A Lower Bound for k-DNF Resolution on Random CNF Formulas via Expansion

Anastasia Sofronova
École Polytechnique Fédérale de Lausanne, Switzerland

Dmitry Sokolov
École Polytechnique Fédérale de Lausanne, Switzerland

Abstract

Random Δ-CNF formulas are one of the few candidates that are expected to be hard for proof systems and SAT algotirhms. Assume we sample m clauses over n variables. Here, the main complexity parameter is **clause density**, $\chi := \frac{m}{n}$. For a fixed Δ, there exists a *satisfiability threshold* c_Δ such that for $\chi > c_\Delta$ a formula is unsatisfiable with high probability. and for $\chi < c_\Delta$ it is satisfiable with high probability. Near satisfiability threshold, there are various lower bounds for algorithms and proof systems [12, 13, 5, 22, 34, 25, 20, 37], and for high-density regimes, there exist upper bounds [19, 29, 1, 23].

One of the frontiers in the direction of proving lower bounds on these formulas is the k-DNF Resolution proof system (aka Res(k)). There are several known results for $k = \mathcal{O}\left(\sqrt{\frac{\log n}{\log\log n}}\right)$ [35, 3], that are applicable only for density regime near the threshold. In this paper, we show the first Res(k) lower bound that is applicable in higher-density regimes. Our results work for slightly larger $k = \mathcal{O}\left(\sqrt{\log n}\right)$.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases proof complexity, random CNFs

Digital Object Identifier 10.4230/LIPIcs.CCC.2025.32

Related Version *Full Version*: https://eccc.weizmann.ac.il/report/2022/054/

Funding This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number MB22.00026.

Acknowledgements The authors would like to thank Edward Hirsch for comments on the draft, as well as the anonymous reviewers.

1 Introduction

Proof complexity studies whether there are efficient certificates for the unsatisfiability of boolean formulas. While satisfiability is easy to certify (one could consider a satisfying assignment if it exists), the question whether there exist polynomial-size proofs of unsatisfiability for every boolean formula remains a huge open problem in complexity theory. The non-existence of such proofs in any proof system would separate the classes **NP** and **coNP**. According to Cook's program, the idea is to prove lower bounds for stronger and stronger proof systems, so eventually we would be able to do it in a general case.

One of the difficulties with implementing this plan is the shortage of candidates for hard families of formulas. The intuition here is that any unsatisfiable example a person could invent is most likely accompanied with some natural reasons for its unsatisfiability (e.g. it is not hard to argue in natural language that Pigeonhole Principle or Tseitin formulas are unsatisfiable). One can formalize these reasons to try and produce an efficient proof in some proof system. The same intuition suggests to look at distributions of formulas for the hard candidates. As of now, there are three known distribution-based options:

- random Δ-CNFs;
- pseudorandom generators (aka proof complexity generators);
- clique formulas.

In this work, we focus on the first one. Random Δ-CNF formulas are an important and popular object in various areas of the complexity theory. These formulas are generated as a random subset of m clauses over n variables.

▶ **Definition 1.** *Let $\varphi(m, n, \Delta)$ denote the distribution of random Δ-CNF on n variables obtained by sampling m clauses of width Δ (out of the $\binom{n}{\Delta}2^{\Delta}$ possible clauses) uniformly at random with replacement.*

*We denote a **clause density** by $\chi \coloneqq \frac{m}{n}$.*

It is a well-known fact that such formulas are unsatisfiable with high probability (whp), if m is large enough.

▶ **Lemma 2** (Chvátal–Szemerédi, [15])**.** *For any $\Delta \geq 3$ whp $\varphi \sim \varphi(m, n, \Delta)$ is unsatisfiable if $m \geq \ln 2 \cdot 2^{\Delta} n$.*

In other words, for each Δ there is a density threshold c_{Δ} such that if $\chi > c_{\Delta}$ then whp the formula is unsatisfiable and if $\chi < c_{\Delta}$ then whp the formula is satisfiable.

The mystery of density. A common belief is that solving the satisfiability problem for random Δ-CNF formulas near the density threshold is hard. At the same time if we sample too many clauses, say $m \gg n^{\Delta-1}$, then whp our formula will contain *a local contradiction*, i.e. there will be a subformula on small number of variables that is unsatisfiable and even tree-like Resolution may efficiently certify it. Even for SAT solvers clause density helps to reduce the running time, in particular, the running time of ordered DLL procedure is upper bounded by $\exp\left(\mathcal{O}\left(\frac{n}{\chi^{1/(\Delta-2)}}\right)\right)$ [11]. And yet there is a certain gap between the satisfiability threshold and the density increase that is noticeable by the proof systems in the sense that it reduces the size of the proof. An exciting recent line of work [6, 32, 1, 23] provides strong refutation algorithms for random and semi-random CNFs for certain high-density regimes. Such algorithms found their applications in combinatorics and coding theory [7, 26]. Exploring different density regimes in various proof system thus seems crucial.

Feige's conjecture [18] states: no polynomial time algorithm may *prove* whp the unsatisfiability of a random $\mathcal{O}(1)$-CNF formula with arbitrary large constant clause density. This assumption of hardness on average implies the inapproximability of many NP-hard problems, such as vertex covering, DNF PAC learning, etc.

The sequence of papers that starts with the classical lower bounds by Chvátal and Szemerédi [15] shows the hardness of random Δ-CNF formulas in Resolution for various regimes of density. In [15] the authors show that for any fixed $\chi \geq 2^{\Delta} \ln 2$ there is a constant $\kappa(\chi)$ such that random k-SAT requires length $\exp(\kappa(\chi)n)$ with high probabilty. But κ decays doubly-exponentially as χ increases and lower bound becomes trivial when $m \gg n \log^{1/4} n$. Later lower bounds by Ben-Sasson–Wigderson [14] and by Beame et al [11] reduced the decay in κ to polynomial in χ. Later Ben-Sasson [12] improved the polynomial in the dependency on χ. Similar type of dependencies on the density is known also for several other proof systems: Polynomial Calculus [13, 5], Sum-of-Squares [22]. Res(k) proof system is a notable exception, and we have lower bounds only for density near the satisfiability threshold.

From the proof complexity point of view, random Δ-CNFs are one of the most promising candidates to be hard for any proof system. We know many lower bounds for random formulas even in powerful proof systems like Sum-of-Squares. Such lower bounds are out of reach for other candidates like PRG formulas [4, 33] or Clique formulas [8, 31, 17]. We mention known results for random formulas in Section 1.1.

1.1 Prior Results

The following table summarizes known facts about the complexity of random Δ-CNFs in different proof systems.

Proof system	**Polynomial upper bound**	**Lower bound 2^{n^ε}**
Resolution	$m > \frac{n^{\Delta-1}}{\log^{\Delta-2} n}$ [11]	$m < n^{\frac{\Delta}{2}-o(1)}$ [12]
Polynomial Calculus		$m = \mathcal{O}(n), \Delta \geq 3$ [13] $m = \mathsf{poly}(n), \Delta = 3$ [5]
Sum-of-Squares	$\Delta = k, m = \widetilde{\mathcal{O}}(n^{\frac{k}{2}})$, [6, 32, 1, 23]	$m = \mathsf{poly}(n), \Delta = \mathcal{O}(1)$ [22], [34], [27]
Cutting Planes		$m = \mathsf{poly}(n), \Delta = \Omega(\log n)$ [25], [20], [37]
$\mathbf{TC}_0$-Frege	$\Delta = 3$, $m > n^{1.4}$ [19], [29]	$\times$
Res(k)		$m = \mathcal{O}(n), \Delta \geq 3, k = 2$ [9] $m = \mathcal{O}(n), \Delta \geq 3, k = \mathcal{O}\left(\sqrt{\frac{\log n}{\log\log n}}\right)$ [3] $m = n^{7/6}, \Delta = \mathcal{O}\left(k^2\right), k = \mathcal{O}(1)$ [35]

To clarify the comparison of these results, let us note here than Resolution is a strictly weaker system than all the others present in the table. $\mathbf{TC}_0$ models every other system present in the table, expect Sum-of-Squares, for which their relationship is not known. Everything else is not comparable (depending on the specific field for algebraic systems).

The big long-standing open problem in proof complexity is to show $\mathbf{AC}_0$-Frege lower bounds for random Δ-CNF formulas. Even for non-constant Δ and depth-2 Frege this problem seems to be out of reach for current techniques. The current frontier in this direction is Res(k) proof system that was introduced by Krajíček [28]. This is a subsystem of depth-2 Frege that uses k-DNF formulas as proof lines (see Section 2) rather than general DNF formulas that are used by depth-2 Frege. In fact, it would be enough to have a *robust* (i.e. stable under restrictions of formulas) lower bound for $k = \log^{1+\varepsilon} n$ to extend it to all k's and, therefore, to depth-2 Frege using random restriction, so the gap between current state-of-the-art and this threshold might very well be breachable. Here by robust we mean a technique that is not tailored precisely to a specific unsatisfiable family, but that allows a certain degree of freedom in choosing a hard formula.

Known techniques. All known techniques for proving lower bounds on the proof systems that are at least as powerful as Res(2) are based on the restriction argument. In other words we choose a random partial assignment to the variables from a carefully chosen distribution, hit the formula and the proof by this assignment in order to get an extremely structured proof and leave the restricted formula hard for such proofs. In particular, $\mathbf{AC}_0$-Frege *transforms* into a resolution proof under large partial assignments (we should assign $n - o(n)$ number of variables); this method is also known as switching lemma [2, 10, 24]. We do not know how to make such an assignment and keep random Δ-CNF formula hard for resolution. All known hardness results for refuting random formulas in Res(k) are trying to avoid this problem in different ways and require different properties of random formulas. The key tool is the Small Restriction Switching Lemma, which assigns εn number of variables and reduces a Res(k) proof to a Resolution proof.

- In [35] the authors use the fact that for $\Delta \gtrsim k^2$ it is possible to use the uniform distribution on a certain set of partial restrictions and keep the restricted formula hard for Resolution. This result holds in case of clause density at most $\chi = n^{1/6}$ and k an absolute constant.

This lower bound is not *uniform* in terms of choice of the proof system. In other words, if we want to state that "there is a distribution on formulas that is hard for Res(k) proof systems for all constant k", we would need to purge the dependence between Δ and k.

- Alekhnovich in [3] shows the solution for this problem. The distribution over partial assignments makes use of the structure of the dependency graph of the formula, but for the analysis it was required that this graph has low right degree of all vertices (in other words, any variable should appear in constant number of clauses). This requirement may be achieved only in case of constant clause density of a random formula. k in this setup is allowed to be at most $\mathcal{O}\left(\sqrt{\frac{\log n}{\log\log n}}\right)$.

Both papers in addition require the dependency graph be an expander, which is a standard property for the analysis of hardness (that is almost "necessary", since we have to argue that there are no local unsatisfiable subformulas).

Another relevant work is Razborov's improved small-set switching lemma [33]. Though it builds on an improved technique from [35], the formulas considered (pseudorandom generators) are quite different, so it is not clear if this result is directly comparable with ours.

1.2 Our Results

We suggest a new technique that helps us to extend and unify both mentioned lower bounds. Our results use only the fact that the dependency graph of a formula is a good enough expander. More formally, we show the following in Section 5.

▶ **Theorem 3.** *Let φ be a Δ-CNF formula such that its dependency graph G is an $(r, \Delta, 0.95\Delta)$-boundary expander. Then for any $\delta > 0$ if:*

$$n^{\delta}\left(\frac{n}{0.4r}\right)^{20k^2} = o(r/k)$$

then any Res(k) *proof of φ has size at least $2^{n^{\delta}}$.*

In Section 6 we show the following corollaries:

- an exponential lower bound for any constant k, $\Delta = \mathcal{O}(1)$ in case $m = \mathsf{poly}(n)$ (improvement of the result of Segerlind, Buss, Impagliazzo [35]);
- an exponential lower bound for $k = \mathcal{O}\left(\sqrt{\log n}\right)$, $\Delta = \mathcal{O}(1)$ in case $m = \mathcal{O}(n)$ (improvement of the result of Alekhnovich [3]).

We would like to emphasize that this result is the first that provides a lower bound on the Res(k) proofs for the constant Δ independent on k and polynomially large clause density $m = \mathsf{poly}(n)$.

As a weakness of our results, we should mention the fact that the constant Δ should be big enough for the dependency graph of the formula to be an expander with good parameters. Naive computations say that $\Delta \approx 100$ is enough (see Section C). We did not try to optimize this constant, since we do not see the way to achieve the best possible value 3 (like in [3]).

We describe our technique below.

Our technique. We follow the ideas of random restriction technique [35, 3].

1. Given a Δ-CNF formula φ on n variables and m clauses, we assume that a dependency graph (clauses–variables) is a good enough expander (this holds with probability $1 - o(1)$ for random formulas).

2. For the sake of contradiction assume that there is a small Res(k)-proof π of φ. We would like to create a partial assignment ρ such that:
   - $\varphi|_\rho$ is hard for Resolution (i.e. dependency graph of the restricted formula is still an expander graph);
   - $\pi|_\rho$ transforms into a small Resolution proof.

In this general plan we replace Resolution proof system by a proof system based on the DNF-trees (see Section 5.2) and we prove that expansion properties of $\varphi|_\rho$ also imply a lower bound on the proof system based on these trees (see Section 5.3). We believe that this is a more natural object to consider when proving lower bounds of random CNF formulas.

The most challenging part in this strategy is the choice of ρ and proof of its required properties. In [3, 35] the authors proposed to choose ρ randomly and to prove the following dichotomy to show the required properties of ρ. Here, a *hitting set* for a collection $\{S_1, \ldots, S_l\}$, $S_i \subseteq \mathcal{U}$ is a set $S \subseteq \mathcal{U}$ that intersects each S_i:

- either the terms of k-DNF have a big minimal hitting set (aka covering number), and this line of the proof can be easily killed (satisfied) by a random restriction; so this k-DNF can be simplified to a trivial decision tree;
- or this hitting set is small, and in this case the line can be transformed into a decision tree plus a collection of $(k-1)$-DNFs.

Note that since our goal is to transform k-DNFs into some decision trees, we have to assign at least εn variables (the so-called Tribes function with certain parameters is a canonical example of a function that can be represented as k-DNF and is resistent to simplification under small restrictions [30]). If Δ is a fixed constant and we choose ρ of proper size uniformly at random whp we violate at least one clause. Hence ρ should respect constraints of φ.

Alekhnovich in [3] proposed the solution for the considered problem. With an assignment ρ he associates a subformula of φ and chooses an assignment uniformly at random among assignments that satisfy this subformula (so-called **closure** in terms of bipartite dependency graph on clauses and variables, see Sections 3, 4). Note that in [35] these issues did not arise, since the degree of the dependency graph was large enough.

Unfortunately, we cannot deal with the closure proposed in [3] since the analysis in that paper is based on the fact that clause density is a universal constant. Instead, we use **individual closure** that satisfies some additional properties in comparison to closure used in [3]. We pick ρ from a distribution that satisfies a subformula of φ based on individual closure.

The main technical advantage of individual closure is that it is robust enough to allow us to perform induction on its size even after restricting to certain subgraphs of the expander. In other words, while in [3] the parameter that gets reduced after applying the assignment is the width of the DNFs used in the proof, we instead reduce the sizes of individual closures of the terms of such DNFs. This is, arguably, a more natural measure when it comes to expander graphs, so this allows us more slack in the density of the formula. The properties of individual closure may be, therefore, of independent interest. While we are not aware whether this exact definition has already been introduced elsewhere among the huge variety of different expander closures, to the best of our knowledge, the use of its specific properties is new.

We also have to change the dichotomy, since the covering number does not help us to analyse probabilities in case of large clause density of formula. Here we introduce **closure covering number** that is based on generalization of hitting set notion. The new dichotomy is the following:

- either "individual closures" of terms of k-DNF have a big minimal hitting set, and this line can be easily killed by a random restriction;
- or this hitting set is small, and in this case the line can be transformed into a decision tree plus a collection of k-DNFs, but with smaller individual closures.

By using induction on sizes of individual closures we step by step show that $\pi|_\rho$ can be represented as a sequence of DNF-trees. We do not extract a Resolution proof from this argument, dealing with the directed acyclic graph (dag) of Res(k) proof instead (though we believe that our argument can be rephrased in terms of Resolution proofs). By working directly with Res(k) proofs, we shed some light on the internal mechanism of how they behave under random restrictions. We believe this to be a step to future generalizations and to finding a method to argue about hardness in Res(k) without appealing to Resolution.

1.3 The Outline

In Section 3 we give definitions for expander graphs and a notion of the individual closure, and show the required properties of it. In Section 4 we consider random CNF formulas and random linear systems. We give the criteria that some partial assignments are "independent" which is the key technical tool for the proof of the main result. In Section 5 we focus on the proof of the main Theorem, and we also prove a "Restriction Lemma" that is a translation of our notion of independency into the language of probabilities. In Section 6 we show several applications of the main Theorem for random CNF formulas.

2 Preliminaries

Let x be a propositional variable, i.e., a variable that ranges over the set $\{0,1\}$. A literal of x is either x (denoted sometimes as x^1) or $\neg x$ (denoted sometimes as x^0). A **clause** $C := x_1^{c_1} \vee x_2^{c_2} \cdots \vee x_k^{c_k}$ is a disjunction of literals where $c_1, c_2, \ldots, c_k \in \{0,1\}$. A **CNF formula** $\varphi := C_1 \wedge \cdots \wedge C_m$ is a conjunction of clauses. A **term** is a conjunction of literals. A **DNF formula** $\varphi := t_1 \vee \cdots \vee t_m$ is a disjunction of terms.

Let X be a set of propositional variables. A **partial assignment** or a **restriction** is a mapping $\rho\colon X \to \{0,1,*\}$. We let $\mathrm{supp}(\rho) := \rho^{-1}(\{0,1\})$ denote the set of assigned variables. The restriction of a function f (or a formula φ) by ρ, denoted $f|_\rho$ (respectively, $\varphi|_\rho$), is the Boolean function (propositional formula) obtained from f (respectively, from φ) by setting the value of each $x_i \in \mathrm{supp}(\rho)$ to $\rho(x_i)$ and leaving each $x_i \notin \mathrm{supp}(\rho)$ unassigned.

We say that two partial assignments ρ, ρ' are **consistent** iff for any $x \in \mathrm{supp}(\rho) \cap \mathrm{supp}(\rho')$ the following holds $\rho(x) = \rho'(x)$. In addition, if $\mathrm{supp}(\rho') \subseteq \mathrm{supp}(\rho)$ then we use the notation $\rho' \subseteq \rho$. We refer to ρ as a partial assignment on a set of variables J if $\mathrm{supp}(\rho) = J$.

***k*-DNF Resolution.** In this paper we focus on classical generalization of the Resolution proof system, so-called k-DNF Resolution aka Res(k) [28].

A proof system Res(k) operates with DNFs of width k (or k-DNFs). Here a width of the term is the number of literals in the term, and the width of a DNF is the maximal width of its terms. A Res(k)**-proof** π of an unsatisfiable CNF formula φ is a sequence of k-DNFs $\pi := C_1, \ldots, C_s$ such that $C_s = \emptyset$ is an empty formula. Each C_i either comes from the original formula φ or is inferred from the previous ones using one of the rules (here l and l_i are literals):

Weakening: $\frac{F}{F \vee \ell}$;
And-introduction: $\frac{F \vee \ell_1, \ldots, F \vee \ell_w}{F \vee (\bigwedge_{i=0}^{w} \ell_i)}$;
And-elimination: $\frac{F \vee (\bigwedge_{i=0}^{w} \ell_i)}{F \vee \ell_i}$;
Cut: $\frac{F \vee (\bigwedge_{i=0}^{w} \ell_i), G \vee (\bigvee_{i=0}^{w} \neg \ell_i)}{F \vee G}$.

The **size** of the proof π is s. In fact, more naturally one can define the size of the proof as a sum of sizes of C_i, but all our results holds also for our definition (that is stronger in terms of lower bounds).

3 Expanders

We use the following notation: $\mathrm{N}_G(S)$ is the set of neighbours of the set of vertices S in the graph G, $\partial_G(S)$ is the set of unique neighbours of the set of vertices S in the graph G. A vertex v is a unique neighbour of a set S iff there is exactly one edge between v and S. We omit the index G if the graph is evident from the context. Note that in general, for a vertex v, $\partial_G(v)$ is not necessarily equal to $\mathrm{N}_G(v)$, because there could be parallel edges.

A bipartite graph $G \coloneqq (L, R, E)$ is an (r, Δ, c)**-expander** if all vertices $u \in L$ have degree at most Δ and for all sets $S \subseteq L$, $|S| \leq r$, it holds that $|\mathrm{N}(S)| \geq c \cdot |S|$. Similarly, $G \coloneqq (L, R, E)$ is an (r, Δ, c)**-boundary expander** if all vertices $u \in L$ have degree at most Δ and for all sets $S \subseteq L$, $|S| \leq r$, it holds that $|\partial(S)| \geq c \cdot |S|$. In this context, a simple but useful observation is that

$$|\mathrm{N}(S)| \leq |\partial(S)| + \frac{\Delta|S| - |\partial(S)|}{2} = \frac{\Delta|S| + |\partial(S)|}{2},$$

since all non-unique neighbours have at least two incident edges. This implies that if a graph G is an $(r, \Delta, (1-\varepsilon)\Delta)$-expander then it is also an $(r, \Delta, (1-2\varepsilon)\Delta)$-boundary expander.

The next Lemma is well known in the literature. In this form it was used in [21].

▶ **Lemma 4.** *Let $G = (L, R, E)$ be an (r, Δ, c)-boundary expander. Let $S \subseteq L$ be a set of vertices, $|S| \leq r$. Then there exists an enumeration $S = \{s_1, s_2, \ldots, s_{|S|}\}$ and a partition $\bigsqcup_i R_i = \mathrm{N}(S)$ such that:*

- $R_i = \mathrm{N}(s_i) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}(s_j) \right)$;
- $|\partial(s_i) \cap R_i| \geq c$.

Proof. Since $|S| \leq r$ it holds that $|\partial(S)| \geq c|S|$ and there is a vertex $s_{|S|} \in S$ such that

$$|\partial(s_{|S|}) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}(s_j) \right)| \geq c.$$

Hence we can set $R_{|S|}$ as desired, and repeat the process for $S \setminus \{s_{|S|}\}$. ◀

Since papers [5, 4] a "closure" operation is widely used in proof complexity. In this paper we start with definition from [5] and show some additional properties of it. To emphasize the difference, we call it **individual closure**.

Let $G \coloneqq (L, R, E)$ denote a bipartite graph of left degree at most Δ. We say that a vertex $v \in L$ is **ν-captured** by a set $J \subseteq R$ iff $|\mathrm{N}(v) \cap J| \geq \Delta - \nu$. Let $\mathrm{ICl}^{\nu}_{G}(J) \subseteq L$ be the smallest set of vertices that are ν-captured by $\mathrm{N}(\mathrm{ICl}^{\nu}_{G}(J)) \cup J$. We also can define the set $\mathrm{ICl}^{\nu}_{G}(J)$ inductively: $\mathrm{ICl}^{\nu}_{G}(J)$ may be considered as a maximal sequence of distinct vertices $\{v_1, v_2, v_3, \ldots, v_i, \ldots\}$ such that v_i is ν-captured by $J \cup \bigcup_{j=1}^{i-1} \mathrm{N}(v_j)$. We denote by $\mathrm{Ext}^{\nu}_{G}(J) \coloneqq J \cup \mathrm{N}(\mathrm{ICl}^{\nu}_{G}(J))$ the **extension** of J.

▶ Remark 5. $\mathrm{ICl}^{\nu}_{G}(J)$ is unique and well-defined.

Proof. Fix some set J. Let $V \coloneqq \{v_1, v_2, v_3, \ldots, v_i, \ldots, v_{|V|}\}$ and $U \coloneqq \{u_1, u_2, u_3, \ldots, u_i, \ldots, u_{|U|}\}$ be two sequences that satisfy the required properties. For the sake of contradiction assume that $U \setminus V \neq \emptyset$. Pick the first vertex $u_j \in U$ that does not appear in V. But $|\mathrm{N}(u_j) \cap (J \cup \bigcup_{k=1}^{j-1} \mathrm{N}(u_k))| \geq \Delta - \nu$ and by the choice of u_j: $|\mathrm{N}(u_j) \cap (J \cup \bigcup_{v \in V} \mathrm{N}(v))| \geq \Delta - \nu$. Hence we can extend V by u_j, which contradicts with the maximality. ◀

▶ **Lemma 6.** *Let $c > \nu \geq 0$. Suppose that G is an (r, Δ, c)-boundary expander and that $J \subseteq R$ has size $|J| < (c - \nu)r$. Then $|\mathrm{ICl}^{\nu}(J)| \leq \frac{|J|}{c-\nu}$.*

Proof. Let $V \coloneqq \{v_1, v_2, v_3, \ldots, v_\ell\}$ be a sequence of vertices from L that generates $\mathrm{ICl}^{\nu}(J)$. If $\ell > r$ then $S \subseteq \{v_1, v_2, \ldots, v_r\}$ otherwise $S \coloneqq V$.

Note that $\partial(S) \subseteq \bigcup_{i=1}^{|S|} (\mathrm{N}(v_i) \setminus \mathrm{N}\left(\bigcup_{j=1}^{i-1} v_j\right))$. Hence:

$$\begin{aligned} |\partial(S) \setminus J| &\leq \sum_{i=1}^{|S|} |\mathrm{N}(v_i) \setminus (\mathrm{N}\left(\bigcup_{j=1}^{i-1} v_j\right) \cup J)| \\ &\leq \sum_{i=1}^{|S|} \nu \\ &\leq \nu |S|. \end{aligned}$$

Since $|S| \leq r$ by definition, the expansion property of the graph guarantees that $|\partial(S) \setminus J| \geq c|S| - |J|$. Altogether $|S| \leq \frac{|J|}{c-\nu} < r$ and the conclusion follows. ◀

Suppose $J \subseteq R$ is not too large. Then Lemma 6 shows that the individual closure of J is not much larger. Thus, after removing the closure and its neighbourhood from the graph, we are still left with a decent expander. The following lemma makes this intuition precise.

▶ **Lemma 7.** *Let $G \coloneqq (L, R, E)$ be an (r, Δ, c)-boundary expander and $J_1, J_2, \ldots, J_\ell \subseteq R$. Then the graph $G \setminus \left(\bigcup_{i=1}^{\ell} (\mathrm{Ext}^{\nu_i}(J_i) \cup \mathrm{ICl}^{\nu_i}(J_i))\right)$ is an $(r, \Delta, c - \sum_{i=1}^{\ell} (\Delta - \nu_i))$-boundary expander.*

Proof. Consider a vertex $v \in L$ and suppose that $v \in L \setminus \left(\bigcup_{i=1}^{\ell} \mathrm{ICl}^{\nu_i}(J_i)\right)$. By definition of individual closure for all $i \in [\ell]$: $|\mathrm{N}(v) \cap \mathrm{Ext}^{\nu_i}(J_i)| < \Delta - \nu_i$. Hence:

$$|\mathrm{N}(v) \cap \left(\bigcup_{i=1}^{\ell} \mathrm{Ext}^{\nu_i}(J_i)\right)| < \sum_{i=1}^{\ell} (\Delta - \nu_i).$$

Hence for any $S \subseteq L \setminus \left(\bigcup_{i=1}^{\ell} \mathrm{ICl}^{\nu_i}(J_i) \right)$ of size at most r:

$$|\partial(S) \setminus \left(\bigcup_{i=1}^{\ell} \mathrm{Ext}^{\nu_i}(J_i) \right)| \geq c|S| - \sum_{i=1}^{\ell} (\Delta - \nu_i)|S|. \quad \blacktriangleleft$$

We also need a technical definition for a graph $G \coloneqq (L, R, E)$ that is (r, Δ, c)-boundary expander. We say that a pair (S, T) where $S \subseteq L$ and $T \subseteq R$ is **ζ-reasonable** iff $(L \setminus S, R \setminus (T \cup \mathrm{N}(S)), E)$ is an (r, Δ, ζ)-boundary expander.

▶ Remark 8. A partial case of Lemma 7 may be reformulated as follows.

Let $G \coloneqq (L, R, E)$ be an (r, Δ, c)-boundary expander and $J \subseteq R$. Then a pair $(\mathrm{ICl}^{\nu}(J), \mathrm{Ext}^{\nu}(J))$ is $(c - (\Delta - \nu))$-reasonable.

The following property of individual closure is crucial for our purpose. On the one hand, it is trivial, on the other hand, it is unexpected, since for other definitions of closure (for example [16, 36]) it works in a completely opposite way.

▶ **Lemma 9.** *Let $G \coloneqq (L, R, E)$ be a bipartite graph with left degree at most Δ and $G' \coloneqq (L', R', E)$ be a subgraph of G. For any set $J \subseteq R$ and any ν the following holds.*

1. $\mathrm{ICl}^{\nu}_{G'}(J \cap R') \subseteq \mathrm{ICl}^{\nu}_{G}(J)$.
2. *If $J' \subseteq J$ then* $\mathrm{ICl}^{\nu}_{G}(J') \subseteq \mathrm{ICl}^{\nu}_{G}(J)$.

Proof. Let $\{v_1, v_2, v_3, \ldots, v_i, \ldots\}$ be the sequence that generates $\mathrm{ICl}^{\nu}_{G'}(J \cap R')$. Note that $|\mathrm{N}_{G'}(v_i) \cap (J \cup \mathrm{N}_{G'}\left(\bigcup_{j=1}^{i-1} v_j \right)| \geq \Delta - \nu$ hence $|\mathrm{N}_{G}(v_i) \cap (J \cup \mathrm{N}_{G}\left(\bigcup_{j=1}^{i-1} v_j \right)| \geq \Delta - \nu$. So by induction on i we conclude that all elements $v_i \in \mathrm{ICl}^{\nu}_{G}(J)$.

The second property follows from the similar argument. Let $\{v_1, v_2, v_3, \ldots, v_i, \ldots\}$ be the sequence that generates $\mathrm{ICl}^{\nu}_{G}(J')$. Note that $|\mathrm{N}_{G}(v_i) \cap (J' \cup \mathrm{N}_{G}\left(\bigcup_{j=1}^{i-1} v_j \right)| \geq \Delta - \nu$ hence $|\mathrm{N}_{G}(v_i) \cap (J \cup \mathrm{N}_{G}\left(\bigcup_{j=1}^{i-1} v_j \right)| \geq \Delta - \nu$. So by induction on i we conclude that all elements $v_i \in \mathrm{ICl}^{\nu}_{G}(J)$. $\blacktriangleleft$

Let $G \coloneqq (L, R, E)$ be an (r, Δ, c)-boundary expander and $J, J' \subseteq R$. We say that J, J' are **ν-closure-independent**, if

$$(\mathrm{Ext}^{\nu}(J) \cap \mathrm{Ext}^{\nu}(J')) = \emptyset.$$

For a collection of sets $\mathcal{T} \coloneqq \{T_1, \ldots, T_\ell\}$ we say that a **closure covering number** (denoted as $\mathrm{clv}^{\nu}(\mathcal{T})$) is the least size of a hitting set for the collection of sets $\{\mathrm{Ext}^{\nu}(T_i)\}_{i \in [\ell]}$, i.e. the least size of a set $H \subseteq R$ such that for all $i \in [\ell]$ if $\mathrm{Ext}^{\nu}(T_i)$ is nonempty then there is $h \in H$ such that $h \in \mathrm{Ext}^{\nu}(T_i)$.

4 Random CNF Formulas and Linear Systems

Let φ be a formula in variables from a set X. With this formula, we associate a bipartite dependency graph $G^{\varphi} \coloneqq (L, R, E)$ where L corresponds to the set of clauses of φ (and we identify these two sets), R corresponds to the set of variables (and we also identify these two sets) and $(u, v) \in E$ iff clause u contains a variable v or its negation.

We consider random CNFs as in Definition 1. In Appendix C we present some classical computations that show that randomly sampled graph is a good enough expander (see also [38]).

Let φ be a CNF formula on n variables with m clauses. We define a system of linear equations A_φ over $\mathbb{F}_2$. Let $C \coloneqq x_1^{a_1} \vee \cdots \vee x_w^{a_w}$ be a clause from φ. We add to A_φ the equation $x_1 + \cdots + x_w = 1 + (1 - a_1) + \cdots + (1 - a_w)$. We do this for every clause $C \in \varphi$.

We identify the linear system A and its standard encoding in CNF. Note that φ is a subformula of A_φ, so a lower bound on the length of a refutation for A_φ implies a lower bound for φ as well.

Let A be a linear system over boolean variables from the set X. Suppose that the equations are labeled by the elements of a set Y. Let A^I denote a subsystem of A on equations labeled by the set $I \subseteq Y$. For a partial assignment ρ by $A|_\rho$ we denote a system over variables $X \setminus \operatorname{supp}(\rho)$ that is obtained from A by an application of ρ. We remove all the equations that are satisfied by ρ.

By analogy with dependency graph of a formula φ we define a dependency graph of a linear system A.

▶ **Definition 10.** *Let $G^A \coloneqq (L, R, E)$ be a bipartite graph where the left part L corresponds to equations of A, and the right part R to its variables. We draw an edge (ℓ, r) iff r appears in ℓ where r is a variable and ℓ is an equation.*

Note that G^φ and G^{A_φ} are identical.

4.1 Locally Consistent Assignments

Let A be a linear system based on a graph $G \coloneqq (L, R, E)$ that is an (r, Δ, c)-expander. We say that a partial assignment σ is **locally consistent** iff there is $\zeta > 0$ and a ζ-reasonable pair (S, T) such that:

- $\operatorname{supp}(\sigma) \subseteq T \cup \mathrm{N}(S)$;
- the system $A^S|_\sigma$ is satisfiable.

The next Lemma is an analog of similar statement from [3]. But since we change the definition of a locally consistent assignment we provide a proof in Appendix D.

▶ **Lemma 11.** *Let A be a linear system based on a graph $G \coloneqq (L, R, E)$ that is an (r, Δ, c)-expander. If σ is a locally consistent assignment, then for any I of size at most r the system $A^I|_\sigma$ is satisfiable.*

The following lemma gives us a useful characterisation of locally consistent assignments.

▶ **Lemma 12.** *Let A be a linear system based on a graph $G \coloneqq (L, R, E)$ that is an (r, Δ, c)-expander, $J \subseteq R$ and σ be an assignment on a subset of J.*

1. *If the assignment σ is locally consistent, then $A^{\mathrm{ICl}^\nu(J)}|_\sigma$ is satisfiable for all positive $\nu < c$ such that $|J| < (c - \nu)r$.*
2. *If the system $A^{\mathrm{ICl}^\nu(J)}|_\sigma$ is satisfiable for some positive $\nu < c$ such that $|J| < (c - \nu)r$ and $c > (\Delta - \nu)$, then the assignment σ is locally consistent.*

Proof. Note that if $|J| < (c - \nu)r$, then by Lemma 6 $|\mathrm{ICl}^\nu(J)| \leq r$ and the first statement follows from Lemma 11.

For the second statement note that a pair $(\mathrm{ICl}^\nu(J), \mathrm{Ext}^\nu(J))$ is $c - (\Delta - \nu)$-reasonable by Lemma 7. The statement follows from definition of local consistency. ◀

▶ **Lemma 13** (Alekhnovich [3]). *Let Y be the set of variables. Let ρ be partial assignment uniformly distributed on an affine subspace $A \subseteq \{0,1\}^Y$. Then for every term t in Y variables either $\Pr[t|_\rho = 1] = 0$ or $\Pr[t|_\rho = 1] \geq \frac{1}{2^{|t|}}$.*

4.2 Random Restrictions

▶ **Definition 14.** *Let A be a linear system, $G^A := (L, R, E)$ be an (r, Δ, c)-expander and $T \subseteq R$. We denote a uniform distribution over all locally consistent partial assignments with support T as $\mathfrak{U}^G_T$.*

We define a distribution $\mathfrak{U}_{p,\nu}$ on partial assignments as follows:

- *create a set $J \subseteq R$ by adding each element of R into J uniformly at random with probability p;*
- *pick an assignment from $\mathfrak{U}^G_{\mathrm{Ext}^\nu(J)}$.*

We omit the graph if it is clear from the context.

The following Lemma is a very powerful technical tool that helps to establish that some parts of random restrictions in the considered distributions may be chosen independently.

▶ **Lemma 15.** *Let A be a linear system based on a graph $G := (L, R, E)$ that is (r, Δ, c)-boundary expander where $c > 2(\Delta - \nu)$ for some positive $\nu < c$.*

Let $J \subseteq R$ be a set of size less than $(c-\nu)r$. Consider two sets $S, T \subseteq J$ that are ν-closure independent. If σ, σ' are the locally consistent assignments on S and κ is a locally consistent assignment on T, then:

$$\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \sigma \subseteq \rho] = \Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \sigma' \subseteq \rho].$$

Proof. Consider an arbitrary assignment σ such that $\mathrm{supp}(\sigma) \subseteq J$. Note that by Lemma 12 σ is locally consistent iff $A^{\mathrm{ICl}^\nu(J)}|_\sigma$ is satisfiable.

Fix an arbitrary locally consistent assignment η on S. Since it is locally consistent, $A^{\mathrm{ICl}^\nu(J)}|_\eta$ is satisfiable. Moreover any extension of $\eta' \supseteq \eta$ to the $\mathrm{supp}(\rho) = J$ is locally consistent iff $A^{\mathrm{ICl}^\nu(J)}|_{\eta'}$ is satisfiable. Hence the number of such extensions depends only on the number of linearly independent equations in $A^{\mathrm{ICl}^\nu(J)}|_\eta$ and in $A^{\mathrm{ICl}^\nu(J)}|_{\eta'}$ and does not depends on the values that we assign in η.

This means that under the condition $\eta \subseteq \rho$ the assignment ρ is generated uniformly at random among partial assignments that leave linear system $A^{\mathrm{ICl}^\nu(J)}|_\eta$ satisfiable. Since these conditions are linear, we also may think that under condition $\eta \subseteq \rho$ the assignment ρ is generated in the following way: pick a total extension of η that satisfies $A^{\mathrm{ICl}^\nu(J)}|_\eta$ uniformly at random, and then project in onto $\mathrm{supp}(\rho)$.

Considering the above properties and noticing that $\kappa \subseteq \rho$ is also a linear constraint, we may compute the required probability:

$$\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \eta \subseteq \rho] = \frac{\mathrm{sol}(A^{\mathrm{ICl}^\nu(J)}|_{\eta \cup \kappa})}{\mathrm{sol}(A^{\mathrm{ICl}^\nu(J)}|_\eta)},$$

where sol is the number of solutions. We have already shown that the denominator is independent of the exact values that we assign in η, hence to conclude the proof it is enough to show that numerator is also independent of η and κ. To do it we show that the system $A^{\mathrm{ICl}^\nu(J)}|_{\eta \cup \kappa}$ is satisfiable and hence number of solutions depends only on sizes of η and κ.

By Lemma 4 there is an enumeration $H := \{v_1, \ldots, v_{|H|}\}$ of vertices in $\mathrm{ICl}^\nu(J)$ and a sequence R_i such that:

- $R_i = \mathrm{N}(v_i) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}(v_j) \right)$;
- $|\partial(v_i) \cap R_i| \geq c$.

By Lemma 6 $|\mathrm{ICl}^{\nu}(S)| \leq r$, hence by Lemma 11 system $A^{\mathrm{ICl}^{\nu}(S)}|_{\eta}$ is satisfiable, hence there is an assignment η' on $\mathrm{Ext}^{\nu}(S)$ that is an extension of η and satisfies $A^{\mathrm{ICl}^{\nu}(S)}|_{\eta}$. By Remark 8 (by Lemma 7) $(\mathrm{ICl}^{\nu}(S), \mathrm{Ext}^{\nu}(S))$ is $(c-(\Delta-\nu))$-reasonable and hence η' is locally consistent. By the similar argument we can pick as assignment κ' that is locally consistent extension of κ on $\mathrm{Ext}^{\nu}(T)$. By induction on $i \in [|\mathrm{ICl}^{\nu}(J)|]$ we create an assignment β_i such that:

- $\mathrm{supp}(\beta_i) = R_i$;
- β_i is consistent with $\eta' \cup \kappa'$;
- A^{v_i} is satisfied by $\bigcup_{j=1}^{i} \beta_i$.

Suppose we have already done this for all $j \in [i-1]$. Let us consider the following cases.

1. $v_i \in \mathrm{ICl}^{\nu}(S)$. In this case η' assigns all variables in $R_i \subseteq \mathrm{N}(v_i)$ and β_i assigns all variables wrt to η'. By induction hypothesis β_j is consistent with η, hence by construction of R_i the assignment $\bigcup_{j=1}^{i} \beta_i$ assigns all variables in $\mathrm{N}(v_i)$ wrt to η' and hence it satisfies A^{v_i} since η' satisfies it.
2. $v_i \in \mathrm{ICl}^{\nu}(T)$. Similar to the previous case (we should consider κ' instead of η').
3. $v_i \notin (\mathrm{ICl}^{\nu}(S) \cup \mathrm{ICl}^{\nu}(T))$. By definition of individual closure η' can assign at most $\Delta - \nu$ variables in $\mathrm{N}(v_i)$, the same holds for κ'. Hence η' and κ' together assign at most $2(\Delta-\nu)$ variables, which is strictly less than $c \leq |\partial(v_i) \cap R_i|$ and there is a variable in $\partial(v_i) \cap R_i$ that is unassigned by $\kappa' \cup \eta'$ and we can use it to satisfy the equation A^{v_i}. Hence we can find an assignment β_i that respects $\kappa' \cup \eta'$ and satisfies A^{v_i}. Here we use the fact that S and T are closure independent and hence κ' and η' are disjoint.

The assignment $\bigcup_{i \in [|\mathrm{ICl}^{\nu}(J)|]} \beta_i$ satisfies $A^{\mathrm{ICl}^{\nu}(J)}|_{\kappa \cup \eta}$ by construction. Hence $\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \eta \subseteq \rho]$ is independent of the choice of η and the statement holds. ◀

▶ **Corollary 16.** *Let A be a linear system based on a graph $G := (L, R, E)$ that is (r, Δ, c)-boundary expander where $c > 2(\Delta - \nu)$ for some positive $\nu < c$.*

Let $J \subseteq R$ be a set of size less than $(c-\nu)r$. Consider two sets $S, T \subseteq J$ that are ν-closure independent. If σ is a locally consistent assignment on S and κ is a locally consistent assignment on T then:

$$\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \sigma \subseteq \rho] = \Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho].$$

Proof. Follows from Lemma 15 and observation that $\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho]$ can be obtained from $\Pr_{\rho \sim \mathfrak{U}_J}[\kappa \subseteq \rho \mid \sigma \subseteq \rho]$ by averaging over all locally consistent $\sigma \subseteq \rho$. ◀

5 Lower Bound

In this section we give a proof of the main technical Theorem.

▶ **Theorem 17** (Reformulation of Theorem 3)**.** *Let A be a linear system such that G^A is an $(r, \Delta, (1-\varepsilon)\Delta)$-boundary expander where $\varepsilon = 0.05$. Then for any $\delta > 0$ if:*

$$n^{\delta} \left(\frac{n}{8\varepsilon r} \right)^{k^2/\varepsilon} = o(r/k)$$

then any Res(k) *proof of A has size at least $2^{n^{\delta}}$.*

Following the plan presented in the introduction, we want to hit the proof by an assignment ρ and transform it into a "resolution" (in fact, a structure we call "DNF-tree", which will be defined later) proof. We do it in several steps.

- We start with the technical tool: "Restriction Lemma", Section 5.1 . It states that a k-DNF that contains a lot of *independent* terms (here we use the definition of closure-independent terms) can be easily killed by an assignment from an appropriate distribution. It is our crucial technical tool.
- In Section 5.2, we give the definition of DNF-trees. We then continue with the assumption that we have a short Res(k)-proof π of the system A and give a detailed plan of its transformation to a sequence of DNF-trees in Section 5.3.1.
- In Section 5.3.2 we describe a transformation of Res(k)-proof into DNF-tree proof of A. During this process, we give up on some DNFs that appear in the middle steps of transformation (we call them *broken branches*).
- In Section 5.3.3 we choose a proper partial assignment and use our Restriction Lemma to get rid of all broken branches. That concludes the transformation of π into DNF-tree proof of A_ρ. Moreover, all DNF-trees in this proof will have small height.
- In the last step (Section 5.3.5) we give a direct proof of the lower bound on the height of DNF-trees.

Recall that the plan in the introduction required to prove the dichotomy for k-DNFs (size of hitting set vs. probability of being killed by random restriction). The essential part of this dichotomy is "Restriction Lemma", that we prove by using Lemma 15.

We deal with linear systems based on the expander graphs and we associate variables with the vertices of the right part of the graph. Hence we can define **closure-independent** terms and **a closure covering number** of a collection of terms in a natural way.

Let us start the realization of our plan.

5.1 Restriction vs. Closure Covering Number

We start with a technical lemma. It gives a way to translate a knowledge that some terms are closure-independent to the language of probabilities.

We call the term *locally consistent* if the corresponding partial assignment (that is, the minimal partial assignment satisfying the term) is locally consistent. We denote as vars(t) a set of variables of the term t.

▶ **Lemma 18.** *Let A be a linear system such that $G^A := (L, R, E)$ is an (r, Δ, c)-boundary expander where $c > 2(\Delta - \nu)$ for some positive $\nu < c$. Let $J \subseteq R$ be a set of size less than $(c - \nu)r$. If $T := \{t_1, \dots, t_\ell\}$ is a sequence of locally consistent terms such that for any $i \le \ell$:*

- *vars$(t_i) \subseteq J$;*
- *vars(t_i) is ν-closure-independent of $\bigcup_{j=1}^{i-1}$ vars(t_j);*

then:

$$\Pr_{\rho \sim \mathfrak{U}_J} [\forall i \in [\ell] \colon t_i \mid_\rho \neq 1] \le \left(1 - \frac{1}{2^k}\right)^{|T|}.$$

Proof. We argue by induction on a number of terms that:

$$\Pr_{\rho \sim \mathfrak{U}_J} \left[\left(\bigvee_{j=1}^{i} t_j \right) \mid_\rho = 0 \right] \le \left(1 - \frac{1}{2^k}\right)^{i}.$$

For $i := \ell$ we get the statement of the Lemma.

The base of induction follows from Lemma 13 since t_1 is locally consistent (and by Lemma 11 the probability that it is mapped to 1 by ρ is not zero): $\Pr[t_1|_\rho = 0] \le \left(1 - \frac{1}{2^k}\right)$. Now suppose we proved the statement for the collection $\{t_1, \dots, t_{i-1}\}$. Let us now do the induction step for term t_i.

We can consider a locally consistent assignment σ such that:

- $\mathrm{supp}(\sigma) = t_i$,
- $t_i|_\sigma = 1$,

since t_i is locally consistent. If ρ is consistent with σ then t_i is mapped to 1 by ρ hence $\Pr\limits_{\rho\sim\mathfrak{U}_J}[t_i|_\rho = 1] = \Pr\limits_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho]$.

Let S_i be an event that $\left(\bigvee\limits_{j=1}^{i} t_j\right)|_\rho = 0$. And let $\mathfrak{U}_i$ be the distribution $\mathfrak{U}_J$ conditioned on S_i.

$$
\begin{aligned}
\Pr_{\rho\sim\mathfrak{U}_J}[S_i] &\le \Pr_{\rho\sim\mathfrak{U}_J}[S_{i-1}] \cdot \Pr_{\rho\sim\mathfrak{U}_J}[t_i|_\rho = 0 \mid S_{i-1}] \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \Pr_{\rho\sim\mathfrak{U}_J}[t_i|_\rho = 0 \mid S_{i-1}] && \text{by induction hyp.} \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho\sim\mathfrak{U}_J}[t_i|_\rho = 1 \mid S_{i-1}]\right) && \rho \text{ assigns all variables in } t_i \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho \mid S_{i-1}]\right) \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \mathop{\mathbb{E}}_{\kappa\sim\mathfrak{U}_{i-1}}\left[\Pr_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho \mid \kappa \subseteq \rho]\right]\right) \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \mathop{\mathbb{E}}_{\kappa\sim\mathfrak{U}_{i-1}}\left[\Pr_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho]\right]\right) && \text{by Corollary 16} \\
&\le \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho]\right).
\end{aligned}
$$

We can use Corollary 16 since $\bigcup\limits_i vars(t_i) \subseteq J$ and the support of all assignment does not exceed $(c-\nu)r$, moreover κ is taken over locally consistent assignments since $\mathfrak{U}_J$ is a distribution over locally consistent assignments.

It remains to show that $\Pr\limits_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho] \ge \frac{1}{2^k}$. Note that ρ is consistent with σ iff ρ maps t_i to 1. Hence by Lemma 13 $\Pr\limits_{\rho\sim\mathfrak{U}_J}[\sigma \subseteq \rho] = \Pr\limits_{\rho\sim\mathfrak{U}_J}[t_i|_\rho = 1] \ge \frac{1}{2^{|t_i|}} \ge \frac{1}{2^k}$. ◀

5.2 Tree and DNF

In this section we describe a technical structure that is a mix of DNF and decision tree. Let A be a linear system based on the (r, Δ, c)-expander graph.

▶ **Definition 19.** *A **DNF-tree** is a rooted binary tree such that:*

- *every internal node is labelled with a variable;*
- *the edges leaving this node correspond to whether the variable is set to* 0 *or* 1*;*
- *the leaves are labelled either with constant from* $\{0, 1\}$ *or with DNF-formulas.*

As usual, we assume that on every given path no variable appears more than once. Then every path from the root to a leaf may be viewed as a partial assignment, and this assignment, in turn, will be sometimes identified with the corresponding leaf.

For a DNF-tree T, we denote the set of paths (partial assignments) that lead from the root to a leaf as Br_T. We also denote the set of paths leading to some leaf labelled by $a \in \{0,1\}$ as Br_T^a. Finally, we denote the set of paths (partial assignments) that lead from the root to a leaf labelled by a non-trivial formula by Br_T^*. We say that a DNF-tree T ***strongly represents*** *a DNF formula D if for every $\pi \in \mathrm{Br}_T^0$ and for all $t \in D$, $t|_\pi = 0$ and for every $\pi \in \mathrm{Br}_T^1$, there exists $t \in D$ such that $t|_\pi = 1$.*

Consider a DNF-tree T and a partial assignment ρ. An **application of ρ to T** denoted by $T|_\rho$ is defined in a natural way by induction from leaves to root:

- if ℓ is a leaf marked by 0 or 1 then $\ell|_\rho := \ell$;
- if ℓ is a leaf marked by DNF D then $\ell|_\rho$ is also a single vertex marked by $D|_\rho$ (note that if some term in D is mapped to 1 by ρ then $D|_\rho = 1$ or if all terms are mapped to 0 then $D|_\rho = 0$);
- if T is a tree with the root marked by a variable x and two children T_0 and T_1 then:
  - if $x \notin \mathrm{supp}(\rho)$ then $T|_\rho$ is a tree with a root marked by x and two children $T_0|_\rho$ and $T_1|_\rho$;
  - if $x \in \mathrm{supp}(\rho)$ then $T|_\rho := T_{\rho(x)}|_\rho$.

5.3 Proof of Theorem 17

Fix some parameters:

- $\zeta_i := (1 - i\varepsilon)\Delta$ are various expansion parameters of graphs that appear in the proof;
- $p := \varepsilon \frac{r}{n}$.

Let $\pi := \{D_1, D_2, \ldots, D_s\}$ be a $\mathrm{Res}(k)$ proof of A of size at most 2^{n^δ}.

5.3.1 Plan of the Proof

We say that a partial assignment σ is **ν-closed** wrt G iff there is a set J_σ such that $\mathrm{supp}(\sigma) = \mathrm{Ext}_G^\nu(J_\sigma)$. For a collection of ν-closed partial assignments $\sigma_1, \sigma_2, \ldots, \sigma_\ell$ we define a graph $G^{\sigma_1,\sigma_2,\ldots,\sigma_\ell} := (L \setminus \bigcup_{i=1}^{\ell} \mathrm{ICl}_G^\nu(J_{\sigma_i}), R \setminus \bigcup_{i=1}^{\ell} \mathrm{Ext}_G^\nu(J_{\sigma_i}), E)$.

Let us say that a DNF-tree T is **closed (wrt a system A)** iff for every branch σ the assignment σ is ζ_2-closed wrt G^A.

In this section, when we deal with locally consistent assignments wrt to a linear system A based on a graph G, we omit the mention of A, as it is fixed. We refer to such assignments as locally consistent wrt to a graph G.

We think of π as a sequence of closed DNF-trees $\{T_1^1, T_2^1, \ldots, T_s^1\}$ where T_i^1 is a tree that consists of single node marked by the formula D_i.

We make $\frac{k}{\varepsilon}$ iterations of modification of these trees. On i-th iteration we create a collection $\{T_1^{i+1}, T_2^{i+1}, \ldots, T_s^{i+1}\}$. We also divide branches into three groups:

- $B_j^{i+1} \subseteq \mathrm{Br}^*_{T_j^{i+1}}$ is a collection of **broken** branches that we create during our process;
- $\sigma \in \mathrm{Br}_{T_j^{i+1}}$ that are locally inconsistent wrt G are **dead** branches;
- all other branches are **alive**.

For all $j \in [s]$ the set B_j^1 is empty.

We maintain an upper bound of the height of the trees and the **correctness** property, i.e.

- T_j^i strongly represents D_j,
- moreover each branch $\sigma \in \mathrm{Br}_{T_j^i}$ is marked by $D_j|_\sigma$ (it can possibly turn to a constant after applying the restriction).

After $\frac{k}{\varepsilon}$ iterations we stop modifications and try to find a set of variables $J \subseteq R$ and some ζ_2-closed partial assignment ρ on $\mathrm{Ext}_G^{\zeta_2}(J)$ that helps to achieve an additional property for each branch σ of tree T_j^i:

- if $\sigma \in B_j^i$ then:
  - either σ is inconsistent with ρ,
  - or there is a term $t \in D_j$ such that $t|_{\sigma\cup\rho} = 1$;
- if σ is alive then it is marked by a constant or by a collection of locally inconsistent terms wrt $G^{\sigma,\rho}$ (or in other words G without $(\mathrm{ICl}_G^{\zeta_2}(J_\sigma) \cup \mathrm{ICl}_G^{\zeta_2}(J), \mathrm{Ext}_G^{\zeta_2}(J_\sigma) \cup \mathrm{Ext}_G^{\zeta_2}(J)))$.

We say that a tree that satisfies all required properties is **perfect**. In section 5.3.5 we show the lower bound on the height of trees in the collection of perfect trees that corresponds to the proof of $A|_\rho$.

5.3.2 From $\mathrm{Res}(k)$ to Perfect DNF-trees

Let us fix some parameters:

- $d_i \coloneqq 2n^\delta \left(\frac{8}{p}\right)^{(i-1)k}$ is an upper bound on the sizes of sets J_σ for branches σ that appear in the trees T_j^i. Here J_σ is defined as in the beginning of 5.3.1;
- $s_i \coloneqq s2^{d_i/\varepsilon}$ is an upper bound on the total number on branches in these trees;
- $b_i \coloneqq n^\delta \left(\frac{8}{p}\right)^{ik}$ is a threshold for coverings.

Here i is the number of the iteration, and is in the range $[1, \frac{k}{\varepsilon}]$.

Now we describe a construction of $\{T_1^{i+1}, T_2^{i+1}, \ldots, T_s^{i+1}\}$ from $\{T_1^i, T_2^i, \ldots, T_s^i\}$. Suppose that before i-th iteration we have a sequence $\{T_1^i, T_2^i, \ldots, T_s^i\}$ of correct DNF-trees. Let $T \coloneqq T_j^i$. Consider a branch $\sigma \in \mathrm{Br}_T$. If $\sigma \in \mathrm{Br}_T^*$ then it is marked by $D_j|_\sigma$, so let F_σ be a DNF formula that consists of terms of $D_j|_\sigma$ that are locally consistent wrt G^σ.

There are four cases:

- Branch $\sigma \in B_j^a$ for some $a \le i$ or dead. We do not modify σ.
- Branch σ is marked by a constant. We do not modify σ.
- $\mathrm{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) \le b_i$. Let C be the set of variables on which the value of $\mathrm{clv}_{G^\sigma}^{\zeta_4}(F_\sigma)$ is achieved. We add a full binary tree that splits over all variables from

  $$\mathrm{Ext}_G^{\zeta_2}(J_\sigma \cup C) \setminus \mathrm{Ext}_G^{\zeta_2}(J_\sigma)$$

  (see fig. 1). We mark the new leaves by the appropriately restricted DNF formulas and a set $J_\sigma \cup C$. Note that $|J_\sigma \cup C| \le 2n^\delta \left(\frac{8}{p}\right)^{(i-1)k} + n^\delta \left(\frac{8}{p}\right)^{ik} \le 2n^\delta \left(\frac{8}{p}\right)^{ik} = d_{i+1}$. The height of these branches is $|\mathrm{Ext}_G^{\zeta_2}(J_\sigma \cup C)|$. By Lemma 6, $|\mathrm{ICl}_G^{\zeta_2}(J_\sigma \cup C)| \le \frac{d_{i+1}}{2\varepsilon}$, so it follows that $|\mathrm{Ext}_G^{\zeta_2}(J_\sigma \cup C)| \le \frac{d_{i+1}}{\varepsilon}$.
- $\mathrm{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) > b_i$. We put σ into B_j^{i+1}.

We say that $T_j^{i+1} \coloneqq T$. We satisfy the correctness property by construction.

5.3.3 Perfectness. Broken Branches

We pick an assignment ρ from distribution $\mathfrak{U}_{p,\zeta_2}$. By construction, this assignment is ζ_2-closed, and the witness of this property is $J_\rho \coloneqq J$, where J is a set from the algorithm that generates this assignment.

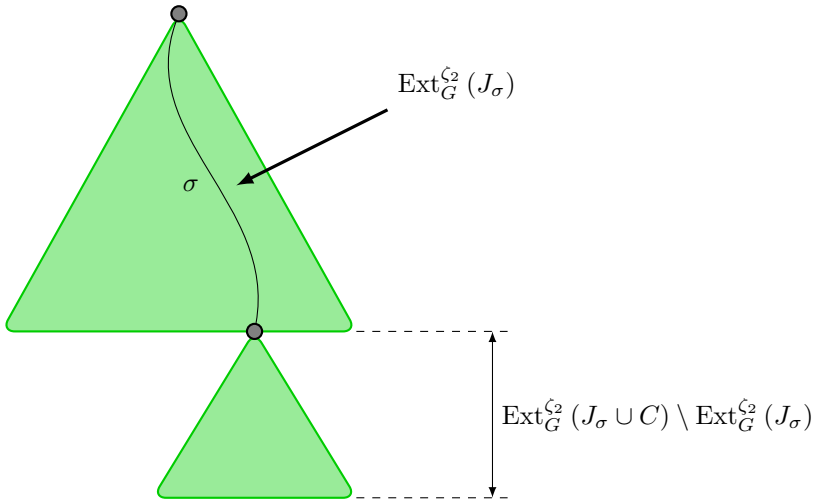

Figure 1 Modification of a branch.

Note that by Chernoff bound:

$$\Pr[|J| \geq 2pn] \leq \exp\left[-\frac{4}{3}pn\right] \leq \exp\left[-\frac{4}{3}\varepsilon r\right].$$

So we assume that $|J| < 2pn$.

Consider some branch $\sigma \in B_j^i$ that is consistent with ρ. Note that:

- G^σ is a dependency graph of $A|_\sigma$;
- G^σ is the (r, Δ, ζ_3)-boundary expanders by Lemma 7.

Let us remind that F_σ consists of locally consistent (wrt graph G^σ) terms of the label of branch $\sigma \in B_j^i$.

We want to show that if $\mathrm{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) > b_i$ then ρ satisfies F_σ whp.

Since $\sigma \in B_j^i$ then $\mathrm{clv}_{G^\sigma}^{\zeta_4}(F) > b_i$. We apply Lemma 27 for graph G^σ, a collection of terms F_σ, and $c \coloneqq \zeta_3$ and $\nu \coloneqq \zeta_4$ and get a sequence of terms $T \coloneqq \{t_1, \ldots, t_a\}$ from F such that:

- for any $j \leq a$, $\mathrm{vars}(t_j)$ is ζ_4-closure independent of $\bigcup_{e=1}^{j-1} \mathrm{vars}(t_e)$;
- $a \geq \frac{1}{(1+\frac{1}{\varepsilon})k} b_i > \frac{\varepsilon}{2k} b_i$.

The set J contains the set t_j with probability at least $p^{|t_j|} \geq p^k$. And since for any $j, j' \in [a]$: $t_j \cap t_{j'} = \emptyset$ we can apply Chernoff bound and say:

$$\begin{aligned}
\Pr\left[J \text{ contains less than } \frac{1}{2} \cdot \frac{\varepsilon}{2k} b_i p^k \text{ terms of } T\right] &\leq \exp\left[-\frac{1}{8} \cdot \frac{1}{2} \cdot \frac{\varepsilon}{2k} b_i p^k\right] \\
&\leq \exp\left[-\frac{1}{8} \cdot \frac{1}{2} \cdot \frac{\varepsilon}{2k} n^\delta \left(\frac{8}{p}\right)^{ik} p^k\right] \\
&\leq \exp\left[-\frac{1}{8} \cdot \frac{1}{2} \cdot \frac{\varepsilon 8^k}{2k} n^\delta \left(\frac{8}{p}\right)^{(i-1)k}\right] \\
&\leq \exp\left[-\frac{1}{8} \cdot \frac{1}{2} \cdot \frac{\varepsilon^2 8^k}{2k} \log s_i\right] \\
&\leq \left(\frac{1}{s_i}\right)^{4^k}.
\end{aligned}$$

Consider some J that contains at least $\frac{\varepsilon}{4k} b_i p^k$ terms of T. Let $T' \coloneqq \{t'_1, \ldots, t'_{a'}\}$ be a subsequence of T that consists of terms that are subsets of J. Note that for any $j \leq a'$, $\mathrm{vars}(t'_j)$ and $\bigcup_{e=1}^{j-1} \mathrm{vars}(t'_e)$ are ζ_4-closure-independent wrt G^σ. See fig. 2.

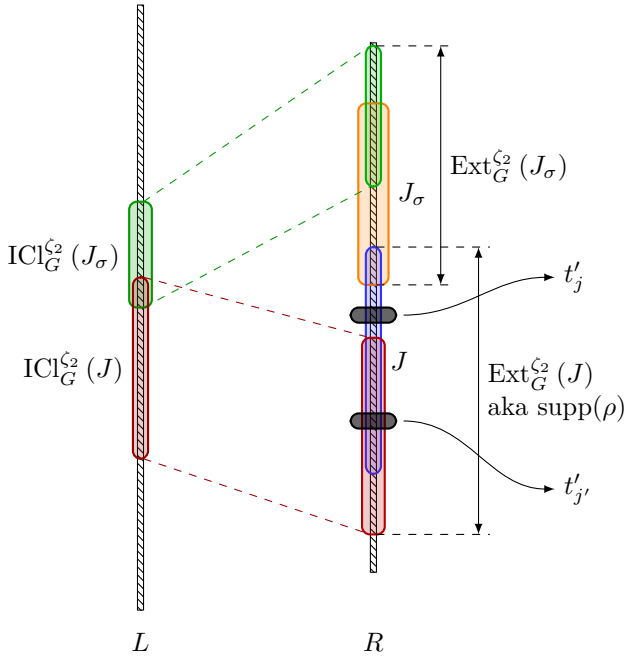

Figure 2 Graph G and sets (proportions may be incorrect).

To estimate probability that we satisfy at least one term from T' we want to use Lemma 18. In order to do that, let us make the following observation.

▶ Remark 20. A pair $(\mathrm{ICl}_G^{\zeta_2}(J), \mathrm{supp}(\rho))$ is ζ_5-reasonable wrt G^σ.

Proof. Note that $G^\sigma = (L \setminus \mathrm{ICl}_G^{\zeta_2}(J_\sigma), R \setminus \mathrm{Ext}_G^{\zeta_2}(J_\sigma), E)$. Hence if we erase the pair $(\mathrm{ICl}_G^{\zeta_2}(J), \mathrm{supp}(\rho))$ from G^σ, the resulting graph will be $G^{\sigma,\rho}$ and the statement follows from Lemma 7. ◀

Let $G^\sigma \coloneqq (L^\sigma, R^\sigma, E)$. For fixed J, assuming that ρ is consistent with σ, we may think that ρ is taken from $\mathfrak{U}_{\mathrm{Ext}_G^{\zeta_2}(J) \cap R^\sigma}$ and the Remark 20 states that it is a locally consistent assignment wrt G^σ, which gives us an access to Lemma 18. So we apply Lemma 18 with the following parameters: a graph G^σ, $J \coloneqq \mathrm{supp}(\rho) \cap R^\sigma$ and a collection T'. Here we use an assumption that $|J| < 2\varepsilon r$ and hence $|\mathrm{supp}(\rho)|$ is at most $\left(1 + \Delta \cdot \frac{1}{\varepsilon\Delta}\right) \cdot 2\varepsilon r \leq 2.1 \cdot r \leq \varepsilon \Delta r$ by Lemma 6. We conclude that probability that ρ does not satisfy any term from T' is at most:

$$\begin{aligned}
\left(1 - \frac{1}{2^k}\right)^{\frac{\varepsilon}{4k} b_{i+1} p^k} &\leq \exp\left[-\frac{\varepsilon}{4k2^k} b_{i+1} p^k\right] \\
&\leq \exp\left[-\frac{\varepsilon}{4k2^k} n^\delta \left(\frac{8}{p}\right)^{ik} p^k\right] \\
&\leq \exp\left[-\frac{\varepsilon^2 8^k}{8k2^k} \log s_i\right] \\
&\leq \left(\frac{1}{s_i}\right)^{4^k}.
\end{aligned}$$

Probability of Fail. We fail the process in two cases:

- J is too large and we cannot use our lemmas for expander graphs. That happens with probability $\exp\left[-\frac{4}{3}\varepsilon r\right]$;
- ρ does not map to 1 any term in some branch $\sigma \in B^i_j$. That happens with probability at most $\sum\limits_{i\in[k/\varepsilon]} |\bigcup\limits_{j=1}^{s} B^i_j| \cdot 2\left(\frac{1}{s_i}\right)^{4^k}$ (either J does not cover enough terms or ρ does not satisfy at least one of covered terms). To conclude the counting, note that $\left|\bigcup\limits_{j=1}^{s} B^i_j\right| \leq s_i$.

Hence whp our transformation satisfies perfectness for branches from all sets B^i_j.

5.3.4 Perfectness. Alive Branches

This is the place where we use the properties of individual closure. Let us consider some $\sigma \in \mathrm{Br}^*_{T^i_j} \setminus B^i_j$ that is marked by a DNF D and an arbitrary locally consistent term $t \in D$. Note that $\mathrm{clv}^{\zeta_2}_{G^\sigma}(D) \leq b_i$. Let C be the set of variables on which the value of $\mathrm{clv}^{\zeta_2}_{G^\sigma}(D)$ is achieved. At this iteration we split according to the variables in some set $S \supseteq C$. Consider an assignment σ' to the variables of S. Note that $|\mathrm{Ext}^{\zeta_4}_{G^\sigma}(t|_{\sigma'})| \leq |\mathrm{Ext}^{\zeta_4}_{G^\sigma}(t)| - 1$ by the definition of closure covering and Lemma 9. Again note that $|\mathrm{Ext}^{\zeta_4}_{G^{\sigma\cup\sigma'}}(t|_{\sigma'})| \leq |\mathrm{Ext}^{\zeta_4}_{G^\sigma}(t|_{\sigma'})|$ by Lemma 9. Hence for any term t' that corresponds to some branch $\sigma' \in \mathrm{Br}_{T^i_j} \setminus B^i_j$ and survives after $i+1$-th iteration we note that $|\mathrm{Ext}^{\zeta_4}_{G^{\sigma'}}(t')|$ is strictly less than $|\mathrm{Ext}^{\zeta_4}_{G^\sigma}(t)|$ where t is term in $\sigma \in \mathrm{Br}_{T^i_j}$ that generates t' after application of our transformation of the trees.

Note that for any term t'' that appears in the original proof $|\mathrm{Ext}^{\zeta_4}_{G}(t'')| \leq \left(1+\frac{1}{3\varepsilon}\right)k \leq \frac{k}{\varepsilon}$ by Lemma 6. Hence after $\frac{k}{\varepsilon}$ iterations for any locally consistent term t: $|\mathrm{Ext}^{\zeta_4}_{G^\sigma}(t)| = 0$, or in other words it is mapped to a constant and the desired statement follows.

5.3.5 Lower Bound on Height

Now we have a sequence of perfect trees $\{T^{k/\varepsilon+1}_1, T^{k/\varepsilon+1}_2, \ldots, T^{k/\varepsilon+1}_s\}$ and we want to show non-existence of such sequence. We say that a branch $\sigma \in \mathrm{Br}_{T^{k/\varepsilon+1}_j}$ has **survived** iff σ is consistent with ρ and $\sigma \cup \rho$ is locally consistent.

▶ Remark 21. In fact, one can extract a resolution proof of $A|_\rho$ of small enough width from these trees, but it requires much more technical work and accuracy. And we believe that the direct proof of the height lower bound is more useful for future generalizations.

Let $T_j \coloneqq T^{k/\varepsilon+1}_j$. Note that T_j strongly represents $D_j|_\rho$ by construction. We consider a dag of the proof π. Starting from the vertex s in this dag, we trace the path p to the initial clause. In the node $v \in p$ we maintain a partial assignment κ_v such that:

- $\kappa_v \in \mathrm{Br}^*_{T_v} \cup \mathrm{Br}^0_{T_v}$;
- κ_v have survived.

Tree T_s is a tree that consists of a single node marked by 0 and we take $\kappa_s \coloneqq \emptyset$.

Consider a node v of the dag of π. Assume that D_v is derived from $D_{i_1}, \ldots, D_{i_k}$. We have an assignment κ_v that satisfies the required properties. Our goal is to find a branch among branches of trees $T_{i_1}, \ldots, T_{i_k}$ that also satisfies the required properties. We will do it by increasing κ_v step by step. On each step we will have a closed assignment $\kappa \supseteq \kappa_v$ and a set J_κ such that:

- κ and ρ are consistent;
- $\operatorname{supp}(\kappa) = \operatorname{Ext}_G^{\zeta_2}(J_\kappa)$;
- κ satisfies $A^{\operatorname{ICl}_G^{\zeta_2}(J_\kappa)}$;
- $|\operatorname{supp}(\kappa)| = o(r)$.

Note that assignment $\kappa_v \in \operatorname{Br}_{T_v}$ is closed. Hence the set J_{κ_v} satisfies the required properties, and in the beginning κ is well-defined. Now we apply the following procedure to the assignment κ.

Algorithm 1 Branch search.

$j \coloneqq 1$
κ is the current partial assignment
while $j \le k$ **do**
  u is the root of T_{i_j}
  while u is not a leaf **do**
    x is a label of u
    if $x \in \operatorname{supp}(\kappa) \cup \operatorname{supp}(\rho)$ **then**
      Let v be a child of that correspond to $(\kappa \cup \rho)(x)$
      $u \coloneqq v$
    else
      Pick η on $\operatorname{Ext}_G^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \operatorname{Ext}_{G_\ell}^{\zeta_2}(J_\kappa)$ in a way that:
        - it satisfies $A^{\operatorname{ICl}_{G_\ell}^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \operatorname{ICl}_{G_\ell}^{\zeta_2}(J_\kappa)}$;
        - it is consistent with ρ
      $\kappa \coloneqq \kappa \cup \eta$
      $J_\kappa \coloneqq J_\kappa \cup \{x\}$
  if $u \in \operatorname{Br}^*_{T_{i_j}} \cup \operatorname{Br}^0_{T_{i_j}}$ **then return** i_j, u, κ

Note that height of the trees is at most $\frac{d_{k/\varepsilon+1}}{\varepsilon} = \frac{2}{\varepsilon} n^\delta \left(\frac{8}{p}\right)^{k^2/\varepsilon} = o(r/k)$ and hence κ has size $o(r)$ by construction and Lemma 6.

We have to show the existence of η and that we stop on some iteration. We start with the existence. Fix some iteration of the inner loop. Note that $\operatorname{supp}(\kappa) = \operatorname{Ext}_G^{\zeta_2}(J_\kappa)$ and $\operatorname{supp}(\rho) = \operatorname{Ext}_G^{\zeta_2}(J_\rho)$ which by Lemma 7 implies that $G^{\sigma,\rho}$ is an (r, Δ, ζ_5)-expander. Moreover $G^{\sigma,\rho}$ is a dependency graph of $A|_{\kappa\cup\rho}$. Hence by Lemma 11 there is a total assignment η' that satisfies $A^{\operatorname{ICl}_{G_\ell}^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \operatorname{ICl}_{G_\ell}^{\zeta_2}(J_\kappa)}|_{\kappa\cup\rho}$. Let η be a restriction of η' on $\operatorname{Ext}_G^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \operatorname{Ext}_{G_\ell}^{\zeta_2}(J_\kappa)$.

Now we want to show that we stop after some iteration. Note that:

- κ and ρ are consistent (by construction);
- κ is an extension of κ_v (by construction);
- $\kappa \cup \rho$ satisfies $A^{\operatorname{ICl}_G^{\zeta_2}(J_\kappa) \cup \operatorname{ICl}_G^{\zeta_2}(J_\rho)}$ (by construction);
- For any I of size at most r: $A^I|_{\rho\cup\kappa}$ is satisfiable (by Lemma 11).

For the sake of contradiction, assume that on each iteration of outer loop we found some leaf from $\operatorname{Br}^1_{T_{i_j}}$. Consider three cases.

- D_v is obtained by using weakening or AND-elimination rule from D_{i_1}. Assignment $\kappa \cup \rho$ maps some term of D_{i_1} to 1 and hence it is also maps some term of D_v to 1.

- D_v is obtained by using AND-introduction $\frac{F\vee\ell_1,\ldots,F\vee\ell_w}{F\vee(\bigwedge_{i=0}^{w}\ell_i)}$. If $\kappa\cup\rho$ maps some term $t\in F$ to 1, then $t\in D_v$ is also mapped to 1. If $\kappa\cup\rho$ maps all ℓ_j to 1 then $(\bigwedge_{i=0}^{w}\ell_i)\in D_v$ is also mapped to 1.
- D_v is obtained by using cut rule $\frac{F\vee(\bigwedge_{i=0}^{w}\ell_i),G\vee(\bigvee_{i=0}^{w}\neg\ell_i)}{F\vee G}$. Note that $\kappa\cup\rho$ maps some term $t\in F\vee(\bigwedge_{i=0}^{w}\ell_i)$ to 1 and some term $t'\in G\vee(\bigvee_{i=0}^{w}\neg\ell_i)$, hence $\kappa\cup\rho$ maps some term in $F\vee G=D_v$ to 1.

In all cases we conclude that $\kappa\cup\rho$ maps some term $t\in D_v$ to 1. But note that a pair $(\mathrm{ICl}_G^{\zeta_2}(J_\kappa)\cup\mathrm{ICl}_G^{\zeta_2}(J_\rho),\mathrm{Ext}_G^{\zeta_2}(J_\kappa)\cup\mathrm{Ext}_G^{\zeta_2}(J_\rho))$ is ζ_5-reasonable by Lemma 7, hence $\kappa\cup\rho$ is the witness of local satisfiability of t. That contradicts with the choice of branch κ_v, since any term of D_v is mapped by κ_v either to constant 0 or to locally inconsistent term, and $\kappa\cup\rho$ is an extension of κ_v.

Our algorithm returns some triple (i_j,u,κ). We define $\kappa_{i_j}:=u$. Note that $\kappa_{i_j}\subseteq\kappa$ hence $\kappa_{i_j}\cup\rho$ does not violate any initial clause and $\kappa_{i_j}\in\mathrm{Br}^0_{T_{i_j}}\cup\mathrm{Br}^*_{T_{i_j}}$.

By tracing the path in π we reach a tree T that strongly represents an initial clause D. We have a branch $\kappa\in\mathrm{Br}_T$ such that:

- κ and ρ are consistent;
- $\kappa\in\mathrm{Br}^*_T\cup\mathrm{Br}^0_T$, which implies that κ violates D;
- $\kappa\cup\rho$ does not violate any initial clause.

That is a contradiction.

6 Application to Random Formulas

▶ **Theorem 22.** *Let $\Delta>120$, $\eta>0$ be arbitrary constants. If $\varphi\sim\varphi(m,n,\Delta)$ where $m\le\eta n$, then there are constants $\delta,\nu>0$ such that whp any $\mathrm{Res}(k)$ proof of φ has size at least 2^{n^δ} where $k\le\nu\sqrt{\log n}$.*

Proof. Applying Theorem 28, we conclude that the dependency graph of our formula is an $(r,\Delta,0.95\Delta)$-boundary expander, where $r:=\delta n$ for some constant δ that depends only on η and Δ.

Note that:

$$n^\delta\left(\frac{n}{8\varepsilon r}\right)^{k^2/\varepsilon}=n^\delta\left(\frac{1}{8\varepsilon\delta}\right)^{\nu^2\log n/\varepsilon}\le n^\delta n^{\nu^2\log(1/8\varepsilon\delta)/\varepsilon}=o(r/k)$$

where the last inequality holds by the choice of ν. The statement follows from Theorem 17. ◀

▶ **Theorem 23.** *For any $h>0$ there is $\Delta>0$ such that if $\varphi\sim\varphi(m,n,\Delta)$ where $m\le n\log^h n$, then there are constants $\delta,\nu>0$ such that whp any $\mathrm{Res}(k)$ proof of φ has size at least 2^{n^δ} where $k\le\nu\sqrt{\frac{\log n}{\log\log n}}$.*

Proof. Applying Theorem 29 we conclude that there is $\Delta>0$ such that dependency graph of our formula is an $(r,\Delta,0.95\Delta)$-boundary expander where $r:=n/\log^\ell n$ for some constant ℓ that depends only on h and Δ.

Note that:

$$n^{\delta}\left(\frac{n}{8\varepsilon r}\right)^{k^2/\varepsilon} = n^{\delta}\left(\frac{\log^{\ell} n}{8\varepsilon}\right)^{\nu^2 \log n/\varepsilon \log\log n} \leq n^{\delta} n^{\nu^2 \ell \log(1/8\varepsilon)/\varepsilon} = o(r/k)$$

where the last inequality holds by the choice of ν. The statement follows from Theorem 17. ◀

▶ **Theorem 24.** *For any $h > 0$ there is $\Delta > 0$ such that if $\varphi \sim \varphi(m, n, \Delta)$ where $m \leq n^h$, then for any constant k there is constant $\delta > 0$ such that whp any* Res(k) *proof of φ has size at least $2^{n^{\delta}}$.*

Proof. Applying Theorem 30 we can choose any constant $\delta' > 0$ and $\Delta > 0$ that depends only on δ such that dependency graph of our formula is an $(r, \Delta, 0.95\Delta)$-boundary expander where $r \coloneqq n^{1-\delta'}$.

Note that:

$$n^{\delta}\left(\frac{n}{8\varepsilon r}\right)^{k^2/\varepsilon} = n^{\delta}\left(\frac{n^{\delta'}}{8\varepsilon}\right)^{k^2/\varepsilon} \leq n^{\delta} n^{\delta' k^2 \log(1/8\varepsilon)/\varepsilon} = o(r/k)$$

where the last inequality holds by the choice of δ'. The statement follows from Theorem 17. ◀

▶ **Theorem 25.** *For any $h > 0$ there are $\delta, \nu > 0$ such that if $\varphi \sim \varphi(m, n, \Delta)$ where $m \leq n^{\log\log^h n}$ and $\Delta \coloneqq \log n$, then whp any* Res(k) *proof of φ has size at least $2^{n^{\delta}}$ where $k \leq \nu\sqrt{\frac{\log n}{\log\log n}}$.*

Proof. Applying Theorem 31 we conclude that dependency graph of our formula is an $(r, \Delta, 0.95\Delta)$-boundary expander where $r \coloneqq n/\log^{\ell} n$ for some constant ℓ that depends only on h.

Note that:

$$n^{\delta}\left(\frac{n}{8\varepsilon r}\right)^{k^2/\varepsilon} = n^{\delta}\left(\frac{\log^{\ell} n}{8\varepsilon}\right)^{\nu^2 \log n/\varepsilon \log\log n} \leq n^{\delta} n^{\nu^2 \ell \log(1/8\varepsilon)/\varepsilon} = o(r/k)$$

where the last inequality holds by the choice of ν. The statement follows from Theorem 17. ◀

References

1 Jackson Abascal, Venkatesan Guruswami, and Pravesh K. Kothari. Strongly refuting all semi-random boolean csps. In Dániel Marx, editor, *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 454–472. SIAM, 2021. doi:10.1137/1.9781611976465.28.

2 Miklós Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994. doi:10.1007/BF01302964.

3 Michael Alekhnovich. Lower bounds for k-dnf resolution on random 3-cnfs. *Comput. Complex.*, 20(4):597–614, 2011. doi:10.1007/s00037-011-0026-0.

4 Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM J. Comput.*, 34(1):67–88, 2004. doi:10.1137/S0097539701389944.

5 Michael Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: Non-binomial case. *Proceedings of the Steklov Institute of Mathematics*, 242:18–35, 2003. Available at http://people.cs.uchicago.edu/~razborov/files/misha.pdf. Preliminary version in *FOCS '01*.

6 Sarah R. Allen, Ryan O'Donnell, and David Witmer. How to refute a random CSP. In Venkatesan Guruswami, editor, *IEEE 56th Annual Symposium on Foundations of Computer Science, FOCS 2015, Berkeley, CA, USA, 17-20 October, 2015*, pages 689–708. IEEE Computer Society, 2015. doi:10.1109/FOCS.2015.48.

7 Omar Alrabiah, Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. A near-cubic lower bound for 3-query locally decodable codes from semirandom CSP refutation. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1438–1448. ACM, 2023. doi:10.1145/3564246.3585143.

8 Albert Atserias, Ilario Bonacina, Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, and Alexander A. Razborov. Clique is hard on average for regular resolution. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 866–877. ACM, 2018. doi:10.1145/3188745.3188856.

9 Albert Atserias, Maria Luisa Bonet, and Juan Luis Esteban. Lower bounds for the weak pigeonhole principle and random formulas beyond resolution. *Inf. Comput.*, 176(2):136–152, 2002. doi:10.1006/inco.2002.3114.

10 Paul Beame, Russell Impagliazzo, Jan Krajícek, Toniann Pitassi, and Pavel Pudlák. Lower bound on hilbert's nullstellensatz and propositional proofs. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 794–806, 1994. doi:10.1109/SFCS.1994.365714.

11 Paul Beame, Richard M. Karp, Toniann Pitassi, and Michael E. Saks. The efficiency of resolution and davis–putnam procedures. *SIAM J. Comput.*, 31(4):1048–1075, 2002. doi:10.1137/S0097539700369156.

12 Eli Ben-Sasson. *Expansion in proof complexity.* PhD thesis, Hebrew University of Jerusalem, Israel, 2001. URL: https://huji-primo.hosted.exlibrisgroup.com/permalink/f/13ns5ae/972HUJI_ALMA21159933340003701.

13 Eli Ben-Sasson and Russell Impagliazzo. Random cnf's are hard for the polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, pages 415–421. IEEE Computer Society, 1999. doi:10.1109/SFFCS.1999.814613.

14 Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow – resolution made simple. *J. ACM*, 48(2):149–169, 2001. doi:10.1145/375827.375835.

15 Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, October 1988. doi:10.1145/48014.48016.

16 Susanna F. de Rezende, Jakob Nordström, Kilian Risse, and Dmitry Sokolov. Exponential resolution lower bounds for weak pigeonhole principle and perfect matching formulas over sparse graphs. *CoRR*, abs/1912.00534, 2019. arXiv:1912.00534.

17 Susanna F. de Rezende, Aaron Potechin, and Kilian Risse. Clique is hard on average for unary sherali-adams. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 12–25. IEEE, 2023. doi:10.1109/FOCS57990.2023.00008.

18 Uriel Feige. Relations between average case complexity and approximation complexity. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity, Montréal, Québec, Canada, May 21-24, 2002*, page 5. IEEE Computer Society, 2002. doi:10.1109/CCC.2002.10006.

19 Uriel Feige, Jeong Han Kim, and Eran Ofek. Witnesses for non-satisfiability of dense random 3cnf formulas. In *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), 21-24 October 2006, Berkeley, California, USA, Proceedings*, pages 497–508. IEEE Computer Society, 2006. doi:10.1109/FOCS.2006.78.

20 Noah Fleming, Denis Pankratov, Toniann Pitassi, and Robert Robere. Random Θ(log n)-cnfs are hard for cutting planes. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 109–120. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.19.

21 Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. Optimal sherali-adams gaps from pairwise independence. In Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 125–139, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. doi:10.1007/978-3-642-03685-9_10.

22 Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1):613–622, 2001. doi:10.1016/S0304-3975(00)00157-2.

23 Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. Algorithms and certificates for boolean CSP refutation: smoothed is no harder than random. In Stefano Leonardi and Anupam Gupta, editors, *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 678–689. ACM, 2022. doi:10.1145/3519935.3519955.

24 Johan Håstad. On small-depth frege proofs for tseitin for grids. *J. ACM*, 68(1):1:1–1:31, 2021. doi:10.1145/3425606.

25 Pavel Hrubes and Pavel Pudlák. Random formulas, monotone circuits, and interpolation. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 121–131. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.20.

26 Pravesh K. Kothari and Peter Manohar. An exponential lower bound for linear 3-query locally correctable codes. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 776–787. ACM, 2024. doi:10.1145/3618260.3649640.

27 Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 132–145. ACM, 2017. doi:10.1145/3055399.3055485.

28 Jan Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170:123–140, January 2001. doi:10.4064/fm170-1-8.

29 Sebastian Müller and Iddo Tzameret. Short propositional refutations for dense random 3cnf formulas. *Ann. Pure Appl. Log.*, 165(12):1864–1918, 2014. doi:10.1016/j.apal.2014.08.001.

30 Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. doi:10.1017/CBO9781139814782.

31 Shuo Pang. Large clique is hard on average for resolution. In Rahul Santhanam and Daniil Musatov, editors, *Computer Science - Theory and Applications - 16th International Computer Science Symposium in Russia, CSR 2021, Sochi, Russia, June 28 - July 2, 2021, Proceedings*, volume 12730 of *Lecture Notes in Computer Science*, pages 361–380. Springer, 2021. doi:10.1007/978-3-030-79416-3_22.

32 Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random csps below the spectral threshold. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 121–131. ACM, 2017. doi:10.1145/3055399.3055417.

33 Alexander A. Razborov. Pseudorandom generators hard for k-dnf resolution and polynomial calculus resolution. *Ann. of Math.*, 181:415–472, 2015. doi:10.4007/annals.2015.181.2.1.

34 Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 593–602. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.74.

35 Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. A switching lemma for small restrictions and lower bounds for k-dnf resolution. *SIAM J. Comput.*, 33(5):1171–1200, 2004. doi:10.1137/S0097539703428555.

36 Dmitry Sokolov. (semi)algebraic proofs over ±1 variables. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 78–90. ACM, 2020. doi:10.1145/3357713.3384288.

37 Dmitry Sokolov. Random (log n)-cnf are hard for cutting planes (again). In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 2008–2015. ACM, 2024. doi:10.1145/3618260.3649636.

38 Salil P. Vadhan. *Pseudorandomness*. Now Publishers Inc., Hanover, MA, USA, 2012.

A Chernoff Bound

▶ **Lemma 26** (Chernoff bound). *Let $X_1, \ldots, X_n$ be independent random variables taking values in $\{0,1\}$, $X \coloneqq \sum X_i$ and $\mu \coloneqq \mathbb{E}[X]$.*

- $\Pr[X \leq (1-\delta)\mu] \leq \exp\left[-\frac{\delta^2}{2}\mu\right]$;
- $\Pr[X \geq (1+\delta)\mu] \leq \exp\left[-\frac{\delta^2}{2+\delta}\mu\right]$.

B Graph Properties

▶ **Lemma 27.** *Let $G \coloneqq (L, R, E)$ be an (r, Δ, c)-boundary expander, $\mathcal{S} \coloneqq \{S_1, S_2, \ldots, S_\ell\}$ be a collection of subsets of R such that $|S_i| \leq k$. Then for each $\nu < c$ it is possible to pick a sequence $\{B_1, \ldots, B_h\}$ where:*

- *for all $i \in [h]$ there is $j \in [\ell]$ such that $B_i = S_j$;*
- *B_i is ν-closure-independent of $\bigcup_{j=1}^{i-1} B_j$;*
- $h \geq \min\left(r/k, \frac{\mathrm{clv}(\mathcal{S})}{(1+\frac{\Delta}{c-\nu})k}\right)$.

Proof. Let us start picking B's in a greedy way. Suppose we picked i terms for some $0 < i < r/k$, and we are not able to pick the term $i+1$. This means that the set of vertices $\mathrm{Ext}^\nu\left(\bigcup_{j<i} B_j\right)$ is a closure covering for $\mathcal{S}$.

$$\begin{aligned}\mathrm{clv}\,(\mathcal{S}) &\leq |\mathrm{Ext}^\nu\left(\bigcup_{j<i} B_j\right)| \\ &\leq \left(1+\frac{\Delta}{c-\nu}\right)|\bigcup_{j<i} B_j| \\ &\leq \left(1+\frac{\Delta}{c-\nu}\right) ik,\end{aligned}$$

hence $i \geq \frac{\mathrm{clv}(\mathcal{S})}{(1+\frac{\Delta}{c-\nu})k}$. ◀

C Random Graph is an Expander

For $m, n, \Delta \in \mathbb{N}$, we denote by $\mathfrak{G}(m, n, \Delta)$ the distribution over bipartite graphs with disjoint vertex sets $U \coloneqq \{u_1, \ldots, u_m\}$ and $V \coloneqq \{v_1, \ldots, v_n\}$ where the neighbourhood of a vertex $u \in U$ is chosen by sampling a subset of size Δ uniformly at random from V.

Let G be a randomly sampled graph from $\mathfrak{G}(m,n,\Delta)$ and $\varepsilon < 1/2$. We estimate the probability that G is not an $(r,\Delta,(1-\varepsilon)\Delta)$-boundary expander for some parameter r.

Let $G \coloneqq (U,V,E)$. We first estimate the probability that a set $S \subseteq U$ of size at most r violates the boundary expansion. For brevity, let us write $s = |S|$ and $c = (1-\frac{\varepsilon}{2})\Delta$. The probability that S violates the boundary expansion can be bounded by:

$$\begin{aligned}\Pr[|\partial(S)| < (1-\varepsilon)\Delta s] &\le \Pr[|\mathrm{N}(S) < cs] \\ &\le \binom{n}{cs} \cdot \left(\frac{\binom{cs}{\Delta}}{\binom{n}{\Delta}}\right)^s \\ &\le \binom{n}{cs} \cdot \left(\frac{cs}{n}\right)^{\Delta s} \\ &\le \left[\left(\frac{en}{cs}\right)^c \cdot \left(\frac{cs}{n}\right)^{\Delta}\right]^s\end{aligned}$$

Hence, the probability that G is not a boundary expander can be bounded by

$$\begin{aligned}\Pr[G \text{ is not an expander}] &\le \sum_{s\in[r]} \binom{m}{s} \left[\left(\frac{en}{cs}\right)^c \cdot \left(\frac{cs}{n}\right)^{\Delta}\right]^s \\ &\le \sum_{s\in[r]} \left(\frac{me}{s}\right)^s \left[\left(\frac{en}{cs}\right)^c \cdot \left(\frac{cs}{n}\right)^{\Delta}\right]^s \\ &\le \sum_{s\in[r]} \left[\frac{me}{s}\left(\frac{en}{cs}\right)^c \cdot \left(\frac{cs}{n}\right)^{\Delta}\right]^s \\ &\le \sum_{s\in[r]} \left[e^{1+c}\frac{m}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s\end{aligned}$$

Now we can formulate some classical results about the existence of expander graphs.

▶ **Theorem 28.** *Let $\frac{1}{2} > \varepsilon > 0$, $\Delta > 6/\varepsilon$ be arbitrary constants. If $m \le \eta n$, there is a constant $\delta > 0$ such that whp for $r \coloneqq \delta n$ a randomly sampled graph $G \sim \mathfrak{G}(m,n,\Delta)$ is an $(r,\Delta,(1-\varepsilon)\Delta)$-boundary expander.*

Proof. Let $c \coloneqq (1-\frac{\varepsilon}{2})\Delta$ and $\delta' \coloneqq \frac{\Delta r}{n}$. Note that G is not a boundary expander with probability at most:

$$\begin{aligned}\sum_{s\in[r]} \left[e^{1+c}\frac{m}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s &\le \sum_{s\in[r]} \left[e^{1+c}\frac{\eta n}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s \\ &= \sum_{s\in[r]} \left[e^{1+c}\eta c\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta-1}\right]^s \\ &\le \sum_{s\in[r]} \left[e^{1+c}\eta c\,(\delta')^{\frac{\varepsilon}{2}\Delta-1}\right]^s.\end{aligned}$$

And if $\Delta > 6/\varepsilon$ we can choose δ to make sure that this sum is at most 0.01. ◀

▶ **Theorem 29.** *Let $m \le n\log^h n$ for some universal constant h and $\varepsilon \coloneqq 0.01$. For any constant $\ell > 0$ there is a constant $\Delta > 0$ such that whp for $r \coloneqq n/\log^\ell n$ a randomly sampled graph $G \sim \mathfrak{G}(m,n,\Delta)$ is an $(r,\Delta,(1-\varepsilon)\Delta)$-boundary expander.*

Proof. Let $c \coloneqq (1-\frac{\varepsilon}{2})\Delta$. Note that G is not a boundary expander with probability at most:

$$\sum_{s\in[r]}\left[e^{1+c}\frac{m}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s = \sum_{s\in[r]}\left[e^{1+c}\frac{mc}{n}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta-1}\right]^s.$$
$$\leq \sum_{s\in[r]}\left[e^{1+c}c\log^h n\left(\Delta\log^{-\ell} n\right)^{\frac{\varepsilon}{2}\Delta-1}\right]^s.$$

And if $\Delta > \frac{6(h+\ell)}{\varepsilon\ell}$ this sum is $o(1)$. ◀

▶ **Theorem 30.** *Let $m \leq n^h$ for some universal constant h and $\varepsilon \coloneqq 0.01$. For any constant $\delta > 0$ there is a constant $\Delta > 0$ such that whp for $r \coloneqq n^{1-\delta}$ a randomly sampled graph $G \sim \mathfrak{G}(m,n,\Delta)$ is an $(r,\Delta,(1-\varepsilon)\Delta)$-boundary expander.*

Proof. Let $c = (1-\frac{\varepsilon}{2})\Delta$. Note that G is not a boundary expander with probability at most:

$$\sum_{s\in[r]}\left[e^{1+c}\frac{m}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s \leq \sum_{s\in[r]}\left[e^{1+c}n^h\left(n^{-\delta/2}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s.$$

And if $\Delta > \frac{6h}{\varepsilon\delta}$ this sum is $o(1)$. ◀

▶ **Theorem 31.** *Let $m \leq n^{\log\log^h n}$ for some universal constant h, $\varepsilon \coloneqq 0.01$. For any constant $\delta > 0$ there is a constant $\ell > 0$ such that whp for $r \coloneqq n/\log^\ell n$ a randomly sampled graph $G \sim \mathfrak{G}(m,n,\Delta)$ is an $(r,\Delta,(1-\varepsilon)\Delta)$-boundary expander where $\Delta \coloneqq \log n$.*

Proof. Let $c = (1-\frac{\varepsilon}{2})\Delta$. Note that G is not a boundary expander with probability at most:

$$\sum_{s\in[r]}\left[e^{1+c}\frac{m}{s}\left(\frac{cs}{n}\right)^{\frac{\varepsilon}{2}\Delta}\right]^s \leq \sum_{s\in[r]}\left[e^{1+c}n^{\log\log^h n}\left(\log^{-\ell/2} n\right)^{\frac{\varepsilon}{2}\Delta}\right]^s.$$

And if $\ell > \frac{6h}{\varepsilon}$ this sum is $o(1)$. ◀

D Proof of Lemma 11

▶ **Lemma 32.** *Let A be a linear system based on a graph $G \coloneqq (L,R,E)$ that is an (r,Δ,c)-expander. If σ is a locally consistent assignment, then for any I of size at most r the system $A^I|_\sigma$ is satisfiable.*

Proof. Let a pair (S,T) be a witness of the consistency of σ. So (S,T) is a ζ-reasonable pair for some $\zeta > 0$. Let σ' be an extension of σ on $T \cup \mathrm{N}(S)$ such that $A^S|_{\sigma'}$ is satisfied (it exists since $A^S|_\sigma$ is satisfiable).

Pick an arbitrary set I of size at most r. Note that σ' satisfies all constraints from $I \cap S$. Let $I' \coloneqq I \setminus S$. Consider a graph G' obtained by removing a pair $(S, T \cup \mathrm{N}(S))$, that is (r,Δ,ζ)-boundary expander. By Lemma 4 (applied to G') there is an enumeration $I' = \{v_1, v_2, \ldots, v_{|I'|}\}$ and a partition $\bigsqcup_i R_i = \mathrm{N}_{G'}(I')$ such that:

- $R_i = \mathrm{N}(v_i) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}(v_j)\right)$;
- $|\partial(v_i) \cap R_i| \geq \zeta$.

For each $i \in [|I'|]$ we extend σ' on R_i by choosing an arbitrary assignment that satisfies constraint $A^{v_i}|_{\sigma'}$. Since $|\partial(v_i) \cap R_i| > 0$ there is at least one such assignment and we are done. ◀