: a proof of Steel's conjecture". In: *Probab. Theory Related Fields* 149.1-2 (2011), pp. 149–189. ISSN: 0178-8051. DOI: 10.1007/s00440-009-0246-2. URL: http://dx.doi.org/10.1007/s00440-009-0246-2.

[DSS13] Jian Ding, Allan Sly, and Nike Sun. "Maximum independent sets on random regular graphs". In: *arXiv preprint arXiv:1310.4787* (2013).

[DSS15] Jian Ding, Allan Sly, and Nike Sun. "Proof of the satisfiability conjecture for large k". In: *Proc. 47th STOC*. New York: ACM, 2015, pp. 59–68.

[DSS16] Jian Ding, Allan Sly, and Nike Sun. "Satisfiability threshold for random regular NAE-SAT". In: *Comm. Math. Phys.* 341.2 (2016), pp. 435–489. ISSN: 0010-3616. DOI: 10.1007/s00220-015-2492-8. URL: http://dx.doi.org/10.1007/s00220-015-2492-8.

[Dur10] Rick Durrett. *Probability: theory and examples*. Fourth. Vol. 31. Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, Cambridge, 2010, pp. x+428. ISBN: 978-0-521-76539-8. DOI: 10.1017/CBO9780511779398. URL: http://dx.doi.org/10.1017/CBO9780511779398.

[Eft15] Charilaos Efthymiou. "Reconstruction/non-reconstruction thresholds for colourings of general Galton-Watson trees". In: *Approximation, randomization, and combinatorial optimization. Algorithms and techniques*. Vol. 40. LIPIcs. Leibniz Int. Proc. Inform. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2015, pp. 756–774.

[Eva+00] William Evans et al. "Broadcasting on trees and the Ising model". In: *Ann. Appl. Probab.* 10.2 (2000), pp. 410–433. ISSN: 1050-5164. DOI: 10.1214/aoap/1019487349. URL: http://dx.doi.org/10.1214/aoap/1019487349.

[FL03] Silvio Franz and Michele Leone. "Replica bounds for optimization problems and diluted spin systems". In: *J. Statist. Phys.* 111.3-4 (2003), pp. 535–564. ISSN: 0022-4715. DOI: 10.1023/A:1022885828956. URL: http://dx.doi.org/10.1023/A:1022885828956.

[Fri99] Ehud Friedgut. "Sharp thresholds of graph properties, and the k-sat problem". In: *J. Amer. Math. Soc.* 12.4 (1999). With an appendix by Jean Bourgain, pp. 1017–1054. ISSN: 0894-0347. DOI: 10.1090/S0894-0347-99-00305-7. URL: http://dx.doi.org/10.1090/S0894-0347-99-00305-7.

[FV07] Alan Frieze and Eric Vigoda. "A survey on the use of Markov chains to randomly sample colourings". In: *Combinatorics, complexity, and chance*. Vol. 34. Oxford Lecture Ser. Math. Appl. Oxford Univ. Press, Oxford, 2007, pp. 53–71. DOI: 10.1093/acprof:oso/9780198571278.003.0004. URL: http://dx.doi.org/10.1093/acprof:oso/9780198571278.003.0004.

[Gam14] David Gamarnik. "Right-convergence of sparse random graphs". In: *Probab. Theory Related Fields* 160.1-2 (2014), pp. 253–278. ISSN: 0178-8051. DOI: 10.1007/s00440-013-0528-6. URL: http://dx.doi.org/10.1007/s00440-013-0528-6.

[Geo11] Hans-Otto Georgii. *Gibbs measures and phase transitions*. Second. Vol. 9. de Gruyter Studies in Mathematics. Walter de Gruyter & Co., Berlin, 2011, pp. xiv+545. ISBN: 978-3-11-025029-9. DOI: 10.1515/9783110250329. URL: http://dx.doi.org/10.1515/9783110250329.

[GJK10] Leslie Ann Goldberg, Mark Jerrum, and Marek Karpinski. "The mixing time of Glauber dynamics for coloring regular trees". In: *Random Structures Algorithms* 36.4 (2010), pp. 464–476. ISSN: 1042-9832. DOI: 10.1002/rsa.20303. URL: http://dx.doi.org/10.1002/rsa.20303.

[Goe96] Andreas Goerdt. "A threshold for unsatisfiability". In: *J. Comput. System Sci.* 53.3 (1996). 1994 ACM Symposium on Parallel Algorithms and Architectures (Cape May, NJ, 1994), pp. 469–486. ISSN: 0022-0000. DOI: 10.1006/jcss.1996.0081. URL: http://dx.doi.org/10.1006/jcss.1996.0081.

[GS14] David Gamarnik and Madhu Sudan. "Performance of the Survey Propagation-guided decimation algorithm for the random NAE-K-SAT problem". In: *arXiv preprint arXiv:1402.0052* (2014).

[GT03] Francesco Guerra and Fabio Lucio Toninelli. "Infinite volume limit and spontaneous replica symmetry breaking in mean field spin glass models". In: *Ann. Henri Poincaré* 4.suppl. 1 (2003), S441–S444. ISSN: 1424-0637. DOI: 10.1007/s00023-003-0934-x. URL: http://dx.doi.org/10.1007/s00023-003-0934-x.

[Gue03] Francesco Guerra. "Broken replica symmetry bounds in the mean field spin glass model". In: *Comm. Math. Phys.* 233.1 (2003), pp. 1–12. ISSN: 0010-3616. DOI: 10.1007/s00220-002-0773-5. URL: http://dx.doi.org/10.1007/s00220-002-0773-5.

[JM04] Svante Janson and Elchanan Mossel. "Robust reconstruction on trees is determined by the second eigenvalue". In: *Ann. Probab.* 32.3B (2004), pp. 2630–2649. ISSN: 0091-1798. DOI: 10.1214/009117904000000153. URL: http://dx.doi.org/10.1214/009117904000000153.

[Jon02] Johan Jonasson. "Uniqueness of uniform random colorings of regular trees". In: *Statist. Probab. Lett.* 57.3 (2002), pp. 243–248. ISSN: 0167-7152. DOI: 10.1016/S0167-7152(02)00054-8. URL: http://dx.doi.org/10.1016/S0167-7152(02)00054-8.

[Kar72] Richard M. Karp. "Reducibility among combinatorial problems". In: (1972), pp. 85–103.

[Krz+07] Florent Krząkała et al. "Gibbs states and the set of solutions of random constraint satisfaction problems". In: *Proc. Natl. Acad. Sci. USA* 104.25 (2007), 10318–10323 (electronic). ISSN: 1091-6490. DOI: 10.1073/pnas.0703685104. URL: http://dx.doi.org/10.1073/pnas.0703685104.

[LMP09] Brendan Lucier, Michael Molloy, and Yuval Peres. "The Glauber dynamics for colourings of bounded degree trees". In: *Approximation, randomization, and combinatorial optimization.* Vol. 5687. Lecture Notes in Comput. Sci. Springer, Berlin, 2009, pp. 631–645. DOI: 10.1007/978-3-642-03685-9_47. URL: http://dx.doi.org/10.1007/978-3-642-03685-9_47.

[Mar99] Fabio Martinelli. "Lectures on Glauber dynamics for discrete spin models". In: *Lectures on probability theory and statistics (Saint-Flour, 1997).* Vol. 1717. Lecture Notes in Math. Springer, Berlin, 1999, pp. 93–191. DOI: 10.1007/978-3-540-48115-7_2. URL: http://dx.doi.org/10.1007/978-3-540-48115-7_2.

[Mas14] Laurent Massoulié. "Community detection thresholds and the weak Ramanujan property". In: *Proc. 46th STOC.* New York: ACM, 2014, pp. 694–703.

[MM06] Marc Mézard and Andrea Montanari. "Reconstruction on trees and spin glass transition". In: *J. Stat. Phys.* 124.6 (2006), pp. 1317–1350. ISSN: 0022-4715. DOI: 10.1007/s10955-006-9162-3. URL: http://dx.doi.org/10.1007/s10955-006-9162-3.

[MM09] Marc Mézard and Andrea Montanari. *Information, physics, and computation*. Oxford Graduate Texts. Oxford University Press, Oxford, 2009, pp. xiv+569. ISBN: 978-0-19-857083-7. DOI: 10.1093/acprof:oso/9780198570837.001.0001. URL: http://dx.doi.org/10.1093/acprof:oso/9780198570837.001.0001.

[MMW07] Elitza Maneva, Elchanan Mossel, and Martin J. Wainwright. "A new look at survey propagation and its generalizations". In: *J. ACM* 54.4 (2007), Art. 17, 41. ISSN: 0004-5411. DOI: 10.1145/1255443.1255445. URL: http://dx.doi.org/10.1145/1255443.1255445.

[MNS15] Elchanan Mossel, Joe Neeman, and Allan Sly. "Reconstruction and estimation in the planted partition model". In: *Probab. Theory Related Fields* 162.3-4 (2015), pp. 431–461. ISSN: 0178-8051. DOI: 10.1007/s00440-014-0576-6. URL: http://dx.doi.org/10.1007/s00440-014-0576-6.

[Mol12] Michael Molloy. "The freezing threshold for k-colourings of a random graph". In: *STOC'12—Proceedings of the 2012 ACM Symposium on Theory of Computing*. ACM, New York, 2012, pp. 921–929. DOI: 10.1145/2213977.2214060. URL: http://dx.doi.org/10.1145/2213977.2214060.

[Mos04] Elchanan Mossel. "Survey: information flow on trees". In: *Graphs, morphisms and statistical physics*. Vol. 63. DIMACS Ser. Discrete Math. Theoret. Comput. Sci. Amer. Math. Soc., Providence, RI, 2004, pp. 155–170.

[MP03] Elchanan Mossel and Yuval Peres. "Information flow on trees". In: *Ann. Appl. Probab.* 13.3 (2003), pp. 817–844. ISSN: 1050-5164. DOI: 10.1214/aoap/1060202828. URL: http://dx.doi.org/10.1214/aoap/1060202828.

[MRS08] Andrea Montanari, Federico Ricci-Tersenghi, and Guilhem Semerjian. "Clusters of solutions and replica symmetry breaking in random k-satisfiability". In: *J. Stat. Mech.* 2008.04 (2008), P04004. URL: http://stacks.iop.org/1742-5468/2008/i=04/a=P04004.

[MRTZ03] M. Mézard, F. Ricci-Tersenghi, and R. Zecchina. "Two solutions to diluted p-spin models and XORSAT problems". In: *J. Statist. Phys.* 111.3-4 (2003), pp. 505–533. ISSN: 0022-4715. DOI: 10.1023/A:1022886412117. URL: http://dx.doi.org/10.1023/A:1022886412117.

[MSW04] Fabio Martinelli, Alistair Sinclair, and Dror Weitz. "Glauber dynamics on trees: boundary conditions and mixing time". In: *Comm. Math. Phys.* 250.2 (2004), pp. 301–334. ISSN: 0010-3616. DOI: 10.1007/s00220-004-1147-y. URL: http://dx.doi.org/10.1007/s00220-004-1147-y.

[MSW07] Fabio Martinelli, Alistair Sinclair, and Dror Weitz. "Fast mixing for independent sets, colorings, and other models on trees". In: *Random Structures Algorithms* 31.2 (2007), pp. 134–172. ISSN: 1042-9832. DOI: 10.1002/rsa.20132. URL: http://dx.doi.org/10.1002/rsa.20132.

[MZ02] Marc Mézard and Riccardo Zecchina. "Random k-satisfiability problem: From an analytic solution to an efficient algorithm". In: *Physical Review E* 66.5 (2002), p. 056126.

[Pan13] Dmitry Panchenko. *The Sherrington-Kirkpatrick model*. Springer Monographs in Mathematics. Springer, New York, 2013, pp. xii+156. ISBN: 978-1-4614-6288-0; 978-1-4614-6289-7. DOI: 10.1007/978-1-4614-6289-7. URL: http://dx.doi.org/10.1007/978-1-4614-6289-7.

[Par02] Giorgio Parisi. *On local equilibrium equations for clustering states*. arXiv:cs/0212047. 2002.

[PT04] Dmitry Panchenko and Michel Talagrand. "Bounds for diluted mean-fields spin glass models". In: *Probab. Theory Related Fields* 130.3 (2004), pp. 319–336. ISSN: 0178-8051. DOI: 10.1007/s00440-004-0342-2. URL: http://dx.doi.org/10.1007/s00440-004-0342-2.

[RV14] Mustazee Rahman and Balint Virag. "Local algorithms for independent sets are half-optimal". In: *arXiv preprint arXiv:1402.0485* (2014).

[SC97] Laurent Saloff-Coste. "Lectures on finite Markov chains". In: *Lectures on probability theory and statistics (Saint-Flour, 1996)*. Vol. 1665. Lecture Notes in Math. Springer, Berlin, 1997, pp. 301–413. DOI: 10.1007/BFb0092621. URL: http://dx.doi.org/10.1007/BFb0092621.

[Sem08] Guilhem Semerjian. "On the freezing of variables in random constraint satisfaction problems". In: *J. Stat. Phys.* 130.2 (2008), pp. 251–293. ISSN: 0022-4715. DOI: 10.1007/s10955-007-9417-7. URL: http://dx.doi.org/10.1007/s10955-007-9417-7.

[Sly09] Allan Sly. "Reconstruction of random colourings". In: *Comm. Math. Phys.* 288.3 (2009), pp. 943–961. ISSN: 0010-3616. DOI: 10.1007/s00220-009-0783-7. URL: http://dx.doi.org/10.1007/s00220-009-0783-7.

[Sly11] Allan Sly. "Reconstruction for the Potts model". In: *Ann. Probab.* 39.4 (2011), pp. 1365–1406. ISSN: 0091-1798. DOI: 10.1214/10-AOP584. URL: http://dx.doi.org/10.1214/10-AOP584.

[SSZ16] Allan Sly, Nike Sun, and Yumeng Zhang. "The number of solutions for random regular NAE-SAT". In: *Foundations of Computer Science (FOCS), 2016 IEEE 57th Annual Symposium on*. IEEE. 2016, pp. 724–731.

[SZ14] Allan Sly and Yumeng Zhang. "Glauber Dynamics of colorings on trees". In: *arXiv preprint arXiv: 1412.3156* (2014).

[SZ16] Allan Sly and Yumeng Zhang. "Reconstruction of colourings without freezing". In: *arXiv preprint arXiv:1610.02770* (2016).

[Tet+12] Prasad Tetali et al. "Phase transition for the mixing time of the Glauber dynamics for coloring regular trees". In: *Ann. Appl. Probab.* 22.6 (2012), pp. 2210–2239. ISSN: 1050-5164. DOI: 10.1214/11-AAP833. URL: http://dx.doi.org/10.1214/11-AAP833.

[Vig00] Eric Vigoda. "Improved bounds for sampling colorings". In: *J. Math. Phys.* 41.3 (2000). Probabilistic techniques in equilibrium and nonequilibrium statistical physics, pp. 1555–1569. ISSN: 0022-2488. DOI: 10.1063/1.533196. URL: http://dx.doi.org/10.1063/1.533196.

[Wei04] Dror Weitz. *Mixing in time and space for discrete spin systems*. Thesis (Ph.D.)–University of California, Berkeley. ProQuest LLC, Ann Arbor, MI, 2004, p. 175. ISBN: 978-0496-05573-9. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:3147046.

[ZK07] Lenka Zdeborová and Florent Krząkała. "Phase transitions in the coloring of random graphs". In: *Phys. Rev. E (3)* 76.3 (2007), pp. 031131, 29. ISSN: 1539-3755. DOI: 10.1103/PhysRevE.76.031131. URL: http://dx.doi.org/10.1103/PhysRevE.76.031131.

[ZM08] Lenka Zdeborová and Marc Mézard. "Constraint satisfaction problems with isolated solutions are hard". In: *Journal of Statistical Mechanics: Theory and Experiment* 2008.12 (2008), P12004.