Random 3-XOR Formulas are Hard for Resolution over k-DNFs

—an exposition—

Ilario Bonacina*

December 4, 2017

Abstract

Let F be a random 3-XOR formula in n variables and Δn linear constraints. Then, asymptotically almost surely, every k-DNF resolution refutation of F requires length at least $\exp(n/\Delta^{O(k^2)})$. This result was proved in [Alekhnovich 2011]. In this note we give an exposition and a generalization of it to 3-XOR formulas whose adjacency graphs are *expanders*.

Contents

1 Introduction

First we introduce k-DNF resolution and the 3-XOR formulas we consider. This note in meant to be as self-contained as possible, with the exception of the (quite standard) results recalled in this introduction.

1.1 Resolution over k-DNF Formulas

A *k-DNF formula* is a propositional formula over the logic connectives $\{\vee, \wedge, \neg\}$ which is a disjunction ($\vee$) of conjunctions ($\wedge$) of at most k literals (that is Boolean variables or negated ($\neg$) Boolean variables). A *clause* is a disjunction of literals. A *term* is a conjunction of literals.

*Universitat Politècnica de Catalunya, Dept. Ciències de la Computació, Jordi Girona Salgado 31, Omega-223 08034 Barcelona, Catalonia, Spain, bonacina@cs.upc.edu

⚠ This is **a draft** that has not been peer reviewed yet: comments or bug-reports are more than welcome.

A Boolean variable x and its negation $\neg x$ are sometimes respectively denoted as x^1 and x^0. The XOR logic operator is denoted with $\oplus$. Given a set of propositional formulas A (over $\{\vee, \wedge, \oplus, \neg\}$), $\mathrm{vars}(A)$ is the set of Boolean variables mentioned in A. Given two terms t and t', t' is a *subterm* of t, $t' \subseteq t$, if the set of literals of t' is a subset of the set of literals of t.

The propositional proof system *k-DNF resolution*, introduced in [Kra01], is a generalization of the well-studied propositional proof system *resolution* [Bla37, Rob65]. A *k-DNF resolution refutation* of an unsatisfiable set of clauses F is a sequence of k-DNF formulas $(G_1, \ldots, G_m)$ where $G_m = \bot$, the empty trivially false clause, and each G_i is either a clause from F or it is obtained applying one of the following inference rules to G_j and $G_{j'}$ with $j, j' < i$:

$$\frac{C \vee \bigwedge_{i \in I} \ell_i, \quad C \vee \ell}{C \vee (\ell \wedge \bigwedge_{i \in I} \ell_i)} \quad |I| < k\,, \qquad \frac{C \vee \bigwedge_{i \in I} \ell_i}{C \vee \ell_i} \quad i \in I\,, \tag{1a}$$

$$\frac{C \vee \bigwedge_{i \in I} \ell_i \qquad D \vee \bigvee_{i \in I} \neg \ell_i}{C \vee D} \quad |I| \leqslant k\,, \tag{1b}$$

where C, D are k-DNF formulas and ℓ, ℓ_i are literals. The *length* of a refutation $(G_1, \ldots, G_m)$ is m. The minimum length of a k-DNF resolution refutation of F is $\mathrm{S}_k(F \vdash \bot)$. (If F is satisfiable $\mathrm{S}_k(F \vdash \bot) = \infty$.) It is well known that k-DNF resolution is sound and complete, in the sense that it can refute any unsatisfiable set of clauses and no satisfiable set of clauses has a refutation.

Resolution is just another name for 1-DNF resolution and in resolution there is another well-studied and important complexity measure: the *width*. Given a resolution refutation $\pi = (C_1, \ldots, C_m)$, the *width* of π is the maximum number of literals in any of the C_i in π.

1.2 The 3-XOR Formulas and Expansion

A 3-*XOR formula* F in n Boolean variables $x_1, \ldots, x_n$ and m linear constraints is a formula of the form

$$F = L_1 \wedge \cdots \wedge L_m\,, \tag{2}$$

where each L_i is either the XOR ($\oplus$, the sum mod 2) of at most 3 Boolean variables, or the negation of a XOR of at most 3 Boolean variables. We say that $F = L_1 \wedge \cdots \wedge L_m$ is an *exact* 3-XOR formula if each L_i has exactly 3 variables in it.

The satisfiability of 3-XOR formulas can be decided in polynomial time: those formulas are a system of linear equations over $\mathbb{F}_2$, hence Gaussian elimination can be used to check wether the system is satisfiable or not. Still, if F is unsatisfiable, proving its unsatisfiability in weak proof systems might be hard.

Notice that, a 3-XOR formula F is not a set of clauses but it can trivially be written as an equi-satisfiable set of clauses as follows. To each L_i we associate a set of clauses S_i and then to F we associate the set of clauses $\bigcup_{i \in [m]} S_i$, where the sets S_i are defined as follows. If $L_i = x_{i_1} \oplus x_{i_2} \oplus x_{i_3}$ let

$$S_i = \{x_{i_1}^{\epsilon_1} \vee x_{i_2}^{\epsilon_2} \vee x_{i_3}^{\epsilon_3} \mid \epsilon_1 + \epsilon_2 + \epsilon_3 \equiv 1 \pmod 2\}\,, \tag{3}$$

otherwise if $L_i = \neg(x_{i_1} \oplus x_{i_2} \oplus x_{i_3})$, let

$$S_i = \{x_{i_1}^{\epsilon_1} \vee x_{i_2}^{\epsilon_2} \vee x_{i_3}^{\epsilon_3} \mid \epsilon_1 + \epsilon_2 + \epsilon_3 \equiv 0 \pmod 2\}\,. \tag{4}$$

It is clear from the definition of $\oplus$ that F and $\bigcup_{i \in [m]} S_i$ are equisatisfiable. Indeed, we talk about k-DNF resolution refutations of F but with this we actually mean refutations of $\bigcup_{i \in [m]} S_i$.

We only consider a specific class of 3-XOR formulas, those that are good *expanders*. The notion of expansion in proof complexity has proven to be very important for lower bound proofs, see for instance [BS01, BSW01]. It is relevant also for us, so let define precisely it in this context.

Given a 3-XOR formula $F = L_1 \wedge \cdots \wedge L_m$ we provide $\{L_1, \ldots, L_m\} \cup \mathrm{vars}(F)$ with the graph structure given by the set of edges $\{\{L_i, x\} \mid x \in \mathrm{vars}(L_i)\}$. Call this graph the *adjacency graph of* F and denote it with $\mathcal{G}_F$. Then we use a function, the *unique neighbors* $\partial_F(\cdot)$, from subsets of $\{L_1, \ldots, L_m\}$ to $\mathrm{vars}(F)$. This function is defined as follows: for each $A \subseteq \{L_1, \ldots, L_m\}$

$$\partial_F(A) = \{x \in \mathrm{vars}(F) \mid \exists! L \in A, x \in \mathrm{vars}(L)\}\,. \tag{5}$$

Definition 1.1 ((r,c)-∂-expander)**.** We say that a 3-XOR formula $F = L_1 \wedge \cdots \wedge L_m$ is an *(r,c)-∂-expander* if for every $A \subseteq \{L_1, \ldots, L_m\}$ such that $|A| \leqslant r$, then $|\partial_F(A)| \geqslant c|A|$.

This is the usual notion of unique neighbors expanders in the adjacency graph $\mathcal{G}_F$. We omit to mention the graph $\mathcal{G}_F$ unless where it is strictly needed. We now recall some—quite standard—facts about 3-XOR formulas from the literature.

Fact 1.2 (folklore[1])**.** *Let $F = L_1 \wedge \cdots \wedge L_m$ be a 3-XOR formula that is an (r,c)-∂-expander with $c > 0$ and let $A \subseteq \{L_1, \ldots, L_m\}$ be such that $|A| \leqslant r$. Then A is satisfiable.* ∎

Fact 1.3 ([BSW01, ∼Theorem 4.15][2])**.** *If F be an unsatisfiable 3-XOR formula that is an (r,c)-∂-expander, then every resolution refutation of F require width at least $rc/2$.* ∎

Do 3-XOR formulas that are expanders actually exist? Yes, for instance a (randomized) construction are the *random* 3-XOR formulas.

A *random 3-XOR formula* in n variables and m linear constraints is a 3-XOR formula $F = L_1 \wedge \cdots \wedge L_m$ where the L_i are chosen according to the following process: For each $i \in [m]$ independently and uniformly at random choose a set $S_i = \{i_1, i_2, i_3\} \subseteq [n]$ of size at most 3 and a bit $b_i \in \{0,1\}$ and, if $b_i = 1$ set $L_i = x_{i_1} \oplus x_{i_2} \oplus x_{i_3}$ otherwise set $L_i = \neg(x_{i_1} \oplus x_{i_2} \oplus x_{i_3})$. As before, if all the S_i have size exactly 3 we say that F is an *exact* random 3-XOR formula. It is known that random 3-XOR formulas are good expanders.

Fact 1.4 ([BKPS02, ∼Lemma 5.5][3])**.** *Let F be an exact random 3-XOR in n variables and Δn linear equations, and let $0 < c < 1$ be a real. Then, asymptotically almost surely, F is an (r,c)-∂-expander with $r = Cn\Delta^{-2/(1-c)}$ and C a constant only depending on c.* ∎

Regarding the satisfiability of exact random 3-XOR formulas, asymptotically almost surely, for any $m > \theta n$, an exact random 3-XOR formula F in n variables and m linear constraints is unsatisfiable [DM02] (and for $m < \theta n$ it is satisfiable asymptotically almost surely) where $\theta \sim 0.917935\ldots$.[4]

Moreover, for $m > \theta n$, asymptotically almost surely, there is an algorithm that produces a resolution refutation of F in time $2^{O(n^2/m)} n^{O(1)}$[BKPS02, Theorem 6.3]. Hence if $m = \Omega(n^2/\log n)$ then there exists a resolution (and hence a k-DNF resolution) refutation of F of polynomial size.

Regarding the lower bounds, [BS01] proved that, asymptotically almost surely, an exact random 3-XOR formula in n variables and m linear equations ($m > \theta n$) needs resolution refutations of size $2^{\Omega(n^2/m)}$. (The same lower bound is also true in polynomial calculus over

[1] (*Proof sketch*) The assumption in Fact 1.2 implies the existence of a matching from A to the variables of $\partial_F(A)$, in the adjacency graph of F. Then set all the other variables not in the matching arbitrarily and use the variables in the matching to satisfy A.

[2] Theorem 4.15 in [BSW01] is stated for a different family of formulas, the *Graph Pigeonhole Principle*, but that proof can be trivially adapted to 3-XOR formulas.

[3] Lemma 5.5 in [BKPS02] is stated for a different family of formulas, the *random k-CNF formulas*, but that proof can be trivially adapted to random 3-XOR formulas. This is due to the fact that the adjacency graph for a 3-XOR formula or for a 3-CNF formula—as considered in [BKPS02]—is exactly the same.

[4] More precisely, as shown in [DM02], $\theta = \frac{\lambda}{3(1-\mathrm{e}^{-\lambda})^2}$ and λ is the positive root of $(x-3)\mathrm{e}^x + 2x + 3 = 0$.

$\mathbb{F}_p$, with $p \neq 2$ a prime, a proof system able to encode Gaussian eliminations over $\mathbb{F}_p$ [BSI10]. While, of course, any unsatisfiable 3-XOR formula in n variables and m linear equations has polynomial calculus over $\mathbb{F}_2$ refutations of size $m^{O(1)}$.)

1.3 Results

Very informally, the main result of this note is a lower bound on the length of k-DNF resolution refutations of 3-XOR formulas that are good expanders.

Theorem 1.5. *Let F be an exact 3-XOR formula in n variables and m linear constraints that is (r, c)-∂-expander with c s.t. $c > \frac{1}{2}$. Then for any $k \leqslant \frac{cr}{4}$ and $m > \min\{cr, n\}/12$, there exists a constant C depending only on c such that*

$$\mathrm{S}_k(F \vdash \bot) \geqslant \exp\left(r \cdot \left(\frac{r^2}{nm}\right)^{Ck^2}\right) . \tag{6}$$

The high level idea of the proof of this result goes as follows. Suppose, for sake of contradiction, that F has a short k-DNF resolution refutation π. Using a Switching Lemma (Theorem 3.2) we prove that there exists a partial assignment σ such that the restricted proof $\pi\restriction\sigma$ only contains k-DNF formulas with "low complexity". But then those "low complexity" k-DNFs can be used to convert the k-DNF resolution refutation of F into a resolution refutation of F in small width W (Theorem 3.1). But, as a consequence of Fact 1.3, we prove a that every resolution refutation of $F\restriction\sigma$ require width at least $W + 1$. Thus there cannot be short k-DNF resolution refutations of F and so we have our lower bound. The formal proof of Theorem 1.5 is in section 3.

A notable (immediate) application of Fact 1.4 and Theorem 1.5 is a lower bound for exact random 3-XOR formulas.

Corollary 1.6. *Let F be an exact random 3-XOR formula in n variables and Δn linear constraints. Then, asymptotically almost surely, for any $\Delta > 1$,*

$$\mathrm{S}_k(F \vdash \bot) \geqslant 2^{n/\Delta^{O(k^2)}} . \tag{7}$$

Comparison with [Ale11] and [SBI04] Corollary 1.6 corresponds to [Ale11, Theorem 4.1]. The main result we show, Theorem 1.5, is more general although the proof scheme of it is basically the same. Both results rely on the Switching Lemma from [SBI04], a version of which, for sake of completeness, is proved in this note too. Our version of that Switching Lemma is Theorem 3.5 and it is based on [SBI04, Theorem 3.3 and Corollary 3.4] although less general than the corresponding results. In this note, we follow more closely [Ale11] but with some relevant simplifications and we correct some inaccuracies. In particular the first equation of [Ale11, Lemma 3.8] is not correct (although fixable).

1.4 Open Problems

For k-DNF resolution there are basically two Switching Lemmas in the literature, [SBI04, Theorem 3.3] and [Raz15, Lemma 4.4]. Theorem 3.5 in this note corresponds to the Switching Lemma from [SBI04]. The Switching Lemma from [Raz15] has a quadratic improvement in the parameter k w.r.t. the Switching Lemma from [SBI04]. For instance [SBI04] proved that asymptotically almost surely random $O(k^2)$-CNF formulas in n variables must have k-DNF resolution refutations of size $n^{\omega(1)}$, as long as $k = o(\sqrt{\log n / \log\log n})$. This result, applying the Switching Lemma from [Raz15] can be easily improved[5] to show that asymptotically almost

[5] This was observed by Massimo Lauria (*pers. comm.*).

surely random $O(k)$-CNF formulas in n variables must have k-DNF resolution refutations of size $n^{\omega(1)}$, as long as $k = o(\log n/\log\log n)$. Unfortunately the Switching Lemma from [Raz15] does not apply to exact random 3-XOR (or random 3-CNFs as well).

Question 1.7. Let F be an exact random 3-XOR formula in n variables and Δn linear constraints. Prove that, asymptotically almost surely, for any $\Delta > 1$,

$$\mathrm{S}_k(F \vdash \bot) \geqslant 2^{n/\Delta^{O(k)}}. \tag{8}$$

This result might follow from some non-trivial adaptation of the arguments in this note and the Switching Lemma from [Raz15].

1.5 More Standard Definitions and Results

We conclude this introductory part recalling all the remaining standard definitions and facts from the literature that we will need.

Partial Assignments Given a set of variables X, a *partial assignment over* X is a function $\sigma : X \to \{0,1\} \cup X$ such that for each $x \in X$ either $\sigma(x) \in \{0,1\}$ or $\sigma(x) = x$. The *domain of* σ, $\mathrm{dom}(\sigma)$, is the set $\sigma^{-1}(\{0,1\})$. A partial assignment σ naturally extends to a function from the set of propositional formulas over X to itself in the natural way respecting the semantics of $\wedge, \vee, \neg, \oplus$. We denote with $F\restriction\sigma$, the application of σ to a propositional formula F.[6]

Given two partial assignments σ and σ' over X with $\mathrm{dom}(\sigma) \cap \mathrm{dom}(\sigma') = \emptyset$, we define their *union* to be $\sigma \cup \sigma'$: for every $x \in X$,

$$\sigma \cup \sigma'(x) = \begin{cases} \sigma(x) & \text{if } x \notin \mathrm{dom}(\sigma')\,, \\ \sigma'(x) & \text{otherwise}\,. \end{cases} \tag{9}$$

It immediate to see that partial assignments preserve the validity of k-DNF resolution refutations. More precisely, if $\pi = (G_1, \ldots, G_\ell)$ is a k-DNF resolution refutation of a formula F and σ is a partial assignment, then $\pi\restriction\sigma = (G_1\restriction\sigma, \ldots, G_\ell\restriction\sigma)$ is a k-DNF resolution refutation of $F\restriction\sigma$.

Minimally Unsatisfiable Formulas Let $F = L_1 \wedge \cdots \wedge L_m$ be a 3-XOR formula and t be a term. We say that $F \wedge t$ is *minimally unsatisfiable* if $F \wedge t$ is unsatisfiable but $\bigwedge_{L\in A} L \wedge t'$ is satisfiable for each $A \subset \{L_1, \ldots, L_m\}$ and each $t' \subset t$. With a slight abuse of notation we will write $A \wedge t$ even when A is a set of linear equations, meaning actually $\bigwedge_{L\in A} L \wedge t$. Given $F \wedge t$ that is unsatisfiable there is always a minimally unsatisfiable part of it, that is a $A \wedge t'$ minimally unsatisfiable with $A \subseteq \{L_1, \ldots, L_m\}$ and $t' \subseteq t$.

Fact 1.8. *Let F be a 3-XOR formula, t a term and suppose that $F \wedge t$ is minimally unsatisfiable. Then $\partial(F) \subseteq \mathrm{vars}(t)$ and the adjacency graph of F, $\mathcal{G}_F$ is connected.* ∎

This fact is immediate from the definition of $\mathcal{G}_F$ and the minimality condition on $F \wedge t$, so the proof is left to the reader.

[6] More precisely the application of σ to a propositional formula F, that is $F\restriction\sigma$, it is defined recursively as follows: if $F = \neg G$, then $F\restriction\sigma = \neg(G\restriction\sigma)$; if $F = G \odot H$, then $F\restriction\sigma = (G\restriction\sigma) \odot (H\restriction\sigma)$, whenever $\odot \in \{\wedge, \vee, \oplus\}$; if x is a variable $x\restriction\sigma = \sigma(x)$. The corresponding formula is then simplified syntactically according to the following rules: $\neg 0 = 1$, $\neg 1 = 0$, $0 \vee A = A$, $1 \vee A = 1$, $1 \wedge A = A$, $0 \wedge A = 0$, $0 \oplus A = A$ and $1 \oplus A = \neg A$.

Probability preliminaries We use boldface fonts to denote random variables. To upper bound events stating that binomial variables are far from their expected value, we use the Chernoff bound.

Fact 1.9 (Chernoff bound)**.** *Let $\boldsymbol{X}$ be a binomial random variable and let $\mu = \mathbb{E}[\boldsymbol{X}]$, then* $\Pr[\boldsymbol{X} > 2\mu] \leqslant \mathrm{e}^{-\mu/4}$ *and* $\Pr[\boldsymbol{X} < \frac{\mu}{2}] \leqslant \mathrm{e}^{-\mu/8}$. ∎

The second fact that we will use is a way to obtain, given a satisfiable system of linear constraints A, a random partial assignment uniformly distributed among all the partial assignments satisfying A.

Fact 1.10. *Let A be a satisfiable system of linear constraints over n variables $x_1, \ldots, x_n$ and let X be a subset of those variables. Let $\boldsymbol{\rho}_0$ be the identity over $\{x_1, \ldots, x_n\}$. Then for each $i \in [n]$, let $\boldsymbol{\rho}_i(x_j) = \boldsymbol{\rho}_{i-1}(x_j)$ for $j \neq i$ and for $j = i$ let*

$$\boldsymbol{\rho}_i(x_i) = \begin{cases} x_i & \text{if } x_i \notin X\,, \\ 1 & \text{if } \boldsymbol{\rho}_{i-1} \cup \{x_i = 0\} \text{ falsifies } A\,, \\ 0 & \text{if } \boldsymbol{\rho}_{i-1} \cup \{x_i = 1\} \text{ falsifies } A\,, \\ 1 & \text{with probability } \frac{1}{2}\text{, if none of the above happens}\,, \\ 0 & \text{otherwise}\,. \end{cases} \tag{10}$$

Then $\boldsymbol{\rho}_n$ is uniformly distributed in the set of partial assignments with domain X satisfying A, no matter of the ordering of the variables $x_1, \ldots, x_n$. ∎

This result follows easily from the basics of linear algebra and relies on the observation that the set of solutions of A is an affine subspace of $\{0,1\}^n$.

2 Closures and Proofs in Normal Form

In this section we construct a notion of *closure* of a set of variables, we relate it to expansion and we use it to construct a normal form for k-DNF resolution refutations of 3-XOR formulas.

Definition 2.1 ((r,c)-closure)**.** Let $F = L_1 \wedge \cdots \wedge L_m$ be a 3-XOR formula and r and c be two real numbers. Given a set $J \subseteq \mathrm{vars}(F)$ we say that a set $S \subseteq \{L_1, \ldots, L_m\}$ is an (r,c)*-closure of J (in F)* if for every $A \subseteq \{L_1, \ldots, L_m\} \setminus S$ with $|A| \leqslant r$ it holds that $|\partial_F(A) \setminus (J \cup \mathrm{vars}(S)| \geqslant c|A|$.

Given a 3-XOR formula F and a set of variables J, a *closure* S of J captures a set of linear constraints of F with the property that when we set the variables in $J \cup \mathrm{vars}(S)$ by some partial assignment σ that satisfies S then the restricted 3-XOR formula $F{\restriction}\sigma$ is a good expander. More formally the result is the following.

Lemma 2.2. *Let $F = L_1 \wedge \cdots \wedge L_m$ be a 3-XOR formula, let $J \subseteq \mathrm{vars}(F)$ and let $S \subseteq \{L_1, \ldots, L_m\}$ be an (r,c)-closure of J. Suppose that S is satisfiable and let σ be any partial assignment satisfying S with domain $J \cup \mathrm{vars}(S)$. Then $F{\restriction}\sigma$ is an (r,c)-∂-expander.*

Proof. Let $F{\restriction}\sigma = L_{i_1}{\restriction}\sigma \wedge \cdots \wedge L_{i_\ell}{\restriction}\sigma$, let $A \subseteq \{L_{i_1}{\restriction}\sigma, \ldots, L_{i_\ell}{\restriction}\sigma\}$ such that $|A| \leqslant r$ and let A' be the set of linear constraints of F corresponding to the linear constraints in A. That is $L_{i_j} \in A'$ if and only if $L_{i_j}{\restriction}\sigma \in A$. By construction, all the linear constraints in S are satisfied by σ, hence $A' \cap S = \emptyset$. Hence, by definition of S and σ it must be that:

$$|\partial_{F{\restriction}\sigma}(A)| = |\partial_F(A') \setminus (J \cup \mathrm{vars}(S))| \geqslant c|A'| = c|A|\,. \qquad ∎$$

To apply the previous result we actually need that (1) closures *exist* and (2) they don't have too large size, so it is not the case that the previous lemma is just vacuously true.

Proposition 2.3. *Let $F = L_1 \wedge \cdots \wedge L_m$ be a 3-XOR formula that is an (r, c)-∂-expander, let $J \subseteq \mathrm{vars}(F)$ and $A \subseteq \{L_1, \ldots, L_m\}$ such that $|A| \leqslant r/2$, $|\partial_F(A) \smallsetminus J| < \frac{c}{2}|A|$ and $|J| \leqslant rc/4$. Then there exists an $(\frac{r}{2}, \frac{c}{2})$-closure S of J such that $S \supseteq A$ and $|S| \leqslant \frac{2}{c}|J|$.*[7]

Proof. Take a maximal collection of pairwise disjoint non-empty sets $S_1, \ldots, S_\ell$ from $\{L_1, \ldots, L_m\}$ such that $S_1 = A$ and for every $i \geqslant 1$

1. $|S_i| \leqslant \frac{r}{2}$; and
2. $\left|\partial_F(S_i) \smallsetminus (J \cup \mathrm{vars}(\bigcup_{j<i} S_j))\right| < \frac{c}{2}|S_i|$.

The set $S = \bigcup_{i \in [\ell]} S_i$, by maximality, is an $(\frac{r}{2}, \frac{c}{2})$-closure of J and by construction $S \supseteq A$.

So far we din't use neither the fact that F is an (r, c)-∂-expander nor that $|J| \leqslant rc/4$. We use those assumptions to prove that $|S| \leqslant \frac{2}{c}|J|$. For sake of conciseness let $S_{\leqslant i} = \bigcup_{j \leqslant i} S_j$. First we prove by induction on i that for each $1 \leqslant i \leqslant \ell$,

$$|\partial_F(S_{\leqslant i}) \smallsetminus J| < \frac{c}{2}|S_{\leqslant i}|\,. \tag{11}$$

For $i = 1$, eq. 11 holds just by assumption. For the inductive step, we just have the following chain of inequalities:

$$\begin{aligned}
|\partial_F(S_{\leqslant i+1}) \smallsetminus J| &= |\partial_F(S_{\leqslant i} \cup S_{i+1}) \smallsetminus J| && (12)\\
&\leqslant |\partial_F(S_{\leqslant i}) \smallsetminus J| + |\partial_F(S_{i+1}) \smallsetminus (J \cup \mathrm{vars}(S_{\leqslant i}))| && (13)\\
&< \frac{c}{2}(|S_{\leqslant i}| + |S_{i+1}|) && (14)\\
&= \frac{c}{2}(|S_{\leqslant i} \cup S_{i+1}|)\,, && (15)
\end{aligned}$$

where in eq. 14 we used the inductive hypothesis and construction of S and in eq. 15 we used the fact that by definition $S_{\leqslant i} \cap S_{i+1} = \emptyset$.

Suppose now, for sake of contradiction, that $|S| \geqslant \frac{2}{c}|J|$ and let i be the first index such that $|S_{\leqslant i}| \geqslant \frac{2}{c}|J|$. Let $S_{\leqslant i} = S_{\leqslant i-1} \cup S_i$, we have that

$$|S_{\leqslant i}| = |S_{\leqslant i-1}| + |S_i| \leqslant \frac{2}{c}|J| + \frac{r}{2} \leqslant r\,. \tag{16}$$

Hence $|\partial_F(S_{\leqslant i})| \geqslant c|S_{\leqslant i}|$ and we have the following chain of inequalities

$$|\partial_F(S_{\leqslant i}) \smallsetminus J| \geqslant |\partial_F(S_{\leqslant i})| - |J| \geqslant c|S_{\leqslant i}| - \frac{c}{2}|S_{\leqslant i}| = \frac{c}{2}|S_{\leqslant i}|. \tag{17}$$

Now eq. 11 and eq. 17 immediately contradict each other. So, it must be that $|S| < \frac{2}{c}|J|$ ∎

We now define a notion of *normal form* for DNF formulas. This concept allows us to obtain, without loss of generality, k-DNF resolution refutations that we can control better.

Definition 2.4 (r-normal form)**.** Given a 3-XOR formula $F = L_1 \wedge \cdots \wedge L_m$, we say that a DNF G is in *r-normal form w.r.t F* if for every term t in G and every set $A \subseteq \{L_1, \ldots, L_m\}$ with $|A| \leqslant r$ we have that $A \wedge t$ is satisfiable.

[7] Notice that the statement of the theorem becomes trivial if there is no set $A \subseteq \{L_1, \ldots, L_m\}$ such that $|A| \leqslant r/2$ and $|\partial_F(A) \smallsetminus J| < \frac{c}{2}|A|$. In that case $S = \emptyset$ is an $(\frac{r}{2}, \frac{c}{2})$-closure of J and the size upper bound clearly holds.

Actually, in the previous definition it is enough to check wether $A \wedge t$ is satisfiable just for all $A \subseteq \{L_1, \ldots, L_m\}$ that are an (r, c)-closure of $\mathrm{vars}(t)$. These sets could have size much smaller than r.

Lemma 2.5. *Let F be a 3-XOR formula that is (r, c)-∂-expander and G be a k-DNF with $k \leqslant \frac{rc}{4}$. Then if G is in $\frac{2k}{c}$-normal form w.r.t F then G is in $\frac{r}{2}$-normal form too.*

Proof. Let $F = L_1 \wedge \cdots \wedge L_m$. For sake of contradiction, assume that there exists a term t in G and $A \subseteq \{L_1, \ldots, L_m\}$ such that $|A| \leqslant \frac{r}{2}$ and $A \wedge t$ is unsatisfiable. Let $t' \subseteq t$ and $A' \subseteq A$ such that $A \wedge t'$ is minimally unsatisfiable. Then, by Fact 1.8, $\partial(A') \subseteq \mathrm{vars}(t') \subseteq \mathrm{vars}(t)$. Hence by Proposition 2.3 there exists an $(\frac{r}{2}, \frac{c}{2})$-closure S of $\mathrm{vars}(t)$ such that $S \supseteq A'$ and $|S| \leqslant \frac{2}{c}|\mathrm{vars}(t)| \leqslant \frac{2k}{c}$. By assumption then $S \wedge t$ is satisfiable and hence $A' \wedge t'$ is satisfiable too. ∎

Resolution refutations—of exact 3-XOR formulas that are expanding—are always in normal form.

Lemma 2.6. *Let F be an exact 3-XOR formula that is a (r, c)-∂-expander with $c > 1/2$ and let C be a clause. Then every resolution derivation of C from F has lines in r-normal form w.r.t. F.*

Proof. Let π be a resolution derivation of C from of $F = L_1 \wedge \cdots \wedge L_m$. The only terms apperaring in a resolution refutations are literals. For sake of contradiction suppose that ℓ is a literal in π and there exists $A \subseteq \{L_1, \ldots, L_m\}$ with $|A| \leqslant r$ and such that $A \wedge \ell$ is unsatisfiable. Since F is an (r, c)-∂-expander, then Fact 1.2, implies that A is satisfiable. Let $A' \subseteq A$ such that $A' \wedge \ell$ is minimally unsatisfiable. We have that $|\partial_F(A')| > 1$. If $|A'| = 1$ then $|\partial_F(A')| = 3$ since F is an exact 3-XOR formula. If $|A'| \geqslant 2$ then, since F is (r, c)-∂-expander and $|A'| \leqslant |A| \leqslant r$, it must be that $|\partial_F(A')| \geqslant c|A'| \geqslant 2c > 1$ by the assumption that $c > 1/2$.

On the other hand since $A' \wedge \ell$ is minimally unsatisfiable, by Fact 1.8, $\partial_F(A') \subseteq \{x\}$, where $\ell = x^b$. Hence we immediately got a contradiction. ∎

The previous lemma is not true for k-DNF resolution. But, with a small increase in length, we can assume that k-DNF resolution refutations—of exact 3-XOR formulas that are expanding—consist of DNF formulas in normal form.

Lemma 2.7. *Let F be an exact 3-XOR formula that is a (r, c)-∂-expander with $c > 1/2$. Suppose that $k \leqslant \frac{cr}{4}$ and let L be the length of the shortest k-DNF resolution refutation of F. Then there exists a k-DNF resolution refutation $\pi' = (G'_1, \ldots, G'_s)$ of F with $\mathrm{S}_k(\pi') \leqslant L \cdot 2^{2k/c}$ and each G'_i in $\frac{r}{2}$-normal form w.r.t. F.*

Proof. Let $F = L_1 \wedge \cdots \wedge L_m$ and let $\pi = (G_1, \ldots, G_m)$ be any k-DNF resolution refutation of F of the shortest length possible L. Suppose, G_i is the first line of the proof that is not in r-normal form. Then G_i contains a k-term t for which there exists a set $A \subseteq \{L_1, \ldots, L_m\}$ with $|A| \leqslant \frac{r}{2}$ and $A \wedge t$ is unsatisfiable. Hence there exists a resolution derivation of the clause $\neg t$ from A of length at most $2^{|A|}$.

Moreover, by Lemma 2.5, we can assume that $|A| \leqslant \frac{2k}{c}$. Hence there exists a resolution derivation of $\neg t$ from F of size at most $2^{2k/c}$. This derivation, by Lemma 2.6 is in r-normal form w.r.t. F (and henceforth in $\frac{r}{2}$-normal form w.r.t. F).

By the minimality of G_i it must be that t was obtained by the inference rule from eq. 1a, that is $t = \ell \wedge \bigwedge_{i \in I} \ell_i$ and it was obtained as an application of

$$\frac{C \vee \bigwedge_{i \in I} \ell_i, \quad C \vee \ell}{C \vee (\ell \wedge \bigwedge_{i \in I} \ell_i)} \quad |I| < k\,, \tag{18}$$

with both $\bigwedge_{i\in I}\ell_i$ and ℓ such that for every $A\subseteq\{L_1,\dots,L_m\}$ with $|A|\leqslant\frac{r}{2}$, $A\wedge\ell$ and $A\wedge\bigwedge_{i\in I}\ell_i$ are satisfiable. Using the resolution derivation of $\neg t$ we found before we can then infer from the premises of eq. 18 the stronger k-DNF C using the cut rule. This introduces in the proof new terms that are of the form $\bigwedge_{i\in J}\ell_i$ for each $J\subseteq I$. But clearly those are not problematic: for every $A\subseteq\{L_1,\dots,L_m\}$ with $|A|\leqslant r$, $A\wedge\bigwedge_{i\in J}\ell_i$ is satisfiable.

We then proceed along the proof π substituting all non problematic terms in this way. We get a k-DNF resolution refutation π' of F of length $L\cdot 2^{2k/c}$. All its lines are in $\frac{r}{2}$-normal form because of what we argued before and the fact that we modify the proof using resolution derivations which are in r-normal form due to Lemma 2.6. ∎

3 Proof of the main result

In this section we give the proof of Theorem 1.5. This is the whole proof except that some more technical parts are postponed a bit. In particular the proof of Theorem 1.5 relies on the fact that there exists a function $\mathrm{W}(\cdot)$ mapping k-DNF formulas to natural numbers that makes the following two results true.

Theorem 3.1. *Let F be an unsatisfiable 3-XOR formula, π be a k-DNF resolution refutation of F and σ be a partial assignment. Then either $F\restriction\sigma$ is not an (r,c)-∂-expander or for every k-DNF formula $G\in\pi\restriction\sigma$, $\mathrm{W}(\pi\restriction\sigma)<\frac{rc}{6}$.*

Theorem 3.2 (Switching Lemma)**.** *Let $k\geqslant 1$ be an integer, s be a positive real number and $F=L_1\wedge\cdots\wedge L_m$ a 3-XOR formula in n variables that is an (r,c)-∂-expander and such that each variable appears in at most D of the L_i. If $crD^{C_1k}\geqslant 4kn$ for some constant C_1, then exists a distribution over partial assignments $\mathcal{D}$ and constants C_2,C_3 depending only on c and C_1 such that*

$$\Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[F\restriction\boldsymbol{\rho}\text{ is not an }(\frac{r}{2},\frac{c}{2})\text{-}\partial\text{-expander}]\leqslant \mathrm{e}^{-C_2r}\,, \tag{19}$$

and moreover for every k-DNF formula G in r-normal form,

$$\Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[\mathrm{W}(G\restriction\boldsymbol{\rho})\geqslant s]\leqslant\exp\left(-s\,(r/nD)^{C_3k^2}\right)\,. \tag{20}$$

There are many possible examples of functions $\mathrm{W}(\cdot)$ satisfying the previous two theorems and, in the proof of Theorem 1.5, the particular choice of $\mathrm{W}(\cdot)$ will not matter. For the moment we focus on proving Theorem 1.5, restated below for convenience of the reader, given Theorem 3.1 and Theorem 3.2.

Theorem 1.5. *Let F be an exact 3-XOR formula in n variables and m linear constraints that is (r,c)-∂-expander with c s.t. $c>\frac{1}{2}$. Then for any $k\leqslant\frac{cr}{4}$ and $m>\min\{cr,n\}/12$, there exists a constant C depending only on c such that*

$$\mathrm{S}_k(F\vdash\bot)\geqslant\exp\left(r\cdot\left(\frac{r^2}{nm}\right)^{Ck^2}\right)\,. \tag{6}$$

Proof. Let F be a random 3-XOR formula satisfying the hypothesis of the theorem and let π be a k-DNF resolution refutation of F of minimal length. The only two problems in applying Theorem 3.2 directly are that π might not be in normal form and that some variable of F might appear in too many linear constraints.

Since F is an exact 3-XOR formula then we can apply Lemma 2.7 and find a k-DNF resolution refutation $\tilde{\pi}$ of F in $\frac{r}{2}$-normal form and of length at most $|\pi|2^{k/2}$.

The *degree* of a variable x is the number of linear constraints of F that mention x. To get rid of the variables of too large degree take J to be a set of the $\frac{cr}{4}$ largest degree variables. Let S be a $(\frac{r}{2}, \frac{c}{2})$-closure of J. By Proposition 2.3, $|S| < \frac{2}{c}|J| = \frac{r}{2}$. By Fact 1.2 then S is satisfiable. Let σ be any partial assignment of domain $J \cup \mathrm{vars}(S)$ that satisfies S. By Lemma 2.2, $F\restriction\sigma$ is $(\frac{r}{2}, \frac{c}{2})$-$\partial$-expander. Suppose now that a variable in $F\restriction\sigma$ has degree d in $F\restriction\sigma$, then all variables in J must have degree at least d. Since the total degree of the variables of F is at most $3m$ then it must be that $3m \geqslant d|J|$. That is $d \leqslant \frac{12m}{cr}$.

So we found a restriction σ such that $F\restriction\sigma$ is $(\frac{r}{2}, \frac{c}{2})$-$\partial$-expander and each variable of $F\restriction\sigma$ appears in at most $D = \frac{12m}{cr}$ equations of $F\restriction\sigma$. After applying the restriction σ to $\tilde{\pi}$, we are left with the k-DNF resolution refutation $\tilde{\pi}\restriction\sigma$ of $F\restriction\sigma$. For simplicity let $F' = F\restriction\sigma$ and $\pi' = \tilde{\pi}\restriction\sigma$. From now on we focus on F' and its k-DNF resolution refutation π'. Since $\tilde{\pi}$ was in $\frac{r}{2}$-normal form then also π' is in $\frac{r}{2}$-normal form.

Let then $\mathcal{D}$ be the distribution over partial assignments from Theorem 3.2. Then by Theorem 3.1:

$$1 = \Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[\exists G \in \pi' \ \mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant \frac{rc}{24} \vee F'\restriction\boldsymbol{\rho} \text{ is not } (\tfrac{r}{4}, \tfrac{c}{4})\text{-}\partial\text{-expander}]\,. \tag{21}$$

Then the following chain of inequalities concludes the proof:

$$1 = \Pr[F'\restriction\boldsymbol{\rho} \text{ is not an } (\tfrac{r}{4}, \tfrac{c}{4})\text{-}\partial\text{-expander} \vee \exists G \in \pi' \ \mathrm{W}(G\restriction\boldsymbol{\rho}) > \frac{rc}{24}] \tag{22}$$

$$\leqslant \Pr[F'\restriction\boldsymbol{\rho} \text{ is not an } (\tfrac{r}{4}, \tfrac{c}{4})\text{-}\partial\text{-expander}] + \sum_{G\in\pi'} \Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant \frac{rc}{24}] \tag{23}$$

$$\leqslant \mathrm{e}^{-C_2 r} + |\pi'| \exp\left(-\frac{rc}{24}\left(\frac{r^2}{nm}\right)^{C_3 k^2}\right) \tag{24}$$

$$\leqslant \mathrm{e}^{-C_2 r} + |\pi| 2^{2k/c} \exp\left(-\frac{rc}{24}\left(\frac{r^2}{nm}\right)^{C_3 k^2}\right), \tag{25}$$

where eq. 23 is just an union bound. In eq. 24 we just applied Theorem 3.2 and C_2, C_3 are just the constants (depending only on c) provided by that theorem. Notice that to apply Theorem 3.2 we also need to show that $crD^{C_1 k} \geqslant 4kn$. This is implied by the fact that for a large enough constant C_1 it holds that $(12m/cr)^{C_1 k - 1} \geqslant 4k$, since by assumption $12m/cr > 1$. Hence $cr(12m/cr)^{C_1 k} \geqslant 12m4k > 4kn$, by the assumption that $m > n/12$.

The lower bound for $|\pi|$ follows then immediately from eq. 25. ∎

We now prove Theorem 3.1 and Theorem 3.2. Analogous results were proven in [SBI04, Ale11] taking as $\mathrm{W}(\cdot)$ the minimal depth of a binary decision tree representing the k-DNF. In our exposition $\mathrm{W}(G)$ is the minimum width needed to refute unsatisfiable set of clauses we can associate to the k-DNF formula G.

Definition 3.3 (clause representation)**.** Given a DNF formula G and two disjoint set of clauses G^0 and G^1, we say that (G^0, G^1) is a *representation* of G if for every clause $C \in G^1$ it holds that $\neg C \models G$ and for every clause $C \in G^0$, $\neg C \models \neg G$.[8]

Clearly for every DNF formulas G there are a lot of representations (G^0, G^1), but we just focus on the ones such that $G^0 \cup G^1$ is *refutable* in resolution.[9]

[8] Recall that given two DNF formulas F and G, $F \models G$ if and only if for every partial assignment σ such that $F\restriction\sigma = 1$ it holds that $G\restriction\sigma = 1$.

[9] Notice that for every DNF G in n variables there is always at least a refutable representation (that needs very large width and size resolutions proofs). Namely (G^0, G^1) with G^1 all the clauses in n literals C such that $\neg C \models G$; and G^0 defined analogously.

Definition 3.4 ($\mathrm{W}(G)$)**.** Let G be a DNF formula. We define $\mathrm{W}(G)$ as the minimum integer w such that there exist a representation (G^0, G^1) of G such that $G^0 \cup G^1$ has a resolution refutation of width w.

3.1 Proof of Theorem 3.1

Let F be an unsatisfiable 3-XOR formula, π be a k-DNF resolution refutation of F and σ be a partial assignment. We show that if for every k-DNF formula $G \in \pi\restriction\sigma$, $\mathrm{W}(\pi\restriction\sigma) < \frac{rc}{6}$ then $F\restriction\sigma$ has a resolution refutation of width strictly less than $\frac{rc}{2}$. Which by Fact 1.3 means that $F\restriction\sigma$ cannot be an (r, c)-∂-expander.

This follows from a completely generic result: given any CNF formula F' and any k-DNF resolution refutation $\pi' = (G_1, \ldots, G_m)$ of F; if for every i, $\mathrm{W}(G_i) \leqslant w$ then there exists a resolution refutation of F' of width at most $3w$.[10]

Let (G_i^0, G_i^1) be a clause representation of G_i such that $G_i^0 \cup G_i^1$ is refutable in width w (it exists by hypothesis). By induction on i, we show that for each G_i and for each $C \in G_i^0$, there exists a resolution derivation of C from F' of width at most $3w$. Since $G_m = \bot$ and $(\{\bot\}, \emptyset)$ represents $\bot$, at the m-th step we get a resolution refutation of F' of width at most $3w$.

The base case is trivial since G_1 is a clause from F'. Say $G_1 = \bigvee_{i \in I} x_i^{b_i}$, then $(\{G_1\}, \{x_i^{1-b_i} \mid i \in I\})$ is a clause representation of G_1 refutable in resolution in width at most w by hypothesis.

In the inductive step G_i is derived from two previous DNF formulas G_j and $G_{j'}$.[11] Let $C \in G_i^0$, we use the resolution refutations of $G_j^0 \cup G_j^1$ and $G_{j'}^0 \cup G_{j'}^1$ to build the width-bounded resolution derivation of C from F'. We start constructing a clause representation (G^0, G^1) of $G_j \wedge G_{j'}$:

$$G^0 = G_j^0 \cup G_{j'}^0\,, \tag{26a}$$

$$G^1 = \{C' \vee C'' \mid C' \in G_j^1 \text{ and } C'' \in G_{j'}^1\}\,. \tag{26b}$$

It is easy to see from this definition that (G^0, G^1) represents $G_j \wedge G_{j'}$ and moreover it can be refuted in resolution in width $2w$. So let $(C_1, \ldots, C_{\ell-1}, \bot)$ be a refutation of $G^0 \cup G^1$ and consider the derivation $\pi = (C_1 \vee C, \ldots, C_{\ell-1} \vee C, C)$ of C from $\{C \vee \tilde{C} \mid \tilde{C} \in G^0 \cup G^1\}$. This is a derivation of width at most $3w$ and moreover all the clauses in G^0, by induction, can be derived from F' in width at most $3w$. So, by weakening, the same is true for clauses in $\{C \vee \tilde{C} \mid \tilde{C} \in G^0\}$. We claim that all the clauses of the form $C \vee \tilde{C}$ with $\tilde{C} \in G^1$ are tautological and hence redundant. Suppose, for sake of contradiction, that there is a falsifiable $C \vee \tilde{C}$ with $\tilde{C} \in G^1$. Let σ be a partial assignment falsifying $C \vee \tilde{C}$. Since $C \in G_i^0$ then $G_i\restriction\sigma = 0$. On the other hand $\tilde{C} \in G^1$ so $G_j \wedge G_{j'}\restriction\sigma = 1$ so there must be two terms $t \in G_j$ and $t' \in G_{j'}$ satisfied by σ. By the syntax of the k-DNF resolution inference rules then it is immediate to see that there must be a term $s \in G_i$ satisfied by σ. Which is impossible since $G_i\restriction\sigma = 0$. ∎

3.2 Proof of Theorem 3.2, the Switching Lemma

The proof of Theorem 3.2 is way more involved than the one we just saw and it relies on the following result, which is based on [SBI04, Theorem 3.3 and Corollary 3.4].[12]

Theorem 3.5. *Let $k \geqslant 1$, s be a positive real number, $\delta \in (0, \frac{2}{3}]$, let Γ be a set of DNF formulas closed under restrictions and let $\boldsymbol{\rho}$ be a random partial assignment s.t. for every k-DNF formula*

[10] This claim and its proof are very close to [SBI04, Theorem 5.1].

[11] This is since we defined k-DNF resolution to have binary inference rules.

[12] The actual statements of [SBI04, Theorem 3.3 and Corollary 3.4] give a stronger and more general result than the one stated here but we don't not need such extra generality in this note.

$G \in \Gamma$,

$$\Pr[G\restriction\boldsymbol{\rho} \neq 1] \leqslant 2^{-\delta \operatorname{cov}(G)}\,, \tag{27}$$

where $\operatorname{cov}(G)$ *is the minimum size of a set of variables* S *such that for every term* t *in* G, $\operatorname{vars}(t) \cap S \neq \emptyset$. *Then for every* k*-DNF formula* $G \in \Gamma$,

$$\Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant s] \leqslant 2^{-s(\delta/2)^k}\,. \tag{28}$$

Proof of Theorem 3.5. We always have that

$$\Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant s] \leqslant \Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \neq 0] \leqslant \Pr[G\restriction\boldsymbol{\rho} \neq 1] \leqslant 2^{-\delta \operatorname{cov}(G)}\,, \tag{29}$$

where the second inequality follows from the fact that if $G\restriction\boldsymbol{\rho} = 1$ then $(\emptyset, \{\bot\})$ is a representation of it and hence $\mathrm{W}(G\restriction\boldsymbol{\rho}) = 0$. The last inequality is by hypothesis.

Now, if G is a k-DNF and $\operatorname{cov}(G) \geqslant \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}$, from eq. 29 we immediately get the inequality in eq. 28. Otherwise, assume $\operatorname{cov}(G) < \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}$ and argue by induction on k.

If $k = 1$, that is $G = \bigvee_{i\in I} x_i^{b_i}$ we can take as a clause representation of G the following: $(\{G\}, \{x_i^{1-b_i} \mid i \in I\})$. Hence,

$$\mathrm{W}(G\restriction\boldsymbol{\rho}) \leqslant \mathrm{W}(G) = |G| = \operatorname{cov}(G) < \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1} < s\,. \tag{30}$$

Hence $\Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant s] = 0$ and the inequality in eq. 28 clearly holds.

Assume now the inequality eq. 28 holds for every $(k-1)$-DNF formula and let's prove it for each k-DNF G. We start building a clause representation of $G\restriction\boldsymbol{\rho}$. Let S be a set of variables realizing $\operatorname{cov}(G\restriction\boldsymbol{\rho})$. In particular S and $\operatorname{dom}(\boldsymbol{\rho})$ are disjoint sets. Recall that we can assume that $|S| = \operatorname{cov}(G\restriction\boldsymbol{\rho}) \leqslant \operatorname{cov}(G) < \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}$.

Consider the set CT_S of all clauses of width $|S|$ over the variables in S. Clearly CT_S has size $2^{|S|}$ and it is unsatisfiable. For each clause $C \in \mathrm{CT}_S$ consider a clause representation (G^0_C, G^1_C) realizing $\mathrm{W}(G\restriction\boldsymbol{\rho} \cup \sigma_C)$, where σ_C is the partial assignment falsifying C with domain S. Now we claim that (G^0, G^1) constructed as follow is a representation of $G\restriction\boldsymbol{\rho}$:

$$G^0 = \{C \vee D \mid C \in \mathrm{CT}_S \text{ and } D \in G^0_C\}\,, \tag{31a}$$

$$G^1 = \{C \vee D \mid C \in \mathrm{CT}_S \text{ and } D \in G^1_C\}\,. \tag{31b}$$

Let $C \vee D$ with $C \in \mathrm{CT}_S$ and $D \in G^0_C \cup G^1_C$ and let $\sigma_{C\vee D}$ be the partial assignment with domain $\operatorname{vars}(C \vee D)$ falsifying $C \vee D$. Analogously define σ_C and σ_D. Then $(G\restriction\boldsymbol{\rho})\restriction\sigma_{C\vee D} = (G\restriction\boldsymbol{\rho}\cup\sigma_C)\restriction\sigma_D$ and, by construction, for each $C \in \mathrm{CT}_S$, (G^0_C, G^1_C) represents $G\restriction\boldsymbol{\rho} \cup \sigma_C$ so it is immediate to see that (G^0, G^1) represents $G\restriction\boldsymbol{\rho}$.

The set of clauses $G^0 \cup G^1$ is unsatisfiable and a possible resolution refutation is to use the fact that for each $C \in \mathrm{CT}_S$, $G^0_C \cup G^1_C$ is unsatisfiable to derive C from $G^0 \cup G^1$ and then refute CT_S once we derived all its clauses. This is a resolution refutation of width

$$|S| + \max_{C\in\mathrm{CT}_S} \mathrm{W}(G\restriction\boldsymbol{\rho} \cup \sigma_C) < \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1} + \max_{C\in\mathrm{CT}_S} \mathrm{W}(G\restriction\boldsymbol{\rho} \cup \sigma_C)\,. \tag{32}$$

We distinguish two cases according to how large is $\max_{C\in\mathrm{CT}_S} \mathrm{W}(G\restriction\boldsymbol{\rho} \cup \sigma_C)$.

Case 1. If $\max_{C\in\mathrm{CT}_S} \mathrm{W}(G\restriction\boldsymbol{\rho} \cup \sigma_C) \leqslant s - \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}$, then $\mathrm{W}(G\restriction\boldsymbol{\rho}) < s$. Hence, again, $\Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant s] = 0$, so the inequality in eq. 28 clearly holds.

Case 2. If $\max_{C\in \mathrm{CT}_S} \mathrm{W}(G\restriction \boldsymbol{\rho}\cup\sigma_C) > s - \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}$ we use the inductive hypothesis. The set S has non-empty intersection with the variables in each of the terms of $G\restriction\boldsymbol{\rho}$, hence $G\restriction\boldsymbol{\rho}\cup\sigma_C$ is a $(k-1)$-DNF and we can apply to it the inductive hypothesis. Concluding, we have that

$$\begin{aligned}\Pr[\mathrm{W}(G\restriction\boldsymbol{\rho}) \geqslant s] &\leqslant \Pr[\exists C\in \mathrm{CT}_S,\ \mathrm{W}(G\restriction\boldsymbol{\rho}\cup\sigma_C) \geqslant s - \frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}] &(33)\\ &\leqslant 2^{|S|}2^{-\left(\frac{\delta}{2}\right)^{k-1}\left(s-\frac{s}{2}\left(\frac{\delta}{2}\right)^{k-1}\right)} &(34)\\ &\leqslant 2^{-\frac{s}{2}\cdot\left(\frac{\delta}{2}\right)^{k-1}\left(1-\left(\frac{\delta}{2}\right)^{k-1}\right)} &(35)\\ &\leqslant 2^{-s\left(\frac{\delta}{2}\right)^{k}}, &(36)\end{aligned}$$

where the last inequality follows from the fact that for $k\geqslant 2$ and $\delta\leqslant\frac{2}{3}$, we have that $1-\left(\frac{\delta}{2}\right)^{k-1}\geqslant 1-\frac{\delta}{2}\geqslant\delta$. ∎

Let $F = L_1\wedge\cdots\wedge L_m$ be a 3-XOR formula in n variables that is an (r,c)-∂-expander such that each variable appears in at most D of the L_i and let Γ be the set of all DNF formulas in r-normal form. Moreover suppose that $crD^{Ck}\geqslant 4kn$ for some large enough constant C. To prove Theorem 3.2 we just need to construct a distribution over partial assignments $\mathcal{D}$ such that

$$\Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[F\restriction\boldsymbol{\rho} \text{ is not an } (\frac{r}{2},\frac{c}{2})\text{-}\partial\text{-expander}] \leqslant \mathrm{e}^{-\Theta(r)}, \tag{37}$$

and to which we can apply Theorem 3.5 with $\delta = \left(\frac{r}{nD}\right)^{C'k}$, for some constant C' large enough to have $\left(\frac{r}{nD}\right)^{C'k}\leqslant\frac{2}{3}$. That is we need to prove that for every k-DNF formula G in r-normal form,

$$\Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[G\restriction\boldsymbol{\rho}\neq 1] \leqslant \exp\left(-\operatorname{cov}(G)\left(\frac{r}{nD}\right)^{Ck}\right), \tag{38}$$

for some constant C large enough. Then Theorem 3.2 follows immediately from eq. 37, eq. 38 and Theorem 3.5. Hence we focus on constructing a distribution $\mathcal{D}$ over partial assignment such that eq. 37 and eq. 38 hold.

Definition 3.6 ($\boldsymbol{\rho}\sim\mathcal{D}$)**.** We say that a random partial assignment $\boldsymbol{\rho}$ is from the support of the distribution $\mathcal{D}$, $\boldsymbol{\rho}\sim\mathcal{D}$, if it is constructed according to the following process. Construct a random set of variables $\boldsymbol{Y}\subseteq\operatorname{vars}(F)$ independently for each $x\in\operatorname{vars}(F)$ choosing to put it in $\boldsymbol{Y}$ with probability $\frac{cr}{8n}$. Let $\boldsymbol{S}\subseteq\{L_1,\ldots,L_m\}$ be an $(\frac{r}{2},\frac{c}{2})$-closure of $\boldsymbol{Y}$ of size at most $\frac{2}{c}|\boldsymbol{Y}|$.[13] If there are no such $\boldsymbol{S}$ or if $\boldsymbol{S}$ is unsatisfiable, set the partial assignment $\boldsymbol{\rho}$ to be the empty partial assignment. Otherwise $\boldsymbol{\rho}$ is chosen uniformly at random from the set of partial assignments with domain $\boldsymbol{Y}\cup\operatorname{vars}(\boldsymbol{S})$ satisfying $\boldsymbol{S}$.

Proving eq. 37 is straightforward. By construction, $\mathbb{E}[|\boldsymbol{Y}|] = \frac{cr}{8}$. Moreover, if $|\boldsymbol{Y}|\leqslant\frac{cr}{4}$, Proposition 2.3 implies that there exists an $(\frac{r}{2},\frac{c}{2})$-closure $\boldsymbol{S}$ of $\boldsymbol{Y}$ of size at most $\frac{r}{2}$. So $\boldsymbol{S}$ is satisfiable, by Fact 1.2. Then, by Lemma 2.2, $F\restriction\boldsymbol{\rho}$ is an $(\frac{r}{2},\frac{c}{2})$-$\partial$-expander. Hence:

$$\begin{aligned}\Pr_{\boldsymbol{\rho}\sim\mathcal{D}}[F\restriction\boldsymbol{\rho} \text{ is not an } (\tfrac{r}{2},\tfrac{c}{2})\text{-}\partial\text{-expander}] &\leqslant \Pr[|\boldsymbol{Y}| > \frac{cr}{4}] &(39)\\ &\leqslant \mathrm{e}^{-cr/32}, &(40)\end{aligned}$$

where the last inequality is just the application of the Chernoff bound to the binomial random variable $|\boldsymbol{Y}|$.

[13] Say that $\boldsymbol{S}$ is chosen uniformly at random. It doesn't actually matter how it is chosen.

The proof of eq. 38 is less immediate. Suppose we are given a k-DNF G in r-normal form (with terms ordered according to an order we will choose later) and $\boldsymbol{\rho} \sim \mathcal{D}$.

During the construction of $\boldsymbol{\rho}$ we built a random set of variables $\boldsymbol{Y} \subseteq \mathrm{vars}(F)$. Let $G_{\boldsymbol{Y}}$ be the random sub-DNF of G corresponding to a maximum size disjunction of variable-disjoint terms t of G s.t. $\mathrm{vars}(t) \subseteq \boldsymbol{Y}$. We have that $|G_{\boldsymbol{Y}}|$ is a binomial random variable. For shortness let $p = \frac{cr}{8n}$. For each $t \in G$, $\Pr[\mathrm{vars}(t) \subseteq \boldsymbol{Y}] \geqslant p^k$ and for terms that are variable-disjoint those probabilities are independent. Moreover, there are at least $\frac{\mathrm{cov}(G)}{k}$ variable-disjoint terms in G, so $\mathbb{E}[|G_{\boldsymbol{Y}}|] \geqslant \frac{\mathrm{cov}(G)}{k} p^k$.

Let R be the event that $|\boldsymbol{Y}| \leqslant \frac{cr}{4}$ and $|G_{\boldsymbol{Y}}| \geqslant \frac{\mathrm{cov}(G)}{2k} \cdot p^k$. We can then proceed to bound $\Pr[G\restriction\boldsymbol{\rho} \neq 1]$ from above. For each term t_i in G, let E_i the event "$t_i\restriction\boldsymbol{\rho} = 1$". We then have the following:

$$\Pr[G\restriction\boldsymbol{\rho} \neq 1] \leqslant \Pr[\bigwedge_{t_i \in G} \neg E_i \mid R] + \Pr[\neg R] \tag{41}$$

$$= \prod_{t_i \in G} \left(1 - \Pr[E_i \mid \neg E_1 \wedge \cdots \wedge \neg E_{i-1} \wedge R]\right) + \Pr[\neg R]\,. \tag{42}$$

Let's start bounding $\Pr[\neg R]$ from above. Both $|\boldsymbol{Y}|$ and $|G_{\boldsymbol{Y}}|$ are binomial random variables, hence by the union bound and the Chernoff's bound we have that

$$\Pr[\neg R] \leqslant \exp(-\frac{pn}{4}) + \exp(-\frac{\mathrm{cov}(G)}{8k} p^k)\,. \tag{43}$$

We now build an ordering of the terms of G such for each $i < T$,

$$\Pr[E_{i+1} \mid \neg E_1 \wedge \cdots \wedge \neg E_i \wedge R] \geqslant 2^{-k}\,, \tag{44}$$

and $T \geqslant \frac{\mathrm{cov}(G)}{D^{\Theta(k)}} p^k$. If we are able to prove this then we are done:

$$\Pr[G\restriction\boldsymbol{\rho} \neq 1] \leqslant (1 - 2^{-k})^T + \exp(-\frac{pn}{4}) + \exp\left(-\frac{\mathrm{cov}(G)}{8k} p^k\right) \tag{45}$$

$$\leqslant \exp(-\frac{T}{2^k}) + \exp(-\frac{pn}{4}) + \exp\left(-\frac{\mathrm{cov}(G)}{8k} p^k\right) \tag{46}$$

$$\leqslant \exp\left(-\frac{\mathrm{cov}(G)}{2^k D^{\Theta(k)}} p^k\right) + \exp(-\frac{pn}{4}) + \exp\left(-\frac{\mathrm{cov}(G)}{8k} p^k\right) \tag{47}$$

$$\leqslant \exp\left(-\frac{\mathrm{cov}(G)}{D^{\Theta(k)}} p^k\right) \tag{48}$$

$$\leqslant \exp\left(-\,\mathrm{cov}(G) \left(\frac{r}{nD}\right)^{C'k}\right)\,, \tag{49}$$

for some constant C' large enough. Recall that $\mathcal{G}_F$ denotes the bipartite graph with vertices $\{L_1, \ldots, L_m\} \cup \mathrm{vars}(F)$ and $\{L_j, x\}$ is an edge in $\mathcal{G}_F$ iff $x \in \mathrm{vars}(L_j)$. By assumption every vertex in $\mathcal{G}_F$ has degree at most D.

We say that terms $t_1, \ldots, t_T$ in $G_{\boldsymbol{Y}}$ are chosen according to the process P_ℓ, if the following holds. The first term t_1 is any term in $G_{\boldsymbol{Y}}$, then suppose we have found $t_1, \ldots, t_i$ in $G_{\boldsymbol{Y}}$ according to P_ℓ and we want to find t_{i+1} in $G_{\boldsymbol{Y}}$. Let $V_i = \bigcup_{j \leqslant i} \mathrm{vars}(t_j)$ and let $S_i \subseteq \{L_1, \ldots, L_m\}$ be an $(\frac{r}{2}, \frac{c}{2})$-closure of V_i.[14] Let $B(i, \ell)$ be the ball of radius ℓ around $V_i \cup S_i$ in $\mathcal{G}_F$. If there is some

[14] Notice that we do not assume any upper bound on $|S_i|$.

term t in $G_{\boldsymbol{Y}}$ such that $B(i,\ell) \cap \mathrm{vars}(t) = \emptyset$, we then set t_{i+1} be any of such terms; otherwise we end the process and let $T = i$.[15]

The goal now is to show that there exists some ℓ such that the process P_ℓ produces terms $t_1, \ldots, t_T$ both with $T \geqslant \frac{\mathrm{cov}(G)}{D^{\Theta(k)}} p^k$ and such that for each $i \leqslant T$, eq. 44 holds. Consider then terms $t_1, \ldots, t_T$ in $G_{\boldsymbol{Y}}$ chosen according to the process P_ℓ.

The lower bound on T will hold whenever $\ell = O(k)$. If $T > \frac{cr}{4k}$ then by assumption $T \geqslant \frac{n}{D^{Ck}}$ and hence clearly $T \geqslant \frac{\mathrm{cov}(G)}{D^{\Theta(k)}}$. If $T \leqslant \frac{cr}{4k}$, then $|V_T| \leqslant kT \leqslant \frac{cr}{4}$ and hence, by Proposition 2.3, $|S_T| \leqslant \frac{2|V_T|}{c} \leqslant \frac{2kT}{c}$. Then we have the following chain of inequalities:

$$\frac{\mathrm{cov}(G)}{2k} \cdot p^k \leqslant |G_{\boldsymbol{Y}}| = \mathrm{cov}(G_{\boldsymbol{Y}}) \leqslant |B(T,\ell)| \leqslant (|V_T| + |S_T|) \cdot D^\ell \leqslant (kT + \frac{2kT}{c}) \cdot D^\ell \,, \tag{50}$$

where the first inequality is by the assumption that $\boldsymbol{\rho}$ is good, the second inequality holds just by construction of T, the third is the trivial upper bound on the size of the ball $B(T,\ell)$ in a graph of degree at most D. In the last inequality we just plug-in the upper bounds for $|V_T|$ and $|S_T|$ we just computed. From eq. 50 it follows that

$$T \geqslant \frac{|G_{\boldsymbol{Y}}|}{D^\ell k(1+\frac{2}{c})} \geqslant \frac{\mathrm{cov}(G)}{(2+\frac{4}{c})D^\ell k^2} p^k \geqslant \frac{\mathrm{cov}(G)}{D^{\Theta(k)}} p^k \,, \tag{51}$$

where the last inequality holds if $\ell = \Theta(k)$.

We can focus now on proving that there exists an ℓ such that eq. 44 holds for every $i \leqslant T$. By construction, for each $i < T$ we have that if $t_i \restriction \boldsymbol{\rho} \neq 1$ then $t_i \restriction \boldsymbol{\rho} = 0$, so imposing that $\neg E_1 \wedge \cdots \wedge \neg E_i$ happens is the same as imposing that the k-CNF $(\neg t_1 \wedge \cdots \wedge \neg t_i)$ is satisfied by $\boldsymbol{\rho}$. Let Ψ be $(\neg t_1 \wedge \cdots \wedge \neg t_i)$ written as a i-DNF and let $\boldsymbol{t}$ be a term in Ψ satisfied by $\boldsymbol{\rho}$. Take an ordering of the variables of $\mathrm{vars}(F)$ starting with the variables of $\boldsymbol{t}$ and then with the variables of t_{i+1}. We are conditioning on the event R to happen, in particular then $|\boldsymbol{Y}| \leqslant \frac{cr}{4}$ and, by Proposition 2.3, there are $(\frac{r}{2}, \frac{c}{2})$-closures of $\boldsymbol{Y}$ of size at most $\frac{2}{c}|\boldsymbol{Y}|$ to choose from when constructing the partial assignment $\boldsymbol{\rho}$. Let $\boldsymbol{S}$ be the closure coming from the construction of $\boldsymbol{\rho}$: it is satisfiable and moreover $\boldsymbol{S} \wedge \boldsymbol{t}$ is satisfiable too (by the conditioning in eq. 44). Moreover, since $|\boldsymbol{Y}| \leqslant \frac{cr}{4}$ then $\boldsymbol{S} \leqslant \frac{r}{2}$ and, since G is in r-normal form, then $t_{i+1} \wedge \boldsymbol{S}$ is also satisfiable.

Either $\boldsymbol{t} \wedge t_{i+1} \wedge \boldsymbol{S}$ is unsatisfiable or, by Fact 1.10, t_{i+1} is satisfied by the result of at most $|t_{i+1}|$ coin tosses each with probability $\frac{1}{2}$ of setting the correct value for $\boldsymbol{\rho}$, hence in this case $\Pr[E_{i+1} \mid \neg E_1 \wedge \cdots \wedge \neg E_i \wedge R] \geqslant 2^{-|t_{i+1}|} \geqslant 2^{-k}$, as we wanted to show.

Suppose then, for sake of contradiction, that $t_{i+1} \wedge \boldsymbol{S} \wedge t$ is unsatisfiable and let

$$s_{i+1} \wedge A \wedge s \text{ be minimally unsatisfiable,} \tag{52}$$

with s_{i+1} a sub-term of t_{i+1}, $A \subseteq \boldsymbol{S}$ and s a sub-term of $\boldsymbol{t}$. By what we observed before, both s_{i+1} and s must be non-empty. Let $\mathcal{G}_A$ be the subgraph of $\mathcal{G}_F$ induced by the vertices $A \cup \mathrm{vars}(s_{i+1} \wedge A \wedge s)$. By minimality and Fact 1.8, $\mathcal{G}_A$ is connected.

Hence there is a path in $\mathcal{G}_F$ from $\mathrm{vars}(s)$, which is a subset of $V_i \cup S_i$, to $\mathrm{vars}(t_{i+1})$ touching only linear constraints in A (and variables). So this means we can connect $S_i \cup V_i$ to t_{i+1} with a path of length at most $2|A \setminus S_i| + 1$. Since by construction $t_{i+1} \notin B(i,\ell)$ we must have that

$$|A \setminus S_i| > \frac{\ell - 1}{2} \,. \tag{53}$$

By the minimality in eq. 52 and Fact 1.8, we also know that

$$\partial_F(A) \subseteq \mathrm{vars}(s_{i+1}) \cup \mathrm{vars}(s) \subseteq \mathrm{vars}(t_{i+1}) \cup V_i \,, \tag{54}$$

[15] This process of course depends not only on ℓ but also on how S_i and t_i are chosen but those choices will not matter in the argument.

so $|\partial_F(A) \smallsetminus V_i| \leqslant |\mathrm{vars}(t_{i+1})| \leqslant k$. Now,

$$|\partial_F(A \smallsetminus S_i) \smallsetminus (V_i \cup \mathrm{vars}(S_i))| \leqslant |\partial_F(A) \smallsetminus V_i| \leqslant k\,, \tag{55}$$

so, if $k \leqslant \frac{c}{2} \cdot \frac{\ell-1}{2}$, then eq. 53 and eq. 55 will contradict the fact that S_i is an $(\frac{r}{2}, \frac{c}{2})$-closure of V_i. Hence, whenever the terms $t_1, \ldots, t_T$ are chosen in $G_{\boldsymbol{Y}}$ according to the process P_ℓ with $\ell \geqslant \frac{4k}{c} + 1$ then eq. 44 holds. ∎

Acknowledgements. The author thanks Jakob Nordström (KTH, Stockholm), Marc Vinyals (Tata Institute, Mumbai), Massimo Lauria and Nicola Galesi (Sapienza Universitá di Roma) for valuable discussions. This note is loosely based on some lectures given by the author at the KTH Royal Institute of Technology during Fall 2016. The author was partially funded by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no. 279611 and by the European Union's Horizon 2020 Research and Innovation Programme / ERC grant agreement no. 648276 AUTAR.

References

[Ale11] Michael Alekhnovich. Lower Bounds for k-DNF Resolution on Random 3-CNFs. *Computational Complexity*, 20(4):597–614, 2011.

[BKPS02] 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.

[Bla37] Archie Blake. *Canonical Expressions in Boolean Algebra*. PhD thesis, 1937. University of Chicago.

[BS01] Eli Ben-Sasson. *Expansion in Proof Complexity*. PhD thesis, 2001. Hebrew University.

[BSI10] Eli Ben-Sasson and Russell Impagliazzo. Random CNF's are hard for the polynomial calculus. *computational complexity*, 19(4):501–519, Dec 2010.

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow—resolution made simple. *J. ACM*, 48(2):149–169, March 2001.

[DM02] Olivier Dubois and Jacques Mandler. The 3-XORSAT threshold. In *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, pages 769–778, 2002.

[Kra01] Jan Krajíček. On the weak pigeonhole principle. *Fund. Math.*, 170(1-2):123–140, 2001. Dedicated to the memory of Jerzy Łoś.

[Raz15] Alexander A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Ann. Math. (2)*, 181(2):415–472, 2015.

[Rob65] John Alan Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12(1):23–41, 1965.

[SBI04] Nathan Segerlind, Sam Buss, and Russell Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. *SIAM J. Comput.*, 33(5):1171–1200, May 2004.