

Resolution Lower Bounds for Refutation Statements

Michal Garlík*

Dept. Ciències de la Computació
Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3
08034 Barcelona, Spain
email: mgarlik@cs.upc.edu

May 25, 2019

Abstract

For any unsatisfiable CNF formula we give an exponential lower bound on the size of resolution refutations of a propositional statement that the formula has a resolution refutation. We describe three applications. (1) An open question in [2] asks whether a certain natural propositional encoding of the above statement is hard for Resolution. We answer by giving an exponential size lower bound. (2) We show exponential resolution size lower bounds for reflection principles, thereby improving a result in [1]. (3) We provide new examples of CNFs that exponentially separate Res(2) from Resolution (an exponential separation of these two proof systems was originally proved in [9]).

1 Introduction

Proving lower bounds on the size of propositional proofs is the central task of proof complexity theory. After Cook and Reckhow [4] motivated this line of research as an approach towards establishing $NP \neq coNP$, some initial success for weak proof systems followed, e.g., the first exponential size lower bound for Resolution was proved by Haken [5]. Nevertheless, many important open problems from the 1980s and 1990s remain unsolved, and it seems that proving nontrivial lower bounds on the size of propositional proofs is hard. If it is hard for people, it is natural to ask if it is also hard for the proof systems themselves. In trying to formalize this question so that it makes sense to a proof system, we must say what we mean by ‘proving is hard’. It can be ‘there are no short proofs’, a statement which occurs as a part of reflection principles. By ‘short’ we mean polynomial in the size of the formula being proven or refuted. The negation of the *reflection principle* for a proof system P is a conjunction of the statement ‘ y is a P -refutation of length s of formula x of length n ’ and the statement ‘ z is a satisfying

*Funded by European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme, grant agreement ERC-2014-CoG 648276 (AUTAR).

assignment of formula x' . In a propositional formulation of the principle, P, s, n are fixed parameters and x, y, z are disjoint sets of variables. A possible way to formalize the above question is then to take the first conjunct of the negation of the reflection principle and plug in for the x -variables some formula F of length n . The resulting formula was discussed and utilized by Pudlák [8]; we denote it by $\text{REF}_{P,s}^F$ and call it a *refutation statement* for P . We may now ask whether some proof system Q can shortly refute $\text{REF}_{P,s}^F$, and if it can not, we can interpret this to mean that lower bounds for P -refutations of F are hard for Q .

Pudlák [8] found connections between the reflection principles and automatizability, and these were elaborated on in [1]. Following [3], a proof system P is *automatizable* if there is a deterministic algorithm that when given as input an unsatisfiable CNF formula F outputs its P -refutation in time polynomial in the size of the shortest P -refutation of F . Recently, Atserias and Müller [2] showed that Resolution is not automatizable unless $P = \text{NP}$. Refutation statements for Resolution play a prominent role in their proof. They show that strong enough resolution size lower bounds for $\text{REF}_{\text{Res},s}^F$ with an unsatisfiable F imply their result. However, they leave the lower bound problem for $\text{REF}_{\text{Res},s}^F$ as an open question, and in place of $\text{REF}_{\text{Res},s}^F$ they use in the proof a different formulation of the refutation statement, obtained by a *relativization* of $\text{REF}_{\text{Res},s}^F$, for which lower bounds are easier to get. In this paper we focus mainly on giving an answer to the question.

1.1 Results in This Paper

The result that requires the most work is the following lower bound.

Theorem 1. *For each $\epsilon > 0$ there is $\delta > 0$ and an integer t_0 such that if n, r, s, t are integers satisfying $t \geq s \geq n + 1$, $r \geq n \geq 2$, $t \geq r^{3+\epsilon}$, $t \geq t_0$, and F is an unsatisfiable CNF consisting of r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n , then any resolution refutation of $\text{REF}_{s,t}^F$ has length greater than 2^{t^δ} .*

Here $\text{REF}_{s,t}^F$, missing the lower index denoting the proof system as we concentrate on resolution refutation statements, is a variant of the refutation statement insisting that the resolution refutation it describes has the form of a levelled graph. A similar simplifying assumption, making it more practical to design random restrictions, is used in [10] for a propositional version of the coloured polynomial local search principle. Our proof proceeds with defining a random restriction tailored to $\text{REF}_{s,t}^F$ and to an adversary argument. The nature of the refutation statement and the fact that the relations between refutation lines are encoded in unary, rather than in binary, necessitate a more complicated adversary argument than in [7] or [10], and this in turn poses more requirements on the random restriction. We discuss these details after the proof, in Remarks 20 and 21.

We then show that Theorem 1 implies an exponential resolution size lower bound for the encoding of the refutation statement for which the lower bound question in [2] is originally asked.

We see two reasons for working with the unary encoding of $\text{REF}_{s,t}^F$. First, $\text{REF}_{s,t}^F$ is weaker than refutation statements encoded in binary or relativized refutation statements. Hence lower bounds for $\text{REF}_{s,t}^F$ imply lower bounds for the other encodings. Second, researchers who dealt with propositional encodings of reflection principles or refutation statements opted for the unary encoding [1, 6, 8].

Our next result is that the negation of the reflection principle for Resolution, expressed by the formula $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$, exponentially separates the system Res(2) from Resolution. It was shown by Atserias and Bonnet [1] that a similar encoding of the negation of the reflection principle separates the two theories almost-exponentially (giving a $2^{\Omega(2^{\log^c n})}$ resolution lower bound and a polynomial Res(2) upper bound). The exponential separation of Res(2) from Resolution was originally proved in [9] using a variation of the graph ordering principle. Our lower bound is stated in Theorem 2 below.

Theorem 2. *For every $c > 4$ there is $\delta > 0$ and an integer n_0 such that if n, r, s, t are integers satisfying $t \geq s \geq n + 1$, $r \geq n \geq n_0$, $n^c \geq t \geq r^4$, then any resolution refutation of $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ has length greater than 2^{n^δ} .*

The proof of the theorem also yields new examples of CNFs exponentially separating Res(2) from Resolution.

Theorem 3. *Let $\delta_1 > 0$ and let $\{A_n\}_{n \geq 1}$ be a family of unsatisfiable CNFs such that A_n is in n variables, has the number of clauses polynomial in n , and has no resolution refutations of length at most $2^{n^{\delta_1}}$. Then there is $\delta > 0$ and a polynomial p such that $A_n \wedge \text{REF}_{n+1, p(n)}^{A_n}$ has no resolution refutations of length at most 2^{n^δ} and has polynomial size Res(2) refutations.*

A Res(2) upper bound for $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$, needed for completing the separation by this formula as well as by the formulas in Theorem 3, is stated in the following theorem.

Theorem 4. *The negation of the reflection principle for Resolution expressed by the formula $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ has Res(2) refutations of size $O(trn^2 + tr^2 + st^2n^3 + st^3n)$.*

A polynomial size Res(2) upper bound on a similar encoding of the negation of the reflection principle for Resolution was proved in [1]. We simplify the proof and adapt it to $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$.

1.2 Outline of the Paper

The rest of the paper is organized as follows.

In Section 2 we give the necessary preliminaries.

In Section 3, Resolution of s levels of t clauses is introduced, and the clauses of the refutation statement $\text{REF}_{s,t}^F$ for this refutation system are listed. We show that this system simulates Resolution with at most quadratic increase in length.

In Section 4 we prove Theorem 1. That Theorem 1 also answers the original lower bound question from [2] is shown in Appendix A.

In Section 5 we define the formula $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ and we prove Theorems 2 and 3.

In Section 6 we prove Theorem 4.

2 Preliminaries

For an integer s , the set $\{1, \dots, s\}$ is denoted by $[s]$. We write $\text{dom}(\sigma), \text{im}(\sigma)$ for the domain and image of a function σ . Two functions σ, τ are *compatible* if $\sigma \cup \tau$ is a function. If x is a propositional variable, the *positive literal* of x , denoted by x^1 , is x , and the *negative literal* of x , denoted by x^0 , is $\neg x$. A *clause* is a set of literals. A clause is written as a disjunction of its elements. A *term* is a set of literals, and is written as

a conjunction of the literals. A *CNF* is a set of clauses, written as a conjunction of the clauses. A *k-CNF* is a CNF whose every clause has at most k literals. A *DNF* is a set of terms, written as a disjunction of the terms. A *k-DNF* is a DNF whose every term has at most k literals. We will identify 1-DNFs with clauses. A clause is *non-tautological* if it does not contain both the positive and negative literal of the same variable. A clause C is a *weakening* of a clause D if $D \subseteq C$. A clause D is the *resolvent* of clauses C_1 and C_2 on a variable x if $x \in C_1, \neg x \in C_2$ and $D = (C_1 \setminus \{x\}) \cup (C_2 \setminus \{\neg x\})$. If E is a weakening of the resolvent of C_1 and C_2 on x , we say that E is obtained by the *resolution rule* from C_1 and C_2 , and we call C_1 and C_2 the *premises* of the rule.

Let F be a CNF and C a clause. A *resolution derivation* of C from F is a sequence of clauses $\Pi = (C_1, \dots, C_s)$ such that $C_s = C$ and for all $u \in [s]$, C_u is a weakening of a clause in F , or there are $v, w \in [u - 1]$ such that C_u is obtained by the resolution rule from C_v and C_w . A *resolution refutation* of F is a resolution derivation of the empty clause from F . The *length* of a resolution derivation $\Pi = (C_1, \dots, C_s)$ is s . For $u \in [s]$, the *height* of u in Π is the maximum h such that there is a subsequence $(C_{u_1}, \dots, C_{u_h})$ of Π in which $u_h = u$ and for each $i \in [h - 1]$, C_{u_i} is a premise of a resolution rule by which $C_{u_{i+1}}$ is obtained in Π . The *height* of Π is the maximum height of u in Π for $u \in [s]$.

A *partial assignment* to the variables x_1, \dots, x_n is a partial map from $\{x_1, \dots, x_n\}$ to $\{0, 1\}$. Let σ be a partial assignment. The CNF $F \upharpoonright \sigma$ is formed from F by removing every clause containing a literal satisfied by σ , and removing every literal falsified by σ from the remaining clauses. If $\Pi = (C_1, \dots, C_s)$ is a sequence of clauses, $\Pi \upharpoonright \sigma$ is formed from Π by the same operations. Note that if Π is a resolution refutation of F , then $\Pi \upharpoonright \sigma$ is a resolution refutation of $F \upharpoonright \sigma$.

The $\text{Res}(k)$ refutation system is a generalization of Resolution. Its lines are k -DNFs and it has the following inference rules (A, B are k -DNFs, $j \in [k]$, and l, l_1, \dots, l_j are literals):

$$\frac{A \vee l_1 \quad B \vee (l_2 \wedge \dots \wedge l_j)}{A \vee B \vee (l_1 \wedge \dots \wedge l_j)} \wedge\text{-introduction} \qquad \frac{}{x \vee \neg x} \text{Axiom}$$

$$\frac{A \vee (l_1 \wedge \dots \wedge l_j) \quad B \vee \neg l_1 \vee \dots \vee \neg l_j}{A \vee B} \text{Cut} \qquad \frac{A}{A \vee B} \text{Weakening}$$

Let F be a CNF. A *Res(k) derivation from F* is a sequence of k -DNFs (D_1, \dots, D_s) so that each D_i either belongs to F or follows from the preceding lines by an application of one of the inference rules. A *Res(k) refutation of F* is a $\text{Res}(k)$ derivation from F whose final line is the empty clause. The *size* of a $\text{Res}(k)$ derivation is the number of symbols in it.

3 Resolution Refutations of s Levels of t Clauses

We introduce a variant of Resolution in which the clauses forming a refutation are arranged in layers.

Definition 5. Let F be a CNF of r clauses in n variables x_1, \dots, x_n . We say that F has a *resolution refutation of s levels of t clauses* if there is a sequence of clauses $C_{i,j}$ indexed by all pairs $(i, j) \in [s] \times [t]$, such that each clause $C_{1,j}$ on the first level is a weakening of a clause in F , each clause $C_{i,j}$ on level $i \in [s] \setminus \{1\}$ is a weakening of the resolvent of two clauses from level $i - 1$ on a variable, and the clause $C_{s,t}$ is empty.

The following proposition shows that this system quadratically simulates Resolution and preserves the refutation height. The proof uses a simple self-replicating pattern both to transport a premise of the resolution rule to the required level and to fill in all clauses $C_{i,j}$ that do not directly participate in the simulation.

Proposition 6. *If a $(n - 1)$ -CNF F in n variables has a resolution refutation of height h and length s , then F has a resolution refutation of h levels of $3s$ clauses.*

Proof. Let Π be a resolution refutation of F of height h and length s . Assume that Π is (C_1, \dots, C_s) , and that without loss of generality C_j , $j \in [s]$, is non-tautological and either $C_j \in F$ or C_j is the resolvent of C_{j_1}, C_{j_2} for some $j_1, j_2 < j$. For $j \in [s]$, let h_j be the height of j in Π . We prove by induction on $s' \in [s]$ the following: There is a resolution derivation of $C_{s'}$ of h levels of $3s'$ clauses such that for each $j \in [s']$ and $i \in \{h_j, \dots, h\}$, $C_{i,3j} = C_j$.

Base step: $s' = 1$. Pick a variable x such that no literal of x is in C_1 . Such a variable exists by our assumptions. For all $i \in [h]$, set $(C_{i,1}, C_{i,2}, C_{i,3}) = (C_1 \cup \{x\}, C_1 \cup \{\neg x\}, C_1)$. This is a valid resolution derivation of h levels of 3 clauses: the clauses on the first level are weakenings of $C_1 \in F$, and each clause on any subsequent level is derived from the first and second clause of the previous level.

Induction step: Assume the statement holds for s' , as witnessed by a derivation Π' . We prove it for $s' + 1$. Pick a variable x such that no literal of x is in $C_{s'+1}$; it exists by our assumptions. If $C_{s'+1} \in F$, define, for each $i \in [h]$, $(C_{i,3s'+1}, C_{i,3s'+2}, C_{i,3s'+3}) = (C_{s'+1} \cup \{x\}, C_{s'+1} \cup \{\neg x\}, C_{s'+1})$. If $C_{s'+1}$ is obtained by the resolution rule in Π , the premises of the rule appear on level $h_{s'+1} - 1$ in Π' by the induction hypothesis. So we can extend Π' by defining, for $i \in \{h_{s'+1}, \dots, h\}$, $(C_{i,3s'+1}, C_{i,3s'+2}, C_{i,3s'+3}) = (C_{s'+1} \cup \{x\}, C_{s'+1} \cup \{\neg x\}, C_{s'+1})$. Next, for each $i \in [h_{s'+1} - 1]$, define $(C_{i,3s'+1}, C_{i,3s'+2}, C_{i,3s'+3}) = (C_1 \cup \{x\}, C_1 \cup \{\neg x\}, C_1)$. It is easy to check that this is a valid derivation and it satisfies the required properties. \square

We proceed to our formalization of the refutation statement for this refutation system. Let n, r, s, t be integers. Let F be a CNF consisting of r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n . We define a propositional formula $\text{REF}_{s,t}^F$ expressing that F has a resolution refutation of s levels of t clauses.

We first list the variables of $\text{REF}_{s,t}^F$. *D-variables* $D(i, j, \ell, b)$, $i \in [s]$, $j \in [t]$, $\ell \in [n]$, $b \in \{0, 1\}$, encode clauses $C_{i,j}$ as follows: $D(i, j, \ell, 1)$ (resp. $D(i, j, \ell, 0)$) means that the literal x_ℓ (resp. $\neg x_\ell$) is in $C_{i,j}$. *L-variables* $L(i, j, j')$ (resp. *R-variables* $R(i, j, j')$), $i \in [s] \setminus \{1\}$, $j, j' \in [t]$, say that $C_{i-1,j'}$ is a premise of the resolution rule by which $C_{i,j}$ is obtained, and it is the premise containing the positive (resp. negative) literal of the resolved variable. *V-variables* $V(i, j, \ell)$, $i \in [s] \setminus \{1\}$, $j \in [t]$, $\ell \in [n]$, say that $C_{i,j}$ is obtained by resolving on x_ℓ . *I-variables* $I(j, m)$, $j \in [t]$, $m \in [r]$, say that $C_{1,j}$ is a weakening of C_m .

$\text{REF}_{s,t}^F$ is the union of the following fifteen sets of clauses:

$$\neg I(j, m) \vee D(1, j, \ell, b) \qquad j \in [t], m \in [r], b \in \{0, 1\}, x_\ell^b \in C_m, \quad (1)$$

clause $C_{1,j}$ contains the literals of C_m assigned to it by $I(j, m)$,

$$\neg D(i, j, \ell, 1) \vee \neg D(i, j, \ell, 0) \qquad i \in [s], j \in [t], \ell \in [n], \quad (2)$$

no clause $C_{i,j}$ contains x_ℓ and $\neg x_\ell$ at the same time,

$$\neg L(i, j, j') \vee \neg V(i, j, \ell) \vee D(i-1, j', \ell, 1) \quad i \in [s] \setminus \{1\}, j, j' \in [t], \ell \in [n], \quad (3)$$

$$\neg R(i, j, j') \vee \neg V(i, j, \ell) \vee D(i-1, j', \ell, 0) \quad i \in [s] \setminus \{1\}, j, j' \in [t], \ell \in [n], \quad (4)$$

clause $C_{i-1,j'}$ used as the premise given by $L(i, j, j')$ (resp. $R(i, j, j')$) in resolving on x_ℓ must contain x_ℓ (resp. $\neg x_\ell$),

$$\begin{aligned} \neg L(i, j, j') \vee \neg V(i, j, \ell) \vee \neg D(i-1, j', \ell', b) \vee D(i, j, \ell', b) \\ i \in [s] \setminus \{1\}, j, j' \in [t], \ell, \ell' \in [n], b \in \{0, 1\}, (\ell', b) \neq (\ell, 1), \end{aligned} \quad (5)$$

$$\begin{aligned} \neg R(i, j, j') \vee \neg V(i, j, \ell) \vee \neg D(i-1, j', \ell', b) \vee D(i, j, \ell', b) \\ i \in [s] \setminus \{1\}, j, j' \in [t], \ell, \ell' \in [n], b \in \{0, 1\}, (\ell', b) \neq (\ell, 0), \end{aligned} \quad (6)$$

clause $C_{i,j}$ derived by resolving on x_ℓ must contain each literal different from x_ℓ (resp. $\neg x_\ell$) from the premise given by $L(i, j, j')$ (resp. $R(i, j, j')$),

$$\neg D(s, t, \ell, b) \quad \ell \in [n], b \in \{0, 1\}, \quad (7)$$

clause $C_{s,t}$ is empty,

$$V(i, j, 1) \vee V(i, j, 2) \vee \dots \vee V(i, j, n) \quad i \in [s] \setminus \{1\}, j \in [t], \quad (8)$$

$$I(j, 1) \vee I(j, 2) \vee \dots \vee I(j, r) \quad j \in [t], \quad (9)$$

$$L(i, j, 1) \vee L(i, j, 2) \vee \dots \vee L(i, j, t) \quad i \in [s] \setminus \{1\}, j \in [t], \quad (10)$$

$$R(i, j, 1) \vee R(i, j, 2) \vee \dots \vee R(i, j, t) \quad i \in [s] \setminus \{1\}, j \in [t], \quad (11)$$

$$\neg V(i, j, \ell) \vee \neg V(i, j, \ell') \quad i \in [s] \setminus \{1\}, j \in [t], \ell, \ell' \in [n], \ell \neq \ell', \quad (12)$$

$$\neg I(j, m) \vee \neg I(j, m') \quad j \in [t], m, m' \in [r], m \neq m', \quad (13)$$

$$\neg L(i, j, j') \vee \neg L(i, j, j'') \quad i \in [s] \setminus \{1\}, j, j', j'' \in [t], j' \neq j'', \quad (14)$$

$$\neg R(i, j, j') \vee \neg R(i, j, j'') \quad i \in [s] \setminus \{1\}, j, j', j'' \in [t], j' \neq j'', \quad (15)$$

the V, I, L, R -variables define functions with the required domains and ranges.

4 A Lower Bound on Lengths of Resolution Refutations of Resolution Refutation Statements

We restate Theorem 1 from the Introduction.

Theorem 7. *For each $\epsilon > 0$ there is $\delta > 0$ and an integer t_0 such that if n, r, s, t are integers satisfying*

$$t \geq s \geq n + 1, \quad r \geq n \geq 2, \quad t \geq r^{3+\epsilon}, \quad t \geq t_0, \quad (16)$$

and F is an unsatisfiable CNF consisting of r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n , then any resolution refutation of $\text{REF}_{s,t}^F$ has length greater than 2^{t^δ} .

The rest of this section is devoted to a proof of the theorem. We argue by contradiction. Fix $\epsilon > 0$ and assume that for each $\delta > 0$ and t_0 there are integers n, r, s, t satisfying (16), an unsatisfiable CNF F , and a resolution refutation Π of $\text{REF}_{s,t}^F$, such

that F consists of r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n , and Π has length at most 2^{t^δ} .

The forthcoming distribution on partial assignments to the variables of $\text{REF}_{s,t}^F$ employs in its definition and analysis two important parameters, p and w . We choose them in function of t and ϵ as follows:

$$p = t^{-a} \text{ with } a = \min \left\{ \frac{2 + \epsilon/2}{3 + \epsilon/2}, \frac{3}{4} \right\}, \quad w = t^{4/5}.$$

We now fix values of t_0, δ for which we will get the desired contradiction. Take t_0 so large and $\delta > 0$ so small that the inequalities

$$\max \left\{ e^{-\frac{pw}{3}} + 2s \cdot e^{-\frac{pt}{3}}, e^{-\frac{pt}{8r}} \right\} \cdot 2^{t^\delta} + 3s \cdot e^{-\frac{pt}{3}} + 3p + 67p^3st < 1, \quad (17)$$

$$10pt + 4w < \frac{t}{4}, \quad (18)$$

$$e^{e^{\ln(t) - \frac{pt}{3}}} < 2, \quad (19)$$

hold for any n, r, s, t satisfying (16).

Definition 8. For $i \in [s], j, j' \in [t], \ell \in [n], b \in \{0, 1\}, m \in [r]$, we say that (i, j) is the *home pair* of the variable $D(i, j, \ell, b)$ (resp. $R(i, j, j')$; $L(i, j, j')$; $V(i, j, \ell')$; $I(j, m)$ if $i = 1$).

We write $V(i, j, \cdot)$ to stand for the set $\{V(i, j, \ell) : \ell \in [n]\}$. Similarly, we write $I(j, \cdot), L(i, j, \cdot), R(i, j, \cdot)$ to stand for the corresponding sets of variables, and we denote by $D(i, j, \cdot, \cdot)$ the set of variables $\{D(i, j, \ell, b) : \ell \in [n], b \in \{0, 1\}\}$.

Let σ be a partial assignment. We say that $V(i, j, \cdot)$ is *set to ℓ by σ* if $\sigma(V(i, j, \ell)) = 1$ and $\sigma(V(i, j, \ell')) = 0$ for all $\ell' \in [n], \ell' \neq \ell$. Similarly for $I(j, \cdot), L(i, j, \cdot), R(i, j, \cdot)$. We say that $D(i, j, \cdot, \cdot)$ is *set to a clause $C_{i,j}$ by σ* if for all $\ell \in [n], b \in \{0, 1\}$, $\sigma(D(i, j, \ell, b)) = 1$ if $x_\ell^b \in C_{i,j}$ and $\sigma(D(i, j, \ell, b)) = 0$ if $x_\ell^b \notin C_{i,j}$.

For $Y \in \{D(i, j, \cdot, \cdot), V(i, j, \cdot), I(j, \cdot), R(i, j, \cdot), L(i, j, \cdot)\}$, we say that Y is *set by σ* if Y is set to v by σ for some value v . We will often omit saying ‘‘by σ ’’ if σ is clear from the context.

Definition 9. A *random restriction* ρ is a partial assignment to the variables of $\text{REF}_{s,t}^F$ given by the following experiment:

1. For each pair $(i, j) \in [s] \times [t]$, with independent probability p include (i, j) in a set A_D . Then for each $(i, j) \in A_D$ and for each $\ell \in [n]$, independently, with probability $1/2$ choose between including the literal x_ℓ or $\neg x_\ell$ in a clause $C_{i,j}$. Set $D(i, j, \cdot, \cdot)$ to $C_{i,j}$.
2. For each $j \in [t]$, with independent probability p include the pair $(1, j)$ in a set A_I . Then for each $(1, j) \in A_I \setminus A_D$, independently, choose at random $m \in [r]$ and set $I(j, \cdot)$ to m .
3. For each pair $(i, j) \in \{2, \dots, s\} \times [t]$, with independent probability p include (i, j) in a set A_V . Then for each $(i, j) \in A_V$, independently, choose at random $\ell \in [n]$ and set $V(i, j, \cdot)$ to ℓ .

4. For each pair $(i, j) \in \{2, \dots, s\} \times [t]$, with independent probability p include the pair (i, j) in a set A_{RL} . Then, for each $i \in \{2, \dots, s\}$, define $A_i := A_{RL} \cap (\{i\} \times [t])$ and do the following. If $|A_i| > 2pt$, define $h_i := \emptyset$, $B_{i-1} := \emptyset$. Otherwise, choose at random an injection h_i from $\{L(i, j, \cdot) : (i, j) \in A_i\} \cup \{R(i, j, \cdot) : (i, j) \in A_i\}$ to $[t]$. Define $B_{i-1} := \{(i-1, j) : j \in \text{im}(h_i)\}$. Set $L(i, j, \cdot)$ to $h_i(L(i, j, \cdot))$ and $R(i, j, \cdot)$ to $h_i(R(i, j, \cdot))$ for all $(i, j) \in A_i$.

Lemma 10. *With probability at least $1 - 3s \cdot e^{-pt/3}$, all of the following are satisfied.*

- (i) *For each $i \in [s]$, the cardinality of $A_D \cap (\{i\} \times [t])$ is at most $2pt$.*
- (ii) *For each $i \in \{2, \dots, s\}$, the cardinality of A_i is at most $2pt$ and the cardinality of $A_V \cap (\{i\} \times [t])$ is at most $2pt$.*
- (iii) *The cardinality of A_I is at most $2pt$.*

Proof. By the Chernoff bound and the union bound it follows that item (i) is false with probability at most $s \cdot e^{-pt/3}$. Similarly for the remaining items. \square

Definition 11. Denote by G_ρ the graph with vertices $A_D \cup A_V \cup A_I \cup A_{RL} \cup \bigcup_{i \in [s-1]} B_i$, and with edges only between vertices on neighboring levels, such that (i, j) is connected by an edge to $(i-1, j')$ if and only if $h_i(L(i, j, \cdot)) = j'$ (then $(i-1, j')$ is called the *left child* of (i, j)) or $h_i(R(i, j, \cdot)) = j'$ (then $(i-1, j')$ is the *right child* of (i, j)).

The following lemma will be used later to show that a random restriction likely does not falsify any clause of $\text{REF}_{s,t}^F$.

Lemma 12. *With probability at least $1 - 3p - 67p^3st$, the following are both satisfied.*

- (i) $(s, t) \notin (A_D \cup A_{RL} \cup A_V)$.
- (ii) *There is no triple $((i_1, j_1), (i_2, j_2), (i_3, j_3))$ of elements of $[s] \times [t]$, such that all the following hold:*
 - (a) *For each $u \in [3]$ there is $X \in \{D, V, I, RL\}$ with $(i_u, j_u) \in A_X$,*
 - (b) $|\{(i_u, j_u, X) : u \in [3], X \in \{D, V, I, RL\}, (i_u, j_u) \in A_X\}| \geq 3$,
 - (c) *the subgraph of G_ρ consisting of the vertices that are in the triple and their children and all edges that go from a vertex of the triple to its children, is connected.*

Proof. The probability that item (i) is true is $(1-p)^3 \geq 1-3p$.

Regarding item (ii), we distinguish several cases based on the relative positions of the elements in a triple $((i_1, j_1), (i_2, j_2), (i_3, j_3))$. Note that the order in which the elements of the triple are listed does not matter in what we are proving, but some of the elements may coincide. When considering the cases, recall that due to our choice of the function h_i in the definition of ρ , two vertices in G_ρ cannot share a child.

In case all the elements of the triple are the same, (b) is satisfied only if the element is chosen to A_X for three distinct values of X . This cannot happen on level 1, and on the other levels it happens with probability p^3 . There are st many triples considered in the present case, so by the union bound the probability that there is any such triple satisfying all conditions in (ii) is at most p^3st .

In case $(i_1, j_1) \neq (i_2, j_2) = (i_3, j_3)$, condition (c) is satisfied only if $i_1 = i_2 + 1$ or $i_2 = i_1 + 1$. In each of these two subcases, there are at most st^2 such triples. In the former subcase, we must have $(i_1, j_1) \in A_{RL}$ and at the same time $h_{i_1}(R(i_1, j_1, \cdot)) = j_2$ or $h_{i_1}(L(i_1, j_1, \cdot)) = j_2$. This happens with probability at most $2p/t$. Also, (i_2, j_2) has to be in A_X and $A_{X'}$ for distinct X, X' , which happens with probability at most $3p^2$. So, the probability that any triple considered in this subcase satisfies (a) - (c) is at most $st^2 \cdot 6p^3/t = 6p^3st$. In the latter subcase, (i_2, j_2) has to be in A_{RL} , connected to (i_1, j_1) , and additionally it has to be in A_D or A_V , while (i_1, j_1) has to be in arbitrary possible A_X . This happens with probability at most $2p/t \cdot 2p \cdot 3p = 12p^3/t$, so the probability that any such triple satisfies (a) - (c) is at most $12p^3st$.

In case all the elements of the triple are distinct, we again consider two subcases: first, $i_1 = i_2 + 1 = i_3 + 2$, and second, $i_1 - 1 = i_2 = i_3$. Each subcase concerns at most st^3 triples. In the first subcase, (i_3, j_3) has to be a child of (i_2, j_2) , which in turn has to be a child of (i_1, j_1) , and (i_3, j_3) also has to be in arbitrary possible A_X . This happens with probability at most $12p^3/t^2$. Hence the probability that any such triple satisfies (a) - (c) is at most $12p^3st$. In the second subcase, (i_1, j_1) has to have children (i_2, j_2) and (i_3, j_3) , and each child has to be in some A_X for any suitable X . This happens with probability at most $2p/(t(t-1)) \cdot (3p)^2 = 18p^3/(t(t-1)) \leq 36p^3/t^2$. Hence the probability that any such triple satisfies (a) - (c) is at most $36p^3st$. \square

We now define some specific ways to measure a clause and we use them in the next lemma to describe how a clause simplifies under a restriction.

Definition 13. Let E be a clause in $\Pi \upharpoonright \rho$, and let $(i, j) \in [s] \times [t]$. If E contains a literal of a variable from $D(i, j, \cdot, \cdot)$ (resp. $R(i, j, \cdot)$; $L(i, j, \cdot)$; $V(i, j, \cdot)$; $I(j, \cdot)$ and $i = 1$), we say that the pair (i, j) is *D-mentioned* (resp. *R-mentioned*; *L-mentioned*; *V-mentioned*; *I-mentioned*) in E .

We say that pair (i, j) is *mentioned in E* if it is Z -mentioned in E for some $Z \in \{D, V, I, R, L\}$.

We say that (i, j) is *V-important* (resp. *L-important*; *R-important*; *I-important*) in E if E contains the negative literal of a variable in $V(i, j, \cdot)$ (resp. $L(i, j, \cdot)$; $R(i, j, \cdot)$; $I(j, \cdot)$ and $i = 1$) or if E contains at least $n/2$ (resp. $t/2$; $t/2$; $r/2$) positive literals of variables in $V(i, j, \cdot)$ (resp. $L(i, j, \cdot)$; $R(i, j, \cdot)$; $I(j, \cdot)$ and $i = 1$). A pair is *D-important in E* if it is D -mentioned in E .

Lemma 14. *With probability at least $1 - \max\left\{e^{-\frac{pw}{3}} + 2s \cdot e^{-\frac{pt}{3}}, e^{-\frac{pt}{8r}}\right\} \cdot 2t^\delta$, for every clause E in $\Pi \upharpoonright \rho$ all of the following are satisfied.*

- (i) *At most w many pairs (i, j) are D -mentioned in E .*
- (ii) *At most w many pairs $(1, j)$ are I -important in E .*
- (iii) *At most w many pairs (i, j) are V -important in E .*
- (iv) *At most w many pairs (i, j) are L -important in E .*
- (v) *At most w many pairs (i, j) are R -important in E .*
- (vi) *For each $m \in [r]$, $|\{j : I(j, m) \in E\}| \leq \frac{t}{4}$.*
- (vii) *For each $i \in \{s - n + 1, \dots, s - 1\}$ and $\ell \in [n]$, $|\{j : V(i, j, \ell) \in E\}| \leq \frac{t}{4}$.*

Proof. It is sufficient to prove that if E' is a clause in Π that violates any of (i) - (vii), then with probability at least $1 - \max\left\{e^{-\frac{pw}{3}} + 2s \cdot e^{-\frac{pt}{3}}, e^{-\frac{pt}{8r}}\right\}$, E' is satisfied by ρ . Since Π has length at most 2^{t^δ} , the lemma then follows by the union bound.

Regarding item (i), assume that E' in Π D -mentions more than w pairs (i, j) . This means that a literal of a variable in $D(i, j, \cdot, \cdot)$ is in E' for more than w many pairs (i, j) . For each such (i, j) , such a literal is satisfied by ρ with probability at least $p/2$. So the probability that none of these literals in E' is satisfied is at most $(1 - p/2)^w < e^{-pw/2}$.

Regarding item (ii), suppose that more than w pairs $(1, j)$ are I -important in E' . For each such $(1, j)$, the probability that $(1, j) \in A_I \setminus A_D$ is $p(1 - p)$, and provided this happens, the probability that ρ satisfies a literal in E' of a variable in $I(j, \cdot)$ is at least $\min\{(r - 1)/r, 1/2\} = 1/2$. Hence the probability that E' is not satisfied by ρ is at most $(1 - p(1 - p)/2)^w < (1 - p/3)^w < e^{-pw/3}$ (the first inequality follows from (18)).

Regarding item (iii), a calculation similar to that for (ii) gives that a clause E' in Π with more than w many V -important pairs (i, j) is not satisfied by ρ with probability at most $(1 - p/2)^w < e^{-pw/2}$.

Regarding item (iv), suppose that more than w many pairs (i, j) from $\{2, \dots, s\} \times [t]$ are L -important in E' . For each $i \in \{2, \dots, s\}$, assume without loss of generality that the set of pairs (i, j) that are L -important in E' is the set $\{(i, 1), \dots, (i, w_i)\}$; denote it by W_i . Note that the distribution of ρ does not change if we choose A_i and h_i in t many steps as follows. Start with $A_{i,0} = h_{i,0} = \emptyset$. At step $j = 1, 2, \dots, t$, first add (i, j) to $A_{i,j-1}$ with probability p to get $A_{i,j}$. Then, if $|A_{i,j}| \leq 2pt$ and $(i, j) \in A_{i,j}$, choose at random two distinct elements j', j'' from $[t] \setminus \text{im}(h_{i,j-1})$, and define $h_{i,j} := h_{i,j-1} \cup \{(L(i, j, \cdot), j'), (R(i, j, \cdot), j'')\}$. If $|A_{i,j}| \leq 2pt$ and $(i, j) \notin A_{i,j}$, define $h_{i,j} := h_{i,j-1}$. If $|A_{i,j}| > 2pt$ define $h_{i,j} := \emptyset$. This finishes step j . Finally, define $A_i := A_{i,t}$ and $h_i := h_{i,t}$.

For $i \in \{2, \dots, s\}$, let H_i be the set of literals in E' of a variable in $L(i, j, \cdot)$ for some $(i, j) \in W_i$. Also, for $(i, j) \in W_i$, let $T_{i,j}$ be the set of those $j' \in [t]$ such that the partial assignment given by setting $L(i, j, \cdot)$ to j' satisfies some literal in H_i . We know that $|T_{i,j}| \geq t/2$ for each $(i, j) \in W_i$.

The event that no literal in H_i is satisfied by ρ is a subset of the union of events (a) $|A_{i,t}| > 2pt$, and (b) $|A_{i,w_i}| \leq 2pt$ and for each $(i, j) \in A_{i,w_i}$, $h_{i,j}(L(i, j, \cdot)) \notin T_{i,j}$. Event (a) happens with probability at most $e^{-pt/3}$ by the Chernoff bound. We bound the probability of event (b). For each $j \in [w_i]$, if $(i, j) \in A_{i,j}$ and $|A_{i,j}| \leq 2pt$, then the probability that $h_{i,j}(L(i, j, \cdot)) \in T_{i,j}$ is at least $(|T_{i,j} \setminus \text{im}(h_{i,j-1})|)/t \geq (t/2 - 4pt)/t = (1 - 8p)/2 \geq 1/3$ (the last inequality follows from (18)). Therefore, denoting $l := \min\{2pt, w_i\}$, the probability of event (b) is at most

$$\sum_{k=0}^l \binom{w_i}{k} p^k (1 - p)^{w_i - k} \left(\frac{2}{3}\right)^k \leq \sum_{k=0}^{w_i} \binom{w_i}{k} \left(\frac{2p}{3}\right)^k (1 - p)^{w_i - k} = (1 - p/3)^{w_i}.$$

Thus, the probability that no literal in H_i is satisfied by ρ is at most $e^{-pt/3} + e^{-pw_i/3}$, and, denoting $S := \{i \in \{2, \dots, s\} : w_i \neq 0\}$, the probability that no literal in $\bigcup_{i \in S} H_i$ is

satisfied by ρ is at most

$$\begin{aligned}
\prod_{i \in S} \left(e^{-\frac{pw_i}{3}} + e^{-\frac{pt}{3}} \right) &\leq e^{-\frac{pw}{3}} + \sum_{k=1}^{|S|} \binom{|S|}{k} e^{-\frac{ptk}{3}} \\
&\leq e^{-\frac{pw}{3}} + |S| \cdot e^{-\frac{pt}{3}} \sum_{k=1}^{|S|} \binom{|S|-1}{k-1} e^{-\frac{pt(k-1)}{3}} \\
&= e^{-\frac{pw}{3}} + |S| \cdot e^{-\frac{pt}{3}} \cdot \left(1 + e^{-\frac{pt}{3}} \right)^{|S|-1} \\
&\leq e^{-\frac{pw}{3}} + s \cdot e^{-\frac{pt}{3}} \cdot e^{e^{\ln(t)} - \frac{pt}{3}} \leq e^{-\frac{pw}{3}} + 2s \cdot e^{-\frac{pt}{3}},
\end{aligned}$$

where the penultimate inequality follows from $|S| - 1 \leq s \leq t$, and the last inequality follows from (19).

Item (v) is handled in the same way as (iv).

Regarding item (vi), suppose that for some $m \in [r]$ there are more than $t/4$ of $I(j, m)$ in E' . Similarly to the case (ii), each such $I(j, m)$ is satisfied by ρ with independent probability at least $p(1-p)/r > p/(2r)$, so E' is not satisfied with probability at most $(1 - p/(2r))^{t/4} < e^{-pt/(8r)}$.

Item (vii) is treated similarly to (vi), with the resulting probability of not satisfying E' being $(1 - p/n)^{t/4} < e^{-pt/(4n)} < e^{-pt/(8r)}$, where the last inequality follows from (16). \square

By (17) and by Lemmas 10, 12, and 14, there is a restriction ρ satisfying all the assertions of the lemmas. Fix any such ρ .

Definition 15. A partial assignment σ to the variables of $\text{REF}_{s,t}^F$ is called an *admissible assignment* if it extends ρ and satisfies all the following conditions.

- (C1) For each $(i, j) \in [s] \times [t]$, $D(i, j, \cdot, \cdot)$ (resp. $V(i, j, \cdot)$, $I(j, \cdot)$, $L(i, j, \cdot)$, $R(i, j, \cdot)$) either is set to some clause (resp. some $\ell \in [n]$, some $m \in [r]$, some $j' \in [t]$, some $j' \in [t]$) by σ or contains no variable that is in $\text{dom}(\sigma)$.
- (C2) For each $(i, j) \in [s] \times [t]$, if $L(i, j, \cdot)$ or $R(i, j, \cdot)$ is set to some $j' \in [t]$, then both $D(i, j, \cdot, \cdot)$ and $D(i-1, j', \cdot, \cdot)$ are set.
- (C3) For each $(i, j) \in [s] \times [t]$, if $D(i, j, \cdot, \cdot)$ is set, then $V(i, j, \cdot)$ is set (if $i \in \{2, \dots, s\}$) or $I(j, \cdot)$ is set (if $i = 1$).
- (C4) For each $(i, j) \in [s] \times [t]$, if $D(i, j, \cdot, \cdot)$ is set to a clause $C_{i,j}$, then $C_{i,j}$ is non-tautological and has at least $\min\{s-i, n\}$ many literals. If $D(i, j, \cdot, \cdot)$ is set to a clause $C_{i,j}$ with less than n literals and $V(i, j, \cdot)$ is set to some $\ell \in [n]$, then none of the literals of x_ℓ is in $C_{i,j}$.
- (C5) If $D(s, t, \cdot, \cdot)$ is set, it is set to the empty clause.
- (C6) For each $j \in [t]$, if $D(1, j, \cdot, \cdot)$ and $I(j, \cdot)$ are set, then σ satisfies all clauses in (1) with this j .
- (C7) For each $i \in \{2, \dots, s\}$, $j, j' \in [t]$, if $L(i, j, \cdot)$ (resp. $R(i, j, \cdot)$) is set to j' and both $V(i, j, \cdot)$, $D(i-1, j', \cdot, \cdot)$ are set, then σ satisfies all clauses in (3) (resp. (4)) with these i, j, j' .

(C8) For each $i \in \{2, \dots, s\}, j, j' \in [t]$, if $L(i, j, \cdot)$ (resp. $R(i, j, \cdot)$) is set to j' and $V(i, j, \cdot), D(i, j, \cdot, \cdot), D(i-1, j', \cdot, \cdot)$ are set, then σ satisfies all clauses in (5) (resp. (6)) with these i, j, j' .

(C9) For each $i \in \{2, \dots, s\}$, the binary relation $h_{\sigma, i} := \{(Z(i, j, \cdot), j') : j, j' \in [t], Z \in \{L, R\}, \text{ and } Z(i, j, \cdot) \text{ is set to } j' \text{ by } \sigma\}$ is a partial injection from $\{Z(i, j, \cdot) : j \in [t], Z \in \{L, R\}\}$ to $[t]$.

We now prove that an admissible assignment cannot falsify a clause of $\text{REF}_{s,t}^F \upharpoonright \rho$ (Lemma 16), that admissible assignments exist (Lemma 17), and that if for a clause E in $\Pi \upharpoonright \rho$ there is an admissible assignment that falsifies a literal in E whenever it evaluates its variable and that evaluates each D - (resp. V -, I -, L -, R -) variable with a home pair D - (resp. V -, I -, L -, R -) important in E , then there is also an admissible assignment that does the same for at least one clause in $\Pi \upharpoonright \rho$ from which E was obtained by the resolution rule (Lemma 19). This is a contradiction, which concludes the proof of Theorem 7.

Lemma 16. *No clause in $\text{REF}_{s,t}^F \upharpoonright \rho$ is falsified by any admissible assignment.*

Proof. Let σ be an admissible assignment. It suffices to show that σ does not falsify any clause of $\text{REF}_{s,t}^F$. This is guaranteed for each clause from (1) by (C1), (C6); from (2) by (C1), (C4); from (3) and (4) by (C1), (C7); from (5) and (6) by (C1), (C8); from (7) by (C1), (C5); and from (8) - (15) by (C1). \square

Lemma 17. *There is an admissible assignment.*

Proof. We first verify that ρ satisfies the conditions of Definition 15 except possibly for (C2), (C3). Then we extend ρ by only assigning some D, V, I -variables to satisfy these remaining two conditions without violating the others.

Conditions (C1), (C4), (C6) and (C9) are satisfied by construction: for (C4) recall that for each $(i, j) \in [s] \times [t]$, if $D(i, j, \cdot, \cdot)$ is set to some clause by ρ then the clause has exactly n literals; for (C6) observe that its hypothesis is not satisfied by ρ ; and for (C9) note that $h_{\rho, i} = h_i$ for $i \in \{2, \dots, s\}$. Condition (C5) follows from item (i) of Lemma 12. Item (ii) of the same lemma implies that neither the hypothesis in (C7) nor the hypothesis in (C8) is met.

To extend ρ to an admissible assignment, we distinguish cases based on the isomorphism type of the component in G_ρ containing a pair for which (C2) or (C3) is not satisfied. By item (ii) of Lemma 12, there are only three types of components in G_ρ : 1) an isolated vertex, 2) a vertex with its two children and edges from the vertex to the children, and 3) two vertices with their children and edges from each of the two vertices to its children, such that one of the two vertices is a child of the other.

In case 1), let (i, j) be the isolated vertex. Only (C3) may be unsatisfied; assume this is the case. Recall again that whenever ρ sets $D(i, j, \cdot, \cdot)$ to some clause $C_{i,j}$, the clause contains n literals and is non-tautological. Now, if $i \in \{2, \dots, s\}$, set $V(i, j, \cdot)$ arbitrarily. For $i = 1$, since F is unsatisfiable, it must contain a clause C_m , for some $m \in [r]$, of which $C_{i,j}$ is a weakening. Set $I(j, \cdot)$ to m .

In case 2), since one of the three vertices of the component is in A_{RL} and its children are not, item (ii) of Lemma 12 implies that there is at most one triple (i, j, Y) such that (i, j) is a vertex of the three forming the component, $Y \in \{D(i, j, \cdot, \cdot), V(i, j, \cdot), I(j, \cdot)\}$, and Y is set by ρ . We set the remaining $D(i, j, \cdot, \cdot), V(i, j, \cdot), I(j, \cdot)$ for all vertices (i, j) of the component in any way that respects how Y is set, only uses clauses of n literals to assign to the vertices (to satisfy (C4)), and satisfies (C6), (C7), (C8) for these vertices.

In case 3), there are exactly two vertices of the component that are in A_{RL} , hence item (ii) of Lemma 12 implies that there is no triple (i, j, Y) such that (i, j) is a vertex of the component, $Y \in \{D(i, j, \cdot, \cdot), V(i, j, \cdot), I(j, \cdot)\}$, and Y is set by ρ . Hence we can set $D(i, j, \cdot, \cdot), V(i, j, \cdot), I(j, \cdot)$ for all vertices (i, j) of the component in any way that only uses clauses of n literals to assign to the vertices (to satisfy (C4)), and satisfies (C6), (C7), (C8) for these vertices.

Extending ρ for every component of G_ρ in this way satisfies (C1) - (C4), does not affect (C5) and (C9), and satisfies (C6), (C7), (C8) because whenever we assigned all literals of a clause in (1), (3), (4), (5), (6), we made sure the clause was satisfied. \square

Definition 18. For a partial assignment σ to the variables of $\text{REF}_{s,t}^F$ that satisfies (C1) and (C9) of Definition 15, denote by G_σ the graph with vertex set $\bigcup_{i \in [s-1]} \{(i, j) : j \in \text{im}(h_{\sigma, i+1})\} \cup \{(i, j) : (i, j) \text{ is the home pair of a variable in } \text{dom}(\sigma)\}$ and edges between $(i, j), (i', j') \in [s] \times [t]$ if and only if $i = i' + 1$ and $h_{\sigma, i}(L(i, j, \cdot)) = j'$ or $h_{\sigma, i}(R(i, j, \cdot)) = j'$.

Lemma 19. *Suppose that a clause E in $\Pi \upharpoonright \rho$ is obtained by the resolution rule from clauses E_0 and E_1 . Suppose further that there is an admissible assignment σ which satisfies both conditions*

- (i) every literal in E of a variable in $\text{dom}(\sigma)$ is falsified by σ ,
- (ii) for each $Z \in \{D, V, I, R, L\}$, each Z -variable with a home pair Z -important in E is in $\text{dom}(\sigma)$.

Then there is an admissible assignment τ and $b \in \{0, 1\}$ such that (i) and (ii) hold with τ in place of σ and E_b in place of E .

Proof. Let σ be an admissible assignment that satisfies (i) and (ii). We first subject σ to the following three-step cleanup process to obtain the minimal admissible sub-assignment σ_1 of σ that satisfies (i) and (ii).

Step 1: Remove from $\text{dom}(\sigma)$ each variable in $L(i, j, \cdot)$ (resp. $R(i, j, \cdot)$) that is not in $\text{dom}(\rho)$ such that (i, j) is not L -important (resp. R -important) in E . Denote by σ' the new partial assignment.

Step 2: Remove from $\text{dom}(\sigma')$ each variable in $D(i, j, \cdot, \cdot)$ that is not in $\text{dom}(\rho)$ such that (i, j) is not D -important in E and no edge in $G_{\sigma'}$ is incident to (i, j) . Denote by σ'' the new partial assignment.

Step 3: For each $(i, j) \in [s] \times [t]$, remove from $\text{dom}(\sigma'')$ each variable in $V(i, j, \cdot, \cdot)$ (resp. $I(j, \cdot)$ if $i = 1$) that is not in $\text{dom}(\rho)$ such that (i, j) is not V -important (resp. I -important) in E and $D(i, j, \cdot, \cdot)$ is not set by σ'' . Let σ_1 stand for the resulting partial assignment.

It is straightforward to check that that $\sigma', \sigma'', \sigma_1$ are admissible assignments (the order of the steps was chosen to maintain (C2) and (C3) satisfied during the process; (C1) follows since we always unassign variables in groups listed there, and the remaining conditions of Definition 15 cannot turn from being true to false by unassigning variables), and that they satisfy (i) and (ii). The three steps and the order of their execution ensure that σ_1 is the minimal admissible sub-assignment of σ satisfying (i) and (ii).

Let Q be the variable resolved on to obtain E from E_0 and E_1 . Suppose that Q is a Z -variable, $Z \in \{D, V, I, L, R\}$, with a home pair $(i, j) \in [s] \times [t]$.

If $Q \in \text{dom}(\sigma_1)$, then σ_1 with either E_0 or E_1 already satisfy (i) and (ii).

If $Q \notin \text{dom}(\sigma_1)$ and (i, j) is not Z -important in $E \cup \{Q\}$, then (i, j) cannot be Z -important in E_b either, where $b \in \{0, 1\}$ is such that $Q \in E_b$, and therefore σ_1 with E_b already satisfy (i) and (ii).

Otherwise, we have that $Q \notin \text{dom}(\sigma_1)$ and (i, j) is Z -important in $E \cup \{Q\}$. It is enough to show how to extend σ_1 to an admissible assignment τ which assigns a value to Q such that (i) and (ii) are satisfied with τ in place of σ and $E \cup \{Q^{1-\tau(Q)}\}$ in place of E .

Observe that (i, j) is not Z -important in E . This is because σ_1 with E satisfy (ii) and $Q \notin \text{dom}(\sigma_1)$. We consider three cases.

Case 1. Suppose that $Q \in V(i, j, \cdot)$ (resp. $Q \in I(j, \cdot)$ and $i = 1$). Because (i, j) is not V - (resp. I -) important in E , there are less than $n/2$ (resp. $r/2$) positive and no negative literals of variables from $V(i, j, \cdot)$ (resp. $I(j, \cdot)$) in E . Pick any $\ell \in [n]$ such that $V(i, j, \ell) \notin E \cup \{Q\}$ (resp. any $m \in [r]$ such that $I(j, m) \notin E \cup \{Q\}$) and extend σ_1 to τ by setting $V(i, j, \cdot)$ to ℓ (resp. $I(j, \cdot)$ to m). This choice makes τ with $E \cup \{Q\}$ satisfy (i) and (ii). From the construction and the fact that σ_1 is an admissible assignment it follows that τ is too. In particular, to see that (C4) - (C8) are satisfied by τ , note that since σ_1 satisfies (C2), (C3) and $Q \notin \text{dom}(\sigma_1)$, no variable from $D(i, j, \cdot, \cdot)$ is in $\text{dom}(\sigma_1)$ (and hence is not in $\text{dom}(\tau)$ either), and there is no edge in G_{σ_1} incident to (i, j) (and hence there is no such edge in G_τ either).

Case 2. Suppose that $Q \in D(i, j, \cdot, \cdot)$. Since (i, j) is not D -important in E , no literal of a variable from $D(i, j, \cdot, \cdot)$ is in E . Because σ_1 satisfies (C2) and $Q \notin \text{dom}(\sigma_1)$, there is no edge of G_{σ_1} incident to (i, j) . But $V(i, j, \cdot)$ (resp. $I(j, \cdot)$ if $i = 1$) may be set by σ_1 . If $(i, j) \in \{2, \dots, s\} \times [t]$, set $D(i, j, \cdot, \cdot)$ to an arbitrary non-tautological clause with n literals, unless $(i, j) = (s, t)$, in which case set $D(i, j, \cdot, \cdot)$ to the empty clause. Then, set $V(i, j, \cdot)$, unless it is already set by σ_1 , to any value $\ell \in [n]$ such that $V(i, j, \ell) \notin E$. Such ℓ exists, because if $V(i, j, \cdot)$ is not set by σ_1 then (i, j) is not V -important in E , and hence there are more than $n/2$ available values to choose ℓ from. If $i = 1$, either $I(j, \cdot)$ is set by σ_1 to some $m \in [r]$ and we set $D(1, j, \cdot, \cdot)$ to any non-tautological clause with n literals that contains the literals of C_m , or $I(j, \cdot)$ is not set by σ_1 , in which case we first set it to any $m \in [r]$ such that $I(j, m) \notin E$ and then we set $D(1, j, \cdot, \cdot)$ as before; such m exists because if $I(j, \cdot)$ is not set by σ_1 then $(1, j)$ is not I -important in E , and hence there are more than $r/2$ available values to choose m from. Like in the previous case, it is easy to check that in each of the subcases considered we extended σ_1 to an admissible assignment τ such that τ with $E \cup \{Q^{1-\tau(Q)}\}$ satisfy (i) and (ii).

Case 3. Suppose that $Q \in L(i, j, \cdot)$ (if $Q \in R(i, j, \cdot)$ we proceed in a completely analogous way). We may assume that $V(i, j, \cdot)$ is set to some clause $C_{i,j}$ and $D(i, j, \cdot, \cdot)$ is set to some $\ell \in [n]$ by σ_1 ; if not, perform the steps in Case 2 to set them both. We have to set $L(i, j, \cdot)$ to some j' , i.e., we have to add to G_{σ_1} an edge from (i, j) to a left child $(i-1, j')$, and the first set U_1 of pairs $(i-1, j')$ we would like to avoid are the vertices of G_{σ_1} . To upper bound the number of vertices of its subgraph G_ρ that are on level $i-1$, we use items (i) - (iii) of Lemma 10. According to these items, G_ρ has on level $i-1$: at most $|A_{i-1}| \leq 2pt$ endpoints of edges between levels $i-1$ and $i-2$, further, at most $|B_{i-1}| = 2|A_i| \leq 4pt$ endpoints of edges between levels i and $i-1$, and at most $|A_D| + |A_V| \leq 4pt$ (or $|A_D| + |A_I| \leq 4pt$ if $i-1 = 1$) isolated vertices. To upper bound the number of vertices in G_{σ_1} on level $i-1$ that are not in G_ρ , note that by the minimality of σ_1 , each such vertex either is or shares an edge with a Z' -important pair in E for some $Z' \in \{D, V, I, R, L\}$. By items (i) - (v) of Lemma 14, there are at most $4w$ pairs that can in this way give rise to a vertex in G_{σ_1} on level $i-1$ that is not in G_ρ . Hence

$$|U_1| \leq 10pt + 4w.$$

The second set U_2 of pairs $(i-1, j')$ we would like to avoid when looking for a suitable left child of (i, j) are those with $L(i, j, j') \in E$ (because we want τ to satisfy (i)). Because (i, j) is not L -important in E , we have $|U_2| < t/2$.

The third set U_3 of pairs $(i-1, j')$ we would like the left child of (i, j) to avoid depends on whether $i = 2$ or $i \in \{3, \dots, s\}$. If $i = 2$, since σ_1 satisfies (C4), we know that $C_{2,j}$ has at least $n-1$ literals (because $s \geq n+1$) and that the clause at the left child of $(2, j)$ is completely determined by $C_{2,j}$ (because we want τ to satisfy (C4)): it is the clause $(C_{2,j} \setminus \{\neg x_\ell\}) \cup \{x_\ell\}$. Pick some $m \in [r]$ such that the clause C_m of F is a subset of $(C_{2,j} \setminus \{\neg x_\ell\}) \cup \{x_\ell\}$. For some $j' \in [t]$, we want to set $D(i-1, j', \cdot, \cdot)$ to $(C_{2,j} \setminus \{\neg x_\ell\}) \cup \{x_\ell\}$ and $I(j', \cdot)$ to m by τ (in order to satisfy (C6)), but this is not possible if $I(j', m) \in E$. For this reason, in the case $i = 2$ we define $U_3 := \{(1, j') : I(j', m) \in E\}$. By item (vi) of Lemma 14, $|U_3| \leq t/4$.

If $i \in \{3, \dots, s\}$, we are concerned with the case that $C_{i,j}$ has less than $n-1$ literals; otherwise we leave U_3 empty. Since σ_1 satisfies (C4), no literal of x_ℓ is in $C_{i,j}$, and $C_{i,j}$ has at least $s-i$ literals. Pick some $\ell' \in [n]$ such that no literal of $x_{\ell'}$ is in $C_{i,j} \cup \{x_\ell\}$. For some $j' \in [t]$, we want to set $D(i-1, j', \cdot, \cdot)$ to $C_{i,j} \cup \{x_\ell\}$ and $V(i-1, j')$ to ℓ' (to make τ satisfy (C4)). But this is not possible to do if $V(i-1, j', \ell') \in E$. Therefore, in the case $i \in \{3, \dots, s\}$ we define $U_3 := \{(i-1, j') : V(i-1, j', \ell') \in E\}$. Thanks to item (vii) of Lemma 14, we have $|U_3| \leq t/4$ again.

Now set $L(i, j, \cdot)$ to j' such that $(i-1, j') \notin U_1 \cup U_2 \cup U_3$. Such j' exists because $|U_1 \cup U_2 \cup U_3| \leq 10pt + 4w + t/2 + t/4 < t$ by (18). Also, set $D(i-1, j', \cdot, \cdot)$ and either $I(j', \cdot)$ (if $i = 2$) or $V(i-1, j', \cdot)$ (if $i \in \{3, \dots, s\}$) as indicated at the definition of U_3 . In the case where we left U_3 empty, set $D(i-1, j', \cdot, \cdot)$ to $(C_{i,j} \setminus \{\neg x_\ell\}) \cup \{x_\ell\}$ and set $V(i-1, j', \cdot)$ to any $\ell' \in [n]$ such that $V(i-1, j', \ell') \notin E$; such ℓ' exists because $(i-1, j')$ is not V -important in E (by avoiding U_1). This finishes the definition of τ . Item (ii) is satisfied by τ and $E \cup \{Q^{1-\tau(Q)}\}$ because $D(i, j, \cdot, \cdot)$ is set by τ . Item (i) follows for the variables in $D(i, j, \cdot, \cdot)$, $V(i, j, \cdot)$ because we set them using Case 2; for the variables in $L(i, j, \cdot)$ because $(i-1, j') \notin U_2$; and for the variables in $D(i-1, j', \cdot, \cdot)$, $V(i-1, j', \cdot)$, $I(j', \cdot)$ by avoiding U_3 and because $(i-1, j')$ is neither D - nor V - nor I -important in E (due to avoiding U_1). Finally, τ is an admissible assignment: the reasons why (C4) and (C6) are satisfied at $(i-1, j')$ are given at the definition of U_3 , and the remaining conditions are easy to check due to avoiding U_1 . \square

Remark 20. If we assume $s = n+1$ in Theorem 7 (instead of assuming only $s \geq n+1$) then we can allow t to be smaller: it is enough to assume that $t \geq r^{2+\epsilon}$. This can be useful if one wants to reduce the number of variables of $\text{REF}_{s,t}^F$ while keeping the lower bound of the theorem valid. The latter can be showed by making only the following modification in the proof of Theorem 7: change the definition of p to $p = s^{-1/3}t^{-a'}$ with $a' = \min\{\frac{1+\epsilon}{3+\epsilon}, \frac{1}{2}\}$, and change the definition of w to $w = s^{1/3}t^{3/5}$.

We note that if in the definition of $\text{REF}_{s,t}^F$ we encode the functions determined by V - and I -variables in binary instead of in unary, the assumption $t \geq r^{3+\epsilon}$ in Theorem 7 is not necessary (and the proof of the theorem simplifies somewhat), and, in addition, the L - and R -variables can be encoded in binary too (with some further simplifications of the proof). This reduces the number of variables of $\text{REF}_{s,t}^F$ in two ways, by allowing a smaller t and by using a more efficient encoding.

Remark 21. Most of the obstacles our proof has to overcome are caused by the nature of the object described by $\text{REF}_{s,t}^F$ and by the fact that the functions determined by V, I, L, R -

variables are encoded in unary, rather than in binary. This forces us to work with several notions of width of two kinds, and we cannot keep as an invariant of the maintained partial assignment that it falsifies all literals of a clause as we traverse the refutation (as is the case e.g. in [10]). Moreover, keeping falsified just the literals with important indices and adding some simple conditions about not directly falsifying an axiom (a method which works e.g. in [7] for the pigeonhole principle) is not enough either, because we need to be prepared to consistently answer the prover's questions about clauses situated at remote parts of the same not too small component (learnt through the L - and R -variables). This is further complicated by the need to respond by adding a fresh literal to a clause that has too few literals to make sure its width grows fast enough (such clauses originate in the component of the empty clause), and by the necessity to arrive to a weakening of a clause in F when asked how a clause on level 2 is derived; both are more difficult to meet under the unary encoding and pose specific requirements on random restrictions. Our strategy stores some useful information in the form of negating some other literals than just those with important indices in a clause, as can be seen in the hierarchy of setting of variables of different kinds in Definition 15.

5 Reflection Principle for Resolution

We express the negation of the reflection principle for Resolution by a CNF in the form of a conjunction $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$. The only shared variables by the formulas $\text{SAT}^{n,r}$ and $\text{REF}_{s,t}^{n,r}$ encode a CNF with r clauses in n variables. The meaning of $\text{SAT}^{n,r}$ is that the encoded CNF is satisfiable, while the meaning of $\text{REF}_{s,t}^{n,r}$ is that it has a resolution refutation of s levels of t clauses. A formal definition is given next.

Formula $\text{SAT}^{n,r}$ has the following variables. *C-variables* $C(m, \ell, b)$, $m \in [r], \ell \in [n], b \in \{0, 1\}$, encode clauses C_m as follows: $C(m, \ell, 1)$ (resp. $C(m, \ell, 0)$) means that the literal x_ℓ (resp. $\neg x_\ell$) is in C_m . *T-variables* $T(\ell)$, $\ell \in [n]$, and $T(m, \ell, b)$, $m \in [r], \ell \in [n], b \in \{0, 1\}$, encode that an assignment to variables x_1, \dots, x_n satisfies the CNF $\{C_1, \dots, C_r\}$. The meaning of $T(\ell)$ is that the literal x_ℓ is satisfied by the assignment. The meaning of $T(m, \ell, 1)$ (resp. $T(m, \ell, 0)$) is that clause C_m is satisfied through the literal x_ℓ (resp. $\neg x_\ell$).

We list the clauses of $\text{SAT}^{n,r}$:

$$T(m, 1, 1) \vee T(m, 1, 0) \vee \dots \vee T(m, n, 1) \vee T(m, n, 0) \quad m \in [r], \quad (20)$$

$$\neg T(m, \ell, 1) \vee T(\ell) \quad m \in [r], \ell \in [n], \quad (21)$$

$$\neg T(m, \ell, 0) \vee \neg T(\ell) \quad m \in [r], \ell \in [n], \quad (22)$$

$$\neg T(m, \ell, b) \vee C(m, \ell, b) \quad m \in [r], \ell \in [n], b \in \{0, 1\}. \quad (23)$$

The meaning of (20) is that clause C_m is satisfied through at least one literal. The meaning of (21) and (22) is that if C_m is satisfied through a literal, then the literal is satisfied. The meaning of (23) is that if C_m is satisfied through a literal, then it contains the literal.

Variables of $\text{REF}_{s,t}^{n,r}$ are the variables $C(m, \ell, b)$ of $\text{SAT}^{n,r}$ together with all the variables of $\text{REF}_{s,t}^F$ for some (and every) F of r clauses in n variables. That is, $\text{REF}_{s,t}^{n,r}$ has the following variables: $C(m, \ell, b)$ for $m \in [r], \ell \in [n], b \in \{0, 1\}$; $D(i, j, \ell, b)$ for $i \in [s], j \in [t], \ell \in [n], b \in \{0, 1\}$; $R(i, j, j')$ and $L(i, j, j')$ for $i \in [s] \setminus \{1\}, j, j' \in [t]$; $V(i, j, \ell)$ for $i \in [s] \setminus \{1\}, j \in [t], \ell \in [n]$; $I(j, m)$ for $j \in [t], m \in [r]$.

The clauses of $\text{REF}_{s,t}^{n,r}$ are (2) - (15) of $\text{REF}_{s,t}^F$ together with the following clauses (to replace clauses (1)):

$$\neg I(j, m) \vee \neg C(m, \ell, b) \vee D(1, j, \ell, b) \quad j \in [t], m \in [r], \ell \in [n], b \in \{0, 1\}, \quad (24)$$

saying that if clause $C_{1,j}$ is a weakening of clause C_m , then the former contains each literal of the latter. So the difference from (1) is that C_m is no longer a clause of some fixed formula F , but it is described by C -variables.

Lemma 22. *Let F be a CNF with r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n , and let γ_F be an assignment such that its domain are all C -variables and $\gamma_F(C(m, \ell, b)) = 1$ if $x_\ell^b \in C_m$ and $\gamma_F(C(m, \ell, b)) = 0$ if $x_\ell^b \notin C_m$. There is a substitution τ that maps the variables of $\text{SAT} \upharpoonright \gamma_F$ to $\{0, 1\} \cup \{x_\ell^b : \ell \in [n], b \in \{0, 1\}\}$ such that $(\text{SAT} \upharpoonright \gamma_F) \upharpoonright \tau$ is F together with some tautological clauses.*

Proof. Define τ as follows. If $\gamma_F(C(m, \ell, b)) = 0$, then $\tau(T(m, \ell, b)) = 0$. This satisfies (21) - (23) and deletes $T(m, \ell, b)$ from (20). If $\gamma_F(C(m, \ell, b)) = 1$, then (23) has been satisfied and we define $\tau(T(m, \ell, b)) = x_\ell^b$ and $\tau(T(\ell)) = x_\ell$. This choice turns (21) - (22) into a tautological clauses and correctly substitutes the remaining literals of (20) to yield the clause C_m of F . \square

A polynomial size $\text{Res}(2)$ upper bound for $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$, is proved in Section 6. We now prove the lower bound, stated in the introduction as Theorem 2 and restated below as Theorem 23.

Theorem 23. *For every $c > 4$ there is $\delta > 0$ and an integer n_0 such that if n, r, s, t are integers satisfying*

$$t \geq s \geq n + 1, \quad r \geq n \geq n_0, \quad n^c \geq t \geq r^4, \quad (25)$$

then any resolution refutation of $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ has length greater than 2^{n^δ} .

Proof. Fix $c > 4$. We first observe that if Π is a resolution refutation of $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ and γ is a partial assignment such that its domain are all C -variables, then $\Pi \upharpoonright \gamma$ is either a refutation of $\text{REF}_{s,t}^{n,r} \upharpoonright \gamma$, or a refutation of $\text{SAT}^{n,r} \upharpoonright \gamma$. This is because $\Pi \upharpoonright \gamma$ is a resolution refutation and the two restricted formulas do not share any variables.

Let F be a CNF with r clauses in n variables, and let γ_F be a partial assignment defined in Lemma 22, which evaluates the C -variables so that they describe the clauses of F . Notice that $\text{REF}_{s,t}^{n,r} \upharpoonright \gamma_F$ is $\text{REF}_{s,t}^F$, since γ_F turns the clauses (24) into the clauses (1) (and removes the satisfied clauses). Therefore, in the case that $\Pi \upharpoonright \gamma_F$ is a refutation of $\text{REF}_{s,t}^{n,r} \upharpoonright \gamma_F$ and F is unsatisfiable, the lower bound of Theorem 7 applies (setting $\epsilon = 1$ in that theorem, there is n_0 such that conditions (16) on n, r, s, t follow from (25)): the theorem yields some $\delta_1 > 0$ such that the length of $\Pi \upharpoonright \gamma_F$ is at least $2^{n^{\delta_1}}$.

On the other hand, if $\Pi \upharpoonright \gamma_F$ is a refutation of $\text{SAT}^{n,r} \upharpoonright \gamma_F$, the substitution τ from Lemma 22 takes it into a not larger resolution refutation of F (since tautological clauses can be removed from any resolution refutation).

It remains to take any unsatisfiable formula F whose number of clauses is polynomially related to the number of variables and that requires resolution refutations of exponential length, e.g. negation of the pigeonhole principle [5]. A trivial modification of F to serve also in the extreme case $r = n$ allowed by (25) yields $\delta_2 > 0$ such that any resolution refutation of F has length greater than $2^{n^{\delta_2}}$, where n is the number of variables of F .

Setting δ to the minimum of δ_1 and δ_2 concludes the proof of the theorem. \square

A similar proof gives Theorem 3. We restate the theorem below for convenience.

Theorem 24. *Let $\delta_1 > 0$ and let $\{A_n\}_{n \geq 1}$ be a family of unsatisfiable CNFs such that A_n is in n variables, has the number of clauses polynomial in n , and has no resolution refutations of length at most $2^{n^{\delta_1}}$. Then there is $\delta > 0$ and a polynomial p such that $A_n \wedge \text{REF}_{n+1,p(n)}^{A_n}$ has no resolution refutations of length at most 2^{n^δ} and has polynomial size Res(2) refutations.*

Proof. Let $p(n) \geq \max\{r^4, t_0\}$, where r is the maximum of the number of clauses of A_n and n , and t_0 is given by Theorem 7 for $\epsilon = 1$. That theorem and the assumptions on A_n give the required lower bound. To get the upper bound, start with the Res(2) refutation of $\text{SAT}^{n,r} \wedge \text{REF}_{n+1,p(n)}^{n,r}$ given by Theorem 4. Take the substitutions γ_{A_n} and τ from Lemma 22 and observe that $((\text{SAT}^{n,r} \wedge \text{REF}_{n+1,p(n)}^{n,r}) \upharpoonright \gamma_{A_n}) \upharpoonright \tau$ is $A_n \wedge \text{REF}_{n+1,p(n)}^{A_n}$ together with some tautological clauses. \square

6 The Upper Bounds

We restate and prove Theorem 4 from the Introduction.

Theorem 25. *The negation of the reflection principle for Resolution expressed by the formula $\text{SAT}^{n,r} \wedge \text{REF}_{s,t}^{n,r}$ has Res(2) refutations of size $O(trn^2 + tr^2 + st^2n^3 + st^3n)$.*

Proof. By induction on $i \in [s]$ we derive for each $j \in [t]$ the formula

$$D_{i,j} := \bigvee_{\ell \in [n], b \in \{0,1\}} (D(i, j, \ell, b) \wedge T(\ell)^b). \quad (26)$$

Then, cutting $D_{s,t}$ with (7) for each $\ell \in [n]$ and $b \in \{0, 1\}$, yields the empty clause.

Base case: For each $j \in [t]$ we shall derive $D_{1,j}$. For each $m \in [r], \ell \in [n], b \in \{0, 1\}$, cut (23) with (24) to obtain $\neg I(j, m) \vee \neg T(m, \ell, b) \vee D(1, j, \ell, b)$. Applying \wedge -introduction to this and $\neg T(m, \ell, b) \vee T(\ell)^b$ (which is either (21) or (22)) yields

$$\neg I(j, m) \vee \neg T(m, \ell, b) \vee (D(1, j, \ell, b) \wedge T(\ell)^b). \quad (27)$$

Cutting (27) for each $\ell \in [n]$ and $b \in \{0, 1\}$ with (20) gives $\neg I(j, m) \vee D_{1,j}$. Cutting these clauses for $m \in [r]$ with (9) yields $D_{1,j}$.

Induction step: Assume we have derived $D_{i-1,j'}$ for all $j' \in [t]$. For each $j \in [t]$ we shall derive $D_{i,j}$. Write P_1 in place of L and P_0 in place of R .

For each $\ell \in [n], b \in \{0, 1\}, j' \in [t]$, cut $\neg D(i-1, j', \ell, 1) \vee \neg D(i-1, j', \ell, 0)$ (from (2)) with $\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee D(i-1, j', \ell, 1-b)$ (which is from (3) or (4)) to obtain $\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee \neg D(i-1, j', \ell, b)$. Cut this with $D_{i-1,j'}$ to get

$$\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee (D_{i-1,j'} \setminus \{D(i-1, j', \ell, b) \wedge T(\ell)^b\}). \quad (28)$$

Cutting (28) with axiom $T(\ell) \vee \neg T(\ell)$ yields

$$\begin{aligned} &\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee T(\ell)^{1-b} \\ &\quad \vee (D_{i-1,j'} \setminus \{D(i-1, j', \ell, 0) \wedge \neg T(\ell), D(i-1, j', \ell, 1) \wedge T(\ell)\}). \end{aligned} \quad (29)$$

Next, for each $\ell' \in [n] \setminus \{\ell\}$ and $b' \in \{0, 1\}$, apply \wedge -introduction to $T(\ell') \vee \neg T(\ell')$ and $\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee \neg D(i-1, j', \ell', b') \vee D(i, j, \ell', b')$ (from (5) or (6)) to get

$$\begin{aligned} \neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee \left(D(i, j, \ell', b') \wedge T(\ell')^{b'} \right) \\ \vee \neg D(i-1, j', \ell', b') \vee T(\ell')^{1-b'}. \end{aligned} \quad (30)$$

Cutting (30), for each $\ell' \in [n] \setminus \{\ell\}$ and $b' \in \{0, 1\}$, with (29) results, after a weakening, in

$$\neg P_{1-b}(i, j, j') \vee \neg V(i, j, \ell) \vee T(\ell)^{1-b} \vee D_{i,j}. \quad (31)$$

Recall that we have obtained (31) for each $\ell \in [n]$, $b \in \{0, 1\}$, $j' \in [t]$. For each $\ell \in [n]$ and $b \in \{0, 1\}$, cut the clauses (31), $j' \in [t]$, with $\bigvee_{j' \in [t]} P_{1-b}(i, j, j')$ (from (10) or (11)) to derive

$$\neg V(i, j, \ell) \vee T(\ell)^{1-b} \vee D_{i,j}. \quad (32)$$

For each $\ell \in [n]$, cut 32 for $b = 0$ and $b = 1$ on variable $T(\ell)$ to get $\neg V(i, j, \ell) \vee D_{i,j}$, and from these clauses derive $D_{i,j}$ by cuts with (8).

As for bounding the size of the refutation, the size of the base case is $O(trn^2 + tr^2)$, the total size of the induction steps is $O(st^2n^3 + st^3n)$, and the size of the finish is $O(n^2)$. \square

Acknowledgement. I thank Albert Atserias, Ilario Bonacina, Tuomas Hakoniemi and Moritz Müller for their comments.

References

- [1] Albert Atserias and María Luisa Bonet. On the automatizability of resolution and related propositional proof systems. *Information and Computation*, 189(2):182–201, 2004.
- [2] Albert Atserias and Moritz Müller. Automating resolution is NP-hard. *arXiv e-prints*, Apr 2019. [arXiv:1904.02991v1](https://arxiv.org/abs/1904.02991v1).
- [3] María Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. *SIAM J. Comput.*, 29(6):1939–1967, 2000. doi:10.1137/S0097539798353230.
- [4] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.
- [5] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39(2–3):297–308, 1985.
- [6] Jan Krajíček, Alan Skelley, and Neil Thapen. NP search problems in low fragments of bounded arithmetic. *The Journal of Symbolic Logic*, 72(2):649 – 672, 2007.
- [7] Pavel Pudlák. Proofs as games. *American Mathematical Monthly*, 107(6):541–550, 2000. doi:10.2307/2589349.
- [8] Pavel Pudlák. On reducibility and symmetry of disjoint NP-pairs. *Theoretical Computer Science*, 295:323–339, 2003.

- [9] Nathan Segerlind, Samuel R. Buss, and Russel Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. *SIAM Journal on Computing*, 33(5):1171–1200, 2004.
- [10] Neil Thapen. A tradeoff between length and width in resolution. *Theory of Computing*, 12(5):1–14, 2016.

A Formula REF of Atserias and Müller

The purpose of this section is to give an answer to the lower bound question from [2] in its original formulation, in which the refutation statement is formulated a bit differently from our $\text{REF}_{s,t}^F$.

We list the clauses of the formula $\text{REF}(F, \tilde{s})$ of [2]:

$$V[u, 0] \vee V[u, 1] \vee \dots \vee V[u, n] \quad u \in [\tilde{s}], \quad (33)$$

$$I[u, 0] \vee I[u, 1] \vee \dots \vee I[u, r] \quad u \in [\tilde{s}], \quad (34)$$

$$L[u, 0] \vee L[u, 1] \vee \dots \vee L[u, \tilde{s}] \quad u \in [\tilde{s}], \quad (35)$$

$$R[u, 0] \vee R[u, 1] \vee \dots \vee R[u, \tilde{s}] \quad u \in [\tilde{s}], \quad (36)$$

$$\neg V[u, i] \vee \neg V[u, i'] \quad u \in [\tilde{s}], i, i' \in [n] \cup \{0\}, i \neq i', \quad (37)$$

$$\neg I[u, j] \vee \neg I[u, j'] \quad u \in [\tilde{s}], j, j' \in [r] \cup \{0\}, j \neq j', \quad (38)$$

$$\neg L[u, v] \vee \neg L[u, v'] \quad u \in [\tilde{s}], v, v' \in [\tilde{s}] \cup \{0\}, v \neq v', \quad (39)$$

$$\neg R[u, v] \vee \neg R[u, v'] \quad u \in [\tilde{s}], v, v' \in [\tilde{s}] \cup \{0\}, v \neq v', \quad (40)$$

$$\neg I[u, 0] \vee \neg V[u, 0] \quad u \in [\tilde{s}], \quad (41)$$

$$I[u, 0] \vee V[u, 0] \quad u \in [\tilde{s}], \quad (42)$$

$$\neg I[u, 0] \vee \neg L[u, 0] \quad u \in [\tilde{s}], \quad (43)$$

$$\neg I[u, 0] \vee \neg R[u, 0] \quad u \in [\tilde{s}], \quad (44)$$

$$\neg L[u, v] \quad u, v \in [\tilde{s}], u \leq v, \quad (45)$$

$$\neg R[u, v] \quad u, v \in [\tilde{s}], u \leq v, \quad (46)$$

$$\neg L[u, v] \vee \neg V[u, i] \vee D[v, i, 1] \quad u, v \in [\tilde{s}], i \in [n], b \in \{0, 1\}, \quad (47)$$

$$\neg R[u, v] \vee \neg V[u, i] \vee D[v, i, 0] \quad u, v \in [\tilde{s}], i \in [n], b \in \{0, 1\}, \quad (48)$$

$$\neg L[u, v] \vee \neg V[u, i] \vee \neg D[v, i', b] \vee D[u, i', b] \quad u, v \in [\tilde{s}], i, i' \in [n], b \in \{0, 1\}, i \neq i', \quad (49)$$

$$\neg R[u, v] \vee \neg V[u, i] \vee \neg D[v, i', b] \vee D[u, i', b] \quad u, v \in [\tilde{s}], i, i' \in [n], b \in \{0, 1\}, i \neq i', \quad (50)$$

$$\neg I[u, j] \vee D[u, i, b] \quad u \in [\tilde{s}], j \in [r], x_i^b \in C_j, \quad (51)$$

$$\neg D[u, i, 0] \vee \neg D[u, i, 1] \quad u \in [\tilde{s}], i \in [n], \quad (52)$$

$$\neg D[\tilde{s}, i, b] \quad i \in [n], b \in \{0, 1\}. \quad (53)$$

The meanings of the variables and clauses of $\text{REF}(F, \tilde{s})$ are very similar to those of $\text{REF}_{s,t}^F$, which we described in words in detail, so let us concentrate on the main differences. First of all, the clauses described by $\text{REF}(F, \tilde{s})$ through D -variables are indexed from 1 to \tilde{s} ; this is their order in the refutation they should form (and they are not arranged in levels). Moreover, unlike in $\text{REF}_{s,t}^F$ where each clause described by D -variables, with the exception of clauses on level 1, has to be derived only by the resolution rule, in $\text{REF}(F, \tilde{s})$ there are both options (weakening of a clause in F and the resolution rule). That exactly one of these options must be chosen in a valid resolution refutation

is ensured with the help of (41), (42), and the additional value 0 that the second index of V, I, L, R -variables can attain. In particular, any assignment satisfying $\text{REF}(F, \tilde{s})$ evaluates to 1 exactly one of the variables in $\{I[u, j] : j \in [r]\} \cup \{V[u, i] : i \in [n]\}$.

We show how a lower bound on the length of resolution refutations for the formula $\text{REF}(F, \tilde{s})$ follows from the lower bound for $\text{REF}_{n+1,t}^F$.

Let F be a CNF in n variables with r clauses and assume the parameter \tilde{s} in $\text{REF}(F, \tilde{s})$ is such that $t = \lfloor \frac{\tilde{s}}{n+1} \rfloor$ satisfies condition (16) of Theorem 7 for $\text{REF}_{n+1,t}^F$.

It is straightforward to assign some variables of $\text{REF}(F, \tilde{s})$ so that after removing the satisfied clauses, the formula becomes $\text{REF}_{n+1,t}^F$ up to a renaming of variables (and after removing certain clauses from (5) and (6) in $\text{REF}_{n+1,t}^F$, which immediately follow from (2) - (4) anyway). First, set the appropriate variables in $\text{REF}(F, \tilde{s})$ so that the clauses $D_1, D_2, \dots, D_{s-t(n+1)}$ described by the formula are all obtained, say, by a weakening of the clause $C_1 \in F$, and that none of these clauses is used as a premise of the resolution rule. Then, arrange the remaining clauses into $n + 1$ levels of t clauses. Evaluate to 1 all variables $L[u, 0], R[u, 0]$ with u on the first level, and evaluate to 0 all the remaining $L[u, v], R[u, v]$ except for those with u on the first highest level than v . Further, evaluate to 1 all variables $V[u, 0]$ with u on the first level, and evaluate to 0 all the remaining $V[u, i]$ except for those with u from second to last level and a non-zero i . Next, evaluate to 1 all $I[u, 0]$ with u from second to last level, and evaluate to 0 all the remaining $I[u, j]$ variables except for those on the first level with a non-zero j . Finally, replace all the non-evaluated variables by the corresponding variables of $\text{REF}_{n+1,t}^F$, respecting the above chosen arrangement to $n + 1$ levels of t clauses.

Since the substitution just described takes any refutation of $\text{REF}(F, \tilde{s})$ to a refutation of $\text{REF}_{n+1,t}^F$ without any increase in size, Theorem 7 implies an exponential resolution size lower bound for the original formula $\text{REF}(F, \tilde{s})$ of Atserias and Müller, as stated in the following theorem.

Theorem 26. *For each $\epsilon > 0$ there is $\delta > 0$ and an integer t_0 such that if n, r, \tilde{s} are integers satisfying*

$$r \geq n \geq 2, \quad \left\lfloor \frac{\tilde{s}}{n+1} \right\rfloor \geq r^{3+\epsilon}, \quad \left\lfloor \frac{\tilde{s}}{n+1} \right\rfloor \geq t_0,$$

and F is an unsatisfiable CNF consisting of r clauses C_1, \dots, C_r in n variables x_1, \dots, x_n , then any resolution refutation of $\text{REF}(F, \tilde{s})$ has length greater than $2^{\lfloor \frac{\tilde{s}}{n+1} \rfloor^\delta}$.