Fixing Variables in Random Satisfiability Problems

Mette Marie Skjøtt Rasmussen

Ph.D. Dissertation

August 2025

Colophon

Fixing Variables in Random Satisfiability Problems

The Stochastics Group
Department of Mathematics
Aarhus University
Ny Munkegade 118
8000 Aarhus C
Denmark
E-mail: mette.marie.skjoett@gmail.com

Also affiliated with Kvantify ApS
Rosenvængets Allé 25, st.
2100 København Ø
Denmark

Ph.D. thesis by Mette Marie Skjøtt Rasmussen. Written under supervision of professor Andreas Basse O'Connor, Department of Mathematics, Aarhus University, and Allan Grønlund, Kvantify Aps.

Layout and typography by the author based on a template by Josefine Bjørndal Robl. Typeset by the author with LaTeX and the memoir document class, using Linux Libertine 11pt on B5 paper.

Electronic version.

Abstract

The satisfiability problem (SAT) is one of the most mathematically fundamental decision problems, that serves as a central model for studying complexity of high-dimensional discrete structures. Formally, SAT asks whether a collection of Boolean constraints (disjunctive clauses) can be satisfied simultaneously. The SAT problem is intractable in the worst case, and much research goes into understanding which structural phenomena make the problem computationally hard.

To understand this, researchers have focused on average-case behavior through the random k-SAT model, where $m \sim \alpha n$ clauses of size k are sampled uniformly at random over n Boolean variables. This model is believed to exhibit rich structural phenomena, the most prominent being the satisfiability threshold conjecture, which claims a sharp phase transition at a critical clause-to-variable ratio.

This dissertation investigates the probabilistic effects of fixing variables in random SAT formulas, which is motivated both by theory and the practical role of partial assignments in SAT solving. We show that fixing variables smooths the satisfiability curve, which contrasts the expected sharp threshold of the standard model. The number of variables required to induce smoothing scales as $n^{1/2}$ for random 2-SAT below the satisfiability threshold, as $n^{2/3}$ for random 3-SAT below density $\alpha = 3.145$, and (weakly) as $n^{1/3}$ at the critical point of random 2-SAT. These results highlight sharp structural differences between 2- and 3-SAT, and between subcritical and critical 2-SAT.

Building on this, we define threshold functions π_k describing the asymptotic probability of satisfiability under partial assignments. We derive closed-form expressions for $k = 2$ and $k = 3$, with an unresolved gap in the 3-SAT case near the conjectured phase transition. Using analytic continuation, we prove that π_2 is regular (smooth and continuous), while π_3 is necessarily irregular. Thus, this rigorously separates the inherent structure of 2-SAT and 3-SAT. Simulations and an analysis of the related 3-XORSAT model further support that the irregularity in 3-SAT occurs at its conjectured satisfiability threshold.

Finally, from an algorithmic perspective, we study how fixing strategies affect satisfiability. Comparing random fixing with a majority rule policy that maximizes immediate clause satisfaction, we again obtain closed-form asymptotic probabilities, showing that informed fixing significantly improves performance.

Resume

Satisfiability-problemet (SAT) er et af de mest grundlæggende matematiske beslutningsproblemer, som ofte bruges som en model til at studere kompleksitet af højdimensionale diskrete strukturer. Formelt spørger SAT, om en mængde boolske restriktioner (disjunktive klausuler) kan opfyldes samtidigt. SAT problemet er NP-komplet i værste fald, og meget forskning forsøger at afdække, hvilke strukturelle fænomener, der medfører denne beregningsmæssige kompleksitet.

For at skabe en dybere forståelse for dette, betragter man ofte random k-SAT-modellen, hvor $m \sim \alpha n$ uafhængige klausuler af størrelse k vælges uniformt blandt n variable. Man formoder at denne model udviser en række strukturelle fænomener, hvoraf det mest velkendte er satisfiability threshold-formodningen, der postulerer en skarp faseovergang ved et kritisk klausul-til-variabel-forhold.

Vi undersøger hvilke sandsynlighedsteoretiske konsekvenser det har at fastlægge variable i random SAT-formler. Dette er motiveret både af teori og af den praktiske rolle som variabel-fastlæggelse har i SAT-solvere. Vi viser at variabel-fastlæggelse udglatter satisfiability-kurven, der før havde en skarp faseovergang. Ydermere viser vi, at antallet af variable, der skal fastlægges for at frembringe denne udglatning skalerer som $n^{1/2}$ for random 2-SAT, som $n^{2/3}$ for random 3-SAT, når $\alpha < 3.145$, og (svagt) som $n^{1/3}$ ved det kritiske punkt for 2-SAT. Resultaterne viser dermed tydelige strukturelle forskelle mellem de betragtede modeller.

Hernæst defineres tærskelfunktionerne π_k, der beskriver den asymptotiske sandsynlighed for, at en formel med fastlagte variable, er løselig. Vi udleder lukkede udtryk for tilfældende $k = 2$ og $k = 3$, men i 3-SAT-tilfældet er kurven stadig ukendt for α-værdier tæt på den formodede faseovergang. Vi kan dog ved hjælp af kompleks funktionsteori konkludere, at π_2 er regulær (glat og kontinuert), mens π_3 nødvendigvis er irregulær. Dermed adskiller 2- og 3-SAT sig fundamentalt. Simuleringer af tærskelfunktionerne samt en analyse af den beslægtede 3-XORSAT-model underbygger yderligere, at irregulariteten i 3-SAT indtræffer ved den formodede satisfiability-faseovergang.

Til sidst undersøges det, hvordan forskellige strategier for variabel-fastlægning påvirker den samlede løselighed af random SAT formler. Vi sammenligner tilfældig fastlægning med en strategi, hvor variable fastlægges således, at flest mulige klausuler straks opfyldes. Også her kan vi udlede lukkede udtryk for sandsynlighederne, hvilket giver præcise resultater for, hvordan informeret variabel-fastlæggelse markant øger sandsynligheden for, at en delvis løsning kan udvides til en fuldstændig løsning.

Acknowledgements

First and foremost, I would like to thank my university supervisor, Andreas Basse-O'Connor. Throughout this project, you consistently guided me and ensured that the plan remained clear and well-defined. Beyond your academic guidance, I am deeply grateful for your understanding and genuine support. These past three years would not have been the same without you. Next, I would like to thank my collaborator and fellow PhD student, Tobias Lindhardt Overgaard, for your unwavering belief in our project and for always bringing positivity and clarity when I needed it. Finally, I want to thank the other PhD students in the department, who became not only colleagues but also friends. I am truly glad to have you in my life today.

I would like to thank Innovation Fund Denmark for financing the project, and Kvantify for making it possible for me to pursue a PhD in the first place. I am also grateful to my company supervisor, Allan Grønlund, for welcoming me from the very beginning and making me feel like a part of the company. I want to thank my office mates and fellow PhD students at the company, Anton Alnor Christensen, Frederik Kofoed Marqversen, and Josefine Bjørndal Robl, for bringing humor and energy into everyday work life and for making it something I truly enjoyed. A special thanks goes to Anton for patiently looking over my shoulder during tedious calculations, and to Sebastian Yde Madsen for helping me whenever my own coding skills fell short. You have both dedicated many hours to helping me, and for that I am truly grateful.

I am also very grateful for the opportunity to do a research stay at the Technical University of Eindhoven. Thank you to my host Noela Müller. You welcomed me as part of the group from day one, and consistently took the time to meet with me and involve me in your research. I would also like to thank the many wonderful people I met in Eindhoven. Among them, I want to mention my office mates, Connor Riddlesden, Purva Joshi, and Sanne van Kempen, who made me feel genuinely welcomed and included from the very beginning, with a warmth and kindness that went far beyond anything I could have hoped for.

I owe a very special thank you to my previous study buddy and now very close friend, Mikael Møller Høgsgaard. Not only were you the one who made it possible for me to do this PhD in the first place, but you have also always believed in me like no other. You have always had my back, whether in work or in personal life.

I also want to thank the amazing people that I live with on Mejlgade, both past, present, and extended group. You have very quickly become some of my closest friends. Every day around you is a joy, and on the days when I feel down, you immediately make me feel better. You always keep an eye on me and make me believe in myself. I feel very blessed to have you in my life.

Lastly, I want to thank my family. To my parents, thank you for always encouraging me to do my best and, from the very beginning, for teaching me to prioritize school, put in effort, and not give up. And thank you to my sister. We have had each other since the very beginning, and I know you are always by my side. Thank you for always paying attention and checking in on me when I need it.

Contents

Preface

This thesis begins with an introduction to the main subject of the project, together with a presentation of the results obtained during my studies. This is followed by an overview of the proof strategies employed across the different articles. Following this are four self-contained papers, and finally a project containing some unfinished work:

Article A: Andreas Basse-O'Connor, Tobias Overgaard, and Mette Skjøtt,
Some Results on Random Mixed SAT Problems,
Accepted in proceedings of 23rd EYSM,
arXiv:2311.02644v1 [math.PR].

Article B: Andreas Basse-O'Connor, Tobias Overgaard, and Mette Skjøtt,
On the Regularity of Random 2-SAT and 3-SAT,
Preprint available on arXiv (2025),
arXiv:2504.11979v1 [math.PR].

Article C: Andreas Basse-O'Connor, and Mette Skjøtt,
Degrees of Freedom for Critical Random 2-SAT,
Preprint available on arXiv (2025),
arXiv:2505.15940v1 [math.PR].

Article D: Andreas Basse-O'Connor, Tobias Overgaard, and Mette Skjøtt,
Majority Rule Policy in Random 2-SAT and 3-SAT,
Manuscript in preparation (2025).

Project E: Andreas Basse-O'Connor, Tobias Overgaard, and Mette Skjøtt,
Regularity of Random 3-XORSAT,
Preliminary work (2025).

Article A and an early version of Article B were also included in my progress report for the Part A exam. All articles have been slightly adapted from their arXiv versions to ensure consistency of format and notation throughout the thesis.

1 Introduction

1.1 The Satisfiability Problem

The satisfiability problem, also referred to as the SAT problem, is a foundational problem that lies in the intersection between theoretical computer science and mathematical logic. It concerns the existence of solutions to general Boolean formulas which correspond to finding solutions to discrete logical expressions. To be more precise, the satisfiability problem asks a simple question: Given a logical formula φ built from Boolean variables, i.e. variables taking the values `true` and `false`, is there a way to assign the values of those variables such that the entire formula evaluates to `true`? If so, we write $\varphi \in \mathsf{SAT}$.

Thus, a logical formula consists of a set of Boolean variables $x_1, x_2, \ldots, x_n$ each of which takes values in $\mathbb{B} := \{\texttt{true}, \texttt{false}\}$. The logical formula is then formed using logical operators like negation ($\neg$), conjunction ($\wedge$), disjunction ($\vee$), implications ($\Rightarrow$), etc. Therefore, a logical formula could take the form

$$(x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \Rightarrow x_2), \quad (x \in \mathbb{B}^2).$$

The above expression states that either x_1 or x_2 should be `true`, either x_1 or x_2 should be `false`, and if x_1 is `true` then x_2 has to be `true` as well. The only variable assignment satisfying this is $x_1 = \texttt{false}$, and $x_2 = \texttt{true}$.

1.1.1 CNF and Standard Formulations

Both in practice and theory, SAT is usually studied using formulas in a specific form called conjunctive normal form, abbreviated CNF. In this work, we only consider Boolean formulas in this general form. A CNF formula is a conjunction, i.e. the logical `AND` of clauses, where each clause is a disjunction, i.e. the logical `OR` of literals, and a literal is either a variable or its negation. For example:

$$(x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_2 \vee \neg x_3) \wedge (x_2 \vee \neg x_4), \quad (x \in \mathbb{B}^4),$$

is a CNF formula with three clauses and four variables. Every Boolean formula can be converted into an equivalent formula in CNF, see Prop. 1.5 in [Men09]. Thus, the SAT problem with formulas written in CNF remains as general as the original formulation of the problem, and this formulation of the problem is simpler to study mathematically and algorithmically. A sub-class of problems that is often considered in theory are problems where clauses are restricted to have a certain length k. This problem is then referred to as the k-SAT problem.

1.1.2 Computational complexity and NP-completeness

The satisfiability problem holds a central role in computational complexity theory due to its role as the first problem proven to be NP-complete, [Coo71]. This result laid the foundation for the theory of NP-completeness, which classifies problems based on their inherent computational difficulty.

The class NP consists of all decision problems for which a solution, if given, can be verified in polynomial time. A problem is NP-complete if it is in NP and is also as hard as any other problem in NP, meaning that every problem in this class can be reduced to it in polynomial time.

As SAT is NP-complete it is considered one of the "hardest" problems in NP. If one could find a polynomial-time algorithm to solve SAT, it would imply that every problem in NP can also be solved in polynomial time, leading to the conclusion that $P = NP$. However, despite decades of research, no such algorithm has been found, and $P \neq NP$ remains one of the most important and unresolved questions in mathematics and computer science.

The standing conjecture is that $P \neq NP$ which would imply that the computational effort required to solve SAT grows exponentially with the size of the input. This exponential blow-up is what makes SAT and other NP-complete problems fundamentally hard.

Although the general SAT problem is in NP, there are subclasses that differ significantly in complexity. One notable exception is 2-CNF formulas, which can be solved in polynomial time. However, for every $k \geq 3$, the k-SAT problem is NP-complete. Since all NP-complete problems are equivalent in terms of computational difficulty (up to polynomial factors), much of the theoretical research has focused on 3-CNF formulas as a canonical representative of NP-completeness. Consequently, there is considerable interest in understanding the structural and computational differences that make 2-SAT easily solvable while 3-SAT is believed to be hard. In addition, much research is devoted to identifying which instances of 3-SAT are hard, and what structural properties make them hard. In this thesis, we contribute towards answering these questions.

1.1.3 Practical Applications of SAT

Despite being a theoretically hard problem, SAT has proven to be very useful in practice. Over the past few decades, significant progress has been made in designing algorithms that can efficiently determine the satisfiability of large CNF formulas in many real-world cases. Therefore, SAT is widely used in a variety of domains, including:

- **Hardware and Software Verification:** Ensuring that digital circuits or programs behave correctly on all possible inputs can be translated into a SAT problem.
- **Artificial intelligence and planning:** Many constraint satisfaction and planning problems can be encoded as SAT instances.
- **Combinatorial problems:** Problems such as scheduling, resource allocation, and puzzle solving can often be reformulated as a SAT problem.

For references, see e.g. [GGW06; Mar08; Knu15]. The practical success of SAT solvers demonstrates that while the worst-case complexity of SAT is high, many instances arising in practice are solvable in reasonable time. This paradox is a key area of ongoing research, aiming to better understand the boundary between tractable and intractable SAT instances.

1.1.4 The Random Satisfiability Problem

The gap between the theoretical hardness of SAT on one side and the practical efficiency of modern SAT solvers on the other side has led researchers to develop models that capture typical-case behavior rather than worst-case complexity (see [Gol79; FP83; CKT91; SML96]). This led to the development of the random SAT model, which shifts the focus to average-case complexity and permits the derivation of statistical properties of SAT instances.

In the random SAT framework, Boolean formulas are generated according to a specified probability distribution. The most widely studied variant is the random k-SAT model, where each formula has a fixed number of variables n and a number of clauses m, that are sampled independently. Each clause is formed by selecting k literals uniformly at random. Whether the literals are sampled with or without replacement varies across formulations, but this detail typically does not affect the asymptotic behavior in most analyses. In Articles A to C we consider the model, where each clause consists of distinct variables, whereas Article D considers the model where all literals are sampled independently, and thus clauses with duplicate variables can occur.

In the random k-SAT model, it has especially been studied how the satisfiability of a sampled formula depends on the clause-to-variable ratio $\alpha = m/n$. Empirical and theoretical investigations indicate that as this ratio α increases the probability that a random formula is satisfiable drops from one to zero, and asymptotically in n this threshold is sharp. This conjecture was originally stated in [CR92], where this phenomena was also proven for $k = 2$, and it was further established that the 2-SAT satisfiability threshold appears at $\alpha = 1$, see [CR92],[Goe96]. Very recently, the satisfiability conjecture was also established for all $k \geq k_0$, where k_0 is a large and unknown constant, see [DSS22]. However, for all remaining values of k the existence of the satisfiability threshold is a standing conjecture. A step towards proving this conjecture was established by Friedgut. His result states that if a limiting probability curve exists, then it will be sharp:

Theorem 1.1 (Friedgut, [Fri99]). *Let $k \geq 2$. There exists a sequence $\{a_k(n)\}_{n=1}^{\infty}$ such that for every $\varepsilon > 0$ it holds that:*

- *If Φ is a random CNF formula with n variables and $m(n) = \lfloor (a_k(n) - \varepsilon)n \rfloor$ clauses, then*
$$\lim_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) = 1,$$
- *If Φ is a random CNF formula with n variables and $m(n) = \lfloor (a_k(n) + \varepsilon)n \rfloor$ clauses, then*
$$\lim_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) = 0.$$

The study of the random SAT model has further led to insights about the internal structure of the solution space. For instance, in certain regimes, it is believed that satisfying assignments tend to cluster into exponentially many disconnected components, a phenomenon that mirrors behaviors seen in statistical physics, particularly in spin glass theory. This connection has inspired the use of tools from statistical physics, such as replica symmetry breaking and the cavity method, to analyze the geometry and complexity of solution spaces in random SAT. For more information, see e.g. [BCM02], [MM09] and references therein.

1.2 Fixing Variables in Satisfiability Problems

The work of this thesis is concerned with the probabilistic effects of fixing a subset of the input variables in random satisfiability formulas. More precisely, it is studied how the assignment of Boolean values to a small subset of the input variables, either chosen uniformly at random or according to specific heuristics, impacts the overall satisfiability of the formula. This idea is motivated by both practical and theoretical considerations.

On the practical side, many modern SAT solvers rely on early decisions, which correspond to partial assignments of the input variables, and the success of these solvers often depends on how those decisions reduce the problem's complexity.

Moreover, fixing variables is closely connected to having clauses of length one, also referred to as unit clauses. These clauses will often appear during the SAT solving process. A sub-routine in most modern SAT solvers, called the unit propagation procedure, exploits these unit clauses and that they directly determine the value of specific variables, effectively fixing them. Fixing these variables simplifies the formula, potentially generating new unit clauses and triggering a cascading effect of further variable assignments. Understanding the probabilistic impact of variable fixing can therefore provide valuable algorithmic insights. Besides appearing during the SAT solving process, unit clauses also often arise in real-world applications where some variables are known in advance or constrained by external factors. Thus, this underscores the practical significance of understanding variable fixing. For more information on the practical implications of variable fixing see e.g. [Knu15] p. 31, 39, and 62.

From a theoretical perspective, variable fixing provides a useful tool for analyzing the hardness of SAT instances. According to the satisfiability conjecture, most random k-CNF formulas are either asymptotically satisfiable or asymptotically unsatisfiable as the number of variables tends to infinity, exhibiting a sharp threshold at a critical clause-to-variable ratio. However, this sharp threshold behavior disappears when a subset of variables is fixed in random k-SAT. By fixing a carefully selected fraction of the input variables, the satisfiability probability transitions smoothly from near zero to near one as the clause-to-variable ratio varies. This is the main result of Article B.

The number of variables that must be fixed to induce such a smooth transition reveals important information about the underlying dependency structure of the variables of the formula. It also sheds light on how the geometry of the solution space changes with varying clause lengths and clause-to-variable densities. In particular, this highlights how different levels of local constraints influence global satisfiability, and how contradictions begin to emerge as an increasing fraction of variables is fixed.

1.2.1 Degrees of freedom in random satisfiability problems

Let Φ be a random CNF formula with n variables and m clauses. We consider a subset $\mathcal{L} \subseteq \pm[n] := \{-n, \dots, -1, 1, \dots, n\}$, which consists of $|\mathcal{L}| = f(n)$ elements. Moreover, we choose this set such that if $\ell \in \mathcal{L}$ then $-\ell \notin \mathcal{L}$, and we say that this set is *consistent*. We will now fix the variables dictated by $\mathcal{L}$ by having $x_v = \texttt{true}$ if $v \in \mathcal{L}$ and $x_v = \texttt{false}$ if $-v \in \mathcal{L}$. For $x \in \mathbb{B}^n$, we let $x_{\mathcal{L}} \in \mathbb{B}^n$ be the vector where the v'th entry is given by $(x_{\mathcal{L}})_v = \texttt{true}$ when $v \in \mathcal{L}$, $(x_{\mathcal{L}})_v = \texttt{false}$, when $-v \in \mathcal{L}$, and $(x_{\mathcal{L}})_v = x_v$ otherwise. Then we define the CNF formula with fixed variables as

$$\Phi_{\mathcal{L}}(x) = \Phi(x_{\mathcal{L}}), \quad (x \in \mathbb{B}^n). \tag{1.2.1}$$

Now, the previous considerations concerning fixing of variables in random CNF formulas lead us to the following definition:

Definition 1.2 (Degrees of freedom in the random k-SAT problem). *Let Φ be a random k-CNF formula with n variables, and $m = m(n)$ clauses. Then Φ is said to have $f_\star = f_\star(n)$* degrees of freedom *if for all $f = f(n)$, and all consistent (non-random) subsets $\mathcal{L} \subseteq \pm[n]$, with $|\mathcal{L}| = f$, it is the case that $f_\star$ is a threshold in f for the satisfiability of $\Phi_{\mathcal{L}}$, i.e. if*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \begin{cases} 1, & \textit{when } f/f_* \to 0, \\ 0, & \textit{when } f/f_* \to \infty. \end{cases} \tag{1.2.2}$$

The main result of Article B states that the random 2-SAT problem sampled strictly below the satisfiability threshold (referred to as a subcritical formula) has degrees of freedom scaling as $n^{1/2}$. In contrast, for random 3-SAT instances with a clause-to-variable ratio below 3.145 the degrees of freedom scale as $n^{2/3}$. Thus, the degrees of freedom depend heavily on the clause size. This difference indicates that variables in random 2-SAT instances are more tightly constrained and exhibit stronger dependencies than those in random 3-CNF formulas.

For structures that exhibit phase transitions, the critical point, where the sharp transition occurs, is often of particular interest. However, analyzing such critical formulas is typically more challenging, as structural complexity tends to peak near the threshold. In Article C, 2-SAT is analyzed at the critical ratio, and the degrees of freedom are found in a weak sense, see the following definition:

Definition 1.3 (Weak degrees of freedom in the random k-SAT problem). *Let Φ be a random k-CNF formula with n variables, and $m = m(n)$ clauses. Then Φ is said to have $f_\star = f_\star(n)$ degrees of freedom weakly if for all $f = f(n)$, and all consistent (non-random) subsets $\mathcal{L} \subseteq \pm[n]$, with $|\mathcal{L}| = f$ it is the case that $f_\star$ is a weak threshold in f for the satisfiability of $\Phi_{\mathcal{L}}$, that is for any $\varepsilon > 0$ we have that*

(1) Whenever $f/f_\star \le n^{-\varepsilon}$, then

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) > 0.$$

(2) Whenever $f/f_\star \ge n^{\varepsilon}$, then

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0.$$

The main result of Article C shows that a random 2-CNF formula with n variables and n clauses, i.e. sampled precisely at the point of phase transition, has degrees of freedom (in a weak sense) that scale as $n^{1/3}$. This marks a sharp change in the structure of the solution space and in the variable dependency at criticality compared to at the subcritical regime.

Although this change in structure has been proven only for random 2-SAT (which is computationally easy), this might still provide valuable insights to why computational hardness of problems often increases tremendously close to the (expected) phase transition, as seen on fig. 1.1. The sudden reduction in degrees of freedom suggests that at the critical point even fixing only very few variables can have global effects, which might explain why solving random formulas becomes much harder close to the point of criticality.

Combining the results of Article B and Article C we get the below theorem.

Theorem 1.4. *Let Φ be a random k-CNF formula with n variables and $m \sim \alpha n$ clauses.*

- *If $k = 2$, and $\alpha \in (0, 1)$, then the degrees of freedom of Φ scale as $n^{1/2}$.*
- *If $k = 3$, and $\alpha \in (0, 3.145)$, then the degrees of freedom of Φ scale as $n^{2/3}$.*
- *If $k = 2$ and $\alpha = 1$ then the weak degrees of freedom of Φ scale as $n^{1/3}$.*

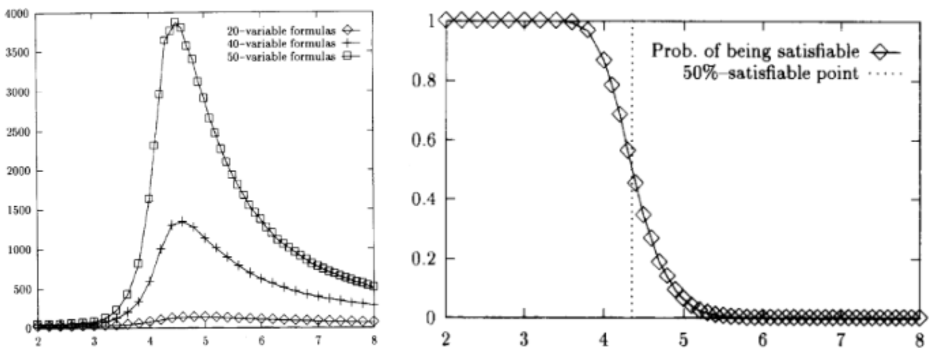


Figure 1.1: Left: Fig. 2 from [SML96] showing median "hardness" as a function of clause-to-variable density for random 3-SAT. Right: Fig. 4 from [SML96] showing the corresponding empirical probability of satisfiability.

1.3 Phase Transition Curves

As previously mentioned, a key property of the random k-SAT problem is its conjectured sharp phase transition when the clause-to-variable ratio surpasses a critical value. For $k = 2$, this phase transition has been rigorously proven. However, for $k \geq 3$ it remains an open conjecture that is only supported by empirical evidence and heuristic arguments.

1.3.1 Phase Transitions in Mixed SAT Problems

Random mixed CNF formulas, i.e. those involving clauses of varying lengths, have also received attention in the literature. In [Ach+01], the authors study a mixed 2- and 3-SAT model. They show that adding $(2/3)n$ independent, and uniformly distributed random 3-clauses to a random 2-CNF formula does not affect its satisfiability w.h.p. Furthermore, they prove that if a limiting satisfiability curve exists, it must exhibit a sharp threshold behavior, i.e. a result like Theorem 1.1 also applies here.

In contrast, a different phenomenon arises when 1-clauses are added to a random k-CNF formula. Here, the presence of unit clauses smooths the satisfiability curve, making the transition more gradual rather than abrupt. A more comprehensive overview of results on mixed CNF formulas, along with the theoretical foundations and remaining open questions, is provided in the survey paper Article A. In Article B we provide the exact limiting probability curve for mixed 1- and k-SAT, $k = 2, 3$:

Theorem 1.5. *Let Φ_1 be a random 1-CNF formula with n variables and $\sim \beta n^{1/2}$ clauses for some $\beta > 0$. Let Φ_k be a random k-CNF formula with n variables and $\sim \alpha n$ clauses, for some $\alpha > 0$. Let $\Phi_1 \wedge \Phi_k$ denote the mixed CNF formula.*

- *If $k = 2$, and $\alpha \in (0, 1)$ then $\lim_{n\to\infty} \mathbb{P}(\Phi_1 \wedge \Phi_2 \in \mathsf{SAT}) = e^{-(\beta/2)^2(1-\alpha)^{-1}}$.*
- *If $k = 3$, and $\alpha \in (0, 3.145)$ then $\lim_{n\to\infty} \mathbb{P}(\Phi_1 \wedge \Phi_3 \in \mathsf{SAT}) = e^{-(\beta/2)^2}$.*

Note that in the case $k = 2$, the limiting probability curve is smooth and depends jointly on the number of both 1- and 2-clauses present. In contrast, for $k = 3$ the limiting probability curve depends only on the amount of 1-clauses. Consequently, adding or removing (some) 3-clauses has no effect on the overall satisfiability of the formula. This illustrates that random mixed 1- and 2-SAT behaves fundamentally differently from random mixed 1- and 3-SAT.

1.3.2 Smooth Phase Transitions when Fixing Variables

The main difference between fixing variables and adding unit clauses is whether or not we allow contradictions initially. Consequently, Theorem 1.5 can be reformulated such that variable fixing is considered instead. Therefore, Article B also establishes the following theorem:

Theorem 1.6. *Let Φ be a random k-CNF formula with n variables and $m \sim \alpha n$ clauses. Let $\mathcal{L} \subseteq \pm[n]$ be a consistent set with $|\mathcal{L}| = f = f(n)$. Let also $\gamma \in (0, \infty)$.*

- *If $k = 2$, $\alpha \in (0, 1)$, and $f\sqrt{m}/n \to \gamma$, then*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^2(1-\alpha)^{-1}}.$$

- *If* $k = 3$, $\alpha \in (0, 3.145)$, *and* $f m^{1/3}/n \to \gamma$, *then*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^3}.$$

Thus, fixing variables smooths the phase transition curve, making it vary gradually between zero and one rather than exhibiting a sharp threshold. This reflects a more gradual structural change as the clause-to-variable ratio slowly approaches the (expected) phase transition. Moreover, for both $k = 2$ and $k = 3$, the limiting probability curve depends on the number of unit clauses as well as the number of k-clauses (since γ depends on both α and β). When $k = 3$ this stands in contrast to the case of mixed formulas. The difference arises because, in mixed 1- and 3-SAT, the limiting probability is determined solely by whether the unit clauses contradict each other, whereas under variable fixing it instead equals the probability that the forced variable assignments cause a 3-clause to be immediately unsatisfiable.

1.3.3 Simulations

To examine whether theory and practice align, random CNF formulas have been generated, where a subset of input variables are fixed. Using the SAT solving algorithm MiniSAT22, available through the Python package [IMM18], the proportion of such formulas that are satisfiable was computed. The simulations were carried out for $k = 2$ and $k = 3$ across varying values of n, m, and f, and the results are shown in fig. 1.2.

From the plot, we note that the probability converges faster for random 2-SAT than for random 3-SAT. Furthermore, the rate of convergence decreases noticeably as the system approaches the (expected) phase transition point, which for 2-SAT is at $\alpha = 1$ and for 3-SAT is conjectured to be at $\alpha \approx 4.267$, [KS94].

1.4 Regularity of Random SAT

It turns out that Theorem 1.6 not only provides valuable insights into the effects of fixing variables, but it also reveals a striking structural difference between 2-SAT and 3-SAT that, to the best of our knowledge, has not been rigorously established before.

1.4.1 The Threshold Function

Theorem 1.6 implies that we can define a threshold function for a random k-CNF formula. For $k = 2, 3$, and $\alpha > 0$ we can let Φ be a random k-CNF formula with n variables and m clauses, where $m \sim \alpha n$. If we further let $\mathcal{L} \subseteq \pm[n]$ with $|\mathcal{L}| = f(n)$, where $f/n^{1-1/k} \to \beta$, then we can define the following threshold function:

$$\pi_k(\alpha, \beta) = \lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}),$$

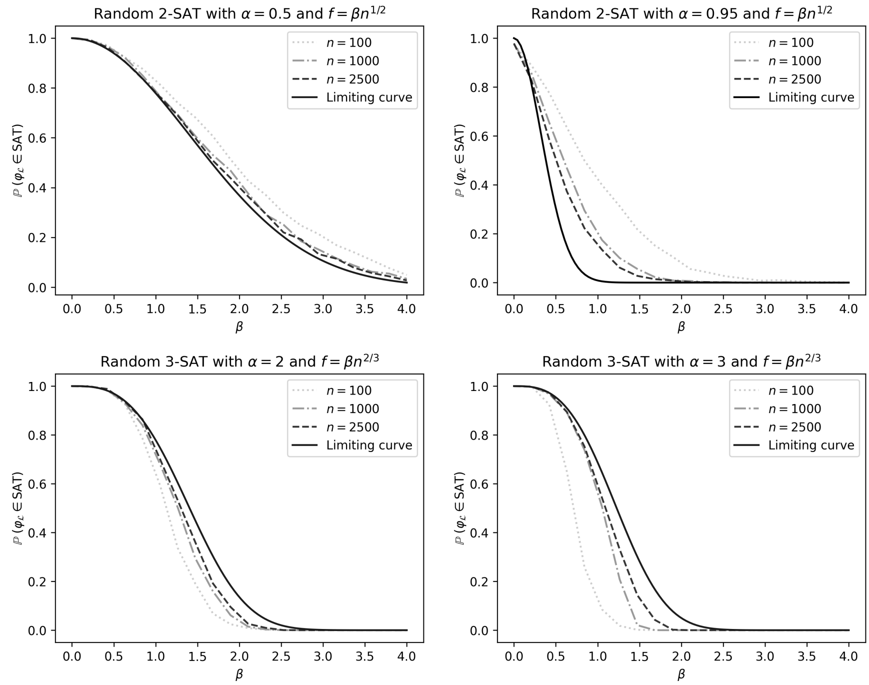


Figure 1.2: Simulations of the satisfiability of random 2- and 3-SAT problems with fixed variables. Each datapoint (40 for each curve) is made from 2000 simulations. The figure is also included in Article B.

when the limit exists and depends only on α and β, and we let $\pi_k(\alpha, \beta) = 0$ in the remaining cases. Theorem 1.6 implies that

$$\begin{aligned} \pi_2(\alpha,\beta) &= e^{-(\beta/2)^2 \frac{\alpha}{1-\alpha}}, \quad \text{when } 0 < \alpha < 1, \\ \pi_3(\alpha,\beta) &= e^{-(\beta/2)^3 \alpha}, \quad \text{when } 0 < \alpha < 3.145. \end{aligned} \tag{1.4.1}$$

The proven 2-SAT satisfiability threshold implies that $\pi_2(\alpha, \beta) = 0$ when $\alpha > 1$. Moreover, in the article [Día+09] they prove that when $\alpha > 4.4898$ in random 3-SAT, then the formula is asymptotically unsatisfiable, and this is currently the best upper bound. Consequently, for such α it is the case that $\pi_3(\alpha, \beta) = 0$. Using this and eq. (1.4.1) the functions π_2 and π_3 can be plotted for some values of α and β. These plots can be seen on fig. 1.3.

Note that $\pi_3(\alpha, \beta)$ is known for all α's except the ones belonging to the interval $[3.145, 4.4898]$. This explains the gap in the plot at the right of fig. 1.3. What happens for α belonging to the interval $[3.145, 4.4898]$ remains an open question, and there are several different possibilities for what could happen.

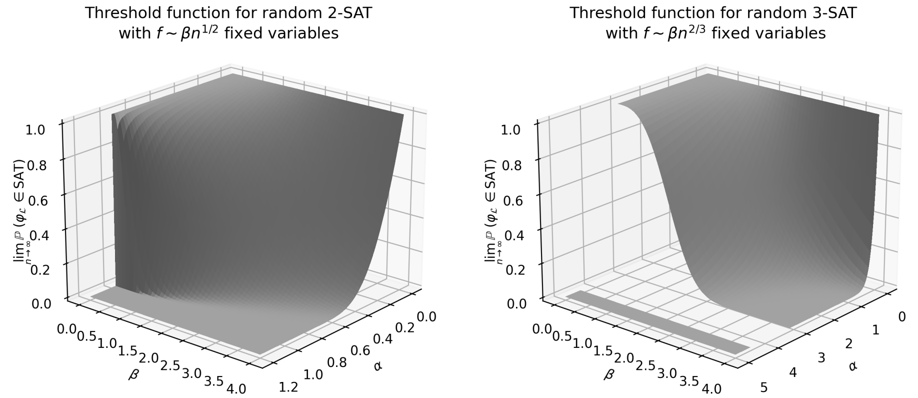


Figure 1.3: The threshold functions corresponding to the degrees of freedom in the random 2-SAT and 3-SAT problems. This figure is also included in Article B.

For the random 2-SAT problem, we see that the threshold function is continuous and even smooth for $\alpha \in (0, 1)$. When for any fixed $\beta > 0$, the threshold function for a random k-SAT problem is smooth for $\alpha \in (0, \alpha_{\text{supp}}(k))$, with $\alpha_{\text{supp}}(k) := \inf\{\alpha : \pi_k(\alpha, \beta) = 0\}$, and continuous for all $\alpha > 0$, we refer to it as a *regular* threshold function. It is remarkable that even though the threshold function for the random 3-SAT problem is not fully known, we can conclude that it is *not* regular. This follows from the identity theorem for analytic functions. This is remarkable as nothing was previously proven mathematically for any α belonging to the interval $[3.52, 4.49]$, see [HS03; KKL06; Día+09].

We have concluded, that there must be some irregularity in the curve $\pi_3(\alpha, \beta)$ over the interval $\alpha \in [3.145, 4.4898]$. This suggests a fundamental shift in the structure of the solution space of random 3-CNF formulas as α varies smoothly close to the expected phase transition, and this irregularity is not seen for random 2-SAT. These considerations correspond to the following corollary:

Corollary 1.7. *For the random 2-SAT problem, the threshold function $\pi_2(\alpha, \beta)$ is regular, while for the random 3-SAT problem it is irregular, i.e. it cannot be both analytic for $\alpha \in (0, \alpha_{\text{supp}}(3))$ and continuous for all $\alpha > 0$.*

The above corollary *rigorously* separates random 2-SAT and random 3-SAT showing that the problems belong to different *universality classes* with respect to their phase transitions, and thus the 3-SAT problem is provably more irregular than the 2-SAT problem. This irregularity may help explain why computational hardness peaks near the expected satisfiability threshold in random 3-SAT, and why 2- and 3-SAT problems differ so fundamentally in computational complexity.

1.4.2 The Backbone of Random SAT

For decades, researchers have sought to understand the structural differences between computationally easy and hard problems. One influential line of work, inspired by statistical physics, compares random SAT instances to spin systems, where sharp phase transitions are known to occur.

This analogy led to the introduction of the so-called *backbone* of random SAT, an order parameter that captures structural rigidity in satisfying assignments. The backbone is defined as the set of variables that take the same value in all assignments satisfying the maximum possible number of clauses. Such variables are often referred to as *frozen variables*. For many years, the backbone has served as a key tool for understanding the behavior of random SAT (see, e.g., [Mon+99]).

Using non-rigorous but powerful methods from statistical physics (e.g., replica symmetry breaking and the cavity method), physicists have suggested that in random 2-SAT the backbone grows continuously as the clause density α increases, whereas in random 3-SAT the backbone exhibits a discontinuous jump at the conjectured satisfiability threshold. Moreover, estimates of the backbone density for random 3-SAT vary widely (from roughly 0.4 to 0.94) depending on the method of analysis (see [Mon+99]). A major difficulty in estimating the backbone lies in its definition: determining it requires finding assignments that maximize the number of satisfied clauses, an NP-hard task that is even harder than finding a single satisfying assignment (which is "only" in NP).

When Article B introduces the fixing of variables, this can be viewed as a related but distinct order parameter, in some sense dual to the backbone. Unlike the backbone, however, this new order parameter admits a mathematically rigorous closed-form characterization for both $k = 2$ and $k = 3$, where also regularity has been established for random 2-SAT, and irregularity has been established for random 3-SAT.

1.4.3 The Gap in the 3-SAT Threshold Function

Corollary 1.7 implies that the threshold function for 3-SAT, π_3, exhibits a break in regularity for some α within the interval $[3.145, 4.4898]$. This break can happen in several ways. The most natural conjecture, supported by the backbone predictions from statistical physics (and consistent with our own view), is that the break occurs precisely at the satisfiability threshold, believed to be at $\alpha \approx 4.267$ [KS94]. If this is the case, then π_3 would have the strongest possible form of irregularity. Alternatively, assuming the 3-SAT satisfiability threshold exists, the break could occur at a lower value of α, either as a loss of smoothness or continuity. Besides the satisfiability transition itself, other sharp structural transitions in the solution space are believed to take place, such as *condensation* and *freezing*. These transitions are linked to drastic changes in the geometry and connectivity of the solution space, and it is also possible that the irregularity in π_3 arises at one of these critical densities rather than at the satisfiability threshold.

To gain insight into this open interval where π_3 is unknown, we carried out numerical experiments using the Backtracking Survey Propagation (SP) algorithm introduced in [MPR16] and implemented in [MM20]. Since SP is incomplete, the resulting satisfiability curves may underestimate the true probabilities. Our simulations were performed for instance sizes up to $n = 100.000$, and we generated satisfiability curves both for plain random 3-SAT and for 3-SAT with fixed variables, as seen on fig. 1.4.

Although π_3 remains undetermined for $\alpha \in [3.145, 4.4898]$, the simulations suggest that the threshold curve is smooth all the way up to at least $\alpha \approx 4$ (when $\beta = 1$). Interestingly, when variables are fixed, the convergence rate of the satisfiability curve slows dramatically starting from around $\alpha = 3$, whereas for standard 3-SAT the convergence to a sharp drop in satisfiability occurs much more quickly. We do not currently have a conjecture for why this is the case.

1.4.4 Threshold Function for Random 3-XORSAT

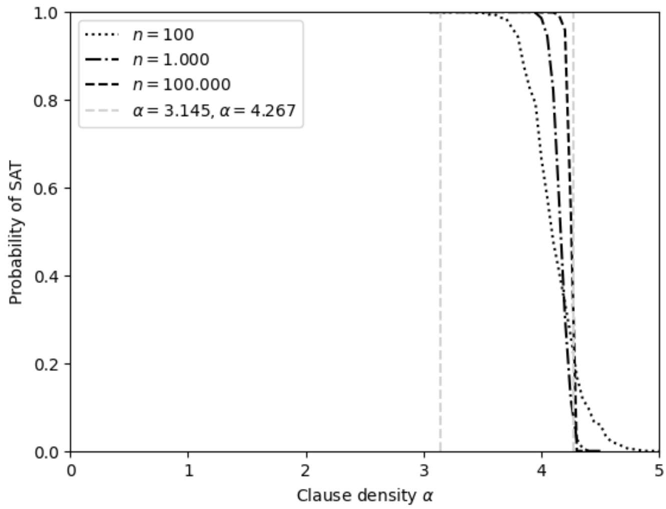
An alternative way of supporting the conjecture that random 3-SAT exhibits a discontinuity at its phase transition is to establish the corresponding result for a closely related model. Therefore, we consider the random 3-XORSAT model Φ^{XOR} with $m \sim \alpha n$ clauses over n Boolean variables. Here, each clause consists of three variables sampled uniformly at random from $[n]$, along with a uniformly random boolean value. Then each constraint is the logical `xor` of the variables that has to equal the sampled boolean value. Thus, Φ^{XOR} corresponds to a system of m linear equations in n variables over the field $\mathbb{F}_2$, with each equation involving exactly three nonzero coefficients. The goal is to determine whether there exists an assignment satisfying all equations.

Compared to random 3-SAT, the random 3-XORSAT model is better understood (see [DM02a; AM15; Ibr+15a; PS16; Ayr+20; Coj+24]). In particular, it has been rigorously established that 3-XORSAT has a sharp satisfiability threshold. This is noteworthy since random 3-SAT and 3-XORSAT are believed to share many structural similarities. For example, 3-XORSAT has been shown to undergo a clustering phase transition [Ibr+15b], a phenomenon also conjectured to occur in random 3-SAT [MPR16].

Let $\mathcal{L} \subseteq \pm[n]$ with $|\mathcal{L}| \sim \beta n^{2/3}$ and consider the formula with fixed variables $\Phi^{\text{XOR}}_{\mathcal{L}}$ defined as in eq. (1.2.1). In Project E, we provide calculations suggesting that

$$\pi_3^{\text{XOR}}(\alpha, \beta) := \lim_{n\to\infty} \mathbb{P}(\Phi^{\text{XOR}}_{\mathcal{L}} \in \mathsf{SAT}) = e^{-\beta^3 \alpha/2}. \tag{1.4.2}$$

for α up until the phase transition at $\alpha \approx 0.928$, [DM02b]. These preliminary results indicate that 3-SAT and 3-XORSAT exhibit similar behavior when partial



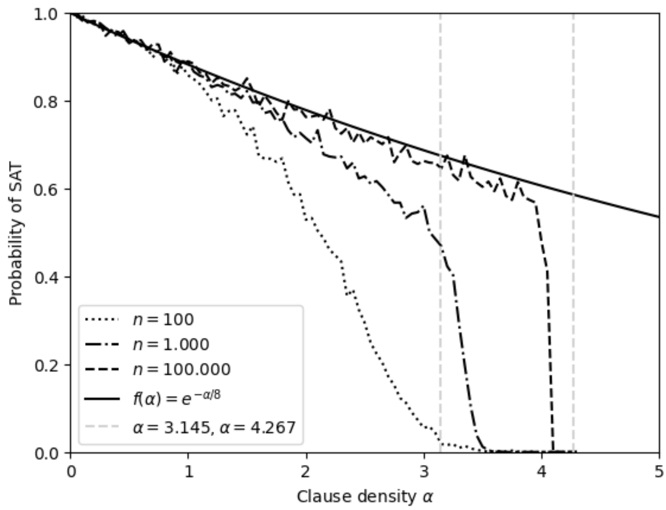


Figure 1.4: Top: Empirical probability of satisfiability for random 3-SAT as a function of α. Bottom: Empirical estimates of $\pi_3(\alpha, 1)$ as a function of α. Each data point in each curve is based on 1.000 samples.

assignments are introduced, and thus strengthens the conjecture that the irregularity of 3-SAT appears at its conjectured phase transition.

As a first step, we aim to establish that the asymptotic probability of $\Phi_{\mathcal{L}}^{\text{XOR}}$ being satisfiable equals zero only when the clause-to-variable ratio exceeds the satisfiability threshold. While the proof is not yet complete, the ongoing calculations supporting this claim are presented in Project E.

1.5 Algorithms for Solving Satisfiability Problems

As previously discussed, the concept of variable fixing is closely connected to SAT solving. This relationship is affirmed in Knuth's book [Knu15], where he states: "Algorithms for SAT usually deal exclusively with consistent partial assignments; the goal is to convert them to consistent total assignments, by gradually eliminating the unknown values." Algorithms that gradually fix variables are commonly referred to as DPLL algorithms. These methods exploit unit clauses that emerge during the solving process, which in turn trigger further variable assignments. Even modern SAT solvers, such as state-of-the-art conflict-driven clause learning (CDCL) solvers, rely heavily on variable fixing (see [Knu15], p. 62). Consequently, understanding how this mechanism affects SAT solving is essential. Conceptually, variable fixing corresponds to a systematic traversal of the search tree of the problem, see fig. 1.5. If variables are fixed without taking the structure of the CNF formula into account, then in the case of random 2-SAT, contradictions arise after asymptotically on the order of $n^{1/2}$ variables have been fixed. For random 3-SAT, contradictions will appear after $n^{2/3}$ variables are fixed asymptotically. This was the result of Theorem 1.4

1.5.1 Fixing Variables According to Majority Rule Policy

In Article D we consider what happens when variables are fixed dependently on the CNF formula in consideration. To be more precise we decide which variables to fix independently of the random formula, and then the signs are chosen dependently such that the maximum number of clauses become satisfied from these initial variable assignments.

Let Φ be a random CNF formula over n variables. For each $v \in [n]$, let the random variables A_v^+ and A_v^- denote the number of times the literals v and $-v$, respectively, appear in Φ. Given a subset $\mathcal{L} \subseteq [n]$, we then fix the variables corresponding to the set:

$$\mathcal{L}_{\mathrm{MR}} := \left\{ S \cdot v \colon v \in \mathcal{L}, S = \operatorname{sgn}(A_v^+ - A_v^-) \right\}, \tag{1.5.1}$$

where we define $\operatorname{sgn}(0) := 1$. By definition, we get that $\mathcal{L}_{\mathrm{MR}}$ is consistent, and unlike previously, this set depends on the random formula Φ. When variables are fixed according to this set, we refer to the strategy as the *majority rule policy*. The main result of Article D is the following:

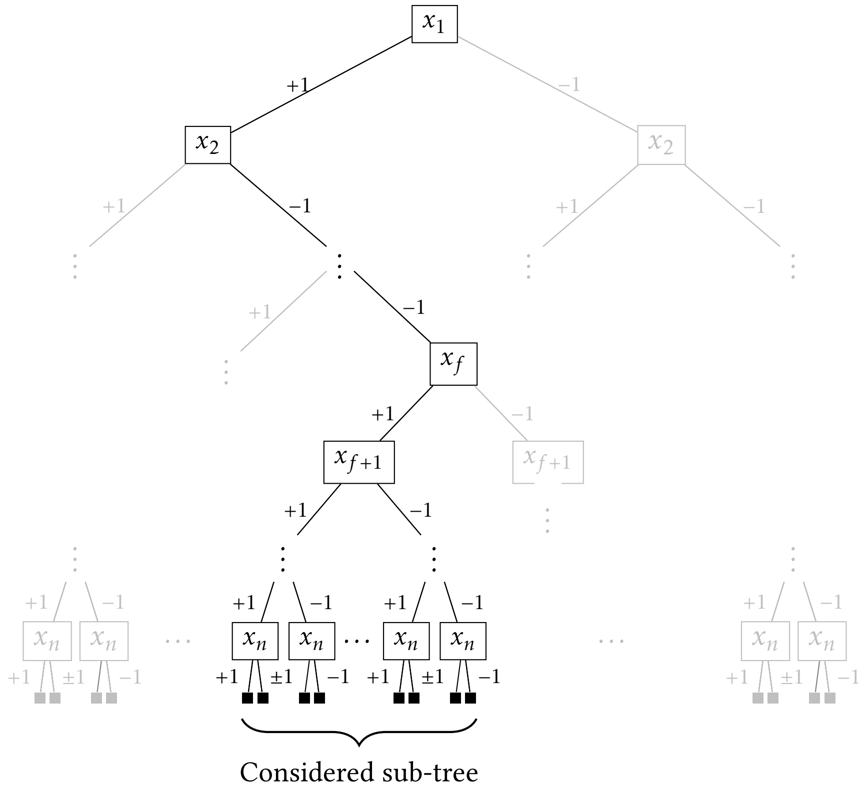


Figure 1.5: Traversing f nodes in the search tree and thus only considering assignments $x \in \mathbb{B}^n$ on one of the sub-trees branching out at x_f. The figure is also included in Article B.

Theorem 1.8. *Let $k = 2$ or $k = 3$. If $k = 2$ let $\alpha \in (0, 1)$, and if $k = 3$, let $\alpha \in (0, 3.145)$. Moreover, let $\beta \in (0, \infty)$. Let Φ be a random k-CNF formula with n variables and $m \sim \alpha n$ clauses, and let $\mathcal{L} \subseteq [n]$ be a non-random set such that $|\mathcal{L}|/n^{1-1/k} \to \beta$. Then*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \begin{cases} \exp\left(-\left(\frac{\beta}{2}\right)^2 \frac{\alpha}{1-\alpha}\left[1 - e^{-2\alpha}(I_0 + I_1)(2\alpha)\right]^2\right), & \text{if } k = 2, \\ \exp\left(-\left(\frac{\beta}{2}\right)^3 \alpha\left[1 - e^{-3\alpha}(I_0 + I_1)(3\alpha)\right]^3\right), & \text{if } k = 3, \end{cases}$$

where I_0 and I_1 are modified Bessel functions of the first kind.

The above theorem gives the exact limiting probability that a random CNF formula in which variables are fixed according to the majority rule policy, is satisfiable.

1.5.2 Comparison of strategies

As theorem 1.6 gives the exact limiting probability of a formula being satisfiable when variables are fixed independently of the CNF formula, while theorem 1.8 establishes this limit when the majority rule policy is used, this allows us to compare the two policies. Define

$$\mu_z := e^{-z}(I_0(z) + I_1(z)) = \frac{1}{\pi}\int_0^{\pi} e^{z(\cos(t)-1)}(\cos(t))\,dt, \tag{1.5.2}$$

where the second equality stems from the integral representations of the modified Bessel functions of the first kind. In Article D we also have the following corollary:

Corollary 1.9. *Let $k = 2$ or $k = 3$. If $k = 2$ let $\alpha \in (0, 1)$, and if $k = 3$, let $\alpha \in (0, 3.145)$. Moreover, let $\beta \in (0, \infty)$. Let Φ be a random k-CNF formula with n variables and $m \sim \alpha n$ clauses. Let $\mathcal{L}_0 \subseteq \pm[n]$ be a non-random consistent set with $|\mathcal{L}_0|/n^{1-1/k} \to \beta_0$ and let $\mathcal{L} \subseteq [n]$, with $|\mathcal{L}|/n^{1-1/k} \to \beta_{MR}$. Let finally $\mathcal{L}_{MR}$ be defined from $\mathcal{L}$ and Φ as defined in eq.* (1.5.1)*. Then*

$$\mathbb{P}(\Phi_{\mathcal{L}_0} \in \mathsf{SAT}) \sim \mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT})$$

if and only if

$$\beta_{\mathrm{MR}} = (1 - \mu_{k\alpha})^{-1}\beta_0.$$

By computing the values of μ_z numerically, we can quantify how many more variables can be fixed under the majority rule policy compared to fixing variables arbitrarily, while maintaining the same asymptotic probability that the random formula remains satisfiable. For random 2-SAT, we find that $(1 - \mu_2)^{-1} \approx 2.09$, indicating that the majority rule allows us to fix more than twice as many variables. In the case of random 3-SAT, we obtain $(1 - \mu_{3\cdot 3.145})^{-1} \approx 1.34$, meaning the majority rule permits fixing roughly one-third more variables than without any policy.

References

[Ach+01] Dimitris Achlioptas et al. “Rigorous results for random $(2+p)$-SAT”. In: *Theoret. Comput. Sci.* 265.1-2 (2001), pp. 109–129.

[AM15] Dimitris Achlioptas and Michael Molloy. “The solution space geometry of random linear equations”. In: *Random Structures Algorithms* 46.2 (2015), pp. 197–231.

[Ayr+20] Peter Ayre et al. “The satisfiability threshold for random linear equations”. In: *Combinatorica* 40.2 (2020), pp. 179–235.

[BCM02] Giulio Biroli, Simona Cocco, and Rémi Monasson. “Phase transitions and complexity in computer science: an overview of the statistical physics approach to the random satisfiability problem”. In: *Physica A: Statistical Mechanics and its Applications* 306 (2002), pp. 381–394.

[CKT91] Peter Cheeseman, Bob Kanefsky, and William M. Taylor. “Where the *really* hard problems are”. In: *Proceedings of the 12th International Joint Conference on Artificial Intelligence - Volume 1*. IJCAI’91. Sydney, New South Wales, Australia: Morgan Kaufmann Publishers Inc., 1991, pp. 331–337.

[Coj+24] Amin Coja-Oghlan et al. “The k-XORSAT threshold revisited”. In: *Electron. J. Combin.* 31.2 (2024), Paper No. 2.16, 33.

[Coo71] Stephen A. Cook. “The Complexity of Theorem-Proving Procedures”. In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC ’71. 1971, pp. 151–158.

[CR92] Vašek Chvátal and Bruce Reed. “Mick gets some (the odds are on his side)(satisfiability)”. In: *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*. SFCS ’92. 1992, pp. 620–627.

[Día+09] Josep L. Díaz et al. “On the satisfiability threshold of formulas with three literals per clause”. In: *Theoret. Comput. Sci.* 410.30-32 (2009), pp. 2920–2934.

[DM02a] Olivier Dubois and Jacques Mandler. “The 3-XORSAT threshold”. In: *C. R. Math. Acad. Sci. Paris* 335.11 (2002), pp. 963–966.

[DM02b] Olivier Dubois and Jacques Mandler. “The 3-XORSAT threshold”. In: *Comptes Rendus Mathematique* 335.11 (2002), pp. 963–966.

[DSS22] Jian Ding, Allan Sly, and Nike Sun. “Proof of the satisfiability conjecture for large k”. In: *Ann. of Math. (2)* 196.1 (2022), pp. 1–388.

[FP83] John Franco and Marvin Paull. “Probabilistic analysis of the Davis-Putnam procedure for solving the satisfiability problem”. In: *Discrete Appl. Math.* 5.1 (1983), pp. 77–87.

[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.

[GGW06] Aarti Gupta, Malay K. Ganai, and Chao Wang. "SAT-Based Verification Methods and Applications in Hardware Verification". In: *Formal Methods for Hardware Verification.* Ed. by Marco Bernardo and Alessandro Cimatti. Springer Berlin Heidelberg, 2006, pp. 108–143.

[Goe96] Andreas Goerdt. "A Threshold for Unsatisfiability". In: *J. Comput. Syst. Sci.* 53.3 (1996), pp. 469–486.

[Gol79] Allen T. Goldberg. "On the Complexity of the Satisfiability Problem". In: *Fourth Workshop on Automated Deduction.* CADE-4. Austin, Texas, USA: Association for Automated Reasoning Inc., 1979, pp. 1–6.

[HS03] Mohammad Taghi Hajiaghayi and Gregory B. Sorkin. *The Satisfiability Threshold of Random* 3*-SAT Is at Least* 3.52. 2003.

[Ibr+15a] Morteza Ibrahimi et al. "The set of solutions of random XORSAT formulae". In: *Ann. Appl. Probab.* 25.5 (2015), pp. 2743–2808.

[Ibr+15b] Morteza Ibrahimi et al. "The set of solutions of random XORSAT formulae". In: *The Annals of Applied Probability* 25.5 (Oct. 2015).

[IMM18] Alexey Ignatiev, Antonio Morgado, and Joao Marques-Silva. "PySAT: A Python Toolkit for Prototyping with SAT Oracles". In: *SAT.* 2018, pp. 428–437.

[KKL06] Alexis C. Kaporis, Lefteris M. Kirousis, and Efthimios G. Lalas. "The probabilistic analysis of a greedy satisfiability algorithm". In: *Random Structures Algorithms* 28.4 (2006), pp. 444–480.

[Knu15] Donald E Knuth. *The art of computer programming, Volume 4, Fascicle 6: Satisfiability.* Addison-Wesley Professional, 2015.

[KS94] Scott Kirkpatrick and Bart Selman. "Critical behavior in the satisfiability of random Boolean expressions". In: *Science* 264.5163 (1994), pp. 1297–1301.

[Mar08] João Marques-Silva. "Practical applications of Boolean Satisfiability". In: *2008 9th International Workshop on Discrete Event Systems.* 2008, pp. 74–80.

[Men09] Elliott Mendelson. *Introduction to mathematical logic.* Chapman and Hall/CRC, 2009.

[MM09] Marc Mezard and Andrea Montanari. *Information, physics, and computation.* Oxford University Press, 2009.

[MM20] Raffaele Marino and Salvatore Mandrà. *The-Backtracking-Survey-Propagation-Algorithm-code*. `https://github.com/RaffaeleMarino/The-Backtracking-Survey-Propagation-Algorithm-code`. 2020.

[Mon+99] Rémi Monasson et al. "Determining computational complexity from characteristic "phase transitions"". In: *Nature* 400.6740 (1999), pp. 133–137.

[MPR16] Raffaele Marino, Giorgio Parisi, and Federico Ricci-Tersenghi. "The backtracking survey propagation algorithm for solving random K-SAT problems". In: *Nat Commun* 7 (2016).

[PS16] Boris Pittel and Gregory B. Sorkin. "The satisfiability threshold for k-XORSAT". In: *Combin. Probab. Comput.* 25.2 (2016), pp. 236–268.

[SML96] Bart Selman, David G. Mitchell, and Hector J. Levesque. "Generating Hard Satisfiability Problems". In: *Artif. Intell.* 81 (1996), pp. 17–29.

Proof Sketches 2

2.1 General Proof Idea

The proofs of especially Article B and C are long and technical. This chapter aims to outline the overall proof strategy without delving into the detailed technicalities. All articles are based on the same decomposition of the probability under consideration. In this subsection, we introduce the main setup and define the core elements that are used consistently throughout the articles.

2.1.1 Notation

In the following proof sketches we adopt the following notation. For $n \in \mathbb{N}$, let $[n] := \{1, 2, \ldots, n\}$ and $[n]_0 := \{0, 1, \ldots, n\}$. For a set $A \subseteq \mathbb{Z}$, define $-A := \{-a : a \in A\}$, $\pm A := A \cup (-A)$, and $A_{\text{abs}} := \{|a| : a \in A\}$. We write $|A|$ for the cardinality of A. We also let $\mathbb{B} := \{\texttt{true}, \texttt{false}\}$ and $K_h := \{1, 2, \ldots, h, \star\}$. Finally, note that when a random CNF formula is said to have a non-integer number of clauses or variables, it is understood that these quantities are rounded down to the nearest integer.

2.1.2 The random SAT model

In the following, we consider k-CNF formulas with n variables and m clauses for some $k, n, m \in \mathbb{N}$. We start by noting that a literal can be seen as a mapping that for an $x \in \mathbb{B}^n$ either maps $x \mapsto x_v$ or $x \mapsto \neg x_v$, for some $v \in [n]$. Thus, the literal is either a projection mapping or the composition of a negation and a projection. This implies that an alternative way of representing literals is by an integer $\ell \in \pm[n]$, where if $\ell > 0$ we have $\ell(x) = x_\ell$ and if $\ell < 0$, then $\ell(x) = \neg x_{|\ell|}$. Thus, a k-CNF formula φ can be defined from a set of integers $\ell_{j,i} \in \pm[n]$, $j \in [m]$, $i \in [k]$, where the vector $(\ell_{j,1},\dots,\ell_{j,k})$, $j \in [m]$, belongs to the set

$$\mathcal{D}_k = \{(\ell_1,\dots,\ell_k) \in (\pm[n])^k : |\ell_1| < \cdots < |\ell_k|\}. \tag{2.1.1}$$

Then φ is the Boolean function

$$\varphi = \bigwedge_{j\in[m]} \left(\ell_{j,1} \vee \cdots \vee \ell_{j,k}\right).$$

We can now proceed by considering the random case. A random k-CNF formula Φ with n variables and m clauses is defined from a set of random literals $L_{j,i}$, $j \in [m]$, $i \in [k]$, where the random vectors $(L_{j,1},\dots,L_{j,k})$, $j \in [m]$ are independent and uniformly distributed over the set $\mathcal{D}_k$. We denote this model $F_k(n,m)$. The variables of the random function will be denoted $V_{j,i} = |L_{j,i}|$.

2.1.3 Fixing variables and the unit propagation algorithm

The articles included in this thesis are concerned with variable fixing in random CNF formulas. In this section, we formalize this procedure mathematically. For a (non-random) k-CNF formula φ with n variables and m clauses defined by the literals $\ell_{j,i}$, $j \in [m]$, $i \in [k]$, and a consistent set $\mathcal{L} \subseteq \pm[n]$, with $|\mathcal{L}| = f$, we define the formula with fixed variables $\varphi_{\mathcal{L}}$ in correspondence with eq. (1.2.1). Furthermore, we write

$$\varphi_{\mathcal{L}} = \bigwedge_{j=1}^{m} (\ell_{j,1} \vee \cdots \vee \ell_{j,k})_{\mathcal{L}},$$

where a clause with fixed variables $(\ell_{j,1} \vee \cdots \vee \ell_{j,k})_{\mathcal{L}}$, $j \in [m]$, belongs to one of $k+2$ sets depending on how the literals of the clause are affected by the fixing of variables. For $h \in [k]_0$ we have:

- If $(k-h)$ literals of a clause are fixed to being `false` and the remaining h literals are not fixed then the clause is said to be an h-clause

We let $\mathcal{C}_h$ be the set consisting of the j's for which the j'th clause is an h-clause. Moreover, a 0-clause is also referred to as an unsatisfied clause. Note that for $j \in \mathcal{C}_h$ we have that for all $x \in \mathbb{B}^n$ it is the case that

$$(\ell_{j,1} \vee \cdots \vee \ell_{j,h})_{\mathcal{L}}(x) = (\ell_{j,i_{j_1}} \vee \cdots \vee \ell_{j,i_{j_h}})(x), \tag{2.1.2}$$

where $\ell_{j,i_1},\dots,\ell_{j,i_h}$ are the literals that are not affected by the fixing of variables. Thus, if j belongs to $\mathcal{C}_h$, then the given clause with fixed variables corresponds to a clause of size h. Now, the last subset of clauses is defined as

- If at least one literal of a clause is fixed to being `true` then the clause is said to be satisfied.

We let $\mathcal{C}_\star$ consist of the j's for which the j'th clause is a satisfied clause, and we note that if $j \in \mathcal{C}_\star$ then for all $x \in \mathbb{B}^n$ it is the case that

$$(\ell_{j,1} \vee \cdots \vee \ell_{j,k})_{\mathcal{L}}(x) = \texttt{true}.$$

Using the above defined elements, we can let

$$M_h = |\mathcal{C}_h|, \quad h \in K_k, \tag{2.1.3}$$

and further for $h \in [k]$ we can let

$$\varphi_h := \bigwedge_{j \in \mathcal{C}_h} \left(\ell_{j,i_{j_1}} \vee \cdots \vee \ell_{j,i_{j_h}}\right). \tag{2.1.4}$$

Note that all of the above literals will belong to the set $\pm([n] \backslash \mathcal{L}_{\text{abs}})$. Thus, φ_h can be seen as a h-CNF formula with $n - f$ variables and M_h clauses. Moreover, the above considerations imply that

$$\varphi_{\mathcal{L}} \in \mathsf{SAT} \quad \Leftrightarrow \quad M_0 = 0 \quad \text{and} \quad \left(\bigwedge\nolimits_{h \in [k]} \varphi_h\right) \in \mathsf{SAT}. \tag{2.1.5}$$

We will now look further into when the last CNF formula in (2.1.5) is satisfiable. Note that $\wedge_{h \in [k]} \varphi_h$ is a mixed CNF formula, where also unit-clauses are present. Thus, letting $\mathcal{L}(\varphi_1) = \{\ell_{j,i_{j_1}}\}_{j \in \mathcal{C}_1}$, when $\varphi_1 \in \mathsf{SAT}$, and deleting duplicate variables when $\varphi_1 \notin \mathsf{SAT}$, we have a consistent set, and

$$\varphi_{\mathcal{L}} \in \mathsf{SAT} \quad \Leftrightarrow \quad M_0 = 0, \quad \varphi_1 \in \mathsf{SAT} \quad \text{and} \quad \left(\bigwedge\nolimits_{h \in [2,k]} \varphi_h\right)_{\mathcal{L}(\varphi_1)} \in \mathsf{SAT}. \tag{2.1.6}$$

The above decomposition is a key tool in all articles and projects included in this dissertation. Moreover, it is exploited that the just described procedure can now be applied to the last term of eq. (2.1.6), and hereby our fixing of variables becomes recursive. A lot of work in the articles B and C and project E goes into controlling this process.

In the following, we will only consider the random case, where we initially have a random k-CNF formula Φ. All of the above considerations then still apply, and the inferred notation will also be used in this random case.

2.1.4 Decomposition of the probability

Consider a random k-CNF formula Φ with n variables and m clauses, i.e. $\Phi \sim F_k(n, m)$. Let $\mathcal{L} \subseteq \pm[n]$ be a consistent set with $|\mathcal{L}| = f$. We will analyze the unit propagation procedure that starts when the variables dictated by $\mathcal{L}$ are fixed in Φ.

Initial round: Let $M_h^{(1)}$ for $h \in K_k$ be the random variables defined in eq. (2.1.3). Moreover, let $\Phi_h^{(1)}$, $h \in [k]$ be the random formulas corresponding to the definitions in eq. (2.1.4). Finally, let $\mathcal{L}^{(1)}$ be the set defined from $\Phi_1^{(1)}$, also as defined in section 2.1.3. The decomposition in eq. (2.1.6) implies that

$$\mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) = \mathbb{P}\Big(M_0^{(1)} = 0,\ \Phi_1^{(1)} \in \mathsf{SAT},\ (\Phi_2^{(1)} \wedge \cdots \wedge \Phi_k^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big). \quad (2.1.7)$$

As the clauses of Φ are independent, the events on the right of eq. (2.1.7) are only dependent through the random vector $(M_h^{(1)})_{h\in K_k}$. In the different cases that are considered in the different articles, we find that the entries of this random vector concentrate around their means which implies that the events at the right of eq. (2.1.7) are asymptotically independent. Thus

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \approx \mathbb{P}\Big(M_0^{(1)} = 0\Big)\mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)} \wedge \cdots \wedge \Phi_k^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big), \quad (2.1.8)$$

where the equality holds up to some error term.

Subsequent rounds: The procedure of the initial round can now be repeated in a recursive way. We replace Φ with $(\Phi_2^{(1)} \wedge \cdots \wedge \Phi_k^{(1)})$, and $\mathcal{L}$ with $\mathcal{L}^{(1)}$, hereby producing new random elements $(M_h^{(2)})_{h\in K_k}$, $\Phi_h^{(2)}$, $h \in [k]$, and $\mathcal{L}^{(2)}$. We then continue recursively, and in this way elements $(M_h^{(r)})_{h\in K_k}$, $\Phi_h^{(r)}$, $h \in [k]$, and $\mathcal{L}^{(r)}$ are produced for each $r \in [R]$, where R is an integer that will be specified later on. The decomposition in eq. (2.1.8) is now repeated by which we get

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \approx \mathbb{P}\Big((\Phi_2^{(R)} \wedge \cdots \wedge \Phi_k^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big)\prod_{r=1}^{R}\mathbb{P}\Big(M_0^{(r)} = 0\Big)\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big), \quad (2.1.9)$$

again up to some error term. The primary challenge in Article B and C lies in controlling the size of the error terms produced during this unit propagation procedure, and in ensuring that their total contribution vanishes as $n \to \infty$. These technical details, however, will be omitted in the forthcoming proof sketches.

To evaluate the terms in the decomposition in eq. (2.1.9), we first need a few technical lemmas. The first lemma characterizes the distribution of the random vector $(M_h)_{h\in K_k}$.

Lemma 2.10. *Let Φ be a random k-CNF formula with n variables and m clauses, and let $\mathcal{L}$ be a consistent set with $|\mathcal{L}| = f$. Let $(M_h)_{h\in K_k}$ be the random vector defined in eq.* (2.1.3). *Then*

$$(M_h)_{h\in K_k} \sim \mathit{Binomial}(m, p),$$

where $p = (p_h)_{h\in K_k}$, $\sum_{h\in K_k} p_h = 1$, *and for* $h \in [k]_0$

$$p_h = \binom{k}{h} \prod_{i=0}^{h-1} \frac{n-f-i}{n-i} \prod_{i=0}^{k-h-1} \frac{f-i}{2(n-h-i)}.$$

Proof. The above lemma follows directly from the i.i.d. structure of the clauses, together with an evaluation of the terms $\mathbb{P}(j \in \mathcal{C}_h)$ for $h \in K_k$. □

The next lemma establishes the conditional distribution of the random functions Φ_h, $h \in [k]$, see (eq. (2.1.4)), given the vector $(M_h)_{h\in K_k}$.

Lemma 2.11. *Let* Φ *be a random* k*-CNF formula with* n *variables and* m *clauses, and let* $\mathcal{L}$ *be a consistent set with* $|\mathcal{L}| = f$*. Define the random elements* $(M_h)_{h\in K_k}$*, and* Φ_h*,* $h \in [k]$ *in correspondence with eqs.* (2.1.3) *and* (2.1.4)*. Then for* $h \in [k]$

$$\Phi_h | (M_h)_{h\in K_k} \sim F_h(n-f, M_h),$$

(up to a renaming of the variables), and the random functions are conditionally independent given $(M_h)_{h\in K_k}$*.*

Proof. This lemma again follows from the i.i.d. structure of the clauses, and by computing the conditional probabilities $\mathbb{P}(L_{j,i_1} = \ell_1, \ldots, L_{j,i_h} = \ell_h \mid j \in \mathcal{C}_h)$ for $j \in [m]$, $h \in [k]$, and $\ell_1, \ldots, \ell_h \in \pm[n]$. □

By recursively using Lemma 2.10 and 2.11, we get that the random vectors $(M_h^{(r)})_{h\in K_k}$, for $r \in [R]$, are multinomially distributed with both the number parameter and the probability parameter being random variables. In the following proof sketches, we will approximate these random variables with their mean and ignore their randomness. This will yield the right result, as the fluctuations of the random variables are negligible as $n \to \infty$. Likewise, Lemma 2.11 shows that the function $\Phi_h^{(r)}$ is a random h-CNF formula, for $h \in [k]$ and $r \in [R]$, with a random number of variables and a random number of clauses, but this randomness will also be disregarded in the proof sketches.

Now lastly, when all the distributions of the random elements are known, we will need a last technical lemma that finally allows us to evaluate the terms of eq. (2.1.9).

Lemma 2.12. *Let* $X \sim$ *Binomial*(m,p)*, and* $\Phi \sim F_1(n,f)$*, with* $m \sim \alpha n$*,* $f \sim \beta(n)\sqrt{n}$*, and* $p \sim \gamma(n)n^{-1}$ *for* $\beta = O(1)$*,* $\gamma = O(1)$*. Then*

$$\mathbb{P}(X = 0) \sim \exp(-\alpha\gamma(n)), \qquad \text{and} \qquad \mathbb{P}(\Phi \in \mathsf{SAT}) \sim \exp(-\beta(n)^2/4).$$

Proof. This lemma can be proven by combinatorial arguments, and standard approximation arguments. □

The main remaining part of the proofs in Articles B and C is to control the sizes of the entries of the random vectors $(M_h^{(r)})_{h\in K_k}$ during the rounds in which a significant number of unit clauses is still present, and when these sizes are estimated the probabilities of the decomposition (2.1.9) can be calculated.

2.2 Proof Sketch for Article B

In Article B both random 2- and 3-CNF formulas are considered. Firstly, in the case $k=2$, we consider $\Phi \sim F_2(n,m)$, with $m \sim \alpha n$, for some $\alpha \in (0,1)$, and for a consistent set $\mathcal{L} \subseteq \pm[n]$ with $|\mathcal{L}| \sim \beta\sqrt{n}$, for some $\beta > 0$, we will establish that

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \exp\Big(-\frac{\alpha\beta^2}{4(1-\alpha)}\Big). \tag{2.2.1}$$

This will imply that a subcritical random 2-CNF formula has degrees of freedom on the order of $\sqrt{n}$. Next, we consider the case $k=3$ where $\Phi \sim F_3(n,m)$, with $m \sim \alpha n$, for some $\alpha \in (0,3.145)$, and we let $\mathcal{L} \subseteq \pm[n]$ be consistent, with $|\mathcal{L}| \sim \beta n^{2/3}$ for some $\beta > 0$. We will establish that in this setup

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \exp\Big(-\frac{\alpha\beta^3}{8}\Big). \tag{2.2.2}$$

This implies that the random 3-CNF formula has degrees of freedom on the order of $n^{2/3}$.

2.2.1 Random 2-SAT

We first consider the case $k=2$. Let the number of rounds $R = \Theta(\log n)$. Firstly, we will need to bound the size of the random vector $(M_h^{(r)})_{h\in K_2}$ for each $r \in [R]$. We have the following lemma:

Lemma 2.13. *Let for every $r \in [R]$*

$$f_\pm^{(r)} = \alpha^r f \pm r\alpha^r n^{3/8}, \quad m^{(r)} = m - 3(f + n^{3/8})\sum_{s=1}^{r} \alpha^s.$$

With notation continued from above, we have that $f_-^{(r)} \le M_1^{(r)} \le f_+^{(r)}$, and $m^{(r)} \le M_2^{(r)} \le m$ for all $r \in [R]$ w.h.p. In particular, we have that $M_1^{(r)} \sim \alpha^r\beta\sqrt{n}$, and $M_2^{(r)} \sim \alpha n$ for all $r \in [R]$ w.h.p.

Proof. The proof is highly technical and contains long and tedious calculations, as the terms of the decomposition in eq. (2.1.9) need to be carefully monitored in order for the total error to approach zero. The details are skipped in this proof sketch. We proceed by induction on r. Assume that $M_1^{(r-1)} \sim \alpha^{r-1}\beta\sqrt{n}$, $M_2^{(r-1)} \sim \alpha n$, and $\Phi_2^{(r-1)} \sim F_2(n, \alpha n)$. By Lemma 2.11, $M_1^{(r)}$ follows a binomial distribution with number parameter $M_2^{(r-1)} \sim \alpha n$, and probability parameter that is on the order of $M_1^{(r-1)}/n \sim \alpha^{r-1}\beta n^{-1/2}$, see Lemma 2.10. Hence, $\mathbb{E}[M_1^{(r)}] \sim \alpha^r f$, and via a Chernoff bound we can bound $M_1^{(r)}$ by $\mathbb{E}[M_1^{(r)}] \pm f_\pm^{(r)}$ w.h.p. For the binary clauses, note that $\sum_{h\in\{0,1,\star\}} M_h^{(r-1)}$ is also binomially distributed, with parameters given by Lemma 2.10. Another Chernoff bound then gives that $\sum_{h\in\{0,1,\star\}} M_h^{(r-1)} \leq 3(f + n^{3/8})\sum_{s=1}^{r} \alpha^s$ w.h.p. and this implies the bound on $M_2^{(r)}$. Finally, Lemma 2.11 yields $\Phi_2^{(r)} \sim F_2(n, \alpha n)$. □

Combining Lemma 2.10, 2.11, and 2.13, we get that for each $r \in [R]$

$$M_0^{(r)} \sim \text{Binomial}\Big(\alpha n, (\alpha^{r-1}\beta)^2/4n\Big), \quad \text{and} \quad \Phi_1^{(r)} \sim F_1(n, \alpha^r\beta\sqrt{n}).$$

Thus, using Lemma 2.12, we get that

$$\mathbb{P}(M_0^{(r)} = 0) \sim \exp\Big(-\frac{\alpha^{2r-1}\beta^2}{4}\Big), \quad \text{and} \quad \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) \sim \exp\Big(-\frac{\alpha^{2r}\beta^2}{4}\Big).$$

Inserting the above in eq. (2.1.9) we get

$$\mathbb{P}(\Phi \in \mathsf{SAT}) \sim \mathbb{P}\Big((\Phi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big)\exp\Big(-\frac{\alpha\beta^2}{4(1-\alpha)}\Big).$$

Thus, we will only need to consider the remaining 2-CNF formula. By Lemma 2.13, we have $\Phi_2^{(R)} \sim F_2(n, \alpha n)$ and using the definition of R, we further get that $M_1^{(R)} = o(\sqrt{n})$. Using an argument analogous to the snakes-and-snares method employed in the proof of the random 2-SAT satisfiability threshold, see [Knu15] p. 52, one can show that $(\Phi_2^{(R)})_{\mathcal{L}^{(R)}}$ is satisfiable w.h.p. This completes the proof of eq. (2.2.1).

2.2.2 Random 3-SAT

Next we consider the case $k = 3$. Note that in a 3-clause, two literals must be fixed for the clause to become a unit-clause that triggers further variable fixings. Consequently, the unit propagation procedure terminates more quickly in this model.

In this setting, we let the number of rounds $R = 3$. By Lemma 2.10, $M_0^{(1)} \sim \text{Binomial}(\alpha n, \beta^3/(8n))$, and $M_1^{(1)} = O(n^{1/3})$ w.h.p. Thus, $\Phi_1^{(1)}$ is a random 1-CNF formula with $O(n^{1/3})$ clauses, see Lemma 2.11. Lemma 2.12 gives that

$$\mathbb{P}(M_0^{(1)} = 0) \sim \exp\Big(-\frac{\alpha\beta^3}{8}\Big), \quad \text{and} \quad \mathbb{P}(\Phi_1^{(1)} \in \mathsf{SAT}) \sim 1.$$

Also $|\mathcal{L}^{(1)}| = O(n^{1/3})$, and $\Phi_2^{(1)}$ and $\Phi_3^{(1)}$ are random CNF formulas with $O(n^{2/3})$ and $\Theta(\alpha n)$ clauses, respectively, see Lemma 2.11. The process of fixing variables can be continued in this setup, where we find the number of different clauses produced in each round by considering the 2- and 3-CNF formula separately. During this process, we find, using Lemma 2.10 to 2.12, that no empty clauses are generated w.h.p., and all the produced 1-CNF formulas are satisfiable w.h.p. In the third round it is further found that $\mathcal{L}^{(R)} = \emptyset$ w.h.p. Thus, we are left with considering the formula $\Phi_2^{(3)} \wedge \Phi_3^{(3)}$, which is asymptotically satisfiable by Theorem 2 in [Ach00]. Thus, eq. (2.2.2) is established.

2.3 Proof Sketch for Article C

Let Φ be a critical 2-CNF formula, i.e. $\Phi \sim F_2(n,n)$. Let further $\mathcal{L} \subseteq \pm[n]$ be a consistent set with $|\mathcal{L}| = f$. We consider the formula with fixed variables $\Phi_{\mathcal{L}}$. Firstly, we will establish that

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0, \tag{2.3.1}$$

when $f = n^q$ with $q = 1/3 + \varepsilon$ for some $\varepsilon > 0$. This will imply the result for a general $f = \Omega(n^{1/3+\varepsilon})$ as the probability in consideration is monotone in f. Next, we will establish that when $f = n^q$ with $q = 1/3 - \varepsilon$, for some $\varepsilon > 0$, then

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq \liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}). \tag{2.3.2}$$

As $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})$ is decreasing in f this will imply an equality in eq. (2.3.2), which is our claim. The monotonicity of f further implies the result for general $f = O(n^{1/3-\varepsilon})$.

2.3.1 Fixing variables makes formula unsatisfiable

First, let $f = n^q$, with $q = 1/3 + \varepsilon$ for some $\varepsilon > 0$. Let $R = n^{1-2q} \log n$. We will upper bound the terms of the decomposition in (2.1.9). To do so, we will establish that the sequence $(M_1^{(r)})_{r\in[R]}$ remains on the order of n^q.

Lemma 2.14. *With the notation from above, there exist constants $c, C > 0$ such that*

$$\lim_{n\to\infty} \mathbb{P}\Big(M_1^{(r)} \in [cn^q, Cn^q]\ \forall r \in [R]\Big) = 1.$$

Proof. Careful calculations using Lemma 2.10 and Lemma 2.11 give that $\mathbb{E}[M_1^{(r)}] = \Theta(n^q)$ and $\mathbb{V}(M_1^{(r)}) = O(n^{1-q})$ for all $r \in [R]$. This along with Chebyshev's inequality imply that for any $q_1 \in (\frac{1-q}{2}, q)$ we have that

$$\mathbb{P}\Big(|M_1^{(R)} - \mathbb{E}[M_1^{(R)}]| > n^{q_1}\Big) \leq \frac{\mathbb{V}(M_1^{(R)})}{n^{2q_1}} = n^{1-q-2q_1} \to 0, \quad \text{as } n \to \infty.$$

Thus, $M_1^{(R)} = \Theta(n^q)$ w.h.p., and there exist constants $C, c > 0$ and $\delta > 0$ small, such that

$$\lim_{n\to\infty} \mathbb{P}(M_1^{(R)} \in [(c+\delta)n^q, (C-\delta)n^q]) = 1. \tag{2.3.3}$$

To establish a bound uniformly for all $r \in [R]$ we argue by contradiction. Assuming that $\lim_{n\to\infty} \mathbb{P}(\exists r \in [R] : M_1^{(r)} \notin [cn^q, Cn^q]) > 0$, and then conditioning on this event, it can be found that the asymptotic conditional probability that $M_1^{(R)}$ belongs to $[(c+\delta)n^q, (C-\delta)n^q]$ is strictly less than one. This contradicts eq. (2.3.3) and thus establishes the lemma. □

Now, by a recursive argument using Lemma 2.10, 2.11, and 2.14, we get that $M_0^{(r)}$ is binomially distributed, with number parameter asymptotically equivalent to n, and probability parameter greater than $c^2 n^{2(q-1)}/4$ uniformly for all $r \in [R]$. Then, using Lemma 2.12 and the definition of R we get

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \prod_{r=1}^{R} \mathbb{P}(M_0^{(r)} = 0) \leq \exp\Big(-R\tfrac{(cn^q)^2}{4n}\Big) = \exp\Big(-\tfrac{1}{4}c^2 \log n\Big),$$

and the last term above approaches zero as $n \to \infty$. Thus, we have established eq. (2.3.1).

2.3.2 Fixing of variables does not affect satisfiability

Next, we will establish eq. (2.3.2), where we remember that $f = n^q$ with $q = 1/3 - \varepsilon$. Let $R = n^{1-2q}\log^{-3} n$. We again need to control the size of the sequence $(M_1^{(r)})_{r\in[R]}$.

Lemma 2.15. *With the already inferred notation we have that*

$$(a)\ \lim_{n\to\infty} \mathbb{P}(M_1^{(r)} \leq n^q \log n\ \forall r \in [R]) = 1, \qquad (b)\ \lim_{n\to\infty} \mathbb{P}(M_1^{(R)} = 0) = 1.$$

Proof. (a): Using Lemma 2.10 it can be found that for each $r \in [R]$ we have that $\mathbb{E}[M_1^{(r)} | M_1^{(r-1)}, \dots, M_1^{(1)}] \leq M_1^{(r-1)}$. Thus, the sequence $(M_1^{(r)})_{r\in[R]}$ is a supermartingale. Consider the stopping time

$$\tau = \min\{r \in [R] : M_1^{(r)} = 0 \text{ or } M_1^{(r)} \geq n^q \log n\}.$$

The optional stopping theorem (see e.g. Thm. 28, Chapter V in [DM11]) gives that

$$n^q = \mathbb{E}[M_1^{(0)}] \geq \mathbb{E}[M_1^{(\tau)}] \geq 0 \cdot \mathbb{P}(M_1^{(\tau)} = 0) + n^q \log n \cdot \mathbb{P}(M_1^{(\tau)} \geq n^q \log n).$$

Rearranging the above terms, we see that $M_1^{(\tau)} = 0$ w.h.p. which in turn implies that the sequence $(M_1^{(r)})_{r\in[R]}$ will be in the absorbing state zero before exceeding $n^q \log n$ w.h.p.

(b): The sequence $(M_1^{(r)})_{r\in[R]}$ can be approximated by a critical Galton-Watson tree with Poisson offspring. Using standard results for such processes (see e.g. Chapter II in [ANN04]) along with our definition of R, gives that $\mathbb{P}(M_1^{(R)} = 0) \sim \exp(-n^{3q-1}\log^{-3} n)$. Thus, the probability approaches one as desired. □

Lemma 2.15 (a) along with Lemma 2.10 and 2.11, can be used to establish that $\Phi_2^{(R)} \sim F_2(n,n)$ and (b) of Lemma 2.15 implies that $\mathcal{L}^{(R)} = \emptyset$ w.h.p. Moreover, by Lemma 2.15 it holds that $\Phi_1^{(r)}$ has on the order of n variables and less than $n^q \log n$ clauses for all $r \in [R]$, and also using Lemma 2.10 we get that $M_0^{(r)}$ is multinomially distributed with number parameter n and probability parameter upper bounded by $n^{2(q-1)}\log^2 n/4$ for all $r \in [R]$. Thus, Lemma 2.12 implies

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) &\geq \mathbb{P}(\Phi \in \mathsf{SAT}) \prod_{r=1}^{R} \exp\Big(-\tfrac{(n^q \log n)^2}{4n}\Big)\exp\Big(-\tfrac{(n^q \log n)^2}{4n}\Big)\\ &= \mathbb{P}(\Phi \in \mathsf{SAT})\exp\Big(-\tfrac{2}{\log n}\Big).\end{aligned}$$

Taking the limit, we obtain eq. (2.3.2). It is worth noting that the exact computations involve conditional expectations, and as a result, Fatou's Lemma is applied, leading to the conclusion only being true with limit inferior.

2.4 Proof Sketch for Article D

Since this setup differs slightly from the previous proofs, we begin by specifying the new framework. We then estimate the sizes of the relevant random quantities, and finally use these estimates to evaluate the probabilities of interest.

2.4.1 General setup

For the proof of Article D we consider a different random SAT model, the need for which will become clear later. Let Φ be a random k-CNF formula on n variables with m clauses specified by literals $L_{j,i}$, where $j \in [m]$ and $i \in [k]$. We assume that the literals are i.i.d. and uniformly distributed on $\pm[n]$, and we denote this model by $G_k(n,m)$.

For each $v \in [n]$, define the random variables

$$A_v^+ = \Big|\{(j,i) \in [m]\times[k] : L_{j,i} = v\}\Big|, \quad A_v^- = \Big|\{(j,i) \in [m]\times[k] : L_{j,i} = -v\}\Big|. \tag{2.4.1}$$

Let $\mathcal{L} \subseteq [n]$ denote the set of variables that we want to fix. For each $v \in \mathcal{L}$ we assign a value to x_v so as to maximize the number of satisfied clauses. Concretely, we let $x_v = \texttt{true}$ if $\operatorname{sgn}(A_v^+ - A_v^-) \geq 0$ and let $x_v = \texttt{false}$ otherwise.

That is, we fix the variables in the set

$$\mathcal{L}_{\mathrm{MR}} = \{s \cdot v : v \in \mathcal{L},\ s = \operatorname{sgn}(A_v^+ - A_v^-)\}, \tag{2.4.2}$$

where $\operatorname{sgn}(0) := 1$. We will establish that

$$\lim_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}\Big) = \begin{cases} \exp\Big(-\big(\frac{\beta}{2}\big)^2 \frac{\alpha}{1-\alpha}\Big[1 - e^{-2\alpha}(I_0 + I_1)(2\alpha)\Big]^2\Big), & \text{if } k = 2, \\ \exp\Big(-\big(\frac{\beta}{2}\big)^3 \alpha\Big[1 - e^{-3\alpha}(I_0 + I_1)(3\alpha)\Big]^3\Big), & \text{if } k = 3, \end{cases} \tag{2.4.3}$$

where I_0 and I_1 denote modified Bessel functions of the first kind.

In what follows, we define M_h for $h \in K_k$ and Φ_h for $h \in [k]$, in accordance with (2.1.3) and (2.1.4), respectively. We also define the random set $\mathcal{L}^{(1)}$ from $\Phi^{(1)}$, as described in Section 2.1.3. For each $h \in [k]$, the random function Φ_h is a random h-CNF formula (see Lemma 2.11). However, the vector $(M_h)_{h\in K_k}$ is not multinomially distributed, since whether a literal of a clause is fixed to `true` or `false` depends on the literals of the other clauses.

2.4.2 Bounding the random variables

For each $v \in [n]$, define $A_v = A_v^+ + A_v^-$ and $\hat{A}_v = \min\{A_v^+, A_v^-\}$. Note that $A_v \sim \operatorname{Binomial}(m\cdot k, 1/n)$, and $\hat{A}_v \mid A_v \sim \min\{X, A_v - X\}$, where $X \sim \operatorname{Binomial}(A_v, 1/2)$. Using this and standard calculations then give

$$\mathbb{E}[\hat{A}_v] \sim \tfrac{1}{2} k\alpha\Big(1 - \mu_{k\alpha}\Big),$$

where

$$\mu_z := e^{-z}(I_0(z) + I_1(z)) = \frac{1}{\pi}\int_0^\pi e^{z(\cos t - 1)}\Big(\cos t + 1\Big)\,dt.$$

Moreover $\mathbb{E}[\hat{A}_v^2] = O(1)$, and for $v_1 \neq v_2$ we have $\operatorname{Cov}(\hat{A}_{v_1}, \hat{A}_{v_2}) < 0$. Now define $\hat{A}_{\mathcal{L}} = \sum_{v\in\mathcal{L}} \hat{A}_v$. From the above observations we obtain

$$\mathbb{E}[\hat{A}_{\mathcal{L}}] \sim k\alpha\beta n^{1-1/k}, \qquad \operatorname{Var}(\hat{A}_{\mathcal{L}}) = O\Big(n^{1-1/k}\Big). \tag{2.4.4}$$

Thus, by Chebyshev's inequality, it follows that $\hat{A}_{\mathcal{L}} \sim \mathbb{E}[\hat{A}_{\mathcal{L}}]$ w.h.p. Similarly, we let $A_{\mathcal{L}} = \sum_{v\in\mathcal{L}} A_v$, and then similar (but simpler) calculations give that $A_{\mathcal{L}} \sim \mathbb{E}[A_{\mathcal{L}}] \sim k\alpha\beta n^{1-1/k}$.

2.4.3 Calculating limiting probability

We first consider the case $k = 2$, where the number of clauses $m \sim \alpha n$ with $\alpha \in (0, 1)$. The decomposition in eq. (2.1.9) can also be applied here, by which we get

$$\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \mathbb{P}(M_0 = 0)\,\mathbb{P}(\Phi_1 \in \mathsf{SAT})\,\mathbb{P}((\Phi_2)_{\mathcal{L}^{(1)}} \in \mathsf{SAT}),$$

up to an unspecified error term. Using the fact that the literals of Φ are i.i.d., the probability $\mathbb{P}(M_0 = 0)$ can be computed by conditioning on $\hat{A}_{\mathcal{L}}$ and calculating the probability that these literals fixed to `false` end up in distinct clauses. Hereby we find

$$\mathbb{P}(M_0 = 0 \mid \hat{A}_{\mathcal{L}}) = \prod_{h=0}^{\hat{A}_{\mathcal{L}}-1}\left(1 - \frac{h}{2m-h}\right) \sim \exp\left(-\frac{(\hat{A}_{\mathcal{L}})^2}{4m}\right) \sim \exp\left(-\tfrac{1}{4}\alpha\beta^2(1-\mu_{2\alpha})^2\right). \tag{2.4.5}$$

where we lastly used that $\hat{A}_{\mathcal{L}} \sim \mathbb{E}[\hat{A}_{\mathcal{L}}]$ w.h.p., where this last term is known from eq. (2.4.4).

Combining (2.4.4) with Markov's inequality it can be established that $M_1 \sim \mathbb{E}[\hat{A}_{\mathcal{L}}]$, and as Φ_1 is a random 1-CNF formula Lemma 2.12 gives that

$$\lim_{n\to\infty} \mathbb{P}(\Phi_1 \in \mathsf{SAT}) = \exp\left(-\tfrac{1}{4}\alpha^2\beta^2(1-\mu_{2\alpha})^2\right). \tag{2.4.6}$$

Moreover, Markov's inequality implies that $M_2 \sim \alpha n$, and thus $\Phi_2 \sim G_2(n, \alpha n)$. Moreover, $|\mathcal{L}^{(1)}| \sim M_1 \sim \mathbb{E}[\hat{A}_{\mathcal{L}}]$, where this last term is calculated in (2.4.4). Thus, the main theorem of Article B, see eq. (2.2.1) implies that

$$\lim_{n\to\infty} \mathbb{P}((\Phi_2)_{\mathcal{L}^{(1)}} \in \mathsf{SAT}) = \exp\left(-\tfrac{1}{4}\alpha^3\beta^2(1-\mu_{2\alpha})^2(1-\alpha)^{-1}\right). \tag{2.4.7}$$

Combining eqs. (2.4.5) to (2.4.7) implies eq. (2.4.3) in the case $k = 2$.

The same calculations can be made in the case $k = 3$, where we let $m \sim \alpha n$ with $\alpha \in (0, 3.145)$. We have the decomposition from eq. (2.1.9)

$$\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \mathbb{P}(M_0 = 0)\,\mathbb{P}(\Phi_1 \in \mathsf{SAT})\,\mathbb{P}((\Phi_2 \wedge \Phi_3)_{\mathcal{L}^{(1)}} \in \mathsf{SAT}).$$

Markov's inequality implies that $M_1 = O(n^{1/3}\log n)$, $M_2 = O(n^{2/3}\log n)$, and $M_3 \sim \alpha n$. Thus, the last two terms of the decomposition are asymptotically equivalent to one. The term $\mathbb{P}(M_0 = 0)$ becomes slightly more tedious when $k = 3$, as multiple of the $\hat{A}_{\mathcal{L}}$ literals fixed to being `false` can end up in the same clause without creating an unsatisfied clause. Let $M_\dagger$ denote the number of clauses for which all literals are fixed to either `true` or `false`. The i.i.d. structure of the literals of Φ implies that

$$\mathbb{P}(M_0 = 0 \mid M_\dagger, A_{\mathcal{L}}, \hat{A}_{\mathcal{L}}) = \prod_{i=1}^{M_\dagger}\left(1 - \prod_{h=1}^{3}\frac{\hat{A}_{\mathcal{L}} - (3i-h)}{A_{\mathcal{L}} - (3i-h)}\right).$$

Now, $M_\dagger$ has a binomial distribution, why we can average over this random variable. Furthermore, in section 2.4.2 we found that both $A_{\mathcal{L}} \sim \mathbb{E}[A_{\mathcal{L}}]$ and $\hat{A}_{\mathcal{L}} \sim \mathbb{E}[\hat{A}_{\mathcal{L}}]$ w.h.p., why these random variables can be estimated by their means, see section 2.4.2. Hereby, we get

$$\lim_{n\to\infty} \mathbb{P}(M_0 = 0) = \exp\Big(-\tfrac{1}{4}\alpha\beta^2(1-\mu_{2\alpha})^2\Big),$$

and thus, we obtain eq. (2.4.3) in the case $k = 3$.

2.5 Proof Sketch for Project E

In this project, we study the random 3-XORSAT model with n variables and $m \sim \alpha n$ clauses, where $\alpha > 0$. A random formula Φ^{XOR} is defined by a collection of clauses $C_1, \ldots, C_m$. Each clause C_j is specified by three i.i.d. uniformly chosen random variables $V_{j,1}, V_{j,2}, V_{j,3} \in [n]$ and an independent uniform random variable $S_j \in \mathbb{B}$. The clause C_j then corresponds to the random constraint

$$x_{V_{j,1}} \oplus x_{V_{j,2}} \oplus x_{V_{j,3}} = S_j, \quad (x \in \mathbb{B}^n),$$

and we let $\Phi^{\mathrm{XOR}} = C_1 \wedge \cdots \wedge C_m$. Let $\mathcal{L} \subseteq \pm[n]$ be a consistent set with $|\mathcal{L}| \sim \beta n^{2/3}$ for some $\beta > 0$. Extending the idea of fixing input variables to this setting, we define the restricted formula $\Phi^{\mathrm{XOR}}_{\mathcal{L}}$ in analogy with eq. (1.2.1). Our goal is to prove the following result:

$$\begin{aligned} e^{-\beta^3\alpha/2} &\geq \limsup_{n\to\infty} \mathbb{P}(\Phi^{\mathrm{XOR}}_{\mathcal{L}} \in \mathsf{SAT}) \\ &\geq \liminf_{n\to\infty} \mathbb{P}(\Phi^{\mathrm{XOR}}_{\mathcal{L}} \in \mathsf{SAT}) \geq e^{-\beta^3\alpha/2} \liminf_{n\to\infty} \mathbb{P}(\Phi_2 \wedge \Phi_3 \in \mathsf{SAT}), \end{aligned} \tag{2.5.1}$$

where Φ_2 denotes a random 2-XORSAT formula with n variables and $O(n^{2/3})$ 2-XOR-clauses, and Φ_3 denotes a random 3-XORSAT formula with n variables and m 3-XOR-clauses.

Thus, to identify the threshold function for Φ^{XOR}, it is necessary to study a mixed formula containing both 2- and 3-XOR clauses, where the amount of 2-XOR-clauses is small. Our calculations support the conjecture that such a mixed formula remains satisfiable with asymptotic probability bounded away from zero, up to the satisfiability threshold of pure 3-XORSAT.

Fixing a variable in a XOR-clause C_j behaves as follows: assigning the variable to `false` corresponds to deleting it, while assigning it to `true` corresponds to deleting it and simultaneously flipping the sign S_j. In either case, the result is a standard random 2-XOR-clause. Thus, variable fixing affects XOR-clauses differently than disjunctive clauses, but analogues of Lemmas 2.10 and 2.11 remain valid. Moreover, we again obtain the decomposition of eq. (2.1.9), and from this point onward the proof of eq. (2.5.1) proceeds in close analogy with the argument for random 3-SAT in Article B.

Finally, the preliminary calculations suggesting that the mixed 2- and 3-XORSAT formula becomes over-constrained only when the number of 3-XOR-clauses exceeds the critical threshold of the pure 3-XORSAT model are largely inspired by the proof of the 3-XORSAT threshold in [DM02]. We provide some of the calculations, but essential parts of the argument remain unproven and are therefore only conjectural.

References

[Ach00] Dimitris Achlioptas. "Setting 2 variables at a time yields a new lower bound for random 3-SAT (extended abstract)". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. 2000, pp. 28–37.

[ANN04] Krishna B Athreya, Peter E Ney, and PE Ney. *Branching processes*. Courier Corporation, 2004.

[DM02] Olivier Dubois and Jacques Mandler. "The 3-XORSAT threshold". In: *Comptes Rendus Mathematique* 335.11 (2002), pp. 963–966.

[DM11] Claude Dellacherie and P-A Meyer. *Probabilities and potential, c: potential theory for discrete and continuous semigroups*. Elsevier, 2011.

[Knu15] Donald E Knuth. *The art of computer programming, Volume 4, Fascicle 6: Satisfiability*. Addison-Wesley Professional, 2015.

Article A

Some Results on Random Mixed SAT Problems

Andreas Basse-O'Connor[1], Tobias Overgaard[1], and Mette Skjøtt[1,2]

[1]Department of Mathematics, Aarhus University,
[2]Kvantify Aps

November 2023

Abstract: In this short paper we present a survey of some results concerning the random SAT problems. To elaborate, the Boolean Satisfiability (SAT) Problem refers to the problem of determining whether a given set of m Boolean constraints over n variables can be simultaneously satisfied, i.e. all evaluate to 1 under some interpretation of the variables in $\{\pm 1\}$. If we choose the m constraints i.i.d. uniformly at random among the set of disjunctive clauses of length k, then the problem is known as the random k-SAT problem. It is conjectured that this problem undergoes a structural phase transition; taking $m = \alpha n$ for $\alpha > 0$, it is believed that the probability of there existing a satisfying assignment tends in the large n limit to 1 if $\alpha < \alpha_{\text{sat}}(k)$, and to 0 if $\alpha > \alpha_{\text{sat}}(k)$, for some critical value $\alpha_{\text{sat}}(k)$ depending on k. We review some of the progress made towards proving this and consider similar conjectures and results for the more general case where the clauses are chosen with varying lengths, i.e. for the so-called random mixed SAT problems.

A.1 Introduction

The present paper presents a survey of conjectures and results on the phase transitions for the random SAT problems with a focus on mixed formulas. The Boolean Satisfiability Problem (abbreviated: the SAT problem) lies at the heart of the famous P vs. NP Millennium Prize Problem. Indeed, the existence of a polynomial time algorithm for deciding satisfiability is equivalent to $P = NP$ (see [Coo71]). In addition to the theoretical importance of the problem, the SAT problem also holds tremendous practical relevance as it arises in many applied contexts, such as in artificial intelligence, electronic design automation, bioinformatics, and more; see [Mar08]. Motivated mainly by these practical aspects, much work has since the '90s been put into finding optimized algorithms for solving the SAT problem that perform much better than previously thought possible (cf. the $P \neq NP$ conjecture). The apparent discrepancy in the difficulty of solving SAT problem instances has motivated the study of the *typical* structure of the SAT problem, and we will discuss this approach further in the following.

A.2 Preliminaries

The SAT problem asks whether a Boolean function $f : \{\pm 1\}^n \to \{\pm 1\}$ on *conjunctive normal form* (abbreviated CNF) can attain the value 1; in the affirmative case, f is said to be *satisfiable*. CNF means that f is written as a conjunction of disjunctions, or more precisely that $f = C_1 \wedge \cdots \wedge C_m$, where $\wedge$ denotes logical and, and where each of the functions $C_j : \{\pm 1\}^n \to \{\pm 1\}$ is a disjunctive *clause*, i.e. given as the logical or of k variables or their negation. The number k is called the *length* of the clause C_j, and if for some k all clauses $C_1, \dots, C_m$ have length at most k, we say that $C_1 \wedge \cdots \wedge C_m$ is a k-CNF representation. When only considering k-CNF representations for fixed k, the problem is known as the k-SAT problem. For $k = 3$, $n = 7$, and $m = 4$ one could for instance consider the 3-CNF formula

$$f(x) = (x_1 \vee \neg x_3 \vee x_4) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_6 \vee \neg x_7) \wedge x_7.$$

To analyze the typical structure of the k-SAT problems we introduce the following probability distribution over the space of k-CNF formulas referred to as the random k-SAT model F_k.

Definition A.1. *For positive integers k, n, m, we define $F_k(n, m)$ to be the random k-CNF formula in n variables obtained as the conjunction of m i.i.d. random clauses $C_1, \dots, C_m$. Each clause C_j is the disjunction of k literals, chosen by first selecting k distinct variables uniformly at random, and then independently negating variables with probability* $1/2$.

The random k-SAT model is often the one considered in the theoretical literature because of its simple structure. There is however more practical pertinence in analyzing mixed models for random satisfiability; for instance, Gent and Walsh observed in [GW94] that satisfiability problems stemming from the industries most often are mixed (in the sense that the clauses are of varying lengths) and have a very different structure from that of F_k. As a starting point we consider for distinct positive integers k_1 and k_2 the random mixed k_1- and k_2-SAT model F_{k_1,k_2}. In this survey we focus on $F_{1,2}$ and $F_{2,3}$.

Definition A.2. *For all positive integers k_1, k_2, n, m_1, m_2 we define*

$$F_{k_1,k_2}(n, m_1, m_2)$$

to be the conjunction of $F_{k_1}(n, m_1)$ and $F_{k_2}(n, m_2)$ defined above.

A.3 Conjectures

For almost a decade it was unclear how to produce formulas for which deciding satisfiability is hard. In '91, Cheeseman et al. publish the empirical study [CKT91] in which they produced hard satisfiability problems by transforming hard graph coloring problems (and the resulting CNF formulas are mixed). Soon after, Selman et al. found in [SML96] a way to directly produce hard instances using the random 3-SAT model $F_3(n, m)$. By considering the parameter $\alpha = m/n$, the *clause density*, they observed a spike in computational hardness in instances with clause density close to 4.3. This is shown on the left in Figure A.6. Next, they observed that the empirical probability of an $F_3(n, \alpha n)$ instance being satisfiable, when α varies from 0 to ∞, drops rapidly from 1 to 0 at around the same point $\alpha \approx 4.3$.

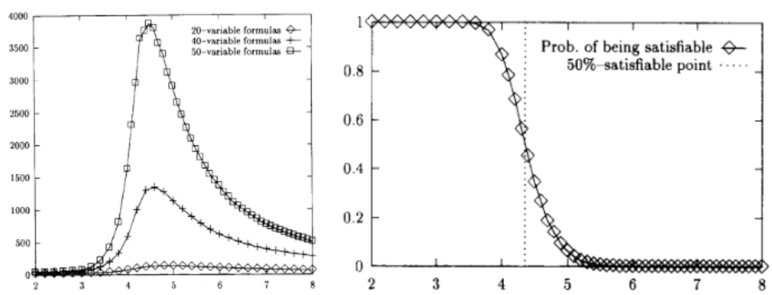


Figure A.6: Left: Fig. 2 from [SML96] showing median "hardness" as a function of α for the model $F_3(n, \alpha n)$ where $n = 20, 40, 50$. Right: Fig. 4 from [SML96] showing the empirical probability of satisfiability for $F_3(50, 50\alpha)$ as a function of α.

A sudden structural shift like the one suggested in Figure A.6 when a parameter passes a single critical value is called a (sharp) *phase transition*, and in 1992 it was famously conjectured by Chvátal and Reed in their paper [CR92] that the random k-SAT problem exhibits such a phenomenon (and proved in the same paper for the case $k = 2$; see current results in the next section):

Conjecture A.3 ([CR92]). *For all $k \geq 2$ there exists a value $\alpha_{\text{sat}}(k) > 0$ separating the with high probability (w.h.p.) satisfiable instances of $F_k(n, \alpha n)$ from the w.h.p. unsatisfiable ones, i.e.*

$$\lim_{n\to\infty} \mathbb{P}(F_k(n,\alpha n) \text{ is satisfiable}) = \begin{cases} 1, & \text{if } \alpha < \alpha_{\text{sat}}(k), \\ 0, & \text{if } \alpha > \alpha_{\text{sat}}(k). \end{cases}$$

Selman et al. [SML96] observed that there seems to be a close connection between the critical point of satisfiability $\alpha_{\text{sat}}(k)$ (if it exists) and the point where one finds hard instances of deciding satisfiability, and in the decades following commenced an intense research effort dedicated to proving Conjecture A.3, and this effort is still ongoing today. In what remains of this paper, we will give an overview of the current status of progress towards Conjecture A.3 and similar conjectures for random mixed models for satisfiability.

For the random mixed 1- and 2-SAT problem, no prior conjectures were put up (and the case $k = 1$ is missing from Conjecture A.3) apart from the following result shown in [Bol+01] hinting at some larger theorem.

Lemma A.4 ([Bol+01]). *For all $d > 0$ it holds that*

$$\lim_{n\to\infty} \mathbb{P}(F_{1,2}(n, \log(n)^d, \alpha n) \text{ is satisfiable}) = \begin{cases} 1, & \text{if } \alpha < \alpha_{\text{sat}}(2), \\ 0, & \text{if } \alpha > \alpha_{\text{sat}}(2). \end{cases}$$

The above result says that one can effectively ignore any polynomial in $\log(n)$ 1-clauses in the random 2-SAT problem when $n \to \infty$. An obvious question is then how many more 1-clauses can be added before they become too numerous to be ignored.

For the $F_{2,3}(n, \alpha_2 n, \alpha_3 n)$ model, it was conjectured in [Mon+96] that when fixing the proportion p of 3-clauses in the mix, i.e. fixing $p = \alpha_3/(\alpha_2 + \alpha_3)$, then there again exists a critical point separating the w.h.p. satisfiable formulas from the w.h.p. unsatisfiable ones.

Conjecture A.5 ([Mon+96]). *For every $p \in [0, 1]$ there exists a value $\alpha_{\text{sat}}(2+p) > 0$ such that for all $\alpha_2, \alpha_3 > 0$ satisfying $\alpha_3/(\alpha_2 + \alpha_3) = p$ it holds that*

$$\lim_{n\to\infty} \mathbb{P}(F_{2,3}(n, \alpha_2 n, \alpha_3 n) \text{ is satisfiable}) = \begin{cases} 1, & \text{if } \alpha < \alpha_{\text{sat}}(2+p), \\ 0, & \text{if } \alpha > \alpha_{\text{sat}}(2+p), \end{cases}$$

where $\alpha = \alpha_2 + \alpha_3$. Furthermore, for $p < 0.413\ldots$ it holds that $\alpha_{\text{sat}}(2 + p) = \alpha_{\text{sat}}(2)/(1 - p)$, and this does not hold for $p \geq 0.413\ldots$.

Notice in the last part of Conjecture A.5 that $\alpha < \alpha_{\text{sat}}(2)/(1-p)$ if and only if $\alpha_2 < \alpha_{\text{sat}}(2)$, which amounts to saying that if the proportion of 3-clauses is low enough in $F_{2,3}(n, \alpha_2 n, \alpha_3 n)$, then they can be ignored, and the problem behaves asymptotically as the $F_2(n, \alpha_2 n)$ subformula. More concretely, one can add $0.703n$ random 3-clauses to $F_2(n, \alpha_2 n)$ for all $\alpha_2 < \alpha_{\text{sat}}(2)$ and still have a w.h.p. satisfiable formula.

A.4 Results

Some serious progress has been made towards proving Conjecture A.3.

Theorem A.6 ([CR92],[Goe96],[DSS22]). *Conjecture A.3 holds for $k = 2$ with $\alpha_{\text{sat}}(2) = 1$. Furthermore, there exists a positive integer k_0 such that Conjecture A.3 holds for all $k \geq k_0$.*

The first part of Theorem A.6 was proved in the early '90s simultaneously by Chvátal and Reed [CR92] and by Andreas Goerdt [Goe96]. More is now known about the random 2-SAT problem; see [Bol+01]. The second part of the Theorem A.6 was recently proved by Jian Ding, Allan Sly, and Nike Sun in [DSS22]. For the remaining k there are upper and lower bounds on $\alpha_{\text{sat}}(k)$ (if they exist) leaving only a gap of constant size (see [DSS22] and references therein).

In regards to Conjecture A.5 we have the following.

Theorem A.7 ([Ach+01]). *Conjecture A.5 holds for all $p \leq 2/5$.*

Achlioptas et al. also give upper and lower bounds for $\alpha_{\text{sat}}(2+p)$ for the remaining $p > 2/5$ in [Ach+01].

Lastly, the random mixed 1- and 2-SAT problem has been completely solved by Andreas Basse-O'Connor, Tobias Overgaard, and Mette Skjøtt in [BOS25], thus "completing" Lemma A.4:

Theorem A.8 ([BOS25]). *For all $\alpha_1 > 0$, $\alpha_2 \in [0, 1)$, and $q > 0$ it holds that*

$$\lim_{n\to\infty} \mathbb{P}(F_{1,2}(n, \alpha_1 n^q, \alpha_2 n) \text{ is satisfiable}) = \begin{cases} 1, & \text{if } q < 1/2, \\ \exp\left(\frac{-\alpha_1^2}{4(1-\alpha_2)}\right), & \text{if } q = 1/2, \\ 0, & \text{if } q > 1/2. \end{cases}$$

Theorem A.8 states that one can add up to an order of $\sqrt{n}$ random 1-clauses to $F_2(n, \alpha_2 n)$ for all $\alpha_2 < 1$ and still have a w.h.p. satisfiable formula. Conditioning on the event that no 1-clauses contradict each other only effects Theorem A.8 in the case $q = 1/2$ where a different limiting value is given. The case $\alpha_2 = 0$ shows that Conjecture A.3 does not hold for $k = 1$, firstly since one should consider in the order of $\sqrt{n}$ 1-clauses as opposed to order n, and secondly since the random 1-SAT problem does not even undergo a phase transition but instead has a smooth limiting probability of satisfiability.

References

[Ach+01] Dimitris Achlioptas et al. “Rigorous results for random $(2+p)$-SAT”. In: *Theoret. Comput. Sci.* 265.1-2 (2001), pp. 109–129.

[Bol+01] Béla Bollobás et al. “The scaling window of the 2-SAT transition”. In: *Random Structures Algorithms* 18.3 (2001), pp. 201–256.

[BOS25] Andreas Basse-O’Connor, Tobias L. Overgaard, and Mette Skjøtt. “On the regularity of random 2-SAT and 3-SAT”. In: *To appear* (2025).

[CKT91] Peter Cheeseman, Bob Kanefsky, and William M. Taylor. “Where the Really Hard Problems Are”. In: *Proceedings of the 12th International Joint Conference on Artificial Intelligence - Volume 1.* IJCAI’91. 1991, pp. 331–337.

[Coo71] Stephen A. Cook. “The Complexity of Theorem-Proving Procedures”. In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing.* STOC ’71. 1971, pp. 151–158.

[CR92] Vašek Chvátal and Bruce Reed. “Mick gets some (the odds are on his side)(satisfiability)”. In: *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science.* SFCS ’92. 1992, pp. 620–627.

[DSS22] Jian Ding, Allan Sly, and Nike Sun. “Proof of the satisfiability conjecture for large k”. In: *Ann. of Math. (2)* 196.1 (2022), pp. 1–388.

[Goe96] Andreas Goerdt. “A Threshold for Unsatisfiability”. In: *J. Comput. Syst. Sci.* 53.3 (1996), pp. 469–486.

[GW94] Ian P. Gent and Toby Walsh. “The SAT Phase Transition”. In: *Proceedings of the 11th European Conference on Artificial Intelligence.* ECAI’94. 1994, pp. 105–109.

[Mar08] Joao Marques-Silva. “Practical applications of Boolean Satisfiability”. In: *2008 9th International Workshop on Discrete Event Systems.* 2008, pp. 74–80.

[Mon+96] Rémi Monasson et al. “Phase transition and search cost in the $(2+p)$-SAT problem”. In: *4th Workshop on Physics and Computation.* 1996.

[SML96] Bart Selman, David G. Mitchell, and Hector J. Levesque. “Generating Hard Satisfiability Problems”. In: *Artif. Intell.* 81 (1996), pp. 17–29.

Article B

On the regularity of random 2-SAT and 3-SAT

Andreas Basse-O'Connor[1], Tobias Overgaard[1], and Mette Skjøtt[1,2]

[1]Department of Mathematics, Aarhus University,
[2]Kvantify Aps

April 2025

Abstract: We consider the random k-SAT problem with n variables, $m = m(n)$ clauses, and clause density $\alpha := \lim_{n\to\infty} m/n$ for $k = 2, 3$. It is known that if α is small enough, then the random k-SAT problem admits a solution with high probability, which we interpret as the problem being under-constrained. In this paper, we quantify exactly how under-constrained the random k-SAT problems are by determining their degrees of freedom, which we define as the threshold for the number of variables we can fix to an arbitrary value before the problem no longer is solvable with high probability. Our main result shows that the random 2-SAT and 3-SAT problems have $n/m^{1/2}$ and $n/m^{1/3}$ degrees of freedom, respectively. We also explicitly compute the corresponding threshold functions. Our result shows that the threshold function for the random 2-SAT problem is regular, while it is non-regular for the random 3-SAT problem. By regular, we mean continuous and analytic on the interior of its support. This result shows that the random 3-SAT problem is more sensitive to small changes in the clause density α than the random 2-SAT problem.

B.1 Introduction

B.1.1 Background

For more than half a century, the Boolean k-satisfiability (k-SAT) problem has enjoyed continued interest in the field of computer science. The 3-SAT problem was one of the five original NP-complete problems from Cooks seminal paper [Coo71], viz. $P = NP$ is equivalent to the existence of a polynomial-time algorithm for solving 3-SAT problem instances. The 3-SAT problem thus lies at the heart of the famous P vs. NP problem. Similarly, the 2-SAT problem lies at the heart of the important L vs. NL problem, as $L = NL$ is equivalent to the existence of a logarithmic-space algorithm for solving 2-SAT problem instances (Thm. 16.3 in [Pap94]), that is, the 2-SAT problem is NL-complete. The k-SAT problem has also turned out to have great practical significance in artificial intelligence, bioinformatics, hardware verification, and more (see [GGW06; Mar08]).

In applications, there seemed to be a major gap between the theoretical bounds for the runtime of SAT solving algorithms and the comparatively fast performance of SAT solvers (see [Goe96a; FP83; CKT91; SML96]). Thus, the study of the *random* k-SAT problem arose, motivated by an interest in understanding the typical structure of a SAT problem instance (compared to the hitherto worst-case analysis) and understanding where to find the "hard" SAT problems. The random k-SAT problem has for the last three decades remained highly relevant in the fields of probability theory and statistical physics (see [Knu15; DSS22] and references therein).

The random k-SAT problem Φ—also called a random k-CNF formula—with m clauses and n variables is obtained by taking m i.i.d. random disjunctive clauses $C_1, \dots, C_m$ of length k, i.e. of the form $C(x) = s_1 x_{v_1} \vee \dots \vee s_k x_{v_k}$, where $s_1, \dots, s_k \in \{-1, 1\}$, and where $v_1, \dots, v_k \in [n] := \{1, \dots, n\}$ are pairwise distinct. Each C_j is chosen uniformly at random among the $2^k \binom{n}{k}$ possibilities. Then Φ is the conjunction/minimum of these, $\Phi := C_1 \wedge \dots \wedge C_m$. The problem is to determine whether there exists an assignment $x = (x_1, \dots, x_n) \in \{-1, 1\}^n$ such that $\Phi(x) = 1$, i.e. such that all the clauses are simultaneously "satisfied". We call such an x a *solution* to Φ, and in the affirmative case, we say that Φ is *satisfiable* and write $\Phi \in \mathsf{SAT}$. We will consider the random k-SAT problem asymptotically, so in the following, the random k-SAT problem/a random k-CNF formula with $m = m(n)$ clauses and n variables refers to a *sequence* of random k-CNF formulas, where the n'th term is a random k-CNF formula with $m(n)$ clauses and n variables as described above.

In 1992 it was conjectured in [CR92] that for every $k \geq 2$ there exists a critical value $\alpha_c(k) > 0$, such that if Φ is a random k-CNF formula with $m = m(n)$ clauses and n variables, where $m/n \to \alpha$ as $n \to \infty$, then

$$\lim_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) = \begin{cases} 1, & \text{if } \alpha < \alpha_c(k), \\ 0, & \text{if } \alpha > \alpha_c(k), \end{cases} \tag{B.1.1}$$

that is, the satisfiability of the random k-SAT problem is conjectured to undergo a phase transition as α, the *clause density*, crosses a critical threshold $\alpha_c(k)$. In the regime $\alpha < \alpha_c(k)$ in (B.1.1), where the problem is satisfiable with high probability (w.h.p.), we will call the random k-SAT problem *under-constrained.*

In the present paper, we focus on the random 2-SAT and 3-SAT problems. In regards to the former, the satisfiability conjecture (B.1.1) was proved independently in [CR92] and [Goe96b], where it was shown that $\alpha_c(2) = 1$. Much more has since been discovered about the random 2-SAT problem, and overall it remains an interesting and actively researched problem; see for instance [Goe99; Ver99; Bol+01; Ach+21; Cha+24].

Conjecture (B.1.1) has recently been proved for all $k \geq k_0$ in the monumental work [DSS22], where k_0 is a large unknown constant, but for $k = 3$ the problem remains elusive. Thus, the sharp satisfiability threshold for the random 3-SAT problem is still an important open question. However, much research activity has been directed towards overcoming this challenge, and increasingly tighter bounds on which α's result in asymptotic satisfiability or unsatisfiability have been produced throughout the years (see [FP83; Fra84; BFU93; EF95; Kam+95; FS96; DB97; Kir+98; Zit99; Fri99; Ach00; JSV00; AS00; DBM02; HS03; KKL06; Kap+07; Día+09]), showing for example that the random 3-SAT problem is under-constrained when $\alpha < 3.52$.

B.1.2 Main result

Let Φ be an under-constrained random 2- or 3-CNF formula. We pose and aim to answer the following question: *how* under-constrained is Φ? Our proposed solution is based on the following idea: there are too many degrees of freedom in the variables $x_1, \ldots, x_n$ compared to the number of clauses in Φ, so fix a number, say $f = f(n)$, of the variables $x_1, \ldots, x_n$, each to either 1 or -1. Does there still w.h.p. exist a solution to Φ in this restricted search space? Presumably, if f is large enough, the answer will be no. We will represent the "under-constrainedness" of Φ as the critical mass of the number f of variables needed to be fixed before Φ becomes unsatisfiable w.h.p., and we call this number the *degrees of freedom* in Φ. This is an analogue concept to the nullity, i.e. the size of the kernel/null space, of a (random) matrix; it is the number of variables we can "freely" fix before the corresponding system of equations no longer has a solution (w.h.p.)

We say that a subset $\mathcal{L}$ of $\pm[n] := \{-n, \ldots, -1, 1, \ldots, n\}$ is *consistent* if, for all $v \in [n]$, at most one of v and $-v$ is in $\mathcal{L}$. Here, $v \in \mathcal{L}$ represents fixing x_v to 1 and $-v \in \mathcal{L}$ represents fixing x_v to -1 for each $v \in [n]$. Let $\Phi_{\mathcal{L}}$ denote the formula Φ with these restrictions to its domain.

Definition B.1 (Degrees of freedom in the random k-SAT problem). *The random k-SAT problem Φ with $m = m(n)$ clauses and n variables has $f_* = f_*(n)$* degrees of freedom *if, for all* $f = f(n)$ *and all consistent (non-random) subsets* $\mathcal{L} \subseteq \pm[n]$ *with* $|\mathcal{L}| = f$*, it holds that* f_* *is a threshold in* f *for the satisfiability of* $\Phi_{\mathcal{L}}$*, that is, if*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \begin{cases} 1, & \text{when } f/f_* \to 0, \\ 0, & \text{when } f/f_* \to \infty. \end{cases} \tag{B.1.2}$$

The concept of a threshold hearkens back to the seminal paper [ER60] by Erdős and Rényi. In Theorem B.2 below, we find a threshold f_*, which we also show is unique up to asymptotic order, in the cases $k = 2, 3$. Furthermore, we find an explicit expression for the *threshold function*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \tag{B.1.3}$$

when $0 < \lim_{n\to\infty}(f/f_*) < \infty$. In the following, we interpret $e^{-\infty} := 0$.

Theorem B.2. *Let* Φ *be a random* k*-CNF formula with* $m = m(n)$ *clauses and* n *variables such that* $m \to \infty$ *and* $m/n \to \alpha$*. Let* $\mathcal{L} \subseteq \pm[n]$ *be a consistent set with* $f = f(n)$ *elements. Let finally* $\gamma \in [0, \infty]$*.*

- *If* $k = 2$:, $\alpha \in [0, 1)$ *and* $f\sqrt{m}/n \to \gamma$*, then*

  $$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^2(1-\alpha)^{-1}}.$$

  In particular, the random 2*-SAT problem with* m *clauses and* n *variables has* $n/\sqrt{m}$ *degrees of freedom for clause density* $\alpha < 1$*.*

- *If* $k = 3$, $\alpha \in [0, 3.145)$*, and* $f m^{1/3}/n \to \gamma$*, then*

  $$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^3}.$$

  In particular, the random 3*-SAT problem with* m *clauses and* n *variables has* $n/m^{1/3}$ *degrees of freedom for clause density* $\alpha < 3.145$*.*

Remark B.3. *In both cases* $k = 2, 3$ *in Theorem B.2, there are two distinct scenarios:*

- ***The case*** $\boldsymbol{\alpha = 0}$*: Theorem B.2 in particular applies to the "ultra" under-constrained case not traditionally studied in the literature, showing precisely how the number of constraints in a random* 2*- or* 3*-CNF formula affects the number of degrees of freedom. As an example, the random* 2*-SAT problem with* n *variables and only* $\log(n)$ *clauses has* $n/\sqrt{\log(n)}$ *degrees of freedom.*

- ***The case*** $\boldsymbol{\alpha > 0}$*: In this case, the random* k*-SAT problem with* $m \sim \alpha n$ *clauses and* n *variables has* $n^{1-1/k}$ *degrees of freedom when* $\alpha \in (0, 1)$ *respectively* $0\alpha \in (0, 3.145)$ *for* $k = 2, 3$*. Furthermore, the threshold functions are given by*

$e^{-(\beta/2)^2\alpha(1-\alpha)^{-1}}$ and $e^{-(\beta/2)^3\alpha}$ when $f/n^{1-1/k} \to \beta$ for some $0 \le \beta \le \infty$. This statement is equivalent to Theorem B.2 and follows directly from the asymptotic equivalence $m \sim \alpha n$. An advantage of the parameter β is that it only depends on f, where γ depends on both m and f; indeed, $\gamma = \beta\alpha^{1/k}$.

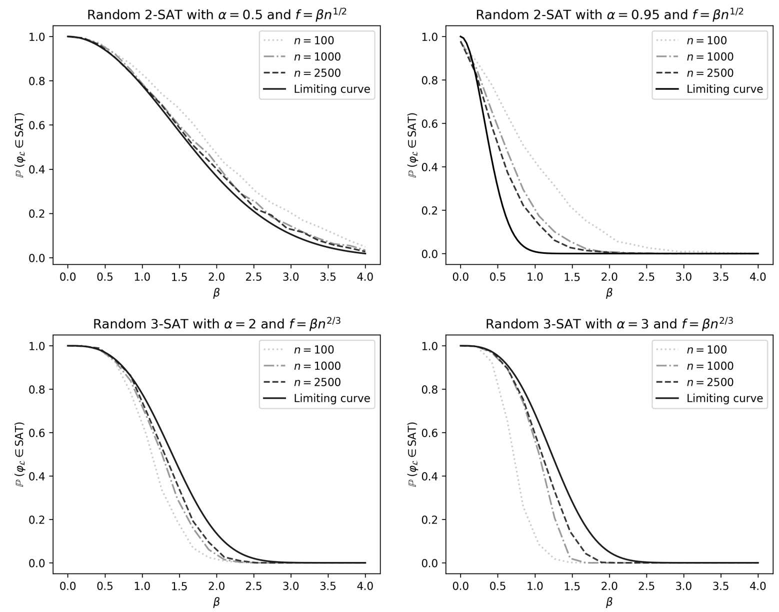


Figure B.7: Finite size sampling of the threshold functions corresponding to the degrees of freedom in the random 2- and 3-SAT problems. Each datapoint (40 for each curve) is comprised of 2000 simulations.

Figure B.7 shows finite size sampling of the threshold functions from Theorem B.2 for fixed values of α. The simulations suggest that the convergence is faster for smaller values of α.

Remark B.4. *We now prove uniqueness modulo asymptotic order of the degrees of freedom for the random k-SAT problem, $k = 2, 3$. Let Φ be a random k-CNF formula with $m = m(n)$ clauses and n variables, $m/n \to \alpha$, where $\alpha < 1$ if $k = 2$ or $\alpha < 3.145$ if $k = 3$, and let $\mathcal{L} \subseteq \pm[n]$ be consistent. We have seen in Theorem B.2 that $f_* = n/m^{1/k}$ is a threshold in $|\mathcal{L}|$ for the satisfiability of $\Phi_{\mathcal{L}}$, cf.* (B.1.2). *Assume that $g_* = g_*(n)$ is another such threshold. Then, taking $|\mathcal{L}| = f_*$, we get $0 < \lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) < 1$ from Theorem B.2. Hence, we cannot have $f_*/g_* \to 0$ or $f_*/g_* \to \infty$ by* (B.1.2), *as this would imply $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 1$ or $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0$, respectively. Furthermore, by considering sub-sequences, we cannot even have $\liminf_{n\to\infty}(f_*/g_*) = 0$ or $\limsup_{n\to\infty}(f_*/g_*) = \infty$, that is, f_* and g_* are of the same asymptotic order.*

We see that the threshold functions $e^{-(\gamma/2)^2(1-\alpha)^{-1}}$ and $e^{-(\gamma/2)^3}$ are real analytic functions in γ that are bounded away from 0 and 1 (when $\gamma \in (0, \infty)$), and thus the threshold f_* in (B.1.2) is *not* sharp. A sharp threshold would correspond to a step function from 1 to 0 at some critical value γ_c, which is not what we find. Hence, this is a markedly different type of threshold compared to the sharp threshold seen for example in the Boolean satisfiability conjecture (B.1.1) (still only conjecture for $k = 3$ but proved for $k = 2$).

Returning again to our original question, we now have a way to quantify under-constraindness in the random k-SAT problem. Let us compare the random 2-SAT and 3-SAT problems: intuitively, clauses of length 3 (ternary clauses) are "less constraining" than clauses of length 2 (binary clauses). Indeed, the degrees of freedom also reflect this; let Φ be a random 3-CNF formula with n variables and $m \sim \alpha n$ clauses, where $\alpha \in (0, 3.145)$. Then from Theorem B.2 it follows that Φ has $n^{2/3}$ degrees of freedom, which is the same as a random 2-CNF formula with n variables and only $\Theta(n^{2/3})$ clauses!

To the best of our knowledge, Theorem B.2 is the first result of its kind. We believe that degrees of freedom will become an important concept in the analysis of random constraint satisfaction problems.

B.1.3 The search tree

When searching for a solution to a given k-SAT instance, a common approach is to fix the value of x_1 (e.g., set $x_1 = 1$). If this assignment does not violate any clauses, we then proceed to fix x_2 (e.g., set $x_2 = -1$). By continuing this process, we generate a *search tree*, as illustrated in Figure B.8. The degrees of freedom f_* for the random k-SAT problem can be thought of as the maximum depth in the search tree that can be reached without violating the k-SAT instance, thus avoiding backtracking. According to Theorem B.2, for the random 2-SAT problem with $\alpha < 1$, this maximum depth is $n/\sqrt{m}$, while for the random 3-SAT problem with $\alpha < 3.145$, the maximum depth is $n/m^{1/3}$. To the best of our knowledge, this is one of the first results quantifying the additional flexibility in solving the random 3-SAT problem compared to the random 2-SAT problem.

B.1.4 Mixed SAT problems

As an almost immediate consequence of Theorem B.2, we get the following characterization of asymptotic satisfiability in the random mixed 1- and k-SAT problem when $k = 2, 3$.

Theorem B.5. *Let Φ_k be a random k-CNF formula with $m = m(n)$ clauses and n variables, where $m/n \to \alpha$, and let Φ_1 be a random 1-CNF formula with $f = f(n)$ clauses and n variables, where $f/\sqrt{n} \to \beta$ for some $\beta \in [0, \infty]$, such that Φ_k and Φ_1 are independent.*

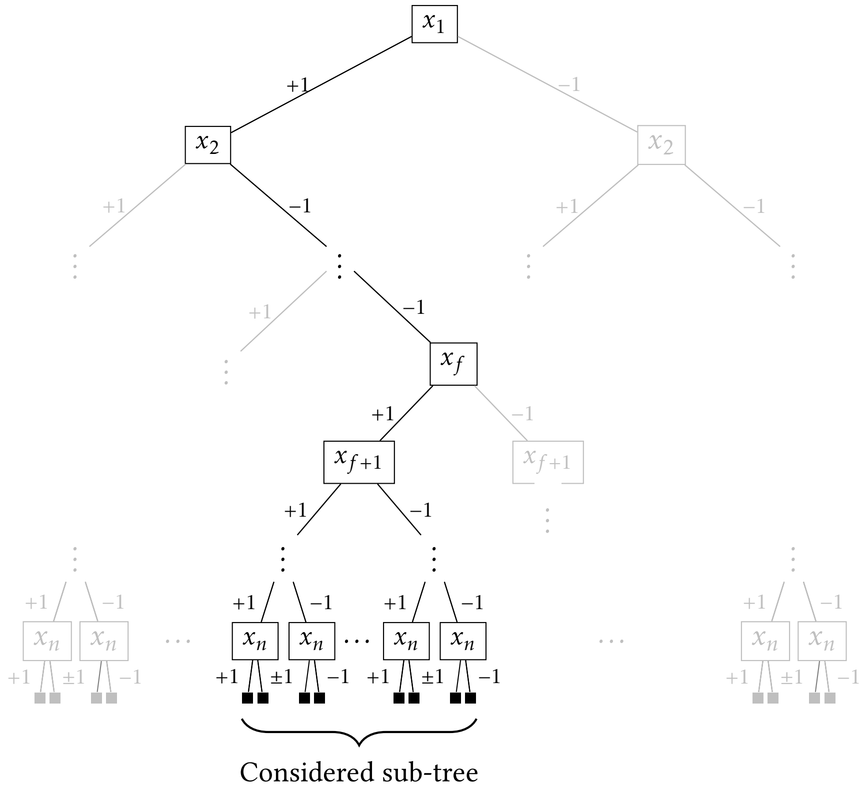


Figure B.8: Going down f steps into the search tree and thus only considering assignments $x \in \{-1, 1\}^n$ on one of the sub-trees branching out at x_{f+1}.

- *If* $k = 2$, *and* $\alpha \in [0, 1)$, *then* $\lim_{n\to\infty} \mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT}) = e^{-(\beta/2)^2(1-\alpha)^{-1}}$.
- *If* $k = 3$, *and* $\alpha \in [0, 3.145)$, *then* $\lim_{n\to\infty} \mathbb{P}(\Phi_3 \wedge \Phi_1 \in \mathsf{SAT}) = e^{-(\beta/2)^2}$.

In Knuth's book on Boolean satisfiability [Knu15], he writes: "unit clauses aren't rare: Far from it. Experience shows that they're almost ubiquitous in practice, so that the actual search trees often involve only dozens of branch nodes instead of thousands or millions." In Theorem B.5, we analyze the effect of adding these ubiquitous unit clauses to the random 2-SAT and 3-SAT problems.

For the random 2-SAT problem, the "missing" factor between the threshold functions in Theorem B.5 and Theorem B.2 is exactly the probability that the random unit clauses comprising Φ_1 cause a contradiction, i.e. the probability that there exists some $v \in [n]$ such that both x_v and $-x_v$ are clauses in Φ_1. If we condition on this event not occurring, then we reclaim the original limit $e^{-(\beta/2)^2\alpha(1-\alpha)^{-1}}$ from Theorem B.2 (see Remark B.3). And indeed, taking $\alpha = 0$ in Theorem B.5 gives the following result: if Φ_1 is a random 1-CNF formula with n variables and f clauses where $f/\sqrt{n} \to \beta$, then

$$\lim_{n\to\infty} \mathbb{P}(\Phi_1 \in \mathsf{SAT}) = e^{-(\beta/2)^2}. \tag{B.1.4}$$

This limit is again an analytic function in β (a Gaussian, even), and thus the random 1-SAT problem does not exhibit a phase transition/sharp threshold in satisfiability. We also see that the relevant parameter to consider in this problem is not the usual clause density α, but rather β, the ratio of clauses to the *square root* of the number of variables. That α is the wrong parameter is no surprise; Chvátal and Reed had naturally realized this and excluded the random 1-SAT problem from Conjecture (B.1.1), and Gent and Walsh even outright state in [GW94] that a random 1-CNF formula with n variables and clause density $\alpha > 0$ is always unsatisfiable with high probability. Despite this, we believe that this paper is the first to identify the correct parameter β and with it completely characterize the random mixed 1- and 2-SAT problem in Theorem B.5.

Theorem B.5 shows that the random mixed 1- and 2-SAT problem behaves like the random 1-SAT problem, in that the limiting probability of satisfiability does not have a sharp threshold, but instead varies smoothly in the parameters α and β, and even the slightest change to either of these affects this limit. The addition of $\beta\sqrt{n}$ random unit clauses has thus "smoothed out" the phase transition of the random 2-SAT problem seen in (B.1.1).

Another property of the random mixed 1- and 2-SAT problem is that we are able to "exchange" unit clauses for binary clauses—or the other way around—without changing the limiting probability of the mixed formula being satisfiable. Indeed, if Φ is again a random CNF formula with $\beta\sqrt{n}$ unit clauses and αn binary clauses, and we want to exchange, say, half of the unit clauses, so that Φ is left with $(\beta/2)\sqrt{n}$ of these, then to compensate we need to add $3n$ random binary clauses and then remove three-quarters of this new total, so that Φ ends up with $((3+\alpha)/4)n$ binary clauses. Doing this exchange, the limiting probability that Φ is satisfiable will remain the same. More generally, if we want to exchange from Φ to a random mixed CNF-formula Φ' with $\beta'\sqrt{n}$ unit clauses and $\alpha' n$ binary clauses, then Φ and Φ' have the same asymptotic satisfiability as long as

$$\left(\frac{\beta'}{\beta}\right)^2 = \frac{1-\alpha'}{1-\alpha}. \tag{B.1.5}$$

This is a very distinct situation from the random mixed 1- and 3-SAT problem, detailed in the second part of Theorem B.5. Indeed, we see from Theorem B.5 that one can add up to $3.145n$ random 3-clauses to *any* random 1-CNF formula without changing the asymptotic probability of satisfiability (compare Theorem B.5 case $k = 3$ with (B.1.4)). Hence, the "exchange rate" between 1- and 3-clauses is infinite, since we are able to add these $< 3.145n$ random 3-clauses "for free".

In regards to exchange rate, the random mixed 1- and 3-SAT problem shows more similarity with the random mixed 2- and 3-SAT problem, which was first studied in the physics literature [Mon+96; MZ98; Mon+99; BMW00] and later given a rigorous treatment in [Ach+01] (slightly improved upon in [ZG13]). Here it was established that one can add at least $(2/3)n$ random 3-clauses, but no more than $2.17n$, to any under-constrained random 2-CNF formula and have the resulting formula remain under-constrained. Again, the exchange rate between 2- and 3-clauses is infinite, and the smaller clauses completely dominate the problem. That is, the asymptotic satisfiability is determined completely by the random 2-CNF sub-formula, just as we saw that the asymptotic satisfiability of a random mixed 1- and 3-CNF formula is determined by the random 1-CNF sub-formula (see Chapter 10 of [BHM21] for a further discussion on exchange rate).

Returning finally to the random mixed 1- and 2-SAT problem again, we note that this problem is not only interesting in its own right, but it is also sometimes useful for proofs. Indeed, in the paper [Ach00], the following result is used: if Φ is a random CNF formula with n variables, αn binary clauses, and any polynomial in $\log(n)$ unit clauses, then Φ is under-constrained in the usual region $\alpha < 1$. Our Theorem B.5 is obviously a direct strengthening of this, since we show that one can take n^q for any $q < 1/2$ (actually anything in $o(\sqrt{n})$) in place of the polynomial in $\log(n)$ unit clauses and still get the same result. Theorem B.5 also shows that this is *optimal*, in the sense that adding n^q independent random unit clauses to an under-constrained random 2-CNF formula spoils the asymptotic satisfiability when $q \geq 1/2$.

B.1.5 The threshold functions

For $k = 2, 3$, $\alpha > 0$ and $\beta \in [0, \infty)$, let Φ be a random k-CNF formula with $m \sim \alpha n$ clauses and n variables. We recall that Φ has $n^{1-1/k}$ degrees of freedom. Let $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| = f = f(n)$, where $f/n^{1-1/k} \to \beta$. We denote the threshold function from (B.1.3) by

$$\pi_k(\alpha, \beta) := \lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}),$$

when this limit exists (and only depends on α and β), and define $\pi_k(\alpha, \beta) := 0$ otherwise. From Theorem B.2, we have that $\pi_2(\alpha, \beta) = e^{-(\beta/2)^2\alpha(1-\alpha)^{-1}}$ when $\alpha \in (0, 1)$ and $\pi_3(\alpha, \beta) = e^{-(\beta/2)^3\alpha}$ when $\alpha \in (0, 3.145)$. The graphs of π_2 and π_3 are plotted in Figure B.9.

We define $\alpha_{\text{supp}}(k) := \inf\{\alpha\colon \pi_k(\alpha, \beta) = 0\}$, i.e. the right endpoint of $\text{supp}(\pi_k(\cdot, \beta))$. Now, if Φ is unsatisfiable w.h.p., then $\pi_k(\alpha, \beta) = 0$ for all $\beta \geq 0$, so we get $\alpha_{\text{supp}}(3) \leq 4.4898$ from [Día+09], as this is the current best upper bound on $\alpha_{\text{c}}(3)$. Therefore, the value of the threshold function $\pi_3(\alpha, \beta)$ is known for $\alpha < 3.145$ (from our Theorem B.2) and for $\alpha > 4.4898$, which explains the

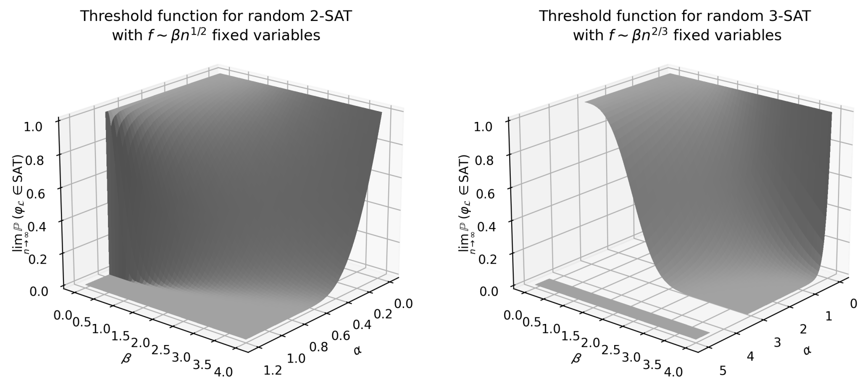


Figure B.9: The threshold functions corresponding to the degrees of freedom in the random 2-SAT and 3-SAT problems.

“gap” in the graph in Figure B.9 r.h.s. For the random 2-SAT problem, we have $\alpha_{\text{supp}}(2) = \alpha_{\text{c}}(2) = 1$ from [CR92] and Theorem B.2.

What happens in this gap $\alpha \in [3.145, 4.4898]$ remains an open problem with several potential scenarios possible. For the random 2-SAT problem, we see that fixing $f \sim \beta\sqrt{n}$ variables ($\beta > 0$) has “smoothed out” the sharp satisfiability threshold at $\alpha_{\text{c}}(2) = 1$ (this sharp threshold is visible at $\beta = 0$). That is, the threshold function $\pi_2(\alpha, \beta)$ is continuous, and even C^∞ (smooth), in α on the entire domain $\alpha > 0$, since $e^{-(\beta/2)^2\alpha(1-\alpha)^{-1}}$, and its derivatives of all orders in α, tend towards 0 as $\alpha \longrightarrow 1$. On the other hand, $e^{-(\beta/2)^3\alpha}$ does not tend towards 0 as $\alpha \longrightarrow \alpha_{\text{supp}}(3)$ (whatever $\alpha_{\text{supp}}(3)$ might be). From these observations and Theorem B.2, we immediately get the following conclusion.

Corollary B.6. *Let $\beta > 0$ be given. For the random 2-SAT problem, the threshold function $\pi_2(\alpha, \beta)$ is analytic for $\alpha \in (0, \alpha_{\text{supp}}(2))$ and continuous (smooth, even) for all $\alpha > 0$. For the random 3-SAT problem, the threshold function $\pi_3(\alpha, \beta)$ is analytic for $\alpha \in (0, 3.145)$, but it* cannot *be both analytic for $\alpha \in (0, \alpha_{\text{supp}}(3))$ and continuous for all $\alpha > 0$.*

Proof. Because of the identity theorem for analytic functions, if $\pi_3(\alpha, \beta)$ is real analytic for $\alpha \in (0, \alpha_{\text{supp}}(3))$, then necessarily $\pi_3(\alpha, \beta) = e^{-(\beta/2)^3\alpha}$ for all $\alpha \in (0, \alpha_{\text{supp}}(3))$, which precludes continuity at $\alpha_{\text{supp}}(3)$. □

Corollary B.6 shows a significant distinction between the random 2-SAT and 3-SAT problems. While the threshold function for random 2-SAT is regular—continuous and analytic on the interior of its support—the threshold function for random 3-SAT is non-regular. Consequently, the random 3-SAT problem is particularly sensitive to variations in the clause density α compared to the random 2-SAT problem.

B.1.6 Structure

The structure of the remainder of the paper is as follows: in Section B.2 we give a sketch of the proof of Theorem B.2, where we explain the main steps and difficulties. In Section B.3 we review the necessary preliminaries for a complete proof of Theorems B.2 and B.5, and in Section B.4 we give the full proof, starting with a number of smaller results required for later.

B.2 Sketch of proof

We begin by outlining a proof of Theorem B.2 in the case $k = 2$ when $\alpha > 0$. The proof relies on the following two special cases: namely (B.1.4), the random 1-SAT problem, a special case of Theorem B.5, and Theorem B.2 in the "subcritical" case where $\beta = 0$. The latter says that fixing $o(\sqrt{n})$ variables in an underconstrained random 2-CNF formula still yields a w.h.p. satisfiable formula, and we prove this using a novel variation on the classic "snakes and snares" proof of $\alpha_c(2) = 1$ from [CR92; Goe96b; Knu15]. The former, i.e. (B.1.4), is proved through a direct counting argument.

The idea of the proof is now as follows: let $\Phi = C_1 \wedge \cdots \wedge C_m$ be a random 2-CNF formula with n variables and $m = m(n)$ clauses, where $m/n \to \alpha$, $\alpha \in (0, 1)$, and let $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| = f = f(n)$, where $f/\sqrt{n} \to \beta$, and we assume without loss of generality that $\beta \in (0, \infty)$. Now, a critical observation is the following: each of the clauses C_j experiences one of four fates when the variables dictated by $\mathcal{L}$ are fixed:

0. it becomes a 0-clause, i.e. is unsatisfied, and thus precludes the satisfiability of $\Phi_{\mathcal{L}}$,
1. it becomes a 1-clause and thus dictates the value of a new variable,
2. it remains unaltered as a 2-clause,

$\star$. it becomes a $\star$-clause, i.e. is satisfied, and thus no longer affects the satisfiability of $\Phi_{\mathcal{L}}$.

The core of the proof is understanding and carefully controlling how many clauses land in each of the four cases above, and especially important are cases 0 and 1. Denote by $\mathcal{C}_1^{(1)}$ the set of $j \in [m]$ for which C_j falls into case 1. The unit clauses corresponding to $\mathcal{C}_1^{(1)}$ form a 1-CNF formula $\Phi_1^{(1)} = \min\{C_j : j \in \mathcal{C}_1^{(1)}\}$, which must be satisfiable for $\Phi_{\mathcal{L}}$ to be satisfiable, and furthermore, they fix the value of $M_1^{(1)} :=$

$|\mathcal{C}_1^{(1)}|$ new variables. Thus, the "remaining" 2-CNF formula (i.e. the conjunction of the clauses in case 2), call it $\Phi_2^{(1)}$, undergoes the same "splitting" into 0-, 1-, 2-, and $\star$-clauses when fixing the variables dictated by $\Phi_1^{(1)}$.

Let $\mathcal{C}_h^{(r)}$ denote the set of $j \in [m]$ for which C_j falls into case $h \in \{0, 1, 2, \star\}$ in the r'th round of this iterative process, and let $M_h^{(r)} := |\mathcal{C}_h^{(r)}|$. We denote by $\Phi_1^{(r)}$ and $\Phi_2^{(r)}$ respectively the random 1-CNF and random 2-CNF formula generated in this round, and let $\mathcal{L}^{(r)}$ denote the set of literals forming $\Phi_1^{(r)}$. For each r we rely on the fact that $(\Phi_2^{(r-1)})_{\mathcal{L}^{(r-1)}}$ (or $\Phi_{\mathcal{L}}$ for $r = 1$) is satisfiable if and only if

$$M_0^{(r)} = 0, \quad \Phi_1^{(r)} \in \mathsf{SAT}, \quad \text{and} \quad (\Phi_2^{(r)})_{\mathcal{L}^{(r)}} \in \mathsf{SAT}.$$

It turns out that these three events are almost independent (the error vanishes as $n \to \infty$), so

$$\mathbb{P}\Big((\Phi_2^{(r-1)})_{\mathcal{L}^{(r-1)}} \in \mathsf{SAT}\Big) \approx \mathbb{P}\Big(M_0^{(r)} = 0\Big) \cdot \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) \cdot \mathbb{P}\Big((\Phi_2^{(r)})_{\mathcal{L}^{(r)}} \in \mathsf{SAT}\Big) \tag{B.2.1}$$

for each $r \in \mathbb{N}$. Using this approach, the important issue becomes: how large are $M_0^{(r)}$ and $M_1^{(r)}$? This is obviously heavily dependent on the previous "rounds", but on average, $M_1^{(r)}$ is of the order $\alpha^r \beta \sqrt{n}$. A core part of the proof is showing that $M_1^{(r)}$ concentrates around this mean. Now, we have suppressed the dependence on n in the notation, but the iterative decomposition (B.2.1) is done for each $n \in \mathbb{N}$. The next step of the proof is to *diagonalize*, taking r dependent on n; specifically, when r becomes larger than $\log(n)$, then $\alpha^r \beta \sqrt{n}$, and thus $M_1^{(r)}$, becomes *smaller* than $\beta n^{1/2+\log(\alpha)}$ (where of course $\log(\alpha) < 0$), and at this point the problem shifts into the subcritical case where the number of variables being fixed is $o(\sqrt{n})$, which is one of the special cases which we already proved. Indeed, taking $R := c\log(n)$, where $c > 0$ is some appropriate constant, we use the decomposition (B.2.1) R times successively to get

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \approx \mathbb{P}\Big((\Phi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big) \prod_{r=1}^{R} \mathbb{P}\Big(M_0^{(r)} = 0\Big) \prod_{r=1}^{R} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big),$$

and the special case gives us $\mathbb{P}((\Phi^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}) \to 1$, and the other special case (B.1.4) gives us (because of the concentration phenomenon)

$$\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) \longrightarrow e^{-\frac{1}{4}\beta^2\alpha^{2r}}$$

for each $r \in [R]$. Finally, we are able to show directly that

$$\mathbb{P}\Big(M_0^{(r)} = 0\Big) \longrightarrow e^{-\frac{1}{4}\beta^2\alpha^{2r-1}}$$

for each $r \in [R]$, which will then imply (with some additional arguments) that

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \longrightarrow \exp\left(\frac{-\beta^2}{4}\sum_{r=1}^{\infty}\alpha^r\right) = \exp\left(\frac{-\beta^2\alpha}{4(1-\alpha)}\right).$$

We see that each even term in the infinite series comes from the probability that the appearing unit clauses cause a contradiction among themselves, and each odd term comes from the probability of the appearance of a 0-clause.

Besides some lemmas and the special cases, the main technical difficulty in converting the idea above into a proof is the concentration of $M_h^{(r)}$, in particular for $h = 1$. We will find bounds $f_-^{(r)}, f_+^{(r)}$ such that $M_1^{(r)}$ stays within $[f_-^{(r)}, f_+^{(r)}]$ w.h.p., and such that both $f_-^{(r)}, f_+^{(r)} \sim \alpha^r\beta\sqrt{n}$. In place of $\Phi_1^{(r)}$ we insert an independent random 1-CNF formula with $f_-^{(r)}$ resp. $f_+^{(r)}$ clauses, which will lead to an asymptotic upper resp. lower bound on $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})$. Namely, the idea will be to choose

$$f_\pm^{(r)} \approx \alpha^r f \pm r\alpha^r n^{3/8},$$

which exactly does the job, as we will see.

Now, if $\alpha = 0$ (and Φ is still a random 2-CNF formula), then already in the first "round" $r = 1$ in the decomposition (B.2.1), the number of 1-clauses generated $|\mathcal{L}^{(1)}|$ is $o(\sqrt{n})$, so the subcritical special case may immediately be invoked.

For the case $k = 3$ in Theorem B.2, the same strategy may be employed. The decomposition (B.2.1) still holds, although we now have a random mixed 2- and 3-CNF formula. Thus, there are more things to keep track of in this case, and we will not have a proof of the subcritical case handy, making the whole thing slightly more tedious. On the other hand, we show that w.h.p. there are no more unit clauses appearing after three rounds, so we avoid infinite series. For this reason, we are also able to prove Theorem B.2 case $k = 3$ for all $\alpha \in [0, 3.145)$ instead of having $\alpha = 0$ separate. The threshold function comes from the fact that

$$\mathbb{P}\left(M_0^{(1)} = 0\right) \longrightarrow e^{-(\beta/2)^3\alpha},$$

which comes from a direct calculation. Thus, it remains to show that the other terms of the decomposition (B.2.1) tend towards 1. This is again achieved via the concentration of the random variables $M_h^{(r)}$. We rely on existing literature to show that the final error term involving a random mixed 2- and 3-CNF formula vanishes.

B.3 Preliminaries

In this section, we will review the necessary preliminary results and notations for Boolean functions $\varphi : \{-1,1\}^n \to \{-1,1\}$ of $n \in \mathbb{N}$ variables needed for the formulation and proof of this paper's results.

B.3.1 Boolean functions

For any $A \subseteq \mathbb{Z}$ we define:

$$A_{\text{abs}} := \{|a|\colon a \in A\}, \quad -A := \{-a\colon a \in A\}, \quad \pm A := A \cup (-A),$$

and $|A|$ for the number of elements in A. For $n \in \mathbb{N}$ we use the notation

$$[n] := \{1, 2, \dots, n\}.$$

We let SAT denote the set of all functions $\varphi : B \to \{-1, 1\}$ with the element 1 contained in the range of φ, where B is a non-empty subset of $\{-1, 1\}^n$ for any n, called the *satisfiable* functions. If $x \in B$ is such that $\varphi(x) = 1$, then φ is said to be *satisfied* at x. The collection of such x is called the *solution space* for φ and is denoted

$$\mathsf{SOL}(\varphi) := \varphi^{-1}(\{1\}) = \{x \in B\colon \varphi(x) = 1\} \subseteq \{-1, 1\}^n.$$

If $\mathcal{B}$ is a set of Boolean functions of n variables, then we will say that $\mathcal{B}$ is *consistent* if it is possible to satisfy all functions in $\mathcal{B}$ simultaneously, i.e. if there exists an $x \in \{-1, 1\}^n$ such that $\varphi(x) = 1$ for all $\varphi \in \mathcal{B}$. If we define a new Boolean function $\min(\mathcal{B}) : \{-1, 1\}^n \to \{-1, 1\}$ by

$$\min(\mathcal{B})(x) := \min_{\varphi \in \mathcal{B}} \varphi(x), \quad (x \in \{-1, 1\}^n), \tag{B.3.1}$$

then $\mathcal{B}$ is consistent if and only if $\min(\mathcal{B}) \in \mathsf{SAT}$.

B.3.2 Literals and fixing variables

A function $l : \{-1, 1\}^n \to \{-1, 1\}$ is called a *literal* if, for some $v \in [n]$,

$$l(x) = x_v \text{ for all } x, \quad \text{or} \quad l(x) = -x_v \text{ for all } x.$$

Each literal (of n variables) corresponds to an element of $\pm[n]$ in the following way: the literal $x \mapsto x_v$ corresponds to v and $x \mapsto -x_v$ corresponds to $-v$. This correspondence is bijective since taking an element $l \in \pm[n]$ to the literal $x \mapsto \operatorname{sgn}(l)x_{|l|}$ is the inverse operation. Thus, the space of literals in n variables is identified with the set $\pm[n]$, and we shall use these two sets interchangeably in the following. So considering e.g. the number -5 as a literal, we have $-5(x) = -x_5$.

Notice that a literal l is satisfied at x (i.e. $l(x) = 1$) exactly when $x_{|l|} = \operatorname{sgn}(l)$. It follows for a set of literals $\mathcal{L} \subseteq \pm[n]$ that, for all $x \in \{-1, 1\}^n$,

$$l(x) = 1 \text{ for all } l \in \mathcal{L} \iff x_{|l|} = \operatorname{sgn}(l) \text{ for all } l \in \mathcal{L},$$

and hence that $\mathcal{L}$ is consistent if and only if either $v \notin \mathcal{L}$ or $-v \notin \mathcal{L}$ for every $v \in [n]$, or equivalently if at most one of v and $-v$ is a member of $\mathcal{L}$ for every $v \in [n]$. We see from this that for a consistent set of literals $\mathcal{L}$, satisfying $\min(\mathcal{L})$ (at x) amounts to fixing certain of the variables x_v; more precisely fixing $x_{|l|}$ to $\operatorname{sgn}(l)$ for every $l \in \mathcal{L}$. Motivated by this we define for every consistent set of literals $\mathcal{L} \subseteq \pm[n]$ and every $v \in [n]$ the set

$$B_v(\mathcal{L}) := \begin{cases} \{1\}, & \text{if } v \in \mathcal{L}, \\ \{-1\}, & \text{if } -v \in \mathcal{L}, \\ \{-1,1\}, & \text{if } v, -v \notin \mathcal{L}, \end{cases} \quad \text{and we define} \quad B(\mathcal{L}) := \bigtimes_{v=1}^{n} B_v(\mathcal{L}). \tag{B.3.2}$$

Then we exactly get $\mathsf{SOL}(\min(\mathcal{L})) = B(\mathcal{L})$ by the preceding discussion (this identity will also hold for contradicting $\mathcal{L}$ if we extend the definition of $B_v(\mathcal{L})$ to $\emptyset$ when both $v, -v \in \mathcal{L}$). This again implies that for any Boolean function $\varphi : \{-1,1\}^n \to \{-1,1\}$ it holds that

$$\varphi \wedge \min(\mathcal{L}) \in \mathsf{SAT} \iff \varphi|_{B(\mathcal{L})} \in \mathsf{SAT},$$

where $\varphi|_{B(\mathcal{L})}$ is the restriction of φ to the set $B(\mathcal{L}) \subseteq \{-1,1\}^n$. Motivated by this, we define for any Boolean function $\varphi : \{-1,1\}^n \to \{-1,1\}$ and any consistent set of literals $\mathcal{L} \subseteq \pm[n]$,

$$\varphi_{\mathcal{L}} := \varphi|_{B(\mathcal{L})}. \tag{B.3.3}$$

Thus, $\varphi_{\mathcal{L}}$ is the function φ but with the variables dictated by $\mathcal{L}$ fixed. More generally we get for $\mathcal{L} \subseteq \pm[n]$ (not necessarily consistent) that

$$\varphi \wedge \min(\mathcal{L}) \in \mathsf{SAT} \iff \min(\mathcal{L}) \in \mathsf{SAT} \quad \text{and} \quad \varphi_{\mathcal{L}} \in \mathsf{SAT}. \tag{B.3.4}$$

Example B.7. *If $\varphi : \{-1,1\}^n \to \{-1,1\}$ ($n \geq 5$ for this example) is again any Boolean function, and $\mathcal{L} = \{1,-2,4\}$, we see that $\mathcal{L}$ is dictating $x_1 = 1$, $x_2 = -1$, and $x_4 = 1$, i.e.*

$$B(\mathcal{L}) = \{1\} \times \{-1\} \times \{-1,1\} \times \{1\} \times \{-1,1\}^{n-4},$$

giving us

$$\varphi_{\mathcal{L}}(x) = \varphi(1,-1,x_3,1,x_5,\dots,x_n), \quad (x \in B(\mathcal{L})).$$

B.3.3 Clauses and CNF formulas

A function $C : \{-1,1\}^n \to \{-1,1\}$ is called a *(disjunctive) clause* if there exist $k \in \mathbb{N}$ and literals $l_1, l_2, \dots, l_k \in \pm[n]$ such that

$$C(x) = l_1(x) \vee l_2(x) \vee \cdots \vee l_k(x) = \max_{i \in [k]} l_i(x), \quad (x \in \{-1,1\}^n).$$

The minimum such k is called the *length* of C, and we call C a k-clause. A 1-clause is just a literal and is also called a *unit clause*. Further, by convention we call the constant function $C \equiv -1$ a 0-clause, i.e. a clause that is always unsatisfied, and the constant function $C \equiv 1$ a $\star$-clause, i.e. a clause that is always satisfied.

If $C_1, C_2, \dots, C_m$ are clauses, then the function $\varphi : \{-1,1\}^n \to \{-1,1\}$ defined by

$$\varphi(x) = C_1(x) \wedge C_2(x) \wedge \cdots \wedge C_m(x) = \min_{j \in [m]} C_j(x), \quad (x \in \{-1,1\}^n), \tag{B.3.5}$$

is said to be a *CNF formula*, and the form in (B.3.5) is called a *CNF representation* for φ (CNF is short for *conjunctive normal form*). We allow $m = 0$ which by convention gives $\varphi := 1$. If each of the clauses $C_1, C_2, \dots, C_m$ has length k (ignoring any $\star$-clauses), then φ is called a k-CNF formula, and (B.3.5) is called a k-CNF representation.

A 1-CNF formula is just a conjunction/minimum of literals, and from any set of literals $\mathcal{L}$ it is of course possible to define a 1-CNF formula φ_1 by taking $\varphi_1 = \min(\mathcal{L})$ as defined in (B.3.1). This operation sends all sets with contradicting literals to the same 1-CNF formula (the constant function $x \mapsto -1$), but when restricted to the consistent sets of literals, it is one-to-one. Indeed, in this case $\mathsf{SOL}(\varphi_1) = B(\mathcal{L})$, and $B(\mathcal{L})$ determines $\mathcal{L}$. Thus, for any *satisfiable* 1-CNF formula ψ with corresponding set of literals $\mathcal{L}$ (i.e. $\psi = \min(\mathcal{L})$) we may and do write φ_ψ instead of $\varphi_{\mathcal{L}}$ for any $\varphi : \{-1,1\}^n \to \{-1,1\}$.

B.3.4 Fixing variables in CNF formulas

Consider first a 2-CNF formula

$$\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m,$$

each clause given by the disjunction of two literals: $C_j = l_{j,1} \vee l_{j,2}$, where $l_{j,i} \in \pm[n]$ for all $j \in [m]$ and $i = 1, 2$, and consider in addition a consistent set of literals $\mathcal{L} \subseteq \pm[n]$. In the formula $\varphi_{\mathcal{L}}$, each literal $l_{j,i}$ has a possibility of being fixed, and this happens exactly when $l_{j,i} \in \pm\mathcal{L}$. More precisely, if $l_{j,i} \in \mathcal{L}$, then $(l_{j,i})_{\mathcal{L}} \equiv 1$, and if $l_{j,i} \in -\mathcal{L}$, then $(l_{j,i})_{\mathcal{L}} \equiv -1$, and lastly if $l_{j,i} \notin \pm\mathcal{L}$, then $(l_{j,i})_{\mathcal{L}} = l_{j,i}$. This yields the following cases for $(C_j)_{\mathcal{L}}$ for each $j \in [m]$:

0. If both literals get fixed to -1, i.e. $l_{j,1}, l_{j,2} \in -\mathcal{L}$, then $(C_j)_{\mathcal{L}} \equiv -1$ can never be satisfied.

1. If one literal gets fixed to -1, say $l_{j,1} \in -\mathcal{L}$, but the other is not fixed, i.e. $l_{j,2} \notin \pm\mathcal{L}$, then $(C_j)_{\mathcal{L}} = -1 \vee l_{j,2} = l_{j,2}$, so $(C_j)_{\mathcal{L}}$ is the unit clause $l_{j,2}$. Similarly if $l_{j,2} \in -\mathcal{L}$ and $l_{j,1} \notin \pm\mathcal{L}$, then $(C_j)_{\mathcal{L}} = l_{j,1}$.

2. If no literal gets fixed, i.e. both $l_{j,1}, l_{j,2} \notin \pm\mathcal{L}$, then $(C_j)_{\mathcal{L}} = C_j$.

$\star$. If one or both literals gets fixed to 1, i.e. $l_{j,1} \in \mathcal{L}$ or $l_{j,2} \in \mathcal{L}$, then $(C_j)_{\mathcal{L}} \equiv 1$ is always satisfied.

We see that each of the clauses $(C_j)_{\mathcal{L}}$ either becomes unsatisfiable (case 0), is transformed to a unit clause (case 1), remains intact (case 2), or is immediately satisfied (case ★). Let for $h \in \{0,1,2,\star\}$

$$\mathcal{C}_h := \{j \in [m] \colon j \text{ is in case } h\}, \quad \text{and} \quad M_h := |\mathcal{C}_h|, \tag{B.3.6}$$

where we suppress the dependence on the $l_{j,i}$'s and $\mathcal{L}$ in the notation. That is, $\mathcal{C}_h$ consists of exactly those $j \in [m]$ where C_j becomes a h-clause when fixing the variables dictated by $\mathcal{L}$, i.e.

$$j \in \mathcal{C}_h \iff (C_j)_{\mathcal{L}} \text{ is a } h\text{-clause.}$$

We can now split $\varphi_{\mathcal{L}}$ into parts by defining for each $h \in \{0,1,2,\star\}$:

$$\varphi_h := \min_{j \in \mathcal{C}_h} (C_j)_{\mathcal{L}}, \tag{B.3.7}$$

where $\min \emptyset = 1$, so that φ_h is a h-CNF formula, and $\varphi_{\mathcal{L}} = \varphi_0 \wedge \varphi_1 \wedge \varphi_2$. Using the latter and (B.3.4), we find that

$$\varphi_{\mathcal{L}} \in \mathsf{SAT} \iff M_0 = 0, \quad \varphi_1 \in \mathsf{SAT}, \quad \text{and} \quad (\varphi_2)_{\varphi_1} \in \mathsf{SAT}. \tag{B.3.8}$$

This method of "splitting" $\varphi_{\mathcal{L}}$ into its 0-, 1-, and 2-CNF sub-formulas φ_0, φ_1, φ_2, along with the corresponding sets $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$, and in particular the sizes of these sets M_0, M_1, M_2, will play a major role in the proof of the main theorem of this paper.

Consider now a 3-CNF formula $\varphi = C_1 \wedge \cdots \wedge C_m$. By completely analogous considerations to the above, we see that each clause falls into one of of the following five cases when fixing the variables dictated by $\mathcal{L}$: becomes unsatisfiable (case 0), is transformed to a unit clause (case 1), is transformed to a binary clause (case 2), remains intact (case 3), or is immediately satisfied (case ★). Again we may define $\mathcal{C}_h$, φ_h, and M_h for $h \in \{0,1,2,3,\star\}$ as in (B.3.6) and (B.3.7), where then $\varphi_{\mathcal{L}} = \varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \varphi_3$, and we get that

$$\varphi_{\mathcal{L}} \in \mathsf{SAT} \iff M_0 = 0, \quad \varphi_1 \in \mathsf{SAT} \quad \text{and} \quad (\varphi_2 \wedge \varphi_3)_{\varphi_1} \in \mathsf{SAT}. \tag{B.3.9}$$

B.3.5 Random CNF formulas

A random k-CNF formula Φ with m clauses and n variables is obtained by sampling m i.i.d. random k-clauses $C_1, \ldots, C_m$ and taking their conjunction:

$$\Phi := C_1 \wedge \cdots \wedge C_m = \min_{j \in [m]} C_j.$$

Each of the C_j's is obtained by sampling $V_j = (V_{j,1}, \ldots, V_{j,k})$ uniformly at random among all sequences of k *pairwise distinct* variables from $[n]$, and then sampling fair random signs (i.e. equal to -1 or 1, each with probability 1/2) $S_j =$

$(S_{j,1}, \dots, S_{j,k})$ independently of V_j. This gives random literals $L_{j,i} := S_{j,i} V_{j,i}$ and the random k-clause

$$C_j := L_{j,1} \vee \cdots \vee L_{j,k} = \max_{i \in [k]} L_{j,i}.$$

If the lengths of the clauses $C_1, \dots, C_j$ are not all chosen to be equal, we say that Φ is a random *mixed* CNF formula.

B.4 The proof

B.4.1 Lemmas

In this section, we establish a few technical lemmas needed for the proof of Theorem B.2. We will first show that for a random k-CNF formula Φ and a consistent set of literals $\mathcal{L} \subseteq \pm[n]$, the probability that $\Phi_{\mathcal{L}} \in \mathsf{SAT}$ only depends on $\mathcal{L}$ through $|\mathcal{L}|$, the number of variables being fixed, and in a non-increasing way.

Lemma B.8. *Let Φ be a random (possibly mixed) CNF formula with m clauses and n variables, and let $\mathcal{L}, \mathcal{L}' \subseteq \pm[n]$ be two consistent sets of literals.*

(i) If $|\mathcal{L}| = |\mathcal{L}'|$, then $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT})$.

(ii) If $|\mathcal{L}| \geq |\mathcal{L}'|$, then $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT})$.

Proof. Let $L_{j,i} = S_{j,i} V_{j,i}$ for $j \in [m]$ and $i \in [k_j]$ be the literals defining Φ. Assume that $|\mathcal{L}| = |\mathcal{L}'|$ and let $\pi : [n] \to [n]$ be a permutation such that $\pi(\mathcal{L}_{\text{abs}}) = \mathcal{L}'_{\text{abs}}$. Define $\theta, \theta' : [n] \to \{-1, 1\}^n$ by putting

$$\theta(v) := \begin{cases} -1, & \text{if } -v \in \mathcal{L}, \\ 1, & \text{otherwise,} \end{cases} \quad \text{and similarly} \quad \theta'(v) := \begin{cases} -1, & \text{if } -v \in \mathcal{L}', \\ 1, & \text{otherwise.} \end{cases}$$

This definition is such that if $l \in \mathcal{L}$ then $\theta(|l|) = \operatorname{sgn}(l)$ and similarly for θ'. Now define

$$V'_{j,i} := \pi(V_{j,i}), \quad S'_{j,i} := S_{j,i}\theta(V_{j,i})\theta'(V'_{j,i}), \quad \text{and} \quad L'_{j,i} := S'_{j,i} V'_{j,i}$$

for all $j \in [m]$ and $i \in [k]$. Then by direct calculation we find that the random vectors $(L'_{j,i})_{j,i}$ and $(L_{j,i})_{j,i}$ have the same distribution, so Φ and Φ' have the same distribution, where Φ' is the random CNF formula defined from the random literals $L'_{j,i}$ for $j \in [m]$ and $i \in [k_j]$. This implies

$$\mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT}) = \mathbb{P}(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}).$$

We now show that

$$\Phi'_{\mathcal{L}'} \in \mathsf{SAT} \iff \Phi_{\mathcal{L}} \in \mathsf{SAT}.$$

This will follow from the fact that $(L_{j,i})_{\mathcal{L}}(x) = (L'_{j,i})_{\mathcal{L}'}(x')$ for all $j \in [m]$, $i \in [k]$, and $x \in \{-1,1\}^n$, where $x' \in \{-1,1\}^n$ is given by $x'_v = x_{\pi^{-1}(v)}$. There are two cases:

(1) If $V_{j,i} \notin \mathcal{L}_{\text{abs}}$, then $V'_{j,i} \notin \mathcal{L}'_{\text{abs}}$, and in this case $\theta(V_{j,i}) = \theta'(V'_{j,i}) = 1$, yielding

$$(L'_{j,i})_{\mathcal{L}'}(x') = S'_{j,i}x'_{V'_{j,i}} = S_{j,i}x_{\pi^{-1}(V'_{j,i})} = S_{j,i}x_{V_{j,i}} = (L_{j,i})_{\mathcal{L}}(x).$$

(2) If $V_{j,i} \in \mathcal{L}_{\text{abs}}$, then $V'_{j,i} \in \mathcal{L}'_{\text{abs}}$, and by construction we get $B_{V_{j,i}}(\mathcal{L}) = \{\theta(V_{j,i})\}$ and $B_{V'_{j,i}}(\mathcal{L}') = \{\theta'(V'_{j,i})\}$ (see (B.3.2)). This yields (see (B.3.3))

$$\begin{aligned}(L'_{j,i})_{\mathcal{L}'}(x') =& S'_{j,i}\theta'(V'_{j,i}) = S_{j,i}\theta(V_{j,i})\theta'(V'_{j,i})^2 \\ =& S_{j,i}\theta(V_{j,i}) = (L_{j,i})_{\mathcal{L}}(x).\end{aligned}$$

All together we find that

$$\mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT}) = \mathbb{P}(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}) = \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}),$$

proving (i).

Now for (ii), if $|\mathcal{L}| \geq |\mathcal{L}'|$, we consider an injection $\iota : \mathcal{L}' \to \mathcal{L}$. Then it is clear that $\Phi_{\mathcal{L}} \in \mathsf{SAT}$ implies $\Phi_{\iota(\mathcal{L}')} \in \mathsf{SAT}$ (since $\iota(\mathcal{L}') \subseteq \mathcal{L}$), and the result follows from (i) since $|\iota(\mathcal{L}')| = |\mathcal{L}'|$. □

The next lemma shows that adding more clauses to Φ only decreases the probability of satisfiability for $\Phi_{\mathcal{L}}$.

Lemma B.9. *Let Φ and Φ' be random (possibly mixed) CNF formulas with m_k resp. m'_k k-clauses for each k and n variables, and let $\mathcal{L} \subseteq \pm[n]$ be a consistent set of literals. If $m_k \geq m'_k$ for each k, then*

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \mathbb{P}(\Phi'_{\mathcal{L}} \in \mathsf{SAT}),$$

and in particular $\mathbb{P}(\Phi \in \mathsf{SAT}) \leq \mathbb{P}(\Phi' \in \mathsf{SAT})$.

Proof. The result follows from a straightforward coupling argument; let $C_j^{(k)}$ be independent random k-clauses for $j, k \in \mathbb{N}$ (also independent across different values of k), and define

$$\Psi := \min_{k \in \mathbb{N}} \min_{j \in [m_k]} C_j^{(k)}, \quad \text{and} \quad \Psi' := \min_{k \in \mathbb{N}} \min_{j \in [m'_k]} C_j^{(k)}.$$

Then Ψ has the same distribution as Φ and Ψ' has the same distribution as Φ', but it holds by construction that, for every $x \in \{-1,1\}^n$, if $\Psi(x) = 1$, then $\Psi'(x) = 1$, and thus also $\Psi_{\mathcal{L}}(x) = 1$ implies $\Psi'_{\mathcal{L}}(x) = 1$. This yields

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}(\Psi_{\mathcal{L}} \in \mathsf{SAT}) \leq \mathbb{P}(\Psi'_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}(\Phi'_{\mathcal{L}} \in \mathsf{SAT}).$$

The second assertion follows by taking $\mathcal{L} = \emptyset$. □

This next lemma describes the distribution of (Φ_0, Φ_1, Φ_2) and $(\Phi_0, \Phi_1, \Phi_2, \Phi_3)$, the 0-, 1-, 2-CNF (and 3-CNF) subformulas of $\Phi_{\mathcal{L}}$ defined in (B.3.7), when Φ is a random 2- or 3-CNF formula.

Lemma B.10. *Let $k = 2$ or $k = 3$ and let $K = \{0, 1, \dots, k, \star\}$. For $m, n \in \mathbb{N}$ and $f \in \mathbb{N}_0$ with $f < n$, let Φ be a random k-CNF formula with m clauses and n variables, and let $\mathcal{L} = [n] \setminus [n-f]$. Let $(\mathcal{C}_h)_{h\in K}$, $(M_h)_{h\in K}$, and $(\Phi_h)_{h\in K}$ be as defined in* (B.3.6) *and* (B.3.7)*, so in particular $\Phi_{\mathcal{L}} = \Phi_0 \wedge \cdots \wedge \Phi_k$.*

Then $(M_h)_{h\in K} \sim \text{Multinomial}(m, (p_h)_{h\in K})$, and in the conditional distribution given $(\mathcal{C}_h)_{h\in K}$, it holds that the Φ_h's are independent and that Φ_h is a random h-CNF formula with M_h clauses and $n - f$ variables for all $h \in K$. Furthermore, if $k = 2$, then

$$p_0 = \frac{f(f-1)}{4n(n-1)}, \quad p_1 = \frac{f(n-f)}{n(n-1)}, \quad p_2 = \frac{(n-f)(n-f-1)}{n(n-1)},$$

and if $k = 3$, then

$$p_0 = \frac{f(f-1)(f-2)}{8n(n-1)(n-2)}, \qquad p_1 = \frac{3f(f-1)(n-f)}{4n(n-1)(n-2)},$$
$$p_2 = \frac{3f(n-f)(n-f-1)}{2n(n-1)(n-2)}, \qquad p_3 = \frac{(n-f)(n-f-1)(n-f-2)}{n(n-1)(n-2)}.$$

Proof. Assume initially that $k = 2$ and let $L = (L_{j,i})_{j\in[m], i\in[2]}$ be the random literals defining Φ. Notice that $[n] \setminus \mathcal{L} = [n-f]$, and define the sets

$$A_0 := -\mathcal{L} \times -\mathcal{L}, \quad A_1 := (-\mathcal{L} \times \pm[n-f]) \cup (\pm[n-f] \times -\mathcal{L}),$$
$$A_2 := \pm[n-f] \times \pm[n-f], \quad A_\star := (\mathcal{L} \times \pm[n]) \cup (\pm[n] \times \mathcal{L}).$$

Notice for each $h \in K$ that

$$\mathcal{C}_h = \Big\{ j \in [m] \colon (L_{j,1}, L_{j,2}) \in A_h \Big\},$$

where the sets $\mathcal{C}_h$ are those defined in (B.3.6), and let $M_h = |\mathcal{C}_h|$ for $h \in K$. Since $(A_h)_{h\in K}$ is a partition of $\pm[n] \times \pm[n]$, it is clear that $(M_h)_{h\in K}$ follows a multinomial distribution. Now,

$$p_h = \frac{1}{m} \mathbb{E}[M_h] = \frac{1}{m} \mathbb{E}\left[\sum_{j=1}^{m} 1_{\{(L_{j,1}, L_{j,2}) \in A_h\}} \right] = \mathbb{P}\Big((L_{1,1}, L_{1,2}) \in A_h \Big).$$

From the known distribution of the random literals $(L_{1,1}, L_{1,2})$, we find by direct calculations the values of p_0, p_1, p_2 stipulated.

Put $\mathcal{C} := (\mathcal{C}_h)_{h\in K}$. For any $l_{j,i} \in \pm[n]$, $j \in [m]$ and $i = 1, 2$, we immediately find by independence of the $(L_{j,1}, L_{j,2})$ pairs that

$$\begin{aligned} &\mathbb{P}\Big(L = (l_{j,i})_{j\in[m], i\in[2]} \,\Big|\, \mathcal{C} \Big) \\ &= \prod_{h\in K} \prod_{j\in\mathcal{C}_h} \mathbb{P}\Big((L_{j,1}, L_{j,2}) = (l_{j,1}, l_{j,2}) \,\Big|\, (L_{j,1}, L_{j,2}) \in A_h \Big), \end{aligned}$$

so the pairs $(L_{j,1}, L_{j,2})$ for $j \in [m]$ are conditionally independent given $\mathcal{C}$. We further find by direct calculation that for $j \in \mathcal{C}_2$ and $(l_{j,1}, l_{j,2}) \in A_2$ with $|l_{j,1}| \neq |l_{j,2}|$,

$$\begin{aligned} &\mathbb{P}\Big((L_{j,1}, L_{j,2}) = (l_{j,1}, l_{j,2}) \,\Big|\, (L_{j,1}, L_{j,2}) \in A_2\Big) \\ =&\frac{1}{4n(n-1)p_2} \\ =&\frac{1}{4(n-f)(n-f-1)}, \end{aligned}$$

showing that $(L_{j,1}, L_{j,2})$ is uniformly distributed over all pairs of strictly distinct literals from $\pm[n-f]$ given $\mathcal{C}$. Also, $(L_{j,1}, L_{j,2}) \in A_2$ is "case 2" described above (B.3.6), so $(L_{j,i})_{\mathcal{L}} = L_{j,i}$ for $i = 1, 2$ almost surely given $\mathcal{C}$. Recalling that

$$\Phi_h(x) = \min_{j \in \mathcal{C}_h}\Big((L_{j,1})_{\mathcal{L}}(x) \vee (L_{j,2})_{\mathcal{L}}(x)\Big), \quad (x \in \{-1, 1\}^n),$$

for $h = 0, 1, 2$, it follows that in the conditional distribution given $\mathcal{C}$, Φ_2 is indeed a random 2-CNF formula (defined from the random literals $(L_{j,i})_{j \in \mathcal{C}_2, i \in [2]}$). An analogous argument shows that given $\mathcal{C}$, Φ_1 is a random 1-CNF formula. By independence of the $(L_{j,1}, L_{j,2})$ pairs in the conditional distribution, Φ_0, Φ_1 and Φ_2 are independent given $\mathcal{C}$.

Completely analogous considerations establish the result for $k = 3$. □

The final lemma in this section concerns the amount of duplicate literals in a random 1-CNF formula. We show that there are loosely speaking very few duplicates if the number of clauses/literals is proportional to the square root of the number of variables.

Lemma B.11. *Let $n \in \mathbb{N}$ and $f = f(n)$ be such that $f/\sqrt{n} \to \beta$, where $\beta \in [0, \infty)$. Consider i.i.d. random literals $L_1, L_2, \ldots, L_f$ uniformly distributed on $\pm[n]$. Put $\mathcal{L} := \{L_1, \ldots, L_f\}$. Then*

$$\mathbb{P}\Big(|\mathcal{L}| < f - w\Big) \leq \frac{4\beta^2}{w}$$

for all $w = w(n)$ when n is large enough.

Proof. Let $V_j := |L_j|$ for each $j \in [f]$, so that $\mathcal{L}_{\text{abs}} = \{V_1, \ldots, V_f\}$. Define for each $v \in [n]$

$$N_v := \Big|\Big\{j \in [f] \colon V_j = v\Big\}\Big|.$$

Then $(N_1, \ldots, N_n) \sim \text{Multinomial}(f, (1/n, \ldots, 1/n))$, and we see that

$$|\mathcal{L}_{\text{abs}}| = f - \sum_{v \in [n]} (N_v - 1) \mathbb{1}_{\{N_v \geq 2\}}.$$

We split the sum as follows:

$$\sum_{v\in[n]}(N_v-1)\mathbb{1}_{\{N_v\geq 2\}} = \sum_{v\in[n]}(N_v-1)\mathbb{1}_{\{N_v\geq 3\}} + \sum_{v\in[n]}\mathbb{1}_{\{N_v=2\}}.$$

Cauchy-Schwarz yields

$$\mathbb{E}[(N_v-1)\mathbb{1}_{\{N_v\geq 3\}}] \leq \mathbb{E}[N_v\mathbb{1}_{\{N_v\geq 3\}}] \leq \mathbb{E}[N_v^2]^{1/2}\,\mathbb{P}(N_v\geq 3)^{1/2},$$

where

$$\mathbb{E}[N_v^2] = \frac{f(f-1)}{n^2} + \frac{f}{n} \leq \frac{f^2}{n^2} + \frac{f}{n} \leq 2\frac{f}{n},$$

where we in the end use that $f/n \to 0$ as $n \to \infty$, so $f/n \leq 1$ when n is large enough, and thus $\mathbb{E}[N_v^2]^{1/2} \leq \sqrt{2f}/\sqrt{n}$ when n is large enough. For the second factor we notice that $N_v \geq 3$ if and only if there exists $j_1 < j_2 < j_3$ such that $V_{j_1} = V_{j_2} = V_{j_3} = v$, so that

$$\mathbb{P}(N_v \geq 3) = \sum_{j_1<j_2<j_3} \mathbb{P}(V_{j_1} = V_{j_2} = V_{j_3} = v) = \binom{f}{3}\frac{1}{n^3} \leq \frac{f^3}{n^3},$$

since the $V_1,\dots,V_f$ are i.i.d. uniformly distributed on $[n]$. We note for later that, in particular,

$$\begin{aligned}&\mathbb{P}(N_v \geq 3 \text{ for some } v\in[n])\\ &\leq \sum_{v\in[n]}\mathbb{P}(N_v\geq 3) \leq \frac{f^3}{n^2}\\ &= \left(\frac{f}{\sqrt{n}}\right)^3\frac{1}{\sqrt{n}} \longrightarrow 0\end{aligned} \tag{B.4.1}$$

as $n \to \infty$, so that $N_v \leq 2$ for all $v \in [n]$ w.h.p. Together this shows that

$$\sum_{v\in[n]}\mathbb{E}[(N_v-1)\mathbb{1}_{\{N_v\geq 3\}}] \leq \sqrt{2}\frac{f^2}{n} = \sqrt{2}\left(\frac{f}{\sqrt{n}}\right)^2 \longrightarrow \sqrt{2}\beta^2 \quad \text{as } n\to\infty,$$

so this sum is smaller than $2\beta^2$ when n is large enough. For the other sum we note that, as before, $N_v \geq 2$ if and only if there exists $j_1 < j_2$ such that $V_{j_1} = V_{j_2} = v$, so by a similar argument,

$$\mathbb{E}\left[\sum_{v\in[n]}\mathbb{1}_{\{N_v=2\}}\right] = \sum_{v\in[n]}\mathbb{P}(N_v\geq 2) \leq \frac{f^2}{n} = \left(\frac{f}{\sqrt{n}}\right)^2 \longrightarrow \beta^2 \quad \text{as } n\to\infty,$$

so this sum is also smaller than $2\beta^2$ when n is large enough. Taken together:

$$\mathbb{E}\left[\sum_{v\in[n]}(N_v-1)\mathbb{1}_{\{N_v\geq 2\}}\right] \leq 4\beta^2$$

when n is large enough, and thus by Markov's inequality:

$$\mathbb{P}\Big(|\mathcal{L}_{\mathrm{abs}}| < f - w\Big) = \mathbb{P}\Bigg(\sum_{v\in[n]} (N_v - 1)\mathbb{1}_{\{N_v\geq 2\}} > w\Bigg) \leq \frac{4\beta^2}{w}$$

when n is large enough. As $|\mathcal{L}| \geq |\mathcal{L}_{\mathrm{abs}}|$, we are done. □

B.4.2 Special cases

We need to prove two special cases of our main result, which we will need for the proof itself. The characterization of the random 1-SAT problem (B.1.4) is the first special case which shall actually play an important role in the proof of Theorem B.2.

Lemma B.12 (The random 1-SAT problem). *For $\beta \in [0,\infty]$, let Φ_1 be a random 1-CNF formula with $f = f(n)$ clauses and n variables, where $n \to \infty$ and $f/\sqrt{n} \to \beta$. Then*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_1 \in \mathsf{SAT}) = e^{-(\beta/2)^2}.$$

Proof. Assume initially that $\beta < \infty$. Let the random literals corresponding to Φ_1 be $L_1, L_2, \ldots, L_f$, where $S_j = \mathrm{sgn}(L_j)$ and $V_j = |L_j|$. For each $v \in [n]$ we put

$$N_v := \Big|\Big\{j \in [f]\colon\ V_j = v\Big\}\Big|.$$

Then $N := (N_1, \ldots, N_n) \sim \mathrm{Multinomial}(f, (1/n, \ldots, 1/n))$. From (B.4.1) we have that $N_v \leq 2$ for all $v \in [n]$ w.h.p., so when writing

$$\begin{aligned}\mathbb{P}(\Phi_1 \in \mathsf{SAT}) = {}&\mathbb{P}(\Phi_1 \in \mathsf{SAT}, N_v \geq 3 \text{ for some } v \in [n]) \\ &+ \mathbb{P}(\Phi_1 \in \mathsf{SAT}, N_v \leq 2 \text{ for all } v \in [n]),\end{aligned}$$

we see that the first term vanishes as $n \to \infty$, and in regards to the second term we have:

$$\{N_v \leq 2 \text{ for all } v \in [n]\} = \bigcup_{\substack{\eta\in\{0,1,2\}^n\colon\\ \eta_1+\cdots+\eta_n = f}} \{N = \eta\} = \bigcup_{h=0}^{\lfloor f/2\rfloor} \bigcup_{\eta\in H_h} \{N = \eta\},$$

where

$$H_h := \Big\{\eta \in \{0,1,2\}^n\colon\ \eta_1 + \cdots + \eta_n = f, |\{v \in [n]\colon\ \eta_v = 2\}| = h\Big\},$$

i.e. we have divided the union into sub-unions depending on how many entries of η are equal to 2, so that $\eta \in H_h$ when there are h entries of η equal to 2. Since the events on the right-hand side are disjoint, we may write

$$\mathbb{P}(\Phi_1 \in \mathsf{SAT}, N_v \leq 2 \text{ for all } v \in [n]) = \sum_{h=0}^{\lfloor f/2\rfloor} \sum_{\eta\in H_h} \mathbb{P}(\Phi_1 \in \mathsf{SAT}, N = \eta). \qquad \text{(B.4.2)}$$

Notice that $|H_h| = \binom{n-h}{f-2h}\binom{n}{h}$, corresponding to firstly choosing h entries of η to equal 2 and then choosing $f-2h$ of the remaining $n-h$ entries to equal 1 (the remaining entries will equal 0).

Now, for fixed $h \in \{0, 1, \ldots, \lfloor f/2 \rfloor\}$ and $\eta \in H_h$ we find by definition of N that $N = \eta$ if and only if $(V_1, \ldots, V_f) = \underline{v}$ for some $\underline{v} \in [n]^f$ satisfying $|\{j \in [f] : \underline{v}_j = v\}| = \eta_v$ for all $v \in [n]$. Hence,

$$\mathbb{P}(\Phi_1 \in \mathsf{SAT}, N = \eta) = \sum_{\substack{\underline{v} \in [n]^f : \\ |\{j \in [f] : \underline{v}_j = v\}| = \eta_v \\ \text{for all } v \in [n]}} \mathbb{P}(\Phi_1 \in \mathsf{SAT}, V = \underline{v}), \tag{B.4.3}$$

where $V := (V_1, \ldots, V_f)$. Notice now that $\Phi_1 \in \mathsf{SAT}$ if and only if there are no contradictions in the literals $L_1, \ldots, L_f$, i.e. we don't have $L_{j_1} = -L_{j_2}$ for any $j_1 < j_2$, which is to say that $\Phi_1 \in \mathsf{SAT}$ if and only if $V_{j_1} = V_{j_2}$ implies $S_{j_1} = S_{j_2}$. But since V and $S := (S_1, \ldots, S_f)$ are independent, we find that:

$$\begin{aligned}\mathbb{P}(\Phi_1 \in \mathsf{SAT}, V = \underline{v}) &= \mathbb{P}(S_{j_1} = S_{j_2} \text{ for all } j_1 < j_2 \text{ with } \underline{v}_{j_1} = \underline{v}_{j_2})\,\mathbb{P}(V = \underline{v}) \\ &= 2^{-h}\,\mathbb{P}(V = \underline{v}),\end{aligned}$$

since there are exactly h pairs (j_1, j_2) satisfying $j_1 < j_2$ and $\underline{v}_{j_1} = \underline{v}_{j_2}$ by choice of η. Inserting this into (B.4.3) and using the known distribution of N together with the fact that exactly h entries of η are 2 and the rest are 1 or 0, we get:

$$\mathbb{P}(\Phi_1 \in \mathsf{SAT}, N = \eta) = 2^{-h}\,\mathbb{P}(N = \eta) = \frac{f!}{4^h n^f},$$

and inserting this further into (B.4.2) yields:

$$\mathbb{P}(\Phi_1 \in \mathsf{SAT}, N_v \leq 2 \text{ for all } v \in [n]) = \sum_{h=0}^{\lfloor f/2 \rfloor} \binom{n-h}{f-2h}\binom{n}{h}\frac{f!}{4^h n^f} \tag{B.4.4}$$

$$= \sum_{h=0}^{\infty}\left(\prod_{i=0}^{2h-1}\frac{f-i}{\sqrt{n}}\right)\left(\prod_{i=0}^{f-h-1}\frac{n-i}{n}\right)\frac{1}{4^h h!}\mathbb{1}_{[0,\lfloor f/2 \rfloor]}(h), \tag{B.4.5}$$

where we in the second equality simply have rearranged the factors in each term. For fixed h we see that

$$\lim_{n\to\infty}\prod_{i=0}^{2h-1}\frac{f-i}{\sqrt{n}} = \prod_{i=0}^{2h-1}\lim_{n\to\infty}\left(\frac{f}{\sqrt{n}} - \frac{i}{\sqrt{n}}\right) = \beta^{2h},$$

and also for large enough n (independent of h) we have $f/\sqrt{n} \leq \beta + 1$, so:

$$\prod_{i=0}^{2h-1}\frac{f-i}{\sqrt{n}} \leq (\beta+1)^{2h}. \tag{B.4.6}$$

In regards to the other product we use that $\log(1+t)/t \to 1$ as $t \to 0$, so that for any $\varepsilon \in (0,1)$ we have $(1-\epsilon)t \le \log(1+t) \le (1+\epsilon)t$ whenever t is close enough to 0. This yields

$$(1-\epsilon)\sum_{i=0}^{f-h-1} \frac{-i}{n} \le \sum_{i=0}^{f-h-1} \log\left(1-\tfrac{i}{n}\right) \le (1+\epsilon)\sum_{i=0}^{f-h-1} \frac{-i}{n}$$

whenever n is large enough, and since

$$\sum_{i=0}^{f-h-1} \frac{-i}{n} = \frac{-1}{2}\cdot\frac{f-h-1}{\sqrt{n}}\cdot\frac{f-h}{\sqrt{n}} \longrightarrow \frac{-\beta^2}{2} \quad \text{as } n\to\infty,$$

we get by taking $\epsilon \to 0$ that

$$\lim_{n\to\infty}\prod_{i=0}^{f-h-1}\frac{n-i}{n} = \lim_{n\to\infty}\exp\left[\sum_{i=0}^{f-h-1}\log\left(1-\tfrac{i}{n}\right)\right] = e^{-\frac{1}{2}\beta^2}.$$

Of course, we also have for all $n \in \mathbb{N}$

$$\prod_{i=0}^{f-h-1}\frac{n-i}{n} \le 1. \tag{B.4.7}$$

Thus, by (B.4.6) and (B.4.7), the h'th term in (B.4.5) is bounded by $(\beta+1)^{2h}/(4^h h!)$ when n is large enough (independent of h), so by appealing to dominated convergence we get

$$\lim_{n\to\infty}\mathbb{P}(\Phi_1 \in \mathsf{SAT}) = e^{-\frac{1}{2}\beta^2}\sum_{h=0}^{\infty}\frac{\beta^{2h}}{4^h h!} = e^{-\frac{1}{4}\beta^2},$$

as claimed.

Now, if $\beta = \infty$, we consider for an arbitrary $T > 0$ a 1-CNF formula Ψ_1 with $\lfloor T\sqrt{n}\rfloor$ clauses and n variables. Since $f/\sqrt{n} \to \infty$ as $n \to \infty$, we have for large enough n that $f \ge \lfloor T\sqrt{n}\rfloor$, so for such large n we also have by Lemma B.9

$$\mathbb{P}(\Phi_1 \in \mathsf{SAT}) \le \mathbb{P}(\Psi_1 \in \mathsf{SAT}),$$

and $\mathbb{P}(\Psi \in \mathsf{SAT}) \to e^{-(T/2)^2}$ as $n \to \infty$ by what we have proved thus far. Taking then $T \to \infty$ yields

$$\lim_{n\to\infty}\mathbb{P}(\Phi_1 \in \mathsf{SAT}) = 0$$

as desired. □

The second special case which we need to prove separately is the subcritical case $\beta = 0$ in Theorem B.2 case $k = 2$. To prove this, we employ a new variation of the classical "snakes and snares" proof of the sharp satisfiability threshold in the random 2-SAT problem. In this variation, we show that a 2-CNF formula that has its satisfiability spoiled by fixing some amount of variables must contain a "cobra", which we define shortly. We then show that the mean number of cobras in a random 2-CNF formula vanishes if we fix asymptotically fewer variables than the square root of the total number of variables, i.e. if $\beta = 0$.

Let $m, n, N \in \mathbb{N}$ and $\mathcal{L} \subseteq \pm[n]$ be a set of literals. Then an *$\mathcal{L}$-cobra* (of size N) is a sequence $l_0, l_1, \dots, l_N \in \pm[n]$ of literals such that

(c1) The variables $|l_0|, |l_1|, \dots, |l_{N-1}|$ are pairwise distinct,

(c2) $|l_0| \in \mathcal{L}_{\text{abs}}$,

(c3) $|l_N| \in \mathcal{L}_{\text{abs}} \cup \{|l_0|, |l_1|, \dots, |l_{N-1}|\}$.

Let φ be a (non-random) 2-CNF formula with n variables and m clauses of the form $\ell_{j,1} \vee \ell_{j,2}$, $j \in [m]$. We say that φ *contains* the sequence $(l_0, l_1, \dots, l_N)$ if there for all $t \in [N]$ exists some $j \in [m]$ such that $\{-l_{t-1}, l_t\} = \{\ell_{j,1}, \ell_{j,2}\}$.

Lemma B.13. *For $\alpha \in [0,1)$, let Φ be a random 2-CNF formula with $m = m(n)$ clauses and n variables, where $n \to \infty$ and $m/n \to \alpha$, and let $\mathcal{L} \subseteq \pm[n]$ be a consistent set of literals with $|\mathcal{L}| = f = f(n)$, where $f/\sqrt{n} \to 0$ as $n \to \infty$. Then it holds that*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 1.$$

Proof. Let $(L_{j,i})_{j\in[m],i\in[2]}$ denote the random literals defining Φ, and let $C_1, C_2, \dots, C_m$ denote the random clauses of Φ, i.e. $C_j = L_{j,1} \vee L_{j,2}$, and let $\mathcal{C}_k^{(1)}$, and $M_k^{(1)}$ denote the random set and variable defined in (B.3.6) for each $k \in \{0, 1, 2, \star\}$. Define the corresponding random CNF formulas (cf. (B.3.7))

$$\Phi_1^{(1)} := \min_{j\in\mathcal{C}_1^{(1)}} (C_j)_{\mathcal{L}}, \quad \text{and} \quad \Phi_2^{(1)} := \min_{j\in\mathcal{C}_2^{(1)}} (C_j)_{\mathcal{L}} = \min_{j\in\mathcal{C}_2^{(1)}} C_j.$$

Define also $\mathcal{L}^{(1)} := \left\{(C_j)_{\mathcal{L}} \colon j \in \mathcal{C}_1^{(1)}\right\}$, the set of random literals in $\Phi_1^{(1)}$, i.e. $\Phi_1^{(1)} = \min(\mathcal{L}^{(1)})$. Then by (B.3.8),

$$\Phi_{\mathcal{L}} \in \mathsf{SAT} \iff M_0^{(1)} = 0, \quad \Phi_1^{(1)} \in \mathsf{SAT}, \quad \text{and} \quad (\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}.$$

We now repeat this with $(\Phi_2^{(1)})_{\mathcal{L}^{(1)}}$ in place of $\Phi_{\mathcal{L}}$, giving us for each $r \in \mathbb{N}$ sets and variables $\mathcal{C}_k^{(r)}, M_k^{(r)}$ for $k \in \{0, 1, 2, \star\}$ stemming from $(\Phi_2^{(r-1)})_{\mathcal{L}^{(r-1)}}$, and random CNF formulas

$$\Phi_1^{(r)} := \min_{j\in\mathcal{C}_1^{(r)}} (C_j)_{\mathcal{L}^{(r-1)}}, \quad \text{and} \quad \Phi_2^{(r)} := \min_{j\in\mathcal{C}_2^{(r)}} (C_j)_{\mathcal{L}^{(r-1)}} = \min_{j\in\mathcal{C}_2^{(r)}} C_j,$$

and we finally also define $\mathcal{L}^{(r)} := \left\{(C_j)_{\mathcal{L}^{(r-1)}} : j \in \mathcal{C}_1^{(r)}\right\}$ so that $\Phi_1^{(r)} = \min(\mathcal{L}^{(r)})$. We here take $\Phi^{(0)} := \Phi$ and $\mathcal{L}^{(0)} := \mathcal{L}$. Now, notice that

$$\mathcal{C}_2^{(r)} = \bigcup_{k \in \{0,1,2,\star\}} \mathcal{C}_k^{(r+1)}$$

for each $r \in \mathbb{N}$, and of course the sets $\mathcal{C}_0^{(r)}, \mathcal{C}_1^{(r)}, \mathcal{C}_2^{(r)}, \mathcal{C}_\star^{(r)}$ are pairwise disjoint. In particular, $M_2^{(1)}, M_2^{(2)}, M_2^{(3)}, \ldots$ is a decreasing sequence, and thus it must at some point become constant, i.e. there exists an $R \in \mathbb{N}$ such that $M_2^{(r)} = M_2^{(r+1)}$ for all $r \geq R$ (this happens precisely the first time $M_1^{(r)} = 0$, but this is irrelevant). In particular we get for $r \geq R$ that $\Phi_2^{(r)} = \Phi_2^{(r+1)}$ and $M_k^{(r+1)} = 0$ for $k \in \{0, 1, \star\}$, and thus also $\mathcal{L}^{(r+1)} = \emptyset$. We are thus able to define

$$\Phi_2^{(\infty)}(x) := \lim_{r\to\infty} \Phi_2^{(r)}(x) = \min\left\{C_j(x) : j \in \bigcap_{r\in\mathbb{N}} \mathcal{C}_2^{(r)}\right\}, \quad (x \in \{-1,1\}^n),$$

which we immediately see has the property $\Phi_2^{(\infty)}(x) \geq \Phi(x)$ for all x, so $\Phi \in \mathsf{SAT}$ implies $\Phi_2^{(\infty)} \in \mathsf{SAT}$. Further, we see that when $r > R$,

$$(\Phi_2^{(r)})_{\mathcal{L}^{(r)}} = (\Phi_2^{(\infty)})_\emptyset = \Phi_2^{(\infty)},$$

so using (B.3.8) iteratively on $(\Phi_2^{(r)})_{\mathcal{L}^{(r)}}$ for each $r \in \mathbb{N}$ yields

$$\Phi_{\mathcal{L}} \in \mathsf{SAT} \iff M_0^{(r)} = 0 \text{ and } \Phi_1^{(r)} \in \mathsf{SAT} \text{ for all } r \in \mathbb{N}, \text{ and } \Phi_2^{(\infty)} \in \mathsf{SAT}.$$

Now define the event

$$F := \bigcup_{r\in\mathbb{N}} \left(\left\{M_0^{(r)} > 0\right\} \cup \left\{\Phi_1^{(r)} \notin \mathsf{SAT}\right\}\right),$$

so that, by the above,

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}\left(F^c \cap \{\Phi_2^{(\infty)} \in \mathsf{SAT}\}\right). \tag{B.4.8}$$

Since Φ is satisfiable w.h.p. [CR92; Goe96b], so is $\Phi_2^{(\infty)}$, and it thus only remains to prove that F^c also occurs w.h.p., which is the same as proving that $\mathbb{P}(F) \to 0$ as $n \to \infty$.

We first prove that, if F occurs, then Φ contains an $\mathcal{L}$-cobra. We introduce the "flipping" map $\rho : [2] \to [2]$ given by

$$\rho(i) = 3 - i = \begin{cases} 2, & \text{if } i = 1, \\ 1, & \text{if } i = 2, \end{cases} \quad (i \in [2]),$$

so that for any $j \in [m]$ and $i \in [2]$ we have $C_j = L_{j,i} \vee L_{j,\rho(i)}$. Assume then that F occurs, meaning there exists an $r \in \mathbb{N}$ such that $M_0^{(r)} > 0$ or $\Phi_1^{(r)} \notin \mathsf{SAT}$. Let N' be the smallest such r.

Assume first that $\Phi_1^{(N')} \notin \mathsf{SAT}$. This means that there exists two clauses C_j and $C_{j'}$, which at "timepoint" $N'-1$ are still 2-clauses, but when fixing the variables dictated by $\mathcal{L}^{(N'-1)}$, they each become 1-clauses that contradict each other. That is to say, there exists $j(1), j'(1) \in [m]$ and $i(1), i'(1) \in [2]$ such that

$$L_{j(1),i(1)} = -L_{j'(1),i'(1)}, \quad \text{and} \quad -L_{j(1),\rho(i(1))}, -L_{j'(1),\rho(i'(1))} \in \mathcal{L}^{(N'-1)}. \tag{B.4.9}$$

Now, $-L_{j(1),\rho(i(1))}$ being an element in $\mathcal{L}^{(N'-1)}$ means that there exists $j(2) \in [m]$ and $i(2) \in [2]$ such that

$$-L_{j(1),\rho(i(1))} = L_{j(2),i(2)}, \quad \text{and} \quad -L_{j(2),\rho(i(2))} \in \mathcal{L}^{(N'-2)}.$$

We continue this recursively, giving sequences $j(1), j(2), \dots, j(N') \in [m]$ and $i(1), i(2), \dots, i(N') \in [2]$ such that

$$-L_{j(t),\rho(i(t))} = L_{j(t+1),i(t+1)}, \quad \text{and} \quad -L_{j(t+1),\rho(i(t+1))} \in \mathcal{L}^{(N'-(t+1))} \tag{B.4.10}$$

for all $t \in [N'-1]$. In the same way we also get sequences $j'(1), j'(2), \dots, j'(N') \in [m]$ and $i'(1), i'(2), \dots, i'(N') \in [2]$ such that

$$-L_{j'(t),\rho(i'(t))} = L_{j'(t+1),i'(t+1)}, \quad \text{and} \quad -L_{j'(t+1),\rho(i'(t+1))} \in \mathcal{L}^{(N'-(t+1))} \tag{B.4.11}$$

for all $t \in [N'-1]$. We now define for each $t \in \{0, 1, \dots, N'-1\}$:

$$l_t := -L_{j(N'-t),\rho(i(N'-t))}.$$

Then $l_0 = -L_{j(N'),\rho(i(N'))} \in \mathcal{L}^{(0)} = \mathcal{L}$ by (B.4.10), so condition (c2) in the definition of an $\mathcal{L}$-cobra is satisfied. Now define further for $t \in \{0, 1, \dots, N'-1\}$:

$$l_{N'+t} := -L_{j'(t+1),i'(t+1)}.$$

We now verify that the sequence $(l_0, l_1, \dots, l_{2N'-1})$ is "contained" in Φ in the sense defined above the formulation of Lemma B.13. For $t \in [N'-1]$ we have

$$\begin{aligned}(-l_{t-1}, l_t) &= \left(L_{j(N'-t+1),\rho(i(N'-t+1))}, -L_{j(N'-t),\rho(i(N'-t))}\right) \\ &= \left(L_{j(N'-t+1),\rho(i(N'-t+1))}, L_{j(N'-t+1),i(N'-t+1)}\right),\end{aligned}$$

using (B.4.10) in the second equality, as desired. From (B.4.9) we get

$$(-l_{N'-1}, l_{N'}) = \left(L_{j(1),\rho(i(1))}, -L_{j'(1),i'(1)}\right) = \left(L_{j(1),\rho(i(1))}, L_{j(1),i(1)}\right),$$

and lastly for $t \in [N'-1]$:

$$(-l_{N'+t-1}, l_{N'+t}) = \Big(L_{j'(t),i'(t)}, -L_{j'(t+1),i'(t+1)}\Big) = \Big(L_{j'(t),i'(t)}, L_{j'(t),\rho(i'(t))}\Big),$$

using this time (B.4.11). Hence, $(l_0, l_1, \dots, l_{2N'-1})$ is contained in Φ. Now, if there exists a $t \in [2N'-1]$ such that $|l_t| \in \{|l_0|, |l_1|, \dots, |l_{t-1}|\}$, then let N be the smallest such t. Then $(l_0, l_1, \dots, l_N)$ is clearly an $\mathcal{L}$-cobra contained in Φ as desired. If not, then the variables $|l_0|, |l_1|, \dots, |l_{2N'-1}|$ are pairwise distinct, and we take $N := 2N'$ and define finally

$$l_N := L_{j'(N'),\rho(i'(N'))}.$$

It follows immediately from (B.4.11) that $-l_N \in \mathcal{L}^{(0)} = \mathcal{L}$, so of course $|l_N| \in \mathcal{L}_{\text{abs}}$, and the sequence $(l_0, l_1, \dots, l_N)$ is thus an $\mathcal{L}$-cobra. It is also contained in Φ since

$$(-l_{N-1}, l_N) = \Big(L_{j'(N'),i'(N')}, L_{j'(N'),\rho(i'(N'))}\Big).$$

This concludes the case where $\Phi_1^{(N')} \notin \mathsf{SAT}$.

Assume now instead that $M_0^{(N')} > 0$. That is, there exists a clause C_j that at "timepoint" $N'-1$ is still a 2-clause, but when fixing the variables dictated by $\mathcal{L}^{(N'-1)}$, it becomes a 0-clause. More precisely, there exists a $j \in [m]$ such that

$$-L_{j,1}, -L_{j,2} \in \mathcal{L}^{(N'-1)}.$$

Taking $j(1) := j'(1) := j$ and $i(1) := 1$, $i'(1) := 2$, this is the second statement in (B.4.9), so again we can find $j(2), j'(2), \dots, j(N'), j'(N') \in [m]$ and $i(2), i'(2), \dots, i(N'), i'(N') \in [2]$ such that (B.4.10) and (B.4.11) hold. We then define for $t \in \{0, 1, \dots, N'-1\}$:

$$l_t := -L_{j(N'-t),\rho(i(N'-t))}, \quad \text{and} \quad l_{N'+t} := L_{j'(t+1),\rho(i'(t+1))},$$

where we see that the first of the two definitions coincides with what we had in the case $\Phi_1^{(N')} \notin \mathsf{SAT}$, so we need only verify that

$$(-l_{N'-1}, l_{N'}) = \Big(L_{j(1),\rho(i(1))}, L_{j'(1),\rho(i'(1))}\Big) = (L_{j,2}, L_{j,1}),$$

and, using (B.4.11),

$$\begin{aligned}(-l_{N'+t-1}, l_{N'+t}) &= \Big(-L_{j'(t),\rho(i'(t))}, L_{j'(t+1),\rho(i'(t+1))}\Big)\\ &= \Big(L_{j'(t+1),i'(t+1)}, L_{j'(t+1),\rho(i'(t+1))}\Big),\end{aligned}$$

for all $t \in [N'-1]$, so that $(l_0, l_1, \dots, l_{2N'-1})$ is indeed contained in Φ. As before we also have $|l_0| \in \mathcal{L}_{\text{abs}}$, so if there exists a $t \in [2N'-1]$ such that $|l_t| \in \{|l_0|, |l_1|, \dots, |l_{t-1}|\}$, then we take N to be the smallest such t, and $(l_0, l_1, \dots, l_N)$ is an $\mathcal{L}$-cobra contained in Φ. If there does not exist such a t, then $(l_0, l_1, \ldots, l_{2N'-1})$ does the trick; indeed, we are only missing a verification of (c3), but

$$-l_{2N'-1} = -L_{j'(N'),\rho(i'(N'))} \in \mathcal{L}^{(0)} = \mathcal{L}$$

by (B.4.11), so indeed $|l_{2N'-1}| \in \mathcal{L}_{\text{abs}}$ as required.

Now let $\mathfrak{C}_N$ denote the set of $\mathcal{L}$-cobras of size N for each $N \in \mathbb{N}$, and put

$$Z := \sum_{N\in\mathbb{N}} \sum_{l\in\mathfrak{C}_N} \mathbb{1}_{\{\Phi \text{ contains } l\}},$$

i.e. Z is the number of $\mathcal{L}$-cobras contained in Φ. We have just shown that $F \subseteq \{Z > 0\}$, so if we can only show that $\mathbb{E}[Z] \to 0$ as $n \to \infty$, then the first moment method (Markov's inequality) asserts that

$$\mathbb{P}(F) \le \mathbb{P}(Z > 0) \le \mathbb{E}[Z] \longrightarrow 0 \quad \text{as } n \to \infty,$$

thus finishing the proof of Lemma B.13. To calculate the large n limit of $\mathbb{E}[Z]$, we first give an upper bound on $|\mathfrak{C}_N|$, i.e. the number of $\mathcal{L}$-cobras of size N. Since $\mathcal{L}$ is consistent, $|\mathcal{L}_{\text{abs}}| = |\mathcal{L}| = f$, and so there are f possible choices for $|l_0|$ by (c2), and taking the sign into consideration gives $2f$ possible choices for l_0. Then each of $l_1, l_2, \ldots, l_{N-1}$ can be chosen freely as long as $|l_0|, |l_1|, \ldots, |l_{N-1}|$ are pairwise distinct by (c1), so choosing them one after the other gives $2(n-t)$ choices for l_t, where $t \in [N-1]$. Finally, $|l_N|$ must be chosen from $\mathcal{L}_{\text{abs}} \cup \{|l_0|, |l_1|, \ldots, |l_{N-1}|\}$ by (c3), so this gives at the most $2(f+N)$ possible choices for l_N. All in all, we have

$$|\mathfrak{C}_N| \le 2^{N+1} f(n-1)(n-2)\ldots(n-(N-1))(f+N) \le 2^{N+1} n^{N-1} f(f+N). \quad \text{(B.4.12)}$$

Now, given some $l \in \mathfrak{C}_N$, what is the probability that Φ contains l? Notice that the sets

$$\{-l_0, l_1\}, \{-l_1, l_2\}, \ldots, \{-l_{N-1}, l_N\}$$

are pairwise different by property (c1), and again by (c1), each of the sets contain exactly two elements (literals), *except* for possibly the last set $\{-l_{N-1}, l_N\}$, where we might have $-l_{N-1} = l_N$. For any $l, l' \in \pm[n]$ and $j \in [m]$ we have

$$\mathbb{P}\Big(\{L_{j,1}, L_{j,2}\} = \{l, l'\}\Big) = \begin{cases} 2/(2n)^2 = 1/(2n^2), & \text{if } l \ne l', \\ 1/(2n)^2 = 1/(4n^2), & \text{if } l = l', \end{cases}$$

but in all cases $\mathbb{P}\Big(\{L_{j,1}, L_{j,2}\} = \{l, l'\}\Big) \le 1/(2n^2)$. Next we note that, for pairwise different $j_1, j_2, \ldots, j_N \in [m]$,

$$\begin{aligned} &\mathbb{P}\Big(\{L_{j_t,1}, L_{j_t,2}\} = \{-l_{t-1}, l_t\} \text{ for all } t \in [N]\Big) \\ &= \prod_{t\in[N]} \mathbb{P}\Big(\{L_{j_t,1}, L_{j_t,2}\} = \{-l_{t-1}, l_t\}\Big) \le \frac{1}{(2n^2)^N}, \end{aligned}$$

and since there are $\binom{m}{N}$ choices for $j_1, j_2, \ldots, j_N$ and $N!$ ways to arrange these, we get the following bound for the probability that Φ contains l:

$$\mathbb{P}(\Phi \text{ contains } l) \leq \binom{m}{N} \frac{N!}{2^N n^{2N}}. \tag{B.4.13}$$

Putting (B.4.12) and (B.4.13) together yields

$$\begin{aligned}\mathbb{E}[Z] &= \sum_{N\in\mathbb{N}} \sum_{l\in\mathfrak{C}_N} \mathbb{P}(\Phi \text{ contains } l) \\ &\leq \sum_{N\in\mathbb{N}} \frac{m! 2f(f+N)}{(m-N)! n^{N+1}} \\ &\leq \frac{f}{\sqrt{n}} \sum_{N\in\mathbb{N}} 2\left(\frac{m}{n}\right)^N \frac{f+N}{\sqrt{n}}.\end{aligned}$$

We now choose $\epsilon > 0$ small enough that $\alpha + \epsilon < 1$, and since $m/n \to \alpha$ as $n \to \infty$, we get for large enough n that $m/n \leq \alpha + \epsilon$. On the other hand, $f/\sqrt{n} \to 0$ as $n \to \infty$, so for n large enough we have $f/\sqrt{n} \leq 1 \leq N$ for all $N \in \mathbb{N}$, so

$$\sum_{N\in\mathbb{N}} 2\left(\frac{m}{n}\right)^N \frac{f+N}{\sqrt{n}} \leq \sum_{N\in\mathbb{N}} 4(\alpha+\epsilon)^N N =: \kappa < \infty,$$

where the first inequality holds when n is large enough, and κ is a fixed number that does not depend on n, and thus

$$\mathbb{E}[Z] \leq \frac{f}{\sqrt{n}} \kappa \longrightarrow 0 \quad \text{as } n \to \infty,$$

which was the final thing missing. □

We now have all necessary results in place and are thus equipped to prove Theorem B.2. We prove initially the case $k = 2$ when $\alpha > 0$, which is the most difficult part of the theorem. We proceed by showing that the claimed limit is both an asymptotic upper- and lower bound on the quantity under consideration.

B.4.3 Lower bound

We now begin our proof of Theorem B.2 in the case $k = 2$ when $\alpha > 0$. Thus, Φ is a random 2-CNF formula with n variables and $m \sim \alpha n$ clauses for $\alpha \in (0,1)$. Also, $\mathcal{L} \subseteq \pm[n]$ has $|\mathcal{L}| = f = f(n)$, where $f/\sqrt{n} \to \beta$, $\beta \in [0,\infty]$. The goal is to compute $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})$. In this section, we give a proof of the lower bound

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq \exp\left(\frac{-\beta^2 \alpha}{4(1-\alpha)}\right).$$

In the case that $\beta = \infty$, the lower bound $\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq 0$ is trivial, so assume without loss of generality that $\beta < \infty$. The case $\beta = 0$ is Lemma B.13, so assume also that $\beta > 0$. We will prove that

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq \exp\left(\frac{-\beta^2(1+\epsilon)\alpha}{4[1-(1+\epsilon)\alpha]}\right)$$

for all $\epsilon > 0$ small enough so that $(1+\epsilon)\alpha < 1$. Taking $\epsilon \to 0$ will then yield the correct lower bound. Thus, let $\epsilon > 0$ be such that $(1+\epsilon)\alpha < 1$, and define for convenience $\alpha_\epsilon := (1+\epsilon)\alpha$.

Let $C_1, \ldots, C_m$ be the random 2-clauses defining Φ. By Lemma B.8 we may assume without loss of generality that $\mathcal{L} = [n] \setminus [n-f]$. Let as before $K := \{0, 1, 2, \star\}$, and let for each $h \in K$ $\mathcal{C}_h^{(1)}$ and $M_h^{(1)}$ denote the set $\mathcal{C}_h$ and variable M_h, respectively, from (B.3.6). Put $\mathcal{C} := (\mathcal{C}_h^{(1)})_{h\in K}$. Let further Φ_1 and Φ_2 be the random functions defined in (B.3.7), i.e.

$$\Phi_h := \min_{j\in\mathcal{C}_h^{(1)}} (C_j)_{\mathcal{L}}, \quad (h = 1, 2).$$

Define finally

$$n^{(1)} := n - f, \quad f^{(1)} := \left\lfloor \alpha_\epsilon f + \alpha_\epsilon n^{3/8} \right\rfloor, \quad \mathcal{L}^{(1)} := [n^{(1)}] \setminus [n^{(1)} - f^{(1)}],$$

(and note that all of $n^{(1)}$, $f^{(1)}$, and $\mathcal{L}^{(1)}$ depend on n), and let $\Phi_1^{(1)}$ denote a random 1-CNF formula with $f^{(1)}$ clauses and $n^{(1)}$ variables, and let $\Phi_2^{(1)}$ denote a random 2-CNF formula with m clauses and $n^{(1)}$ variables. The exponent $3/8$ in the definition of $f^{(1)}$ could be any number strictly between $1/4$ and $1/2$, as the proof will show. With all this in place, we get from (B.3.8) that

$$\begin{aligned}
\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) &= \mathbb{P}\left(M_0^{(1)} = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\right) \\
&\geq \mathbb{P}\left(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\right) \\
&= \mathbb{E}\left[\mathbb{P}\left(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\middle|\, \mathcal{C}\right) \mathbb{1}_{\{M_0^{(1)}=0,\, M_1^{(1)} \leq f^{(1)}\}}\right].
\end{aligned}$$

By Lemma B.10 Φ_1, and Φ_2 are independent random 1- and 2-CNF formulas with $M_1^{(1)}$, and $M_2^{(1)}$ clauses, respectively, and $n^{(1)}$ variables under $\mathbb{P}(\cdot|\mathcal{C})$. Hence, letting $\mathcal{B}$ denote the set of all satisfiable 1-CNF formulas with $M_1^{(1)}$ clauses and $n^{(1)}$

variables, we get, on the event $\{M_1^{(1)} \le f^{(1)}\}$, that

$$
\begin{aligned}
&\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi, (\Phi_2)_{\varphi} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi \,\Big|\, \mathcal{C}\Big) \mathbb{P}\Big((\Phi_2)_{\varphi} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\ge \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \mathbb{P}\Big((\Phi_2)_{\mathcal{L}^{(1)}} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\ge \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big),
\end{aligned}
\tag{B.4.14}
$$

where in the first inequality we have used Lemma B.8(ii) (since $|\mathcal{L}^{(1)}| = f^{(1)} \ge M_1^{(1)}$), and in the final inequality we used Lemma B.9 with the fact that $\Phi_1^{(1)}$ has more clauses than Φ_1 and $\Phi_2^{(1)}$ has more clauses than Φ_2. Using this, we get

$$
\begin{aligned}
&\mathbb{E}\Big[\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \mathbb{1}_{\{M_0^{(1)}=0\ M_1^{(1)} \le f^{(1)}\}}\Big] \\
&\ge \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) \mathbb{P}\Big(M_1^{(1)} \le f^{(1)}, M_0^{(1)} = 0\Big) \\
&= \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) \mathbb{P}\Big(M_0^{(1)} = 0\Big) \mathbb{P}\Big(M_1^{(1)} \le f^{(1)} \,\Big|\, M_0^{(1)} = 0\Big).
\end{aligned}
$$

All together we conclude that

$$
\begin{aligned}
&\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \\
&\ge \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) \mathbb{P}\Big(M_0^{(1)} = 0\Big) \mathbb{P}\Big(M_1^{(1)} \le f^{(1)} \,\Big|\, M_0^{(1)} = 0\Big).
\end{aligned}
\tag{B.4.15}
$$

Notice now that we are in the same situation with $(\Phi_2^{(1)})_{\mathcal{L}^{(1)}}$ as we were with $\Phi_{\mathcal{L}}$, so we can repeat the above procedure. Put

$$
R := \Big\lfloor c \log(n) \Big\rfloor, \quad \text{where} \quad c := \frac{1}{16 \log(1/\alpha_\epsilon)} > 0.
$$

and define for all $r \in [R]$ (where we take $f^{(0)} := f$):

$$
n^{(r)} := n^{(r-1)} - f^{(r-1)}, \quad f^{(r)} := \Big\lfloor \alpha_\epsilon^r f + r \alpha_\epsilon^r n^{3/8} \Big\rfloor, \quad \mathcal{L}^{(r)} := [n^{(r)}] \setminus [n^{(r)} - f^{(r)}],
$$

and let $\mathcal{C}_h^{(r)}$, and $M_h^{(r)}$ denote the set $\mathcal{C}_h$ and variable M_h from (B.3.6) with $\Phi_2^{(r-1)}$ in place of Φ and $\mathcal{L}^{(r-1)}$ in place of $\mathcal{L}$ for each $h \in K$, and denote finally by $\Phi_1^{(r)}$ a random 1-CNF formula with $f^{(r)}$ clauses and $n^{(r)}$ variables, and by $\Phi_2^{(r)}$ a random 2-CNF formula with m clauses and $n^{(r)}$ variables. Redoing the argument above, we get for each $r \in [R]$ the following:

$$\begin{aligned}&\mathbb{P}\Big((\Phi_2^{(r-1)})_{\mathcal{L}^{(r-1)}} \in \mathsf{SAT}\Big)\\ \geq&\,\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(r)})_{\mathcal{L}^{(r)}} \in \mathsf{SAT}\Big)\mathbb{P}\Big(M_0^{(r)} = 0\Big)\mathbb{P}\Big(M_1^{(r)} \leq f^{(r)} \;\Big|\; M_0^{(r)} = 0\Big),\end{aligned}$$

and by successively applying this inequality R times we obtain:

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq&\,\mathbb{P}\Big((\Phi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big)\prod_{r=1}^{R}\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big)\times\\ &\times\prod_{r=1}^{R}\mathbb{P}\Big(M_0^{(r)} = 0\Big)\prod_{r=1}^{R}\mathbb{P}\Big(M_1^{(r)} \leq f^{(r)} \;\Big|\; M_0^{(r)} = 0\Big).\end{aligned} \tag{B.4.16}$$

Hence, the stipulated asymptotic lower bound will follow if we establish the following points:

(L1) $\lim_{n\to\infty}\mathbb{P}\Big((\Phi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big) = 1$,

(L2) $\lim_{n\to\infty}\prod_{r=1}^{R}\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) = \exp\Big(\frac{-\beta^2}{4}\sum_{r=1}^{\infty}\alpha_\epsilon^{2r}\Big)$,

(L3) $\lim_{n\to\infty}\prod_{r=1}^{R}\mathbb{P}\Big(M_0^{(r)} = 0\Big) \geq \exp\Big(\frac{-\beta^2}{4}\sum_{r=1}^{\infty}\alpha_\epsilon^{2r-1}\Big)$,

(L4) $\lim_{n\to\infty}\prod_{r=1}^{R}\mathbb{P}\Big(M_1^{(r)} \leq f^{(r)} \;\Big|\; M_0^{(r)} = 0\Big) = 1$.

It will be useful to note that, according to Lemma B.10, it holds for each $n \in \mathbb{N}$ and $r \in [R]$ that

$$\Big(M_0^{(r)}, M_1^{(r)}, M_2^{(r)}, M_\star^{(r)}\Big) \sim \mathrm{Multinomial}\Big(m, (p_0^{(r)}, p_1^{(r)}, p_2^{(r)}, p_\star^{(r)})\Big), \tag{B.4.17}$$

where

$$p_0^{(r)} = \frac{f^{(r-1)}(f^{(r-1)}-1)}{4n^{(r-1)}(n^{(r-1)}-1)}, \quad p_1^{(r)} := \frac{f^{(r-1)}n^{(r)}}{n^{(r-1)}(n^{(r-1)}-1)}, \quad p_2^{(r)} := \frac{n^{(r)}(n^{(r)}-1)}{n^{(r-1)}(n^{(r-1)}-1)},$$

and lastly $p_\star^{(r)} = 1 - p_0^{(r)} - p_1^{(r)} - p_2^{(r)}$. It will further be useful to note that, for any fixed $r \in [R]$,

$$\lim_{n\to\infty}\frac{f^{(r)}}{\sqrt{n}} = \alpha_\epsilon^r\beta. \tag{B.4.18}$$

Putting then $S := \sup_{n\in\mathbb{N}}(n^{3/8}/f) < \infty$, we get the upper bound

$$f^{(r)} \leq \alpha_\epsilon^r f + r\alpha_\epsilon^r n^{3/8} \leq \alpha_\epsilon^r f + Sr\alpha_\epsilon^r f = (1+Sr)\alpha_\epsilon^r f \tag{B.4.19}$$

for all $r \in [R]$. This yields further the following bound:

$$\sum_{h=0}^{\infty} f^{(h)} \leq \left[\sum_{h=0}^{\infty} \alpha_\epsilon^h + S \sum_{h=0}^{\infty} h\alpha_\epsilon^h\right] f = Cf, \tag{B.4.20}$$

where $C = (1 + (S-1)\alpha_\epsilon)/(1-\alpha_\epsilon)^2 < \infty$. We get from the definition of $n^{(r)}$ and (B.4.20) that

$$n - Cf \leq n^{(r)} \leq n \tag{B.4.21}$$

for all $r \in [R]$ and $n \in \mathbb{N}$, yielding in particular (noticing that also R depends on n)

$$\lim_{n\to\infty} \frac{n^{(r)}}{n} = 1, \quad \text{and} \quad \lim_{n\to\infty} \frac{n^{(R)}}{n} = 1. \tag{B.4.22}$$

Since $c\log(n) \leq R + 1$, $\alpha_\epsilon < 1$ and $c = 1/(16\log(1/\alpha_\epsilon))$, we get the following bounds on α_ϵ^R:

$$\frac{1}{n^{1/16}} = \alpha_\epsilon^{c\log(n)} \leq \alpha_\epsilon^R \leq \alpha_\epsilon^{c\log(n)-1} = \frac{1}{\alpha_\epsilon n^{1/16}}. \tag{B.4.23}$$

Using the lower bound, we find for $r \in [R]$ that $r\alpha_\epsilon^r n^{3/8} \geq \alpha_\epsilon^R n^{3/8} \geq n^{5/16} \geq 1$, so

$$f^{(r)} = \left\lfloor \alpha_\epsilon^r f + r\alpha_\epsilon^r n^{3/8} \right\rfloor \geq \alpha_\epsilon^r f \geq \alpha_\epsilon^R f \geq \frac{f}{n^{1/16}} \tag{B.4.24}$$

for all $r \in [R]$ and $n \in \mathbb{N}$.

Using now the upper bound on $\alpha_\epsilon^{R(n)}$ from (B.4.23), we conclude using initially (B.4.19) that

$$f^{(R)} \leq (1 + SR)\alpha_\epsilon^R f \leq \frac{1 + Sc\log(n)}{n^{1/16}} \cdot \frac{f}{\alpha_\epsilon},$$

so that $f^{(R)}/\sqrt{n} \to 0$. Hence, since $|\mathcal{L}^{(R)}| = f^{(R)}$ and since $\Phi_2^{(R)}$ is a random 2-CNF formula with m clauses and $n^{(R)}$ variables, where we have seen that $n^{(R)}/n \to 1$, we see that (L1) follows from Lemma B.13.

We now establish (L2). Since $\Phi_1^{(r)}$ is a random 1-CNF formula with $f^{(r)}$ clauses and $n^{(r)}$ variables for every $r \in [R]$, Lemma B.12 together with (B.4.18) and (B.4.22) shows that

$$\lim_{n\to\infty} \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) = e^{-\frac{1}{4}\beta^2\alpha_\epsilon^{2r}}.$$

Taking the logarithm, we want to conclude that

$$\lim_{n\to\infty} \sum_{r=1}^{\infty} \log \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) \mathbb{1}_{[R]}(r) = -\frac{1}{4}\beta^2 \sum_{r=1}^{\infty} \alpha_\epsilon^{2r},$$

which we will do by arguing that dominated convergence applies. This requires a uniform (over large enough n) summable (in r) lower bound on $\log \mathbb{P}(\Phi_1^{(r)} \in \mathsf{SAT})$. It follows from (B.4.4) in the proof of Lemma B.12 that

$$\begin{aligned}\mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) &\geq \sum_{h=0}^{\lfloor f^{(r)}/2\rfloor} \binom{n^{(r)}-h}{f^{(r)}-2h}\binom{n^{(r)}}{h}\frac{f^{(r)}!}{4^h (n^{(r)})^{f^{(r)}}}\\ &\geq \binom{n^{(r)}}{f^{(r)}}\frac{f^{(r)}!}{(n^{(r)})^{f^{(r)}}} = \prod_{h=0}^{f^{(r)}-1}\frac{n^{(r)}-h}{n^{(r)}},\end{aligned}$$

where we in the second inequality simply remove all but the first term. Now, from the classical inequality $\log(t) \leq t-1$ for all $t > 0$, we multiply by -1 and evaluate at $t = 1/(1-s)$, yielding

$$\log(1-s) \geq \frac{s}{s-1} \quad \text{for all } s < 1. \tag{B.4.25}$$

Using this and our inequalities above, we get

$$\begin{aligned}\log \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) &\geq \sum_{h=0}^{f^{(r)}-1} \log\left(1-\tfrac{h}{n^{(r)}}\right) \geq \sum_{h=0}^{f^{(r)}-1} \frac{h}{h-n^{(r)}}\\ &\geq \frac{1}{f^{(r)}-n^{(r)}}\sum_{h=0}^{f^{(r)}-1} h = \frac{(f^{(r)}-1)f^{(r)}}{2(f^{(r)}-n^{(r)})} \geq \frac{-(f^{(r)})^2}{2n^{(r+1)}},\end{aligned}$$

where we have used $n^{(r)} - f^{(r)} = n^{(r+1)}$. From here we apply (B.4.19) and (B.4.21) to get

$$\frac{(f^{(r)})^2}{2n^{(r+1)}} \leq (1+Sr)^2\alpha_\epsilon^{2r}\frac{f^2}{2(n-Cf)}.$$

Now, since

$$\frac{f^2}{2(n-Cf)} = \frac{1}{2}\left(\frac{f}{\sqrt{n}}\right)^2\left(\frac{n}{n-Cf}\right) \longrightarrow \frac{\beta^2}{2}$$

as $n \to \infty$, we conclude that, when n is large enough, it holds for all $r \in [R]$ that

$$\log \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) \geq -\beta^2(1+Sr)^2\alpha_\epsilon^{2r},$$

and of course $(1+Sr)^2\alpha_\epsilon^r \to 0$ as $r \to \infty$, so $S' := \sup_{r\in\mathbb{N}}(1+Sr)^2\alpha_\epsilon^r < \infty$, thus

$$\sum_{r=1}^{\infty}(1+Sr)^2\alpha_\epsilon^{2r} \leq S'\sum_{r=1}^{\infty}\alpha_\epsilon^r = S'\frac{\alpha_\epsilon}{1-\alpha_\epsilon} < \infty, \tag{B.4.26}$$

as required.

We now establish (L3). From (B.4.17) it follows that $M_0^{(r)} \sim \text{Binomial}(m, p_0^{(r)})$ for all $r \in [R]$. Writing

$$\begin{aligned}&\mathbb{P}\Big(M_0^{(r)} = 0\Big)\\ =&\Big(1 - p_0^{(r)}\Big)^m = \left(\left(1 - \left(\frac{f^{(r-1)}(f^{(r-1)} - 1)}{n}\right)\left(\frac{n^2}{n^{(r-1)}(n^{(r-1)} - 1)}\right)\frac{1}{4n}\right)^n\right)^{m/n},\end{aligned}$$

we find, using (B.4.18), (B.4.22), and $m/n \to \alpha$, that $\mathbb{P}(M_0^{(r)} = 0) \to e^{-\frac{1}{4}\beta^2\alpha_\epsilon^{2(r-1)}\alpha}$ as $n \to \infty$. Taking the logarithm, we want to conclude that

$$\lim_{n\to\infty}\sum_{r=1}^{\infty}\log\mathbb{P}\Big(M_0^{(r)} = 0\Big)\mathbb{1}_{[R]}(r) = -\frac{1}{4}\beta^2\alpha\sum_{r=1}^{\infty}\alpha_\epsilon^{2(r-1)} \geq -\frac{1}{4}\beta^2\sum_{r=1}^{\infty}\alpha_\epsilon^{2r-1},$$

where the inequality follows from $\alpha \leq (1+\epsilon)\alpha = \alpha_\epsilon$, and the equality will again follow from an application of dominated convergence, once we give a uniform (over large enough n) summable (in r) lower bound on the terms $\log\mathbb{P}(M_0^{(r)} = 0)$. Notice first of all that, using (B.4.20) and (B.4.21),

$$p_0^{(r)} \leq \frac{C^2}{4}\left(\frac{f}{\sqrt{n}}\right)^2\left(\frac{n}{n - Cf - 1}\right)^2\frac{1}{n} \longrightarrow 0 \quad \text{as } n \to \infty,$$

where the convergence is uniform in r (since the upper bound does not depend on r). Thus, when n is large enough, $p_0^{(r)} \leq 1/2$ for all $r \in [R]$. Next, using now (B.4.19) and (B.4.21), we find that

$$mp_0^{(r)} \leq \frac{(1+Sr)^2\alpha_\epsilon^{2r}}{4}\left(\frac{f}{\sqrt{n}}\right)^2\left(\frac{n}{n - Cf - 1}\right)^2\frac{m}{n},$$

where of course

$$\lim_{n\to\infty}\left(\frac{f}{\sqrt{n}}\right)^2\left(\frac{n}{n - Cf - 1}\right)^2\frac{m}{n} = \beta^2\alpha \leq \beta^2\alpha_\epsilon,$$

so it follows that when n is large enough, it holds for all $r \in [R]$ that

$$mp_0^{(r)} \leq \tfrac{1}{2}\beta^2(1+Sr)^2\alpha_\epsilon^{2r-1}. \tag{B.4.27}$$

Thus, when n is large enough to satisfy both (B.4.27) and $p_0^{(r)} \leq \frac{1}{2}$ for all $r \in [R]$, we get by using (B.4.25) that

$$\log\mathbb{P}\Big(M_0^{(r)} = 0\Big) = m\log\Big(1 - p_0^{(r)}\Big) \geq \frac{mp_0^{(r)}}{p_0^{(r)} - 1} \geq -\beta^2(1+Sr)^2\alpha_\epsilon^{2r-1}$$

holds for all $r \in [R]$, where we used $p_0^{(r)} \leq \frac{1}{2}$ in the denominator and (B.4.27) in the numerator, and (B.4.26) shows that this lower bound is summable, proving (L3).

We now establish (L4). Here we will not be able to apply dominated convergence, and it is for this reason that we stop the "splitting" process in (B.4.16) after R steps/rounds. If we were able to establish (L4) with (symbolically) $R = \infty$, then we could have completely bypassed a verification of (L1) and thus the need for Lemma B.13. But alas, we proceed without the comfort of dominated convergence and with the need for a verification of (L1) and Lemma B.13. Also, points (L1) through (L3) could all have been verified with α in place of α_ϵ, and it is only for this point (L4) that we need the "ϵ-breathing room" that α_ϵ provides us over a more direct calculation using α. Finally, it is at this point that we need the exponent 3/8 in the definition of $f^{(r)}$ to be greater than 1/4, and actually the precise definition of $f^{(r)}$ comes into play, where only the first order asymptotics of $f^{(r)}$ mattered for the other points. Thus, point (L4) is by far the most delicate out of the four.

First of all, if we define

$$\xi := \max_{r\in[R]} \mathbb{P}\Big(M_1^{(r)} > f^{(r)} \,\Big|\, M_0^{(r)} = 0\Big),$$

then taking the logarithm gives

$$\begin{aligned}\sum_{r=1}^{R} \log \mathbb{P}\Big(M_1^{(r)} \leq f^{(r)} \,\Big|\, M_0^{(r)} = 0\Big) &\geq R \min_{r\in[R]} \log \mathbb{P}\Big(M_1^{(r)} \leq f^{(r)} \,\Big|\, M_0^{(r)} = 0\Big) \\ &= R\log(1-\xi) \geq R\frac{\xi}{\xi-1} \geq \frac{c\log(n)\xi}{\xi-1},\end{aligned}$$

where we in the second to last inequality use (B.4.25). Hence, if we can show that $\log(n)\xi \to 0$ as $n \to \infty$, then certainly $\xi \to 0$ as well, and thus

$$\lim_{n\to\infty} \frac{c\log(n)\xi}{\xi-1} = 0,$$

from which (L4) follows. Now, from (B.4.17) we get from known results that in the conditional distribution given $M_0^{(r)} = 0$, $M_1^{(r)}$ follows a Binomial distribution with parameters m and

$$p_{1|0}^{(r)} := \frac{p_1^{(r)}}{1-p_0^{(r)}} = \frac{f^{(r-1)}n^{(r)}}{n^{(r-1)}(n^{(r-1)}-1) - \frac{1}{4}f^{(r-1)}(f^{(r-1)}-1)}.$$

Now consider for a moment the expression

$$\begin{aligned}&\frac{mn^{(r)}}{n^{(r-1)}(n^{(r-1)}-1) - \frac{1}{4}f^{(r-1)}(f^{(r-1)}-1)} \\ \leq &\frac{mn}{(n-Cf-1)^2 - \frac{1}{4}(Cf)^2} \longrightarrow \alpha \quad \text{as } n \to \infty,\end{aligned} \tag{B.4.28}$$

where we have used (B.4.20) and (B.4.21), and the convergence is uniform in r. Letting then $N^{(r)} \sim \text{Binomial}(m, p_{1|0}^{(r)})$ under $\mathbb{P}$, we see that

$$\mathbb{E}[N^{(r)}] = mp_{1|0}^{(r)} = f^{(r-1)} \frac{mn^{(r)}}{n^{(r-1)}(n^{(r-1)}-1) - \frac{1}{4}f^{(r-1)}(f^{(r-1)}-1)} \le (1+\epsilon)\alpha f^{(r-1)} = \alpha_\epsilon f^{(r-1)}, \tag{B.4.29}$$

where the last inequality holds for large enough n independent of r thanks to (B.4.28). Furthermore, since $f^{(r-1)} = \lfloor \alpha_\epsilon^{r-1} f + (r-1)\alpha_\epsilon^{r-1} n^{3/8} \rfloor$, we get

$$\alpha_\epsilon f^{(r-1)} \le \alpha_\epsilon^r f + r\alpha_\epsilon^r n^{3/8} - \alpha_\epsilon^r n^{3/8},$$

giving all together

$$\alpha_\epsilon^r f + r\alpha_\epsilon^r n^{3/8} \ge \mathbb{E}[N^{(r)}] + \alpha_\epsilon^r n^{3/8}, \tag{B.4.30}$$

uniformly in r for large enough n. Now,

$$\mathbb{P}\Big(M_1^{(r)} > f^{(r)} \;\Big|\; M_0^{(r)} = 0\Big) = \mathbb{P}\Big(N^{(r)} > f^{(r)}\Big),$$

and since $N^{(r)}$ takes only integer values, rounding down makes no difference, i.e.

$$\mathbb{P}\Big(N^{(r)} > f^{(r)}\Big) = \mathbb{P}\Big(N^{(r)} > \alpha_\epsilon^r f + r\alpha_\epsilon^r n^{3/8}\Big) \le \mathbb{P}\Big(N^{(r)} > \mathbb{E}[N^{(r)}] + \alpha_\epsilon^r n^{3/8}\Big),$$

where we in the inequality have used (B.4.30), so it holds uniformly in r for large enough n. We will now apply Chernoff's bound:

$$\mathbb{P}\Big(N > \mathbb{E}[N] + \delta\,\mathbb{E}[N]\Big) \le e^{-\frac{1}{3}\delta^2\,\mathbb{E}[N]}, \tag{B.4.31}$$

when N is binomially distributed and $0 < \delta < 1$. Taking in our case $N = N^{(r)}$ and

$$\delta = \frac{\alpha_\epsilon^r n^{3/8}}{\mathbb{E}[N^{(r)}]},$$

we find that, as long as $r \in [R]$, (B.4.21) and (B.4.24) give us

$$\mathbb{E}[N^{(r)}] = f^{(r-1)} \frac{mn^{(r)}}{n^{(r-1)}(n^{(r-1)}-1) - \frac{1}{4}f^{(r-1)}(f^{(r-1)}-1)} \ge \frac{f}{n^{1/16}} \cdot \frac{m(n-Cf)}{n^2},$$

so using (B.4.23) in addition to the above we get for all $r \in [R]$:

$$\delta = \frac{\alpha_\epsilon^r n^{3/8}}{\mathbb{E}[N^{(r)}]} \le \frac{1}{n^{1/16}} \cdot \frac{\sqrt{n}}{f} \cdot \frac{n}{m} \cdot \frac{n}{n-Cf} \longrightarrow 0 \quad \text{as } n \to \infty,$$

so naturally $\delta < 1$ for all $r \in [R]$ for large enough n. Hence, Chernoff's bound yields

$$\mathbb{P}\Big(N^{(r)} > \mathbb{E}[N^{(r)}] + \alpha_\epsilon^r n^{3/8}\Big) \leq \exp\bigg(\frac{-\alpha_\epsilon^{2r} n^{3/4}}{3\,\mathbb{E}[N^{(r)}]}\bigg)$$

for all $r \in [R]$ when n is large enough. We saw in (B.4.29) that $\mathbb{E}[N^{(r)}] \leq f^{(r-1)}$ for all $r \in [R]$ when n is large enough, and $f^{(r-1)} \leq Cf$ for all $r \in [R]$, $n \in \mathbb{N}$ by (B.4.20). On the other hand, $\alpha_\epsilon^{2r} \geq \alpha_\epsilon^{2R} \geq n^{-1/8}$ for all $r \in [R]$ and $n \in \mathbb{N}$ by (B.4.23), so taken all together we get when n is large enough:

$$\xi = \max_{r\in[R]} \mathbb{P}\Big(N^{(r)} > f^{(r)}\Big) \leq \max_{r\in[R]} \exp\bigg(\frac{-\alpha_\epsilon^{2r} n^{3/4}}{3\,\mathbb{E}[N^{(r)}]}\bigg) \leq \exp\bigg(\frac{-n^{5/8}}{3Cf}\bigg),$$

and of course $n^{5/8}/(3Cf)$ is asymptotic to $n^{1/8}/(3C\beta)$ as $n \to \infty$, readily yielding $\log(n)\xi \to 0$, completing the proof of (L4) and thus the entire proof of the lower bound.

B.4.4 Upper bound

We now give a proof of the upper bound

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \exp\bigg(-\frac{\beta^2\alpha}{4(1-\alpha)}\bigg).$$

Taken together with the lower bound, this will complete the proof of the case $k = 2$ in Theorem B.2 when $\alpha > 0$. We are still assuming that Φ is a random 2-CNF formula with $m = m(n)$ clauses and n variables, where $n \to \infty$ and $m/n \to \alpha$, and that $|\mathcal{L}| = f = f(n)$, where $f/\sqrt{n} \to \beta$. A priori we have $\alpha \in (0,1)$ and $\beta \in [0,\infty]$, but the case $\beta = 0$ is trivial, so we assume without loss of generality that $\beta > 0$. We will also assume that $\beta < \infty$, since the case $\beta = \infty$ follows. Indeed, let for a given $T > 0$ Ψ denote a random 2-CNF formula with n variables and $\lfloor T\sqrt{n}\rfloor$ clauses. Then $f \geq \lfloor T\sqrt{n}\rfloor$ for large enough n if $\beta = \infty$, so by Lemma B.9 we get

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \limsup_{n\to\infty} \mathbb{P}(\Psi_{\mathcal{L}} \in \mathsf{SAT}) \leq \exp\bigg(-\frac{T^2\alpha}{4(1-\alpha)}\bigg).$$

Letting $T \to \infty$ gives the desired result. Hence, assume $\beta \in (0,\infty)$.

The method for proving the upper bound will be similar to the one for the lower bound. We "reset" the notation from the lower bound and begin anew. Let $\epsilon \in (0,1)$ be given. We prove the bound

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \exp\bigg(\frac{-\beta^2(1-\epsilon)\alpha}{4[1-(1-\epsilon)\alpha]}\bigg),$$

from which the desired bound follows by taking $\epsilon \to 0$. Put $\alpha_\epsilon := (1-\epsilon)\alpha$.

As in the lower bound we assume without loss of generality that $\mathcal{L} = [n] \setminus [n-f]$ by Lemma B.8. Let $K = \{0,1,2,\star\}$, and decompose $\Phi_{\mathcal{L}}$ into Φ_1 and Φ_2 with corresponding random sets $\mathcal{C} = (\mathcal{C}_h^{(1)})_{h\in K}$ and random variables $(M_h^{(1)})_{h\in K}$ according to (B.3.6). Define

$$n^{(1)} := n - f, \quad f^{(1)} := \left\lfloor \alpha_\epsilon f - \alpha_\epsilon n^{3/8} \right\rfloor, \quad w := \left\lfloor n^{1/4} \right\rfloor,$$
$$m^{(1)} := \left\lceil m - 3\alpha\left(f + n^{3/8}\right)\right\rceil, \quad \mathcal{L}^{(1)} := [n^{(1)}] \setminus [n^{(1)} - (f^{(1)} - w)],$$

where $\lceil\cdot\rceil$ denotes the ceiling function (rounding up), and let $\Phi_1^{(1)}$ denote a random 1-CNF formula with $f^{(1)}$ clauses and $n^{(1)}$ variables, and let $\mathcal{L}_1^{(1)}$ denote the set of $f^{(1)}$ random literals defining $\Phi_1^{(1)}$, and let finally $\Phi_2^{(1)}$ denote a random 2-CNF formula with $m^{(1)}$ clauses and $n^{(1)}$ variables.

We get from (B.3.8) that

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) &= \mathbb{P}\Big(M_0^{(1)} = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big)\\ &\le \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \ge f^{(1)}, M_2^{(1)} \ge m^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big)\\ &\quad + \mathbb{P}\Big(M_1^{(1)} < f^{(1)}\Big) + \mathbb{P}\Big(M_2^{(1)} < m^{(1)}\Big).\end{aligned}$$

And

$$\begin{aligned}&\mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \ge f^{(1)}, M_2^{(1)} \ge m^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big)\\ =&\mathbb{E}\Big[\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big)\mathbb{1}_{\{M_0^{(1)}=0,\, M_1^{(1)}\ge f^{(1)},\, M_2^{(1)}\ge m^{(1)}\}}\Big].\end{aligned}$$

When we in the following consider $\mathbb{P}(\cdot|\mathcal{C})$ we will assume that we are on the event $\{M_0^{(1)} = 0,\ M_1^{(1)} \ge f^{(1)},\ M_2^{(1)} \ge m^{(1)}\}$. Note that under $\mathbb{P}(\cdot|\mathcal{C})$ we have that Φ_1 is a random 1-CNF formula with $m - f$ variables and $M_1^{(1)}$ clauses, while Φ_2 is a random 2-CNF formula with $n - f$ variables and $M_2^{(1)}$ clauses. Also, the two random formulas are (conditionally) independent.

The next step of this argument is a bit more involved than in the lower bound, since here, the number of *distinct* clauses in Φ_1 might be lower than $M_1^{(1)}$ owing to duplicates, and thus, Φ_1 might fix fewer than $M_1^{(1)}$ variables in Φ_2. This was of course also the case in the lower bound, but fixing the maximum number of variables only reduced the probability of satisfiability even further; here, we must deal with this issue properly. Let $\mathcal{L}_1$ denote the set of random literals defining Φ_1, i.e. $\Phi_1 = \min(\mathcal{L}_1)$. Notice firstly that, as $M_1^{(1)} \ge f^{(1)}$, then Φ_1 has more clauses than $\Phi_1^{(1)}$, and hence

$$\mathbb{P}\Big(|\mathcal{L}_1| < f^{(1)} - w \,\Big|\, \mathcal{C}\Big) \le \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big).$$

Using this, we have that

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\le \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}, |\mathcal{L}_1| \ge f^{(1)} - w \,\Big|\, \mathcal{C}\Big) + \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big).
\end{aligned}$$

Letting $\mathcal{B}$ denote the set of all satisfiable 1-CNF formulas with at least $f^{(1)} - w$ (distinct) clauses and $n^{(1)}$ variables, we find that

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}, |\mathcal{L}_1| \ge f^{(1)} - w \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi, (\Phi_2)_\varphi \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi \,\Big|\, \mathcal{C}\Big) \mathbb{P}\Big((\Phi_2)_\varphi \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\le \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, |\mathcal{L}_1| \ge f^{(1)} - w \,\Big|\, \mathcal{C}\Big) \mathbb{P}\Big((\Phi_2)_{\mathcal{L}^{(1)}} \in \mathsf{SAT} \Big| \mathcal{C}\Big) \\
&\le \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \mathbb{P}\Big((\Phi_2)_{\mathcal{L}^{(1)}} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\le \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big),
\end{aligned}$$

where we in the first inequality use Lemma B.8 and in the final inequality use Lemma B.9. This yields

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\le \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) + \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big),
\end{aligned}$$

and thus,

$$\begin{aligned}
&\mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \ge f^{(1)}, M_2^{(1)} \ge m^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big) \\
&\quad \le \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \ge f^{(1)}, M_2^{(1)} \ge m^{(1)}\Big) \times \\
&\qquad \times \Big[\mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) + \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big)\Big] \\
&\quad \le \mathbb{P}\Big(M_0^{(1)} = 0\Big) \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) + \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big).
\end{aligned}$$

All in all, we get

$$\begin{aligned}
\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \le\ & \mathbb{P}\Big(M_0^{(1)} = 0\Big) \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) \mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) \\
&+ \mathbb{P}\Big(M_1^{(1)} < f^{(1)}\Big) + \mathbb{P}\Big(M_2^{(1)} < m^{(1)}\Big) + \mathbb{P}\Big(|\mathcal{L}_1^{(1)}| < f^{(1)} - w\Big).
\end{aligned}$$

We now repeat the procedure on $(\Phi_2^{(1)})_{\mathcal{L}^{(1)}}$. Put again

$$R := \big\lfloor c \log(n) \big\rfloor, \quad \text{where} \quad c := \frac{1}{16 \log(1/\alpha_\epsilon)},$$

and define for each $r \in [R]$:

$$n^{(r)} := n - f - \sum_{h=1}^{r-1} (f^{(h)} - w), \quad f^{(r)} := \left\lfloor \alpha_\epsilon^r f - r\alpha_\epsilon^r n^{3/8} \right\rfloor,$$
$$m^{(r)} := \left\lceil m - \frac{3}{1-\epsilon}(f + n^{3/8}) \sum_{h=1}^{r} \alpha_\epsilon^h \right\rceil,$$

and finally $\mathcal{L}^{(r)} := [n^{(r)}] \setminus [n^{(r)} - (f^{(r)} - w)]$, and let $\mathcal{C}_h^{(r)}$ denote the random set $\mathcal{C}_h$ and $M_h^{(r)}$ denote the random variable M_h from (B.3.6) with $\Phi_2^{(r-1)}$ in place of Φ and $\mathcal{L}^{(r-1)}$ in place of $\mathcal{L}$ for each $h \in K$, and denote finally by $\Phi_1^{(r)}$ a random 1-CNF formula with $f^{(r)}$ clauses and $n^{(r)}$ variables, and by $\mathcal{L}_1^{(r)}$ the set of random literals defining $\Phi_1^{(r)}$, and finally by $\Phi_2^{(r)}$ a random 2-CNF formula with $m^{(r)}$ clauses and $n^{(r)}$ variables. Redoing the argument above R times, and finally bounding $\mathbb{P}((\Phi^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}) \leq 1$, we get

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq & \prod_{r=1}^{R} \mathbb{P}\Big(M_0^{(r)} = 0\Big) \prod_{r=1}^{R} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) \\ & + \sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} < f^{(r)}\Big) + \sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < m^{(r)}\Big) \\ & + \sum_{r=1}^{R} \mathbb{P}\Big(|\mathcal{L}_1^{(r)}| < f^{(r)} - w\Big).\end{aligned}$$

The upper bound then follows after a verification of the following points:

(U1) $\lim_{n\to\infty} \prod_{r=1}^{R} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big) = \exp\left(\frac{-\beta^2}{4} \sum_{r=1}^{\infty} \alpha_\epsilon^{2r}\right)$,

(U2) $\lim_{n\to\infty} \prod_{r=1}^{R} \mathbb{P}\Big(M_0^{(r)} = 0\Big) \leq \exp\left(\frac{-\beta^2}{4} \sum_{r=1}^{\infty} \alpha_\epsilon^{2r-1}\right)$,

(U3) $\lim_{n\to\infty} \sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} < f^{(r)}\Big) = 0$,

(U4) $\lim_{n\to\infty} \sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < m^{(r)}\Big) = 0$,

(U5) $\lim_{n\to\infty} \sum_{r=1}^{R} \mathbb{P}\Big(|\mathcal{L}_1^{(r)}| < f^{(r)} - w\Big) = 0$.

We initially note that, by Lemma B.10,

$$\Big(M_0^{(r)}, M_1^{(r)}, M_2^{(r)}, M_\star^{(r)}\Big) \sim \mathrm{Multinomial}\Big(m^{(r-1)}, (p_0^{(r)}, p_1^{(r)}, p_2^{(r)}, p_\star^{(r)})\Big), \tag{B.4.32}$$

where we now have for $r \geq 2$

$$p_0^{(r)} = \frac{(f^{(r-1)} - w)(f^{(r-1)} - w - 1)}{4n^{(r-1)}(n^{(r-1)} - 1)}, \qquad p_1^{(r)} = \frac{(f^{(r-1)} - w)n^{(r)}}{n^{(r-1)}(n^{(r-1)} - 1)},$$
$$p_2^{(r)} = \frac{n^{(r)}(n^{(r)} - 1)}{n^{(r-1)}(n^{(r-1)} - 1)}, \qquad p_\star^{(r)} = 1 - p_0^{(r)} - p_1^{(r)} - p_2^{(r)}.$$

The expressions for $p_h^{(1)}$, $h \in \{0, 1, 2, \star\}$, are the same, except we do not subtract w from f in this case.

We of course still have

$$\lim_{n\to\infty} \frac{f^{(r)}}{\sqrt{n}} = \alpha_\epsilon^r \beta \tag{B.4.33}$$

for all $r \in [R]$, so it follows immediately from Lemma B.11 that

$$\sum_{r=1}^{R} \mathbb{P}\Big(|\mathcal{L}_1^{(r)}| < f^{(r)} - w\Big) \leq \sum_{r=1}^{R} \frac{4\alpha_\epsilon^{2r}\beta^2}{w} \leq 4\beta^2 \frac{R}{w} \longrightarrow 0 \quad \text{as } n \to \infty,$$

proving (U5).

Putting $C := 1/(1-\alpha_\epsilon)$ and $C' := 6C/(1-\epsilon)$, we have

$$f + \sum_{h=1}^{r-1}(f^{(h)} - w) \leq \sum_{h=0}^{r-1} f^{(h)} \leq \sum_{h=0}^{r-1} \alpha_\epsilon^h f \leq Cf \tag{B.4.34}$$

for all $r \in [R]$, and therefore $n - Cf \leq n^{(r)} \leq n$. We also immediately find $m^{(r)} \leq m$, and $f/n^{3/8} \to \infty$ as $n \to \infty$, so $n^{3/8} \leq f$ for large enough n, and after this point

$$\frac{3}{1-\epsilon}\Big(f + n^{3/8}\Big)\sum_{h=1}^{r} \alpha_\epsilon^h \leq \frac{3C}{1-\epsilon}\Big(f + n^{3/8}\Big) \leq C'f,$$

yielding $m^{(r)} \geq m - C'f$ and hence

$$\lim_{n\to\infty} \frac{n^{(r)}}{n} = 1, \quad \text{and} \quad \lim_{n\to\infty} \frac{m^{(r)}}{n} = \alpha \tag{B.4.35}$$

for all $r \in [R]$. Of course, we still have

$$\frac{1}{n^{1/16}} \leq \alpha_\epsilon^R \leq \frac{1}{\alpha_\epsilon n^{1/16}} \tag{B.4.36}$$

by the same argument as in (B.4.23). Now, for a lower bound on $f^{(r)}$ we notice that when $r \in [R]$ we have $r\alpha_\epsilon^r n^{3/8} \leq R\alpha_\epsilon^r n^{3/8}$, and

$$\frac{\frac{1}{2}\alpha_\epsilon^r f}{R\alpha_\epsilon^r n^{3/8}} = \frac{f}{2Rn^{3/8}} \longrightarrow \infty \quad \text{as } n \to \infty,$$

where the convergence is uniform in r, so we have $r\alpha_\epsilon^r n^{3/8} \le \frac{1}{2}\alpha_\epsilon^r f - 1$ for all $r \in [R]$ when n is large enough, and thus

$$f^{(r)} = \left\lfloor \alpha_\epsilon^r f - r\alpha_\epsilon^r n^{3/8} \right\rfloor \ge \frac{\alpha_\epsilon^r f}{2} \ge \frac{f}{2n^{1/16}} \tag{B.4.37}$$

for all $r \in [R]$ when n is large enough, where the last inequality comes from (B.4.36). Further, since $f/n^{1/16}$ is asymptotic to $\beta n^{7/16}$ as $n \to \infty$, we see that

$$w \le n^{1/4} \le \frac{f}{4n^{1/16}} \le \frac{f^{(r)}}{2}$$

for all $r \in [R]$ when n is large enough, using in the end (B.4.37), and from these inequalities follows

$$f^{(r)} - w \ge \tfrac{1}{2} f^{(r)}. \tag{B.4.38}$$

For (U1) we see that, similarly to (L2), since $\Phi_1^{(r)}$ is a random 1-CNF formula with $f^{(r)}$ clauses and $n^{(r)}$ variables, Lemma B.12 together with (B.4.33) and (B.4.35) gives

$$\lim_{n\to\infty} \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) = e^{-\frac{1}{4}\beta^2\alpha_\epsilon^{2r}}$$

for all $r \in [R]$, and to complete the proof of (U1) we need only give a uniform (in large n) summable (in r) lower bound on $\log \mathbb{P}(\Phi_1^{(r)} \in \mathsf{SAT})$ to be able to apply dominated convergence. By the exact same argument as in the proof of (L2) we get

$$\log \mathbb{P}\left(\Phi_1^{(r)} \in \mathsf{SAT}\right) \ge \frac{-(f^{(r)})^2}{2n^{(r+1)}},$$

and we also have

$$\lim_{n\to\infty} \frac{f^2}{2(n - Cf)} = \frac{\beta^2}{2},$$

so using $f^{(r)} \le \alpha_\epsilon^r f$ and $n^{(r+1)} \ge n - Cf$, we conclude that

$$\frac{-(f^{(r)})^2}{2n^{(r+1)}} \ge \alpha_\epsilon^{2r} \frac{-f^2}{2(n - Cf)} \ge -\alpha_\epsilon^{2r}\beta^2,$$

where the last inequality holds for large enough n independent of r.

Now for (U2) we get from (B.4.32) that $M_0^{(r)} \sim \mathrm{Binomial}(m^{(r-1)}, p_0^{(r)})$, so similarly to the argument in the proof of (L3):

$$\mathbb{P}\left(M_0^{(r)} = 0\right) = \left(1 - p_0^{(r)}\right)^{m^{(r-1)}} \longrightarrow e^{-\frac{1}{4}\beta^2\alpha_\epsilon^{2(r-1)}\alpha} \le e^{-\frac{1}{4}\beta^2\alpha_\epsilon^{2r-1}}$$

for all $r \in [R]$, and to complete the proof of (U2) we need only give a uniform (in large n) summable (in r) lower bound on $\log \mathbb{P}(M_0^{(r)} = 0)$. To this end, we again notice that

$$p_0^{(r)} \leq \frac{f^2}{4(n - Cf - 1)^2} \longrightarrow 0$$

uniformly in r, so $p_0^{(r)} \leq \frac{1}{2}$ for all $r \in [R]$ when n is large enough, and

$$m^{(r-1)} p_0^{(r)} \leq \alpha_\epsilon^{2(r-1)} \frac{mf^2}{4(n - Cf - 1)^2} \longrightarrow \frac{1}{4} \alpha_\epsilon^{2(r-1)} \alpha \beta^2 \leq \frac{1}{4} \alpha_\epsilon^{2r-1} \beta^2,$$

so $m^{(r-1)} p_0^{(r)} \leq \frac{1}{2} \alpha_\epsilon^{2r-1} \beta^2$ for all $r \in [R]$ when n is large enough, and hence we conclude using (B.4.25) that

$$\log \mathbb{P}\big(M_0^{(r)} = 0\big) = m^{(r-1)} \log\big(1 - p_0^{(r)}\big) \geq \frac{m^{(r-1)} p_0^{(r)}}{p_0^{(r)} - 1} \geq -\alpha_\epsilon^{2r-1} \beta^2$$

for all $r \in [R]$ when n is large enough.

Now for (U3). We get from (B.4.32) that $M_1^{(r)} \sim \text{Binomial}(m^{(r-1)}, p_1^{(r)})$, so we see that

$$\mathbb{E}[M_1^{(r)}] = \begin{cases} \dfrac{m^{(r-1)}(f^{(r-1)} - w) n^{(r)}}{n^{(r-1)}(n^{(r-1)} - 1)}, & \text{if } r \geq 2, \\ \dfrac{mfn^{(1)}}{n(n-1)}, & \text{if } r = 1, \end{cases}$$

and

$$\frac{m^{(r-1)} n^{(r)}}{n^{(r-1)}(n^{(r-1)} - 1)} \geq \frac{(m - C'f)(n - Cf)}{n^2} \longrightarrow \alpha,$$

so $m^{(r-1)} n^{(r)} / n^{(r-1)}(n^{(r-1)} - 1) \geq \alpha_\epsilon$ for all $r \in [R]$ when n is large enough. Hence, since

$$\begin{aligned} f^{(r-1)} - w &= \left\lfloor \alpha_\epsilon^{r-1} f - (r-1) \alpha_\epsilon^{r-1} n^{3/8} \right\rfloor - \left\lfloor n^{1/4} \right\rfloor \\ &\geq \alpha_\epsilon^{r-1} f - (r-1) \alpha_\epsilon^{r-1} n^{3/8} - 2n^{1/4}, \end{aligned}$$

and of course $f \geq f - 2n^{1/4}$ for the case $r = 1$, we get

$$\mathbb{E}[M_1^{(r)}] \geq \alpha_\epsilon^r f - r\alpha_\epsilon^r n^{3/8} + \alpha_\epsilon^r n^{3/8} - 2\alpha_\epsilon n^{1/4}$$

for all $r \in [R]$ when n is large enough, which is the same as the second inequality in

$$f^{(r)} \leq \alpha_\epsilon^r f - r\alpha_\epsilon^r n^{3/8} \leq \mathbb{E}[M_1^{(r)}] - \alpha_\epsilon^r n^{3/8} + 2\alpha_\epsilon n^{1/4}. \qquad \text{(B.4.39)}$$

Now, if $r \in [R]$, then $\alpha_\epsilon^r \geq n^{-1/16}$ by (B.4.36), and of course $2n^{1/4} \leq \frac{1}{2}n^{5/16}$ for large enough n, so in that case

$$-\alpha_\epsilon^r n^{3/8} + 2\alpha_\epsilon n^{1/4} \leq -n^{5/16} + 2n^{1/4} \leq -\tfrac{1}{2}n^{5/16}$$

for large enough n. We now get from (B.4.39) and the above that

$$\mathbb{P}\Big(M_1^{(r)} < f^{(r)}\Big) \leq \mathbb{P}\Big(M_1^{(r)} < \mathbb{E}[M_1^{(r)}] - \tfrac{1}{2}n^{5/16}\Big)$$

for all $r \in [R]$ when n is large enough. Next, we wish to apply the following Chernoff bound:

$$\mathbb{P}\Big(N < \mathbb{E}[N] - \delta\,\mathbb{E}[N]\Big) \leq e^{-\frac{1}{2}\delta^2\,\mathbb{E}[N]}$$

when N is binomially distributed and $0 < \delta < 1$. Taking in our case $N = M_1^{(r)}$ and

$$\delta = \frac{n^{5/16}}{2\,\mathbb{E}[M_1^{(r)}]} \leq \frac{n^{5/16}}{2\alpha_\epsilon(f^{(r-1)} - w)} \leq \frac{n^{5/16}}{\alpha_\epsilon f^{(r-1)}} \leq \frac{2n^{3/8}}{\alpha_\epsilon f} \longrightarrow 0,$$

where the first inequality comes from the initial bound on $\mathbb{E}[M_1^{(r)}]$, the second comes from (B.4.38), and the final from (B.4.37), and all three inequalities hold for all $r \in [R]$ when n is large enough. Thus, for all $r \in [R]$ it holds for large enough n that $\delta < 1$, so Chernoff's bound gives

$$\mathbb{P}\Big(M_1^{(r)} < \mathbb{E}[M_1^{(r)}] - \tfrac{1}{2}n^{5/16}\Big) \leq \exp\left(\frac{-n^{5/8}}{8\,\mathbb{E}[M_1^{(r)}]}\right).$$

Lastly, we note that

$$\mathbb{E}[M_1^{(r)}] \leq f\frac{mn}{(n - Cf - 1)^2},$$

and $mn/(n - Cf - 1)^2 \to \alpha$ as $n \to \infty$, so for large enough n it holds for all $r \in [R]$ that $\mathbb{E}[M_1^{(r)}] \leq 2\alpha f$, and using this yields

$$\exp\left(\frac{-n^{5/8}}{8\,\mathbb{E}[M_1^{(r)}]}\right) \leq \exp\left(\frac{-n^{5/8}}{16\alpha f}\right).$$

Putting it all together, we get

$$\sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} < f^{(r)}\Big) \leq R\exp\left(\frac{-n^{5/8}}{16\alpha f}\right) \longrightarrow 0 \quad \text{as } n \to \infty,$$

as desired.

Now finally for (U4). We see for all $r \in [R]$ that, since $M_2^{(r)}$ can only attain integer values,

$$\mathbb{P}\Big(M_2^{(r)} < m^{(r)}\Big) = \mathbb{P}\Big(M_2^{(r)} < m - \frac{3}{1-\epsilon}\big(f + n^{3/8}\big)\sum_{h=1}^{r} \alpha_\epsilon^h\Big),$$

and

$$m - \frac{3}{1-\epsilon}\big(f + n^{3/8}\big)\sum_{h=1}^{r} \alpha_\epsilon^h \le m^{(r-1)} - \frac{3}{1-\epsilon}\big(f + n^{3/8}\big)\alpha_\epsilon^r,$$

so

$$\mathbb{P}\Big(M_2^{(r)} < m - \frac{3}{1-\epsilon}\big(f + n^{3/8}\big)\sum_{h=1}^{r} \alpha_\epsilon^h\Big) \le \mathbb{P}\Big(m^{(r-1)} - M_2^{(r)} > \frac{3\alpha_\epsilon^r}{1-\epsilon}\big(f + n^{3/8}\big)\Big).$$

Now, from (B.4.32) we find that $m^{(r-1)} - M_2^{(r)} = M_0^{(r)} + M_1^{(r)} + M_\star^{(r)}$, and

$$M_0^{(r)} + M_1^{(r)} + M_\star^{(r)} \sim \text{Binomial}\Big(m^{(r-1)}, 1 - p_2^{(r)}\Big).$$

Put for convenience $N^{(r)} := M_0^{(r)} + M_1^{(r)} + M_\star^{(r)}$, and notice that for $r \ge 2$, as $n^{(r)} = n^{(r-1)} - (f^{(r-1)} - w)$,

$$p_2^{(r)} = \frac{n^{(r)}(n^{(r)}-1)}{n^{(r-1)}(n^{(r-1)}-1)} = 1 - (f^{(r-1)} - w)\frac{2n^{(r-1)} - (f^{(r-1)} - w) - 1}{n^{(r-1)}(n^{(r-1)}-1)},$$

giving us

$$\begin{aligned} 1 - p_2^{(r)} &= (f^{(r-1)} - w)\frac{2n^{(r-1)} - (f^{(r-1)} - w) - 1}{n^{(r-1)}(n^{(r-1)}-1)} \\ &\le \frac{2}{n^{(r-1)} - 1} f^{(r-1)} \le \frac{2}{n - Cf - 2} f^{(r-1)}, \end{aligned}$$

and of course, for $r = 1$ this is the last inequality in

$$1 - p_2^{(1)} = 1 - \frac{n^{(1)}(n^{(1)}-1)}{n(n-1)} = \frac{2n - f - 1}{n(n-1)} f \le \frac{2}{n-1} f \le \frac{2}{n - Cf - 2} f,$$

which holds, so since $2m/(n - Cf - 2) \to 2\alpha$, we find that

$$\mathbb{E}[N^{(r)}] = m^{(r-1)}\Big(1 - p_2^{(r)}\Big) \le \frac{2m}{n - Cf - 2} f^{(r-1)} \le 3\alpha f^{(r-1)} = \frac{3\alpha_\epsilon}{1-\epsilon} f^{(r-1)}$$

holds for all $r \in [R]$ when n is large enough, and since $f^{(r-1)} \le \alpha_\epsilon^{r-1} f - (r-1)\alpha_\epsilon^{r-1} n^{3/8}$, we get

$$\mathbb{E}[N^{(r)}] \le \frac{3\alpha_\epsilon^r}{1-\epsilon} f - (r-1)\frac{3\alpha_\epsilon^r}{1-\epsilon} n^{3/8} \tag{B.4.40}$$

uniformly in r when n is large enough. Now, continuing our calculations from before and using (B.4.40), we get

$$\begin{aligned}\mathbb{P}\Big(m^{(r-1)} - M_2^{(r)} > \frac{3\alpha_\epsilon^r}{1-\epsilon}\big(f + n^{3/8}\big)\Big) &= \mathbb{P}\Big(N^{(r)} > \frac{3\alpha_\epsilon^r}{1-\epsilon}f + \frac{3\alpha_\epsilon^r}{1-\epsilon}n^{3/8}\Big)\\ &\le \mathbb{P}\Big(N^{(r)} > \mathbb{E}[N^{(r)}] + r\frac{3\alpha_\epsilon^r}{1-\epsilon}n^{3/8}\Big)\end{aligned}$$

for all $r \in [R]$ as long as n is large enough. We are now in a position to apply Chernoff's bound (B.4.31), which will require a lower bound on $\mathbb{E}[N^{(r)}]$. For $r \ge 2$ we find that

$$\begin{aligned}1 - p_2^{(r)} &= \frac{2n^{(r-1)} - (f^{(r-1)} - w) - 1}{n^{(r-1)}(n^{(r-1)} - 1)}(f^{(r-1)} - w)\\ &\ge \frac{2(n - Cf) - f - 1}{2n^2} f^{(r-1)} \ge \frac{n - Cf}{2n^2} f^{(r-1)},\end{aligned}$$

where the first inequality holds when $r \in [R]$ and n is large enough due to (B.4.38), the last inequality holds for large enough n since of course $n - Cf \ge f + 1$ at some point, and by verification the inequality also holds for $r = 1$. Further, if $r \in [R]$ and n is large enough we get $f^{(r-1)} \ge f/(2n^{1/16})$ from (B.4.37), and thus

$$\mathbb{E}[N^{(r)}] = m^{(r-1)}(1 - p_2^{(r)}) \ge \frac{(m - C'f)(n - Cf)}{2n^2} \cdot \frac{f}{2n^{1/16}} \ge \frac{\alpha_\epsilon f}{4n^{1/16}}$$

for all $r \in [R]$ when n is large enough, where the last inequality holds because

$$\lim_{n\to\infty} \frac{(m - C'f)(n - Cf)}{n^2} = \alpha.$$

Now, using the above lower bound on $\mathbb{E}[N^{(r)}]$, we get for the following choice of δ:

$$\delta = \frac{3r\alpha_\epsilon^r n^{3/8}}{(1-\epsilon)\,\mathbb{E}[N^{(r)}]} \le \frac{12Rn^{7/16}}{(1-\epsilon)f} \longrightarrow 0 \quad \text{as } n \to \infty,$$

and hence $\delta < 1$ for all $r \in [R]$ when n is large enough. Chernoff's bound (B.4.31) gives

$$\mathbb{P}\Big(N^{(r)} > \mathbb{E}[N^{(r)}] + r\frac{3\alpha_\epsilon^r}{1-\epsilon}n^{3/8}\Big) \le \exp\Big(\frac{-3r^2\alpha_\epsilon^{2r}n^{3/4}}{(1-\epsilon)^2\,\mathbb{E}[N^{(r)}]}\Big).$$

From (B.4.40) it follows that $\mathbb{E}[N^{(r)}] \le (3\alpha_\epsilon^r f)/(1-\epsilon)$, and inserting this yields the first inequality in:

$$\exp\Big(\frac{-3r^2\alpha_\epsilon^{2r}n^{3/4}}{(1-\epsilon)^2\,\mathbb{E}[N^{(r)}]}\Big) \le \exp\Big(\frac{-r^2\alpha_\epsilon^r n^{3/4}}{(1-\epsilon)f}\Big) \le \exp\Big(\frac{-n^{11/16}}{f}\Big),$$

and the second inequality follows from (B.4.36) and the fact that $r \geq 1$ and $1-\epsilon \leq 1$. The above inequality holds for all $r \in [R]$ when n is large enough. Putting it all together, we conclude that

$$\sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < m^{(r)}\Big) \leq R \exp\bigg(\frac{-n^{11/16}}{f}\bigg) \longrightarrow 0 \quad \text{as } n \to \infty,$$

proving (U4) and hence also finishing the proof of the case $k = 2$ in Theorem B.2 when $\alpha > 0$.

B.4.5 The random mixed 1- and 2-SAT problem

In this section, we give a proof of Theorem B.5, which follows quite readily from the part of Theorem B.2 that we have just proved. Remember that $n \to \infty$, $f/\sqrt{n} \to \beta$, and $m/n \to \alpha$, where $\beta \in [0, \infty]$ and $\alpha \in (0,1)$. We are considering a random 2-CNF formula Φ_2 with m clauses and n variables and a random 1-CNF formula Φ_1 with f clauses and n variables, such that Φ_2 and Φ_1 are independent. Let $\mathcal{L}_1 = \{L_1, L_2, \ldots, L_f\}$ denote the set of the random literals defining Φ_1. From (B.3.4) we get

$$\Phi_2 \wedge \Phi_1 \in \mathsf{SAT} \iff \Phi_1 \in \mathsf{SAT} \quad \text{and} \quad (\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}.$$

Let $\mathcal{L} := [n] \setminus [n-f]$ so that $|\mathcal{L}| = f \geq |\mathcal{L}_1|$, and let $\mathcal{B}$ denote the set of all satisfiable 1-CNF formulas with n variables and at most f clauses. We get from the above and Lemma B.8 that

$$\begin{aligned}
\mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT}) &= \mathbb{P}(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}((\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT} \mid \Phi_1 = \varphi)\, \mathbb{P}(\Phi_1 = \varphi) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}((\Phi_2)_{\varphi} \in \mathsf{SAT})\, \mathbb{P}(\Phi_1 = \varphi) \\
&\geq \mathbb{P}((\Phi_2)_{\mathcal{L}} \in \mathsf{SAT})\, \mathbb{P}(\Phi_1 \in \mathsf{SAT}) \\
&\longrightarrow \exp\bigg(\frac{-\beta^2 \alpha}{4(1-\alpha)}\bigg) \exp\bigg(\frac{-\beta^2}{4}\bigg) \quad (\text{as } n \to \infty) \\
&= \exp\bigg(\frac{-\beta^2}{4(1-\alpha)}\bigg),
\end{aligned}$$

where the convergence comes from the first part of Theorem B.2 and Lemma B.12 respectively.

Now, to get a corresponding upper bound on $\mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT})$ we need a lower bound on $|\mathcal{L}_1|$, i.e. we need to bound the number of duplicates in the random literals defining Φ_1. We get from Lemma B.11 that $|\mathcal{L}_1| \geq f - \lfloor n^{1/4} \rfloor$ with probability tending towards 1. Now put $\mathcal{L}' := [n]\setminus[n-(f-\lfloor n^{1/4}\rfloor)]$ so that $|\mathcal{L}'| = f-\lfloor n^{1/4}\rfloor$, and we repeat the argument from above: let $\mathcal{B}$ denote the set of all satisfiable 1-CNF formulas with n variables and at least $f-\lfloor n^{1/4}\rfloor$ clauses. Then

$$\begin{aligned}\mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT}) = {} & \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}, |\mathcal{L}_1| \geq f - \lfloor n^{1/4}\rfloor\Big) \\ & + \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}, |\mathcal{L}_1| < f - \lfloor n^{1/4}\rfloor\Big),\end{aligned}$$

where of course the second term vanishes, and using Lemma B.8:

$$\begin{aligned}& \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}, |\mathcal{L}_1| \geq f - \lfloor n^{1/4}\rfloor\Big) \\ = & \sum_{\varphi\in\mathcal{B}} \mathbb{P}((\Phi_2)_{\varphi} \in \mathsf{SAT})\,\mathbb{P}(\Phi_1 = \varphi) \\ \leq & \,\mathbb{P}((\Phi_2)_{\mathcal{L}'} \in \mathsf{SAT}) \sum_{\varphi\in\mathcal{B}} \mathbb{P}(\Phi_1 = \varphi) \\ \leq & \,\mathbb{P}((\Phi_2)_{\mathcal{L}'} \in \mathsf{SAT})\,\mathbb{P}(\Phi_1 \in \mathsf{SAT}) \\ \to & \exp\left(\frac{-\beta^2}{4(1-\alpha)}\right), \quad \text{as } n \to \infty,\end{aligned}$$

using in the end Theorem B.2, since $|\mathcal{L}'|/\sqrt{n} \to \beta$, and Lemma B.12. This completes the proof of Theorem B.5, except for the case $\alpha = 0$, which may be proved as follows: let Ψ_2 be a random 2-CNF formula with $\lfloor \epsilon n\rfloor$ clauses and n variables. Then by Lemma B.9,

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT}) \geq \liminf_{n\to\infty} \mathbb{P}(\Psi_2 \wedge \Phi_1 \in \mathsf{SAT}) = \exp\left(\frac{-\beta^2}{4(1-\epsilon)}\right),$$

and

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_2 \wedge \Phi_1 \in \mathsf{SAT}) \leq \limsup_{n\to\infty} \mathbb{P}(\Phi_1 \in \mathsf{SAT}) = \exp\left(\frac{-\beta^2}{4}\right),$$

so taking $\epsilon \to 0$ yields the desired result.

B.4.6 Sublinear number of binary clauses

The only thing missing from a proof of Theorem B.2 in the case $k = 2$ is the verification of

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^2},$$

where Φ is a random 2-CNF formula with $m = m(n)$ clauses and n variables satisfying $m \to \infty$ and $m/n \to 0$, and $\mathcal{L} \subseteq \pm[n]$ is a consistent set of literals with $|\mathcal{L}| = f = f(n)$ such that $f\sqrt{m}/n \to \gamma$. We may assume without loss of generality that $\gamma \in (0,\infty)$, as the cases $\gamma = 0$ and $\gamma = \infty$ then follow by an application of Lemma B.9, as we have shown in similar situations previously. Let $(M_h)_{h\in K}$ be the random variables defined in (B.3.6). As usual we assume without loss of generality that $\mathcal{L} = [n] \setminus [n-f]$, so we get

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}\Big(M_0 = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big)$$

from (B.3.8), and from Lemma B.10:

$$\mathbb{E}[M_0] = m\frac{f(f-1)}{4n(n-1)} = \left(\frac{1}{2}\cdot\frac{f\sqrt{m}}{n}\right)^2 \frac{f-1}{f}\cdot\frac{n}{n-1} \longrightarrow \left(\frac{\gamma}{2}\right)^2,$$

meaning that M_0 is asymptotically Poisson distributed with mean $(\gamma/2)^2$, yielding

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \le \mathbb{P}(M_0 = 0) \longrightarrow e^{-(\gamma/2)^2}.$$

This leaves the lower bound. By the exact same arguments as those leading up to (B.4.15), we get

$$\begin{aligned}&\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})\\ \ge\,&\mathbb{P}(\Phi_1 \in \mathsf{SAT})\,\mathbb{P}((\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT})\,\mathbb{P}(M_0 = 0)\,\mathbb{P}(M_1 \le f_1 | M_0 = 0),\end{aligned}$$

where

$$f_1 := \left\lfloor 2\gamma\sqrt{m} + m^{3/8}\right\rfloor,$$

and Φ_1 is a random 1-CNF formula with f_1 clauses and $n_1 := n - f$ variables, Φ_2 is a random 2-CNF formula with m clauses and n_1 variables, and lastly $\mathcal{L}_1 := [n_1] \setminus [n_1 - f_1]$. Of course, we still have $\mathbb{P}(M_0 = 0) \to e^{-(\gamma/2)^2}$, so we need to show that the other factors tend towards 1. We notice that

$$\frac{f}{n} = \frac{1}{\sqrt{m}}\cdot\frac{f\sqrt{m}}{n} \longrightarrow 0,$$

since $m \to \infty$, so $n_1/n \to 1$, and $f_1/\sqrt{m} \to 2\gamma$, thus

$$\frac{f_1}{\sqrt{n_1}} = \frac{f_1}{\sqrt{m}}\sqrt{\frac{m}{n}}\sqrt{\frac{n}{n_1}} \longrightarrow 0,$$

and with this Lemma B.12 gives $\mathbb{P}(\Phi_1 \in \mathsf{SAT}) \to 1$, and Lemma B.13 gives $\mathbb{P}((\Phi_2)_{\mathcal{L}_1} \in \mathsf{SAT}) \to 1$. Next, M_1 has a binomial distribution with parameters m and

$$p_{1|0} := \frac{f(n-f)}{n(n-1) - \frac{1}{4}f(f-1)}$$

given $M_0 = 0$, again by Lemma B.10. Let $N \sim \text{Binom}(m, p_{1|0})$, and notice that

$$\begin{aligned}\mathbb{E}[N] &= \frac{mf(n-f)}{n(n-1)-\frac{1}{4}f(f-1)} \\ &= \frac{f\sqrt{m}}{n}\cdot\frac{n-f}{n}\cdot\frac{n^2}{n(n-1)-\frac{1}{4}f(f-1)}\sqrt{m},\end{aligned}$$

so since

$$\lim_{n\to\infty}\left[\frac{f\sqrt{m}}{n}\cdot\frac{n-f}{n}\cdot\frac{n^2}{n(n-1)-\frac{1}{4}f(f-1)}\right] = \gamma,$$

we conclude that

$$\tfrac{1}{2}\gamma\sqrt{m} \le \mathbb{E}[N] \le 2\gamma\sqrt{m}$$

when n is large enough. In particular, we have

$$\delta = \frac{m^{3/8}}{\mathbb{E}[N]} \le \frac{2}{\gamma m^{1/8}} < 1$$

for large enough n, so applying Chernoff's bound (B.4.31) yields:

$$\begin{aligned}\mathbb{P}(M_1 > f_1 | M_0 = 0) &= \mathbb{P}(N > f_1) \\ &= \mathbb{P}\Big(N > 2\gamma\sqrt{m} + m^{3/8}\Big) \\ &\le \mathbb{P}\Big(N > \mathbb{E}[N] + m^{3/8}\Big) \\ &\le \exp\left(\frac{-m^{3/4}}{3\,\mathbb{E}[N]}\right) \\ &\le \exp\left(\frac{-m^{1/4}}{6\gamma}\right) \longrightarrow 0\end{aligned}$$

as $n \longrightarrow \infty$, finishing the proof.

B.4.7 Random 3-SAT

We are able to prove Theorem B.2 directly in the case $k = 3$ (without assuming $\alpha > 0$). The proof in this section will follow along the same lines as before, but it is a bit more notationally heavy than in the case $k = 2$, as there are now, in addition to 0-, 1-, and 2-clauses, also 3-clauses appearing, but it is mathematically more elementary, since the decomposition (B.3.9) only occurs three times, so there are no infinite series to deal with. We seek to prove that

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = e^{-(\gamma/2)^3},$$

where Φ is a random 3-CNF formula with $m = m(n)$ clauses and n variables, $\mathcal{L} \subseteq \pm[n]$ is a consistent set of literals with $|\mathcal{L}| = f = f(n)$, and $m \to \infty$, $m/n \to \alpha$, and $fm^{1/3}/n \to \gamma$ as $n \to \infty$, where $\alpha \in [0, 3.145)$ and $\gamma \in [0, \infty]$. Let $\mathcal{C} := (\mathcal{C}_h^{(1)})_{h\in K}$, and $(M_h^{(1)})_{h\in K}$ denote the random functions defined in eq. (B.3.6), where $K := \{0, 1, 2, 3, \star\}$. Assume without loss of generality that $\mathcal{L} = [n] \setminus [n - f]$ and $\gamma \in (0, \infty)$.

From (B.3.9) we have

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}\Big(M_0^{(1)} = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}\Big),$$

and from Lemma B.10 it follows that $M_0^{(1)}$ is Binomially distributed with mean

$$\mathbb{E}[M_0^{(1)}] = m\frac{f(f-1)(f-2)}{8n(n-1)(n-2)} \longrightarrow \frac{\gamma^3}{8},$$

so $M_0^{(1)}$ is asymptotically Poisson-distributed with mean $(\gamma/2)^3$, and thus

$$\lim_{n\to\infty} \mathbb{P}(M_0^{(1)} = 0) = e^{-(\gamma/2)^3},$$

which immediately yields the correct upper bound for the limit $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})$.

For the lower bound we apply the same line of reasoning as in the lower bound in the case $k = 2$. Define

$$f^{(1)} := \Big\lfloor \gamma^2 m^{1/3} + m^{1/5} \Big\rfloor \quad \text{and} \quad m^{(1)} := \Big\lfloor 2\gamma m^{2/3} + m^{2/5} \Big\rfloor.$$

We have

$$\begin{aligned} &\mathbb{P}\Big(M_0^{(1)} = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}\Big) \\ &\quad \geq \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}\Big) \\ &\quad = \mathbb{E}\Big[\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big)\mathbb{1}_{\{M_0^{(1)}=0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\}}\Big]. \end{aligned}$$

When working under the measure $\mathbb{P}(\cdot|\mathcal{C})$ in the following we will assume that we are on the event $\{M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\}$. By the exact same argument as in (B.4.14) we get

$$\begin{aligned} &\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\ &\geq \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big), \end{aligned}$$

where $\Phi_1^{(1)}$ is a random 1-CNF formula with $f^{(1)}$ clauses and $n^{(1)} := n - f$ variables, $\Phi_2^{(1)}$ is a random 2-CNF formula with $m^{(1)}$ clauses and $n^{(1)}$ variables, and $\Phi_3^{(1)}$ is a random 3-CNF formula with m clauses and $n^{(1)}$ variables such that (the clauses of) $\Phi_2^{(1)}$ and $\Phi_3^{(1)}$ are independent, and finally $\mathcal{L}^{(1)} := [n^{(1)}] \setminus [n^{(1)} - f^{(1)}]$. Hence,

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big)\times \\ \times \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\Big).\end{aligned} \tag{B.4.41}$$

Lemma B.10 again tells us that both $M_1^{(1)}$ and $M_2^{(1)}$ are binomially distributed with parameters m and $p_1^{(1)}$ or $p_2^{(1)}$ respectively, where

$$p_1^{(1)} = \frac{3f(f-1)(n-f)}{4n(n-1)(n-2)}, \quad \text{and} \quad p_2^{(1)} = \frac{3f(n-f)(n-f-1)}{2n(n-1)(n-2)}.$$

A quick calculation shows that $\mathbb{E}[M_1^{(1)}]$ is asymptotic to $\frac{3}{4}\gamma^2 m^{1/3}$ and $\mathbb{E}[M_2^{(1)}]$ is asymptotic to $\frac{3}{2}\gamma m^{2/3}$ as $n \to \infty$. Thus, we can apply Chernoff's bound (B.4.31) to receive

$$\begin{aligned}\mathbb{P}\Big(M_1^{(1)} > f^{(1)}\Big) &\leq \mathbb{P}\Big(M_1^{(1)} > \mathbb{E}[M_1^{(1)}] + m^{1/5}\Big) \\ &\leq \exp\left(\frac{-m^{2/5}}{3\,\mathbb{E}[M_1^{(1)}]}\right) \leq \exp\left(\frac{-m^{1/15}}{3\gamma^2}\right),\end{aligned}$$

where the first and last inequality holds for large enough n, so that $M_1^{(1)} \leq f^{(1)}$ w.h.p. By a similar argument we see that $M_2^{(1)} \leq m^{(1)}$ w.h.p. This means that

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\Big) = e^{-(\gamma/2)^3},$$

so it remains only to show that the other factors in (B.4.41) tend towards 1 as $n \to \infty$. We notice that

$$\frac{f}{n} = \frac{f m^{1/3}}{n} \cdot \frac{1}{m^{1/3}} \longrightarrow 0,$$

so $n^{(1)}/n \to 1$, and thus

$$\frac{f^{(1)}}{\sqrt{n^{(1)}}} = \frac{f^{(1)}}{\sqrt{m}}\sqrt{\frac{m}{n}}\sqrt{\frac{n}{n^{(1)}}} \longrightarrow 0.$$

Lemma B.12 thus gives $\mathbb{P}(\Phi_1^{(1)} \in \mathsf{SAT}) \to 1$.

Looking at the final factor, let for each $h \in K$ $M_h^{(2)}(2)$ denote the set of $j \in [m^{(1)}]$ for which the j'th clause of $\Phi_2^{(1)}$ becomes a h-clause when fixing the variables dictated by $\mathcal{L}^{(1)}$ (cf. (B.3.6)), and let $M_h^{(2)}(3)$ denote the corresponding set for $\Phi_3^{(1)}$. Put

$$M_h^{(2)} := M_h^{(2)}(2) + M_h^{(2)}(3),$$

where the two terms are seen to be independent. As before we are able to make the following decomposition:

$$\mathbb{P}\Big((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big) \geq \mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(2)} \wedge \Phi_3^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big)\times \\ \times \mathbb{P}\Big(M_0^{(2)} = 0, M_1^{(2)} \leq f^{(2)}, M_2^{(2)} \leq m^{(2)}\Big),$$

where

$$n^{(2)} := n^{(1)} - f^{(1)}, \qquad f^{(2)} := \lfloor m^{1/5} \rfloor,$$
$$m^{(2)} := \lfloor 3\gamma m^{2/3} + m^{2/5} \rfloor, \qquad \mathcal{L}^{(2)} := [n^{(2)}] \setminus [n^{(2)} - f^{(2)}],$$

and $\Phi_1^{(2)}$ is a random 1-CNF formula with $f^{(2)}$ clauses and $n^{(2)}$ variables, $\Phi_2^{(2)}$ is a random 2-CNF formula with $m^{(2)}$ clauses and $n^{(2)}$ variables, and $\Phi_3^{(2)}$ is a random 3-CNF formula with m clauses and $n^{(2)}$ variables such that (the clauses of) $\Phi_2^{(2)}$ and $\Phi_3^{(2)}$ are independent.

As before $f^{(2)}/\sqrt{n^{(2)}} \to 0$, so Lemma B.12 gives $\mathbb{P}(\Phi_1^{(2)} \in \mathsf{SAT}) \to 1$. Looking at Lemmas B.10, a quick calculation shows that $\mathbb{E}[M_0^{(2)}(2)]$ is asymptotic to $\frac{1}{2}\gamma^5\alpha^{4/3}n^{-2/3} \to 0$, and $\mathbb{E}[M_0^{(2)}(3)]$ is asymptotic to $\frac{1}{8}\gamma^6\alpha^2 n^{-1} \to 0$, and it follows that $M_0^{(2)} = 0$ w.h.p. by an application of Markov's inequality:

$$\mathbb{P}\Big(M_0^{(2)} > 0\Big) \leq \mathbb{E}[M_0^{(2)}] \longrightarrow 0.$$

Next, we find that $\mathbb{E}[M_1^{(2)}(2)] \to 2\gamma^3\alpha$ and $\mathbb{E}[M_1^{(2)}(3)]$ is asymptotic to $\frac{3}{4}\gamma^4\alpha^{5/3}n^{-1/3} \to 0$, so $M_1^{(2)} \leq f^{(2)}$ w.h.p. again by Markov's inequality:

$$\mathbb{P}\Big(M_1^{(2)} > f^{(2)}\Big) \leq \frac{\mathbb{E}[M_1^{(2)}]}{f^{(2)}} \longrightarrow 0.$$

Lastly, $\mathbb{E}[M_2^{(2)}(2)]$ is asymptotic to $2\gamma m^{2/3}$ and $\mathbb{E}[M_2^{(2)}(3)]$ is asymptotic to $\frac{3}{2}\gamma^2\alpha m^{1/3}$, so $\mathbb{E}[M_2^{(2)}] \leq 3\gamma m^{2/3}$ for large enough n, and Chernoff's inequality (B.4.31) yields

$$\mathbb{P}\Big(M_2^{(2)} > m^{(2)}\Big) \leq \mathbb{P}\Big(M_2^{(2)} > \mathbb{E}[M_2^{(2)}] + m^{2/5}\Big) \\ \leq \exp\left(\frac{-m^{4/5}}{3\,\mathbb{E}[M_2^{(2)}]}\right) \leq \exp\left(\frac{-m^{2/15}}{9\gamma^2}\right),$$

and thus $M_2^{(2)} \leq m^{(2)}$ w.h.p. Hence, we are only missing a verification of the fact that $(\Phi_2^{(2)} \wedge \Phi_3^{(2)})_{\mathcal{L}^{(2)}}$ is satisfiable w.h.p. We make the final decomposition:

$$\mathbb{P}\Big((\Phi_2^{(2)} \wedge \Phi_3^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big) \\ \geq \mathbb{P}\Big(\Phi_2^{(3)} \wedge \Phi_3^{(3)} \in \mathsf{SAT}\Big)\mathbb{P}\Big(M_0^{(3)} = 0, M_1^{(3)} = 0, M_2^{(3)} \leq m^{(3)}\Big),$$

where $n^{(3)} := n^{(2)} - f^{(2)}$ and $m^{(3)} := \lfloor 4\gamma m^{2/3} + m^{2/5} \rfloor$, $\Phi_2^{(3)}$ is a random 2-CNF formula with $m^{(3)}$ clauses and $n^{(3)}$ variables, and $\Phi_3^{(3)}$ is a random 3-CNF formula with m clauses and $n^{(3)}$ variables such that (the clauses of) $\Phi_2^{(3)}$ and $\Phi_3^{(3)}$ are independent (this corresponds to taking $f^{(3)} := 0$).

We see that $\mathbb{E}[M_0^{(3)}(2)]$ is asymptotic to $\frac{3}{4}\gamma\alpha^{16/15}n^{-14/15} \to 0$, and $\mathbb{E}[M_0^{(3)}(3)]$ is asymptotic to $\frac{1}{8}\alpha^{8/5}n^{-7/5} \to 0$, so $M_0^{(3)} = 0$ w.h.p. Similarly $\mathbb{E}[M_1^{(3)}(2)]$ is asymptotic to $3\gamma\alpha^{13/15}n^{-2/15} \to 0$, and $\mathbb{E}[M_1^{(3)}(3)]$ is asymptotic to $\frac{3}{4}\alpha^{7/5}n^{-3/5} \to 0$, so again $M_1^{(3)} = 0$ w.h.p. Finally, $\mathbb{E}[M_2^{(3)}(2)]$ is asymptotic to $3\gamma m^{2/3}$ and $\mathbb{E}[M_2^{(3)}(3)]$ is asymptotic to $\frac{3}{2}\alpha m^{1/5}$, so $\mathbb{E}[M_2^{(3)}] \leq 4\gamma m^{2/3}$ for large enough n, and by Chernoff's inequality we find that $M_2^{(3)} \leq m^{(3)}$ w.h.p.

The final step in the proof is to show that the mixed formula $\Phi_2^{(3)} \wedge \Phi_3^{(3)}$ is satisfiable w.h.p. Since $m/n \to \alpha$, $m^{(3)}/m^{2/3} \to 4\gamma$, and $n^{(3)}/n \to 1$, it follows that $m^{(3)} \leq \lfloor 10^{-6} n_3 \rfloor$ for large enough n. It further holds that $m/n^{(3)} \to \alpha < 3.145$, so $m \leq \lfloor 3.145 n^{(3)} \rfloor$ for large enough n. Let Ψ denote a random mixed CNF formula with $n^{(3)}$ variables, $\lfloor 10^{-6} n^{(3)} \rfloor$ 2-clauses, and $\lfloor 3.145 n^{(3)} \rfloor$ 3-clauses. It follows from Lemma B.9 that

$$\liminf_{n\to\infty} \mathbb{P}\left(\Phi_2^{(3)} \wedge \Phi_3^{(3)} \in \mathsf{SAT}\right) \geq \liminf_{n\to\infty} \mathbb{P}(\Psi \in \mathsf{SAT}).$$

From the first lines in the proof of Theorem 1 in [Ach00] it follows that $\liminf_{n\to\infty} \mathbb{P}(\Psi \in \mathsf{SAT}) > 0$, and it then follows from Theorem 2 from [Ach+01] that Ψ is satisfiable w.h.p., completing the proof of our Theorem B.2.

B.4.8 The random mixed 1- and 3-SAT problem

The final part is the proof of Theorem B.5 in the case $k = 3$. Thus, we again have $n \to \infty$, and we let Φ_3 denote a random 3-CNF formula with m clauses and n variables, such that $m/n \to \alpha$ for some $\alpha \in [0, 3.145)$, and let Φ_1 denote a random 1-CNF formula with f clauses and n variables, such that $f/\sqrt{n} \to \beta$ for some $\beta \in [0, \infty]$, where Φ_3 and Φ_1 are independent. Then we immediately have

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_3 \wedge \Phi_1 \in \mathsf{SAT}) \leq \limsup_{n\to\infty} \mathbb{P}(\Phi_1 \in \mathsf{SAT}) = e^{-(\beta/2)^2}$$

from Lemma B.9 and Lemma B.12.

To obtain the corresponding lower bound, we first note from (B.3.4) that

$$\Phi_3 \wedge \Phi_1 \in \mathsf{SAT} \iff \Phi_1 \in \mathsf{SAT} \quad \text{and} \quad (\Phi_3)_{\Phi_1} \in \mathsf{SAT}.$$

Let $\mathcal{L} := [n] \setminus [n-f]$ and note that Φ_1 will always have at most $f = |\mathcal{L}|$ distinct clauses. Thus, letting $\mathcal{B}$ denote the set of all satisfiable 1-CNF formulas with n

variables and at most f (distinct) clauses, we get from the above and Lemma B.8 that

$$\begin{aligned}
\mathbb{P}(\Phi_3 \wedge \Phi_1 \in \mathsf{SAT}) &= \mathbb{P}(\Phi_1 \in \mathsf{SAT}, (\Phi_3)_{\Phi_1} \in \mathsf{SAT}) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}((\Phi_3)_{\Phi_1} \in \mathsf{SAT} \mid \Phi_1 = \varphi)\, \mathbb{P}(\Phi_1 = \varphi) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}((\Phi_3)_{\varphi} \in \mathsf{SAT})\, \mathbb{P}(\Phi_1 = \varphi) \\
&\geq \mathbb{P}((\Phi_3)_{\mathcal{L}} \in \mathsf{SAT})\, \mathbb{P}(\Phi_1 \in \mathsf{SAT}) \\
&\longrightarrow e^{-(\beta/2)^2} \quad \text{as } n \to \infty,
\end{aligned}$$

where we in the end use Lemma B.12 and Theorem B.2. This concludes the proof of Theorem B.5 and thus the entire article.

References

[Ach+01] Dimitris Achlioptas et al. "Rigorous results for random $(2+p)$-SAT". In: *Theoret. Comput. Sci.* 265.1-2 (2001), pp. 109–129.

[Ach+21] Dimitris Achlioptas et al. "The number of satisfying assignments of random 2-SAT formulas". In: *Random Structures Algorithms* 58.4 (2021), pp. 609–647.

[Ach00] Dimitris Achlioptas. "Setting 2 variables at a time yields a new lower bound for random 3-SAT (extended abstract)". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC '00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 28–37.

[AS00] Dmitris Achioptas and Gregory B. Sorkin. "Optimal myopic algorithms for random 3-SAT". In: *Proceedings 41st Annual Symposium on Foundations of Computer Science*. FOCS '00. USA: IEEE Computer Society, 2000, pp. 590–600.

[BFU93] Andrei Z. Broder, Alan M. Frieze, and Eli Upfal. "On the satisfiability and maximum satisfiability of random 3-CNF formulas". In: *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '93. Austin, Texas, USA: Society for Industrial and Applied Mathematics, 1993, pp. 322–330.

[BHM21] Armin Biere, Marijn Heule, and Hans van Maaren, eds. *Handbook of Satisfiability*. Washington, DC: IOS Press, 2021.

[BMW00] Giulio Biroli, Rémi Monasson, and Martin Weigt. "A variational description of the ground state structure in random satisfiability problems". In: *Eur. Phys. J. B* 14 (2000), pp. 551–568.

[Bol+01] Béla Bollobás et al. "The scaling window of the 2-SAT transition". In: *Random Structures Algorithms* 18.3 (2001), pp. 201–256.

[Cha+24] Arnab Chatterjee et al. *The number of random 2-SAT solutions is asymptotically log-normal*. 2024.

[CKT91] Peter Cheeseman, Bob Kanefsky, and William M. Taylor. "Where the *really* hard problems are". In: *Proceedings of the 12th International Joint Conference on Artificial Intelligence - Volume 1*. IJCAI'91. Sydney, New South Wales, Australia: Morgan Kaufmann Publishers Inc., 1991, pp. 331–337.

[Coo71] Stephen A. Cook. "The Complexity of Theorem-Proving Procedures". In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC '71. 1971, pp. 151–158.

[CR92] Vašek Chvátal and Bruce Reed. "Mick gets some (the odds are on his side) (satisfiability)". In: *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science.* SFCS '92. USA: IEEE Computer Society, 1992, pp. 620–627.

[DB97] Olivier Dubois and Yacine Boufkhad. "A general upper bound for the satisfiability threshold of random r-SAT formulae". In: *J. Algorithms* 24.2 (1997), pp. 395–420.

[DBM02] Olivier Dubois, Yacine Boufkhad, and Jacques Mandler. *Typical random* 3*-SAT formulae and the satisfiability threshold.* 2002.

[Día+09] Josep L. Díaz et al. "On the satisfiability threshold of formulas with three literals per clause". In: *Theoret. Comput. Sci.* 410.30-32 (2009), pp. 2920–2934.

[DSS22] Jian Ding, Allan Sly, and Nike Sun. "Proof of the satisfiability conjecture for large k". In: *Ann. of Math. (2)* 196.1 (2022), pp. 1–388.

[EF95] Abdelhakim El Maftouhi and Wenceslao Fernandez de la Vega. "On random 3-sat". In: *Combin. Probab. Comput.* 4.3 (1995), pp. 189–195.

[ER60] Paul Erdős and Alfréd Rényi. "On the evolution of random graphs". In: *Magyar Tud. Akad. Mat. Kutató Int. Közl.* 5 (1960), pp. 17–61.

[FP83] John Franco and Marvin Paull. "Probabilistic analysis of the Davis-Putnam procedure for solving the satisfiability problem". In: *Discrete Appl. Math.* 5.1 (1983), pp. 77–87.

[Fra84] John V. Franco. "Probabilistic analysis of the pure literal heuristic for the satisfiability problem". In: *Ann. Oper. Res.* 1 (1984), pp. 273–289.

[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.

[FS96] Alan Frieze and Stephen Suen. "Analysis of two simple heuristics on a random instance of k-SAT". In: *J. Algorithms* 20.2 (1996), pp. 312–355.

[GGW06] Aarti Gupta, Malay K. Ganai, and Chao Wang. "SAT-Based Verification Methods and Applications in Hardware Verification". In: *Formal Methods for Hardware Verification.* Ed. by Marco Bernardo and Alessandro Cimatti. Springer Berlin Heidelberg, 2006, pp. 108–143.

[Goe96a] Andreas Goerdt. "A Threshold for Unsatisfiability". In: *J. Comput. Syst. Sci.* 53.3 (1996), pp. 469–486.

[Goe96b] 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.

[Goe99] Andreas Goerdt. "A remark on random 2-SAT". In: *Discrete Appl. Math.* 96/97 (1999). The satisfiability problem (Certosa di Pontignano, 1996); Boolean functions, pp. 107–110.

[GW94] Ian P. Gent and Toby Walsh. "The SAT phase transition". In: *Proceedings of the 11th European Conference on Artificial Intelligence.* ECAI'94. USA: John Wiley & Sons, Inc., 1994, pp. 105–109.

[HS03] Mohammad Taghi Hajiaghayi and Gregory B. Sorkin. *The Satisfiability Threshold of Random* 3*-SAT Is at Least* 3.52. 2003.

[JSV00] Svante Janson, Yannis C. Stamatiou, and Malvina Vamvakari. "Bounding the unsatisfiability threshold of random 3-SAT". In: *Random Structures Algorithms* 17.2 (2000), pp. 103–116.

[Kam+95] Anil Kamath et al. "Tail bounds for occupancy and the satisfiability threshold conjecture". In: *Random Structures Algorithms* 7.1 (1995), pp. 59–80.

[Kap+07] Alexis C. Kaporis et al. "The unsatisfiability threshold revisited". In: *Discrete Appl. Math.* 155.12 (2007), pp. 1525–1538.

[Kir+98] Lefteris M. Kirousis et al. "Approximating the unsatisfiability threshold of random formulas". In: *Random Structures Algorithms* 12.3 (1998), pp. 253–269.

[KKL06] Alexis C. Kaporis, Lefteris M. Kirousis, and Efthimios G. Lalas. "The probabilistic analysis of a greedy satisfiability algorithm". In: *Random Structures Algorithms* 28.4 (2006), pp. 444–480.

[Knu15] Donald E Knuth. *The art of computer programming, Volume 4, Fascicle 6: Satisfiability.* Addison-Wesley Professional, 2015.

[Mar08] João Marques-Silva. "Practical applications of Boolean Satisfiability". In: *2008 9th International Workshop on Discrete Event Systems.* 2008, pp. 74–80.

[Mon+96] Rémi Monasson et al. "Phase transition and search cost in the $(2+p)$-SAT problem". In: *4th Workshop on Physics and Computation.* Boston, MA, 1996.

[Mon+99] Rémi Monasson et al. "$2+p$-SAT: relation of typical-case complexity to the nature of the phase transition". In: *Random Structures Algorithms* 15.3-4 (1999). Statistical physics methods in discrete probability, combinatorics, and theoretical computer science (Princeton, NJ, 1997), pp. 414–435.

[MZ98] Rémi Monasson and Riccardo Zecchina. "Tricritical points in random combinatorics: the $(2+p)$-SAT case". In: *J. Phys. A: Math* 31.46 (1998), pp. 9209–9217.

[Pap94] Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994, pp. xvi+523.

[SML96] Bart Selman, David G. Mitchell, and Hector J. Levesque. "Generating Hard Satisfiability Problems". In: *Artif. Intell.* 81 (1996), pp. 17–29.

[Ver99] Yann Verhoeven. "Random 2-SAT and unsatisfiability". In: *Inform. Process. Lett.* 72.3-4 (1999), pp. 119–123.

[ZG13] Guangyan Zhou and Zongsheng Gao. "A new upper bound for random $(2+p)$-SAT by flipping two variables". In: *Internat. J. Found. Comput. Sci.* 24.6 (2013), pp. 899–912.

[Zit99] Michele A. A. Zito. "Randomised Techniques in Combinatorial Algorithmics". PhD thesis. University of Warwick, 1999.

ARTICLE C

Degrees of Freedom for Critical Random 2-SAT

Andreas Basse-O'Connor[1], and Mette Skjøtt[1,2]

[1]Department of Mathematics, Aarhus University,
[2]Kvantify Aps

April 2025

Abstract: The random k-SAT problem serves as a model that represents the 'typical' k-SAT instances. This model is thought to undergo a phase transition as the clause density changes, and it is believed that the random k-SAT problem is primarily difficult to solve near this critical phase. In this paper, we introduce a weak formulation of degrees of freedom for random k-SAT problems and demonstrate that the critical random 2-SAT problem has $\sqrt[3]{n}$ degrees of freedom. This quantity represents the maximum number of variables that can be assigned truth values without affecting the formula's satisfiability. Notably, the value of $\sqrt[3]{n}$ differs significantly from the degrees of freedom in random 2-SAT problems sampled below the satisfiability threshold, where the corresponding value equals $\sqrt{n}$. Thus, our result underscores the significant shift in structural properties and variable dependency as satisfiability problems approach criticality.

C.1 Introduction

C.1.1 Background and motivation

The Boolean satisfiability problem (SAT) is a highly studied topic in computer science, notable for being the first problem proven to be NP-complete, see [Coo71]. Its versatility extends beyond theoretical interest, with practical applications in areas like artificial intelligence, software verification, and optimization (see [Mar08; GGW06; Knu15], and references therein). In recent years, SAT has also attracted significant attention in the fields of discrete probability and statistical physics. This interdisciplinary interest arises because SAT exhibits behaviors, such as phase transitions, making it a compelling subject for studying threshold behavior in combinatorial structures.

A SAT instance is a Boolean function that evaluates multiple Boolean variables and returns a single Boolean value. The function is typically expressed in conjunctive normal form (CNF), meaning it is a conjunction (`and`) of disjunctions (`or`) of literals. Each literal represents a variable or its negation. A formula in which every clause contains exactly k literals is called a k-CNF formula. The following is an example of a 2-CNF formula with four variables and five clauses, where for $x \in \{\texttt{true}, \texttt{false}\}^4$ we define:

$$\varphi(x) = (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_3 \vee x_4) \wedge (\neg x_1 \vee \neg x_4) \wedge (x_2 \vee x_4).$$

The only assignment that makes the above formula evaluate to `true` is (`false`, `true`, `true`, `true`). The objective of the satisfiability problem is to determine whether such an assignment exists; if so, we write $\varphi \in \text{SAT}$. In the context of computational complexity theory, the 2-SAT problem is NL-complete, meaning it can be solved non-deterministically with logarithmic storage space and is one of the most difficult problems within this class (see Thm. 16.3 in [Pap94]). Consequently, a deterministic algorithm that solves 2-SAT using only logarithmic space would imply $L = NL$, which is a standing conjecture. Also, 2-SAT can be solved in polynomial time, while the k-SAT problem is NP-complete for $k \geq 3$, situating it at the core of the famous P vs. NP conjecture. Despite differences in computational complexity, the k-SAT problems for $k \geq 2$ have a lot of structural similarities.

In practical applications, SAT instances are, in most cases, easily solvable, which appears to contradict the problem's computational hardness. This observation inspired the development of the random k-SAT model, designed to generate typical SAT instances, see [Gol79; CKT+91; KS94; GW94]. In this model, the number of input variables n, clauses m, and the clause size k are fixed. Clauses are then sampled independently and uniformly from the $2^k\binom{n}{k}$ clauses with non-overlapping variables. This model is called the random k-SAT model, and the distribution is denoted $F_k(n, m)$. This model becomes particularly interesting when n and m grow large simultaneously. Specifically, by setting $m = \lfloor \alpha n \rfloor$, where $\alpha > 0$

represents the clause density, the random k-SAT problem is believed to undergo a phase transition: the asymptotic probability of satisfiability shifts from one to zero as α surpasses a critical threshold α_k, that is for $k \geq 2$,

$$\lim_{n\to\infty} \mathbb{P}\Big(F_k(n, \lfloor \alpha n \rfloor) \in \mathsf{SAT}\Big) = \begin{cases} 1, & \alpha < \alpha_k, \\ 0, & \alpha > \alpha_k. \end{cases} \tag{C.1.1}$$

A random k-SAT problem that is satisfiable w.h.p. is referred to as under-constrained, while it is called over-constrained when it is unsatisfiable w.h.p. Furthermore, when a phase transition exists, problems at this critical value are referred to as being critical.

As previously discussed, SAT problems are computationally challenging. Notably, it is near the expected phase transition of the random k-SAT model that the hardest instances are thought to arise, see [SML96]. Figure C.10 displays how a spike in computational hardness appears when the clause density approaches the expected phase transition. This highlights why understanding the behavior of random k-SAT in this critical region is of substantial theoretical and practical importance. More broadly, the study of random structures near critical transitions is a significant and complex area of research. The prominence of this field is underscored by the fact that three Fields Medals have been awarded since 2006 for groundbreaking work on critical phenomena, with recipients including H. Duminil-Copin, S. Smirnov, and W. Werner.

The phase transition phenomenon was in 1992 established for $k = 2$ in the articles [Goe96; CR92; La 01], where the authors independently established that $\alpha_2 = 1$. Recently, the sharp satisfiability conjecture (C.1.1) has been affirmatively verified for all $k \geq k_0$, with k_0 being a large and unknown constant, see [SSZ22]. The remaining cases of k constitute an open problem. In 1999, the result on random 2-SAT was further refined in [Bol+01] as the rate of convergence was determined. Additionally, it was shown that the asymptotic probability of satisfiability of a random critical 2-SAT problem is bounded away from both zero and one, though whether this probability converges remains an open question. Recent contributions to the random 2-SAT model have focused on the under-constrained regime, where both the expected number of solutions and a central limit theorem for this quantity (see [Ach+21; Cha+24]) has been established. Thus, while the phase transition of random 2-SAT was proven many years ago, ongoing research continues to uncover new insights into the model, and several open questions remain unresolved.

A recent study [BOS25] examined variable interactions by analyzing the *degrees of freedom* in under-constrained random k-SAT problems. This concept refers to the number of variables that can be fixed without impacting the formula's satisfiability. For under-constrained random 2-SAT problems, where $\alpha < 1$, the degrees

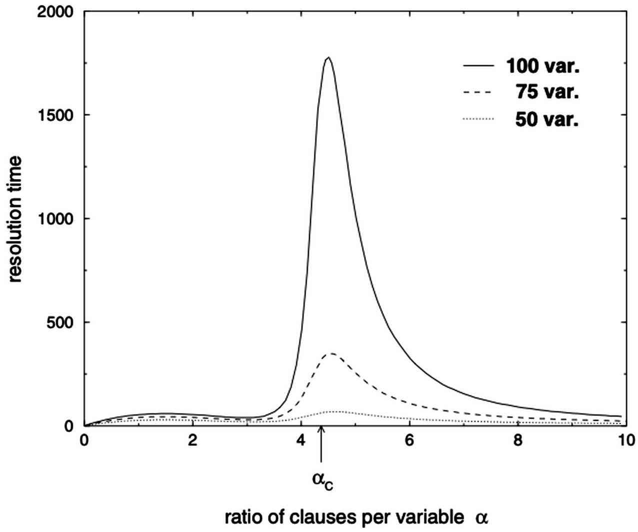


Figure C.10: Computational hardness of random 3-SAT as a function of clause density. The y-axis displays the median resolution time of 10,000 instances solved using the DPLL algorithm. This is figure 8.2 in [BCM02]

of freedom equal $n^{1/2}$, while in random 3-SAT problems well below the phase transition ($\alpha < 3.145$), the degrees of freedom equal $n^{2/3}$.

In this paper, we compute the degrees of freedom in *critical* 2-SAT problems. Our result shows that in this critical setting, the degrees of freedom decrease with a polynomial factor, scaling only as $n^{1/3}$. This finding underscores the emergence of complex structures near the phase transition, where variable interdependencies become significantly more pronounced. Thus, our results highlight this marked shift in variable correlation as random SAT problems approach criticality.

C.1.2 Main result

Consider a random 2-CNF formula Φ sampled at the phase-transition point of the random 2-SAT problem, where the asymptotic probability of satisfiability shifts from one to zero. We aim to determine how many input variables are free, that is, they can be assigned any value without effecting the asymptotic probability that the formula is satisfiable.

Let $\mathcal{L} \subseteq \pm[n] := \{-n, \dots, -1, 1, \dots, n\}$ be a set with $|\mathcal{L}| = f(n)$ elements, chosen such that if $\ell \in \mathcal{L}$, then $-\ell \notin \mathcal{L}$ (we say that $\mathcal{L}$ is *consistent*). This set $\mathcal{L}$ dictates the variables being fixed, having $x_v = \texttt{true}$ when $v \in \mathcal{L}$ and $x_v = \texttt{false}$ when $-v \in \mathcal{L}$. Formally, let $\mathbb{B} = \{\texttt{true}, \texttt{false}\}$. For $x \in \mathbb{B}^n$, we define $x_{\mathcal{L}} \in \mathbb{B}^n$ as the vector with $(x_{\mathcal{L}})_v = \texttt{true}$ when $v \in \mathcal{L}$, $(x_{\mathcal{L}})_v = \texttt{false}$ when $-v \in \mathcal{L}$, and $(x_{\mathcal{L}})_v = x_v$ for all other entries. We then consider

$$\Phi_{\mathcal{L}}(x) = \Phi(x_{\mathcal{L}}). \tag{C.1.2}$$

Note that $\Phi_{\mathcal{L}}$ denotes the mapping Φ with f variables fixed to values specified by $\mathcal{L}$. Our goal is to identify the threshold value of f that separates instances where $\Phi_{\mathcal{L}}$ remains solvable with positive probability from those where $\Phi_{\mathcal{L}}$ becomes unsatisfiable. To formalize this notion, we introduce the following definition, where we recall that $F_k(n, m)$ denotes a random k-CNF formula with n variables and m clauses.

Definition C.1. *The random k-SAT problem with clause density $\alpha > 0$ is said to have $f_\star(n)$ degrees of freedom weakly if, for $\Phi \sim F_k(n, \lfloor \alpha n \rfloor)$, every consistent subset $\mathcal{L} \subseteq \pm[n]$ with $|\mathcal{L}| = f(n)$, and for all $\varepsilon > 0$, the following holds:*

(1) Whenever $f = O(f_\star n^{-\varepsilon})$, then

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) > 0.$$

(2) Whenever $f = \Omega(f_\star n^{\varepsilon})$, then

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0.$$

Condition (1) states that fixing strictly fewer than $f_\star$ variables does not decrease the lower bound on the probability of satisfiability. On the other hand, condition (2) implies that when fixing strictly more than $f_\star$ variables, the problem becomes unsatisfied. This concept is a weaker form of the degrees of freedom notion introduced in [BOS25]; specifically, having $f_\star$ degrees of freedom implies having $f_\star$ degrees of freedom weakly. Note that $f_\star$ is unique up to sub-polynomial factors, meaning that if both $f_\star$ and $g_\star$ are weak degrees of freedom, then for any $\varepsilon > 0$, we have $f_\star n^{-\varepsilon} \le g_\star \le f_\star n^{\varepsilon}$ for sufficiently large n. Our main result is the following:

Theorem C.2. *The random critical 2-SAT problem has $n^{1/3}$ degrees of freedom weakly.*

We recall that *critical* refers to the situation with $\alpha = 1$. Figure C.11 shows simulations indicating that, as n increases, the curve representing the satisfiability of the random critical 2-SAT problem as a function of the number of fixed variables becomes increasingly steep. Moreover, this steepening behavior points to a cutoff occurring at $n^{1/3}$.

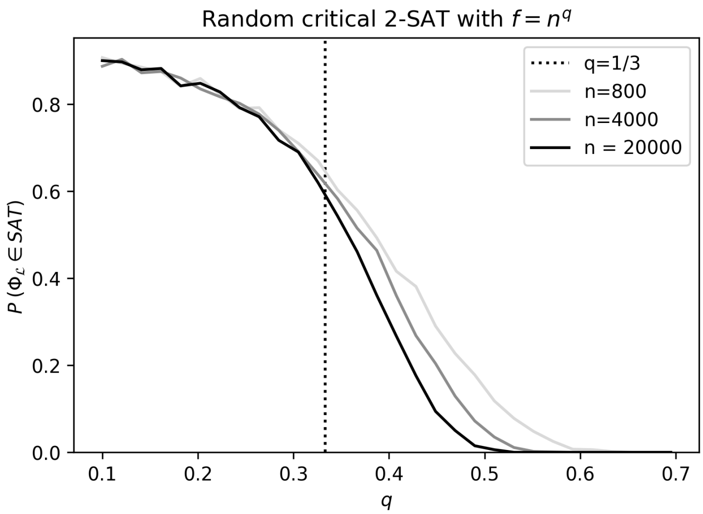


Figure C.11: Satisfiability of random critical 2-SAT as a function of the number of fixed variables. The different curves represent a varying number of input variables. Each data point is comprised of $2,000$ simulations. The vertical dotted line indicates $q = 1/3$.

C.1.3 Related work

In this section, we compare our results to related work, providing new insights and situating our findings within a broader context.

Remark C.3. *Theorem C.2 allows us to compare the critical random 2-SAT problem with general random k-SAT problems:*

- *The paper [BOS25] established that under-constrained random 2-SAT problems have $n^{1/2}$ degrees of freedom, which reveals a pronounced difference with the behavior observed at the critical phase-transition point. At this threshold, a dramatic reduction in degrees of freedom occurs, reflecting a fundamental shift in the underlying structure of the formula. This is not surprising, as at this critical ratio, the system is on the "knife edge" between being satisfiable versus unsatisfiable, and therefore, long-range correlations between variables are expected to appear. To our knowledge, our result is one of the first to indicate this drastic change in variable dependence.*
- *The paper [BOS25] also examines random 3-SAT problems, establishing that when α is significantly below the expected phase-transition threshold ($\alpha < 3.145$), the degrees of freedom are $n^{2/3}$. In comparison, our main theorem shows that the degrees of freedom in critical random 2-SAT equal the square*

root of this amount, indicating a notable contrast in variable flexibility between the two cases.

The computational hardness of the satisfiability problem implies that finding solutions to challenging SAT formulas often requires traversing a substantial portion of the search tree, that is, assigning truth values to variables sequentially and backtracking when encountering contradictions. This approach forms the core of the DPLL algorithm, introduced in 1962 as one of the first SAT-solving algorithms, [DLL62]. Decades later, in the 1990s, CDCL (Conflict-Driven Clause Learning) solvers transformed SAT solving, enabling the solution of instances with thousands or even millions of variables. Despite their modern enhancements, these solvers still rely on the simple procedure of assigning truth values (see p. 62 in [Knu15]). The concept of degrees of freedom quantifies how deep one can navigate in the search tree before a contradiction arises when solving a random SAT problem. Moreover, the drastic change in degrees of freedom when comparing under-constrained problems with critical problems highlights why computational complexity intensifies near the satisfiability threshold. This also aligns with the observations in Figure C.10, which displayed the computation time of the DPLL algorithm when approaching criticality.

Let again $\Phi \sim F_2(n,n)$, $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| = f(n)$, and remember that fixing variables corresponds to shrinking the input space. Thus, it is clear that $\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\} \subseteq \{\Phi \in \mathsf{SAT}\}$. This along with our main theorem implies that whenever $f = O(n^{1/3-\varepsilon})$ for an $\varepsilon > 0$ we have

$$\begin{aligned}\liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big) &\leq \liminf_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \\ &\leq \limsup_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \leq \limsup_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).\end{aligned} \tag{C.1.3}$$

Thus, if $\mathbb{P}(\Phi \in \mathsf{SAT})$ has a limit as $n \to \infty$, then $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT})$ also has a limit, and these two limits coincide. In [Bol+01] it is shown that for all $\delta > 0$ sufficiently small, there exists a $c_\delta > 0$ such that if $\Phi_\alpha \sim F_2(n, \lfloor \alpha n \rfloor)$ with $\alpha \in [1-c_\delta n^{-1/3}, 1+c_\delta n^{-1/3}]$, then

$$\delta \leq \mathbb{P}(\Phi_\alpha \in \mathsf{SAT}) \leq 1-\delta. \tag{C.1.4}$$

Moreover, this interval is the best possible in the sense that if a sufficiently large constant replaces c_δ, the statement becomes false. Combining (C.1.3) and (C.1.4) we get that for $\delta > 0$ small enough

$$\delta \leq \liminf_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \leq \limsup_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \leq 1-\delta,$$

so the limiting probability is bounded away from zero and one, and this interval is not larger than the corresponding interval for satisfiability when no variables are fixed. We observe that the length of the scaling window in [Bol+01] is on the order of $n^{-1/3}$, which is the reciprocal of the degrees of freedom for the critical 2-SAT problem. However, the proof presented in [Bol+01] differs from that of the current paper, and there is no direct coupling between the two results.

The main idea of the proof in [Bol+01] is to consider an order parameter for the phase transition of random 2-SAT. This is a concept often used in statistical physics and it refers to a function that vanishes on one side of a transition and becomes non-zero on the other side. The order parameter that they consider is the average size of the spine, where the spine of a CNF-formula φ is defined to be the set of literals ℓ for which there is a satisfiable sub-formula ψ of φ with $\psi \wedge \ell$ not satisfiable. By carefully controlling this quantity in a random CNF-formula as clauses are added one by one their result follows. Note that the size of the spine equals the number of variables that are free to be given any truth value without making a satisfiable SAT problem unsatisfiable. The spine only describes how each variable on its own affects the satisfiability of a CNF-formula. In contrast, we need to understand how all the fixed variables simultaneously impact the satisfiability of the formula. Multiple other papers, e.g. [CF86; Ach+01b; Ach+01a] also consider the procedure of fixing one single variable at a time, and in [Ach00] they consider fixing two variables at a time. This is different from the approach in the present paper where many variables are fixed simultaneously and hereby long implication chains emerge that intervene with each other and affect satisfiability.

As previously mentioned, the paper [BOS25] was the first to introduce and compute degrees of freedom in certain random under-constrained k-SAT problems. Their proof is based on the idea that fixing variables in a CNF-formula creates clauses of size one, also called unit-clauses. The presence of these unit-clauses, in turn, corresponds to further variable fixing. Thus, variables are fixed repeatedly in rounds, and the probability of encountering a contradiction in each round is calculated. The sequence describing the number of fixed variables throughout the rounds is then studied. This procedure is closely related to the unit-propagation algorithm, a well-studied technique used as a subroutine in most modern SAT solvers. We also base our proof on an appropriate adaptation of the unit propagation algorithm. In the under-constrained regime of random 2-SAT, it is possible to control the number of unit-clauses produced in each round r, and this number decreases exponentially at a rate of α, i.e. as α^r. However, at the phase transition, we have $\alpha = 1$, and thus the expected number of unit-clauses produced in each round remains approximately constant ($\alpha^r = 1$). As a result, controlling unit propagation becomes more challenging because the entire process must be analyzed as a whole, unlike in the under-constrained regime, where the rounds could be considered independently. This again suggests the presence of long-range correlations between variables when $\alpha = 1$. When $f = \Omega(n^{1/3+\varepsilon})$ for some $\varepsilon > 0$ the key idea is to show that the number of unit-clauses produced in each round remains high for a certain number of rounds w.h.p. This implies that a contradiction is likely to occur before the process terminates. On the other hand, when $f = O(n^{1/3-\varepsilon})$ for some $\varepsilon > 0$ we show that the sequence dies out w.h.p. before encountering a contradiction.

The results of [BOS25] extend further as they also determine the limiting satisfiability of the random SAT problem when $\Theta(f_\star)$ variables are fixed, where $f_\star$ represents the degrees of freedom of the random formula. In this setting, they show that the limiting probability remains bounded away from zero and one, and they provide the exact limiting value. By adjusting a parameter, this limiting value smoothly interpolates between the two edge cases. An open question is whether a similar result holds for the random critical 2-SAT problem. Specifically, it remains unknown what happens when $\Theta(n^{1/3})$ variables are fixed in such formulas, and whether the limiting probability will also interpolate between the edge cases.

C.2 Preliminaries

C.2.1 *Notation and conventions*

For any set $A \subseteq \mathbb{Z}$ we define $-A = \{-a : a \in A\}$, $\pm A = A \cup (-A)$ and we denote by $|A|$ the number of elements in A. For elements x_i, $i \in A$ belonging to some space we let $(x_a)_{a \in A}$ denote the vector $(x_{a_1}, \ldots, x_{a_{|A|}})$, where $\{a_1, \ldots, a_{|A|}\} = A$ and $a_1 < a_2 < \cdots < a_{|A|}$. Furthermore, for any $n, m \in \mathbb{N}$ with $m < n$ we let $[n] = \{1, \ldots, n\}$, $[m, n] = \{m, m+1, \ldots, n\}$, and $[0] = \emptyset$. The two sets $\mathbb{B} = \{\texttt{true}, \texttt{false}\}$ and $K = \{0, 1, 2, \star\}$ are also considered repeatedly. For an $x \in \mathbb{R}$ we let $x^+ = \max\{0, x\}$.

When considering random elements a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ will always be given. Whenever new random elements are introduced, unless specified otherwise, they are independent of all previously existing randomness. We define $\frac{0}{0} = 0$. As we will ultimately let n approach infinity, certain inequalities will hold only for sufficiently large n. In such cases, the required size of n for the inequality to hold may depend on q, where $f \sim n^q$, but it will always be independent of the round r. As has been the case thus far, n is often omitted from the notation, even though most elements depend on this parameter.

C.2.2 *The random SAT problem*

Let $n, m \in \mathbb{N}_0$ and $k \in \mathbb{N}$, where $n \geq k$ when $m > 0$. The random k-SAT distribution was defined in section C.1.2, but we will infer some additional notation needed for our proof. Firstly, we will specify the non-random case. When $m > 0$ we let a k-clause over n variables be a vector from the set

$$\mathcal{D} = \Big\{(\ell_1, \ldots, \ell_k) \in (\pm[n])^k : |\ell_1| < \cdots < |\ell_k|\Big\}.$$

The entries of such a vector are called the literals of the clause. Consider m such clauses $(\ell_{j,i})_{i \in [k]}$, $j \in [m]$. From these clauses we define a k-SAT formula φ with n

variables and m clauses by letting

$$\varphi = \bigwedge_{j=1}^{m} \left(\ell_{j,1} \vee \dots \vee \ell_{j,k}\right).$$

We let the order of the clauses matter such that two formulas φ and φ' with literals $((\ell_{j,i})_{i\in[k]})_{j\in[m]}$ and $((\ell'_{j,i})_{i\in[k]})_{j\in[m]}$, respectively, are equal if and only if $\ell_{j,i} = \ell'_{j,i}$ for all $j \in [m]$ and $i \in [k]$. This implies a one-to-one correspondence between a formula and its (ordered set of) literals. Now, we define a mapping related to a SAT-formula. For $\ell \in \pm[n]$ we associate a mapping by letting

$$\ell : \mathbb{B}^n \to \mathbb{B}, \quad \text{where} \quad \ell : x = (x_1, \dots, x_n) \mapsto \begin{cases} x_{|\ell|}, & \text{if } \operatorname{sgn}(\ell) = 1, \\ \neg x_{|\ell|}, & \text{if } \operatorname{sgn}(\ell) = -1. \end{cases} \tag{C.2.1}$$

Letting $\wedge$ denote the logical and and $\vee$ denote the logical or, we associate φ with the function mapping $\mathbb{B}^n$ to $\mathbb{B}$ that is given by

$$\varphi(x) = \left(\bigwedge_{j=1}^{m} \left(\ell_{j,1} \vee \dots \vee \ell_{j,k}\right)\right)(x) = \bigwedge_{j=1}^{m} \left(\ell_{j,1}(x) \vee \dots \vee \ell_{j,k}(x)\right), \quad x \in \mathbb{B}^n.$$

We now define a distribution over the set of k-SAT formulas with n variables and m clauses and we denote this distribution by $F_k(n,m)$. Consider random vectors $(L_{j,i})_{i\in[k]}$, $j \in [m]$, that are uniformly distributed on $\mathcal{D}$. We say that these are random clauses. Furthermore, let

$$\Phi = \bigwedge_{j=1}^{m} \left(L_{j,1} \vee \dots \vee L_{j,k}\right),$$

then Φ has distribution $F_k(n,m)$ and we say that Φ is a random k-SAT formula with n variables and m clauses. For $x \in \mathbb{B}^n$ we let $\Phi(x)$ denote the point-wise evaluation of Φ in x.

C.2.3 Fixing variables and the unit-propagation algorithm

Let $n, m \in \mathbb{N}_0$ and $k \in \mathbb{N}$ with $n \geq k$ when $m > 0$. Let $\mathcal{L} \subseteq \pm[n]$ be consistent. For an $x \in \mathbb{B}^n$ we let the vector $x_{\mathcal{L}}$ be as defined in subsection C.1.2 and for functions $g : \mathbb{B}^n \to \mathbb{B}$ we define $g_{\mathcal{L}}(x) = g(x_{\mathcal{L}})$. Consider a 2-SAT formula φ with n variables and m clauses where its literals are denoted $((\ell_{j,i})_{i\in[2]})_{j\in[m]}$. Consider the formula with fixed variables

$$\varphi_{\mathcal{L}} = \bigwedge_{j=1}^{m} \left(\ell_{j,1} \vee \ell_{j,2}\right)_{\mathcal{L}} = \bigwedge_{j=1}^{m} \left((\ell_{j,1})_{\mathcal{L}} \vee (\ell_{j,2})_{\mathcal{L}}\right).$$

The set $[m]$ is now split into four non-overlapping subsets:

$$\begin{aligned}
\mathcal{C}_0 &= \Big\{ j \in [m] : \ell_{j,1} \in -\mathcal{L} \text{ and } \ell_{j,2} \in -\mathcal{L} \Big\}, \\
\mathcal{C}_1 &= \Big\{ j \in [m] : \ell_{j,i_{j_1}} \notin \pm\mathcal{L} \text{ and } \ell_{j,i_{j_2}} \in -\mathcal{L},\ \{i_{j_1}, i_{j_2}\} = \{1,2\} \Big\}, \\
\mathcal{C}_2 &= \Big\{ j \in [m] : \ell_{j,1} \notin \pm\mathcal{L} \text{ and } \ell_{j,2} \notin \pm\mathcal{L} \Big\}, \\
\mathcal{C}_\star &= \Big\{ j \in [m] : \ell_{j,1} \in \mathcal{L} \text{ or } \ell_{j,2} \in \mathcal{L} \Big\}.
\end{aligned} \tag{C.2.2}$$

Using the definition of i_{j_1} from above we ease notation and let $\ell_{j,i_{j_1}} = \ell_j$ for $j \in \mathcal{C}_1$. Note that

- When $j \in \mathcal{C}_0$ then $(\ell_{j,1} \vee \ell_{j,1})_{\mathcal{L}}(x) = \mathtt{false}$ for all $x \in \mathbb{B}^n$.
- When $j \in \mathcal{C}_1$ then $(\ell_{j,1} \vee \ell_{j,2})_{\mathcal{L}}(x) = \ell_j(x)$ for all $x \in \mathbb{B}^n$.
- When $j \in \mathcal{C}_2$ then $(\ell_{j,1} \vee \ell_{j,2})_{\mathcal{L}}(x) = (\ell_{j,1} \vee \ell_{j,2})(x)$ for all $x \in \mathbb{B}^n$.
- When $j \in \mathcal{C}_\star$ then $(\ell_{j,1} \vee \ell_{j,2})(x) = \mathtt{true}$ for all $x \in \mathbb{B}^n$.

Define

$$\varphi_1 = \bigwedge_{j \in \mathcal{C}_1} (\ell_j), \qquad \text{and} \qquad \varphi_2 = \bigwedge_{j \in \mathcal{C}_2} (\ell_{j,1} \vee \ell_{j,2}). \tag{C.2.3}$$

Note that the above literals will belong to the set $(\pm[n] \setminus \pm \mathcal{L})$. The above implies that $\varphi \in \mathsf{SAT}$ if and only if $\mathcal{C}_0 = \emptyset$ and $(\varphi_1 \wedge \varphi_2) \in \mathsf{SAT}$. We will now further determine when $(\varphi_1 \wedge \varphi_2) \in \mathsf{SAT}$. Define

$$\mathcal{L}(\varphi_1) = \{\ell_j \in \mathcal{C}_1 : -\ell_j \notin \mathcal{C}_1\}. \tag{C.2.4}$$

We let this be the set associated with the 1-SAT formula φ_1, and we note that it is a consistent set. Moreover, for $x \in \mathbb{B}^n$

$$\begin{aligned}
& \varphi_1(x) = \mathtt{true} \\
\iff \quad & x_{|\ell_j|} = \begin{cases} \mathtt{true}, & \text{when } \operatorname{sgn}(\ell_j) = +1, \\ \mathtt{false}, & \text{when } \operatorname{sgn}(\ell_j) = -1. \end{cases} \quad \forall j \in \mathcal{C}_1.
\end{aligned} \tag{C.2.5}$$

This along with the definition of $x_{\mathcal{L}(\varphi_1)}$ implies that when $\varphi_1 \in \mathsf{SAT}$ then for all $x \in \mathbb{B}^n$ we have that $\varphi_1(x) = \mathtt{true}$ if and only if $x = x_{\mathcal{L}(\varphi_1)}$. Therefore

$$\begin{aligned}
(\varphi_1 \wedge \varphi_2) \in \mathsf{SAT} \iff & \ \varphi_1 \in \mathsf{SAT} \text{ and } (\varphi_1 \wedge \varphi_2)_{\mathcal{L}(\varphi_1)} \in \mathsf{SAT} \\
\iff & \ \varphi_1 \in \mathsf{SAT} \text{ and } (\varphi_2)_{\mathcal{L}(\varphi_1)} \in \mathsf{SAT}.
\end{aligned}$$

Thus

$$\varphi \in \mathsf{SAT} \iff \mathcal{C}_0 = \emptyset, \quad \varphi_1 \in \mathsf{SAT}, \quad \text{and} \quad (\varphi_2)_{\mathcal{L}(\varphi_1)} \in \mathsf{SAT}. \tag{C.2.6}$$

This decomposition of the event $\{\varphi \in \mathsf{SAT}\}$ becomes a key tool in the proof. Moreover, note that the same procedure, as just described, can now be applied to the formula $(\varphi_2)_{\mathcal{L}(\varphi_1)}$. Hence, the procedure of fixing variables continues recursively in rounds and this is the idea behind the unit-propagation algorithm. One of the main ingredients in the proof of our main theorem concerns controlling this process.

C.2.4 Sketch of proof

Consider a random 2-CNF formula $\Phi \sim F_2(n,n)$ with literals $(L_{j,i})_{i\in[2],j\in[n]}$, and a consistent set $\mathcal{L} \subseteq \pm[n]$ with $|\mathcal{L}| = f$. We now apply the unit-propagation procedure to Φ, thereby decomposing the probability of interest into a collection of simpler terms.

Initial round: Let $\mathcal{C}_k^{(1)}$, for $k \in K$, be the random sets defined from Φ and $\mathcal{L}$ as described in (C.2.2), and define $M_k^{(1)} = |\mathcal{C}_k^{(1)}|$ for $k \in K$. Additionally, let $\Phi_1^{(1)}$ and $\Phi_2^{(1)}$ be the random formulas constructed from Φ and $\mathcal{L}$, corresponding to the definitions in (C.2.3). Finally, let $\mathcal{L}^{(1)}$ denote the set associated with $\Phi_1^{(1)}$, as defined in (C.2.4). From the decomposition in (C.2.6), we get that

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}(M_0^{(1)} = 0,\ \Phi_1^{(1)} \in \mathsf{SAT},\ (\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}). \tag{C.2.7}$$

The independence of the clauses of Φ implies that the three events in (C.2.7) only are dependent through the random vector $(M_k^{(1)})_{k\in[K]}$. Moreover, the i.i.d. structure of the clauses in Φ implies that this vector has a multinomial distribution, where the entries concentrate around their mean and hence become asymptotically independent. This implies that also the events in (C.2.7) are asymptotically independent, allowing for the desired decomposition:

$$\mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \sim \mathbb{P}\Big(M_0^{(1)} = 0\Big)\mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big). \tag{C.2.8}$$

Subsequent rounds: The procedure from the initial round is now repeated recursively, replacing Φ and $\mathcal{L}$ with $\Phi_2^{(1)}$ and $\mathcal{L}^{(1)}$, respectively. Hereby, new random elements $(M_k^{(2)})_{k\in K}$, $\Phi_1^{(2)}$, $\Phi_2^{(2)}$, and $\mathcal{L}^{(2)}$ are constructed. The procedure is then repeated iteratively on $\Phi_2^{(2)}$ and $\mathcal{L}^{(2)}$, and so on. Continuing a total of R times (R being some suitable integer), we construct the random elements $(M_k^{(r)})_{k\in K}$, $\Phi_1^{(r)}$, $\Phi_2^{(r)}$, and $\mathcal{L}^{(r)}$ for each $r \in [R]$. Using these constructed elements, the probability calculation in (C.2.8) can be extended iteratively, leading to

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \sim \mathbb{P}\Big((\Phi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big)\prod_{r=1}^{R}\mathbb{P}\Big(M_0^{(r)} = 0\Big)\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big). \tag{C.2.9}$$

The probabilistic decomposition in (C.2.9) plays a central role in the overall proof. To evaluate the terms of (C.2.9), we need to know the distributions of the defined elements. As the elements are defined recursively, the distributions can be found as conditional distributions, and when conditioning on the past, we get that

$$M_0^{(r)}|M_1^{(r-1)} \approx \text{Binomial}\left(\left(\frac{M_1^{(r-1)}}{2n}\right)^2, n\right),$$
$$\Phi_1^{(r)}|M_1^{(r)} \approx F_1(n, M_1^{(r)}), \quad (r \in [R]).$$

Thus, it becomes crucial to control the size of the sequence $(M_1^{(r)})_{r\in[R]}$, and the remaining part of the proof concerns this.

Firstly, we establish that $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0$ when $f = n^q$ with $q = 1/3 + \varepsilon$. Here we will prove the existence of constants $c, C > 0$, such that

$$\lim_{n\to\infty} \mathbb{P}\Big(M_1^{(r)} \in [cn^q, Cn^q]\ \forall r \in [R]\Big) = 1, \tag{C.2.10}$$

which will imply that the product in (C.2.9) approaches zero and thus, this implies our main result. When proving (C.2.10) a simple union bound will not do, and thus we will need to exploit the Markov structure of the sequence $(M_1^{(r)})_{r\in[R]}$.

Next, we will establish that $\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq \liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT})$, when $f = n^q$ with $q = 1/3 - \varepsilon$. In this setup, the sequence $(M_1^{(r)})_{r\in[R]}$ is a super-martingale, and thus optional sampling gives that $M_1^{(r)} \leq \log n \cdot n^q$ for all $r \in [R]$. This further implies that the product in (C.2.9) approaches one as $n \to \infty$. Next, we will establish that the sequence $(M_1^{(r)})_{r\in[R]}$ is close in distribution to a critical Galton-Watson tree, and from this we can establish that $M_1^{(R)} = 0$ w.h.p., which implies that $\mathcal{L}^{(R)} = \emptyset$ w.h.p. This further gives that $(\Phi_2^{(R)})_{\mathcal{L}^{(R)}}$ is close in distribution to Φ, and thus the first term of (C.2.9) is asymptotically equivalent to $\mathbb{P}(\Phi \in \mathsf{SAT})$. Thus, this finally proves our main theorem.

C.3 Main decomposition of probability

In this section, we present a mathematically rigorous version of the decomposition in C.2.4. This decomposition will break the proof of our main result into smaller lemmas, which will be proven later. In subsection C.3.1, we introduce the technical lemmas that primarily provide distributional results for the sequences of elements that will be defined in sections C.3.2 and C.3.3. The two sequences defined in these sections both serve as approximations to the unit propagation procedure. Section C.3.2 addresses the case $q > 1/3$, where the corresponding sequence is used to establish an upper bound on the probability, which approaches zero. In Section C.3.3, the other sequence provides a lower bound that is used for the proof in the case $q < 1/3$.

C.3.1 Technical lemmas

The first lemma of this section states that for $\Phi \sim F_2(n,m)$ and a consistent set of literals $\mathcal{L} \subseteq \pm[n]$, with $|\mathcal{L}| = f$ we can construct a coupled SAT-formula Φ' which has the same distribution as Φ but where fixing the literals of $\mathcal{L}$ in Φ corresponds to fixing the literals of the set $[n]\backslash[n-f]$. When considering the different rounds of the unit-propagation algorithm later on, the repeated use of this lemma will allow us to control which variables are fixed.

Lemma C.4. *There exists a function G such that if $\Phi \sim F_2(n,m)$ and $\mathcal{L} \subseteq \pm[n]$ is a consistent set of literals with $|\mathcal{L}| = f$, then $\Phi' := G(\Phi, \mathcal{L}) \stackrel{\mathcal{D}}{=} \Phi$ and*

$$\left\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\right\} = \left\{\Phi'_{[n]\backslash[n-l]} \in \mathsf{SAT}\right\}.$$

The below is an easy consequence of the above lemma.

Fact C.5. *Let $\Phi \sim F_2(n,m)$ and let $\mathcal{L} \subseteq \pm[n]$ be a consistent random set of literals independent of Φ. Then $G(\Phi, \mathcal{L}) \stackrel{\mathcal{D}}{=} \Phi$ and $G(\Phi, \mathcal{L})$ is independent of $\mathcal{L}$.*

The proof of Lemma C.4 relies on the uniformity of the clauses that imply that literals can be swapped without changing the distribution of the formula.

Next, we want to decompose a 2-CNF formula with fixed variables into its 1- and 2-CNF sub-formulas. Let φ be a (non-random) 2-CNF formula with n variables and m clauses and let $\mathcal{L} = [n]\backslash[n-f]$ for some $f \in \mathbb{N}$. Define the sets

$$\mathcal{A}_0 = \mathcal{A}_0(n,f) := -\mathcal{L} \times -\mathcal{L}, \quad \mathcal{A}_1 = \mathcal{A}_1(n,f) := \pm[n-l] \times -\mathcal{L},$$
$$\mathcal{A}_2 = \mathcal{A}_2(n,f) := \pm[n-f] \times \pm[n-f], \quad \mathcal{A}_\star = \mathcal{A}_\star(n,f) := \pm[n] \times \mathcal{L}.$$

Let $(\ell_{j,1}, \ell_{j,2})$, $j \in [m]$, be the literals of φ and define $\mathcal{C}_k = \{j \in [m] : (\ell_{j,1}, \ell_{j,2}) \in \mathcal{A}_k\}$, $k \in K$. Note that this definition corresponds to the definition in (C.2.2). A clause that belongs to $\mathcal{A}_0$ is said to be an unsatisfied clause, and a clause in $\mathcal{A}_\star$ is said to be satisfied. Define

$$G_1(\varphi, f) := \bigwedge_{j \in \mathcal{C}_1} \ell_{j,1}, \quad G_2(\varphi, f) = \bigwedge_{j \in \mathcal{C}_2} (\ell_{j,1} \vee \ell_{j,2}).$$

In (C.2.6) we saw that

$$\begin{aligned} & \varphi_{\mathcal{L}} \in \mathsf{SAT} \\ \iff & \mathcal{C}_0 = \emptyset, \quad G_1(\varphi, f) \in \mathsf{SAT}, \quad G_2(\varphi, f)_{\mathcal{L}(G_1(\varphi,f))} \in \mathsf{SAT}, \end{aligned}$$

where $\mathcal{L}(G_1(\varphi, f))$ is defined in (C.2.4). In the setup with $\mathcal{L} = [n]\backslash[n-f]$ we further note that when $(\ell_{j,1}, \ell_{j,2}) \in \mathcal{A}_1$, then $\ell_{j,1} \in \pm[n-f]$ and when $(\ell_{j,1}, \ell_{j,2}) \in \mathcal{A}_2$ then $(\ell_{j,1}, \ell_{j,2}) \in (\pm[n-f])^2$. Hence both $G_1(\varphi, f)$ and $G_2(\varphi, f)$ can be viewed as boolean functions that map $\mathbb{B}^{n-f}$ into $\mathbb{B}$. The above setup will now be applied to a random 2-CNF formula. The next lemma describes the simultaneous distribution of the elements defined in this setup.

Lemma C.6. *Let $\Phi \sim F_2(n,m)$ and $\mathcal{L} = [n] \backslash [n-f]$. If M_k is the random variable denoting the number of clauses in $\Phi_k := G_k(\Phi, f)$ for $k \in \{1,2\}$, and M_0 and $M_\star$ are the number of unsatisfied- and satisfied clauses, respectively, then*

$$(M_k)_{k\in K} = (M_0, M_1, M_2, M_\star) \sim \textit{Multinomial}\Big(m,\ p(n,f)\Big),$$

where $p = (p_k)_{k\in K}$ and

$$p_0(n,f) = \frac{f(f-1)}{4n(n-1)}, \quad p_1(n,f) = \frac{(n-f)f}{n(n-1)},$$
$$p_2(n,f) = \frac{(n-f)(n-f-1)}{n(n-1)}, \quad p_\star(n,f) = \frac{(n - \frac{f}{4} - \frac{3}{4})f}{n(n-1)}.$$

Furthermore

$$\Phi_k | (M_k)_{k\in K} \sim F_k(n-f,\ M_k), \quad (k \in \{1,2\}),$$

and Φ_1 and Φ_2 are conditionally independent given $(M_k)_{k\in K}$.

This lemma is again a direct consequence of the uniformity and the independence of the clauses of a random 2-CNF formula. The last lemma of this section gives a lower bound on the probability that a 1-CNF formula is satisfiable.

Lemma C.7. *Let $n, m \in \mathbb{N}$ with $n \geq m$ and let $\Phi \sim F_1(n,m)$. Then*

$$\mathbb{P}(\Phi \in \mathsf{SAT}) \geq \left(1 - \tfrac{m}{n}\right)^m.$$

This lemma can be proven in the same way as they prove Lemma 8 in [BOS25]. Thus, we will not repeat the argument here.

C.3.2 Decomposition of probability when many variables are fixed

Let $\Phi \sim F_2(n,n)$, and $\mathcal{L}$ be a consistent set of literals with $|\mathcal{L}| = f = f(n)$, where $f(n) = \Omega(n^{1/3+\varepsilon})$ for a small $\varepsilon > 0$. We will prove that $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = 0$. In this section, the aim is to closely regulate the unit-propagation procedure and hereby establish an upper bound on the probability of interest. Later, it is established that this upper bound approaches zero as $n \to \infty$.

Controlling the unit-propagation procedure

The assumption on f implies that $f(n) \geq n^q$, where $q = 1/3 + \varepsilon$ for some small $\varepsilon > 0$. Let $\mathcal{L}' \subseteq \mathcal{L}$ with $|\mathcal{L}'| = \lfloor n^q \rfloor$. As $\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\} \subseteq \{\Phi_{\mathcal{L}'} \in \mathsf{SAT}\}$ it is sufficient to establish that $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT}) = 0$. Thus, we will WLOG assume that $f(n) = \lfloor n^q \rfloor$ for some $q \in (1/3, 1/2)$.

Next, we define a sequence of random elements that resembles a controlled version of the unit-propagation procedure. First, we define the initial elements of the procedure. Let G be the function defined in Lemma C.4. Then define

$$\Psi_2^{(0)} := G(\Phi, \mathcal{L}), \quad S^{(-1)} = 0, \quad \bar{S}^{(-1)} = 0, \quad S^{(0)} := f,$$
$$M_1^{(0)} = f + 1, \quad \mathcal{L}^{(0)} := [n] \backslash [n - f], \qquad \mathcal{M}^{(0)} := \{\emptyset, \Omega\}.$$

Note that $S^{(0)} = S^{(-1)} + (M_1^{(0)} - 1)^+$, $\mathcal{L}^{(0)} = [n - S^{(-1)}] \backslash [n - S^{(0)}]$, and Lemma C.4 states that $\Psi_2^{(0)}$ is constructed such that

$$\begin{aligned} &\Psi_2^{(0)} \sim F_2(n, n) = F_2\Big(n - S^{(-1)},\ (n - \bar{S}^{(-1)})^+\Big) \\ \text{and} \quad &\Big\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big\} = \Big\{(\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT}\Big\}. \end{aligned} \tag{C.3.1}$$

Furthermore, $\mathcal{M}^{(0)}$ is the trivial σ-algebra and thus it provides no information. Now, additional elements are constructed recursively. Let $R := \lfloor n^{1-2q} \log n \rfloor$ denote the number of rounds. Then for each $r \in [R]$ we define the following recursively.

Let G_1 and G_2 be the functions from Lemma C.6 and define $\Phi_k^{(r)} := G_k(\Psi_2^{(r-1)}, |\mathcal{L}^{(r-1)}|)$ for $k \in \{1, 2\}$. Also, let $M_k^{(r)}$ denote the number of clauses in $\Phi_k^{(r)}$ for $k \in \{1, 2\}$ and let $M_0^{(r)}$ and $M_\star^{(r)}$ denote the number of unsatisfied- and satisfied clauses of $(\Psi_2^{(r-1)})_{\mathcal{L}^{(r-1)}}$, respectively. Define the σ-algebra $\mathcal{M}^{(r)} := \sigma\Big(\mathcal{M}^{(r-1)} \cup \sigma(M_k^{(r)},\ k \in K)\Big)$. The elements are constructed such that

$$\Big\{(\Psi_2^{(r-1)})_{\mathcal{L}^{(r-1)}} \in \mathsf{SAT}\Big\} = \Big\{(\Phi_2^{(r)})_{\mathcal{L}(\Phi_1^{(r)})} \in \mathsf{SAT},\ \Phi_1^{(r)} \in \mathsf{SAT},\ M_0^{(r)} = 0\Big\}, \tag{C.3.2}$$

see (C.2.6), and Lemma C.6 states that

$$(M_k^{(r)})_{k \in K} | \mathcal{M}^{(r-1)} \sim \mathrm{Binomial}\Big((n - \bar{S}^{(r-2)})^+,\ p\Big(n - S^{(r-2)},\ (M_1^{(r-1)} - 1)^+\Big)\Big), \tag{C.3.3}$$

$$\Phi_k^{(r)} | \mathcal{M}^{(r)} \sim F_2(n - S^{(r-1)}, M_k^{(r)}), \quad k \in \{1, 2\}, \tag{C.3.4}$$

and $\Phi_2^{(r)}$ and $\Phi_1^{(r)}$ are independent when conditioning on $\mathcal{M}^{(r)}$. Now, define $\bar{\Psi}_2^{(r)} := G(\Phi_2^{(r)}, \mathcal{L}(\Phi_1^{(r)}))$, where G is the function from Lemma C.4 and the set corresponding to $\Phi_1^{(r)}$ is defined in (C.2.4). As $\Phi_2^{(r)}$ and $\Phi_1^{(r)}$ are independent given $\mathcal{M}^{(r)}$, Fact C.5 states that

$$\bar{\Psi}_2^{(r)} | \mathcal{M}^{(r)} \sim F_2(n - S^{(r-1)}, M_k^{(r)}), \quad \text{and} \quad \bar{\Psi}_2^{(r)} \perp\!\!\!\perp \Phi_1^{(r)} \,|\mathcal{M}^{(r)}.$$

Moreover, if $\bar{M}_1^{(r)} = |\mathcal{L}(\Phi_1^{(r)})|$, then

$$\left\{(\Phi_2^{(r)})_{\mathcal{L}(\Phi_1^{(r)})} \in \mathsf{SAT}\right\} = \left\{(\bar{\Psi}_2^{(r)})_{\bar{\mathcal{L}}^{(r)}} \in \mathsf{SAT}\right\}, \ \bar{\mathcal{L}}^{(r)} := [n - S^{(r-1)}] \backslash [n - S^{(r-1)} - \bar{M}_1^{(r)}]. \tag{C.3.5}$$

Now, we either add clauses to $\bar{\Psi}_2^{(r)}$ or remove clauses. Define $\bar{S}^{(r-1)} = \lfloor \log n \rfloor \cdot S^{(r-1)}$ and let $(L_{j,1}^{(r)}, L_{j,2}^{(r)})$ for $j \in [M_2^{(r)}]$ be the random literals of $\bar{\Psi}_2^{(r)}$. If $M_2^{(r)} < (n - \bar{S}^{(r-1)})^+$ define additional random literals $(L_{j,1}^{(r)}, L_{j,2}^{(r)})$ for $j \in \{M_2^{(r)}, \dots, (n - \bar{S}^{(r-1)})^+\}$ where conditional on $\mathcal{M}^{(r)}$ they are i.i.d. and uniformly distributed on $\mathcal{D}^{(r)} := \{(\ell_1, \ell_2) \in (\pm[n - S^{(r-1)}])^2 : |\ell_1| < |\ell_2|\}$. Define

$$\Psi_2^{(r)} = \bigwedge_{j \in [(n - \bar{S}^{(r-1)})^+]} \left(L_{j,1}^{(r)} \vee L_{j,2}^{(r)}\right),$$

then

$$\Psi_2^{(r)} | \mathcal{M}^{(r)} \sim F_2\left(n - S^{(r-1)}, (n - \bar{S}^{(r-1)})^+\right).$$

Lastly, let

$$S^{(r)} = S^{(r-1)} + (M_1^{(r)} - 1)^+, \quad \text{and} \quad \mathcal{L}^{(r)} = [n - S^{(r-1)}] \backslash [n - S^{(r)}].$$

Then we are in the same setting again and we can repeat the procedure on $\Psi_2^{(r)}$ and $\mathcal{L}^{(r)}$ under the conditional distribution given $\mathcal{M}^{(r)}$, where we note that $\mathcal{L}^{(r)}$ is deterministic given $\mathcal{M}^{(r)}$.

Note that it is mainly the sequence $\{S^{(r)}\}_{r \in [R]}$ that controls the size of the different elements constructed above and this sequence is defined from the sequence $\{M_1^{(r)}\}_{r \in [R]}$. Thus, a big part of the proof in the over-constrained setting is controlling the size of this sequence, which describes the number of unit-clauses constructed in each round. We show that that this number remains on the order of n^q throughout the R rounds as the below lemma states.

Lemma C.8. *There exist constants $c_0 > 0$ and $C_0 > 0$ such that the two events*

$$B_l = \left\{M_1^{(r)} \geq c_0 n^q, \ r \in [R]\right\} \quad \textit{and} \quad B_u = \left\{M_1^{(r)} \leq C_0 n^q, \ r \in [R]\right\}$$

satisfy

$$\lim_{n \to \infty} \mathbb{P}(B_l) = \lim_{n \to \infty} \mathbb{P}(B_u) = 1.$$

As $S^{(r)} \leq \lfloor n^q \rfloor + \sum_{r=1}^R M_1^{(r)}$ the above Lemma also implies that:

Fact C.9. *There exists a constant $C_1 > 0$ such that for $r \in [R]$ (and n large enough) we have*

$$\left\{S^{(r)} \leq C_1 n^{1-q} \log n\right\} \subseteq B_u.$$

Lemma C.8 is technical to prove. It is easy to find constants $c_0 > 0$ and $C_0 > 0$ such that for each $r \in [R]$ we have that $c_0 n^q < M_1^{(r)} < C_0 n^q$ w.h.p. This does however not imply that the entire sequence $\{M_1^{(r)}\}_{r\in[R]}$ is uniformly bounded w.h.p. A union bound is not tight enough to establish the uniform boundedness so the dependence structure of the sequence needs to be exploited. We establish that when $M_1^{(R)}$ is bounded w.h.p. the previous elements will be bounded w.h.p. as well.

Decomposing the probability

The random elements defined in the controlled unit-propagation procedure above will now be related to the probability that $\Phi_{\mathcal{L}}$ is satisfiable. Our aim is to show that the probability tends to zero and thus we want to construct an upper bound on the probability. Let B_u and B_l be the events from Lemma C.8. Using equation (C.3.1) we first note that

$$\mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT},\, B_u,\, B_l\Big) = \mathbb{P}\Big((\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT},\, B_u,\, B_l\Big).$$

Next, using (C.3.2) and (C.3.5) on the term at the right gives that

$$\begin{aligned}
&\mathbb{P}\Big((\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT},\, B_u,\, B_l\Big)\\
=&\mathbb{P}\Big((\Phi_2^{(1)})_{\mathcal{L}(\Phi_1^{(1)})} \in \mathsf{SAT},\, \Phi_1^{(1)} \in \mathsf{SAT},\, M_0^{(1)} = 0,\, B_u,\, B_l\Big)\\
=&\mathbb{P}\Big((\bar{\Psi}_2^{(1)})_{\bar{\mathcal{L}}^{(1)}} \in \mathsf{SAT},\, \Phi_1^{(1)} \in \mathsf{SAT},\, M_0^{(1)} = 0,\, B_u,\, B_l\Big)\\
\le&\mathbb{P}\Big(\big(\bar{\Psi}_2^{(1)}\big)_{\bar{\mathcal{L}}^{(1)}} \in \mathsf{SAT},\, M_0^{(1)} = 0,\, B_u,\, B_l,\, M_1^{(1)} \le \bar{M}_1^{(1)} + 1,\, M_2^{(1)} \ge (n - \bar{S}^{(-1)})^+\Big)\\
&+\mathbb{P}\Big(M_1^{(1)} > \bar{M}_1^{(1)} + 1,\, \Phi_1^{(1)} \in \mathsf{SAT},\, B_u\Big) + \mathbb{P}\Big(M_2^{(1)} < (n - \bar{S}^{(-1)})^+,\, B_u,\, B_l\Big).
\end{aligned} \tag{C.3.6}$$

The first term in the last expression above will now be further decomposed. Note that when $M_1^{(1)} \le \bar{M}_1^{(1)} + 1$ then $\mathcal{L}^{(1)} \subseteq \bar{\mathcal{L}}^{(1)}$ and when $M_2^{(1)} \ge (n - \bar{S}^{(-1)})^+$ then $\Psi_2^{(1)}$ is a sub-formula of $\bar{\Psi}_2^{(1)}$. Thus

$$\begin{aligned}
&\mathbb{P}\Big(\big(\bar{\Psi}_2^{(1)}\big)_{\bar{\mathcal{L}}^{(1)}} \in \mathsf{SAT},\, M_0^{(1)} = 0,\, B_u,\, B_l,\, M_1^{(1)} \le \bar{M}_1^{(1)} + 1,\, M_2^{(1)} \ge (n - \bar{S}^{(-1)})^+\Big)\\
\le&\mathbb{P}\Big((\Psi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}, M_0^{(1)} = 0,\, B_u,\, B_l\Big).
\end{aligned} \tag{C.3.7}$$

Now, recursively repeating (C.3.6) and (C.3.7) R times in total we eventually arrive at the decomposition

$$\begin{aligned}\mathbb{P}\Big((\Phi_{\mathcal{L}} \in \mathsf{SAT},\, B_u,\, B_l\Big) \leq & \mathbb{P}\Big(M_0^{(r)} = 0,\, r \in [R],\, B_u,\, B_l\Big) \\ & + \sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} > \bar{M}_1^{(r)} + 1,\, \Phi_1^{(1)} \in \mathsf{SAT},\, B_u\Big) \\ & + \sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < (n - \bar{S}^{(r-1)})^+,\, B_u,\, B_l\Big).\end{aligned} \tag{C.3.8}$$

The below lemma establishes the limits of the above upper bound.

Lemma C.10. *It holds that*

(1) $\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(r)} = 0,\, r \in [R],\, B_u,\, B_l\Big) = 0$,

(2) $\lim_{n\to\infty} \sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} \geq \bar{M}_1^{(r)} + 2,\, \Phi_1^{(1)} \in \mathsf{SAT},\, B_u\Big) = 0$,

(3) $\lim_{n\to\infty} \sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < (n - \bar{S}^{(r-1)})^+,\, B_u,\, B_l\Big) = 0$.

When proving the above Lemma the events B_u and B_l make it possible to control the sizes of the different random elements. Further, Lemma C.8 makes it possible to evaluate one event at a time by conditioning on previous information and hereby knowing exact distributions.

The above decomposition and lemmas make it straight forward to prove that $\Phi_{\mathcal{L}}$ is indeed asymptotically unsatisfiable.

Proof of Definition C.1 (2). Lemma C.8 implies that it is sufficient to establish that the right-hand side of (C.3.8) tends to zero as $n \to \infty$. But this is a direct consequence of Lemma C.10. □

C.3.3 Decomposition of probability when few variables are fixed

We will now also control the unit-propagation procedure when the problem is asymptotically satisfiable, where we instead need a lower bound. Let $\Phi \sim F_2(n, n)$ and $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| = f(n)$, where $f(n) \leq n^q$, with $q = 1/3 - \varepsilon$ for a small $\varepsilon > 0$. In section C.3.2, we saw that the number of unit-clauses remained of order n^q throughout the R rounds. In this section, we instead want to show that the unit-propagation procedure terminates and thus that the number of unit-clauses reaches zero within the number of rounds we consider. It turns out that the number of unit-clauses generated by this algorithm will be a super-martingale (on a set of probability one) when considering the sequence from round $r = 2$ and onward. This is helpful as we will make use of optional sampling. Therefore, we will start by stating another lemma for which the entire sequence of one-clauses is a super-martingale and then we will connect this lemma to our main theorem.

Lemma C.11. *Let* $0 < q < 1/3$ *and let* $M_1^{(-1)}$ *and* $M_1^{(0)}$ *be random variables taking values in* $[n]$ *satisfying that* $\mathbb{E}[M_1^{(0)}] \leq C_0 n^q$ *for some* $C_0 > 0$ *and also that*

$$\lim_{n\to\infty} \mathbb{P}\Big(M_1^{(-1)} \leq n^q \log n\Big) = \lim_{n\to\infty} \mathbb{P}\Big(M_1^{(0)} \leq n^q \log n\Big) = 1.$$

Define $\mathcal{L}' = [n - M_1^{(-1)}] \backslash [n - M_1^{(-1)} - M_1^{(0)}]$ *and* $\mathcal{M}^{(0)} = \sigma(M_1^{(-1)}, M_1^{(0)})$ *and let* Φ' *be a random function with*

$$\Phi' | \mathcal{M}^{(0)} \sim F_2\Big(n - M_1^{(-1)},\ n - M_1^{(-1)} - M_1^{(0)}\Big).$$

If $\Phi \sim F_2(n, n)$ *then*

$$\liminf_{n\to\infty} \mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big) \geq \liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).$$

Controlling the unit-propagation procedure

The notation used when naming the elements of the unit-propagation procedure in subsection C.3.2 is now reused in this section. As there are small differences in the definitions in the two cases it is important to pay attention to which definitions apply to which lemmas.

Let Φ', $\mathcal{L}'$, $M_1^{(-2)}$ and $M_1^{(-1)}$ be the elements of Lemma C.11. Again we start by defining some initial elements of our unit-propagation procedure:

$$\Psi_2^{(0)} := \Phi', \quad S^{(-1)} = M_1^{(-1)}, \quad S^{(0)} = S^{(-1)} + M_1^{(0)},$$
$$\mathcal{L}^{(0)} := \mathcal{L}', \quad \mathcal{M}^{(0)} = \sigma\Big(M_1^{(-2)}, M_1^{(-1)}\Big).$$

Note that $\mathcal{L}^{(0)} = [n - S^{(-1)}] \backslash [n - S^{(0)}]$ and $\Psi_2^{(0)} | \mathcal{M}^{(0)} \sim F_2(n - S^{(-1)},\ n - S^{(0)})$. Now the rest of the elements are generated recursively. Let $R = \lfloor n^{1-2q} \log^{-3} n \rfloor$ denote the number of rounds. Then for each $r \in [R]$ we define the following recursively. Let G_1 and G_2 be the functions defined in Lemma C.4 and let $\Phi_k^{(r)} = G_k(\Psi_2^{(r-1)}, \mathcal{L}^{(r-1)})$ for $k \in \{1, 2\}$. Also, let $M_k^{(r)}$ be the number of clauses in $\Phi_k^{(r)}$ for $k \in \{1, 2\}$ and let $M_0^{(r)}$ and $M_\star^{(r)}$ denote the number of unsatisfied- and satisfied clauses of $(\Psi_k^{(r-1)})_{\mathcal{L}^{(r-1)}}$, respectively. We further define $\mathcal{M}^{(r)} = \sigma\Big(\mathcal{M}^{(r-1)} \cup \sigma(M_k^{(r)}, k \in K)\Big)$. We have that

$$\Big\{(\Psi_2^{(r-1)})_{\mathcal{L}^{(r-1)}} \in \mathsf{SAT}\Big\} = \Big\{(\Phi_2^{(r)})_{\Phi_1^{(r)}} \in \mathsf{SAT},\ \Phi_1^{(r)} \in \mathsf{SAT},\ M_0^{(r)} = 0\Big\}, \qquad \text{(C.3.9)}$$

see (C.2.6), and Lemma C.6 states that

$$(M_k^{(r)})_{k\in K}|\mathcal{M}^{(r-1)} \sim \mathrm{Binomial}\Big(n - S^{(r-1)},\ p(n - S^{(r-2)},\ M_1^{(r-1)})\Big), \tag{C.3.10}$$

$$\Phi_k^{(r)}|\mathcal{M}^{(r)} \sim F_2(n - S^{(r-1)}, M_k^{(r)}),\ k \in \{1,2\}, \quad \Phi_1^{(r)} \perp\!\!\!\perp \Phi_2^{(r)}|\mathcal{M}^{(r)}. \tag{C.3.11}$$

Now, define $\bar{\Psi}_2^{(r)} := G(\Phi_2^{(r)}, \Phi_1^{(r)})$, where G is the function from Lemma C.4 and $\Phi_1^{(r)}$ is seen as set, see (C.2.4). As $\Phi_2^{(r)}$ and $\Phi_1^{(r)}$ are independent given $\mathcal{M}^{(r)}$, Fact C.5 states that

$$\bar{\Psi}_2^{(r)}|\mathcal{M}^{(r)} \sim F_2(n - S^{(r-1)}, M_k^{(r)}), \quad \text{and} \quad \Psi_2^{(r)} \perp\!\!\!\perp \Phi_1^{(r)}\,|\mathcal{M}^{(r)}. \tag{C.3.12}$$

Moreover, if $\bar{M}_1^{(r)}$ denotes the number of distinct variables appearing in $\Phi_1^{(r)}$, then

$$\Big\{(\Phi_2^{(r)})_{\Phi_1^{(r)}} \in \mathsf{SAT}\Big\} = \Big\{(\bar{\Psi}_2^{(r)})_{\bar{\mathcal{L}}^{(r)}} \in \mathsf{SAT}\Big\}, \quad \bar{\mathcal{L}}^{(r)} := [n - S^{(r-1)}]\backslash[n - S^{(r-1)} - \bar{M}_1^{(r)}]. \tag{C.3.13}$$

Now, we add additional clauses to $\bar{\Psi}_2^{(r)}$ or remove clauses. Let $S^{(r)} = S^{(r-1)} + M_1^{(r)}$. Recall that

$$M_2^{(r)} = M_2^{(r-1)} - \Big(M_0^{(r)} + M_1^{(r)} + M_\star^{(r)}\Big) = \Big(n - S^{(r-1)}\Big) - \Big(M_0^{(r)} + M_1^{(r)} + M_\star^{(r)}\Big) \le n - S^{(r)}.$$

Let $(L_{j,1}^{(r)}, L_{j,2}^{(r)})$, $j \in [M_2^{(r)}]$ be the random random literals of $\bar{\Psi}_2^{(r)}$ and define additional random literals $(L_{j,1}^{(r)}, L_{j,2}^{(r)})$ for $j \in \{M_2^{(r)} + 1, \dots, n - S^{(r)}\}$ that when conditioning on $\mathcal{M}^{(r)}$ are i.i.d. and uniformly distributed on

$$\mathcal{D}^{(r)} := \Big\{(\ell_1, \ell_2) \in (\pm[n - S^{(r-1)}])^2 \,:\, |l_1| < |l_2|\Big\}.$$

Define

$$\Psi_2^{(r)} = \bigwedge_{j\in[n-S^{(r)}]} \Big(L_{j,1}^{(r)} \vee L_{j,2}^{(r)}\Big), \quad \text{then} \quad \Psi_2^{(r)}|\mathcal{M}^{(r)} \sim F_2\Big(n - S^{(r-1)}, n - S^{(r)}\Big).$$

Lastly, define $\mathcal{L}^{(r)} = [n - S^{(r-1)}]\backslash[n - S^{(r)}]$. Now, the same procedure can be applied to $\Psi_2^{(r)}$ and $\mathcal{L}^{(r)}$ in the conditional distribution given $\mathcal{M}^{(r)}$, where we note that $\mathcal{L}^{(r)}$ is deterministic given $\mathcal{M}^{(r)}$.

Decomposing the probability

We will use the elements defined previously to create a lower bound on the probability of $\Phi'_{\mathcal{L}'}$ being satisfiable. The definitions in the initial round imply that

$$\Big\{\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big\} = \Big\{(\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT}\Big\}.$$

Now, using (C.3.9) we get

$$\Big\{(\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT}\Big\} = \Big\{(\Phi_2^{(1)})_{\Phi_1^{(1)}} \in \mathsf{SAT},\ \Phi_1^{(1)} \in \mathsf{SAT},\ M_0^{(1)} = 0\Big\}, \tag{C.3.14}$$

and equation (C.3.13) further implies

$$\Big\{(\Phi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big\} = \Big\{(\bar{\Psi}_2^{(1)})_{\bar{\mathcal{L}}^{(1)}} \in \mathsf{SAT}\Big\}. \tag{C.3.15}$$

As $\bar{M}_1^{(1)} \leq M_1^{(1)}$ we have that $\mathcal{L}^{(1)} \subseteq \bar{\mathcal{L}}^{(1)}$ and also $\Psi_2^{(1)}$ is constructed such that $\bar{\Psi}_2^{(1)}$ is its sub-formula. Thus, we get the inclusions

$$\Big\{(\bar{\Psi}_2^{(1)})_{\bar{\mathcal{L}}^{(1)}} \in \mathsf{SAT}\Big\} \supseteq \Big\{(\Psi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big\}. \tag{C.3.16}$$

Combining all of the above set inclusions imply that

$$\mathbb{P}\Big((\Phi')_{\mathcal{L}'} \in \mathsf{SAT}\Big) \geq \mathbb{P}\Big((\Psi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT},\ \Phi_1^{(1)} \in \mathsf{SAT},\ M_0^{(1)} = 0\Big).$$

Now, we are back at considering the event $\{(\Psi_2^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\}$ and thus (C.3.14), (C.3.15) and (C.3.16) can be repeated for $r = 2, \ldots, R$. Hereby, we eventually get the lower bound

$$\mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big) \geq \mathbb{P}\Big((\Psi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT},\ \Phi_1^{(r)} \in \mathsf{SAT},\ M_0^{(1)} \in \mathsf{SAT},\ r \in [R]\Big). \tag{C.3.17}$$

Our next lemma gives that the above lower-bound tends to one as $n \to \infty$.

Lemma C.12. *We have that*

(1) $\lim_{n\to\infty} \mathbb{P}\Big(M_1^{(r)} \leq n^q \log n,\ r \in [R]\Big) = 1,$

(2) $\lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [R] \Big| M_1^{(r)} \leq n^q \log n,\ r \in \{-1, \ldots, R\}\Big) = 1,$

(3) $\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R] \Big| M_1^{(r)} \leq n^q \log n,\ r \in \{-1, \ldots, R\}\Big) = 1,$

(4) $\lim_{n\to\infty} \mathbb{P}\Big(M_1^{(R)} = 0\Big) = 1.$

That the sequence $(M_1^{(r)})_{r\in[R]}$ is bounded from above follows using optional sampling where we exploit that the sequence turns out to be a super-martingale. Lemma C.12 (2) and (3) are then consequences of Lemma C.6. Lastly (4) is proven by a Poisson approximation and also using theory of Galton-Watson trees. Lemma C.11 is now an easy consequence of Lemma C.12.

Proof of Lemma C.11. The definitions of $M_1^{(-1)}$ and $M_1^{(0)}$ along with Lemma C.12 (1) imply that the event that we condition on in (2) and (3) of Lemma C.12 happens w.h.p. Therefore, Lemma C.12 (2) implies that

$$\lim_{n\to\infty} \mathbb{P}(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [R]) = 1,$$

and Lemma C.12 (3) implies that

$$\lim_{n\to\infty} \mathbb{P}(M_0^{(r)} = 0,\ r \in [R]) = 1.$$

Also, Lemma C.12 (4) implies that $\mathcal{L}^{(R)} = \emptyset$ w.h.p. and when this is the case also $\Psi_2^{(R)} | \mathcal{M}^{(R)} \sim F_2(n - S^{(R-1)}, n - S^{(R-1)})$. Moreover, that $M_1^{(r)} \le n^q \log n$ for all $r \in [R]$ w.h.p. implies that $S^{(R-1)} \le n^{1-q}$ w.h.p. These observations along with Fatou's Lemma give

$$\begin{aligned}
&\liminf_{n\to\infty} \mathbb{P}\Big((\Psi_2^{(R)})_{\mathcal{L}^{(R)}} \in \mathsf{SAT}\Big) \\
&= \liminf_{n\to\infty} \mathbb{E}\Big[\mathbb{P}\Big(\Psi_2^{(R)} \in \mathsf{SAT} \Big| \mathcal{M}^{(R)}\Big) \Big| S^{(R-1)} \le n^{1-q},\ \mathcal{L}^{(R)} = \emptyset\Big] \\
&\ge \mathbb{E}\Big[\liminf_{n\to\infty} \mathbb{P}\Big(\Psi_2^{(R)} \in \mathsf{SAT} \Big| \mathcal{M}^{(R)}\Big) \Big| S^{(R-1)} \le n^{1-q},\ \mathcal{L}^{(R)} = \emptyset\Big] \\
&= \liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).
\end{aligned}$$

Combining these limits with the decomposition in (C.3.17) gives the result. □

C.4 Proofs

In this section we provide proofs of the lemmas stated previously. Sections C.4.1 and C.4.2 are devoted to the case $q > 1/3$ and sections C.4.3 and C.4.4 concern the case $q < 1/3$. Lastly, in section C.4.5 the technical lemmas of section C.3.1 are proven.

C.4.1 Proof of Lemma C.8

In this section, we again consider the elements defined in the unit-propagation procedure of section C.3.2. We establish that the two events $B_u = \{M_1^{(r)} \le C_0 n^q\}$ and $B_l = \{M_1^{(r)} \ge c_0 n^q\}$ happen w.h.p. A problem we encounter is that we cannot control the size of the sequence $\{S^{(r)}\}_{r\in[R]}$. Thus, we will need to define a new sequence of random elements that approximates our previously defined elements but for which we do not have this problem. Let $T^{(-1)} = 0$, $N_1^{(0)} = \lfloor n^q \rfloor$ and define recursively for each $r \in [0, R]$

$$T^{(r)} = \min\Big\{T^{(r-1)} + (N_1^{(r)} - 1)^+,\ \lceil n^{1-q}\log^2 n\rceil\Big\}, \qquad \bar{T}^{(r)} = \lfloor \log n \rfloor \cdot T^{(r)},$$

$$N_1^{(r+1)} | N_1^{(1)}, \ldots, N_1^{(r)} \sim \text{Binomial}\Big(\Big(n - \bar{T}^{(r-2)}\Big)^+,\ p_1\Big(n - S^{(r-1)}, \Big(M_1^{(r-1)} - 1\Big)^+\Big)\Big).$$

Now, the sequence $\{T^{(r)}\}_{r\in[R]}$ is upper-bounded by $\lceil n^{1-q}\log^2 n\rceil$ but at the same time it turns out that it has the same distribution as $\{S^{(r)}\}_{r\in[R]}$ w.h.p. Let $c_0 > 0$ and $C_0 > 0$ be two constants (which will be further specified later) and define the events

$$D_l = \Big\{N_1^{(r)} \geq c_0 n^q\ \forall r \in [R]\Big\}, \qquad D_u = \Big\{N_1^{(r)} \leq C_0 n^q\ \forall r \in [R]\Big\}$$

$$A_S = \Big\{S^{(R)} < n^{1-q}\log^2 n\Big\} \qquad A_T = \Big\{T^{(R)} < n^{1-q}\log^2 n\Big\}.$$

Equation (C.3.3) implies that

$$\Big(\Big\{M_1^{(r)}\mathbb{1}_{A_S}\Big\}_{r\in[R]},\ \mathbb{1}_{A_S}\Big) \stackrel{\mathcal{D}}{=} \Big(\Big\{N_1^{(r)}\mathbb{1}_{A_T}\Big\}_{r\in[R]},\ \mathbb{1}_{A_T}\Big).$$

Moreover, on A_S it holds that $\{M_1^{(r)}\mathbb{1}_{A_S}\}_{r\in[R]} = \{M_1^{(r)}\}_{r\in[R]}$ and on A_T we have $\{N_1^{(r)}\mathbb{1}_{A_T}\}_{r\in[R]} = \{N_1^{(r)}\}_{r\in[R]}$. Thus, if B_l and B_u are the events of Lemma C.8, then

$$\mathbb{P}(B_l^c) \leq \mathbb{P}(B_l^c \cap A_S) + \mathbb{P}(A_S^c) = \mathbb{P}(D_l^c \cap A_T) + \mathbb{P}(A_S^c) \leq \mathbb{P}(D_l^c) + \mathbb{P}(A_S^c),$$

and similarly $\mathbb{P}(B_u^c) \leq \mathbb{P}(D_u^c) + \mathbb{P}(A_S^c)$. Thus, in order to establish Lemma C.8 it is sufficient to establish that $\lim_{n\to\infty}\mathbb{P}(A_S) = 1$ and that $\lim_{n\to\infty}\mathbb{P}(D_l) = \lim_{n\to\infty}\mathbb{P}(D_u) = 1$. Thus, proving Lemma C.8 reduces to proving the below two lemmas

Lemma C.13. *We have* $\lim_{n\to\infty}\mathbb{P}(A_S) = 1$.

Lemma C.14. *We have* $\lim_{n\to\infty}\mathbb{P}(D_l) = \lim_{n\to\infty}\mathbb{P}(D_u) = 1$.

We start by proving the first of the above two lemmas.

Proof of Lemma C.13. We will establish this using Markov's inequality. Note that

$$\mathbb{E}[S^{(R)}] = \lfloor n^q \rfloor + \sum_{r=1}^{R}\mathbb{E}[(M_1^{(r)} - 1)^+] \leq \sum_{r=0}^{R}\mathbb{E}[M_1^{(r)}],$$

and equation (C.3.3) and the definition of p_1 in Lemma C.6 implies

$$\begin{aligned}
\mathbb{E}[M_1^{(r)}] &= \Big(n - \bar{S}^{(r-2)}\Big)^+ \frac{\Big(n - S^{(r-2)} - (M_1^{(r-1)} - 1)^+\Big)(M_1^{(r-1)} - 1)^+}{\Big(n - S^{(r-2)}\Big)\Big(n - S^{(r-2)} - 1\Big)} \\
&\leq \mathbb{E}\Bigg[M_1^{(r-1)} \cdot \frac{(n - \lfloor \log n \rfloor S^{(r-2)})^+}{n - S^{(r-2)} - 1} \cdot \frac{n - S^{(r-2)} - (M_1^{(r-1)} - 1)^+}{n - S^{(r-2)}}\Bigg] \\
&\leq \mathbb{E}\Big[M_1^{(r-1)}\Big].
\end{aligned}$$

In the above, we used that $S^{(r-2)} \geq n^q - 1$ so $n - g(n)S^{(r-2)} \leq n - S^{(r-2)} - 1$. Repeating the above argument we eventually get that

$$\mathbb{E}[M_1^{(r)}] \leq \mathbb{E}[M_1^{(0)}] \leq n^q.$$

Thus, Markov's inequality implies that

$$\begin{aligned}\mathbb{P}(A_S^c) &= \mathbb{P}\Big(S^{(R)} \geq n^{1-q}\log^2 n\Big)\\ &\leq \frac{\mathbb{E}\Big[S^{(R)}\Big]}{n^{1-q}\log^2 n} \leq \frac{(R+1)n^q}{n^{1-q}\log^2 n} \leq \frac{(n^{1-2q}\log n + 1)n^q}{n^{1-q}\log^2 n} \to 0 \text{ as } n \to \infty,\end{aligned}$$

where we use that for $q < 1/2$ we have $1 - q > q$. □

To prove the next Lemma we need the below technical lemma.

Lemma C.15. *Let $r, s \in [0, R]$ with $s < r$. Then*

(1) $\mathbb{E}[N_1^{(r)} | N_1^{(1)}, \ldots, N_1^{(s)}] \leq N_1^{(s)}$,

(2) $\mathbb{E}[(N_1^{(r)})^2 | N_1^{(1)}, \ldots, N_1^{(s)}] \leq RN_1^{(s)} + (N_1^{(s)})^2$,

(3) Assume $N_1^{(s)} \leq C_0 n^q$ for some $C_0 > 0$. Then there exists $C_1 > 0$ (dependent on C_0 but independent of r and s) such that $\mathbb{E}[N_1^{(r)} | N_1^{(1)}, \ldots, N_1^{(s)}] \geq N_1^{(s)} - C_1 n^{1-2q}\log^4 n$

(4) Assume $c_0 n^q \leq N_1^{(s)} \leq C_0 n^q$ for some $c_0, C_0 > 0$. Then there exists $C_2 > 0$ (dependent on c_0 and C_0 but independent of r and s) such that $\mathbb{V}\Big[N_1^{(r)} \Big| N_1^{(1)}, \ldots, N_1^{(s)}\Big] \leq C_2 n^{1-q}\log^4 n.$

Proof. The inequalities will be established one at a time.

(1) Direct calculations give that

$$\begin{aligned}&\mathbb{E}\Big[N_1^{(r)}\Big|N_1^{(1)}, \ldots, N_1^{(s)}\Big]\\ =&\mathbb{E}\Big[\mathbb{E}\Big[N_1^{(r)}\Big|N_1^{(1)}, \ldots, N_1^{(r-1)}\Big]\Big|N_1^{(1)}, \ldots, N_1^{(s)}\Big]\\ =&\mathbb{E}\left[(n - \bar{T}^{(r-2)})\frac{\Big(n - T^{(r-2)} - (N_1^{(r-1)} - 1)^+\Big)(N_1^{(r-1)} - 1)^+}{\Big(n - T^{(r-2)}\Big)\Big(n - T^{(r-2)} - 1\Big)}\middle|N_1^{(1)}, \ldots, N_1^{(s)}\right]\\ \leq&\mathbb{E}\left[N_1^{(r-1)}\frac{(n - \lfloor\log n\rfloor T^{(r-2)})^+}{n - T^{(r-2)} - 1} \cdot \frac{\Big(n - T^{(r-2)} - (N_1^{(r-1)} - 1)^+\Big)}{n - T^{(r-2)}}\middle|N_1^{(1)}, \ldots, N_1^{(s)}\right]\\ \leq&\mathbb{E}\Big[N_1^{(r-1)}\Big|N_1^{(1)}, \ldots, N_1^{(s)}\Big] \leq \cdots \leq N_1^{(s)},\end{aligned}$$

where we in the first inequality use that $T^{(r-2)} \geq n^q - 1$.

(2) For the second moment, we use that when $X \sim \text{Binomial}(n,p)$, then

$$\mathbb{E}[X^2] = np(1-p) + n^2p^2 \leq \mathbb{E}[X] + \Big(\mathbb{E}[X]\Big)^2. \tag{C.4.1}$$

This along with the calculations and result of (1) imply

$$\begin{aligned}
\mathbb{E}\Big[(N_1^{(r)})^2\Big|N_1^{(1)},\dots,N_1^{(s)}\Big] =& \mathbb{E}\Big[\mathbb{E}\Big[(N_1^{(r)})^2\Big|N_1^{(1)},\dots,N_1^{(r-1)}\Big]\Big|N_1^{(1)},\dots,N_1^{(s)}\Big] \\
\leq& \mathbb{E}\Big[N_1^{(r-1)}\Big|N_1^{(1)},\dots,N_1^{(s)}\Big] + \mathbb{E}\Big[(N_1^{(r-1)})^2\Big|N_1^{(1)},\dots,N_1^{(s)}\Big] \\
\leq& \cdots \leq (r-s)N_1^{(s)} + (N_1^{(s)})^2 \\
\leq& RN_1^{(s)} + (N_1^{(s)})^2.
\end{aligned}$$

(3) Next, we want to find a lower bound on the mean. Here we use that $T^{(r-2)} \leq n^{1-q}\log^2 n + 1$ and we also make use of (1) and (2).

$$\begin{aligned}
&\mathbb{E}\Big[N_1^{(r)}\Big|N_1^{(1)},\dots,N_1^{(s)}\Big] \\
=&\mathbb{E}\left[(n-\bar{T}^{(r-2)})\frac{\Big(n-T^{(r-2)}-(M_1^{(r-1)}-1)^+\Big)(N_1^{(r-1)}-1)^+}{(n-T^{(r-2)})(n-T^{(r-2)}-1)}\middle|N_1^{(1)},\dots,N_1^{(s)}\right] \\
\geq&\mathbb{E}\left[\Big(n-n^{1-q}\log^3 n-\log n\Big)\frac{n-\Big(T^{(r-2)}+N_1^{(r-1)}\Big)}{n-T^{(r-2)}}\cdot\frac{N_1^{(r-1)}-1}{n}\middle|N_1^{(1)},\dots,N_1^{(s)}\right] \\
\geq&\frac{n-n^{1-q}\log^3 n-\log n}{n}\cdot\mathbb{E}\left[(N_1^{(r-1)}-1)\left(1-\frac{N_1^{(r-1)}}{n-n^{1-q}\log^2 n-1}\right)\middle|N_1^{(1)},\dots,N_1^{(s)}\right] \\
\geq&\frac{n-n^{1-q}\log^3 n-\log n}{n}\left(\mathbb{E}\Big[N_1^{(r-1)}\Big|N_1^{(1)},\dots,N_1^{(s)}\Big]-1-\frac{\mathbb{E}\Big[(N_1^{(r-1)})^2\Big|N_1^{(1)},\dots,N_1^{(s)}\Big]}{n-n^{1-q}\log^2 n-1}\right) \\
\geq&\frac{n-n^{1-q}\log^3 n-\log n}{n}\cdot\mathbb{E}\Big[N_1^{(r-1)}\Big|N_1^{(1)},\dots,N_1^{(s)}\Big]-1-\frac{RN_1^{(s)}+(N_1^{(s)})^2}{n-n^{1-q}\log^2 n-1} \\
\geq&\cdots\geq\left(\frac{n-n^{1-q}\log^3 n-\log n}{n}\right)^{r-s}N_1^{(s)}-(r-s)\left(1+\frac{RN_1^{(s)}+(N_1^{(s)})^2}{n-n^{1-q}\log^2 n-1}\right).
\end{aligned} \tag{C.4.2}$$

We will now bound the above two terms one at a time. For the first term, we will need the below inequality which is true for $x \geq 2$ and $y > 0$:

$$\left[\Big(1-\tfrac{2}{x}\Big)^x\right]^y = \left[\exp\Big(x\log\Big(1-\tfrac{2}{x}\Big)\Big)\right]^y \geq \left[\exp\Big(x\Big(-\tfrac{4}{x}\Big)\Big)\right]^y = \exp\Big(-4y\Big) \geq 1-4y.$$

This and that $r - s \leq R \leq n^{1-2q} \log n$ now implies

$$\left(\frac{n - n^{1-q}\log^3 n - \log n}{n}\right)^{r-s} \geq \left(\left(1 - \frac{2}{n^q \log^{-3} n}\right)^{n^q \log^{-3} n}\right)^{n^{1-3q}\log^4 n} \geq 1 - 4n^{1-3q}\log^4 n. \tag{C.4.3}$$

For the other term, we use the assumption that $N_1^{(s)} \leq C_0 n^q$. Then as $2q < 1$ we get

$$\frac{RN_1^{(s)} + (N_1^{(s)})^2}{n - n^{1-q}\log^2 n - 1} \leq \frac{C_0 n^{1-q}\log n + C_0^2 n^{2q}}{n - n^{1-q}\log^2 n - 1} \to 0 \quad \text{as } n \to \infty.$$

Thus, for a $C > 1$ we have that

$$(r-s)\left(1 + \frac{RN_1^{(s)} + (N_1^{(s)})^2}{n - n^{1-q}\log^3 n - 1}\right) \leq (r-s)C \leq Cn^{1-2q}\log n. \tag{C.4.4}$$

Now, combining (C.4.2), (C.4.3) and (C.4.4) along with the assumption that $N_1^{(s)} \leq C_0 n^q$ we get that

$$\begin{aligned}
&\mathbb{E}\left[N_1^{(r)} \middle| N_1^{(1)}, \dots, N_1^{(s)}\right] \\
\geq &\left(1 - 4n^{1-3q}\log^4 n\right)N_1^{(s)} - Cn^{1-2q}\log n \\
\geq &N_1^{(s)} - 2n^{1-3q}\log^4 n C_0 n^q - Cn^{1-2q}\log n \geq N_1^{(s)} - C_1 n^{1-2q}\log^4 n.
\end{aligned}$$

(4) Lastly, we combine (2) and (3) along with the extra assumption that $N_1^{(s)} \geq c_0 n^q$ (which implies that $N_1^{(s)} - C_1 n^{1-2q}\log^4 n \geq 0$) to conclude that

$$\begin{aligned}
\mathbb{V}(N_1^{(r)} | N_1^{(1)}, \dots, N_1^{(s)}) &= \mathbb{E}\left[(N_1^{(r)})^2 \middle| N_1^{(1)}, \dots, N_1^{(s)}\right] - \left(\mathbb{E}\left[N_1^{(r)} \middle| N_1^{(1)}, \dots, N_1^{(s)}\right]\right)^2 \\
&\leq RN_1^{(s)} + (N_1^{(s)})^2 - \left(N_1^{(s)} - C_1 n^{1-2q}\log^4 n\right)^2 \\
&\leq RN_1^{(s)} + (N_1^{(s)})^2 - (N_1^{(s)})^2 + 2C_0 n^q C_1 n^{1-2q}\log^4 n \\
&\leq C_2 n^{1-q}\log^4 n.
\end{aligned}$$

□

Fact C.16. *As* $N_1^{(0)} = \lfloor n^q \rfloor$ *the above Lemma implies the existence of constants* $c_1 > 0$ *and* $C_1 > 0$ *such that*

$$\mathbb{E}[N_1^{(R)}] \leq n^q + 1, \qquad \mathbb{E}[N_1^{(R)}] \geq c_1 n^q, \qquad \mathbb{V}[N_1^{(R)}] \leq C_1 n^{1-q}\log^4 n.$$

We are now ready to prove the last lemma of this section which will imply Lemma C.8.

Proof of Lemma C.14. Let $c_1 > 0$ and $C_1 > 0$ be the constants of Fact C.16. We let $c_0 = c_1/2$ and $C_0 = 2C_1$ be the constants of our lemma. Note that when $q > 1/3$ then $(1-q)/2 < q$ why we can choose a $q_1 \in \left(\frac{1-q}{2}, q\right)$. Then using Chebyshev's inequality and Fact C.16 we get

$$\mathbb{P}\left(\left|N_1^{(R)} - \mathbb{E}[N_1^{(R)}]\right| \geq n^{q_1}\right) \leq \frac{\mathbb{V}\left[N_1^{(R)}\right]}{n^{2q_1}} \leq \frac{C_1 n^{1-q} \log^4 n}{n^{2q_1}} \to 0 \quad \text{as } n \to \infty.$$

Fact C.16 then implies

$$\mathbb{P}\left(N_1^{(R)} \leq c_1 n^q - n^{q_1}\right) \to 0 \quad \text{as } n \to \infty, \tag{C.4.5}$$

$$\mathbb{P}\left(N_1^{(R)} \geq C_1 n^q + n^{q_1}\right) \to 0 \quad \text{as } n \to \infty. \tag{C.4.6}$$

The above implies that the sequence is still of order n^q at step R. We will use this to show that the sequence cannot have been too small or too large in previous steps. Remember that we want to establish that $\lim_{n\to\infty} \mathbb{P}(D_l) = 1$, where the complimentary event is given by

$$D_l^c = \left\{\exists r \in [R] \text{ s.t. } N_1^{(r)} < c_0 n^q\right\} = \left\{\exists r \in [R] \text{ s.t. } N_1^{(r)} < \tfrac{1}{2} c_1 n^q\right\}.$$

Using (C.4.5) we see that the above is implied if we show that

$$\liminf_{n\to\infty} \mathbb{P}\left(N_1^{(R)} \leq c_1 n^q - n^{q_1} \middle| D_l^c\right) > 0. \tag{C.4.7}$$

Define

$$D_l^{(r)} = \left\{N_1^{(1)} > \tfrac{1}{2} c_1 n^q,\ N_1^{(2)} > \tfrac{1}{2} c_1 n^q, \ldots, N_1^{(r-1)} > \tfrac{1}{2} c_1 n^q,\ N_1^{(r)} \leq \tfrac{1}{2} c_1 n^q\right\}, \ (r \in [R]).$$

Then the above events are disjoint and $D_l^c = \cup_{r \in [R]} D_l^{(r)}$. Using Markov's inequality we get

$$\begin{aligned} \mathbb{P}(N_1^{(R)} \leq c_1 n^q - n^{q_1} | D_l^{(r)}) &= 1 - \mathbb{P}(N_1^{(R)} > c_1 n^q - n^{q_1} | D_l^{(r)}) \\ &\geq 1 - \frac{\mathbb{E}[N_1^{(R)} | D_l^{(r)}]}{c_1 n^q - n^{q_1}}, \qquad (r \in [R]). \end{aligned} \tag{C.4.8}$$

Next, using Lemma C.15 (1) we see

$$\begin{aligned} \mathbb{E}[N_1^{(R)} | D_l^{(r)}] &= \mathbb{E}\left[\mathbb{E}[N_1^{(R)} | N_1^{(1)}, \ldots, N_1^{(r)}] \middle| D_l^{(r)}\right] \\ &\leq \mathbb{E}[N_1^{(r)} | D_l^{(r)}] \\ &\leq \tfrac{1}{2} c_1 n^q, \qquad (r \in [R]). \end{aligned}$$

This upper bound is then inserted in (C.4.8):

$$\mathbb{P}(N_1^{(R)} \le c_1 n^q - n^{q_1} | D_l^{(r)}) \ge 1 - \frac{\frac{1}{2}c_1 n^q}{c_1 n^q - n^{q_1}} \ge \frac{1}{4}, \quad (r \in [R]).$$

This finally implies that

$$\begin{aligned}\mathbb{P}\Big(N_1^{(R)} \le c_1 n^q - n^{q_1} \Big| D_l^c\Big) &= \frac{\mathbb{P}\Big(\Big\{N_1^{(R)} \le c_1 n^q - n^{q_1}\Big\} \cap D_l^c\Big)}{\mathbb{P}(D_l^c)} \\ &= \frac{\sum_{r=1}^R \mathbb{P}\Big(N_1^{(R)} \le c_1 n^q - n^{q_1} \Big| D_l^{(r)}\Big)\mathbb{P}(D_l^{(r)})}{\mathbb{P}(D_l^c)} \\ &\ge \frac{1}{4}\frac{\sum_{r=1}^R \mathbb{P}(D_l^{(r)})}{\mathbb{P}(D_l^c)} = \frac{1}{4},\end{aligned}$$

which is (C.4.7).

Next, we will establish that $\lim_{n\to\infty} \mathbb{P}(D_u) = 1$, where the complimentary event is given by

$$D_u^c = \Big\{\exists r \in [R] \text{ s.t. } N_1^{(r)} > C_0 n^q\Big\} = \Big\{\exists r \in [R] \text{ s.t. } N_1^{(r)} > 2C_1 n^q\Big\}.$$

Using (C.4.6) we get that this is implied if we can show that

$$\liminf_{n\to\infty} \mathbb{P}\Big(N_1^{(R)} \ge C_1 n^q + n^{q_1} \Big| D_u^c\Big) > 0. \tag{C.4.9}$$

Define for each $r \in [R]$

$$D_u^{(r)} = \Big\{N_1^{(1)} < \lfloor 2C_1 n^q \rfloor, N_1^{(2)} < \lfloor 2C_1 n^q \rfloor, \ldots, N_1^{(r-1)} < \lfloor 2C_1 n^q \rfloor, N_1^{(r)} \ge \lfloor 2C_1 n^q \rfloor\Big\}.$$

Note that the above events are disjoint and $D_u^c \subseteq \cup_{r\in[R]} D_u^{(r)}$. Let $r \in [R]$ be fixed. The event $D_u^{(r)}$ does not give us an upper bound on $N_1^{(r)}$ which implies that we do not have good bounds on $\mathbb{E}[N_1^{(R)} | N_1^{(1)}, \ldots, N_1^{(r)}]$. Therefore, we split the below probability into two terms. Write

$$\begin{aligned}&\mathbb{P}\Big(N_1^{(R)} < C_1 n^q + n^{q_1} \Big| D_u^{(r)}\Big) \\ =&\mathbb{P}\Big(N_1^{(R)} < C_1 n^q + n^{q_1} \Big| D_u^{(r)} \cap \{N_1^{(r)} < 2\lfloor 2C_1 n^q \rfloor\}\Big)\mathbb{P}\Big(N_1^{(r)} < 2\lfloor 2C_1 n^q \rfloor \Big| D_u^{(r)}\Big) \\ +&\mathbb{P}\Big(N_1^{(R)} < C_1 n^q + n^{q_1} \Big| D_u^{(r)} \cap \{N_1^{(r)} \ge 2\lfloor 2C_1 n^q \rfloor\}\Big)\mathbb{P}\Big(N_1^{(r)} \ge 2\lfloor 2C_1 n^q \rfloor \Big| D_u^{(r)}\Big).\end{aligned} \tag{C.4.10}$$

We will now consider the above two terms separately. For the first term, we now have a bound on $N_1^{(r)}$, as we condition on the event $\lfloor 2C_1 n^q \rfloor \le N_1^{(r)} < 2\lfloor 2C_1 n^q \rfloor$.

However, we can not use Markov's inequality as before as our inequality points in the wrong direction. Thus, we will instead use Chebyshev's inequality. In Lemma C.15 the bounds (3) and (4) imply that there exists a constant $C > 0$ (which is independent of r) such that

$$\mathbb{E}[N_1^{(R)}|N_1^{(1)},\ldots,N_1^{(r)}] \geq 2C_1 n^q - Cn^{1-2q}\log^4 n$$

and

$$\mathbb{V}(N_1^{(R)}|N_1^{(1)},\ldots,N_1^{(r)}) \leq Cn^{1-q}\log^4 n.$$

Then

$$\mathbb{E}[N_1^{(R)}|N_1^{(1)},\ldots,N_1^{(r)}] - (C_1 n^q + n^{q_1}) \geq C_1 n^q - Cn^{1-2q}\log^4 n - n^{q_1} > 0,$$

and we can use Chebyshev's inequality to establish that

$$\begin{aligned}
&\mathbb{P}\Big(N_1^{(R)} < C_1 n^q + n^{q_1}\Big|N_1^{(1)},\ldots,N_1^{(r)}\Big)\\
\leq&\mathbb{P}\Big(\Big|N_1^{(R)} - \mathbb{E}[N_1^{(R)}|N_1^{(1)},\ldots,N_1^{(r)}]\Big| > C_1 n^q - Cn^{1-2q}\log^4 n - n^{q_1}\Big|N_1^{(1)},\ldots,N_1^{(r)}\Big)\\
\leq&\frac{\mathbb{V}[N_1^{(R)}|N_1^{(1)},\ldots,N_1^{(r)}]}{(C_1 n^q - Cn^{1-2q}\log^4 n - n^{q_1})^2}\\
\leq&\frac{Cn^{1-q}\log^4 n}{(C_1 n^q - Cn^{1-2q}\log^4 n - n^{q_1})^2} \leq \frac{1}{4}.
\end{aligned} \tag{C.4.11}$$

Lastly, we used that the fraction is of order $n^{1-3q}\log^4 n$ and thus it approaches zero as $n \to \infty$. For the second term of (C.4.10) we want to show that $\mathbb{P}(N_1^{(r)} \geq 2\lfloor 2C_1 n^q\rfloor | D_u^{(r)})$ is small. Note that $D_u^{(r)}$ contains the event $N_1^{(r-1)} < \lfloor 2C_1 n^q \rfloor$ which makes it unlikely that $N_1^{(r)} \geq 2\lfloor 2C_1 n^q\rfloor$. When $N_1^{(r-1)} < \lfloor 2C_1 n^q\rfloor$ we have:

$$\begin{aligned}
&\mathbb{P}\Big(N_1^{(r)} \geq 2\lfloor 2C_1 n^q\rfloor\Big|N_1^{(1)},\ldots,N_1^{(r-1)},\ N_1^{(r)} \geq \lfloor 2C_1 n^q\rfloor\Big)\\
=&\sum_{x=2\lfloor 2C_1 n^q\rfloor}^{n} \mathbb{P}\Big(N_1^{(r)} = x\Big|N_1^{(1)},\ldots,N_1^{(r-1)},\ N_1^{(r)} \geq \lfloor 2C_1 n^q\rfloor\Big)\\
=&\sum_{x=2\lfloor 2C_1 n^q\rfloor}^{n} \frac{\mathbb{P}\Big(N_1^{(r)} = x\Big|N_1^{(1)},\ldots,N_1^{(r-1)}\Big)}{\mathbb{P}\Big(N_1^{(r)} \geq \lfloor 2C_1 n^q\rfloor\Big|N_1^{(1)},\ldots,N_1^{(r-1)}\Big)}\\
\leq&\sum_{x=2\lfloor 2C_1 n^q\rfloor}^{n} \frac{\mathbb{P}\Big(N_1^{(r)} = 2\lfloor 2C_1 n^q\rfloor\Big|N_1^{(1)},\ldots,N_1^{(r-1)}\Big)}{\mathbb{P}\Big(N_1^{(r)} = \lfloor 2C_1 n^q\rfloor\Big|N_1^{(1)},\ldots,N_1^{(r-1)}\Big)}.
\end{aligned} \tag{C.4.12}$$

In the last inequality, we made the nominator larger and the denominator smaller. Here we used that $N_1^{(r)}|N_1^{(1)},\ldots,N_1^{(r-1)}$ has a Binomial distribution and as $N_1^{(r-1)} <$

$\lfloor 2C_1 n^q \rfloor$ the mode of its probability mass function is smaller than $2\lfloor 2C_1 n^q \rfloor$. Now, if $X \sim \text{Binomial}(n, p)$ then

$$\begin{aligned}
\frac{\mathbb{P}\Big(X = 2y\Big)}{\mathbb{P}\Big(X = y\Big)} = \frac{\binom{N}{2y} p^{2y}(1-p)^{n-2y}}{\binom{n}{k} p^y (1-p)^{n-y}} &= \frac{y!}{(2y)!} \frac{(n-y)!}{(n-2y)!} (p)^y (1-p)^{-y} \\
&\leq \frac{e \cdot y \cdot \left(\frac{y}{e}\right)^y}{e \cdot \left(\frac{2y}{e}\right)^{2y}} (np)^y \exp\Big(-y \log(1-p)\Big) \\
&\leq \frac{y}{\left(\frac{4}{e}\right)^y y^y} (np)^y \exp\Big(yp\Big) = y\left(\frac{4}{e}\right)^{-y} \left(\frac{np}{y}\right)^y \exp(yp).
\end{aligned}$$

In the above we have used that $\log(1-p) \geq -p$ and that $e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n$. Furthermore, coupling this with (C.4.12) we note that in our setup we have that the number of trials equals $n - \lfloor \log n \rfloor T^{r-2}$ and the probability parameter equals

$$p_1\Big(n - T^{(r-2)}, N_1^{(r-1)}\Big) \leq \frac{N_1^{(r-1)}}{n - T^{(r-2)}} \leq C n^{q-1}, \tag{C.4.13}$$

for a constant $C > 0$ chosen large enough. This implies that the factor in the middle becomes less than one, so in (C.4.12) we get

$$\begin{aligned}
&\mathbb{P}\Big(N_1^{(r)} > 2\lfloor 2C_1 n^q \rfloor \Big| N_1^{(1)}, \ldots, N_1^{(r-1)},\ N_1^{(r)} \geq \lfloor 2C_1 n^q \rfloor\Big) \\
\leq &\sum_{x=2\lfloor 2C_1 n^q \rfloor}^{n} \frac{\mathbb{P}\Big(N_1^{(r)} = 2\lfloor 2C_1 n^q \rfloor \Big| N_1^{(1)}, \ldots, N_1^{(r-1)}\Big)}{\mathbb{P}\Big(N_1^{(r)} = \lfloor 2C_1 n^q \rfloor \Big| N_1^{(1)}, \ldots, N_1^{(r-1)}\Big)} \\
\leq & n 2C_1 n^q \left(\frac{4}{e}\right)^{-2C_1 n^q} \exp\Big(2C_1 C n^{2q-1}\Big) \leq \frac{1}{4}.
\end{aligned}$$

Lastly, we used that $n^{1+q}(4/e)^{-2C_1 n^q} \to 0$ and $\exp(2C_1 C n^{2q-1}) \to 1$ when $n \to \infty$. Using this and (C.4.11) in (C.4.10) we get

$$\begin{aligned}
&\mathbb{P}\Big(N_1^{(R)} \leq C_1 n^q + n^p \Big| A_u^{(r)}\Big) \\
\leq &\mathbb{E}\Big[\mathbb{P}\Big(N_1^{(R)} \leq C_1 n^q + n^p \Big| N_1^{(1)}, \ldots,\ N_1^{(r)}\Big) \Big| A_u^{(r)} \cap \{N_1^{(r)} \leq 2\lfloor 2C_1 n^q \rfloor\}\Big) \\
&+ \mathbb{E}\Big[\mathbb{P}\Big(N_1^{(r)} > 2\lfloor 2C_1 n^q \rfloor \Big| N_1^{(1)}, \ldots, N_1^{(r-1)},\ N_1^{(r)} \geq \lfloor 2C_1 n^q \rfloor\Big) \Big| A_u^{(r)}\Big] \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.
\end{aligned}$$

This finally implies

$$\begin{aligned}\mathbb{P}\Big(N_1^{(R)} > C_1 n^q + n^p \Big| A_u\Big) =& \frac{\mathbb{P}\Big(\Big\{N_1^{(R)} > C_1 n^q + n^p\Big\} \cap A_u\Big)}{\mathbb{P}(A_u)}\\ =& \frac{\sum_{r=1}^R \mathbb{P}\Big(N_1^{(R)} > C_1 n^q + n^p \Big| A_u^{(r)}\Big)\mathbb{P}(A_u^{(r)})}{\mathbb{P}(A_u^{(r)})}\\ \geq& \frac{1}{2}\frac{\sum_{r=1}^R \mathbb{P}(A_u^{(r)})}{\mathbb{P}(A_u)} = \frac{1}{2},\end{aligned}$$

and this implies (C.4.9) and finishes the proof. □

C.4.2 Proof of Lemma C.10

The three limits of this lemma are established one at a time. Remember that we use the defined elements of Section C.3.2, i.e. the unit-propagation procedure elements constructed for the regime with $q > 1/3$.

We will first establish that

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R],\ B_u,\ B_l\Big) = 0.$$

Proof of Lemma C.10 (1). Let $c_0 > 0$ be the constant of Lemma C.8 and $C_1 > 0$ be the constant of Fact C.9. Remember that $\bar{S}^{(r)} = \lfloor \log n \rfloor S^{(r)}$ for $r \in [R]$. As $n(4\lfloor \log n \rfloor)^{-1} > C_1 n^{1-q} \log n$, we note that it is sufficient to establish that

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(r)} = 0,\ M_1^{(r)} \geq c_0 n^q,\ r \in [R],\ \bar{S}^{(R-2)} < \tfrac{n}{4}\Big) = 0.$$

Recall that for $r \in [R]$ equation (C.3.3) gives that

$$M_0^{(r)} | \mathcal{M}^{(r-1)} \sim \text{Binomial}\bigg((n - \bar{S}^{(r-2)})^+,\ p_0\Big(n - S^{(r-2)},\ (M_1^{(r-1)} - 1)^+\Big)\bigg),$$

and the function p_0, defined in Lemma C.6, is given by

$$p_0\Big(n - S^{(r-2)},\ M_1^{(r-1)}\Big) = \frac{(M_1^{(r-1)} - 1)^+\Big((M_1^{(r-1)} - 1)^+ - 1\Big)}{4(n - S^{(r-2)})(n - S^{(r-2)} - 1)}.$$

Define i.i.d. random variables

$$X^{(1)}, \ldots, X^{(R)} \sim \text{Binomial}\bigg(\Big\lfloor \frac{n}{2} \Big\rfloor,\ \Big(\frac{c_0 n^q - 2}{2n}\Big)^2\bigg).$$

The above considerations imply that

$$
\begin{aligned}
&\mathbb{P}\Big(M_0^{(r)}=0,\ M_1^{(r)}\geq c_0n^q,\ r\in[R],\ \bar{S}^{(R-2)}<\tfrac{n}{4}\Big)\\
\leq&\mathbb{P}\Big(M_0^{(r)}=0,\ r\in[R],\ M_1^{(r)}\geq c_0n^q,\ r\in[R-1],\ \bar{S}^{(R-2)}<\tfrac{n}{4}\Big)\\
=&\mathbb{E}\Big[\mathbb{P}\Big(M_0^{(R)}=0\Big|\mathcal{M}^{(r-1)}\Big)\mathbb{1}_{\{M_0^{(r)}=0,\ M_1^{(r)}\geq c_0n^q,\ r\in[R-1],\ \bar{S}^{(R-2)}<\frac{n}{4}\}}\Big]\\
\leq&\mathbb{E}\Big[\mathbb{P}\Big(X^{(R)}=0\Big)\mathbb{1}_{\{M_0^{(r)}=0,\ M_1^{(r)}\geq c_0n^q,\ r\in[R-1],\ \bar{S}^{(R-2)}<\frac{n}{4}\}}\Big]\\
\leq&\mathbb{P}\Big(X^{(R)}=0\Big)\mathbb{P}\Big(M_0^{(r)}=0,\ M_1^{(r)}\geq c_0n^q,\ r\in[R-1],\ \bar{S}^{(R-3)}\leq\tfrac{n}{4}\Big),
\end{aligned}
$$

where we lastly use that $\bar{S}^{(r)}$ increases in r. Now, the argument can be repeated on the last factor of the above upper bound. Eventually, we then derive that

$$\mathbb{P}\Big(M_0^{(r)}=0,\ M_1^{(r)}\geq c_0n^q\ \forall r\in[R],\ \bar{S}^{(R-2)}<\tfrac{n}{4}\Big)\leq\prod_{r=1}^{R}\mathbb{P}(X^{(r)}=0).$$

Let $c>0$ denote a constant satisfying

$$\lfloor n/2\rfloor\geq cn,\quad R\geq cn^{1-2q}\log n,\quad \left(\frac{c_0n^q-2}{2}\right)^2\geq cn^{2q}.$$

Then

$$
\begin{aligned}
\prod_{r=1}^{R}\mathbb{P}(X^{(r)}=0)&=\left(\left(1-\left(\frac{c_0n^q-2}{2n}\right)^2\right)^{\lfloor n/2\rfloor}\right)^R\\
&\leq\left(\left(1-\frac{c}{n^{2(1-q)}}\right)^{cn}\right)^{cn^{1-2q}\log n}\\
&=\left(\left(1-\frac{c}{n^{2(1-q)}}\right)^{n^{2(1-q)}}\right)^{c^2\log n}\to 0\quad\text{as } n\to\infty,
\end{aligned}
$$

and this finishes the proof. □

The next limit that will be established is the following

$$\lim_{n\to\infty}\sum_{r=1}^{R}\mathbb{P}\Big(M_1^{(r)}\geq\bar{M}_1^{(r)}+2,\ B_u\Big)=0.$$

Proof of Lemma C.10 (2). Let C_0 be the constant of Lemma C.8 and C_1 be the constant of Fact C.9. As $n/2>C_1n^{1-q}\log n$ we note that it is sufficient to establish that

$$\lim_{n\to\infty}\sum_{r=1}^{R}\mathbb{P}\Big(M_1^{(r)}\geq\bar{M}_1^{(r)}+2,\ M_1^{(r)}\leq C_0n^q,\ S^{(r-1)}<\tfrac{n}{2}\Big)=0.$$

Let $r \in [R]$ be fixed and consider the conditional probability

$$\mathbb{P}\Big(M_1^{(r)} \geq \bar{M}_1^{(r)} + 2,\ M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \tfrac{n}{2} \Big| \mathcal{M}^{(r)}\Big).$$

Let $V_1, \ldots, V_{M_1^{(r)}}$ be the variables of the 1-SAT formula $\Phi_1^{(r)}$. From (C.3.4) we get that these are i.i.d. and uniformly distributed on $[n - S^{(r-1)}]$ when conditioning on $\mathcal{M}^{(r)}$. Thus

$$\begin{aligned}
&\mathbb{P}\Big(M_1^{(r)} \geq \bar{M}_1^{(r)} + 2,\ M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \tfrac{n}{2} \ \Big|\ \mathcal{M}^{(r)}\Big) \\
=&\mathbb{P}\Big(\bigcup_{v_1, v_2} \bigcup_{\substack{j_1, j_2, j_3, j_4 \\ \text{distinct}}} \Big\{V_{j_1} = V_{j_2} = v_1,\ V_{j_3} = V_{j_4} = v_2\Big\} \Big|\ \mathcal{M}^{(r)}\Big) \mathbb{1}_{\{M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \frac{n}{2}\}} \\
\leq& \sum_{v_1, v_2} \sum_{\substack{j_1, j_2, j_3, j_4 \\ \text{distinct}}} \mathbb{P}\Big(V_{j_1} = V_{j_2} = v_1,\ V_{j_3} = V_{j_4} = v_2 \ \Big|\ \mathcal{M}^{(r)}\Big) \mathbb{1}_{\{M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \frac{n}{2}\}} \\
\leq& (n - S^{(r-1)})^2 (M_1^{(r)})^4 \left(\frac{1}{n - S^{(r-1)}}\right)^4 \mathbb{1}_{\{M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \frac{n}{2}\}} \\
\leq& \frac{(C_0 n^q)^4}{(n/2)^2} = \frac{C}{n^{2(1-2q)}},
\end{aligned}$$

where we sum over $v_1, v_2 \in [n - S^{(r-1)}]$ and $j_1, j_2, j_3, j_4 \in [M_1^{(r)}]$ and $C = 4C_0^4$. Therefore, we get

$$\begin{aligned}
&\sum_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} \geq \bar{M}_1^{(r)} + 2,\ M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \tfrac{n}{2}\Big) \\
=& \sum_{r=1}^{R} \mathbb{E}\Big[\mathbb{P}\Big(M_1^{(r)} \geq \bar{M}_1^{(r)} + 2,\ M_1^{(r)} \leq C_0 n^q,\ S^{(r-1)} < \tfrac{n}{2} \ \Big|\ \mathcal{M}^{(r)}\Big)\Big] \\
\leq& \sum_{r=1}^{R} \frac{C}{n^{2(1-2q)}} \leq \frac{C \log n}{n^{1-2q}} \to 0 \quad \text{as } n \to \infty,
\end{aligned}$$

as $1 - 2q > 0$ for $q < 1/2$ and this was the claim. □

The last limit to be established in this section is the following

$$\lim_{n \to \infty} \sum_{r=1}^{R} \mathbb{P}\Big(M_2^{(r)} < (n - \bar{S}^{(r-1)})^+,\ B_u,\ B_l\Big) = 0.$$

Proof of Lemma C.10 (3). Let C_0, c_0, and C_1 be the constants of Lemma C.8 and Fact C.9. As $n(4\lfloor \log n \rfloor)^{-1} > C_1 n^{1-q} \log n$ we note that it is sufficient to establish that

$$\lim_{n\to\infty}\sum_{r=1}^{R}\mathbb{P}\Big(M_2^{(r)} < (n-\bar{S}^{(r-1)})^+,\ M_1^{(r-1)} \le C_0 n^q,\ M_1^{(r-1)} \ge c_0 n^q,\ \bar{S}^{(r-2)} < \tfrac{n}{4}\Big) = 0.$$

Let $r \in [R]$ be fixed. We now consider the conditional distribution given $\mathcal{M}^{(r-1)}$ and assume that $M_1^{(r-1)} \le C_0 n^q, M_1^{(r-1)} \ge c_0 n^q$ and $\bar{S}^{(r-2)} < n/4$ which also implies that $S^{(r-2)} < n/4$. Using the definition of equation (C.3.3), and the definition of p_2 in Lemma C.6, we get

$$\begin{aligned}
&\mathbb{E}[M_2^{(r)}|\mathcal{M}^{(r-1)}]\\
=&\Big(n-\bar{S}^{(r-2)}\Big)p_2\Big(n-S^{(r-2)}, (M_1^{(r-1)}-1)^+\Big)\\
=&\Big(n-\bar{S}^{(r-2)}\Big)\frac{\Big(n-S^{(r-2)}-(M_1^{(r-1)}-1)\Big)\Big(n-S^{(r-2)}-(M_1^{(r-1)}-1)-1\Big)}{\Big(n-S^{(r-2)}\Big)\Big(n-S^{(r-2)}-1\Big)}\\
=&\Big(n-\bar{S}^{(r-2)}\Big)\Big(1-\frac{M_1^{(r-1)}-1}{n-S^{(r-2)}}\Big)\Big(1-\frac{M_1^{(r-1)}-1}{n-S^{(r-2)}-1}\Big)\\
\ge&\Big(n-\bar{S}^{(r-2)}\Big)\Big(1-\frac{C_0 n^q}{n/2}\Big)^2\\
\ge&\Big(n-\bar{S}^{(r-2)}\Big)\Big(1-\tfrac{1}{2}Cn^{q-1}\Big)^2,
\end{aligned} \tag{C.4.14}$$

where $C = 4C_0$. Using the above we get

$$\begin{aligned}
&\mathbb{E}[M_2^{(r)}|\mathcal{M}^{(r-1)}]-\Big(n-\bar{S}^{(r-1)}\Big)\\
=&\mathbb{E}[M_2^{(r)}|\mathcal{M}^{(r-1)}]-\Big(n-\bar{S}^{(r-2)}-\lfloor\log n\rfloor\Big(M_1^{(r-1)}-1\Big)\Big)\\
\ge&\Big(n-\bar{S}^{(r-2)}\Big)\Big((1-\tfrac{1}{2}Cn^{q-1})^2-1\Big)+\lfloor\log n\rfloor\Big(M_1^{(r-1)}-1\Big)\\
\ge&\frac{n}{2}\Big(-Cn^{q-1}\Big)+\lfloor\log n\rfloor\Big(c_0 n^q-1\Big)\ge Cn^q,
\end{aligned} \tag{C.4.15}$$

The conditional variance can also be bounded (again when $M_1^{(r-1)} \le C_0 n^q$ and $\bar{S}^{(r-1)} < n/4$). To do so we again make use of (C.3.3) and the calculations in (C.4.14)

$$\begin{aligned}
&\mathbb{V}(M_2^{(r)}|\mathcal{M}^{(r-1)})\\
=&\Big(n-\bar{S}^{(r-2)}\Big)p_2\Big(n-S^{(r-2)}, (M_1^{(r-1)}-1)^+\Big)\Big(1-p_2\Big(n-S^{(r-2)}, (M_1^{(r-1)}-1)^+\Big)\Big)\\
\le&n\Big(1-p_2\Big(n-S^{(r-2)}, (M_1^{(r-1)}-1)^+\Big)\Big)\\
\le&n\Big(1-\Big(1-\tfrac{1}{2}Cn^{q-1}\Big)^2\Big)\le Cn^q.
\end{aligned} \tag{C.4.16}$$

Using (C.4.15) and (C.4.16) along with Chebyshev's inequality we get

$$\begin{aligned}\mathbb{P}\Big(M_2^{(r)} < n - \bar{S}^{(r-1)}\Big|\mathcal{M}^{(r-1)}\Big) \leq& \mathbb{P}\left(\Big|M_2^{(r)} - \mathbb{E}\Big[M_2^{(r)}\Big|\mathcal{M}^{(r-1)}\Big]\Big| > Cn^q \;\Big|\; \mathcal{M}^{(r-1)}\right)\\ \leq& \frac{\mathbb{V}(M_2^{(r)}|M^{(r-1)})}{(Cn^q)^2} \leq \frac{1}{Cn^q}.\end{aligned}$$

This finally implies that

$$\begin{aligned}&\mathbb{P}\Big(M_2^{(r)} < (n - \bar{S}^{(r-1)})^+,\, M_1^{(r-1)} \leq C_0 n^q,\, M_1^{(r-1)} \geq c_0 n^q,\, \bar{S}^{(r-2)} < \tfrac{n}{4}\Big)\\ =&\mathbb{E}\Big[\mathbb{P}\Big(M_2^{(r)} < n - \bar{S}^{(r-1)}\Big|\mathcal{M}^{(r-1)}\Big)\mathbb{1}_{\{M_1^{(r-1)} \leq C_0 n^q,\, M_1^{(r-1)} \geq c_0 n^q,\, \bar{S}^{(r-1)} < \frac{n}{4}\}}\Big]\\ \leq&\frac{1}{Cn^q}\mathbb{P}\Big(M_1^{(r-1)} \leq C_0 n^q,\, M_1^{(r-1)} \geq \lambda n^q,\, S^{(r-1)} < n/4\Big) \leq \frac{1}{Cn^q},\end{aligned}$$

and thus we get the limit

$$\begin{aligned}&\sum_{r=1}^{R}\mathbb{P}\Big(M_2^{(r)} < (n - \bar{S}^{(r-1)})^+,\, M_1^{(r-1)} \leq C_0 n^q,\, M_1^{(r-1)} \geq c_0 n^q,\, \bar{S}^{(r-2)} < \tfrac{n}{4}\Big)\\ &\qquad\leq \sum_{r=1}^{R}\frac{1}{Cn^q} \leq \frac{1}{C}\cdot n^{1-3q}\log n \to 0 \quad \text{as } n \to \infty,\end{aligned}$$

where we use that $1 - 3q < 0$ when $q > 1/3$. □

C.4.3 *Proof of Lemma C.12*

The four limits of this lemma are established one at a time. Remember that we use the defined elements of Section C.3.3, i.e. the unit-propagation procedure elements constructed for the case $q < 1/3$. To begin with we want to show that

$$\lim_{n\to\infty}\mathbb{P}\Big(M_1^{(r)} \leq n^q \log n,\; r \in [R]\Big) = 1.$$

Proof of Lemma C.12 (1). For each $r \in [R]$ we use (C.3.10) and the definition of p_1 in Lemma C.6 to get that

$$\begin{aligned}\mathbb{E}[M_1^{(r)}|\mathcal{M}^{(r-1)}] =& \Big(n - S^{(r-1)}\Big)p_1\Big(n - S^{(r-2)},\, M_1^{(r-1)}\Big)\\ =& \frac{\Big(n - S^{(r-2)} - M_1^{(r-1)}\Big)^2}{\Big(n - S^{(r-2)}\Big)\Big(n - S^{(r-2)} - 1\Big)}\cdot M_1^{(r-1)} \leq M_1^{(r-1)}.\end{aligned}$$

The last inequality is obviously true when $M_1^{(r-1)} \geq 1$ and when $M_1^{(r-1)} = 0$ both sides of the inequality equals zero. Now, by letting $M_1^{(r)} = M_1^{(R)}$ and $\mathcal{M}^{(r)} = \mathcal{M}^{(R)}$

for $r > R$ we can extend our sequence and consider $\{M_1^{(r)}\}_{r\in\mathbb{N}_0}$ which then becomes a super-martingale w.r.t. the filtration $\{\mathcal{M}^{(r)}\}_{r\in\mathbb{N}_0}$. Define the stopping time

$$\tau = \min\Big\{r \in \mathbb{N}_0 \,:\, M_1^{(r)} = 0 \text{ or } M_1^{(r)} > n^q \log n\Big\}.$$

Let C_0 be the constant of Lemma C.11. As our sequence $\{M_1^{(r)}\}_{r\in\mathbb{N}_0}$ is a non-negative super-martingale we can make use of the optional sampling theorem (Thm. 28, Chapter V in [DM11]). Hereby we get that

$$C_0 n^q \geq \mathbb{E}[M_1^{(0)}] \geq \mathbb{E}[M_1^{(\tau)}] \geq n^q \log n \cdot \mathbb{P}\Big(M_1^{(\tau)} > n^q \log n\Big).$$

Rearranging the above terms implies that

$$\mathbb{P}\Big(M_1^{(\tau)} > n^q \log n\Big) \leq C_0 \log^{-1} n.$$

As the sequence terminates when hitting zero this establishes the result. □

The next limit to establish is the following

$$\lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [R] \,\Big|\, M_1^{(r)} \leq n^q \log n,\ r \in [-1, R]\Big) = 1.$$

Proof of Lemma C.12 (2). We will use that when $M_1^{(r)} \leq n^q \log n$ for all $r \in [-1, R]$ then $S^{(r)} \leq \frac{n}{2}$ for all $r \in [0, R]$. We will further use that if X, Y, Z are random variables then

$$X \perp\!\!\!\perp (Y, Z) \Rightarrow (X \perp\!\!\!\perp Y)|Z, \quad \text{and} \quad (X \perp\!\!\!\perp Y)|Z \Rightarrow X|(Y, Z) \overset{\mathcal{D}}{=} X|Z. \qquad \text{(C.4.17)}$$

From (C.3.11) we got that

$$\Phi_1^{(r)} \perp\!\!\!\perp \Phi_2^{(r)} \mid \mathcal{M}^{(r)}, \quad (r \in [R]).$$

The random function $\Psi_2^{(r)}$ is constructed from $\Phi_1^{(r)}$ and $\Phi_2^{(r)}$, but we noticed in (C.3.12) that $\Psi_2^{(r)}$ and $\Phi_1^{(r)}$ are independent given $\mathcal{M}^{(r)}$. From this point and on all remaining random objects are constructed from $\Psi_2^{(r)}$ and from $\mathcal{L}^{(r)}$, which is deterministic given $\mathcal{M}^{(r)}$, and then also from random objects that are defined independently of $\Phi_1^{(r)}|\mathcal{M}^{(r)}$. This implies that

$$\Phi_1^{(r)} \perp\!\!\!\perp \Big[(M_k^{(r+1)})_{k\in K}, \ldots, (M_k^{(R)})_{k\in K}, \Phi_1^{(r+1)}, \ldots, \Phi_1^{(R)}\Big] \Big| \mathcal{M}^{(r)}, \quad (r \in [R]).$$

Thus, the first implication of (C.4.17) implies that

$$\Phi_1^{(r)} \perp\!\!\!\perp \Big(\Phi_1^{(r+1)}, \ldots, \Phi_1^{(R)}\Big) \,\Big|\, \mathcal{M}^{(R)}, \quad (r \in [R]),$$

and the second implication of (C.4.17) gives that

$$\Phi_1^{(r)}|\mathcal{M}^{(r)} \overset{\mathcal{D}}{=} \Phi_1^{(r)}|\mathcal{M}^{(R)}, \quad (r \in [R]).$$

From (C.3.11) we have that

$$\Phi_1^{(r)}|\mathcal{M}^{(r)} \sim F_1\Big(n - S^{(r-1)}, M_1^{(r)}\Big), \quad (r \in [R]),$$

and Lemma C.7 states that if $\Phi_1 \sim F_1(n,m)$ then $\mathbb{P}\big(\Phi_1 \in \mathsf{SAT}\big) \geq \big(1 - \frac{m}{n}\big)^m$. Thus, when $M_1^{(r)} \leq n^q \log n$ it holds that

$$\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT}\Big|\mathcal{M}^{(r)}\Big) \geq \left(1 - \frac{n^q \log n}{n/2}\right)^{n^q \log n}.$$

Combining the above we get that

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [R]\,\Big|\, M_1^{(r)} \leq n^q \log n,\ r \in [-1,R]\Big)\\
=&\mathbb{E}\Big[\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [R]\Big|\mathcal{M}^{(R)}\Big)\Big|M_1^{(r)} \leq n^q \log n,\ r \in [-1,R]\Big]\\
=&\mathbb{E}\Big[\mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big|\mathcal{M}^{(1)}\Big)\mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [2,R]\Big|\mathcal{M}^{(R)}\Big)\Big|M_1^{(r)} \leq n^q \log n,\ r \in [-1,R]\Big]\\
\geq&\left(1 - \frac{n^q \log n}{n/2}\right)^{n^q \log n} \mathbb{P}\Big(\Phi_1^{(r)} \in \mathsf{SAT},\ r \in [2,R]\Big|M_1^{(r)} \leq n^q \log n,\ r \in [-1,R]\Big)\\
\geq&\cdots \geq \left(\left(1 - \frac{n^q \log n}{n/2}\right)^{n^q \log n}\right)^R\\
\geq&\left(\left(1 - \frac{2}{\frac{n^{1-q}}{\log n}}\right)^{\frac{n^{1-q}}{\log n}}\right)^{\frac{1}{\log n}} \to 1 \quad \text{as } n \to \infty
\end{aligned}$$

which was the claim. □

Next up, we will establish that

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R]\,\Big|\, M_1^{(r)} \leq n^q \log n,\ r \in [-1,R]\Big) = 1,$$

Proof of Lemma C.12 (3). In (C.3.10) it is stated that

$$(M_k^{(r)})_{k\in K}\Big|\mathcal{M}^{(r-1)} \sim \text{Multinomial}\Big(n - S^{(r-1)}, p\Big(n - S^{(r-2)}, M_1^{(r-1)}\Big)\Big), \quad (r \in [R]). \tag{C.4.18}$$

We will use the following fact:

$$\begin{aligned} &(X_1,\dots,X_n) \sim \text{Multinomial}\Big(n,(p_1,\dots,p_n)\Big) \\ \Rightarrow\quad & X_i|X_j \sim \text{Binomial}\Big(n-X_j,\tfrac{p_i}{1-p_j}\Big),\quad i\neq j. \end{aligned}$$

This implies that for $r\in[R]$

$$M_0^{(r)}|\mathcal{M}^{(r-1)}, M_1^{(r)} \sim \text{Binomial}\left(n-S^{(r-1)}-M_1^{(r)},\ \frac{p_0\Big(n-S^{(r-2)},M_1^{(r-1)}\Big)}{1-p_1\Big(n-S^{(r-2)},M_1^{(r-1)}\Big)}\right). \tag{C.4.19}$$

Now, given $M_1^{(r)}\leq n^q\log n$ for all $r\in[-1,R]$ we get that $S^{(r)}\leq n/4$ for all $r\in[0,R]$ and using the definitions of p_0 and p_1 given in Lemma C.6 we get for each $r\in[R]$:

$$\begin{aligned} p_0\Big(n-S^{(r-1)},M_1^{(r-1)}\Big) &\leq \frac{(n^q\log n)^2}{(\frac{3}{4}n)^2}, \\ 1-p_1\Big(n-S^{(R-1)},M_1^{(R-1)}\Big) &\geq 1-\frac{n^q\log n}{\frac{3}{4}n}\geq\frac{3}{4}. \end{aligned} \tag{C.4.20}$$

Using (C.3.10) we also note that there exists functions $g^{(r)}$, $r\in[R]$ such that for $r\in[R-1]$ we have that

$$\begin{aligned} &\mathbb{P}\Big(M_1^{(s)}=m^{(s)},\ s\in[r+1,R]\Big|\mathcal{M}^{(r-1)},M_1^{(r)},M_0^{(r)}\Big) \\ =&\mathbb{E}\Big[\mathbb{P}\Big(M_1^{(R)}=m^{(R)}\Big|\mathcal{M}^{(R-1)}\Big)\mathbb{1}_{\{M_1^{(s)}=m^{(s)},\ s\in[r+1,R-1]\}}\Big|\mathcal{M}^{(r-1)},M_1^{(r)},M_0^{(r)}\Big] \\ =&g^{(R)}(M_1^{(-1)},\dots,M_1^{(r)},m^{(r+1)},\dots,m^{(R)})\times \\ &\times\mathbb{P}\Big(M_1^{(s)}=m^{(s)},\ s\in[r+1,R-1]\Big|\mathcal{M}^{(r-1)},M_1^{(r)},M_0^{(r)}\Big) \\ =&\dots=\prod_{s=r+1}^{R} g^{(s)}\Big(M_1^{(-1)},\dots,M_1^{(r)},m^{(r+1)},\dots,m^{(s)}\Big). \end{aligned} \tag{C.4.21}$$

This implies that $(M_1^{(r+1)},\dots,M_1^{(R)})$ is independent of $M_0^{(r)}$ when conditioning on $\mathcal{M}^{(r-1)}$ and $M_1^{(r)}$. Now using (C.4.19) and (C.4.20) we get that

$$\begin{aligned} &\mathbb{P}\Big(M_0^{(r)}=0,\ r\in[R]\Big|M_1^{(r)}\leq n^q\log n,\ r\in[-1,R]\Big) \\ =&\mathbb{E}\Big[\mathbb{P}\Big(M_0^{(R)}=0\Big|\mathcal{M}^{(R-1)},M_1^{(R)}\Big)\mathbb{1}_{\{M_0^{(r)}=0,\ r\in[R-1]\}}\Big|M_1^{(r)}\leq n^q\log n,\ r\in[-1,R]\Big] \\ \geq&\mathbb{E}\left[\left(1-\frac{(n^q\log n)^2}{(\frac{1}{2})^3n^2}\right)^n\mathbb{1}_{\{M_0^{(r)}=0,\ r\in[R-1]\}}\Big|M_1^{(r)}\leq n^q\log n,\ r\in[-1,R]\right] \\ =&\left(1-\frac{(n^q\log n)^2}{(\frac{1}{2})^3n^2}\right)^n\mathbb{P}\Big(M_0^{(r)}=0,\ r\in[R-1]\Big|M_1^{(r)}\leq n^q\log n,\ r\in[-1,R]\Big). \end{aligned}$$

Then using (C.4.21) the above argument can be repeated on the last factor above

$$
\begin{aligned}
&\mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R-1]\Big|M_1^{(r)} \le n^q \log n,\ r \in [-1,R]\Big)\\
=&\mathbb{E}\Big[\mathbb{P}\Big(M_0^{(R-1)} = 0\Big|\mathcal{M}^{(R-2)},\ M_1^{(R-1)},\ M_1^{(R)}\Big)\mathbb{1}_{\{M_0^{(r)}=0,\ r\in[R-2]\}}\Big|M_1^{(r)} \le n^q \log n,\ r \in [-1,R]\Big]\\
=&\mathbb{E}\Big[\mathbb{P}\Big(M_0^{(R-1)} = 0\Big|\mathcal{M}^{(R-2)},\ M_1^{(R-1)}\Big)\mathbb{1}_{\{M_0^{(r)}=0,\ r\in[R-2]\}}\Big|M_1^{(r)} \le n^q \log n,\ r \in [-1,R]\Big]\\
\ge&\left(1 - \frac{(n^q \log n)^2}{(\frac{1}{2})^3 n^2}\right)^n \mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R-2]\Big|M_1^{(r)} \le n^q \log n,\ r \in [-1,R]\Big).
\end{aligned}
$$

Repeating the above R times in total we eventually arrive at the expression

$$
\begin{aligned}
&\mathbb{P}\Big(M_0^{(r)} = 0,\ r \in [R]\,\Big|\,M_1^{(r)} \le n^q \log n,\ r \in [-1,R]\Big)\\
&\ge\left(1 - \frac{(n^q \log n)^2}{(\frac{1}{2})^3 n^2}\right)^{Rn} \ge \left(\left(1 - \frac{2^3}{\frac{n^{2(1-q)}}{\log^2 n}}\right)^{\frac{n^{2(1-q)}}{\log^2 n}}\right)^{\frac{1}{\log n}} \to 1, \quad \text{as } n \to \infty,
\end{aligned}
$$

which was the claim. □

Next, we will establish that

$$
\mathbb{P}\Big(M_1^{(R)} = 0\Big) \to 1 \quad \text{as } n \to \infty,
$$

i.e. we will now establish that our process of 1-clauses terminates in less than R rounds w.h.p. We will show this by proving that our recursive sequence of Binomial random variables can be approximated by a recursive sequence of Poisson random variables. Afterwards, it is proven that the recursive sequence of Poisson random variables terminates.

Lemma C.17. *Let $(X^{(r)})_{r\in[-1,R]}$ be a sequence of random variables where $X^{(-1)} = M_1^{(-1)}$, $X^{(0)} = M_1^{(0)}$ and $X^{(r)}|X^{(r-1)} \sim \text{Poisson}\Big(X^{(r-1)}\Big)$ for $r \in [R]$. Then for $x^{(-1)}, x^{(0)}, \ldots, x^{(R)} \in [0, \lfloor n^q \log n \rfloor]$ it holds that*

$$
\begin{aligned}
&\mathbb{P}\Big(M_1^{(r)} = x^{(r)},\ r \in [R]\Big|M_1^{(-1)} = x^{(-1)}, M_1^{(r)} = x^{(0)}\Big)\\
\ge&\mathbb{P}\Big(X^{(r)} = x^{(r)},\ r \in [R]\Big|X^{(-1)} = x^{(-1)}, X^{(0)} = x^{(0)}\Big) \cdot E(n),
\end{aligned}
$$

where E is a function satisfying that $\lim_{n\to\infty} E(n) = 1$.

Proof. We will make use of the below inequality which holds for $y > x > 0$ and $z > 0$:

$$
\begin{aligned}
\left(1 - \frac{x}{y}\right)^{y-z} &\ge \left(1 - \frac{x}{y}\right)^y = \exp\left(y \log\left(1 - \frac{x}{y}\right)\right)\\
&\ge \exp\left(y\left(-\frac{x}{y} - \frac{x^2}{y^2}\right)\right) = \exp(-x)\exp\left(-\frac{x^2}{y}\right).
\end{aligned}
$$

Let $s^{(-2)} = 0$ and $s^{(r)} = s^{(r-1)} + x^{(r)}$ for $r \in [-1, R]$. The elements $x^{(-1)}, \dots, x^{(R)}$ are chosen such that $s^{(r)} \leq \frac{n}{2}$ for all $r \in [-1, R]$. Also, note that the definition of p_1 in Lemma C.6 implies that

$$\frac{(n-f)f}{n^2} \leq p_1(n, f) \leq \frac{f}{n}, \quad (n \geq f \geq 0).$$

Using the above inequalities along with Lemma C.6 we now get

$$\begin{aligned}
&\mathbb{P}\Big(M_1^{(r)} = x^{(r)},\ r \in [R] \Big| M_1^{(-1)} = x^{(-1)}, M_1^{(0)} = x^{(0)}\Big) \\
=&\prod_{r=1}^{R} \mathbb{P}\Big(M_1^{(r)} = x^{(r)} \Big| M_1^{(s)} = x^{(s)},\ s \in [-1, r-1]\Big) \\
=&\prod_{r=1}^{R} \binom{n - s^{(r-1)}}{x^{(r)}} \Big[p_1(n - s^{(r-2)}, x^{(r-1)})\Big]^{x^{(r)}} \Big[1 - p_1(n - s^{(r-2)}, x^{(r-1)})\Big]^{n - s^{(r-1)} - x^{(r)}} \\
\geq&\prod_{r=1}^{R} \frac{(n - s^{(r-1)} - x^{(r)})^{x^{(r)}}}{x^{(r)}!} \left[\frac{(n - s^{(r-1)})x^{(r-1)}}{(n - s^{(r-2)})^2}\right]^{x^{(r)}} \left[1 - \frac{x^{(r-1)}}{n - s^{(r-2)}}\right]^{n - s^{(r-2)} - (x^{(r-1)} + x^{(r)})} \\
\geq&\prod_{r=1}^{R} \left[\frac{n - s^{(r-2)} - (x^{(r-1)} + x^{(r)})}{n - s^{(r-2)}}\right]^{2x^{(r)}} \exp\left(-\frac{(x^{(r-1)})^2}{n - s^{(r-2)}}\right) \frac{e^{-x^{(r-1)}} (x^{(r-1)})^{x^{(r)}}}{x^{(r)}!} \\
\geq&\prod_{r=1}^{R} \left(1 - \frac{2n^q \log n}{n/2}\right)^{2n^q \log n} \exp\left(-\frac{n^{2q} \log^2 n}{n/2}\right) \mathbb{P}\Big(X^{(r)} = x^{(r)} | X^{(r-1)} = x^{(r-1)}\Big) \\
\geq&\left(\left(1 - \frac{4}{\frac{n^{1-q}}{\log n}}\right)^{\frac{n^{1-q}}{\log n}}\right)^{\frac{2}{\log n}} \exp\left(-\frac{2}{\log n}\right) \times \\
&\times \mathbb{P}\Big(X^{(r)} = x^{(r)},\ r \in [R] \Big| X^{(-1)} = x^{(-1)}, X^{(0)} = x^{(0)}\Big).
\end{aligned}$$

And as

$$\left(\left(1 - \frac{4}{\frac{n^{1-q}}{\log n}}\right)^{\frac{n^{1-q}}{\log n}}\right)^{\frac{2}{\log n}} \exp\left(-\frac{2}{\log n}\right) \to 1 \quad \text{as } n \to \infty,$$

the result follows. □

Let $(X^{(r)})_{r \in [-1, R]}$ be the sequence of random variables from the above lemma. Note that

$$\begin{aligned}
&\mathbb{P}\Big(M_1^{(R)} = 0\Big) \geq \mathbb{P}\Big(M_1^{(R)} = 0, M_1^{(r)} \leq n^q \log n,\ r \in [-1, R]\Big) \\
&= \sum_{x^{(-1)}=0}^{\lfloor n^q \log n \rfloor} \cdots \sum_{x^{(R-1)}=0}^{\lfloor n^q \log n \rfloor} \mathbb{P}\Big(M_1^{(-1)} = x^{(-1)}, \dots, M_1^{(R-1)} = x^{(R-1)}, M_1^{(R)} = 0\Big),
\end{aligned}$$

and using Lemma C.17 and letting $x^{(R)} = 0$ each summand can be upper bounded by

$$\begin{aligned} &\mathbb{P}\Big(M_1^{(-1)} = x^{(-1)}, \ldots, M_1^{(R)} = x^{(R)}\Big) \\ =&\mathbb{P}\Big(M_1^{(r)} = x^{(r)},\ r \in [R] \Big| M_1^{(-1)} = x^{(-1)}, M_1^{(0)} = x^{(0)}\Big)\mathbb{P}\Big(M_1^{(-1)} = x^{(-1)}, M_1^{(0)} = x^{(0)}\Big) \\ \geq&\mathbb{P}\Big(X^{(r)} = x^{(r)},\ r \in [R] \Big| X^{(-1)} = x^{(-1)}, X^{(0)} = x^{(0)}\Big)\mathbb{P}\Big(X^{(-1)} = x^{(-1)}, X^{(0)} = x^{(0)}\Big)E(n) \\ =&\mathbb{P}\Big(X^{(-1)} = x^{(-1)}, \ldots, X^{(R)} = x^{(R)}\Big)E(n). \end{aligned}$$

Inserting this lower bound in the sum gives that

$$\mathbb{P}\Big(M_1^{(R)} = 0\Big) \geq E(n)\mathbb{P}\Big(X^{(R)} = 0,\ X^{(r)} \leq n^q \log n,\ r \in [-1, R-1]\Big), \tag{C.4.22}$$

where E is the function from Lemma C.17. To establish our result we thus only need the two lemmas below

Lemma C.18. *We have that*

$$\mathbb{P}\Big(X^{(r)} \leq n^q \log n,\ r \in [-1, R-1]\Big) \to 1 \quad \text{as } n \to \infty.$$

Lemma C.19. *We have that*

$$\mathbb{P}\Big(X^{(R)} = 0\Big) \to 1 \quad \text{as } n \to \infty.$$

Proof of Lemma C.18. Let $X^{(r)} := X^{(R)}$ for $r > R$ and also define the σ-algebras $\mathcal{F}^{(r)} = \sigma\Big(X^{(-1)}, \ldots, X^{(r)}\Big)$ for $r \geq -1$. Then for each $r \geq -1$ we have

$$\mathbb{E}[X^{(r)} | \mathcal{F}^{(r-1)}] = X^{(r-1)},$$

why $(X^{(r)})_{r \geq -1}$ is a martingale w.r.t. the filtration $(\mathcal{F}^{(r)})_{r \geq -1}$. As it is non-negative, we can make use of optional sampling (Thm. 28, Chapter V of [DM11]). Consider the stopping time

$$\tau = \min\{r \in \mathbb{N}_0 : X^{(r)} = 0 \text{ or } X^{(r)} \geq n^q \log n\},$$

and let C_0 be the constant of Lemma C.11. Then

$$\begin{aligned} & C_0 n^q \geq \mathbb{E}[X^{(0)}] \geq \mathbb{E}\Big[X^{(\tau)}\Big] \geq n^q \log n \mathbb{P}\Big(X^{(\tau)} \geq n^q \log n\Big) \\ \Rightarrow \quad & \mathbb{P}\Big(X^{(\tau)} \geq n^q \log n\Big) \leq \frac{C_0}{\log n}. \end{aligned}$$

As 0 is an absorbing state this implies that

$$\mathbb{P}\Big(X^{(r)} \leq n^q \log n,\ r \in [-1, R]\Big) \to 1 \quad \text{as } n \to \infty,$$

which was the claim. ☐

Proof of Lemma C.19. Note that the distribution of $(X^{(r)})_{r\in[R]}$ has the same law as a critical Galton-Watson tree with offspring distribution Poisson(1) cut off at depth R, see Chapter 1 in [ANN04]. Thus, using standard results for such processes (see e.g. Thm. 1 in section 1.9 of [ANN04]), there exists a constant $C > 0$ such that

$$\begin{aligned}\mathbb{P}(X^{(R)} = 0) &\geq \mathbb{E}\left[\left(1 - \frac{C}{R}\right)^{X^{(0)}}\right] \geq \left(1 - \frac{C}{n^{1-2q}\log^{-3} n}\right)^{\mathbb{E}[X^{(0)}]} \\ &\geq \left(1 - \frac{Cn^{3q-1}\log^3 n}{n^q}\right)^{C_0 n^q} \to 1, \quad \text{as } n \to \infty,\end{aligned}$$

where C_0 is the constant of Lemma C.11 and Jensen's inequality is also used. Thus, the result is established. □

C.4.4 Establishing Definition C.1 (1) using Lemma C.11

We will now couple Lemma C.11 to our main result in the regime $q < 1/3$. We will do this by closely controlling the first couple of rounds in the unit-propagation algorithm. Thus, we will once again repeat the notation used when going through this procedure. However, as this section uses none of the defined elements from the other sections this will not be a problem.

Let $\Phi \sim F_2(n,n)$ and let $\mathcal{L} \subseteq \pm[n]$ be a consistent set of literals with $|\mathcal{L}| = \lfloor n^q \rfloor$. We need to show that $\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT})$. Let G be the function of Lemma C.4 and define

$$\begin{aligned}\Psi_2^{(0)} &:= G(\Phi,\mathcal{L}), \quad N_1^{(0)} = \lfloor n^q \rfloor, \quad T^{(-1)} := 0, \\ T^{(0)} &:= \lfloor n^q \rfloor, \quad \mathcal{L}^{(0)} := [n]\backslash[n - T^{(0)}], \quad \mathcal{N}^{(0)} = \{\emptyset, \Omega\}.\end{aligned}$$

Note that $\Psi_2^{(0)} \sim F_2(n,n)$ and also

$$\Big\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big\} = \Big\{(\Psi_2^{(0)})_{\mathcal{L}^{(0)}} \in \mathsf{SAT}\Big\}. \tag{C.4.23}$$

Unlike previously we now only repeat the unit-propagation procedure twice. Thus, recursively for $r = 1,2$ define the following:

Let G_1 and G_2 be the functions of Lemma C.6 and define $\Phi_k^{(r)} = G_k(\Psi_k^{(r-1)}, \mathcal{L}^{(r-1)})$. Let $N_k^{(r)}$ be the number of clauses in $\Phi_k^{(r)}$ for $k \in \{1,2\}$ and let $N_0^{(r)}$ and $N_\star^{(r)}$ be the number of unsatisfied- and satisfied clauses of $(\Psi_2^{(r-1)})_{\mathcal{L}^{(r-1)}}$, respectively. Define the σ-algebra $\mathcal{N}^{(r)} = \sigma\Big(\mathcal{N}^{(r-1)} \cup \sigma(N_k^{(r)} : k \in K)\Big)$. The elements are constructed such that

$$\Big\{(\Psi_2^{(r-1)})_{\mathcal{L}^{(r-1)}} \in \mathsf{SAT}\Big\} = \Big\{(\Phi_2^{(r)})_{\Phi_1^{(r)}} \in \mathsf{SAT},\ \Phi_1^{(r)} \in \mathsf{SAT},\ N_0^{(r)} = 0\Big\}. \tag{C.4.24}$$

and also

$$(N_k^{(r)})_{k\in K}|\mathcal{N}^{(r-1)} \sim \text{Multinomial}\Big(n-T^{(r-2)},\ p\Big(n-T^{(r-2)}, N_1^{(r-1)}\Big)\Big), \tag{C.4.25}$$
$$\Phi_k^{(r)}|\mathcal{N}^{(r)} \sim F_k(n-T^{(r-1)},\ N_k^{(r)}), \quad (k\in\{1,2\}),$$

and $\Phi_1^{(r)}$ and $\Phi_2^{(r)}$ are conditionally independent. Let $\bar{N}_1^{(r)}$ be the number of distinct variables appearing in $\Phi_1^{(r)}$ and define further

$$T^{(r)} := T^{(r-1)} + N_1^{(r)}, \quad \bar{\mathcal{L}}^{(r)} := [n-T^{(r-1)}]\backslash[n-T^{(r-1)}-\bar{N}_1^{(r)}],$$
$$\mathcal{L}^{(r)} := [n-T^{(r-1)}]\backslash[n-T^{(r)}].$$

Also, let $\Psi_2^{(r)} := G(\Phi_2^{(r)},\ \mathcal{L}(\Phi_1^{(r)}))$, where again G is defined in Lemma C.4. Then using Lemma C.6 we see

$$\Psi_2^{(r)}|\mathcal{N}^{(r)} \sim F_2\Big(n-T^{(r-1)},\ N_2^{(r)}\Big),$$
$$\Big\{(\Phi_2^{(r)})_{\Phi_1^{(r)}} \in \mathsf{SAT}\Big\} = \Big\{(\Psi_2^{(r)})_{\bar{\mathcal{L}}^{(r)}} \in \mathsf{SAT}\Big\} \supseteq \Big\{(\Psi_2^{(r)})_{\mathcal{L}^{(r)}} \in \mathsf{SAT}\Big\}, \tag{C.4.26}$$

where we lastly used that $\bar{\mathcal{L}}^{(r)} \subseteq \mathcal{L}^{(r)}$. Now, we are in the same setup as initially and our recursive step has ended. Combining (C.4.23), (C.4.24), and (C.4.26), we now see

$$\begin{aligned}&\mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big)\\ \geq&\mathbb{P}\Big((\Psi_2^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT},\ \Phi_1^{(2)} \in \mathsf{SAT},\ \Phi_1^{(1)} \in \mathsf{SAT},\ N_0^{(2)}=0,\ N_0^{(1)}=0\Big).\end{aligned} \tag{C.4.27}$$

The above equation implies that it is sufficient to lower bound the right-hand side of the above expression to establish our main theorem in the case $q<1/3$. We do this by proving the below lemmas.

Lemma C.20. *We have*

$$\lim_{n\to\infty} \mathbb{P}\Big(N_0^{(1)}=0\Big) = \lim_{n\to\infty} \mathbb{P}\Big(N_0^{(2)}=0\Big) = 1.$$

and

$$\lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) = \lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big) = 1.$$

Lemma C.21. *We have*

$$\liminf_{n\to\infty} \mathbb{P}\Big((\Psi_2^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big) \geq \liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).$$

These lemmas will imply our main theorem when $q<1/3$

Proof of Definition C.1 (1). As $\{\Phi_{\mathcal{L}} \in \mathsf{SAT}\} \subseteq \{\Phi \in \mathsf{SAT}\}$ this implies that

$$\liminf_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \le \liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).$$

On the other hand, equation (C.4.27) along with Lemma C.20 and Lemma C.21 gives

$$\begin{aligned}&\liminf_{n\to\infty} \mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big)\\ \ge&\liminf_{n\to\infty} \mathbb{P}\Big((\Psi_2^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT},\ \Phi_1^{(2)} \in \mathsf{SAT},\ \Phi_1^{(1)} \in \mathsf{SAT},\ N_0^{(2)} = 0,\ N_0^{(1)} = 0\Big)\\ \ge&\liminf_{n\to\infty} \mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).\end{aligned}$$

Combining the above implies that the two limit infimum coincide.

□

To prove our main theorem it thus suffices to establish Lemma C.20 and C.21. To do so we need the following technical result.

Lemma C.22. *There exists a constant $C_0 > 0$ such that $\mathbb{E}[N_k^{(r)}] \le C_0 n^q$ for $r \in \{1,2\}$ and $k \in \{1,\star\}$. Furthermore,*

$$\lim_{n\to\infty} \mathbb{P}\Big(N_k^{(r)} \le \tfrac{1}{2} n^q \log n\Big) = 1, \quad k \in \{1,\star\},\ r \in \{1,2\},$$

and

$$\lim_{n\to\infty} \mathbb{P}\Big(N_\star^{(1)} + N_\star^{(2)} \ge n^q\Big) = 1.$$

Proof. Note that $p_0(n, \lfloor n^q \rfloor) \le p_1(n, \lfloor n^q \rfloor) \le p_\star(n, \lfloor n^q \rfloor) \le n^{q-1}$, see the definitions in Lemma C.6, and thus

$$\mathbb{E}[N_k^{(1)}] = n \cdot p_k(n, \lfloor n^q \rfloor) \le n^q, \quad (k \in \{0,1,\star\}). \tag{C.4.28}$$

Using the previous observations, we get

$$\mathbb{E}\Big[p_1(n - T^{(0)}, N_1^{(1)})\Big] \le \mathbb{E}\Big[p_\star(n - T^{(0)}, N_1^{(1)})\Big] \le \frac{n^q}{n - n^q - 2},$$

and thus if we let $q_1 \in (\frac{q}{2}, q)$, then

$$\mathbb{E}[N_k^{(2)}] = \mathbb{E}\Big[N_2^{(1)} \cdot p_k(n - T^{(0)}, N_1^{(1)})\Big] \le \frac{n^{1+q}}{n - n^q - 2} \le n^q + n^{q_1}, \quad (k \in \{1,\star\}), \tag{C.4.29}$$

where we used the upper bound $N_2^{(1)} \leq n$. Note that (C.4.28) and (C.4.29) imply the first claim of the lemma. Furthermore, these two equations along with Markov's inequality give for $k \in \{1, \star\}$ and $r \in \{1, 2\}$

$$\mathbb{P}\Big(N_k^{(r)} > \tfrac{1}{2} n^q \log n\Big) < \frac{\mathbb{E}[N_k^{(r)}]}{\frac{1}{2} n^q \log n} \leq \frac{n^q + n^{q_1}}{\frac{1}{2} n^q \log n} \to 0 \quad \text{as } n \to \infty,$$

and this is the second claim of the lemma. Next, using (C.4.25), (C.4.28) and a Chernoff bound we get

$$\begin{aligned} \mathbb{P}\Big(N_k^{(1)} \geq \mathbb{E}[N_k^{(1)}] + n^{q_1}\Big) &\leq \exp\Big(-\tfrac{1}{3} n^{2q_1 - q}\Big), \quad (k \in \{0, 1, \star\}), \\ \mathbb{P}\Big(N_k^{(1)} \leq \mathbb{E}[N_k^{(1)}] - n^{q_1}\Big) &\leq \exp\Big(-\tfrac{1}{3} n^{2q_1 - q}\Big), \quad (k \in \{0, 1, \star\}). \end{aligned}$$

Using this, (C.4.28), and also that $\mathbb{E}[N_k^{(1)}] \geq n^q - n^{q_1}$ for $k \in \{1, \star\}$ (this is a direct consequence of the definition) we see that

$$\begin{aligned} \mathbb{P}\Big(N_k^{(1)} \geq n^q + n^{q_1}\Big) &\leq \exp\Big(-\tfrac{1}{3} n^{2q_1 - q}\Big), \quad (k \in \{0, 1, \star\}), \\ \mathbb{P}\Big(N_1^{(1)} \leq n^q - 2n^{q_1}\Big) &\leq \exp\Big(-\tfrac{1}{3} n^{2q_1 - q}\Big), \quad (k \in \{1, \star\}). \end{aligned} \tag{C.4.30}$$

Next, we again use that for $X \sim \text{Binomial}(n, p)$ we have $\mathbb{E}[X^2] \leq \mathbb{E}[X] + \mathbb{E}[X^2]$, see (C.4.1). Then we get the bound:

$$\begin{aligned} \mathbb{E}\Big[(N_\star^{(2)})^2\Big] &\leq \mathbb{E}\Big[\mathbb{E}[N_\star^{(2)} | \mathcal{N}^{(1)}] + \Big(\mathbb{E}[N_\star^{(2)} | \mathcal{N}^{(1)}]\Big)^2\Big) \\ &= \mathbb{E}\Big[N_2^{(1)} \cdot p_\star(n - T^{(0)},\, N_1^{(1)}) + \Big(N_2^{(1)} \cdot p_\star(n - T^{(0)},\, N_1^{(1)})\Big)^2\Big] \\ &\leq \frac{n}{n - n^q - 2} \mathbb{E}[N_1^{(1)}] + \Big(\frac{n}{n - n^q - 2}\Big)^2 \mathbb{E}\Big[(N_1^{(1)})^2\Big] \\ &\leq \frac{n}{n - n^q - 2} n^q + \Big(\frac{n}{n - n^q - 2}\Big)^2 \Big(\mathbb{E}[N_1^{(1)}] + (\mathbb{E}[N_1^{(1)}])^2\Big) \\ &\leq 2\Big(\frac{n}{n - n^q - 2}\Big)^2 n^q + \Big(\frac{n}{n - n^q - 2}\Big)^4 n^{2q} \\ &\leq n^{2q} + C n^q, \end{aligned} \tag{C.4.31}$$

for a constant C chosen large enough. We also want to lower bound the mean. Using that

$$N_2^{(2)} = n - N_0^{(2)} - N_1^{(2)} - N_\star^{(2)},$$

and that

$$N_\star^{(2)} | \mathcal{N}^{(1)} \sim \text{Binomial}\Big(N_2^{(1)},\, p_\star(n - T^{(0)}, N_1^{(1)})\Big),$$

where $p_\star(n,l) \geq p_1(n,l) \geq \frac{(n-l)l}{n^2}$, we get that

$$\begin{aligned}&\mathbb{E}\Big[N_\star^{(2)} \,\Big|\, N_1^{(1)} > n^q - 2n^{q_1} \text{ and } N_k^{(1)} < n^q + n^{q_1} \text{ for } k \in \{0,1,\star\}\Big]\\ \geq&\Big(n - 3(n^q + n^{q_1})\Big)\frac{\Big(n - n^q - (n^q + n^{q_1})\Big)(n^q - 2n^{q_1})}{n^2} \geq n^q - Cn^{q_1},\end{aligned}$$

again for C chosen large enough. This and (C.4.30) now implies that

$$\begin{aligned}\mathbb{E}[N_\star^{(2)}] \geq&(n^q - Cn^{q_1})\mathbb{P}\Big(N_1^{(1)} > n^q - 2n^{q_1} \text{ and } N_k^{(1)} < n^q + n^{q_1} \text{ for } k \in \{0,1,\star\}\Big)\\ \geq&(n^q - Cn^{q_1})\bigg(1 - \mathbb{P}\Big(N_1^{(1)} \leq n^q - 2n^{q_1}\Big) - \sum_{k\in\{0,1,\star\}} \mathbb{P}\Big(N_k^{(1)} \geq n^q + n^{q_1}\Big)\bigg)\\ \geq&(n^q - Cn^{q_1})\Big(1 - 4\exp\Big(-\tfrac{1}{3}n^{2p_1-q}\Big)\Big),\end{aligned}$$

and by redefining C we get that

$$\mathbb{E}\Big[N_\star^{(2)}\Big] \geq n^q - Cn^{q_1}. \tag{C.4.32}$$

Combining this with (C.4.31) we now get

$$\mathbb{V}\Big(N_\star^{(2)}\Big) = \mathbb{E}[(N_\star^{(2)})^2] - \Big(\mathbb{E}[N_\star^{(2)}]\Big)^2 \leq Cn^{q+q_1},$$

where C is again redefined. Now, let $q_2 \in (\frac{q+q_1}{2}, q)$. Then

$$\mathbb{P}\Big(\Big|N_\star^{(2)} - \mathbb{E}[N_\star^{(2)}]\Big| > n^{q_2}\Big) \leq \frac{\mathbb{V}\Big(N_\star^{(2)}\Big)}{n^{2q_2}} \leq C\frac{n^{q+q_1}}{n^{2q_2}} \to 0 \quad \text{as } n \to \infty.$$

Therefore, using this and (C.4.32) we see

$$\mathbb{P}\Big(N_\star^{(2)} \geq n^q - Cn^{q_1} - n^{q_2}\Big) \to 1 \quad \text{as } n \to \infty$$

and this along with (C.4.30) gives

$$\begin{aligned}&\mathbb{P}\Big(N_\star^{(1)} + N_\star^{(2)} > n^q\Big)\\ \geq&\mathbb{P}\Big(N_\star^{(1)} \geq n^q - 2n^{q_1},\ N_\star^{(2)} \geq n^q - Cn^{q_1} - n^{q_2}\Big) \to 1 \quad \text{as } n \to \infty,\end{aligned}$$

which finishes the proof. □

Now, we can prove our two remaining lemmas of this section.

Proof of Lemma C.20. Using Lemma C.6 we note that $p_0(n,l) \le \frac{l^2}{4(n-1)^2}$, why

$$\mathbb{P}\Big(N_0^{(1)} = 0\Big) \ge \left(1 - \frac{n^{2q}}{4(n-1)^2}\right)^n \to 1, \quad \text{as } n \to \infty,$$

and

$$\begin{aligned}\mathbb{P}\Big(N_0^{(2)} = 0\Big) &\ge \mathbb{P}\Big(N_0^{(2)} = 0\Big| N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big)\mathbb{P}\Big(N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big) \\ &\ge \left(1 - \frac{\left(\frac{1}{2} n^q \log n\right)^2}{4(n - n^q - 2)^2}\right)^n \mathbb{P}\Big(N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big) \to 1 \quad \text{as } n \to \infty,\end{aligned}$$

where we lastly used Lemma C.22. Now, using this Lemma again along with Lemma C.7 we get

$$\begin{aligned}\mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) &\ge \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big| N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big)\mathbb{P}\Big(N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big) \\ &\ge \left(1 - \frac{\frac{1}{2} n^q \log n}{n - n^q - 2}\right)^{\frac{1}{2} n^q \log n} \mathbb{P}\Big(N_1^{(1)} \le \tfrac{1}{2} n^q \log n\Big) \to 1 \quad \text{as } n \to \infty.\end{aligned}$$

A similar argument gives that

$$\begin{aligned}&\mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big) \\ \ge &\mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big| N_1^{(r)} \le \tfrac{1}{2} n^q \log n,\ r \in \{1,2\}\Big)\mathbb{P}\Big(N_1^{(r)} \le \tfrac{1}{2} n^q \log n,\ r \in \{1,2\}\Big) \\ \ge &\left(1 - \frac{\frac{1}{2} n^q \log n}{n - n^q \log n}\right)^{\frac{1}{2} n^q \log n} \mathbb{P}\Big(N_1^{(r)} \le \tfrac{1}{2} n^q \log n,\ r \in \{1,2\}\Big) \to 1 \quad \text{as } n \to \infty.\end{aligned}$$

□

Proof of Lemma C.21. Remember that

$$\mathcal{L}^{(2)} = [n - T^{(1)}] \backslash [n - T^{(2)}] = [n - \lfloor n^q \rfloor - N_1^{(1)}] \backslash [n - \lfloor n^q \rfloor - N_1^{(1)} - N_1^{(2)}],$$

and using that $N_2^{(2)} = n - \sum_{k \in \{0,1,\star\}, r \in \{1,2\}} N_k^{(r)}$ we see

$$\Psi_2^{(2)} | \mathcal{N}^{(2)} \sim F_2(n - T^{(1)},\ N_2^{(2)})$$

where

$$N_2^{(2)} = n - T^{(2)} + \lfloor n^q \rfloor - N_0^{(1)} - N_\star^{(1)} - N_0^{(2)} - N_\star^{(2)}.$$

Let the literals of $\Psi_2^{(2)}$ be given by $(L_{j,1}, L_{j,2})$ for $j \in [N_2^{(2)}]$. If $n - T^{(2)} > N_2^{(2)}$ define additional random variables $(L_{j,1}, L_{j,2})$ for $j \in [N_2^{(2)} + 1, n - T^{(2)}]$, where conditional on $\mathcal{N}^{(2)}$ the pairs of random variables are independent and uniformly distributed in $\{(\ell_1,\ell_2) \in (\pm[n-T^{(1)}])^2 : |\ell_1| < |\ell_2|\}$. Define

$$\Phi' = \bigwedge_{j=1}^{n-T^{(2)}} (L_{j,1} \vee L_{j,2}),$$

and let also $\mathcal{L}' := \mathcal{L}^{(2)}$. Then

$$\begin{aligned}\mathbb{P}\Big((\Psi_2^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big) &\geq \mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT},\ n-T^{(2)} \geq N_2^{(2)}\Big) \\ &\geq \mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big) + \mathbb{P}\Big(n-T^{(2)} \geq N_2^{(2)}\Big) - 1.\end{aligned}$$

Note that

$$\Big\{n-T^{(2)} \geq N_2^{(2)}\Big\} \supseteq \Big\{N_\star^{(1)} + N_\star^{(2)} \geq n^q\Big\},$$

and thus this along with Lemma C.22 implies that $\lim_{n\to\infty}\mathbb{P}\Big(n-T^{(2)} \geq N_2^{(2)}\Big) = 1$. Thus

$$\liminf_{n\to\infty}\mathbb{P}\Big((\Psi_2^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big) \geq \liminf_{n\to\infty}\mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big). \tag{C.4.33}$$

Define now further

$$M_1^{(-1)} := \lfloor n^q \rfloor + N_1^{(1)}, \quad M_1^{(0)} := N_1^{(2)}, \quad \mathcal{M}^{(0)} := \sigma\Big(M_1^{(-1)}, M_1^{(0)}\Big).$$

Note that as $\mathcal{M}^{(0)} \subseteq \mathcal{N}^{(2)}$ and

$$\Phi'|\mathcal{N}^{(2)} \sim F_2\Big(n-T^{(1)}, n-T^{(2)}\Big) = F_2\Big(n-M_1^{(-1)}, n-M_1^{(-1)} + M_1^{(0)}\Big),$$

we get that

$$\Phi'|\mathcal{M}^{(0)} \sim F_2\Big(n-M_1^{(-1)}, M_1^{(-1)} + M_1^{(0)}\Big)$$

Moreover, the definitions imply that

$$\mathcal{L}' = [n-M_1^{(-1)}]\backslash[n-M_1^{(-1)} - M_1^{(0)}].$$

Lemma C.21 also gives that $\mathbb{E}[M_1^{(0)}] \leq C_0 n^q$ for some $C_0 > 0$ and also that

$$\lim_{n\to\infty}\mathbb{P}\Big(M_1^{(-1)} \leq n^q \log n\Big) = \lim_{n\to\infty}\mathbb{P}\Big(M_1^{(0)} \leq n^q \log n\Big) = 1$$

Thus, our defined elements satisfy all assumptions of Lemma C.11. Therefore

$$\liminf_{n\to\infty}\mathbb{P}\Big(\Phi'_{\mathcal{L}'} \in \mathsf{SAT}\Big) \geq \liminf_{n\to\infty}\mathbb{P}\Big(\Phi \in \mathsf{SAT}\Big).$$

Combining this with (C.4.33) establishes the lemma. $\square$

C.4.5 Proof of technical lemmas

We begin by proving Lemma C.4 and this Lemma is established by a coupling argument where literals are swapped. The swapping will not change the distribution of the resulting formula as the clauses are uniformly distributed.

Proof of Lemma C.4. Let φ be a non-random SAT-formula with n variables and m clauses and let $(\ell_{j,i})_{j\in[m],i\in[2]}$ denote its literals. Write $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$, where $|\ell_1| < \dots < |\ell_l|$ and let $\mathcal{L}_{abs} = \{|\ell_j| : j \in [f]\}$. Also let $0 < \ell_{f+1} < \dots < \ell_n \in [n]$ be defined such that $\{|\ell_1|, \dots, |\ell_n|\} = [n]$. Define a function $\Gamma : [n] \to [n]$ by letting $\Gamma(|\ell_i|) = n - i$ for $i \in [n]$. Then Γ is a permutation satisfying that $\Gamma(\mathcal{L}_{abs}) = \mathcal{L}'$, where $\mathcal{L}' = [n]\backslash[n-f]$. Define another function $\theta : [n] \to \{\pm 1\}$ where $\theta(|\ell_i|) = \mathrm{sgn}(\ell_i)$. Define a new SAT-formula φ' with literals $(\ell'_{j,i})_{j\in[m],i\in[2]}$, where

$$\{\ell'_{j,1}, \ell'_{j,2}\Big\} = \Big\{\theta(|\ell_{j,i}|) \cdot \mathrm{sgn}(\ell_{j,i}) \cdot \Gamma(|\ell_{j,i}|) : i \in [2]\Big\}.$$

Then we define $G(\varphi, \mathcal{L}) := \varphi'$. Let $x = (x_1, \dots, x_n) \in \mathbb{B}^n$ and define $x' = (x'_1, \dots, x'_n) \in \mathbb{B}^n$ by letting $x'_v = x_{\Gamma^{-1}(v)}$ for $v \in [n]$. Note that $x \mapsto x'$ is a bijection. Let for $j \in [m]$, $i \in [2]$ be chosen such that $\ell'_{j,1} = \theta(|\ell_{j,i}|) \cdot \mathrm{sign}(\ell_{j,i}) \cdot \Gamma(|\ell_{j,i}|)$.

Now, if $\ell_{j,i} \in \mathcal{L}$ then $(\ell_{j,i})_{\mathcal{L}}(x) = \texttt{true}$. Also, there exists a $v \in [f]$ such that $\ell_{j,i} = \ell_v$ and also $\Gamma(|\ell_v|) \in \mathcal{L}'$. Thus

$$(l'_{j,1})_{\mathcal{L}'}(x') = \Big[\theta(|\ell_v|) \cdot \mathrm{sgn}(\ell_v) \cdot \Gamma(|\ell_v|)\Big]_{\mathcal{L}'}(x') = \Gamma(|\ell_v|)_{\mathcal{L}'}(x') = \texttt{true}.$$

If $-\ell_{j,i} \in \mathcal{L}$ then $(\ell_{j,i})_{\mathcal{L}}(x) = \texttt{false}$. Again there exists $v \in [l]$ such that $\ell_{j,i} = -\ell_v$ and also $\Gamma(|\ell_v|) \in \mathcal{L}'$ and thus

$$(l'_{j,1})_{\mathcal{L}'}(x') = \Big[\theta(|\ell_v|) \cdot \mathrm{sgn}(-\ell_v) \cdot \Gamma(|\ell_v|)\Big]_{\mathcal{L}'}(x') = -\Gamma(|\ell_v|)_{\mathcal{L}'}(x') = \texttt{false}.$$

Lastly, if $\pm\ell_{j,i} \notin \mathcal{L}$ then $(\ell_{j,i})_{\mathcal{L}}(x) = \ell_{j,i}(x)$ and also $\pm\Gamma(|\ell_{j,i}|) \notin \mathcal{L}'$. Therefore

$$(l'_{j,1})_{\mathcal{L}'}(x') = \Big[\mathrm{sgn}(\ell_{j,i}) \cdot \Gamma(|\ell_{j,i}|)\Big](x') = \mathrm{sgn}(\ell_{j,i}) \cdot x'_{\Gamma(|\ell_{j,i}|)} = \mathrm{sgn}(\ell_{j,i}) \cdot x_{|\ell_{j,i}|} = \ell_{j,i}(x).$$

Repeating the argument on $\ell'_{j,2}$ implies that

$$(l_{j,1} \vee l_{j,2})_{\mathcal{L}}(x) = (\ell j, 1' \vee l'_{j,2})_{\mathcal{L}'}(x'),$$

and thus $\varphi_{\mathcal{L}} \in \mathsf{SAT}$ if and only if $\varphi'_{\mathcal{L}'} \in \mathsf{SAT}$.

Let $\Phi \sim F_2(n, m)$ and define $\Phi' = G(\Phi, L)$. Then the above argument implies that

$$\Big\{G(\Phi, L) \in \mathsf{SAT}\Big\} = \Big\{\Phi'_{[n]\backslash[n-l]} \in \mathsf{SAT}\Big\}.$$

Let $(L_{j,i})_{j\in[m],i\in[2]}$ be the random literals of Φ and let $(L'_{j,i})_{j\in[m],i\in[2]}$ be the random literals of Φ'. Note that as the clause $\Big(L'_{j,1}, L'_{j,2}\Big)$ is constructed from $\Big(L_{j,1}, L_{j,2}\Big)$ for each $j \in [m]$ the clauses of Φ' are independent. Let $j \in [m]$ and assume WLOG that $\Gamma(|L_{j,1}|) < \Gamma(|L_{j,2}|)$. Then, for $(\ell_1', \ell_2') \in (\pm[n])^2$ with $|\ell_1'| < |\ell_2'|$ we have

$$\begin{aligned}
&\mathbb{P}\Big(L_{j,i}' = \ell_i',\ i \in [2]\Big) \\
=&\mathbb{P}\Big(\theta(|L_{j,i}|) \cdot \mathrm{sgn}(L_{j,i}) \cdot \Gamma(|L_{j,i}|) = \ell_i',\ i \in [2]\Big) \\
=&\mathbb{P}\Big(|L_{j,i}| = \Gamma^{-1}(|\ell_i'|),\ \mathrm{sgn}(L_{j,i}) = \theta\Big(\Gamma^{-1}(|\ell_i'|)\Big) \cdot \mathrm{sgn}(\ell_i'),\ i \in [2]\Big) \\
=&\mathbb{P}\Big(L_{j,i} = \ell_i,\ i \in [2]\Big),
\end{aligned}$$

where $\ell_i = \theta\Big(\Gamma^{-1}(\ell_i')\Big) \cdot \mathrm{sgn}(\ell_i') \cdot \Gamma^{-1}(|\ell_i'|)$ for $i \in [2]$ and as the clause $(L_{j,1}, L_{j,2})$ is uniformly distributed, the result follows. □

More or less direct calculations imply the next lemma. We recall that equation (C.3.1) defines the sets

$$\begin{aligned}
\mathcal{A}_0(n,f) &:= -\mathcal{L} \times -\mathcal{L}, \quad \mathcal{A}_1(n,f) := \pm[n-f] \times -\mathcal{L}, \\
\mathcal{A}_2(n,f) &:= \pm[n-f] \times \pm[n-f], \quad \mathcal{A}_\star(n,f) := \pm[n] \times \mathcal{L}.
\end{aligned}$$

Proof of Lemma C.6. Let $\Phi \sim F_2(n,m)$ and let $L = (L_{j,i})_{j\in[m], i\in[2]}$ be its literals. As the clauses are i.i.d. and

$$M_k = \Big|\Big\{j \in [m] : (L_{j,1}, L_{j,2}) \in \mathcal{A}_k(n,f)\Big\}\Big|, \quad (k \in K),$$

where each clause belongs to exactly one of the sets $\mathcal{A}_k(n,f)$ for $k \in K$ this implies that

$$M := (M_0, M_1, M_2, M_\star) \sim \mathrm{Multinomial}\Big(m,\ p(n,f)\Big),$$

where $p = (p_0, p_1, p_2, p_\star)$ and $p_k(n,f) = \mathbb{P}\Big((L_{1,1}, L_{1,2}) \in \mathcal{A}_k(n,l)\Big)$ for $k \in K$. As the clauses are uniformly distributed on $\mathcal{D} = \{(\ell_1, \ell_2) \in (\pm[n])^2 : |\ell_1| < |\ell_2|\}$ we further get that $p_k(n,l) = \frac{|\mathcal{A}_k(n,f) \cap \mathcal{D}|}{|\mathcal{D}|}$ for $k \in K$, so

$$\begin{aligned}
p_0(n,f) &= \frac{\binom{f}{2}}{2^2\binom{n}{2}} = \frac{f(f-1)}{4n(n-1)}, \\
p_1(n,f) &= \frac{2(n-f)f}{2^2\binom{n}{2}} = \frac{(n-f)f}{n(n-1)}, \\
p_2(n,f) &= \frac{2^2\binom{n-f}{2}}{2^2\binom{n}{2}} = \frac{(n-f)(n-f-1)}{n(n-1)}, \\
p_\star(n,f) &= 1 - p_0(n,f) - p_1(n,f) - p_2(n,f) = \frac{f(n - \frac{f}{4} - \frac{3}{4}))}{n(n-1)},
\end{aligned}$$

We will need the following result to establish the last part of the lemma. For X, Y independent random functions, sets A, B, and elements x, y with $x \in A$ and $y \in B$ we have

$$\mathbb{P}\Big(X = x, Y = y | X \in A, Y \in B\Big) = \mathbb{P}\Big(X = x | X \in A\Big)\mathbb{P}\Big(Y = y | Y \in B\Big).$$

Define $\mathcal{C}_k = \Big\{j \in [m] : (L_{j,1}, L_{j,2}) \in \mathcal{A}_k(n, f)\Big\}$ for $k \in K$ and let $\mathcal{C} = (\mathcal{C}_k)_{k\in K}$. For elements $\ell_{j,1} \in \pm[n-f]$ for $j \in \mathcal{C}_1$ and $(\ell_{j,1}, \ell_{j,2}) \in \mathcal{A}_2(n, f)$ for $j \in \mathcal{C}_2$ we use the independence of the clauses and the above equation and get

$$\begin{aligned}
\mathbb{P}\Big(\Phi_1 = \bigwedge_{j\in\mathcal{C}_1} (\ell_{j,1})\Big|\mathcal{C}\Big) &= \prod_{j\in\mathcal{C}_1} \mathbb{P}\Big(L_{j,1} = \ell_{j,1}\Big| j \in \mathcal{C}_1\Big), \\
\mathbb{P}\Big(\Phi_2 = \bigwedge_{j\in\mathcal{C}_2} (\ell_{j,1} \vee \ell_{j,2})\Big|\mathcal{C}\Big) &= \prod_{j\in\mathcal{C}_2} \mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2})\Big| j \in \mathcal{C}_2\Big),
\end{aligned} \tag{C.4.34}$$

and

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1 = \bigwedge_{j\in\mathcal{C}_1} (\ell_{j,1}),\ \Phi_2 = \bigwedge_{j\in\mathcal{C}_2} (\ell_{j,1} \vee \ell_{j,2})\Big|\mathcal{C}\Big) \\
&= \prod_{j\in\mathcal{C}_1} \mathbb{P}\Big(L_{j,1} = \ell_{j,1} | j \in \mathcal{C}_1\Big) \prod_{j\in\mathcal{C}_2} \mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2}) | j \in \mathcal{C}_2\Big).
\end{aligned} \tag{C.4.35}$$

Now, using that the clauses are uniformly distributed on $\mathcal{D}$ along with the definitions of the sets $\mathcal{A}_k(n, f)$, $k \in \{1, 2\}$, we first get for $j \in \mathcal{C}_1$

$$\begin{aligned}
\mathbb{P}\Big(L_{j,1} = \ell_{j,1}\Big| j \in \mathcal{C}_1\Big) &= \sum_{\ell_{j,2}\in-\mathcal{L}} \mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2})\Big| j \in \mathcal{C}_1\Big) \\
&= \sum_{\ell_{j,2}\in-\mathcal{L}} \frac{\mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2})\Big)}{\mathbb{P}\Big((L_{j,1}, L_{j,2}) \in \mathcal{A}_1(n, f)\Big)} = l \cdot \frac{\frac{1}{2^2\binom{n}{2}}}{p_1(n, f)} = \frac{1}{2\binom{n-f}{1}},
\end{aligned}$$

and next for $j \in \mathcal{C}_2$

$$\begin{aligned}
\mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2})\Big| j \in \mathcal{C}_2\Big) &= \frac{\mathbb{P}\Big((L_{j,1}, L_{j,2}) = (\ell_{j,1}, \ell_{j,2})\Big)}{\mathbb{P}\Big((L_{j,1}, L_{j,2}) \in \mathcal{A}_2(n, l)\Big)} \\
&= \frac{\frac{1}{2^2\binom{n}{2}}}{p_2(n, f)} = \frac{1}{2^2\binom{n-f}{2}}.
\end{aligned}$$

Inserting this in (C.4.34) gives

$$\mathbb{P}\Big(\Phi_1 = \bigwedge_{j\in\mathcal{C}_1} (\ell_{j,1})\Big|\mathcal{C}\Big) = \left(\frac{1}{2\binom{n-f}{1}}\right)^{M_1}$$

and

$$\mathbb{P}\Big(\Phi_2 = \bigwedge_{j\in\mathcal{C}_2}(\ell_{j,1}\vee\ell_{j,2})\Big|\mathcal{C}\Big) = \left(\frac{1}{2^{2\binom{n-f}{2}}}\right)^{M_2}.$$

Thus for φ_1 a 1-SAT formula with $n-l$ variables and M_1 clauses and φ_2 a 2-SAT formula with $n-l$ variables and M_2 clauses, we get

$$\mathbb{P}\Big(\Phi_1 = \varphi_1\Big|M\Big) = \mathbb{E}\Big[\mathbb{P}\Big(\Phi_1 = \varphi_1\Big|\mathcal{C}\Big)\Big|M\Big] = \left(\frac{1}{2\binom{n-l}{1}}\right)^{M_1},$$
$$\mathbb{P}\Big(\Phi_2 = \varphi_2\Big|M\Big) = \mathbb{E}\Big[\mathbb{P}\Big(\Phi_2 = \varphi_2\Big|\mathcal{C}\Big)\Big|M\Big] = \left(\frac{1}{2^2\binom{n-l}{2}}\right)^{M_2},$$

and this corresponds to having $\Phi_k|M \sim F_k(n-l, M_k)$ for $k\in\{1,2\}$. Repeating this argument with equation (C.4.35) gives that

$$\mathbb{P}\Big(\Phi_1 = \varphi_1,\, \Phi_2 = \varphi_2\Big|M\Big) = \mathbb{P}\Big(\Phi_1 = \varphi_1\Big|M\Big)\mathbb{P}\Big(\Phi_2 = \varphi_2\Big|M\Big)$$

which implies the conditional independence. □

References

[Ach+01a] Dimitris Achlioptas et al. "Rigorous results for random (2+ p)-SAT". In: *Theoretical Computer Science* 265.1-2 (2001), pp. 109–129.

[Ach+01b] 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*. 2001, pp. 721–722.

[Ach+21] Dimitris Achlioptas et al. "The number of satisfying assignments of random 2-SAT formulas". In: *Random structures & algorithms* 58.4 (2021), pp. 609–647.

[Ach00] Dimitris Achlioptas. "Setting 2 variables at a time yields a new lower bound for random 3-SAT (extended abstract)". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC '00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 28–37.

[ANN04] Krishna B Athreya, Peter E Ney, and PE Ney. *Branching processes*. Courier Corporation, 2004.

[BCM02] Giulio Biroli, Simona Cocco, and Rémi Monasson. "Phase transitions and complexity in computer science: an overview of the statistical physics approach to the random satisfiability problem". In: *Physica A: Statistical Mechanics and its Applications* 306 (2002), pp. 381–394.

[Bol+01] Béla Bollobás et al. "The scaling window of the 2-SAT transition". In: *Random Structures & Algorithms* 18.3 (2001), pp. 201–256.

[BOS25] Andreas Basse-O'Connor, Tobias Lindhardt Overgaard, and Mette Skjøtt. "On the Regularity of Random 2-SAT and 3-SAT". In: *arXiv:2504.11979 [math.PR]* (2025).

[CF86] Ming-Te Chao and John Franco. "Probabilistic analysis of two heuristics for the 3-satisfiability problem". In: *SIAM Journal on Computing* 15.4 (1986), pp. 1106–1118.

[Cha+24] Arnab Chatterjee et al. "The number of random 2-SAT solutions is asymptotically log-normal". In: *arXiv preprint arXiv:2405.03302* (2024).

[CKT+91] Peter C Cheeseman, Bob Kanefsky, William M Taylor, et al. "Where the really hard problems are". In: *Ijcai*. Vol. 91. 1991, pp. 331–337.

[Coo71] Stephen A. Cook. "The Complexity of Theorem-Proving Procedures". In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC '71. 1971, pp. 151–158.

[CR92] Vašek Chvátal and Bruce Reed. "Mick gets some (the odds are on his side)(satisfiability)". In: *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*. IEEE Computer Society. 1992, pp. 620–627.

[DLL62] Martin Davis, George Logemann, and Donald Loveland. "A machine program for theorem-proving". In: *Communications of the ACM* 5.7 (1962), pp. 394–397.

[DM11] Claude Dellacherie and P-A Meyer. *Probabilities and potential, c: potential theory for discrete and continuous semigroups*. Elsevier, 2011.

[GGW06] Aarti Gupta, Malay K Ganai, and Chao Wang. "SAT-based verification methods and applications in hardware verification". In: *International School on Formal Methods for the Design of Computer, Communication and Software Systems*. Springer, 2006, pp. 108–143.

[Goe96] Andreas Goerdt. "A threshold for unsatisfiability". In: *Journal of Computer and System Sciences* 53.3 (1996), pp. 469–486.

[Gol79] Allen T. Goldberg. "On the Complexity of the Satisfiability Problem". In: *Fourth Workshop on Automated Deduction*. CADE-4. Austin, Texas, USA: Association for Automated Reasoning Inc., 1979, pp. 1–6.

[GW94] Ian P Gent and Toby Walsh. "The SAT phase transition". In: *ECAI*. Vol. 94. PITMAN. 1994, pp. 105–109.

[Knu15] Donald E Knuth. *The art of computer programming, Volume 4, Fascicle 6: Satisfiability*. Addison-Wesley Professional, 2015.

[KS94] Scott Kirkpatrick and Bart Selman. "Critical behavior in the satisfiability of random boolean expressions". In: *Science* 264.5163 (1994), pp. 1297–1301.

[La 01] W Fernandez de La Vega. "Random 2-SAT: results and problems". In: *Theoretical computer science* 265.1-2 (2001), pp. 131–146.

[Mar08] Joao Marques-Silva. "Practical applications of boolean satisfiability". In: *2008 9th International Workshop on Discrete Event Systems*. IEEE. 2008, pp. 74–80.

[Pap94] Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994, pp. xvi+523.

[SML96] Bart Selman, David G. Mitchell, and Hector J. Levesque. "Generating Hard Satisfiability Problems". In: *Artif. Intell.* 81 (1996), pp. 17–29.

[SSZ22] Allan Sly, Nike Sun, and Yumeng Zhang. "The number of solutions for random regular NAE-SAT". In: *Probab. Theory Related Fields* 182.1-2 (2022), pp. 1–109.

Article D

Majority Rule Policy in Random 2-SAT and 3-SAT

Andreas Basse-O'Connor[1], Tobias Overgaard[1], and Mette Skjøtt[1,2]

[1]Department of Mathematics, Aarhus University,
[2]Kvantify Aps

April 2025

Abstract: The DPLL class of algorithms for the SAT problem constructs consistent partial assignments based on a given heuristic. In this paper, we quantify precisely the impact of using the majority rule heuristic on random k-SAT instances for $k = 2, 3$, compared to a baseline heuristic that selects variable assignments uniformly at random. The main contribution of this paper is the closed-form mathematical expression for this impact. Specifically, we show that, when the probability of generating a consistent partial assignment is fixed, the majority rule allows the algorithm to assign a factor of $(1 - e^{-k\alpha}(I_0 + I_1)(k\alpha))^{-1}$ more variables. Here, α denotes the clause density, and I_0 and I_1 are modified Bessel functions of the first kind.

D.1 Introduction

D.1.1 Background

The Boolean k-satisfiability (k-SAT) problem is a fundamental problem in theoretical computer science; for $k \geq 3$, the problem is NP-complete [Coo71], meaning that an answer to the question of whether it is generally possible to solve the problem in polynomial time resolves the famous P vs. NP problem. Furthermore, the 2-SAT problem is NL-complete [Pap94, Thm. 16.3], meaning that an answer to the question of whether the problem can be solved in logarithmic space resolves the L vs. NL problem. Effective algorithms for solving k-SAT problem instances also have major practical implications for electronic design automation, artificial intelligence, computational biology, and more (see for instance [Mar08]).

The k-SAT problem asks the following: given m k-clauses $C_1, \ldots, C_m$ on n Boolean variables, does there exist an assignment of the variables in $\{-1, 1\}^n$ satisfying all clauses? By a k-clause we understand a function of the form $C(x) = s_1 x_{v_1} \vee \cdots \vee s_k x_{v_k}$ for $s_1, \ldots, s_k \in \{-1, 1\}$ and $v_1, \ldots, v_k \in [n] := \{1, \ldots, n\}$. Putting $\Phi := C_1 \wedge \cdots \wedge C_m$, we say in the affirmative case that Φ is *satisfiable* and write $\Phi \in \mathsf{SAT}$. Here, $\vee$ and $\wedge$ denote maximum and minimum, respectively. We let α denote the *clause density*, $\alpha := m/n$.

In light of the difficulty in finding effective general algorithms for SAT, there has been a focus in the literature on finding algorithms that perform well 'on average' or with high probability (w.h.p.). Such statements require a distribution over the space of k-SAT problem instances, and in this article we adopt the following model: in each clause, the signs $S_1, \ldots, S_k$ and the variables $V_1, \ldots, V_k$ are sampled i.i.d. uniformly at random, and the m clauses $C_1, \ldots, C_m$ are again sampled i.i.d. uniformly at random. Some of the following results mentioned use a slightly different model for sampling random k-SAT instances.

In this paper, we calculate the exact impact of the majority rule policy for choosing the values of the variables x_v in a common type of SAT-solver, namely DPLL. To the best of the authors' knowledge, this is the first result of its kind giving such a precise description of the effect of tweaking certain elements in a SAT-solving algorithm. One consequence of our result is that, for random 2−SAT, the majority rule policy finds at least twice as many "correct" assignments (i.e. that are consistent with the clauses) compared to selecting values randomly. For random 3-SAT, it finds at least 1/3 more.

D.1.2 DPLL algorithms

In [Knu15], Knuth highlights the importance of partial assignments: "Algorithms for SAT usually deal exclusively with consistent partial assignments; the goal is to convert them to consistent total assignments, by gradually eliminating the unknown values." Creating consistent partial assignments boils down to fixing (the value of) the variables $x_1, \dots, x_n$ in a clever way. For convenience we represent the *literals* x_v as v and $-x_v$ as $-v$, and we let $\Phi|sv$ denote the instance Φ with the variable x_v fixed to s, which has the effect of satisfying (and thus removing) all clauses in which the literal sx_v appears, and deleting any appearances of $-sx_v$ in every clause, thus shortening the lengths of the affected clauses. We call a subset $\mathcal{L}$ of $\pm[n] := \{-n, \dots, -1, 1, \dots, n\}$ *consistent* if, for all $v \in [n]$, at most one of v and $-v$ is in $\mathcal{L}$. For a consistent subset $\mathcal{L} = \{s_1 v_1, \dots, s_f v_f\} \subseteq \pm[n]$ we define iteratively

$$\Phi_{\mathcal{L}} := \Phi|s_1 v_1| \cdots |s_f v_f,$$

noting that the order in which we fix the variables is irrelevant.

Algorithms which generate partial assignments by fixing variables one at a time are broadly known as *DPLL* algorithms, named after Davis, Putnam, Logemann, and Loveland in [DP60; DLL62]. The basic form of a DPLL algorithm without backtracking, which we call DPLL$^-$, is outlined in algorithm 1. Here, we define a 0-clause, or empty clause, as the constant function -1, which occurs if all literals are deleted from a clause (leaving it empty). The presence of an empty clause precludes the satisfiability of the corresponding k-SAT instance.

Algorithm 1: Basic form of DPLL without backtracking (DPLL$^-$)

Data: k-SAT instance Φ
Result: Success or Failure to find consistent total assignment

```
while there are unset variables do
    choose unset variable v ∈ [n]
    choose sign s ∈ {−1, 1}
    update Φ ← Φ|sv
end
if Φ has empty clause then
    Failure
else
    Success
end
```

Algorithm 1 represents a class of algorithms, as one must specify which heuristic is used to choose the variable v and sign s, called the *strategy* and *policy*, respectively (terminology from [AS00]). The original algorithm from [DLL62] used the *unit clause* (UC) and *pure literal* strategies. Here, we use the term "DPLL algorithm" more broadly, as "[the term] refers generally to SAT solving via partial assignment and backtracking" (quote from [Knu15]). The vast majority of analytical results concerning the performance of DPLL-type algorithms on the random

k-SAT problem do not consider backtracking, i.e. they analyze the performance of DPLL$^-$. In all cases considered, the strategy and policy take at most polynomial time to employ so that the entire DPLL$^-$ runs in polynomial time.

In this article, we analyze how the specific choice of policy affects the success of DPLL$^-$. Specifically, we quantify the exact impact of the *majority rule* (MR) policy, which selects s based on whether x_v or $-x_v$ appear most often in Φ. This can be seen as a greedy procedure which satisfies as many clauses in Φ as possible at each step. Our main contribution is the closed-form expression of the probability that the procedure generates a consistent partial assignment at any given step, and the impact of the MR policy compared to the naive policy of setting signs randomly, given in Theorem D.1 and Corollary D.2 below, respectively.

Other heuristics, such as UC, pure literal, and *shortest clause* strategy, are well-studied in the literature, see for instance [Gol79; FP83; Fra84; Fra86; CF86; FPR87; FH88; CF90; CR92; BFU93; FS96; SML96; Ach00; AS00; HS03; KKL06; BOS25]. No closed-form expressions of relative algorithm performances using different heuristics were previously found, although in [FS96], the exact probability for success using a generalized version of UC is calculated. Most recently, it was shown in [HS03; KKL06] that a DPLL$^-$ algorithm succeeds on the random 3-SAT problem with probability bounded away from 0 (which can be improved to "w.h.p." by introducing a small amount of backtracking as shown in [FS96]) when $\alpha < 3.52$, showing in particular that random 3-SAT is satisfiable w.h.p. when $\alpha < 3.52$. Experimental evidence suggests that the median running time for complete DPLL-type algorithms on the random 3-SAT problem can be polynomial even for clause densities up till 3.8 (see [Coa+03]), after which they are expected to require exponential time, even though random 3-SAT is believed to be satisfiable w.h.p. for all $\alpha < 4.267\ldots$ [CA96; MZ02].

D.1.3 Main result

Let Φ be the random k-SAT problem with n variables and $m \sim \alpha n$ clauses. Here, $\sim$ means asymptotic equivalence, so $f \sim g$ means $f/g \to 1$ as $n \to \infty$ for positive functions f, g of n. Let A_v^+ (resp. A_v^-) denote the number of times v (resp. $-v$) appears among the random literals defining Φ for each $v \in [n]$.

If $\mathcal{L} \subseteq [n]$ denotes the variables to be fixed (for instance $\mathcal{L} = [f] = \{1, 2, \ldots, f\}$ for some $f = f(n)$), we then define

$$\mathcal{L}_{\mathrm{MR}} := \Big\{ sv \colon v \in \mathcal{L}, s = \operatorname{sgn}(A_v^+ - A_v^-) \Big\},$$

where we take $\operatorname{sgn}(0) := 1$ as our convention. That is, for each $v \in \mathcal{L}$, we are fixing x_v to $s_{\mathrm{MR}} := \operatorname{sgn}(A_v^+ - A_v^-)$, i.e. in accordance with which of x_v and $-x_v$ is in majority in Φ, breaking ties with $s_{\mathrm{MR}} = 1$. It is clear that $\mathcal{L}_{\mathrm{MR}}$ is a consistent (random) subset of $\pm[n]$, which depends on Φ. We put

$$\alpha_{\mathrm{b}}(2) := 1 \quad \text{and} \quad \alpha_{\mathrm{b}}(3) := 3.145.$$

For $k = 2, 3$ it is known that Φ is satisfiable w.h.p. when $\alpha < \alpha_b(k)$ from [CR92; Goe96] and [Ach00], respectively. For 2-SAT, this is the optimal bound in the sense that Φ is unsatisfiable w.h.p. when $\alpha > 1 = \alpha_b(2)$. For 3-SAT, it is still an open question whether there even exists such a sharp threshold for satisfiability. In any case, our result does leave a slight gap to the best known bound for satisfiability of the random 3-SAT problem, namely $\alpha < 3.52$ from [HS03; KKL06]. Our main result is as follows, where we interpret $e^{-\infty} := 0$.

Theorem D.1. *Let $k = 2$ or $k = 3$, $\alpha \in (0, \alpha_b(k))$, and $\beta \in [0, \infty]$. Let Φ be the random k-SAT problem with n variables and $m \sim \alpha n$ clauses, and let $\mathcal{L} \subseteq [n]$ be a non-random set such that $|\mathcal{L}|/n^{1-1/k} \to \beta$. Then*

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \begin{cases} \exp\Big(-\big(\frac{\beta}{2}\big)^2 \frac{\alpha}{1-\alpha}\Big[1 - e^{-2\alpha}(I_0 + I_1)(2\alpha)\Big]^2\Big), & \text{if } k = 2, \\ \exp\Big(-\big(\frac{\beta}{2}\big)^3 \alpha\Big[1 - e^{-3\alpha}(I_0 + I_1)(3\alpha)\Big]^3\Big), & \text{if } k = 3, \end{cases}$$

where I_0 and I_1 are modified Bessel functions of the first kind.

We define for all $z \geq 0$

$$\mu_z := e^{-z}(I_0(z) + I_1(z)) = \frac{1}{\pi}\int_0^\pi e^{z(\cos(t)-1)}(\cos(t) + 1)\,dt, \tag{D.1.1}$$

where the second equality comes from well-known integral representations of the modified Bessel functions of the first kind.

Theorem D.1 gives the exact probability that the partial assignment created by algorithm 1 is still consistent after $|\mathcal{L}|$ steps when using the MR policy (and the "blind" strategy, choosing variables independently from Φ). In particular, this version of DPLL$^-$ can set/fix at most $O(n^{1-1/k})$ variables in the random k-SAT problem while still retaining a positive probability of generating a *consistent* partial assignment when $k = 2, 3$.

To measure the *impact* of the MR policy, we consider as a comparison ground a stripped "baseline" version of DPLL$^-$, which uses the simplest possible strategy and policy—that is, it simply sets each of the variables to 1 (or some other predetermined signs). Let $\mathcal{L}$ be a consistent subset of $\pm[n]$ (e.g. $\mathcal{L} = [f]$), where $|\mathcal{L}|/n^{1-1/k} \to \beta$ for some $\beta \in [0, \infty]$. In [BOS25] it was shown that, for $\alpha \in (0, \alpha_b(k))$:

$$\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \begin{cases} \exp\Big(-\big(\frac{\beta}{2}\big)^2 \frac{\alpha}{1-\alpha}\Big), & \text{if } k = 2, \\ \exp\Big(-\big(\frac{\beta}{2}\big)^3 \alpha\Big), & \text{if } k = 3. \end{cases} \tag{D.1.2}$$

We will use this result as a baseline comparison when introducing the MR policy. Indeed, comparing this baseline version of algorithm 1 with Theorem D.1, we get the following conclusion. Note in regards to the following that $\mathcal{L}_{\mathrm{MR}}$ depends on Φ, while $\mathcal{L}_0$ does not.

Corollary D.2. *Let $k = 2$ or $k = 3$, $\alpha \in (0, \alpha_b(k))$, and $\beta_0, \beta_{MR} \in (0, \infty)$. Let Φ be the random k-SAT problem with n variables and $m \sim \alpha n$ clauses, and let $\mathcal{L}_0 \subseteq \pm[n]$ be consistent and $\mathcal{L} \subseteq [n]$ be arbitrary such that $|\mathcal{L}_0| \sim \beta_0 n^{1-1/k}$ and $|\mathcal{L}| \sim \beta_{MR} n^{1-1/k}$. Then $\mathbb{P}(\Phi_{\mathcal{L}_0} \in \mathsf{SAT}) \sim \mathbb{P}(\Phi_{\mathcal{L}_{MR}} \in \mathsf{SAT})$ if and only if*

$$\beta_{MR} = (1 - \mu_{k\alpha})^{-1} \beta_0.$$

Corollary D.2 quantifies the exact impact of the MR policy. Namely, compared to using the MR policy, the number of variables we can fix drops by a factor of $\mu_{k\alpha}$ when using the trivial policy in algorithm 1 in the random k-SAT problem—for $k = 2, 3$ when $\alpha \in (0, \alpha_b(k))$. Since $I_0(k\alpha) \geq 1$ and $I_1(k\alpha) \geq 0$, we see that $\mu_{k\alpha} > 0$, and hence $\beta_{MR} > \beta_0$. However, in the following, we will find that β_{MR} is (depending on k and α) in most cases quite a bit larger than β_0, meaning that the MR policy has quite a large impact on the performance of algorithm 1. In the following, we study exactly how large this impact is.

D.1.4 The impact of MR

We have seen in Corollary D.2 that, compared to the baseline version of DPLL$^-$, if we retain the same (asymptotic) probability of having generated a consistent partial assignment at any given step, then we are able to increase the number of fixed variables by a factor of $(1 - \mu_{k\alpha})^{-1}$ by employing the MR policy. In this section, we study properties of this factor.

Proposition D.3. *With $\mu_{k\alpha}$ defined in* (D.1.1) *for $k \in \mathbb{N}$ and $\alpha > 0$, it holds that $(1 - \mu_{k\alpha})^{-1}$ is real analytic, strictly decreasing, and convex in α, tends towards ∞ as $\alpha \to 0$, and is strictly decreasing in k.*

Proof. This follows from a standard calculus argument using known properties and derivatives of the modified Bessel functions of the first kind. □

Calculating using Mathematica, we find $(1 - \mu_2)^{-1} \approx 2.09$, so using the MR policy, we can always fix at least twice as many variables than with the trivial policy for random 2-SAT. For random 3-SAT, we get $(1 - \mu_{3 \cdot 3.145})^{-1} \approx 1.34$, so for the regime considered in this article, we can always fix at least a factor 1/3 extra variables. In both cases, this factor can get arbitrarily large as $\alpha \to 0$. Intuitively, this is because the MR policy gets more powerful when there are fewer duplicate variables in Φ; and the average number of times a given variable v occurs (negated or not) is (in the limit) equal to $k\alpha$. This also gives an intuitive explanation for why the MR policy is more powerful for random 2-SAT than 3-SAT; there are fewer duplicate literals in the former.

Since $\mu_{k\alpha}$ is analytic in α, so is the limit $\lim_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}_{MR}} \in \mathsf{SAT})$ from Theorem D.1 as a function of $\alpha < \alpha_b$ for both 2-SAT and 3-SAT. For 2-SAT, the probability

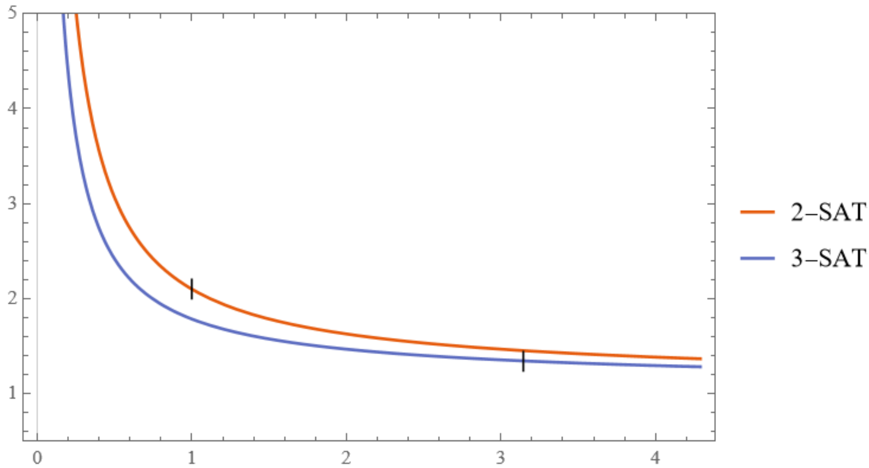


Figure D.12: Plot of $(1-\mu_{k\alpha})^{-1}$ as a function of α for $k=2,3$ with lines indicating $\alpha_{\mathrm{b}}(k)$.

decays to 0 continuously as $\alpha \to 1$, but for 3-SAT the probability does not approach 0 as α approaches any finite value—unless it loses its analyticity at some point after $\alpha_{\mathrm{b}}(3)$. This shows that random 3-SAT is in some sense less "regular", and hence more sensitive to small changes in the clause density α, than random 2-SAT when fixing variables using the MR policy.

D.2 Proof

We now proceed to give a proof of Theorem D.1. We face the minor technical issue that (D.1.2), which is used in the proof of Corollary D.2 and in the following, is proved for a slightly different model—which we will call $F_k(n,m)$—than the one considered in this article—call this model $G_k(n,m)$. We will rectify this in section D.2.3, and so for now we simply assume that these results hold for $G_k(n,m)$. Furthermore, [BOS25] proves a useful result concerning random mixed SAT problems, which we state below and also prove for our model in section D.2.3.

Lemma D.4. *For $k=2,3$, let Φ_k be the random k-SAT problem with m_k clauses and n variables, i.e. Φ_k is distributed according to $G_k(n,m_k)$, where $m_3 \sim \alpha n$ for some $\alpha < \alpha_{\mathrm{b}}(3)$ and $m_2 = o(n)$, such that Φ_3 and Φ_2 are independent, and let $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| = o(n^{2/3})$. Then $(\Phi_3 \wedge \Phi_2)_{\mathcal{L}}$ is satisfiable w.h.p.*

D.2.1 First part: random 2-SAT

Let $\Phi = C_1 \wedge \cdots \wedge C_m$ be the random 2-SAT problem with n variables and $m \sim \alpha n$ clauses where $\alpha \in (0, 1)$. Let $\mathcal{L} \subseteq [n]$ be such that $|\mathcal{L}| \sim \beta\sqrt{n}$. We assume without loss of generality that $\beta > 0$ (the remaining cases follow by taking $\beta \to 0$, and $\beta \to \infty$, respectively). Observe that each of the clauses $C_j = L_{j,1} \vee L_{j,2}$ experiences one of four fates when the variables dictated by $\mathcal{L}_{\mathrm{MR}}$ are fixed:

0) both of $L_{j,1}$ and $L_{j,2}$ get fixed to -1, so C_j becomes a 0-clause, i.e. is unsatisfied, and thus precludes the satisfiability of $\Phi_{\mathcal{L}_{\mathrm{MR}}}$,

1) exactly one of $L_{j,1}$ and $L_{j,2}$ gets fixed to -1, and the other remains unaffected, so C_j becomes a 1-clause and thus dictates the value of a new variable,

2) none of $L_{j,1}$ and $L_{j,2}$ get fixed, so C_j remains unaltered as a 2-clause,

⋆) one of $L_{j,1}$ and $L_{j,2}$ gets fixed to 1, so C_j becomes a ⋆-clause, i.e. is satisfied, and thus no longer affects the satisfiability of $\Phi_{\mathcal{L}_{\mathrm{MR}}}$.

Define $K := \{0, 1, 2, \star\}$. The core of the proof is understanding and carefully controlling how many clauses land in each of the four cases above, and especially important are cases 0) and 1). We denote for each $h \in K$:

$$\mathcal{C}_h := \{j \in [m] \colon C_j \text{ falls into case } h\}, \quad M_h = |\mathcal{C}_h|. \tag{D.2.1}$$

Put $\mathcal{C} := (\mathcal{C}_h)_{h\in K}$. The unit clauses (1-clauses) corresponding to $\mathcal{C}_1$ form a random 1-SAT instance $\Phi_1 := \min\{C_j \colon j \in \mathcal{C}_1\}$, which must be satisfiable in order for $\Phi_{\mathcal{L}_{\mathrm{MR}}}$ to be satisfiable, and furthermore, they dictate the value of M_1 new variables. Let Φ_1 denote the set of random literals forming Φ_1, and notice that Φ_1 is consistent if and only if Φ_1 is satisfiable. Similarly, the clauses corresponding to $\mathcal{C}_2$ form a random 2-SAT sub-instance Φ_2 of Φ. It then holds that

$$\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT} \iff M_0 = 0, \quad \Phi_1 \in \mathsf{SAT}, \quad \text{and} \quad (\Phi_2)_{\Phi_1} \in \mathsf{SAT}. \tag{D.2.2}$$

Hence, we need to calculate the probability of the event on the r.h.s. of (D.2.2), which is the point of departure for our proof.

We assume without loss of generality that $\mathcal{L} = [n] \setminus [n - |\mathcal{L}|]$, i.e. we rename the variables so that we fix the "last" $|\mathcal{L}|$ variables and are left with $1, 2, \ldots, n - |\mathcal{L}|$ (see [BOS25, Lemma 4]). Notice then that, in the conditional distribution given $\mathcal{C}$, Φ_h is a random h-SAT formula with $n - |\mathcal{L}|$ variables and M_h clauses, that is,

$$\Phi_h \mid \mathcal{C} \sim G_h(n - |\mathcal{L}|, M_h)$$

and Φ_1 and Φ_2 are independent (still given $\mathcal{C}$).

A calculation of the probability of (D.2.2) r.h.s. requires control of the size of the random variables M_h, $h \in K$. For this, recall the random variable A_v^+, the number of times v appears in Φ, and similarly A_v^-. Define

$$A_v := A_v^+ + A_v^-, \quad \text{and} \quad \hat{A}_v := \min\{A_v^+, A_v^-\} = \min\{A_v^+, A_v - A_v^+\},$$

the *total* number of times, respectively the *minimum* number of times, the variable v appears, negated or not. Define further

$$A_{\mathcal{L}} := \sum_{v \in \mathcal{L}} A_v, \quad \text{and} \quad \hat{A}_{\mathcal{L}} := \sum_{v \in \mathcal{L}} \hat{A}_v. \tag{D.2.3}$$

Since $A_{\mathcal{L}}$ is the total number of literals appearing in Φ which get fixed by $\mathcal{L}_{\mathrm{MR}}$, it is clear that the number of clauses in Φ which get affected by fixing these literals—that is, the number of clauses which fall *outside* of case 2)—is at most $A_{\mathcal{L}}$. Stated equivalently, the number of clauses that do fall into case 2) is at least $m - A_{\mathcal{L}}$, that is

$$M_2 \geq m - A_{\mathcal{L}}. \tag{D.2.4}$$

Similarly, $\hat{A}_{\mathcal{L}}$ is the total number of literals in Φ which get fixed to -1. A clause containing (at least) one such literal falls into case 0), 1), or $\star$). Indeed, if $\mathcal{C}_{(s,s')}$ denotes the set of $j \in [m]$ for which $L_{j,1}$ gets fixed to s and $L_{j,2}$ gets fixed to s', and $M_{(s,s')} = |\mathcal{C}_{(s,s')}|$ then

$$\hat{A}_{\mathcal{L}} = M_1 + M_{(-1,1)} + M_{(1,-1)} + 2M_0. \tag{D.2.5}$$

Letting $\mathcal{C}_\dagger$ denote the set of $j \in [m]$ for which both of $L_{j,1}$ and $L_{j,2}$ get fixed (to either 1 or -1), and $M_\dagger = |\mathcal{C}_\dagger|$, we have $\mathcal{C}_{(-1,1)} \cup \mathcal{C}_{(1,-1)} \cup \mathcal{C}_0 \subseteq \mathcal{C}_\dagger$, so

$$M_1 \geq \hat{A}_{\mathcal{L}} - 2M_\dagger. \tag{D.2.6}$$

Having now related the random variables M_h to the random variables $A_{\mathcal{L}}$ and $\hat{A}_{\mathcal{L}}$, we next calculate and give bounds on the mean and variance of them with the intention of obtaining concentration results for M_h.

Calculation of mean and variance

For the current section we generalize to all $k \in \mathbb{N}$. Remember that A_v is the number of times the variable v appears in Φ (negated or not), so $(A_v)_{v \in [n]}$ follows a multinomial distribution with parameters km and $(\frac{1}{n})_{v \in [n]}$, since in our model $G_k(n,m)$, the literals are all i.i.d. Furthermore, given $(A_v)_{v \in [n]} = (r_v)_{v \in [n]}$, the variables $A_1^+, \ldots, A_n^+$ are independent, and A_v^+ follows a binomial distribution with parameters r_v and $\frac{1}{2}$. Hence, for $a \geq 1$:

$$\mathbb{E}[\hat{A}_v \mid A_v = r] = \frac{1}{2^r} \sum_{s=0}^{r} \min\{s, r-s\} \binom{r}{s}.$$

We exploit the fact that both $\min\{s, r-s\}$ and $\binom{r}{s}$ are symmetric about $s \leftrightarrow r-s$, yielding

$$\sum_{s=0}^{r} \min\{s, r-s\}\binom{r}{s} = \begin{cases} 2r\sum_{s=0}^{r/2-2}\binom{r-1}{s} + r\binom{r-1}{r/2-1}, & \text{if } r \text{ is even,} \\ 2r\sum_{s=0}^{(r-3)/2}\binom{r-1}{s}, & \text{if } r \text{ is odd.} \end{cases}$$

On the other hand, we have by the binomial formula and again symmetry of $\binom{r-1}{s}$:

$$2^{r-1} = \sum_{s=0}^{r-1}\binom{r-1}{s} = \begin{cases} 2\sum_{s=0}^{r/2-1}\binom{r-1}{s}, & \text{if } r \text{ is even,} \\ 2\sum_{s=0}^{(r-3)/2}\binom{r-1}{s} + \binom{r-1}{(r-1)/2}, & \text{if } r \text{ is odd.} \end{cases}$$

Consequently, we get by combing the two identities above that

$$\mathbb{E}[\hat{A}_v \mid A_v = r] = r\left(\frac{1}{2} - \frac{1}{2^r}\binom{r-1}{\lfloor\frac{r-1}{2}\rfloor}\right).$$

Moreover, we have $\mathbb{E}[\hat{A}_v \mid A_v = 0] = 0$. Now, since, by the law of rare events/Poisson limit theorem, A_v is asymptotically Poisson-distributed with mean $k\alpha$, we find that

$$\mathbb{E}[\hat{A}_v] = \sum_{r=1}^{km}\mathbb{E}[\hat{A}_v \mid A_v = r]\mathbb{P}(A_v = r) \xrightarrow[n\to\infty]{} e^{-k\alpha}\sum_{r=1}^{\infty} r\left(\frac{1}{2} - \frac{1}{2^r}\binom{r-1}{\lfloor\frac{r-1}{2}\rfloor}\right)\frac{(k\alpha)^r}{r!}.$$

Calculating the sum on the r.h.s. above, we first of all see that

$$e^{-k\alpha}\sum_{r=1}^{\infty}\frac{r}{2}\cdot\frac{(k\alpha)^r}{r!} = \frac{k\alpha}{2},$$

from the known formula for the mean of a Poisson-distributed random variable. Secondly, we find that

$$\sum_{r=1}^{\infty}\frac{r}{2^r}\binom{r-1}{\lfloor\frac{r-1}{2}\rfloor}\frac{(k\alpha)^r}{r!} = \sum_{r=1}^{\infty}\frac{(k\alpha/2)^r}{\lfloor\frac{r-1}{2}\rfloor!(r-1-\lfloor\frac{r-1}{2}\rfloor)!} = \tfrac{1}{2}k\alpha(I_1(k\alpha) + I_0(k\alpha)),$$

where the final equality comes from splitting into even and odd terms and the well-known series representation

$$I_p(z) = \sum_{r=0}^{\infty}\frac{(z/2)^{2r+p}}{r!(r+p)!}$$

of the modified Bessel function of the first kind for all $p \in \mathbb{N}_0$. All in all,

$$\lim_{n\to\infty}\mathbb{E}[\hat{A}_v] = \tfrac{1}{2}k\alpha(1 - e^{-k\alpha}(I_0(k\alpha) + I_1(k\alpha))) = \tfrac{1}{2}k\alpha(1 - \mu_{k\alpha}),$$

where $\mu_{k\alpha}$ was defined in (D.1.1).

Finally, if $\mathcal{L} \subseteq [n]$ with $|\mathcal{L}| \sim \beta n^{1-1/k}$, then from (D.2.3) we have $\mathbb{E}[A_{\mathcal{L}}] = |\mathcal{L}| \cdot \mathbb{E}[A_1]$ and $\mathbb{E}[\hat{A}_{\mathcal{L}}] = |\mathcal{L}| \cdot \mathbb{E}[\hat{A}_1]$, giving

$$\mathbb{E}[A_{\mathcal{L}}] \sim k\alpha\beta n^{1-1/k}, \quad \text{and} \quad \mathbb{E}[\hat{A}_{\mathcal{L}}] \sim \tfrac{1}{2}k\alpha\beta(1-\mu_{k\alpha})n^{1-1/k}. \tag{D.2.7}$$

Next, we calculate variances. Since $A_{\mathcal{L}}$ is binomially distributed with parameters km and $|\mathcal{L}|/n$, we have

$$\mathrm{Var}(A_{\mathcal{L}}) = km\frac{|\mathcal{L}|}{n}\left(1 - \frac{|\mathcal{L}|}{n}\right) \sim k\alpha\beta n^{1-1/k}. \tag{D.2.8}$$

For $\hat{A}_{\mathcal{L}}$ we first note that $\hat{A}_v \le A_v$ and that there exists a constant $c > 0$ such that $\mathbb{P}(A_v = r) \le c^r/r!$ for all $r \in \mathbb{N}$, so

$$\mathbb{E}[\hat{A}_v^2] = \sum_{r=1}^{km} \mathbb{E}[\hat{A}_v^2 \mid A_v = r]\,\mathbb{P}(A_v = r) \le \sum_{r=1}^{\infty} r^2 \frac{c^r}{r!} = O(1). \tag{D.2.9}$$

For $v \neq w$ we have

$$\mathrm{Cov}(\hat{A}_v, \hat{A}_w) = \mathbb{E}[\mathrm{Cov}(\hat{A}_v, \hat{A}_w \mid A_v, A_w)] + \mathrm{Cov}(\mathbb{E}[\hat{A}_v \mid A_v], \mathbb{E}[\hat{A}_w \mid A_w]) < 0,$$

where the inequality follows from the fact that $\hat{A}_v$ and $\hat{A}_w$ are independent given (A_v, A_w), and $\mathbb{E}[\hat{A}_v \mid A_v = r]$ is an increasing function of r, so the covariance is negative, as A_v, A_w are entries of a multinomial distribution. This leads to

$$\mathrm{Var}(\hat{A}_{\mathcal{L}}) \le \sum_{v\in\mathcal{L}} \mathrm{Var}(\hat{A}_v) \le \sum_{v\in\mathcal{L}} \mathbb{E}[\hat{A}_v^2] = O(n^{1-1/k}),$$

where we in the end use (D.2.9). By (D.2.8) we also have $\mathrm{Var}(A_{\mathcal{L}}) = O(n^{1-1/k})$. Hence, for any $0 < q < 1$ we get by Chebyshev's inequality that

$$\mathbb{P}(|A_{\mathcal{L}} - \mathbb{E}[A_{\mathcal{L}}]| \ge n^q) \text{ and } \mathbb{P}(|\hat{A}_{\mathcal{L}} - \mathbb{E}[\hat{A}_{\mathcal{L}}]| \ge n^q) \text{ are both } O(n^{1-1/k-2q}). \tag{D.2.10}$$

Upper bound

We now proceed to upper bound $\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT})$. Let first of all

$$m_1 := \left\lfloor \mathbb{E}[\hat{A}_{\mathcal{L}}] - n^{1/3} \right\rfloor, \quad m_2 := \left\lfloor m - \log(n)\,\mathbb{E}[A_{\mathcal{L}}] \right\rfloor,$$
$$n' := n - |\mathcal{L}|, \quad \text{and} \quad \mathcal{L}_1 := [n'] \setminus [n' - (m_1 - \lfloor \log(n) \rfloor)].$$

Let next Ψ_1 denote the random 1-SAT problem with n' variables and m_1 clauses, and let Ψ_2 denote the random 2-SAT problem with n' variables and m_2 clauses. Let $\mathcal{L}'$ denote the set of clauses/literals defining Ψ_1, so that again Ψ_1 is satisfiable if and only if $\mathcal{L}'$ is consistent. Then, using (D.2.2) and following the reasoning in Section 4.4 of [BOS25, page 41–43], we find that

$$\begin{aligned}\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \mathbb{P}\Big(M_0 = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big) \\ \leq \mathbb{P}(M_0 = 0)\,\mathbb{P}(\Psi_1 \in \mathsf{SAT})\,\mathbb{P}((\Psi_2)_{\mathcal{L}_1} \in \mathsf{SAT}) \\ + \mathbb{P}(M_2 < m_2) + \mathbb{P}(M_1 < m_1) + \mathbb{P}(|\mathcal{L}'| < m_1 - \lfloor \log(n) \rfloor).\end{aligned}$$

The inequality is essentially due to the fact that the Φ_h's only depend on each other through M_h, and that satisfiability is a decreasing property in the number of clauses.

We have from (D.2.4) that $M_2 \geq m - A_{\mathcal{L}}$, so

$$\mathbb{P}(M_2 < m_2) \leq \mathbb{P}\Big(A_{\mathcal{L}} \geq \log(n)\,\mathbb{E}[A_{\mathcal{L}}]\Big) \leq \log(n)^{-1}$$

by Markov's inequality, implying that $M_2 \geq m_2$ w.h.p. Next, we have from (D.2.6) that $M_1 \geq \hat{A}_{\mathcal{L}} - 2M_{\dagger}$, so

$$\begin{aligned}\mathbb{P}(M_1 < m_1) &\leq \mathbb{P}\Big(\hat{A}_{\mathcal{L}} - 2M_{\dagger} \leq \mathbb{E}[\hat{A}_{\mathcal{L}}] - n^{1/3}\Big) \\ &\leq \mathbb{P}\Big(\hat{A}_{\mathcal{L}} \leq \mathbb{E}[\hat{A}_{\mathcal{L}}] - \tfrac{1}{2}n^{1/3}\Big) + \mathbb{P}\Big(M_{\dagger} > \tfrac{1}{4}n^{1/3}\Big).\end{aligned} \tag{D.2.11}$$

It follows from (D.2.10) that the first term above vanishes as $n \to \infty$. Notice further that $M_{\dagger}$ is binomially distributed with parameters $m \sim \alpha n$ and $(|\mathcal{L}|/n)^2 \sim \beta^2/n$, so that $\mathbb{E}[M_{\dagger}] \to \alpha\beta^2$ as $n \to \infty$, and thus by Markov's inequality, the second term above also vanishes. Hence, by eq. (D.2.11), $M_1 \geq m_1$ w.h.p. Finally, it follows immediately from [BOS25, Lemma 7] that $|\mathcal{L}'| \geq m_1 - \lfloor \log(n) \rfloor$ w.h.p., since $m_1/\sqrt{n'} \to \alpha\beta(1-\mu_{2\alpha}) < \infty$ by eq. (D.2.7).

We have now argued that

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) \leq \limsup_{n\to\infty}\Big(\mathbb{P}(M_0 = 0)\,\mathbb{P}(\Psi_1 \in \mathsf{SAT})\,\mathbb{P}((\Psi_2)_{\mathcal{L}_1} \in \mathsf{SAT})\Big). \tag{D.2.12}$$

It follows immediately from [BOS25, Lemma 8] and $m_1 \sim \alpha\beta(1-\mu_{2\alpha})\sqrt{n'}$ that

$$\lim_{n\to\infty} \mathbb{P}(\Psi_1 \in \mathsf{SAT}) = \exp\Big(-\tfrac{1}{4}\alpha^2\beta^2(1-\mu_{2\alpha})^2\Big). \tag{D.2.13}$$

Since $m_2 \sim m \sim \alpha n'$ (by (D.2.7)), it follows from (D.1.2) that

$$\lim_{n\to\infty} \mathbb{P}((\Psi_2)_{\mathcal{L}_1} \in \mathsf{SAT}) = \exp\Big(-\tfrac{1}{4}\alpha^3\beta^2(1-\mu_{2\alpha})^2(1-\alpha)^{-1}\Big). \tag{D.2.14}$$

Finally, for 0-clauses, we note again that $\hat{A}_{\mathcal{L}}$ is the number of literals in Φ that get fixed to -1. Hence, given $\hat{A}_{\mathcal{L}} = \eta$, $M_0 = 0$ if and only if these η literals are in distinct clauses. By the i.i.d. nature of the $2m$ literals, we have

$$\begin{aligned}\mathbb{P}(M_0 = 0 \mid \hat{A}_{\mathcal{L}} = \eta) = \frac{\binom{m}{\eta}2^{\eta}}{\binom{2m}{\eta}} = \frac{\prod_{d=0}^{\eta-1}(2m-2d)}{\prod_{d=0}^{\eta-1}(2m-d)} \le \prod_{d=0}^{\eta-1}\left(1-\frac{d}{2m}\right) \\ \le \exp\left(-\sum_{d=0}^{\eta-1}\frac{d}{2m}\right) = \exp\left(-\frac{(\eta-1)\eta}{4m}\right).\end{aligned} \tag{D.2.15}$$

We know from eq. (D.2.7) and eq. (D.2.10) that $\hat{A}_{\mathcal{L}} \sim \alpha\beta(1-\mu_{2\alpha})\sqrt{n}$ w.h.p., and it follows from this and (D.2.15) that

$$\limsup_{n\to\infty} \mathbb{P}(M_0 = 0) \le \exp\left(-\tfrac{1}{4}\alpha\beta^2(1-\mu_{2\alpha})^2\right). \tag{D.2.16}$$

Combining (D.2.12) with (D.2.13), (D.2.14), and (D.2.16), we get

$$\limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) \le \exp\left(-\left(\tfrac{\beta}{2}\right)^2 \tfrac{\alpha}{1-\alpha}(1-\mu_{2\alpha})^2\right) \tag{D.2.17}$$

as desired.

Lower bound

We now seek to establish a corresponding lower bound to (D.2.17). This time define

$$m_1 := \left\lfloor \mathbb{E}[\hat{A}_{\mathcal{L}}] + n^{1/3} \right\rfloor, \quad n' := n - |\mathcal{L}|, \quad \text{and} \quad \mathcal{L}_1 := [n'] \setminus [n'-m_1].$$

We again let Ψ_1 denote the random 1-SAT problem with n' variables and m_1 clauses and Ψ_2 denote the random 2-SAT problem with n' variables and m clauses. Then, using (D.2.2) and the reasoning leading to [BOS25, Equation (4.15)], we get

$$\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) \ge \mathbb{P}(M_0 = 0, M_1 \le m_1)\,\mathbb{P}(\Psi_1 \in \mathsf{SAT})\,\mathbb{P}((\Psi_2)_{\mathcal{L}_1} \in \mathsf{SAT}).$$

As before we have $m_1 \sim \alpha\beta(1-\mu_{2\alpha})\sqrt{n}$, so from analogous arguments we find that (D.2.13) and (D.2.14) still hold true with the current definitions.

Furthermore, we get from (D.2.5) that if $\hat{A}_{\mathcal{L}} \le m_1$, then certainly $M_1 \le m_1$, and the former occurs w.h.p. thanks to (D.2.10), so also $M_1 \le m_1$ w.h.p. Hence, it remains only to bound the probability that $M_0 = 0$. Similarly to (D.2.15), we get, using $1-s \ge \exp(s/(s-1))$ for $s < 1$ in the second inequality,

$$\begin{aligned}\mathbb{P}(M_0 = 0 \mid \hat{A}_{\mathcal{L}} = \eta) = \prod_{d=0}^{\eta-1}\left(1-\frac{d}{2m-d}\right) \ge \prod_{d=0}^{\eta-1}\left(1-\frac{d}{2m-\eta}\right) \\ \ge \exp\left(-\sum_{d=0}^{\eta-1}\frac{d}{2m-\eta-d}\right) \ge \exp\left(-\frac{(\eta-1)\eta}{4m-4\eta}\right).\end{aligned}$$

It again follows from (D.2.7) and (D.2.10) that

$$\liminf_{n\to\infty} \mathbb{P}(M_0 = 0) \geq \exp\Big(-\tfrac{1}{4}\alpha\beta^2(1-\mu_{2\alpha})^2\Big),$$

from which the desired lower bound follows. This completes the proof of Theorem D.1 for random 2-SAT.

D.2.2 Second part: random 3-SAT

Our procedure for random 3-SAT follows along the same lines as random 2-SAT with some modifications. Let $\Phi = C_1 \wedge \cdots \wedge C_m$ denote the random 3-SAT problem with n variables and $m \sim \alpha n$ clauses where $\alpha \in (0, 3.145)$, and let $\mathcal{L} \subseteq [n]$ be such that $|\mathcal{L}| \sim \beta n^{2/3}$ for some $\beta \in (0,\infty)$, and again we can assume without loss of generality that $\mathcal{L} = [n] \setminus [n-|\mathcal{L}|]$.

Here there are five possible outcomes for each clause $C_j = L_{j,1} \vee L_{j,2} \vee L_{j,3}$; case 0)-3); where all, two, a single, or none, respectively, of the literals $L_{j,1}, L_{j,2}, L_{j,3}$ get fixed to -1 with the rest remaining unaffected, and case ⋆); where at least one literals gets fixed to 1. Define $K := \{0,1,2,3,\star\}$, and define again $\mathcal{C}_h$ and M_h analogously to (D.2.1) for each $h \in K$. We have

$$\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT} \iff M_0 = 0, \quad \Phi_1 \in \mathsf{SAT}, \quad \text{and} \quad (\Phi_3 \wedge \Phi_2)_{\Phi_1} \in \mathsf{SAT}, \tag{D.2.18}$$

where $\Phi_h := \min\{C_j : j \in \mathcal{C}_h\}$ denotes the random h-SAT sub-instance of Φ, and Φ_1 denotes the set of literals forming Φ_1.

Upper bound

We immediately get from (D.2.18) that

$$\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}} \in \mathsf{SAT}) = \mathbb{P}\Big(M_0 = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_3 \wedge \Phi_2)_{\Phi_1} \in \mathsf{SAT}\Big) \leq \mathbb{P}(M_0 = 0). \tag{D.2.19}$$

Consider again the set $\mathcal{C}_\dagger$ of $j \in [m]$ for which all three literals in C_j get fixed, and let $M_\dagger = |\mathcal{C}_\dagger|$. Then $M_\dagger$ is binomially distributed with parameters $m \sim \alpha n$ and $|\mathcal{L}|^3/n^3 \sim \beta^3/n$, so

$$\lim_{n\to\infty} \mathbb{E}[M_\dagger] = \alpha\beta^3,$$

and it follows that $M_\dagger \leq \lfloor \log(n) \rfloor$ w.h.p. by Markov's inequality. Consider again also $A_{\mathcal{L}}$ and $\hat{A}_{\mathcal{L}}$, the total number of literals in Φ that get fixed, and the number of literals getting fixed to -1, respectively. The event $M_0 = 0$ occurs when and only when each clause represented in $\mathcal{C}_\dagger$ (i.e. those that get completely fixed) does not have all three literals fixed to -1. Because of the i.i.d. structure of the literals in Φ, this comes out to:

$$\mathbb{P}(M_0 = 0 \mid M_\dagger, A_{\mathcal{L}}, \hat{A}_{\mathcal{L}}) = \prod_{q=1}^{M_\dagger}\left(1 - \prod_{d=1}^{3} \frac{\hat{A}_{\mathcal{L}} - (3q-d)}{A_{\mathcal{L}} - (3q-d)}\right). \tag{D.2.20}$$

Now, taking mean over $M_\dagger$, using the fact that it is at most $\lfloor\log(n)\rfloor$ w.h.p., we get

$$\begin{aligned}\mathbb{P}(M_0 = 0 \mid A_{\mathcal{L}}, \hat{A}_{\mathcal{L}}) &\lesssim \sum_{s=0}^{\lfloor\log(n)\rfloor}\left(1-\left(\frac{\hat{A}_{\mathcal{L}}-3\lfloor\log(n)\rfloor}{A_{\mathcal{L}}}\right)^3\right)^s\binom{m}{s}\left(\frac{|\mathcal{L}|^3}{n^3}\right)^s\left(1-\frac{|\mathcal{L}|^3}{n^3}\right)^{m-s}\\ &\le\left(1-\frac{|\mathcal{L}|^3}{n^3}\right)^{m-\lfloor\log(n)\rfloor}\sum_{s=0}^{\lfloor\log(n)\rfloor}\left(\left(1-\left(\frac{\hat{A}_{\mathcal{L}}-3\lfloor\log(n)\rfloor}{A_{\mathcal{L}}}\right)^3\right)\frac{m|\mathcal{L}|^3}{n^3}\right)^s\frac{1}{s!},\end{aligned}$$

where we by $\lesssim$ mean that $\le$ holds in the limit (limsup or liminf, if the limit does not exist). It follows from (D.2.7) and (D.2.10) that $A_{\mathcal{L}} \sim 3\alpha\beta n^{2/3}$ and $\hat{A}_{\mathcal{L}} \sim \frac{3}{2}\alpha\beta(1-\mu_{3\alpha})n^{2/3}$ w.h.p. Using this, the above, and $m \sim \alpha n$, $|\mathcal{L}| \sim \beta n^{2/3}$, we conclude that

$$\limsup_{n\to\infty}\mathbb{P}(M_0=0)\le\exp(-\alpha\beta^3)\exp\Big((1-\tfrac{1}{8}(1-\mu_{3\alpha})^3)\alpha\beta^3\Big)=\exp\Big(-\Big(\tfrac{\beta}{2}\Big)^3\alpha(1-\mu_{3\alpha})^3\Big), \tag{D.2.21}$$

which, taken together with (D.2.19), yields the correct upper bound.

Lower bound

The final piece missing from a proof of Theorem D.1 (apart from the considerations in section D.2.3) is a corresponding lower bound to (D.2.21). We define

$$\begin{aligned}m_1 &:= \left\lfloor\log(n)n^{1/3}\right\rfloor, \quad m_2 := \left\lfloor\log(n)n^{2/3}\right\rfloor,\\ n' &:= n-|\mathcal{L}|, \quad \text{and} \quad \mathcal{L}_1 := [n']\setminus[n'-m_1],\end{aligned}$$

and we let Ψ_1 denote the random 1-SAT problem with n' variables and m_1 clauses, Ψ_2 denote the random 2-SAT problem with n' variables and m_2 clauses, and Ψ_3 denote the random 3-SAT problem with n' variables and m clauses, where Ψ_2 and Ψ_3 are independent. Now, following the same reasoning which leads up to [BOS25, Equation (4.41)] (and using initially (D.2.18)), we find that

$$\begin{aligned}&\mathbb{P}(\Phi_{\mathcal{L}_{\mathrm{MR}}}\in\mathsf{SAT})\\ &\ge\mathbb{P}\Big(M_0=0, M_1\le m_1, M_2\le m_2\Big)\mathbb{P}(\Psi_1\in\mathsf{SAT})\,\mathbb{P}\Big((\Psi_2\wedge\Psi_3)_{\mathcal{L}_1}\in\mathsf{SAT}\Big).\end{aligned} \tag{D.2.22}$$

It follows immediately from [BOS25, Lemma 8] and Theorem D.4 that both Ψ_1 and $(\Psi_2\wedge\Psi_3)_{\mathcal{L}_1}$ are satisfiable w.h.p. Hence, we consider the first factor on the r.h.s. of (D.2.22).

We again utilize that $\hat{A}_{\mathcal{L}}$ is the number of literals fixed to -1 in $\Phi_{\mathcal{L}_{\mathrm{MR}}}$. Thus, for any $j\in[m]$, we find that

$$\mathbb{P}(j\in\mathcal{C}_1\mid\hat{A}_{\mathcal{L}}=\eta)=\frac{3\eta(\eta-1)(3m-\eta)}{3m(3m-1)(3m-2)}\le\frac{\eta^2}{m(3m-1)}, \tag{D.2.23}$$

as long as $\eta \geq 2$. As before, we have that $\hat{A}_{\mathcal{L}} \sim \frac{3}{2}\alpha\beta(1-\mu_{3\alpha})n^{2/3}$ w.h.p., and it follows from this and (D.2.23) that $\mathbb{E}[M_1] = O(n^{1/3})$. By Markov's inequality, $M_1 \leq m_1$ w.h.p. A similar argument runs for the number of generated 2-clauses; for any $j \in [m]$ we have

$$\mathbb{P}(j \in \mathcal{C}_2 \mid \hat{A}_{\mathcal{L}} = \eta) = \frac{3\eta(3m-\eta)(3m-\eta-1)}{3m(3m-1)(3m-2)} \leq \frac{\eta}{m}.$$

Using then again the known size of $\hat{A}_{\mathcal{L}}$, we get $\mathbb{E}[M_2] = O(n^{2/3})$, and by Markov's inequality, $M_2 \leq m_2$ w.h.p. Hence, it remains only to lower bound the probability of the event $M_0 = 0$.

We again go from (D.2.20) and take mean over M_+, finding

$$\mathbb{P}(M_0 = 0 \mid A_{\mathcal{L}}, \hat{A}_{\mathcal{L}}) \gtrsim \sum_{s=0}^{\lfloor \log(n) \rfloor} \left(1 - \left(\frac{\hat{A}_{\mathcal{L}}}{A_{\mathcal{L}} - 3\lfloor \log(n) \rfloor}\right)^3\right)^s \binom{m}{s} \left(\frac{|\mathcal{L}|^3}{n^3}\right)^s \left(1 - \frac{|\mathcal{L}|^3}{n^3}\right)^{m-s}$$

$$\geq \left(1 - \frac{|\mathcal{L}|^3}{n^3}\right)^m \sum_{s=0}^{\lfloor \log(n) \rfloor} \left(\left(1 - \left(\frac{\hat{A}_{\mathcal{L}}}{A_{\mathcal{L}} - 3\lfloor \log(n) \rfloor}\right)^3\right) \frac{(m - \lfloor \log(n) \rfloor)|\mathcal{L}|^3}{n^3}\right)^s \frac{1}{s!}.$$

which, by the same reasoning as in the upper bound, yields us

$$\liminf_{n \to \infty} \mathbb{P}(M_0 = 0) \geq \exp\left(-\left(\tfrac{\beta}{2}\right)^3 \alpha(1-\mu_{3\alpha})^3\right),$$

as required.

D.2.3 Model conversion

We call the distribution for the random k-SAT problem with m clauses and n variables considered in this article $G_k(n,m)$. Lemma D.4 and Equation (D.1.2) are in [BOS25] proved in the model $F_k(n,m)$, where the signs and the clauses themselves are again sampled uniformly with replacement, but the variables in each clause are sampled uniformly *without* replacement. To convert these results from the model $F_k(n,m)$ to $G_k(n,m)$, we make use of the following observations.

Let Φ denote a random 2-SAT instance following the distribution $G_2(n,m)$, where $m \sim \alpha n$, $\alpha \in (0,1)$. That is, the literals $(L_{j,i})_{j\in[m],i\in[2]}$ defining Φ are i.i.d. Each clause $C_j = L_{j,1} \vee L_{j,2}$ can either be a genuine 2-clause, i.e. when $|L_{j,1}| \neq |L_{j,2}|$. On the other hand, if $L_{j,1} = L_{j,2}$, then C_j is really a 1-clause, or if $L_{j,1} = -L_{j,2}$, then C_j is constantly 1, i.e. a $\star$-clause/tautology. The $\star$-clauses do not affect the satisfiability of Φ. Let us denote by $\mathcal{D}_h$ the set of $j \in [m]$ for which C_j is a h-clause in the sense described above, and let $N_h = |\mathcal{D}_h|$, $h \in \{1,2,\star\}$. Then $(N_2, N_1, N_\star)$ follows a multinomial distribution with parameters m and $(1-\frac{1}{n}, \frac{1}{2n}, \frac{1}{2n})$. Define further

$$\Phi_h := \min_{j \in \mathcal{D}_h} C_j, \quad (h \in \{1,2\}).$$

Then, given $(N_2, N_1) = (m_2, m_1)$, Φ_2 and Φ_1 are independent and distributed according to $F_h(n, m_h)$ for $h = 1, 2$, respectively. We also have that $\mathbb{E}[N_1]$ and $\mathbb{E}[N_\star]$ both converge to $\frac{1}{2}\alpha$, so $N_1, N_\star \leq \log(n)$ w.h.p. by Markov's inequality. Thus also $N_2 \geq m - 2\log(n)$ w.h.p., meaning $N_2 \sim m \sim \alpha n$ w.h.p.

Consider $m_1 = m_1(n)$ and $m_2 = m_2(n)$ such that $m_1 \leq \log(n)$ and $m_2 \sim \alpha n$, and consider further Ψ_1 and Ψ_2 distributed according to $F_1(n, m_1)$ (which is the same as $G_1(n, m_1)$) and $F_2(n, m_2)$, respectively, such that Ψ_1 and Ψ_2 are independent. Let finally $\mathcal{L} \subseteq \pm[n]$ be consistent with $|\mathcal{L}| \sim \beta\sqrt{n}$ for some $\beta \in (0, \infty)$. If we can prove that

$$\lim_{n\to\infty} \mathbb{P}\Big((\Psi_1 \wedge \Psi_2)_{\mathcal{L}} \in \mathsf{SAT}\Big) = \exp\Big(-\Big(\tfrac{\beta}{2}\Big)^2 \tfrac{\alpha}{1-\alpha}\Big),$$

then by the paragraph above, we will have proved (D.1.2) for $k = 2$. Note for this purpose that Ψ_1 is satisfiable w.h.p. by [BOS25, Lemma 8]. Equivalently, $\mathcal{L}'$, the set of literals forming Ψ_1, is consistent w.h.p. Furthermore, $\mathcal{L} \cup \mathcal{L}'$ is consistent w.h.p., since the probability that a variable appears both in $\mathcal{L}$ and $\mathcal{L}'$ (negated or not) is seen to vanish by an application of the union bound. Thus, Ψ_1 simply acts by fixing m_1 further variables in Ψ_2. Since the size of $\mathcal{L}'$ is negligible compared to $|\mathcal{L}|$, i.e. $|\mathcal{L} \cup \mathcal{L}'| \sim \beta\sqrt{n}$, we get from Equation (D.1.2) the second equality in:

$$\lim_{n\to\infty} \mathbb{P}\Big((\Psi_1 \wedge \Psi_2)_{\mathcal{L}} \in \mathsf{SAT}\Big) = \lim_{n\to\infty} \mathbb{P}((\Psi_2)_{\mathcal{L}\cup\mathcal{L}'} \in \mathsf{SAT}) = \exp\Big(-\Big(\tfrac{\beta}{2}\Big)^2 \tfrac{\alpha}{1-\alpha}\Big),$$

as desired.

We employ completely analogous arguments in converting (D.1.2) for $k = 3$ and Lemma D.4 from the $F_k(n, m)$ to the $G_k(n, m)$ model.

References

[Ach00] Dimitris Achlioptas. "Setting 2 variables at a time yields a new lower bound for random 3-SAT (extended abstract)". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. STOC '00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 28–37.

[AS00] Dmitris Achioptas and Gregory B. Sorkin. "Optimal myopic algorithms for random 3-SAT". In: *Proceedings 41st Annual Symposium on Foundations of Computer Science*. FOCS '00. USA: IEEE Computer Society, 2000, pp. 590–600.

[BFU93] Andrei Z. Broder, Alan M. Frieze, and Eli Upfal. "On the satisfiability and maximum satisfiability of random 3-CNF formulas". In: *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '93. Austin, Texas, USA: Society for Industrial and Applied Mathematics, 1993, pp. 322–330.

[BOS25] Andreas Basse-O'Connor, Tobias Lindhardt Overgaard, and Mette Skjøtt. *On the random 2- and 3-SAT Problems*. Unpublished manuscript. 2025.

[CA96] James M. Crawford and Larry D. Auton. "Experimental results on the crossover point in random 3-SAT". In: *Artificial Intelligence* 81.1-2 (1996). Frontiers in problem solving: phase transitions and complexity, pp. 31–57.

[CF86] Ming-Te Chao and John Franco. "Probabilistic analysis of two heuristics for the 3-satisfiability problem". In: *SIAM J. Comput.* 15.4 (1986), pp. 1106–1118.

[CF90] Ming-Te Chao and John Franco. "Probabilistic analysis of a generalization of the unit-clause literal selection heuristics for the k-satisfiability problem". In: *Inform. Sci.* 51.3 (1990), pp. 289–314.

[Coa+03] Cristian Coarfa et al. "Random 3-SAT: The Plot Thickens". In: *Constraints* 8.3 (2003), pp. 243–261.

[Coo71] Stephen A. Cook. "The Complexity of Theorem-Proving Procedures". In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing*. STOC '71. 1971, pp. 151–158.

[CR92] Vašek Chvátal and Bruce Reed. "Mick gets some (the odds are on his side) (satisfiability)". In: *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*. SFCS '92. USA: IEEE Computer Society, 1992, pp. 620–627.

[DLL62] Martin Davis, George Logemann, and Donald Loveland. "A machine program for theorem-proving". In: *Comm. ACM* 5 (1962), pp. 394–397.

[DP60] Martin Davis and Hilary Putnam. "A Computing Procedure for Quantification Theory". In: *J. ACM* 7.3 (1960), pp. 201–215.

[FH88] John Franco and Yuan Chuan Ho. "Probabilistic performance of a heuristic for the satisfiability problem". In: *Discrete Appl. Math.* 22.1 (1988), pp. 35–51.

[FP83] John Franco and Marvin Paull. "Probabilistic analysis of the Davis-Putnam procedure for solving the satisfiability problem". In: *Discrete Appl. Math.* 5.1 (1983), pp. 77–87.

[FPR87] John Franco, J. M. Plotkin, and John W. Rosenthal. "Correction to: "Probabilistic analysis of the Davis-Putnam procedure for solving the satisfiability problem"". In: *Discrete Appl. Math.* 17.3 (1987), pp. 295–299.

[Fra84] John V. Franco. "Probabilistic analysis of the pure literal heuristic for the satisfiability problem". In: *Ann. Oper. Res.* 1 (1984), pp. 273–289.

[Fra86] John Franco. "On the probabilistic performance of algorithms for the satisfiability problem". In: *Information Processing Letters* 23.2 (1986), pp. 103–106.

[FS96] Alan Frieze and Stephen Suen. "Analysis of two simple heuristics on a random instance of k-SAT". In: *J. Algorithms* 20.2 (1996), pp. 312–355.

[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.

[Gol79] Allen T. Goldberg. "On the Complexity of the Satisfiability Problem". In: *Fourth Workshop on Automated Deduction.* CADE-4. Austin, Texas, USA: Association for Automated Reasoning Inc., 1979, pp. 1–6.

[HS03] Mohammad Taghi Hajiaghayi and Gregory B. Sorkin. *The Satisfiability Threshold of Random* 3*-SAT Is at Least* 3.52. 2003.

[KKL06] Alexis C. Kaporis, Lefteris M. Kirousis, and Efthimios G. Lalas. "The probabilistic analysis of a greedy satisfiability algorithm". In: *Random Structures Algorithms* 28.4 (2006), pp. 444–480.

[Knu15] Donald E Knuth. *The art of computer programming, Volume 4, Fascicle 6: Satisfiability.* Addison-Wesley Professional, 2015.

[Mar08] João Marques-Silva. "Practical applications of Boolean Satisfiability". In: *2008 9th International Workshop on Discrete Event Systems.* 2008, pp. 74–80.

[MZ02] Marc Mézard and Riccardo Zecchina. "Random K-satisfiability problem: From an analytic solution to an efficient algorithm". In: *Phys. Rev. E* 66 (5 2002), p. 056126.

[Pap94] Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994, pp. xvi+523.

[SML96] Bart Selman, David G. Mitchell, and Hector J. Levesque. "Generating Hard Satisfiability Problems". In: *Artif. Intell.* 81 (1996), pp. 17–29.

Project E

Regularity of Random 3-XORSAT

Andreas Basse-O'Connor[1], Tobias Overgaard[1], and Mette Skjøtt[1,2]

[1]Department of Mathematics, Aarhus University,
[2]Kvantify Aps

August 2025

E.1 Introduction

Given the interesting phenomena observed in random 3-SAT, it is natural to ask whether similar structural behavior appears in related models. One of the most studied and mathematically tractable alternatives is random 3-XORSAT. Like 3-SAT, the problem involves Boolean variables and random clauses of size three, but instead of disjunctions the constraints are XOR-clauses, i.e. linear equations over $\mathbb{F}_2$. This makes 3-XORSAT particularly appealing: it shares many structural similarities with 3-SAT, yet is more amenable to rigorous mathematical analysis. Random 3-XORSAT has been investigated extensively, and several fundamental results are known:

- **Sharp threshold:** It has been rigorously established that random 3-XORSAT exhibits a sharp satisfiability threshold (see [DM02]). In contrast, for 3-SAT the existence of the satisfiability threshold remain conjectural.
- **Threshold location:** The satisfiability threshold occurs at a critical clause-to-variable-density $\alpha \approx 0.918$ for 3-XORSAT. Below this density, a random instance is satisfiable w.h.p., while above it, it is unsatisfiable w.h.p.
- **Clustering phenomena:** Similar to 3-SAT, the solution space of 3-XORSAT undergoes structural changes. In particular, it has been proven that 3-XORSAT exhibits a clustering transition ([Ibr+15]), where the set of solutions shatters into exponentially many well-separated clusters. This mirrors the heuristic predictions for 3-SAT based on methods from statistical physics.
- **Algorithmic tractability:** Unlike 3-SAT, which is NP-complete, 3-XORSAT is solvable in polynomial time via Gaussian elimination. This allows for sharper probabilistic and structural analysis while retaining many features conjectured to drive hardness in 3-SAT.
- **2-XORSAT** For random 2-XORSAT, there is no sharp phase transition. The asymptotic probability decreases as the clause-to-variable ratio approaches 1/2 after which the problem is asymptotically unsatisfiable, see [HV11]. Thus, this is different from random 2-SAT that has a sharp phase transition.

Studying random 3-XORSAT alongside 3-SAT is therefore of particular interest because of the similarities of the problems. Thus, 3-XORSAT serves as a mathematical proxy for understanding phenomena such as clustering, condensation, and freezing in random 3-SAT, and it provides a test case for extending the analysis of variable-fixing and threshold functions presented in [BOS25]. If 3-XORSAT exhibits irregularities under partial assignments at the satisfiability threshold, this would lend strong support to the conjecture that the irregularity in 3-SAT also coincides with its satisfiability threshold.

E.2 Main result

A random k-XORSAT formula Φ with n variables and m clauses is generated from i.i.d. constraints $C_1,\dots,C_m$. For each $j \in [m]$, the clause C_j is defined by selecting k independent and uniformly distributed random variables $V_{j,1},\dots,V_{j,k} \in [n]$, together with a uniform random sign $S_j \in \mathbb{B} := \{\texttt{true}, \texttt{false}\}$. The resulting constraint corresponds to the linear equation

$$x_{V_{j,1}} \oplus \cdots \oplus x_{V_{j,k}} = S_j, \quad x \in \mathbb{B}^n,$$

where $\oplus$ denotes the exclusive-or operator. Next up, we fix a subset of the input variables of Φ. For this purpose, let $\mathcal{L} \subseteq \pm[n]$, and define $\Phi_{\mathcal{L}}$ in accordance with the notion of variable fixing introduced in Section B.3.2. In this project, we prove the following result.

Proposition E.1. *Let $\alpha, \beta > 0$, and let Φ be a random 3-XORSAT formula with $m \sim \alpha n$ clauses and n variables. Let $\mathcal{L} \subseteq \pm[n]$ be a consistent set of literals with $|\mathcal{L}| = f \sim \beta n^{2/3}$. Then it holds that*

$$\begin{aligned} e^{-\beta^3\alpha/2} &\geq \limsup_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \\ &\geq \liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \geq e^{-\beta^3\alpha/2} \liminf_{n\to\infty} \mathbb{P}(\Phi_2 \wedge \Phi_3 \in \mathsf{SAT}), \end{aligned}$$

where Φ_2 is a random 2-XORSAT formula with $\sim n$ variables, and $\sim 3(1+\epsilon)^3\alpha\beta n^{2/3}$ (for an arbitrary $\epsilon > 0$) 2-XOR-clauses, and Φ_3 is a random 3-XORSAT formula with $\sim n$ variables and m 3-XOR-clauses.

If the addition of $o(n)$ 2-XORSAT clauses to a subcritical 3-XORSAT formula does not affect overall satisfiability, then Proposition E.1 implies that random 3-XORSAT has $n^{2/3}$ degrees of freedom and an order parameter of the form $e^{-C\alpha}$ for some $C > 0$. This observation supports the idea that 3-SAT and 3-XORSAT exhibit analogous behavior under variable fixing.

We have the following conjecture, which states that adding $o(n)$ 2-XORSAT clauses does not spoil satisfiability:

Conjecture E.2. *Let Φ_2 and Φ_3 be random 2- and 3-XORSAT-formulas, respectively, with n variables, and $o(n)$ and $m \sim \alpha n$ clauses, respectively. If $\alpha < 0.918$, then $\Phi_2 \wedge \Phi_3$ is not asymptotically unsatisfiable.*

We will provide calculations that support Conjecture E.2. Taken together, Proposition E.1 and Conjecture E.2 imply that a random 3-XORSAT formula undergoes a shift in regularity at its satisfiability threshold. This, in turn, supports the conjecture that random 3-SAT exhibits the same behavior.

E.3 Proof

A proof of Proposition E.1 and initial calculations supporting Conjecture E.2 are included in this section.

E.3.1 Proof of Proposition E.1

Throughout this section, we use the same notation as in Article B, and therefore do not redefine it here. Prior to proving the Proposition, we provide some technical lemmas that correspond to lemmas already established in Article B. Hereafter, we first construct an upper bound followed by a lower bound on the probability of interest.

Technical lemmas

We have the following technical lemmas.

Lemma E.3. *Let Φ be a random (possibly mixed) XORSAT formula with m clauses and n variables, and let $\mathcal{L}, \mathcal{L}' \subseteq \pm[n]$ be two consistent sets of literals.*

1. *If $|\mathcal{L}| = |\mathcal{L}'|$, then $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) = \mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT})$.*
2. *If $|\mathcal{L}| \geq |\mathcal{L}'|$, then $\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \mathbb{P}(\Phi_{\mathcal{L}'} \in \mathsf{SAT})$.*

Proof. The proof is verbatim the same as that of Lemma B.8. □

Lemma E.4. *Let Φ and Φ' be random (possibly mixed) XORSAT formulas with m_k resp. m'_k k-clauses for each k, and n variables. Let $\mathcal{L} \subseteq \pm[n]$ be a consistent set of literals. If $m_k \geq m'_k$ for each k, then*

$$\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \leq \mathbb{P}(\Phi'_{\mathcal{L}} \in \mathsf{SAT}),$$

and in particular $\mathbb{P}(\Phi \in \mathsf{SAT}) \leq \mathbb{P}(\Phi' \in \mathsf{SAT})$.

Proof. The proof is verbatim the same as that of Lemma B.9. □

Lemma E.5. *Let $k = 2$ or $k = 3$, and let $K = \{0, 1, \ldots, k, \star\}$. For $m, n, f \in \mathbb{N}$ with $2 \leq f < n$, let Φ be a random k-XORSAT formula with m clauses and n variables, and let $\mathcal{L} = [n] \setminus [n-f]$. Let $\mathcal{C} := (\mathcal{C}_h)_{h \in K}$, $(M_h)_{h \in K}$ and $(\Phi_h)_{h \in K}$ be defined as usual, see B.3.6 and B.3.7.*

Then $(M_h)_{h \in K} \sim \mathrm{Multinomial}(m, (p_h)_{h \in K})$, and in the conditional distribution given $\mathcal{C}$, it holds that the Φ_h's are independent and that Φ_h is a random h-XORSAT *formula with M_h clauses and $n-f$ variables for all $h \in K$. Furthermore, if $k=3$, then*

$$p_0 = p_\star = \frac{f(f-1)(f-2)}{2n(n-1)(n-2)}, \quad p_1 = \frac{3f(f-1)(n-f)}{n(n-1)(n-2)},$$
$$p_2 = \frac{3f(n-f)(n-f-1)}{n(n-1)(n-2)}, \quad p_3 = \frac{(n-f)(n-f-1)(n-f-2)}{n(n-1)(n-2)}.$$

If instead $k=2$, then

$$p_0 = p_\star = \frac{f(f-1)}{2n(n-1)}, \quad p_1 = \frac{2f(n-f)}{n(n-1)}, \quad p_2 = \frac{(n-f)(n-f-1)}{n(n-1)}.$$

Proof. The proof is completely similar to the proof of Lemma B.10, and only depends on direct calculations. □

Note that we of course still have the important bi-implication (eq. (B.3.8)) for random 3-XORSAT formulas:

$$\Phi_{\mathcal{L}} \in \mathsf{SAT} \iff M_0 = 0, \quad \Phi_1 \in \mathsf{SAT} \quad \text{and} \quad (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}.$$

Lower bound

Assume without loss of generality that $\mathcal{L} = [n] \setminus [n-f]$. Let $\epsilon > 0$ be arbitrary. Define $(\Phi_h)_{h\in K}$, and $(\mathcal{C}_h)_{h\in K}$ in correspondence with B.3.6 and B.3.7, and let $M_h^{(1)} := |\mathcal{C}_h|$ for $h \in K$. For values of $f^{(r)}$ and $m^{(r)}$, which we may choose later, we put recursively

$$n^{(r)} := n^{(r-1)} - f^{(r-1)}, \quad \mathcal{L}^{(r)} := [n^{(r)}] \setminus [n^{(r+1)}],$$

so in particular $|\mathcal{L}^{(r)}| = f^{(r)}$. We will always choose $f^{(r)} = o(n)$, so $n^{(r)} \sim n$. We find that

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_{\mathcal{L}} \in \mathsf{SAT}\Big) \\
=&\mathbb{P}\Big(M_0 = 0, \Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}\Big) \\
\geq&\mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}, \Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT}\Big) \\
=&\mathbb{E}\Big[\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big)\mathbb{P}(\mathcal{C})\mathbb{1}_{\{M_0^{(1)}=0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\}}\Big],
\end{aligned}$$

where $\mathcal{C} = (\mathcal{C}_k^{(1)})_{k\in K}$. When in the following considering the conditional probability $\mathbb{P}(\cdot|\mathcal{C})$ we will assume that we are on the set $\{M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\}$. Note that under $\mathbb{P}(\cdot|\mathcal{C})$ the random XORSAT-formulas Φ_1, Φ_2, and Φ_3 are independent with Φ_k having $M_k^{(1)}$ clauses and $n^{(1)}$ variables for each $k \in [3]$. Now, let $\mathcal{B}$ denote the set of all satisfiable 1-XORSAT formulas with $M_1^{(1)}$ clauses and $n^{(1)}$ variables. We then see that

$$\begin{aligned}
&\mathbb{P}\Big(\Phi_1 \in \mathsf{SAT}, (\Phi_2 \wedge \Phi_3)_{\Phi_1} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi, (\Phi_2 \wedge \Phi_3)_{\varphi} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&= \sum_{\varphi \in \mathcal{B}} \mathbb{P}\Big(\Phi_1 = \varphi \,\Big|\, \mathcal{C}\Big)\mathbb{P}\Big((\Phi_2 \wedge \Phi_3)_{\varphi} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\geq \mathbb{P}\Big(\Phi_1 \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big)\mathbb{P}\Big((\Phi_2 \wedge \Phi_3)_{\mathcal{L}^{(1)}} \in \mathsf{SAT} \,\Big|\, \mathcal{C}\Big) \\
&\geq \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big),
\end{aligned}$$

where $\Phi_1^{(1)}$ is a random 1-XORSAT formula with $f^{(1)}$ clauses and $n^{(1)}$ variables, $\Phi_2^{(1)}$ is a random 2-XORSAT formula with $m^{(1)}$ clauses and $n^{(1)}$ variables, and $\Phi_3^{(1)}$ is a random 3-XORSAT formula with m clauses and $n^{(1)}$ variables, such that (the clauses of) $\Phi_2^{(1)}$ and $\Phi_3^{(1)}$ are independent. Thus, we have now used all our lemmas. Combining our calculations, we get:

$$\begin{aligned}
&\mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \\
&\geq \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}\Big)\times \\
&\quad \times \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \leq f^{(1)}, M_2^{(1)} \leq m^{(1)}\Big).
\end{aligned}$$

We now choose

$$f^{(1)} := \Big\lfloor 4\alpha\beta^2 n^{1/3} + n^{1/5} \Big\rfloor, \quad \text{and} \quad m^{(1)} := \Big\lfloor 3(1+\epsilon)\alpha\beta n^{2/3} + n^{2/5} \Big\rfloor.$$

We have that $M_0^{(1)}$ is asymptotically Poisson-distributed with mean $\beta^3\alpha/2$, and generally that $\mathbb{E}[M_k^{(1)}] = mp_k^{(1)}$, for $k \in K$ where $p_k^{(1)}$ comes from Lemma E.5. This shows that

$$\mathbb{E}[M_1^{(1)}] \sim 3\alpha\beta^2 n^{1/3} \quad \text{and} \quad \mathbb{E}[M_2^{(1)}] \sim 3\alpha\beta n^{2/3}.$$

Now,

$$\mathbb{P}\Big(M_1^{(1)} > f^{(1)}\Big) = \mathbb{P}\Big(M_1^{(1)} > 4\alpha\beta^2 n^{1/3} + n^{1/5}\Big) \leq \mathbb{P}\Big(M_1^{(1)} > \mathbb{E}[M_1^{(1)}] + n^{1/5}\Big),$$

where the inequality holds for large enough n, as eventually $\mathbb{E}[M_1^{(1)}] \leq 4\alpha\beta^2 n^{1/3}$. Using Chernoff's bound yields

$$\mathbb{P}\Big(M_1^{(1)} > \mathbb{E}[M_1^{(1)}] + n^{1/5}\Big) \leq \exp\left(\frac{-n^{2/5}}{3\,\mathbb{E}[M_1^{(1)}]}\right),$$

and the r.h.s. tends towards 0 as $n \to \infty$, as $\mathbb{E}[M_1^{(1)}]$ grows as $n^{1/3}$, which is slower than $n^{2/5}$. Hence, $M_1^{(1)} \le f^{(1)}$ w.h.p. A completely similar argument shows that $M_2^{(1)} \le m^{(1)}$ w.h.p. In conclusion,

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(1)} = 0, M_1^{(1)} \le f^{(1)}, M_2^{(1)} \le m^{(1)}\Big) = e^{-\beta^3\alpha/2}.$$

Now, since $f^{(1)}/\sqrt{n^{(1)}} \sim f^{(1)}/\sqrt{n} \to 0$, we also immediately get

$$\lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(1)} \in \mathsf{SAT}\Big) = 1,$$

where we use that a random 1-XORSAT formula behaves like a random 1-SAT formula. We are now left with the satisfiability of $(\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}}$. We again decompose. This time, we denote by $M_k^{(2)}(2)$ the number of (indices for the) k-clauses generated from $\Phi_2^{(1)}$, and similarly $M_k^{(2)}(3)$ for $\Phi_3^{(1)}$. Put $M_2^{(k)} := M_k^{(2)}(2) + M_k^{(2)}(3)$. By the same argument as before, we have

$$\begin{aligned}\mathbb{P}((\Phi_2^{(1)} \wedge \Phi_3^{(1)})_{\mathcal{L}^{(1)}} \in \mathsf{SAT}) \ge \mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big)\mathbb{P}\Big((\Phi_2^{(2)} \wedge \Phi_3^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}\Big)\\ \times \mathbb{P}\Big(M_0^{(2)} = 0, M_1^{(2)} \le f^{(2)}, M_2^{(2)} \le m^{(2)}\Big),\end{aligned}$$

where $\Phi_1^{(2)}$ is a random 1-XORSAT formula with $f^{(2)}$ clauses and $n^{(2)}$ variables, $\Phi_2^{(2)}$ is a random 2-XORSAT formula with $m^{(2)}$ clauses and $n^{(2)}$ variables, and $\Phi_3^{(2)}$ is a random 3-XORSAT formula with m clauses and $n^{(2)}$ variables, such that (the clauses of) $\Phi_2^{(2)}$ and $\Phi_3^{(2)}$ are independent. We choose

$$f^{(2)} := \Big\lfloor n^{1/5} \Big\rfloor, \quad \text{and} \quad m^{(2)} := \Big\lfloor 3(1+\epsilon)^2\alpha\beta n^{2/3} + n^{2/5} \Big\rfloor,$$

which immediately yields $f^{(2)}/\sqrt{n^{(2)}} \to 0$, so

$$\lim_{n\to\infty} \mathbb{P}\Big(\Phi_1^{(2)} \in \mathsf{SAT}\Big) = 1.$$

We now calculate

$$\mathbb{E}[M_0^{(2)}(2)] = m^{(1)} \frac{f^{(1)}(f^{(1)}-1)}{2n^{(1)}(n^{(1)}-1)} \sim 24(1+\epsilon)\alpha^3\beta^5 n^{-2/3} \longrightarrow 0,$$

and similarly

$$\mathbb{E}[M_0^{(2)}(3)] = m \frac{f^{(1)}(f^{(1)}-1)(f^{(1)}-2)}{2n^{(1)}(n^{(1)}-1)(n^{(1)}-2)} \sim 32\alpha^4\beta^6 n^{-1} \longrightarrow 0,$$

showing that $\mathbb{E}[M_0^{(2)}]$ vanishes, so by an application of Markov's inequality, $M_0^{(2)} = 0$ w.h.p. Considering now the unit clauses, we see that

$$\mathbb{E}[M_1^{(2)}(2)] = m^{(1)} \frac{3f^{(1)}(n^{(1)} - f^{(1)})}{n^{(1)}(n^{(1)} - 1)} \longrightarrow 36(1+\epsilon)\alpha^2\beta^3,$$

and similarly

$$\mathbb{E}[M_1^{(2)}(3)] = m \frac{3f^{(1)}(f^{(1)} - 1)(n^{(1)} - f^{(1)})}{n^{(1)}(n^{(1)} - 1)(n^{(1)} - 2)} \sim 48\alpha^3\beta^4 n^{-1/3} \longrightarrow 0,$$

so that $\mathbb{E}[M_1^{(2)}]$ converges to a constant, and again by an application of Markov's inequality, $M_1^{(2)} \leq f^{(2)}$ w.h.p. Finally, for binary clauses, we find that

$$\mathbb{E}[M_2^{(2)}(2)] = m^{(1)} \frac{(n^{(1)} - f^{(1)})(n^{(1)} - f^{(1)} - 1)}{n^{(1)}(n^{(1)} - 1)} \sim 3(1+\epsilon)\alpha\beta n^{2/3},$$

and

$$\mathbb{E}[M_2^{(2)}(3)] = m \frac{3f^{(1)}(n^{(1)} - f^{(1)})(n^{(1)} - f^{(1)} - 1)}{n^{(1)}(n^{(1)} - 1)(n^{(1)} - 2)} \sim 12\alpha^2\beta^2 n^{1/3},$$

so that $\mathbb{E}[M_2^{(2)}] \leq 3(1+\epsilon)^2\alpha\beta n^{2/3}$ for large enough n, and thus by Chernoff's inequality:

$$\mathbb{P}\Big(M_2^{(2)} > m^{(2)}\Big) \leq \mathbb{P}\Big(M_2^{(2)} > \mathbb{E}[M_2^{(2)}] + n_0^{2/5}\Big) \leq \exp\left(\frac{-n^{4/5}}{\mathbb{E}[M_2^{(2)}]}\right),$$

so $M_2^{(2)} \leq m^{(2)}$ w.h.p. Hence,

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(2)} = 0, M_1^{(2)} \leq f^{(2)}, M_2^{(2)} \leq m^{(2)}\Big) = 1,$$

and we are again left with the satisfiability of $(\Phi_2^{(2)} \wedge \Phi^{(2)})_{\mathcal{L}^{(2)}}$. This brings us to the final decomposition:

$$\mathbb{P}((\Phi_2^{(2)} \wedge \Phi_3^{(2)})_{\mathcal{L}^{(2)}} \in \mathsf{SAT}) \geq \mathbb{P}\Big(\Phi_2^{(3)} \wedge \Phi_3^{(3)} \in \mathsf{SAT}\Big)\mathbb{P}\Big(M_0^{(3)} = 0, M_1^{(3)} = 0, M_2^{(3)} \leq m^{(3)}\Big),$$

where $\Phi_2^{(3)}$ is a random 2-XORSAT formula with $m^{(3)}$ clauses and $n^{(3)}$ variables, and $\Phi_3^{(3)}$ is a random 3-XORSAT formula with m clauses and $n^{(3)}$ variables, such that (the clauses of) $\Phi_2^{(3)}$ and $\Phi_3^{(3)}$ are independent, and where we choose

$$f^{(3)} := 0, \quad \text{and} \quad m^{(3)} := \Big\lfloor 3(1+\epsilon)^3\alpha\beta n^{2/3} + n^{2/5} \Big\rfloor.$$

As before, we calculate

$$\mathbb{E}[M_0^{(3)}(2)] = m^{(2)}\frac{f^{(2)}(f^{(2)}-1)}{2n^{(2)}(n^{(2)}-1)} \sim \tfrac{3}{2}(1+\epsilon)^2\alpha\beta n^{-14/15} \longrightarrow 0,$$

and

$$\mathbb{E}[M_0^{(3)}(3)] = m\frac{f^{(2)}(f^{(2)}-1)(f^{(2)}-2)}{2n^{(2)}(n^{(2)}-1)(n^{(2)}-2)} \sim \tfrac{1}{2}\alpha n^{-7/5} \longrightarrow 0,$$

so $\mathbb{E}[M_0^{(3)}]$ vanishes, hence $M_0^{(3)} = 0$ w.h.p. by Markov's inequality. For unit clauses,

$$\mathbb{E}[M_1^{(3)}(2)] = m^{(2)}\frac{2f^{(2)}(n^{(2)}-f^{(2)})}{n^{(2)}(n^{(2)}-1)} \sim 6(1+\epsilon)^2\alpha\beta n^{-2/15} \longrightarrow 0,$$

and

$$\mathbb{E}[M_1^{(3)}(3)] = m\frac{3f^{(2)}(f^{(2)}-1)(n^{(2)}-f^{(2)})}{n^{(2)}(n^{(2)}-1)(n^{(2)}-2)} \sim 3\alpha n^{-3/5} \longrightarrow 0,$$

so for this round, $\mathbb{E}[M_1^{(3)}]$ vanishes, hence $M_1^{(3)} = 0$ w.h.p. by Markov's inequality. The argument that $M_2^{(3)} \le m^{(3)}$ is exactly the same as in the two previous rounds. Hence,

$$\lim_{n\to\infty} \mathbb{P}\Big(M_0^{(3)} = 0, M_1^{(3)} = 0, M_2^{(3)} \le m^{(3)}\Big) = 1,$$

which, tallying everything up, yields

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_{\mathcal{L}} \in \mathsf{SAT}) \ge e^{-\beta^3\alpha/2} \liminf_{n\to\infty} \mathbb{P}\Big(\Phi_2^{(3)} \wedge \Phi_3^{(3)} \in \mathsf{SAT}\Big).$$

E.3.2 Calculations for Conjecture E.2

We will need to establish that that probability that a random mixed 2- and 3-XORSAT formula is satisfiable is bounded away from zero, when the clause-to-variable ratio of 3-XOR-clauses is below ≈ 0.918, while the amount of 2-XOR-clauses is $o(n)$, n being the number of variables.

Our proof strategy is closely inspired by the proof in [DM02]. Their proof proceeds in two steps: first, they establish a satisfiability threshold for a related model; second, they reduce the standard random 3-XORSAT model to this auxiliary model, thereby proving the satisfiability threshold for random 3-XORSAT. In our case, we partially replicate the first step, showing that a related mixed 2- and 3-XORSAT model remains satisfiable with positive probability up to the phase transition point of the pure 3-XORSAT component.

Initial calculations

We consider a mixed 2- and 3-XORSAT formulae consisting of $m_2 := c_2 n$ equations of length two and $m_3 := c_3 n$ equations of length three, the equations being in n variables and each variable occurring at least twice.

Let $m := m_2 + m_3$, and define further $m_\star = 2m_2 + 3m_3$, and $c_\star = 2c_2 + 3c_3$. We let a formula be given by an ordered set of $m_\star$ places that are filled with variables, and each equation has to either equal `true` or `false`. We consider the uniform distribution over this set of formulas and denote such a random formula by Φ. As variables appear at least twice, this model is different from the standard random XORSAT-model, and the aim is to establish that such a formula is satisfiable with probability bounded away from zero (asymptotically), when c_2 is small and $c_3 < 1$.

Let N denote the number of solutions of the formula Φ. Note that deciding whether the formula Φ is satisfiable corresponds to deciding whether $N > 0$. We will use the second moment method, stating that $\mathbb{P}(N > 0) \leq \mathbb{E}[N]^2/\mathbb{E}[N]^2$, to establish that the probability that such a formula is satisfiable is bounded away from zero (asymptotically). Note that

$$\mathbb{E}[N] = \sum_{\sigma \in \mathbb{B}^n} \mathbb{P}\Big(\Phi(\sigma) = \texttt{true}\Big) = 2^n \frac{1}{2^m} = 2^{n - m_2 - m_3}. \tag{E.3.1}$$

We further need to estimate $\mathbb{E}[N^2]$. Let $\mathcal{F}$ denote the support of φ and $|\mathcal{F}|$ denote the size of the support. First, we will calculate $|\mathcal{F}|$. Let $S(m, n, 2)$ denote the number of partitions of m elements into n subsets each having at least 2 elements. These are the generalized Stirling numbers of the second kind, see e.g. [Hen94; Tem93]. Now

$$|\mathcal{F}| = 2^m S(m_\star, n, 2) n! \tag{E.3.2}$$

In order to calculate the second moment, we will sum over pairs (σ, τ) of satisfying assignments. Then

$$\mathbb{E}[N^2] = \frac{1}{|\mathcal{F}|} \sum_{\varphi \in \mathcal{F}} N^2(\varphi) = \frac{1}{|\mathcal{F}|} \sum_{\sigma, \tau} \sum_{\varphi \in \mathcal{F}} \mathbb{1}_{\{\varphi(\sigma) = \varphi(\tau) = \texttt{true}\}}.$$

Given φ, σ, and τ, we let α denote the proportion of variables having the same value in both assignments. We let r_2 denote the proportion of the m_2 2-clauses that contain at least one of these αn variables. Let r_3 denote the proportion of the last $3m_3$ places that contain one of the αn variables. Once we fill the entries of an equation, the right-hand side is uniquely determined, and so does not intervene in the enumeration. We must, however, ensure that the left-hand side evaluates to the same value in both variable assignments. This implies that the equations of length two either contain two variables that have the same value in both assignments or two variables that contain distinct values in the two assignments.

On the other hand, for the equations of length three, an equation must consist of either three variables with the same value in both assignments, or of two variables each with different values, and a third one with the same value. Letting $I_k = \{0, 1/k, 2/k, \ldots, (k-1)/k, 1\}$, we get that

$$\begin{aligned}|\mathcal{F}| \cdot \mathbb{E}[N^2] = \sum_{\alpha \in I_n} \sum_{r_2 \in I_{m_2}} \sum_{r_3 \in I_{3m_3} \cap [1/3,1]} 2^n \binom{n}{\alpha n} \binom{m_2}{(1-r_2)2m_2/2} \binom{m_3}{(1-r_3)3m_3/2} \times \\ \times 3^{(1-r_3)3m_3/2} S(2r_2m_2 + 3r_3m_3, \alpha n, 2)[\alpha n]! \times \\ \times S(2(1-r_2)m_2 + 3(1-r_3)m_3, (1-\alpha)n, 2)[(1-\alpha)n]!. \end{aligned} \tag{E.3.3}$$

In order to analyze all of the above expressions, we need to get a hold on the terms $S(m, n, 2)$. Thus, we use the below lemma (which is also included in [DM02], but with a typo):

Lemma E.6 ([Hen94] eq. (4.9)). *Let x_0 be the positive root of the saddle point equation*

$$\frac{n}{m} x_0 = \frac{e^{x_0} - 1 - x_0}{e^{x_0} - 1},$$

and define

$$t_0 = \frac{m - 2n}{n}, \quad f_2(t_0, x_0) = \sqrt{\frac{t_0}{x_0(t_0 + 1) - t_0(t_0 + 2)}}.$$

Then uniformly as m and n both tend to infinity $S(m, n, 2) \sim \theta(m, n)\psi(m, n)$, where the exponential part of the equivalent is

$$\psi(m, n) = (e^{x_0} - 1 - x_0)^n \left(\frac{m}{x_0 e}\right)^m \left(\frac{n}{e}\right)^{-n},$$

and the non-exponential part is

$$\theta(m, n) = \frac{1}{\sqrt{2\pi n}} \sqrt{\frac{m}{m - 2n}} f_2(t_0, x_0).$$

When finding asymptotic equivalents of functions in the following we will split it up, such that we find the exponential part and the non-exponential part separately. For functions f and g, we write $f \asymp g$ if they have the same exponential equivalent. Using Lemma E.6 on eq. (E.3.2), we get that

$$|\mathcal{F}| \asymp 2^{(c_2+c_3)n} \left(e^{x_0} - 1 - x_0\right)^n \left(\frac{(2c_2 + 3c_3)n}{x_0 e}\right)^{(2c_2+3c_3)n}, \tag{E.3.4}$$

where x_0 solves the equation

$$\frac{1}{2c_2+3c_3}x_0 = \frac{e^{x_0}-1-x_0}{e^{x_0}-1}. \tag{E.3.5}$$

The binomial coefficients can be approximated using Stirlings approximation, where for $c \in I_n$

$$\binom{n}{cn} \sim \left[\frac{1}{2\pi nc(1-c)}\right]\left[\frac{1}{c^{cn}(1-c)^{(1-c)n}}\right]. \tag{E.3.6}$$

Note that the first part is the exponential part, while the second is the non-exponential. Using eq. (E.3.6) and Lemma E.6 we find the exponential part of eq. (E.3.3)

$$\begin{aligned}|\mathcal{F}|\cdot\mathbb{E}[N^2] \asymp \sum_{\alpha\in I_n}\sum_{r_2\in I_{m_2}}\sum_{r_3\in I_{3m_3}\cap[1/3,1]} & 2^n\Big(\alpha^\alpha(1-\alpha)^{1-\alpha}\Big)^{-n}\Big((1-r_2)^{1-r_2}r_2^{r_2}\Big)^{-c_2 n}\\ &\times\bigg(\Big((1-r_3)3/2\Big)^{(1-r_3)3/2}\Big(1-(1-r_3)3/2\Big)^{1-(1-r_3)3/2}3^{(1-r_3)3/2}\bigg)^{-c_3 n}\\ &\times\Big(e^{x_2}-1-x_2\Big)^{\alpha n}\left(\frac{2r_2c_2n+3r_3c_3n}{x_2 e}\right)^{2r_2c_2n+3r_3c_3n}\\ &\times\left(e^{x_1}-1-x_1\right)^{(1-\alpha)n}\left(\frac{2(1-r_2)c_2n+3(1-r_3)c_3n}{x_1 e}\right)^{2(1-r_2)c_2n+3(1-r_3)c_3n},\end{aligned} \tag{E.3.7}$$

where we also use that the sum consists of a polynomial number of terms, while the terms of the sum are exponential, and thus each term can be substituted with its equivalent. Moreover, x_1 and x_2 are defined as being the positive roots of the equations

$$\frac{\alpha}{2r_2c_2+3r_3c_3}x_2 = \frac{e^{x_2}-1-x_2}{e^{x_2}-1}, \quad \frac{1-\alpha}{2(1-r_2)c_2+3(1-r_3)c_3}x_1 = \frac{e^{x_1}-1-x_1}{e^{x_1}-1}. \tag{E.3.8}$$

Using the rewritings in eqs. (E.3.4) and (E.3.7) we can write

$$\mathbb{E}[N^2] \asymp \sum_{\alpha\in I_n}\sum_{r_2\in I_{m_2}}\sum_{r_3\in I_{3m_3}\cap[1/3,1]} \exp\Big[nf(\alpha,r)\Big], \tag{E.3.9}$$

where

$$
\begin{aligned}
f(\alpha, r_2, r_3) =& (1-c_2-c_3)\ln 2 - \alpha\ln\alpha - (1-\alpha)\ln(1-\alpha) - c_2(1-r_2)\ln(1-r_2) \\
& - c_2 r_2 \ln r_2 - 3c_3(1-r_3)/2\ln((1-r_3)/2) \\
& - c_3\Big(1-3(1-r_3)/2\Big)\ln\Big(1-3(1-r_3)/2\Big) \\
& + \alpha\ln(e^{x_2}-1-x_2) + (2r_2c_2+3r_3c_3)\ln(2r_2c_2+3r_3c_3) \\
& - (2r_2c_2+3r_3c_3)\ln x_2 + (1-\alpha)\ln\Big(e^{x_1}-1-x_1\Big) \\
& + \Big(2(1-r_2)c_2+3(1-r_3)c_3\Big)\ln\Big(2(1-r_2)c_2+3(1-r_3)c_3\Big) \\
& - \Big(2(1-r_2)c_2+3(1-r_3)c_3\Big)\ln x_1 - n\ln\Big(e^{x_0}-1-x_0\Big) \\
& - (2c_2+3c_2)\ln(2c_2+3c_3) + (2c_2+3c_3)\ln x_0.
\end{aligned}
\tag{E.3.10}
$$

In the remainder of the proof we conjecture that when $c_3 < 1$, and c_2 is small, then within the domain $[0,1]\times[0,1]\times[1/3,1]$, the function of eq. (E.3.10) attains its global maximum at the point $f(1/2,1/2,1/2)$. Although we do not yet have a proof of this fact (and we do not expect the proof to be easy), we proceed under this assumption. This will allow us to apply a discrete version of the three-dimensional Laplace method. Again, a similar Lemma is included in [DM02], but with a typo.

Lemma E.7. *If f and g are smooth (C^2) real-valued functions of three variables, and if h has a single maximum on $[a,\infty)\times[b,\infty)\times[c,\infty)$, situated at $(x_\star, y_\star, z_\star)$, with $x_\star > a$, $y_\star > b$, and $z_\star > c$; and if further the determinant D of the Hessian of h at $(x_\star, y_\star, z_\star)$ is not zero, then*

$$
\begin{aligned}
&\sum_{i=an}^{n}\sum_{j=b\lambda n}^{\lambda n}\sum_{k=c\gamma n}^{\gamma n} g\Big(\frac{i}{n},\frac{j}{\lambda n},\frac{k}{\gamma n}\Big)\exp\Big(nf\Big(\frac{i}{n},\frac{j}{\lambda n},\frac{k}{\gamma n}\Big)\Big) \\
&\sim \frac{(2\pi n)^{3/2}\lambda\gamma}{\sqrt{|D|}} g(x_\star, y_\star, z_\star)\exp\Big(nh(x_\star, y_\star, z_\star)\Big).
\end{aligned}
$$

Proof. This follows directly by combining Laplace's method for approximating integrals with a Riemann sum approximation of the integral. □

Lemma E.7 implies that in order to find the asymptotic equivalent of $\mathbb{E}[N^2]$ (and given that f has its maximum at $(1/2,1/2,1/2)$) we only need to evaluate the exponential part of the equivalent, and the non-exponential part of the equivalent in $(1/2,1/2,1/2)$, and then further calculate the determinant of the exponential part of the equivalent.

Calculating determinant

The main difficulty in using Lemma E.7 is evaluating the determinant of the Hessian, as the function in (E.3.10) contains the implicitly given variables x_0, x_1, x_2.

We start by calculating the first-order derivatives

$$\begin{aligned}
&\frac{\partial f(\alpha, r_2, r_3)}{\partial \alpha} \\
&= \ln\left(\frac{1-\alpha}{\alpha}\right) + \ln\left(e^{x_2} - 1 - x_2\right) + \left[\alpha \cdot \frac{e^{x_2} - 1}{e^{x_2} - 1 - x_2} - \frac{2r_2c_2 + 3r_3c_3}{x_2}\right]\frac{\partial x_2}{\partial \alpha} \\
&\quad - \ln\left(e^{x_1} - 1 - x_1\right) + \left[(1-\alpha) \cdot \frac{e^{x_1} - 1}{e^{x_1} - 1 - x_1} - \frac{2(1-r_2)c_2 + 3(1-r_3)c_3}{x_1}\right]\frac{\partial x_1}{\partial \alpha} \\
&= \ln\left(\frac{1-\alpha}{\alpha}\right) + \ln\left(e^{x_2} - 1 - x_2\right) - \ln\left(e^{x_1} - 1 - x_1\right),
\end{aligned}$$

where the saddle point equations in (E.3.8) are used to cancel terms. Similar reductions are used in the following calculations:

$$\begin{aligned}
\frac{\partial f(\alpha, r_2, r_3)}{\partial r_2} =& c_2 \ln\left(\frac{1-r_2}{r_2}\right) + 2c_2 \ln(2r_2c_2 + 3r_3c_3) \\
&+ 2c_2 - 2c_2 \ln x_2 + \left[\alpha \frac{e^{x_2} - 1}{e^{x_2} - 1 - x_2} - \frac{2r_2c_2 + 3c_3r_3}{x_2}\right]\frac{\partial x_2}{\partial r_2} \\
&- 2c_2 \ln\left(2(1-r_2)c_2 + 3(1-r_3)c_3\right) - 2c_2 + 2c_2 \ln x_1 \\
&+ \left[(1-\alpha)\frac{e^{x_1} - 1}{e^{x_1} - 1 - x_1} - \frac{2(1-r_2)c_2 + 3(1-r_3)c_3}{x_1}\right]\frac{\partial x_1}{\partial r_2} \\
=& c_2 \ln\left(\frac{1-r_2}{r_2}\right) + 2c_2 \ln(2r_2c_2 + 3r_3c_3) - 2c_2 \ln x_2 \\
&- 2c_2 \ln\left(2(1-r_2)c_2 + 3(1-r_3)c_3\right) + 2c_2 \ln x_1,
\end{aligned}$$

and

$$\begin{aligned}
\frac{\partial f(\alpha, r_2, r_3)}{\partial r_3} =& \, 3c_3/2 \ln\left((1-r_3)/2\right) + 3c_3/2 - 3c_3/2 \ln\left(1 - 3(1-r_3)/2\right) - 3c_3/2 \\
&+ \alpha \frac{e^{x_2} - 1}{e^{x_2} - 1 - x_2} \cdot \frac{\partial x_2}{\partial r_3} + 3c_3 \ln(2r_2c_2 + 3r_3c_3) + 3c_3 - 3c_3 \ln x_2 \\
&- \frac{2r_2c_2 + 3r_3c_3}{x_2}\frac{\partial x_2}{\partial r_3} + (1-\alpha)\frac{e^{x_1} - 1}{e^{x_1} - 1 - x_1}\frac{\partial x_1}{\partial r_3} \\
&- 3c_3 \ln\left(2(1-r_2)c_2 + 3(1-r_3)c_3\right) \\
&- 3c_3 + 3c_3 \ln x_1 - \frac{2(1-r_2)c_2 + 3(1-r_3)c_3}{x_1}\frac{\partial x_1}{\partial r_3} \\
=& 3c_3/2 \ln\left(\frac{(1-r_3)/2}{1 - 3(1-r_3)/2}\right) + 3c_3 \ln(2r_2c_2 + 3r_3c_3) - 3c_3 \ln x_2 \\
&- 3c_3 \ln\left(2(1-r_2)c_2 + 3(1-r_3)c_3\right) + 3c_3 \ln x_1.
\end{aligned}$$

Next up, the second order derivatives are calculated

$$\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial\alpha^2} = \frac{1}{(\alpha-1)\alpha} + \frac{e^{x_2}-1}{e^{x_2}-1-x_2}\cdot\frac{\partial x_2}{\partial\alpha} - \frac{e^{x_1}-1}{e^{x_1}-1-x_1}\frac{\partial x_1}{\partial\alpha}.$$

$$\begin{aligned}\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial r_2^2} =& \frac{c_2}{(r_2-1)r_2} + \frac{(2c_2)^2}{2r_2c_2+3r_3c_3} - \frac{2c_2}{x_2}\frac{\partial x_2}{\partial r_2} \\ &+ \frac{(2c_2)^2}{2(1-r_2)c_2+3(1-r_3)c_3} + \frac{2c_2}{x_1}\frac{\partial x_1}{\partial r_2}.\end{aligned}$$

$$\begin{aligned}\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial r_3^2} =& \frac{3c_3}{3r_3^2-4r_3+1} + \frac{(3c_3)^2}{2r_2c_2+3r_3c_3} - \frac{3c_3}{x_2}\frac{\partial x_2}{\partial r_3} \\ &+ \frac{(3c_3)^2}{2(1-r_2)c_2+3(1-r_3)c_3} + \frac{3c_3}{x_1}\frac{\partial x_1}{\partial r_3}\end{aligned}$$

$$\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial\alpha\partial r_2} = \frac{e^{x_2}-1}{e^{x_2}-1-x_2}\frac{\partial x_2}{\partial r_2} - \frac{e^{x_1}-1}{e^{x_1}-1-x_1}\frac{\partial x_1}{\partial r_2}$$

$$\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial\alpha\partial r_3} = \frac{e^{x_2}-1}{e^{x_2}-1-x_2}\frac{\partial x_2}{\partial r_3} - \frac{e^{x_1}-1}{e^{x_1}-1-x_1}\frac{\partial x_1}{\partial r_3}$$

$$\begin{aligned}\frac{\partial^2 f(\alpha,r_2,r_3)}{\partial r_2\partial r_3} =& \frac{6c_2c_3}{2r_2c_2+3r_3c_3} - \frac{2c_2}{x_2}\frac{\partial x_2}{\partial r_3} \\ &+ \frac{6c_2c_3}{2(1-r_2)c_2+3(1-r_3)c_3} + \frac{2c_2}{x_1}\frac{\partial x_1}{\partial r_3}\end{aligned}$$

The second order derivatives are evaluated at the (conjectured) maximum $(1/2, 1/2, 1/2)$ at which $x_0 = x_1 = x_2$. As we in the following will only consider functions evaluated at this point, we will omit indicating this in the notation:

$$\begin{aligned}
\frac{\partial^2 f}{\partial \alpha^2} &= -2^2 + \frac{2c_2+3c_3}{x_0}\left(\frac{\partial x_2}{\partial \alpha} - \frac{\partial x_1}{\partial \alpha}\right),\\
\frac{\partial^2 f}{\partial r_2^2} &= -2^2 c_2 + \frac{2^4 c_2^2}{2c_2+3c_3} + \frac{2c_2}{x_0}\left(\frac{\partial x_1}{\partial r_2} - \frac{\partial x_2}{\partial r_2}\right),\\
\frac{\partial^2 f}{\partial r_3^2} &= -3\cdot 2^2 c_3 + \frac{2^2\cdot 3^2 c_3^2}{2c_2+3c_3} + \frac{3c_3}{x_0}\left(\frac{\partial x_1}{\partial r_3} - \frac{\partial x_2}{\partial r_3}\right),\\
\frac{\partial^2 f}{\partial \alpha \partial r_2} &= \frac{2c_2+3c_3}{x_0}\left(\frac{\partial x_2}{\partial r_2} - \frac{\partial x_1}{\partial r_2}\right),\\
\frac{\partial^2 f}{\partial \alpha \partial r_3} &= \frac{2c_2+3c_3}{x_0}\left(\frac{\partial x_2}{\partial r_3} - \frac{\partial x_1}{\partial r_3}\right),\\
\frac{\partial^2 f}{\partial r_2 \partial r_3} &= \frac{3\cdot 2^3 c_2 c_3}{2c_2+3c_3} + \frac{2c_2}{x_0}\left(\frac{\partial x_1}{\partial r_3} - \frac{\partial x_2}{\partial r_3}\right).
\end{aligned} \tag{E.3.11}$$

Next, we need to find explicit expressions of the above partial derivatives. Differentiating both sides of the saddle point equation in eq. (E.3.8), and evaluating in $(1/2, 1/2, 1/2)$, we get

$$\frac{2x_0}{c_\star} + \frac{1}{c_\star}\cdot\frac{\partial x_2}{\partial \alpha} = \left(1 - \frac{1}{c_\star}\cdot\frac{x_0 e^{x_0}}{e^{x_0}-1}\right)\cdot\frac{\partial x_2}{\partial \alpha} \quad\Rightarrow\quad \frac{\partial x_2}{\partial \alpha} = \frac{2x_0}{c_\star - 1 - \frac{x_0 e^{x_0}}{e^{x_0}-1}}.$$

The saddle point equation in eq. (E.3.5) implies.

$$\frac{x_0}{c_\star} = \frac{e^{x_0}-1-x_0}{e^{x_0}-1} = 1 - \frac{x_0}{e^{x_0}-1} \Rightarrow 1 = x_0\left(\frac{1}{c_\star} + \frac{1}{e^{x_0}-1}\right).$$

This implies that

$$\frac{1}{e^{x_0}-1} = \frac{1}{x_0} - \frac{1}{c_\star}, \qquad \text{and} \qquad e^{x_0} = \frac{1}{\frac{1}{x_0} - \frac{1}{c_\star}} + 1.$$

Using this, we can do the following rewriting

$$\frac{x_0 e^{x_0}}{e^{x_0}-1} = x_0\left(1 + \frac{1}{\frac{1}{x_0} - \frac{1}{c_\star}}\right)\left(\frac{1}{x_0} - \frac{1}{c_\star}\right) = x_0\left(\frac{1}{x_0} - \frac{1}{c_\star} + 1\right) = 1 - \frac{x_0}{c_\star} + x_0,$$

and this implies that

$$\frac{\partial x_2}{\partial \alpha} = \frac{2x_0}{c_\star - 1 - 1 + \frac{x_0}{c_\star} - x_0} = -\frac{2x_0 c_\star}{x_0(c_\star - 1) - (c_\star - 2)c_\star} = -2x_0\Gamma,$$

where we define

$$\Gamma := \frac{c_\star}{x_0(c_\star - 1) - (c_\star - 2)c_\star}.$$

Similar calculations give that

$$\frac{\partial x_2}{\partial r_2} = \frac{2c_2}{c_\star} 2x_0\Gamma, \qquad \frac{\partial x_2}{\partial r_3} = \frac{3c_3}{c_\star} \cdot 2x_0\Gamma, \qquad \frac{\partial x_1}{\partial \alpha} = 2x_0\Gamma,$$
$$\frac{\partial x_1}{\partial r_2} = -\frac{2c_2}{c_\star} 2x_0\Gamma, \qquad \frac{\partial x_1}{\partial r_3} = -\frac{3c_3}{c_\star} 2x_0\Gamma.$$

Inserting in eq. (E.3.11) implies

$$\begin{aligned}
\partial_{\alpha,\alpha} &:= \frac{\partial^2 f}{\partial \alpha^2} = -2^2\Big(1 + c_\star\Gamma\Big)\\
\partial_{r_2,r_2} &:= \frac{\partial^2 f}{\partial r_2^2} = -2^2\Big(c_2 - 2^2\frac{c_2^2}{c_\star} + 2^2\frac{c_2^2}{c_\star}\Gamma\Big)\\
\partial_{r_3,r_3} &:= \frac{\partial^2 f}{\partial r_3^2} = -2^2\Big(3c_3 - \frac{3^2c_3^2}{c_\star} + 3^2\frac{c_3^2}{c_\star}\Gamma\Big)\\
\partial_{\alpha,r_2} &:= \frac{\partial^2 f}{\partial \alpha \partial r_2} = 2^3c_2\Gamma\\
\partial_{\alpha,r_3} &:= \frac{\partial^2 f}{\partial \alpha \partial r_3} = 2^2 3c_3\Gamma\\
\partial_{r_2,r_3} &:= \frac{\partial^2 f}{\partial r_2 \partial r_3} = 2^2\Big(2\cdot 3\frac{c_2c_3}{c_\star} - 2\cdot 3\frac{c_2c_3}{c_\star}\Gamma\Big).
\end{aligned}$$

The determinant of the Hessian of f consists of the following terms, that we evaluate one by one:

$$D = \partial_{\alpha,\alpha}\partial_{r_2,r_2}\partial_{r_3,r_3} - \partial_{\alpha,\alpha}\partial^2_{r_2,r_3} - \partial^2_{\alpha,r_2}\partial_{r_3,r_3} - \partial^2_{\alpha,r_3}\partial_{r_2,r_2} + 2\partial_{\alpha,r_2}\partial_{r_2,r_3}\partial_{\alpha,r_3}$$

Letting $\Gamma_0 := \lim_{c_2\to 0}\Gamma$, we have that

$$\begin{aligned}
\partial_{\alpha,\alpha}\partial_{r_2,r_2}\partial_{r_3,r_3} &= 2^6 3c_2c_3 \cdot D_1, &&\text{with } D_1 \to -\Gamma_0 - 3c_3\Gamma_0^2, &&\text{as } c_2 \to 0,\\
-\partial_{\alpha,\alpha}\partial^2_{r_2,r_3} &= 2^6 3c_2c_3 \cdot D_2, &&\text{with } D_2 \to 0, &&\text{as } c_2 \to 0,\\
-\partial^2_{\alpha,r_2}\partial_{r_3,r_3} &= 2^6 3c_2c_3 \cdot D_3, &&\text{with } D_3 \to 0, &&\text{as } c_2 \to 0,\\
-\partial^2_{\alpha,r_3}\partial_{r_2,r_2} &= 2^6 3c_2c_3 \cdot D_4, &&\text{with } D_4 \to 3c_3\Gamma_0^2, &&\text{as } c_2 \to 0,\\
2\partial_{\alpha,r_2}\partial_{r_2,r_3}\partial_{\alpha,r_3} &= 2^6 3c_2c_3 \cdot D_5, &&\text{with } D_5 \to 0, &&\text{as } c_2 \to 0.
\end{aligned}$$

Let $D_. = D_1 + \cdots + D_5$. Using the above notation, we have that $D = 2^6 3c_2c_3D_.$, and further $D_. \to -\Gamma_0$ as $c_2 \to 0$. Remember, that c_2 describes the number of 2-XOR-clauses, and we already assume that this parameter is arbitrarily small, as we optimally only want to consider a formula with $o(n)$ 2-XOR-clauses.

Obtaining final expression

When using Lemma E.7 to find the asymptotic equivalent of $\mathbb{E}[N^2]/\mathbb{E}[N]^2$, we have that $h = f - 2(1 - c_2 - c_3)\ln 2$, see eqs. (E.3.1) and (E.3.10). Evaluated at $(1/2, 1/2, 1/2)$, where $x_0 = x_1 = x_2$, we get that $f(1/2, 1/2, 1/2) = 2(1-c_2-c_3)\ln 2$, and thus $h(1/2, 1/2, 1/2) = 0$. On the other hand, g consists of all the non-exponential parts of the functions that stem from the binomial coefficients and the Stirling numbers of the second kind $S(m, n, 2)$. Thus g can be calculated from eq. (E.3.6) and Lemma E.6. Hereby, direct calculations give

$$g(1/2, 1/2, 1/2) = \frac{1}{(n\pi)^{3/2}} \sqrt{\frac{2^5}{3} \frac{1}{c_2 c_3} \Gamma}.$$

Lastly, when using Lemma E.7, we have that $\lambda = c_2$, and $\gamma = 3c_3$. Now, we can finally evaluate the fraction of interest using Lemma E.7

$$\frac{\mathbb{E}[N^2]}{\mathbb{E}[N]^2} \sim \frac{(2\pi n)^{3/2} \cdot c_2 \cdot 3c_3}{|\sqrt{|2^6 3 c_2 c_3 D_.|}} \frac{1}{(n\pi)^{3/2}} \sqrt{\frac{2^5}{3} \frac{1}{c_2 c_3} \Gamma} = 2\sqrt{\frac{\Gamma}{|D_.|}}. \tag{E.3.12}$$

Remember, that when $c_2 \to 0$, then $\Gamma/|D_.| \to 1$. For an $\varepsilon > 0$ we let Φ_ε denote the random mixed XORSAT-model with n variables each appearing at least twice, and with $c_3 n$ 3-XOR-clauses, and εn 2-XOR-clauses. Moreover, let N_ε denote its number of solutions. Let $c_3 < 1$, and choose $\varepsilon > 0$ small enough, such that

$$\liminf_{n\to\infty} \mathbb{P}(\Phi_\varepsilon \in \mathsf{SAT}) = \liminf_{n\to\infty} \mathbb{P}(N_\varepsilon > 0) \geq \liminf_{n\to\infty} \frac{\mathbb{E}[N_\varepsilon]^2}{\mathbb{E}[N_\varepsilon^2]} \geq \frac{1}{2+\varepsilon},$$

where the last inequality comes from (E.3.12). Let now Φ instead consist of $c_3 n$ 3-XOR-clauses, and $o(n)$ 2-XOR-clauses in n variables, each variable again appearing at least twice. As the asymptotic satisfiability of Φ is upper bounded by the asymptotic satisfiability of Φ_ε for any $\varepsilon > 0$, we get that

$$\liminf_{n\to\infty} \mathbb{P}(\Phi \in \mathsf{SAT}) \geq \frac{1}{2},$$

which finishes our calculations.

Extending to standard model

In addition to establishing that the function f defined in eq. (E.3.10) attains its maximum at $(1/2, 1/2, 1/2)$, we must also extend the argument to XORSAT formulas without restrictions on the number of occurrences of each variable. For such a formula, the idea is to iteratively delete clauses containing variables that appear only once, since these clauses can always be satisfied by assigning the variable an appropriate Boolean value. Once this elimination process terminates, we obtain a random XORSAT formula in which every variable appears at least twice. For this reduced formula, we have already (partly) established that the satisfiability threshold occurs at a clause-to-variable ratio of one. The main task is therefore to carefully control the number of variables and clauses remaining after the elimination, since we ultimately need to decide whether asymptotically more clauses than variables remain.

This type of analysis has already been carried out for pure 3-XORSAT in [DM02], and we have no reason to believe that a similar argument cannot be extended to mixed 2- and 3-XORSAT formulas.

References

[BOS25] Andreas Basse-O'Connor, Tobias Lindhardt Overgaard, and Mette Skjøtt. "On the Regularity of Random 2-SAT and 3-SAT". In: *arXiv:2504.11979 [math.PR]* (2025).

[DM02] Olivier Dubois and Jacques Mandler. "The 3-XORSAT threshold". In: *Comptes Rendus Mathematique* 335.11 (2002), pp. 963–966.

[Hen94] François Hennecart. "Stirling distributions and Stirling numbers of the second kind. Computational problems in statistics". In: *Kybernetika* 30.3 (1994), pp. 279–288.

[HV11] Daudé Hervé and Ravelomanana Vlady. "Random 2 XORSAT phase transition". In: *Algorithmica* 59.1 (2011), pp. 48–65.

[Ibr+15] Morteza Ibrahimi et al. "The set of solutions of random XORSAT formulae". In: *The Annals of Applied Probability* 25.5 (2015).

[Tem93] Nico M Temme. "Asymptotic estimates of Stirling numbers". In: *Studies in Applied Mathematics* 89.3 (1993), pp. 233–243.