



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

Anastasia Sofronova Dmitry Sokolov St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences  St. Petersburg State University 

April 21, 2022

Abstract

Random Δ -CNF formulas are one of the few candidates that are expected to be hard to refute in any proof system. One of the frontiers in the direction of proving lower bounds on these formulas is the k -DNF Resolution proof system (aka $\text{Res}(k)$). Assume we sample m clauses over n variables. There are two known lower bounds.

- Segerlind, Buss, Impagliazzo [SBI04] showed an exponential lower bound for any constant k , $\Delta = \mathcal{O}(k^2)$ in case $m = \mathcal{O}(n^{7/6})$.
- Alekhnovich [Ale11] showed lower bound for $k = \mathcal{O}\left(\sqrt{\frac{\log n}{\log \log n}}\right)$, any $\Delta \geq 3$ in case $m = \mathcal{O}(n)$.

Both of these papers used the same technique: the so-called *small restriction switching lemma*. However, they used different properties of the dependency graph of the random formula. In this paper we present a new technique with the same flavour though based on a different complexity measure that we call *closure covering*. We use only the expansion of the dependency graph of the formula. This technique allows us to unify and improve both of these bounds simultaneously. In particular, as a corollary we show:

- an exponential lower bound for any constant k , $\Delta = \mathcal{O}(1)$ in case $m = \text{poly}(n)$;
- an exponential lower bound for $k = \mathcal{O}(\sqrt{\log n})$, $\Delta = \mathcal{O}(1)$ in case $m = \mathcal{O}(n)$.

It is the first lower bound that works for clause density $\frac{m}{n} > n^{1/6}$ (density can even be superpolynomial for random $\log n$ -CNF).

1 Introduction

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. It is known that for each Δ there is a density threshold c_Δ such that if $\frac{m}{n} > c_\Delta$ then whp formula is unsatisfiable and if $\frac{m}{n} < c_\Delta$ then whp formula is satisfiable. A common belief is that solving the satisfiability problem for random Δ -CNF formulas near the density threshold is hard. Some formal conjectures were formulated by Feige [Fei02]: no polynomial time algorithm may *prove* whp the unsatisfiability of a random $\mathcal{O}(1)$ -CNF formula with arbitrary large constant clause density. Assuming Feige's conjecture it is known that some problems are hard to approximate: vertex covering, DNF PAC learning, etc.

Random Δ -CNF formulas are actively studied from the proof complexity point of view. It is one of the few candidate for hard examples for all proof system. It is also one the most promising candidates. 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 [Ale+04; Raz15] or Clique formulas [Ats+18; Pan21]. We mention known results for random formulas in Section 1.1.

In this paper we focus on lower bounds for the $\text{Res}(k)$ proof system that was introduced by Krajíček [Kra01]. This is a subsystem of AC_0 -Frege (even a subsystem of depth-2 Frege) that is a current frontier for proving lower bounds on the random CNF formulas in subsystems of Frege proof system (any lower bound for Frege systems is a long-standing open problem in proof complexity).

In addition to the motivation that we presented, lower bounds on random Δ -CNF formulas on the subsystems of AC_0 -Frege system are interesting from the technical points of view. Most results that we have for AC_0 -Frege system are obtained by using variations of Switching Lemma (for example [UF96], [Hås21]), but it seems that for random CNF formulas it is not applicable and any potential lower bound will need a new general technique.

1.1 Prior Results

Proof system	Polynomial upper bound	Lower bound 2^{n^ϵ}
Resolution	$m > \frac{n^{\Delta-1}}{\log^{\Delta-2} n}$ [Bea+02]	$m \leq n^{(\Delta+2)/4}$ [Bea+02]
Polynomial Calculus		$m = \mathcal{O}(n), \Delta \geq 3$ [BI99] $m = \text{poly}(n), \Delta = 3$ [AR03]
Sum-of-Squares		$m = \text{poly}(n), \Delta = \mathcal{O}(1)$ [Gri01], [Sch08]
Cutting Planes		$m = \text{poly}(n), \Delta = \Omega(\log n)$ [HP17], [Fle+17]
TC_0 -Frege	$\Delta = 3, m > n^{1.4}$ [FKO06], [MT14]	\times
$\text{Res}(k)$		$m = \mathcal{O}(n), \Delta \geq 3, k = 2$ [ABE02] $m = \mathcal{O}(n), \Delta \geq 3, k = \mathcal{O}\left(\sqrt{\frac{\log n}{\log \log n}}\right)$ [Ale11] $m = n^{7/6}, \Delta = \mathcal{O}(k^2), k = \mathcal{O}(1)$ [SBI04]

In fact, all lower bounds that are mentioned in the table (except $\text{Res}(k)$ and the best result for Resolution) are based only on the fact that dependency graph is a good enough expander (for different proof systems lower bounds require different expansion parameter). Hence we can change parameters as long as the random graph satisfies the required expansion.

1.2 Our Results

We suggest a technique for proving lower bounds on CNF formulas with the only requirement that the dependency graph is a good enough expander. More formally, we show the following Theorem in Section 5.

Theorem 1.1

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 $\text{Res}(k)$ proof of φ has size at least 2^{n^δ} .

In Section 6 we show the following corollaries:

- an exponential lower bound for any constant k , $\Delta = \mathcal{O}(1)$ in case $m = \text{poly}(n)$ (improvement of the result of Segerlind, Buss, Impagliazzo [SBI04]);
- an exponential lower bound for $k = \mathcal{O}(\sqrt{\log n})$, $\Delta = \mathcal{O}(1)$ in case $m = \mathcal{O}(n)$ (improvement of the result of Alekhovich [Ale11]).

We would like to emphasize that this result is the first that provides a lower bound on the $\text{Res}(k)$ proofs for the constant Δ independent on k and polynomially large clause density $\frac{m}{n}$. As the table in Section 1.1 illustrates, there are non-trivial upper bounds in strong proof systems that depend on density, so the authors find it crucial to explore how does the proof complexity of random formulas behave with density increasing.

As a weakness of our results, we would 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 [Ale11]).

The new measure “closure covering” that we use in our paper, along with the properties of our “closure”, has an independent interest. We keep all useful properties from earlier definitions of closure in expander graphs while equipping our definition with the new ones, such as uniqueness and that, in some sense, it is preserved after taking a subgraph.

As mentioned above, earlier lower bounds on random CNFs in $\text{Res}(k)$ are based on the technique of Small Restriction Switching Lemma [SBI04], [Raz15], which is a very general and powerful tool, used mostly in a manner of a black box. Due to switching to the new measure, our technique does not fit into the framework of Small Restriction Switching Lemma. It is also worth noting that all current lower bounds in $\text{Res}(k)$ are obtained by reduction to Resolution in one way or another. We work in somehow different manner. While we still argue about decision trees of DNFs, we do not extract the Resolution proof from this argument, dealing with the dag of $\text{Res}(k)$ proof instead (though this can be rephrased in terms of Resolution proofs). By working directly with $\text{Res}(k)$ 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 the method to argue about hardness in $\text{Res}(k)$ 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** $C := x_1^{c_1} \vee x_2^{c_2} \dots \vee x_k^{c_k}$ is a disjunction of literals where $c_1, c_2, \dots, c_k \in \{0, 1\}$. A **CNF formula** $\varphi := C_1 \wedge \dots \wedge C_m$ is a conjunction of clauses. A **term** is a conjunction of literals. A **DNF formula** $\varphi := t_1 \vee \dots \vee t_m$ is a disjunction of terms.

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

We say that two partial assignments ρ, ρ' are **consistent** iff for any $x \in \text{supp}(\rho) \cap \text{supp}(\rho')$ the following holds $\rho(x) = \rho'(x)$. In addition, if $\text{supp}(\rho') \subseteq \text{supp}(\rho)$ then we use a notation $\rho' \subseteq \rho$.

k -DNF Resolution. In this paper we focus on classical generalization of the Resolution proof system, so-called k -DNF Resolution aka $\text{Res}(k)$ [Kra95].

A proof system $\text{Res}(k)$ operates with k -DNFs. A $\text{Res}(k)$ -**proof** π of an unsatisfiable CNF formula φ is an ordered sequence of k -DNFs $\pi := C_1, \dots, C_s$ such that $C_s = \emptyset$ is an empty formula. Each C_i either comes from the original formula φ or is inferred using one of the rules:

$$\begin{aligned} \text{Weakening: } & \frac{F}{F \vee \ell}; \\ \text{AND-introduction: } & \frac{F \vee \ell_1, \dots, F \vee \ell_w}{F \vee (\bigwedge_{i=0}^w \ell_i)}; \\ \text{AND-elimination: } & \frac{F \vee (\bigwedge_{i=0}^w \ell_i)}{F \vee \ell_i}; \\ \text{Cut: } & \frac{F \vee (\bigwedge_{i=0}^w \ell_i), G \vee (\bigvee_{i=0}^w \neg \ell_i)}{F \vee G}. \end{aligned}$$

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: $N_G(S)$ 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 . We omit the index G if the graph is evident from the context.

A bipartite graph $G := (L, R, E)$ 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 $|N(S)| \geq c \cdot |S|$. Similarly, $G := (L, R, E)$ 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

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

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 [GMT09].

Lemma 3.1

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 $S = \{s_1, s_2, \dots, s_{|S|}\}$ and a partition $\bigsqcup_i R_i = N(S)$ such that:

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

Proof. Since $|S| \leq r$ it holds that $|\partial(S)| \geq c|S|$ and there is a vertex $s_{|S|} \in S$ such that $|\partial(s_{|S|})| \geq c$. Let $R_{|S|} := \partial(s_{|S|})$, and repeat the process for $S \setminus \{s_{|S|}\}$. \square

Since papers [AR03; Ale+04] a “closure” operation is widely used in proof complexity. In this paper we start with definition from [AR03] and show some additional properties of it. To emphasize the difference, we call it **individual closure**.

Let $G := (L, R, E)$ 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 $|\mathbf{N}(v) \cap J| \geq \Delta - \nu$. Let $\text{ICl}_G^\nu(J) \subseteq L$ be the smallest set of vertices that are ν -captured by $\mathbf{N}(\text{ICl}_G^\nu(J)) \cup J$. We also can define the set $\text{ICl}_G^\nu(J)$ inductively: $\text{ICl}_G^\nu(J)$ may be considered as a maximal sequence of distinct vertices $\{v_1, v_2, v_3, \dots, v_i, \dots\}$ such that v_i is ν -captured by $J \cup \bigcup_{j=1}^{i-1} \mathbf{N}(v_j)$. We denote by $\text{Ext}_G^\nu(J) := J \cup \mathbf{N}(\text{ICl}_G^\nu(J))$ the **extension** of J .

Remark 3.2

$\text{ICl}_G^\nu(J)$ is unique and well-defined.

Proof. Fix some set J . Let $V := \{v_1, v_2, v_3, \dots, v_i, \dots\}$ and $U := \{u_1, u_2, u_3, \dots, u_i, \dots\}$ 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 $|\mathbf{N}(u_j) \cap (J \cup \bigcup_{k=1}^{j-1} \mathbf{N}(u_k))| \geq \Delta - \nu$ and by the choice of u_j : $|\mathbf{N}(u_j) \cap (J \cup \bigcup_{v \in V} \mathbf{N}(v))| \geq \Delta - \nu$. Hence we can extend V by u_j , which contradicts with the maximality. \square

Lemma 3.3

Suppose that G is an (r, Δ, c) -boundary expander and that $J \subseteq R$ has size $|J| \leq (c - \nu)r$. Then $|\text{ICl}_G^\nu(J)| < \frac{|J|}{c - \nu}$.

Proof. Let $V := \{v_1, v_2, v_3, \dots, v_\ell\}$ be the sequence of vertices from L that generates $\text{ICl}_G^\nu(J)$. If $\ell > r$ then $S \subseteq \{v_1, v_2, \dots, v_r\}$ otherwise $S := V$.

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

$$\begin{aligned} |\partial(S) \setminus J| &\leq \\ 2 \sum_{i=1}^{|S|} |\mathbf{N}(v_i) \setminus (\mathbf{N}(\bigcup_{j=1}^{i-1} v_j) \cup J)| &\leq \\ \sum_{i=1}^{|S|} \nu &\leq \\ \nu |S|. & \end{aligned}$$

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

Suppose $J \subseteq R$ is not too large. Then Lemma 3.3 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 3.4

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

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

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

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

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

□

We also need a technical definition for a graph $G := (L, R, E)$ 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 $(L \setminus S, R \setminus (T \cup \mathbb{N}(S)), E)$ is an (r, Δ, ζ) -boundary expander.

Remark 3.5

A partial case of Lemma 3.4 may be reformulated as follows.

Let $G := (L, R, E)$ be an (r, Δ, c) -boundary expander and $J \subseteq R$. Then a pair $(\text{ICl}^{\nu}(J), \text{Ext}^{\nu}(J))$ 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 (for example [Rez+19; Sok20]) it works in completely opposite way.

Lemma 3.6

Let $G := (L, R, E)$ be a bipartite graph and $G' := (L', R', E)$ be a subgraph of G . For any set $J \subseteq R$ and any ν the following holds.

1. If $G' := (L', R', E)$ is a subgraph of G then $\text{ICl}_{G'}^{\nu}(J \cap R') \subseteq \text{ICl}_G^{\nu}(J)$.
2. If $J' \subseteq J$ then $\text{ICl}_G^{\nu}(J') \subseteq \text{ICl}_G^{\nu}(J)$.

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

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

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

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

For a collection of sets $\mathcal{T} := \{T_1, \dots, T_\ell\}$ we say that a **closure covering number** (denoted as $\text{clv}^\nu(\mathcal{T})$) is the least number of vertices from R to cover a collection of sets $\{\text{Ext}^\nu(T_i)\}_{i \in [\ell]}$.

4 Random CNF Formulas and Linear Systems

Let φ be a formula on X variables. With this formula, we associate a bipartite dependency graph $G^\varphi := (L, R, E)$ where L corresponds to the set of clauses of φ (and we identify these two sets), R correspond 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.

Definition 4.1

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

Lemma 4.2 ([CS88])

For any $\Delta \geq 3$ whp $\varphi \sim \varphi(m, n, \Delta)$ is unsatisfiable if $m \geq \ln 2 \cdot 2^\Delta n$.

In the section C we present some classical computations that show that randomly sampled graph is a good enough expander (see also [Vad12]).

Let φ be a CNF formula on n variables with m clauses. We define a system of linear equation A_φ . Let $C := x_1^{a_1} \vee \dots \vee x_w^{a_w}$ be a clause from φ . We add to A_φ an equation $x_1 + \dots + x_w = a_1 + \dots + a_w$. 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 A_φ implies a lower bound on φ .

Let A be a linear system over boolean variables from the set X . Let A^I denote a subsystem of A on equations obtained from the subset of equations I . For a partial assignment ρ by $A|_\rho$ we denote a system over variables $X \setminus \text{supp}(\rho)$ 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 4.3

Let $G^A := (L, R, E)$ 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 $r \in \ell$ 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 $G := (L, R, E)$ 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:

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

The next Lemma is an analog of similar statement from [Ale11]. But since we change the definition of a locally consistent assignment we provide a proof in the Appendix D.

Lemma 4.4

Let A be a linear system based on a graph $G := (L, R, E)$ 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 4.5

Let A be a linear system based on a graph $G := (L, R, E)$ that is an (r, Δ, c) -expander, $J \subseteq R$ and σ be an assignment on J .

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

Proof. Note that if $|J| \leq (c - \nu)r$, then by Lemma 3.3 $|\text{ICl}^\nu(J)| \leq r$ and the first statement follows from Lemma 4.4.

For the second statement note that a pair $(\text{ICl}^\nu(J), \text{Ext}^\nu(J))$ is $c - (\Delta - \nu)$ -reasonable by Lemma 3.4. The statement follows from definition of local consistency. \square

Lemma 4.6 (Alekhovich [Ale11])

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 4.7

Let A be a linear system, $G^A := (L, R, E)$ be an (r, Δ, c) -expander and $T \subseteq R$. We define a uniform distribution over all locally consistent partial assignments on T as \mathfrak{U}_T^G .

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 $\mathfrak{U}_{\text{Ext}^\nu(J)}^G$.

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 4.8

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 at most $(c - \nu)r$. 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. Fix an arbitrary locally consistent assignment η on S . The condition $\eta \subseteq \rho$ is a linear system, since it can be rewritten in the following way: $\rho(x) = \eta(x)$ for all $x \in \text{supp}(\eta)$. Since η is locally consistent and by Lemma 3.3 $|\text{ICl}^\nu(J)| \leq r$ then by Lemma 4.5 the system $A^{\text{ICl}^\nu(J)}|_\eta$ is satisfiable. Hence the number of extensions of η to the $\text{supp}(\rho)$ is independent on the values that we assign in η and under the condition $\eta \subseteq \rho$ the assignment ρ is generated as an assignment that satisfies linear system $A^{\text{ICl}^\nu(J)}|_\eta$ uniformly at random.

Again the condition $\kappa \subseteq \rho$ is a linear system hence:

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

where sol is the number of solutions. We have already shown 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 $A^{\text{ICl}^\nu(J)}|_{\eta \cup \kappa}$ is satisfiable and hence number of solutions depends only on sizes of η and κ .

By Lemma 3.1 there is an enumeration $H := \{v_1, \dots, v_{|H|}\}$ and sequence R_i such that:

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

By Lemma 3.3 $|\text{ICl}^\nu(S)| \leq r$, hence by Lemma 4.4 system $A^{\text{ICl}^\nu(S)}|_\eta$ is satisfiable, hence there is an assignment η' on $\text{Ext}^\nu(S)$ that is an extension of η and satisfies $A^{\text{ICl}^\nu(S)}|_{\eta'}$. By Remark 3.5 (by Lemma 3.4) $(\text{ICl}^\nu(S), \text{Ext}^\nu(S))$ 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 $\text{Ext}^\nu(T)$. By induction on $i \in [|\text{ICl}^\nu(J)|]$ we create an assignment β_i such that:

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

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

1. $v_i \in \text{ICl}^\nu(S)$. In this case η' assigns all variables in $R \subseteq N(v_i)$ 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 $\bigcup_{j=1}^i \beta_j$ assigns all variables in $N(v_i)$ wrt to η' and hence it satisfies A^{v_i} since η' satisfies it.
2. $v_i \in \text{ICl}^\nu(T)$. Similar to the previous case (we should consider κ' instead of η').
3. $v_i \notin (\text{ICl}^\nu(S) \cup \text{ICl}^\nu(T))$. By definition of individual closure η' can assign at most $\Delta - \nu$ variables in $N(v_i)$, the same holds for κ' . Hence η' and κ' together assign at most $2(\Delta - \nu)$ variables, which is strictly less than $c \leq |R_i|$ and there is a variable in 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 $\bigcup_{i \in [|\text{ICl}^\nu(J)|]} \beta_i$ satisfies $A^{\text{ICl}^\nu(J)}|_{\kappa \cup \eta}$ by construction. Hence $\Pr_{\rho \sim \mathcal{U}_J} [\kappa \subseteq \rho \mid \eta \subseteq \rho]$ is independent of the choice of η and the statement holds. \square

Corollary 4.9

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 at most $(c - \nu)r$. 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:

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

Proof. Follows from Lemma 4.8 and observation that $\Pr_{\rho \sim \mathcal{U}_J} [\kappa \subseteq \rho]$ can be obtained from $\Pr_{\rho \sim \mathcal{U}_J} [\kappa \subseteq \rho \mid \sigma' \subseteq \rho]$ by averaging over all proper σ' . \square

5 Lower Bound

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

Theorem 5.1 (Reformulation of Theorem 1.1)

Let A be the linear system such that G^A is a $(r, \Delta, (1 - \varepsilon)\Delta)$ -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 $\text{Res}(k)$ proof of A has size at least 2^{n^δ} .

The plan of the proof of the Theorem 5.1 now is as follows.

- We start with the “Restriction Lemma” that transforms the notion of closure independent terms into the language of probabilities. It is our crucial technical tool.
- For the sake of contradiction we assume that we have a short proof.

- In the first step we transform a given short proof into a sequence of “DNF trees” (which is a mix of decision trees and DNF formulas).
- In the second step we modify the trees. We want to transform them into a sequence of ordinary decision tree (since we know that such a sequence may be transformed into a small resolution proof), but we reach much less ambitious goal and create a sequence of “perfect DNF trees” of small height (here we hit our formula and sequence of trees by random restriction).
- In the last step we give a direct proof of the lower bound on the height of perfect DNF trees.

We deal with linear system 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.

Lemma 5.2

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 at most $(c - \nu)r$. If $T := \{t_1, \dots, t_\ell\}$ is a sequence of locally consistent terms such that:

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

then:

$$\Pr_{\rho \sim \mathcal{U}_J} [\forall i \in [\ell]: t_i |_{\rho} \neq 1] \leq \left(1 - \frac{1}{2^k}\right)^{|T|}.$$

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

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

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

The base of induction follows from Lemma 4.6 since t_1 is locally consistent (and by Lemma 4.4 the probability that it is mapped to 1 by ρ is not zero): $\Pr[t_1 |_{\rho} = 0] \leq (1 - \frac{1}{2^k})$. 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 aim to satisfy t_i with its closure simultaneously, so let us impose even stronger conditions than simply satisfying t_i . We can pick some locally consistent assignment σ such that:

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

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

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

$$\begin{aligned}
& \Pr_{\rho \sim \mathfrak{U}_J} [S_i] \leq \\
& \Pr_{\rho \sim \mathfrak{U}_J} [S_{i-1}] \cdot \Pr_{\rho \sim \mathfrak{U}_J} [t_i |_{\rho} = 0 | S_{i-1}] \leq \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \Pr_{\rho \sim \mathfrak{U}_J} [t_i |_{\rho} = 0 | S_{i-1}] \leq && \text{by induction hyp.} \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho \sim \mathfrak{U}_J} [t_i |_{\rho} = 1 | S_{i-1}]\right) \leq && \rho \text{ assigns all variables in } t_i \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho | S_{i-1}]\right) \leq \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \mathbb{E}_{\kappa \sim \mathfrak{U}_{i-1}} \left[\Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho | \kappa \subseteq \rho] \right]\right) \leq \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \mathbb{E}_{\kappa \sim \mathfrak{U}_{i-1}} \left[\Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho] \right]\right) \leq && \text{by Corollary 4.9} \\
& \left(1 - \frac{1}{2^k}\right)^{i-1} \left(1 - \Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho]\right).
\end{aligned}$$

We can use Corollary 4.9 since $\bigcup_i t_i \subseteq J$ 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 $\Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho] \geq \frac{1}{2^k}$. Note that ρ is consistent with σ iff ρ maps t_i to 1. Hence by Lemma 4.6 $\Pr_{\rho \sim \mathfrak{U}_J} [\sigma \subseteq \rho] = \Pr_{\rho \sim \mathfrak{U}_J} [t_i |_{\rho} = 1] \geq \frac{1}{2^{|t_i|}} \geq \frac{1}{2^k}$. \square

5.2 Tree and DNF

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

Definition 5.3

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 decision tree T , we denote the set of paths (partial assignments) that lead from the root to a leaf labelled by $a \in \{0, 1\}$ as Br_T^a . We denote the set of paths (partial assignments) that lead from the root to a leaf labelled by non-trivial formula by Br_T^* . We say that a decision tree T **strongly represents** a DNF formula D if for every $\pi \in \text{Br}_T^0$ and for all $t \in D$, $t|_{\pi} = 0$ and for every $\pi \in \text{Br}_T^1$, 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 $x \notin \text{supp}(\rho)$ then $T|_\rho$ is a tree with a root marked by x and two children $T_0|_\rho$ and $T_1|_\rho$;
 - if $x \in \text{supp}(\rho)$ then $T|_\rho := T_{\rho(x)}|_\rho$.

5.3 Proof of Theorem 5.1

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 $\pi := \{D_1, D_2, \dots, D_s\}$ be a $\text{Res}(k)$ 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 $\text{supp}(\sigma) = \text{Ext}_G^\nu(J_\sigma)$. For a collection of ν -closed partial assignments $\sigma_1, \sigma_2, \dots, \sigma_\ell$ we define a graph $G^{\sigma_1, \sigma_2, \dots, \sigma_\ell} := (L \setminus \bigcup_{i=1}^\ell \text{ICl}_G^\nu(J_{\sigma_i}), R \setminus \bigcup_{i=1}^\ell \text{Ext}_G^\nu(J_{\sigma_i}), E)$.

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 .

We think of π as about the sequence of closed DNF-trees $\{T_1^1, T_2^1, \dots, T_s^1\}$ 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 $\{T_1^{i+1}, T_2^{i+1}, \dots, T_s^{i+1}\}$. We also divide branches into three groups:

- $B_j^{i+1} \subseteq \text{Br}_{T_j^{i+1}}^*$ is a collection of **broken** branches that we create during our process;
- $\sigma \in T_j^{i+1}$ 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 $\sigma \in T_j^i$ is marked by $D_j|_\sigma$ (it can be a constant if it is allowed by the definition of strong representation).

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 $\text{Ext}_G^{\zeta_2}(J)$ 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 $(\text{ICl}_G^{\zeta_2}(J_\sigma) \cup \text{ICl}_G^{\zeta_2}(J), \text{Ext}_G^{\zeta_2}(J_\sigma) \cup \text{Ext}_G^{\zeta_2}(J))$).

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 $\text{Res}(k)$ to Perfect DNF-trees

Let us fix some parameters:

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

Now we describe a construction of $\{T_1^{i+1}, T_2^{i+1}, \dots, T_s^{i+1}\}$ from $\{T_1^i, T_2^i, \dots, T_s^i\}$. Suppose that before i -th iteration we have a sequence $\{T_1^i, T_2^i, \dots, T_s^i\}$ of consistent DNF-trees that satisfy ρ -consistency property. Let $T := T_j^i$. Consider a branch $\sigma \in T$. If $\sigma \in \text{Br}_T^*$ 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 $a \leq i$ or dead. We do not modify σ .
- Branch σ is marked by a constant. We do not modify σ .
- $\text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) \leq b_i$. We add a full binary tree that splits over all variables from

$$\text{Ext}_G^{\zeta_2}(J_\sigma \cup \text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma)) \setminus \text{Ext}_G^{\zeta_2}(J_\sigma)$$

(see fig. 1). We mark new leaves by proper DNF formulas and a set $J_\sigma \cup \text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma)$. Note that $|J_\sigma \cup \text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma)| \leq 2n^\delta \left(\frac{8}{p}\right)^{(i-1)k} + n^\delta \left(\frac{8}{p}\right)^{ik} \leq 2n^\delta \left(\frac{8}{p}\right)^{ik} = d_{i+1}$. The height of these branches is $|\text{Ext}_G^{\zeta_2}(J_\sigma \cup \text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma))|$ which is at most $\frac{d_{i+1}}{\varepsilon}$ by Lemma 3.3.

- $\text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) > b_i$. We put σ into B_j^{i+1} .

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

5.3.3 Perfectness. Broken Branches

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

Note that by Chernoff bound:

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

So we assume that $|J| \leq 2pn$.

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

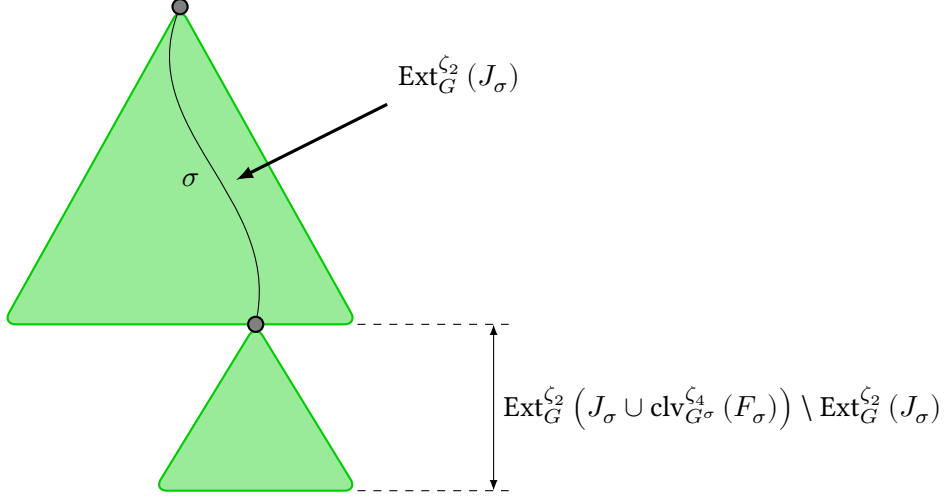


Figure 1: Modification of a branch

- G^σ is a dependency graph of $A|_\sigma$;
- G^σ is the (r, Δ, ζ_3) -boundary expanders by Lemma 3.4.

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 $\text{clv}_{G^\sigma}^{\zeta_4}(F_\sigma) > b_i$ then ρ satisfies F_σ whp.

Since $\sigma \in B_j^i$ then $\text{clv}_{G^\sigma}^{\zeta_4}(F) > b_i$. We apply Lemma B.1 for graph G^σ , a collection of terms F_σ , and $c := \zeta_3$ and $\nu := \zeta_4$ and get a sequence of terms $T := \{t_1, \dots, t_a\}$ from F such that:

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

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 $T' := \{t'_1, \dots, t'_{a'}\}$ be a subsequence of T that consists of terms that are subsets of J . Note that t'_j and $\bigcup_{e=1}^{j-1} t'_e$ are ζ_4 -closure-independent wrt G^σ . See fig. 2.

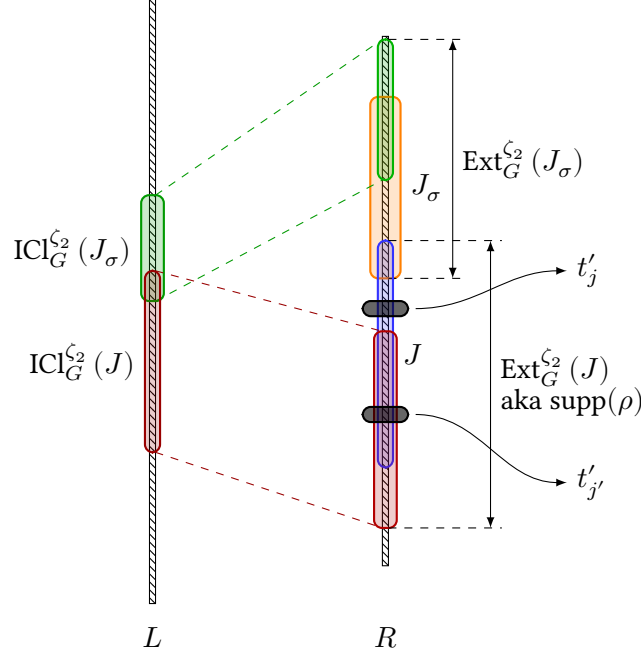


Figure 2: Graph G and sets (proportions may be incorrect)

To estimate probability that we satisfy at least one term from T' we want to use Lemma 5.2. In order to do that, let us make the following observation.

Remark 5.4

A pair $(\text{ICI}_G^{\zeta_2}(J), \text{supp}(\rho))$ is ζ_5 -reasonable wrt G^σ .

Proof. Note that $G^\sigma = (L \setminus \text{ICI}_G^{\zeta_2}(J_\sigma), R \setminus \text{Ext}_G^{\zeta_2}(J_\sigma), E)$. Hence if we erase the pair $(\text{ICI}_G^{\zeta_2}(J), \text{supp}(\rho))$ from G^σ , the resulting graph will be $G^{\sigma, \rho}$ and the statement follows from Lemma 3.4. \square

Let $G^\sigma := (L^\sigma, R^\sigma, E)$. For fixed J , assuming that ρ is consistent with σ , we may think that ρ is taken from $\mathfrak{U}_{\text{Ext}_G^{\zeta_2}(J) \cap R^\sigma}$ and the Remark 5.4 states that it is locally consistent assignment wrt G^σ , which gives us an access to Lemma 5.2. So we apply Lemma 5.2 with the following parameters: a graph G^σ , $J := \text{supp}(\rho) \cap R^\sigma$ and a collection T' . Here we use an assumption that $|J| \leq 2\varepsilon r$ and hence $|\text{supp}(\rho)|$ is at most $(1 + \frac{1}{\varepsilon \Delta}) \cdot 2\varepsilon r \leq \varepsilon \Delta r$ by Lemma 3.3. 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 $\sigma \in B_j^i$. That happens with probability at most $\sum_{i \in [k/\varepsilon]} \left| \bigcup_{j=1}^s B_j^i \right| \cdot 2 \left(\frac{1}{s_i}\right)^{4^k}$ (either J does not cover enough terms or ρ does not satisfy at least one of covered terms). To conclude the counting, note that $\left| \bigcup_{j=1}^s B_j^i \right| \leq s_i$.

Hence whp our transformation satisfies perfectness for branches from all sets B_j^i .

5.3.4 Perfectness. Alive Branches

This is the place where we use the properties of individual closure. Let us consider some $\sigma \in \text{Br}_{T_j^i}^* \setminus B_j^i$ that is marked by a DNF D and an arbitrary locally consistent term $t \in D$. Note that $\text{clv}_{G^\sigma}^{\zeta_2}(D) \leq b_i$, and we split according to the variables in the set $S \supseteq \text{clv}_{G^\sigma}^{\zeta_2}(D)$. Consider an assignment σ' to the variables of S . Note that $|\text{Ext}_{G^\sigma}^{\zeta_4}(t|_{\sigma'})| \leq |\text{Ext}_{G^\sigma}^{\zeta_4}(t)| - 1$ by the definition of closure covering and Lemma 3.6. Again note that $|\text{Ext}_{G^{\sigma \cup \sigma'}}^{\zeta_4}(t|_{\sigma'})| \leq |\text{Ext}_{G^\sigma}^{\zeta_4}(t|_{\sigma'})|$ by Lemma 3.6. Hence for any term t' that corresponds to some branch $\sigma' \in T_j^i \setminus B_j^i$ and survives after $i+1$ -th iteration we note that $|\text{Ext}_{G^{\sigma'}}^{\zeta_4}(t')|$ is strictly less than $|\text{Ext}_{G^\sigma}^{\zeta_4}(t)|$ where t is term in $\sigma \in T_j^i$ that generates t' after application of our transformation of the trees.

Note that for any term t'' that appears in the original proof $|\text{Ext}_G^{\zeta_4}(t'')| \leq (1 + \frac{1}{3\varepsilon})k \leq \frac{k}{\varepsilon}$ by Lemma 3.3. Hence after $\frac{k}{\varepsilon}$ iterations for any locally consistent term t : $|\text{Ext}_{G^\sigma}^{\zeta_4}(t)| = 0$, 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 $\{T_1^{k/\varepsilon+1}, T_2^{k/\varepsilon+1}, \dots, T_s^{k/\varepsilon+1}\}$ and we want to show non-existence of such sequence. We say that a branch $\sigma \in T_j^{k/\varepsilon+1}$ have **survived** iff σ is consistent with ρ and $\sigma \cup \rho$ is locally consistent.

Remark 5.5

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 $T_j := T_j^{k/\varepsilon+1}$. 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:

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

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

Consider a node v of the dag of π . Assume that D_v is derived from D_{i_1}, \dots, 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}, \dots, 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;
- $\text{supp}(\kappa) = \text{Ext}_G^{\zeta_2}(J_\kappa)$;
- κ satisfies $A^{\text{ICl}_G^{\zeta_2}(J_\kappa)}$;
- $|\text{supp}(\kappa)| = o(r)$.

Note that assignment $\kappa_v \in T_v$ 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

```

1:  $j := 1$ 
2:  $\kappa$  is the current partial assignment
3: while  $j \leq k$  do
4:    $u$  is the root of  $T_{i_j}$ 
5:   while  $u$  is not a leaf do
6:      $x$  is a label of  $u$ 
7:     if  $x \in \text{supp}(\kappa) \cup \text{supp}(\rho)$  then
8:       Let  $v$  be a child of that correspond to  $(\kappa \cup \rho)(x)$ 
9:        $u := v$ 
10:    else
11:      Pick  $\eta$  on  $\text{Ext}_G^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \text{Ext}_G^{\zeta_2}(J_\kappa)$  in a way that:
          • it satisfies  $A^{\text{ICl}_{G_\ell}^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \text{ICl}_{G_\ell}^{\zeta_2}(J_\kappa)}$ ;
          • it is consistent with  $\rho$ 
12:       $\kappa := \kappa \cup \eta$ 
13:       $J_\kappa := J_\kappa \cup \{x\}$ 
14:    if  $u \in \text{Br}_{T_{i_j}}^* \cup \text{Br}_{T_{i_j}}^0$  then return  $i_j, u, \kappa$ 

```

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 3.3.

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 $\text{supp}(\kappa) = \text{Ext}_G^{\zeta_2}(J_\kappa)$ and $\text{supp}(\rho) = \text{Ext}_G^{\zeta_2}(J_\rho)$ which by Lemma 3.4 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 4.4 there is a total assignment η' that satisfies $A^{\text{ICI}_G^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \text{ICI}_G^{\zeta_2}(J_\kappa)}|_{\kappa \cup \rho}$. Let η be a restriction of η' on $\text{Ext}_G^{\zeta_2}(J_\kappa \cup \{x\}) \setminus \text{Ext}_G^{\zeta_2}(J_\kappa)$.

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 $A^{\text{ICI}_G^{\zeta_2}(J_\kappa) \cup \text{ICI}_G^{\zeta_2}(J_\rho)}$ (by construction);
- For any I of size at most r : $A^I|_{\rho \cup \kappa}$ is satisfiable (by Lemma 4.4).

For the sake of contradiction, assume that on each iteration of outer loop we found some leaf from $\text{Br}_{T_{i_j}}^1$. 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 $\frac{F \vee \ell_1, \dots, F \vee \ell_w}{F \vee (\bigwedge_{i=0}^w \ell_i)}$. 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 $\frac{F \vee (\bigwedge_{i=0}^w \ell_i), G \vee (\bigvee_{i=0}^w -\ell_i)}{F \vee G}$. Note that $\kappa \cup \rho$ maps some term $t \in F \vee (\bigwedge_{i=0}^w \ell_i)$ to 1 and some term $t' \in G \vee (\bigvee_{i=0}^w -\ell_i)$, 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 $(\text{ICI}_G^{\zeta_2}(J_\kappa) \cup \text{ICI}_G^{\zeta_2}(J_\rho), \text{Ext}_G^{\zeta_2}(J_\kappa) \cup \text{Ext}_G^{\zeta_2}(J_\rho))$ is ζ_5 -reasonable by Lemma 3.4, 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 $\kappa_{i_j} \in \text{Br}_{T_{i_j}}^0 \cup \text{Br}_{T_{i_j}}^*$.

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

- κ and ρ are consistent;
- $\kappa \in \text{Br}_T^* \cup \text{Br}_T^0$, 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 6.1

For any $\eta > 0$ there is $\Delta > 0$ such that if $\varphi \sim \varphi(m, n, \Delta)$ where $m \leq \eta n$, then there are constants $\delta, \nu > 0$ such that whp any $\text{Res}(k)$ proof of φ has size at least 2^{n^δ} where $k \leq \nu \sqrt{\log n}$.

Proof. Applying Theorem C.1 we conclude that there is $\Delta > 0$ such that dependency graph of our formula is an $(r, \Delta, 0.95\Delta)$ -boundary expander where $r := \delta n$ for some constant δ that depends only on η and Δ .

Note that:

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

where the last inequality holds by the choice of ν . The statement follows from Theorem 5.1. \square

Theorem 6.2

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

Proof. Applying Theorem C.2 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 5.1. \square

Theorem 6.3

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 $\text{Res}(k)$ proof of φ has size at least 2^{n^δ} .

Proof. Applying Theorem C.3 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 $r := n^{1-\delta'}$.

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 5.1. \square

Theorem 6.4

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 $\Delta := \log n$, then whp any $\text{Res}(k)$ proof of φ has size at least 2^{n^δ} where $k \leq \nu \sqrt{\frac{\log n}{\log \log n}}$.

Proof. Applying Theorem C.4 we conclude 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 .

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 5.1. \square

Acknowledgements

The authors would like to thank Edward Hirsch for comments on the draft. Research is partially supported by Huawei (grant TC20211214628).

References

- [ABE02] Albert Atserias, Maria Luisa Bonet, and Juan Luis Esteban. “Lower Bounds for the Weak Pigeonhole Principle and Random Formulas beyond Resolution.” In: *Inf. Comput.* 176.2 (2002), pp. 136–152. DOI: 10.1006/inco.2002.3114. URL: <https://doi.org/10.1006/inco.2002.3114>.
- [Ale+04] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. “Pseudorandom Generators in Propositional Proof Complexity.” In: *SIAM J. Comput.* 34.1 (2004), pp. 67–88. DOI: 10.1137/S0097539701389944. URL: <https://doi.org/10.1137/S0097539701389944>.
- [Ale11] Michael Alekhnovich. “Lower Bounds for k-DNF Resolution on Random 3-CNFs.” In: *Comput. Complex.* 20.4 (2011), pp. 597–614. DOI: 10.1007/s00037-011-0026-0. URL: <https://doi.org/10.1007/s00037-011-0026-0>.
- [AR03] Michael Alekhnovich and Alexander A. Razborov. “Lower Bounds for Polynomial Calculus: Non-Binomial Case.” In: *Proceedings of the Steklov Institute of Mathematics* 242 (2003). Available at <http://people.cs.uchicago.edu/~razborov/files/misha.pdf>. Preliminary version in *FOCS '01.*, pp. 18–35.
- [Ats+18] 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: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*. Ed. by Ilias Diakonikolas, David Kempe, and Monika Henzinger. ACM, 2018, pp. 866–877. DOI: 10.1145/3188745.3188856. URL: <https://doi.org/10.1145/3188745.3188856>.
- [Bea+02] Paul Beame, Richard M. Karp, Toniann Pitassi, and Michael E. Saks. “The Efficiency of Resolution and Davis–Putnam Procedures.” In: *SIAM J. Comput.* 31.4 (2002), pp. 1048–1075. DOI: 10.1137/S0097539700369156. URL: <https://doi.org/10.1137/S0097539700369156>.

- [BI99] 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*. IEEE Computer Society, 1999, pp. 415–421. DOI: 10.1109/SFFCS.1999.814613. URL: <https://doi.org/10.1109/SFFCS.1999.814613>.
- [CS88] Vašek Chvátal and Endre Szemerédi. “Many Hard Examples for Resolution.” In: *J. ACM* 35.4 (Oct. 1988), pp. 759–768. ISSN: 0004-5411. DOI: 10.1145/48014.48016. URL: <http://doi.acm.org/10.1145/48014.48016>.
- [Fei02] 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*. IEEE Computer Society, 2002, p. 5. DOI: 10.1109/CCC.2002.10006. URL: <http://doi.ieeecomputersociety.org/10.1109/CCC.2002.10006>.
- [FKO06] 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*. IEEE Computer Society, 2006, pp. 497–508. DOI: 10.1109/FOCS.2006.78. URL: <https://doi.org/10.1109/FOCS.2006.78>.
- [Fle+17] Noah Fleming, Denis Pankratov, Toniann Pitassi, and Robert Robere. “Random $\Theta(\log n)$ -CNFs Are Hard for Cutting Planes.” In: *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*. Ed. by Chris Umans. IEEE Computer Society, 2017, pp. 109–120. DOI: 10.1109/FOCS.2017.19. URL: <https://doi.org/10.1109/FOCS.2017.19>.
- [GMT09] Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. “Optimal Sherali-Adams Gaps from Pairwise Independence.” In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Ed. by Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 125–139. ISBN: 978-3-642-03685-9.
- [Gri01] Dima Grigoriev. “Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity.” In: *Theoretical Computer Science* 259.1 (2001), pp. 613–622. ISSN: 0304-3975. DOI: [https://doi.org/10.1016/S0304-3975\(00\)00157-2](https://doi.org/10.1016/S0304-3975(00)00157-2). URL: <http://www.sciencedirect.com/science/article/pii/S0304397500001572>.
- [Hås21] Johan Håstad. “On Small-depth Frege Proofs for Tseitin for Grids.” In: *J. ACM* 68.1 (2021), 1:1–1:31. DOI: 10.1145/3425606. URL: <https://doi.org/10.1145/3425606>.
- [HP17] Pavel Hrubes and Pavel Pudlák. “Random Formulas, Monotone Circuits, and Interpolation.” In: *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*. Ed. by Chris Umans. IEEE Computer Society, 2017, pp. 121–131. DOI: 10.1109/FOCS.2017.20. URL: <https://doi.org/10.1109/FOCS.2017.20>.
- [Kra01] Jan Krajíček. “On the weak pigeonhole principle.” In: *Fundamenta Mathematicae* 170 (Jan. 2001), pp. 123–140. DOI: 10.4064/fm170-1-8.
- [Kra95] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*. Vol. 60. Encyclopedia of mathematics and its applications. Cambridge University Press, 1995. ISBN: 978-0-521-45205-2.
- [MT14] Sebastian Müller and Iddo Zameret. “Short propositional refutations for dense random 3CNF formulas.” In: *Ann. Pure Appl. Log.* 165.12 (2014), pp. 1864–1918. DOI: 10.1016/j.apal.2014.08.001. URL: <https://doi.org/10.1016/j.apal.2014.08.001>.

- [Pan21] Shuo Pang. “Large Clique is Hard on Average for Resolution.” In: *Computer Science - Theory and Applications - 16th International Computer Science Symposium in Russia, CSR 2021, Sochi, Russia, June 28 - July 2, 2021, Proceedings*. Ed. by Rahul Santhanam and Daniil Musatov. Vol. 12730. Lecture Notes in Computer Science. Springer, 2021, pp. 361–380. DOI: 10.1007/978-3-030-79416-3_22. URL: https://doi.org/10.1007/978-3-030-79416-3%5C_22.
- [Raz15] Alexander A. Razborov. “Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution.” In: *Ann. of Math.* 181 (2 2015), pp. 415–472. DOI: <https://doi.org/10.4007/annals.2015.181.2.1>.
- [Rez+19] 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.” In: *CoRR* abs/1912.00534 (2019). arXiv: 1912.00534. URL: <http://arxiv.org/abs/1912.00534>.
- [SBI04] Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. “A Switching Lemma for Small Restrictions and Lower Bounds for k-DNF Resolution.” In: *SIAM J. Comput.* 33.5 (2004), pp. 1171–1200. DOI: 10.1137/S0097539703428555. URL: <https://doi.org/10.1137/S0097539703428555>.
- [Sch08] 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*. IEEE Computer Society, 2008, pp. 593–602. DOI: 10.1109/FOCS.2008.74. URL: <https://doi.org/10.1109/FOCS.2008.74>.
- [Sok20] Dmitry Sokolov. “(Semi)Algebraic proofs over ± 1 variables.” In: *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*. Ed. by Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy. ACM, 2020, pp. 78–90. DOI: 10.1145/3357713.3384288. URL: <https://doi.org/10.1145/3357713.3384288>.
- [UF96] Alasdair Urquhart and Xudong Fu. “Simplified Lower Bounds for Propositional Proofs.” In: *Notre Dame J. Formal Log.* 37.4 (1996), pp. 523–544. DOI: 10.1305/ndjfl/1040046140. URL: <https://doi.org/10.1305/ndjfl/1040046140>.
- [Vad12] Salil P. Vadhan. *Pseudorandomness*. Hanover, MA, USA: Now Publishers Inc., 2012. ISBN: 1601985940, 9781601985941.

A Chernoff Bound

Lemma A.1 (Chernoff bound)

Let X_1, \dots, X_n be independent random variables taking values in $\{0, 1\}$, $X := \sum X_i$ and $\mu := \mathbb{E}[X]$.

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

B Graph Properties

Lemma B.1

Let $G := (L, R, E)$ be an (r, Δ, c) -boundary expander, $\mathcal{S} := \{S_1, S_2, \dots, S_\ell\}$ 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 $\{B_1, \dots, B_h\}$ where:

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

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

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

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

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 $U := \{u_1, \dots, u_m\}$ and $V := \{v_1, \dots, v_n\}$ where the neighbourhood of a vertex $u \in U$ is chosen by sampling a subset of size Δ uniformly at random from V .

Let us make some standard computations. Let G be a randomly sampled graph from $\mathfrak{G}(m, n, \Delta)$. Fix $\varepsilon := 0.01$ and try to estimate the probability that G is not an $(r, \Delta, (1 - \varepsilon)\Delta)$ -boundary expander for some parameter r .

Let $G := (U, V, E)$. 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:

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

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

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

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

Theorem C.1

Let $m \leq \eta n$ for some universal constant η and $\varepsilon := 0.01$. There are constants $\Delta, \delta > 0$ such that whp for $r := \delta n$ a randomly sampled graph $G \sim \mathfrak{G}(m, n, \Delta)$ is an $(r, \Delta, (1 - \varepsilon)\Delta)$ -boundary expander.

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

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

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

Theorem C.2

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

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

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

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

Theorem C.3

Let $m \leq n^h$ for some universal constant h and $\varepsilon := 0.01$. For any constant $\delta > 0$ there is a constant $\Delta > 0$ such that whp for $r := n^{1-\delta}$ 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:

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

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

Theorem C.4

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

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

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

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

D Proof of Lemma 4.4

Lemma D.1

Let A be a linear system based on a graph $G := (L, R, E)$ 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 $T \cup N(S)$ 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 $I' := I \setminus S$. Consider a graph G' obtained by removing a pair $(S, T \cup N(S))$, that is (r, Δ, ζ) -boundary expander. By Lemma 3.1 (applied to G') there is an enumeration $I' = \{v_1, v_2, \dots, v_{|I'}\}$ and a partition $\bigsqcup_i R_i = N_{G'}(I')$ such that:

- $R_i = N(v_i) \setminus \left(\bigcup_{j=1}^{i-1} N(v_j) \right)$;

- $|R_i| \geq \zeta$.

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