A New Kind of Tradeoffs in Propositional Proof Complexity

ALEXANDER RAZBOROV

We exhibit an unusually strong tradeoff in propositional proof complexity that significantly deviates from the established pattern of almost all results of this kind. Namely, restrictions on one resource (width in our case) imply an increase in another resource (tree-like size) that is exponential not only with respect to the complexity of the original problem, but also to the whole class of all problems of the same bit size. More specifically, we show that for any parameter \( k = k(n) \) there are unsatisfiable \( k \)-CNFs that possess refutations of width \( O(k) \), but such that any tree-like refutation of width \( n^{1-\epsilon/k} \) must necessarily have doubly exponential size \( \exp(n^{\Omega(k)}) \). This means that there exist contradictions that allow narrow refutations, but in order to keep the size of such a refutation even within a single exponent, it must necessarily use a high degree of parallelism.

Our construction and proof methods combine, in a non-trivial way, two previously known techniques: the hardness escalation method based on substitution formulas and expansion. This combination results in a hardness compression approach that strives to preserve hardness of a contradiction while significantly decreasing the number of its variables.

CCS Concepts: •Theory of computation → Proof complexity;

Additional Key Words and Phrases: Hardness compression, Resolution, Tradeoff

1. INTRODUCTION

Tradeoff results is quite a popular topic in complexity theory and beyond. Whenever they apply, this serves as a rigorous demonstration of our inherent inability to achieve two conflicting goals at once. These results have the following form that we purposely describe in very generic terms. We are given a task \( T \) and a set of protocols \( P_T \) that achieve this task; for simplicity, we confine ourselves to non-uniform models when everything is finite. The set \( P_T \) is equipped with two complexity measures \( \mu \) and \( \nu \), usually of a rather different nature. Then tradeoff results claim that after we restrict \( P_T \) to those protocols \( P \) for which \( \mu(P) \) is small, the minimum complexity with respect to the second measure, \( \min_{P \in P_T} \nu(P) \), increases drastically, in many cases exponentially. Earlier results along these lines primarily focussed on the pair \( \mu = \) "computational space", \( \nu = \) "computational time", see [Borodin 1993] for a survey. But, as we already mentioned, at the moment this paradigm is omnipresent and \( (\mu, \nu) \) can be literally anything. Specifically, there are many tradeoff results of all kinds in proof complexity [Nordström 2013].

In this paper we demonstrate an example of a tradeoff whose behavior is drastically different from most known cases. The discussion below is aimed at articulating this difference; the reader primarily interested in our technical contribution may safely skip this part and jump to the description of our concrete result on page 3.

It would be instructive to resort to a simple and necessarily schematic picture. On Figure 1, \( \mu_{\text{min}} \) is simply \( \min_{P \in P_T} \mu(P) \), that is the complexity of our task \( T \) with respect
to \( \mu \) alone. \( \mu_{\text{max}} \) is the “saturation level” in the resource \( \mu \), that is its maximal amount any “reasonable” protocol can possibly consume. The right end \( \mu_{\text{max}} \) of the interval of interest is actually not very important for making our point, whenever it is not clear from the context the reader can assume instead \( \mu_{\text{max}} = \infty \).

Tradeoff results of any kind are trying to pinpoint the behavior of the function
\[
f(\mu) \overset{\text{def}}{=} \min \{ \nu(P) \mid P \in \mathcal{P}_T \land \mu(P) \leq \mu \}
\]
in the interval \( \mu \in [\mu_{\text{min}}, \mu_{\text{max}}] \); more specifically, prove that it is (as sharply as possible) decreasing. Ordinary tradeoffs normally consist of two parts: a lower bound on \( f(\mu) \), shown in red, along with an upper bound stating, as the very minimum, that at the right end \( \mu_{\text{max}} \) this lower bound is close to tight. These two facts together imply that the actual curve \( f(\mu) \) does have a slope. We would like to note that we drew the red curve as a nice convex function mostly as a sign of respect to earlier results that almost always had the form of a lower bound on \( \mu(P)\nu(P) \). In the plethora of examples found since that, it can be anything non-increasing: we will see below one example (5) that is a lower bound on \( \mu(P) \log \nu(P) \); it can be a step function when the lower bound part simply breaks down for some \( \mu \in [\mu_{\text{min}}, \mu_{\text{max}}] \) etc. But, repeating our point, two ingredients are paramount to any tradeoff result: a lower bound on \( f(\mu) \) at \( \mu = \mu_{\text{min}} \) (and, preferably, as much to the right of it as possible), as well as an upper bound at \( \mu = \mu_{\text{max}} \) (extended as much as possible to the left).

So far we have discussed one particular task, \( T \). But since the complexity theory is about algorithmic problems, \( T \) is never in isolation, it is always a member of a large but finite\(^1\) family of tasks \( T_n \), where the subscript \( n \) stands for the “size” of \( T \). As it turns out, in virtually all cases of interest there exists a "natural" upper bound \( \nu_{\text{cr}}(n) \) on the \( \nu \)-complexity \( \min_{P \in \mathcal{P}_T} \nu(P) \) of any task \( T^* \in T_n \), usually provided by a trivial (aka "straightforward", "brute-force" etc.) protocol. For example, when \( \nu = "\text{circuit size}" \) in circuit complexity or \( \nu = "\text{proof length}" \) in proof complexity, \( \nu_{\text{cr}}(n) = 2^n \).

\(^1\)Recall that we are considering non-uniform models.
In communication complexity, \( \nu_{cr}(n) = n \), the bit size of the input. Etc. In some cases, like circuit complexity, this upper bound is known to be tight for the worst or even typical task \( T^* \in \mathcal{T}_n \) (so-called Shannon effect), and in other cases, like strong propositional proof systems, this is wide open. But, implicitly or explicitly, \( \nu_{cr}(n) \) is always there and determines the range in which interesting developments occur.

As it turns out, in the vast majority of known tradeoff results, the red curve is below the critical horizontal line \( \nu = \nu_{cr}(n) \). That is, \( \mu \)-restricted protocols for \( T \) are compared with unrestricted protocols \( P \) for the task \( T \) itself; they can be managed to be at most as \( \nu \)-bad as trivial protocols for all tasks \( T^* \in \mathcal{T}_n \).

In this paper we exhibit a tradeoff result that operates entirely above the critical line \( \nu = \nu_{cr}(n) \). In other words, the lower bound in a vicinity of \( \mu_{min} \) (that in our result actually extends almost all the way up to \( \mu_{max} \)) is so strong that it exponentially beats the generic upper bound \( \nu_{cr}(n) \) holding for all tasks \( T^* \) of comparable size \( n \). The second ingredient in ordinary tradeoff results, which is the upper bound on \( \nu \) at \( \mu = \mu_{max} \), need not be proven separately: it automatically follows from the membership \( T \in \mathcal{T}_n \), or, putting it differently, the upper bound is provided by the naive brute-force protocol.

This phenomenon seems to be extremely rare (we will review below those few examples we have been able to find after an earlier version of this paper was disseminated), and we think it deserves at least a certain amount of attention and contemplation.

Our concrete result belongs to the area of propositional proof complexity that has seen a rapid development since its inception in the seminal paper by Cook and Reckhow [Cook and Reckhow 1979]. This success is in part due to being well-connected to a number of other disciplines, and one of these connections that has seen a particularly steady growth in very recent years is the interplay between propositional proof complexity and practical SAT solving. As a matter of fact, SAT solvers that seem to completely dominate the landscape at the moment, like those employing conflict-driven clause learning, are inherently based on the resolution proof system dating back to the papers by Blake [Blake 1937] and [Robinson 1965]. This somewhat explains the fact that resolution is by far the most studied system in proof complexity, and much of this study has concentrated on simple complexity measures for resolution proofs like size, width and space, and on relations existing between them.

Our paper also exclusively deals with the resolution proof system. The first measure of interest to us is width. This measure is extremely natural and robust, and in fact it is not very specific to resolution. As is well-known, width \( w \) proofs can more instructively be viewed as semantic proofs operating with arbitrary Boolean expressions and equally arbitrary (sound) inference rules with the sole restriction that every line depends on at most \( w \) variables.

Ben-Sasson and Wigderson [Ben-Sasson and Wigderson 2001] brought into focus of proof complexity the importance of width by showing that short proofs can be transformed into proofs of small width (see (1) and (2) below), while Atserias and Dalmau [Atserias and Dalmau 2008] did this for proofs that have small clause space. Thus, despite its deluding simplicity, the class of contradictions possessing small-width refutations is rich.

In this paper we give (yet another) confirmation of this thesis “from the opposite side”: there exist contradictions that do have small-width refutations, but the latter are highly sequential and non-efficient, and any attempts to simplify them must necessarily lead to a dramatic blow-up in width. Before reviewing some relevant work in this direction and stating our own contribution, it will be convenient to fix some basic notation (we will recall exact definitions in Section 2). For a CNF contradiction \( \tau_n \) in \( n \) variables, let \( w(\tau_n \vdash 0) \) be the minimum possible width [size, respectively] of
any resolution refutation of \( \tau_n \), \( S_T(\tau_n \vdash 0) \) is the minimum size with respect to tree-like refutations, and \( w(\tau_n) \) is the maximum width of a clause in \( \tau_n \) itself.

In this notation, the main results from [Ben-Sasson and Wigderson 2001] can be stated as follows:

\[
\begin{align*}
  w(\tau_n \vdash 0) &\leq \log S_T(\tau_n \vdash 0) + w(\tau_n); \quad (1) \\
  w(\tau_n \vdash 0) &\leq O(n \cdot \log S(\tau_n \vdash 0)^{1/2} + w(\tau_n). \quad (2)
\end{align*}
\]

Bonet and Galesi [Bonet and Galesi 1999] proved that (2) is (almost) tight by exhibiting contradictions \( \tau_n \) such that \( w(\tau_n) \leq O(1), S(\tau_n \vdash 0) \leq n^{O(1)} \) while \( w(\tau_n \vdash 0) \geq \Omega(n^{1/2}). \) As for (1), it is tight for obvious reasons: the Complete Tree contradiction \( CT_n \) consisting of all \( 2^n \) possible clauses in \( n \) variables satisfies \( w(CT_n) = w(CT_n \vdash 0) = n \) and \( S_T(CT_n \vdash 0) = 2^n. \)

In the opposite direction, resolution size can be trivially bounded by width as follows:

\[
S(\tau_n \vdash 0) \leq n^{O(w(\tau_n \vdash 0))}; \quad (3)
\]

the right-hand side here simply bounds the overall number of all possible clauses of width \( \leq w. \)

Atserias, Lauria and Nordström [Atserias et al. 2014] have recently shown that this bound is also tight for an arbitrary \( w = w(n) \leq n^{1/2-\Omega(1)} \) there exist contradictions \( \tau_n \) with \( w(\tau_n \vdash 0) \leq w \) while \( S(\tau_n \vdash 0) \geq n^{\Omega(w)}. \) An earlier result by Ben-Sasson, Impagliazzo and Wigderson [Ben-Sasson et al. 2004] can be viewed as an ultimate demonstration that no simulation like (3) is possible for tree-like resolution. Namely, they gave an example of contradictions \( \tau_n \) such that

\[
w(\tau_n \vdash 0) \leq O(1), \quad S_T(\tau_n \vdash 0) \geq \exp(\Omega(n/\log n)). \quad (4)
\]

Having briefly discussed simulation and separation results, let us review what has been known before in terms of tradeoffs. Ben-Sasson [Ben-Sasson 2009] established a tradeoff between width and tree-like resolution size. Namely, he constructed contradictions \( \tau_n \) that have tree-like refutations of either constant width or polynomial size but such that

\[
w(\Pi) \cdot \log |\Pi| \geq \Omega(n/\log n) \quad (5)
\]

for any tree-like refutation \( \Pi \) of \( \tau_n \) (\( w(\Pi) \) and \( |\Pi| \) being its width and size respectively). As for the general case, strong tradeoffs are precluded by (3) and the observation that the naive resolution refutation it represents still has the minimum possible width \( w(\tau_n \vdash 0). \) Hence, in sharp contrast with (5), every contradiction \( \tau_n \) has a DAG-like refutation \( \Pi \) such that

\[
w(\Pi) \cdot \log |\Pi| \leq O(\log n \cdot w(\tau_n \vdash 0)^2). \]

Even with this severe restriction interesting results along these lines have been reported in [Nordström 2009; Thapen 2014]. They are, however, best viewed in the dual coordinate system \( \mu \) = "size", \( \nu \) = "width" (in terms of Figure 1).

Our main result, Theorem 3.1 is a far-reaching generalization of the previous contributions (4), (5). For any parameter \( k = k(n) \) we construct a sequence of \( k \)-CNF contradictions \( \tau_n \) such that \( w(\tau_n \vdash 0) \leq O(k) \) while

\[
|\Pi| \geq \exp\left(n^{\Omega(k)}\right) \quad (6)
\]

for any tree-like refutation \( \Pi \) of width \( \leq n^{1-\epsilon}/k. \) Thus, when \( k, \) say, is a sufficiently large constant our bound becomes super-exponential in \( n, \) and for (say) \( k = n^{1/3} \) it becomes doubly exponential. As such, it perfectly fits the paradigm we described in
the beginning: in terms of Figure 1, we have \( \mu = \text{"width"}, \nu = \text{"tree-like size"}, \mu_{\max} = O(k), \mu_{\min} = n \) and \( \nu_{\max} = 2^n \).

On less general level, our result is complementary to that of Atserias et al. [Atserias et al. 2014]. Namely, they proved that the obvious brute-search refutation of size \( n^{\Omega(w)} \) (cf. (3)) in general can not be shortened. What we prove is that if we additionally want to keep the width reasonably small, and keep the size sane (at most single exponential), we need a high degree of parallelism as afforded by general, DAG-like resolution.

Let us now review a few previous examples that are relevant to this framework.

Resolution proofs, \( \mu = \text{"width"}, \nu = \text{"logical depth"} \). Then \( \mu_{\max} = n \) and \( \nu_{\max} = n \). Let us choose \( \mu_{\min} \) arbitrarily. The proof method of a result by Berkholz [Berkholz 2012, Theorem 5] gives a tradeoff similar to ours: every refutation of the minimum width \( k \) must have depth at least \( n^k \). This lower bound, however, breaks down already for refutations of width \( (k+1) \).

Resolution proofs (and beyond), \( \mu = \text{"proof length"}, \nu = \text{"clause space"} \). We have \( \mu_{\max} = 2^n \), \( \nu_{\min} = n \). For any \( \mu_{\min} \in [n^{\log n}, 2^n] \), the result by Beame, Beck and Impagliazzo [Beame et al. 2012] gives contradictions \( \tau_n \) that have refutations of length \( \mu_{\min} \) but such that every refutation of length \( \leq \mu_{\min} \) must have clause space \( \mu_{\min}^{\Omega(1)} \). Beck, Nordström and Tang [Beck et al. 2013, Theorem 4] generalized this result to the polynomial calculus with resolution and also pushed down the lower bound on \( \mu_{\min} \) to \( n^C \).

It is worth noting, however, that in the dual regime \( \mu = \text{"clause space"}, \nu = \text{"proof length"} \) that is, perhaps, more natural, “supercritical” tradeoffs are hindered by the observation that every clause space \( S \) refutation can be assumed to be of length \( \exp(O(S\log n)) \). This is true simply because \( \exp(O(S\log n)) \) is the trivial upper bound on the overall number of different configurations with space \( \leq S \).

Other than these results about resolution, we are only aware of a conjecture in information complexity due to Ganor, Kal and Raz (private communication) that is of a very similar flavor. The reader wishing to connect the description below to Figure 1 should think of \( \mu \) as the information complexity \( IC(T) \) of a task \( T \) and of \( \nu \) as its (randomized) communication complexity \( CC(T) \); see [Braverman 2014] for a general overview of the area.

More precisely, Braverman [Braverman 2012] proved the simulation \( CC(T) \leq 2^{IC(T)} \), and it was shown to be tight by Ganor, Kal and Raz in [Ganor et al. 2014]. An interesting feature of Braverman’s protocol, however, is that its information complexity is in general exponentially larger than \( IC(T) \): this is the price one has to pay for bounding the communication complexity even by an exponential function in \( IC(T) \). The conjecture, roughly speaking, says that if we are not willing to pay this price, the situation becomes even worse: every protocol (for the same task \( T \) as in [Ganor et al. 2014]) whose information complexity is nearly optimal\(^2\), has communication complexity that is doubly exponential in \( IC(T) \).

**Technical contributions.** Our construction and the proof combine two very popular techniques in proof complexity: hardness escalation and expansion. The former method converts every contradiction \( \tau_n \) into another contradiction \( \hat{\tau}_n \), so that relatively mild hardness properties of \( \tau_n \) transfer to lower bounds for \( \hat{\tau}_n \) in stronger proof systems. So far this technique has been used in two main flavors: substitution formulas (see e.g. [Nordström 2013, Section 2.4]) and lifting formulas introduced in [Beame et al. 2010].

\(^2\)we deliberately leave this quantitatively imprecise
Expander graphs have been extensively used in proof complexity since [Chvátal and Szemerédi 1988; Ben-Sasson and Wigderson 2001; Alekhnovich et al. 2004]. The general paradigm used in many different scenarios can be, very roughly and somewhat superficially, described as follows. Assume that the constraint-variable graph of a given contradiction is a good bipartite expander. Then it allows us to control “the flow of information” between different constraints in a prospective refutation. As a result, it is possible to “localize” it in such a way that every part of it can “depend” only on a small number of constraints or at least can be built from these local pieces by simple operations (as is often the case for algebraic and semi-algebraic proof systems).

Our work combines these two paradigms; let us discuss it in a few technical details. Like in the method of substitution formulas, we start with a contradiction $\tau_m$ but, unlike with that method, we already know from previous work that it possesses exactly the hardness properties we are shooting for, and for exactly the same model. What prevents us from going above the critical line on Figure 1 is the fact that the number of variables $m$ and, consequently, $\nu_{cr}(m)$ is very large. Our solution is to lower the critical line by compressing the number of variables in $\tau_m$ while preserving its hardness.

We achieve this task by substituting into $\tau_m(y_1, \ldots, y_m) \mathbb{F}_2$-linear forms in new variables $x_1, \ldots, x_n$, where $n \ll m$, according to a $m \times n$ 0-1 matrix $A$. In previous applications of substitution formulas, these linear forms (that is, rows of the matrix $A$) had pairwise disjoint sets of variables. It allowed to prove that the resulting CNF $\tau_m[A]$ has even stronger hardness properties than the original CNF $\tau_m$; this is so-called hardness escalation. We prove in Theorem 3.2 that a similar conclusion can be achieved under the much weaker condition that $A$ is a sufficiently good expander; this allows us to do the variable compression. In fact, hardness escalation from resolution depth to tree-like size also takes place, but this part was known before [Urquhart 2011, Theorem 5.4], and it is not very important for our purposes in this paper.

On an even more technical level, we largely follow the same routine as most expansion-based arguments in proof complexity. We identify an appropriate notion of a closed set of $x$-variables (see the beginning of Section 4) and show that every narrow clause $C$ can be “localized” to a closed set $J$ (Lemma 2.3). This closed set uniquely defines the set $\text{Ker}(J)$ of “determined” variables $y_i$, i.e. those for which the corresponding linear form is entirely contained in $J$. For the sake of this discussion let us denote by $J^*$ the set of all $j \in J$ for which $x_j$ is actually contained in at least one of these forms. It is important to stress that $\text{Vars}(C)$ and $J^*$ are in general position and we can not do anything about it; the only thing we know is that both these sets of variables are contained in the same ambient closed set $J$.

The heart of the argument (Claim 4.1) proven by induction says that in this setup, any short tree-like resolution proof $\Pi$ of $C$ can be converted into a small depth resolution proof of any clause $E$ in the variables $\{y_i \mid i \in \text{Ker}(J)\}$ that is “relevant” to $C$. Again, most of our analysis is typical for arguments that involve both substitution formulas and expansion, so we confine ourselves to highlighting just two ideas that are perhaps at least somewhat novel.

(1) Since $\text{Vars}(C)$ and $J^*$ are in general position, there could be several different sensible ways to define the concept of “relevance” between $C$ and $E$. It turns out that in order for induction to work, we must take the most minimalistic, intuitionistic approach and promise the small depth derivation of $E$ whenever $C$ and $E$ can be potentially simultaneously falsified by at least one total assignment.

(2) As even the depth of the derivation we are working against is exponential, there is no way the ambient closed set $J$ can be adjusted along with the progress of the derivation. Thus in the proof of Claim 4.1 we do not even try to relate the closed sets
associated to the premises and the conclusion of a resolution rule but immediately re-compute the former (see the definition of $\tilde{J}$) from the scratch.

After we prove this “transfer principle” (that is, Claim 4.1), the rest is straightforward. The only remaining thing to be remarked is that our method does not have enough room to work for very small $k$ ($k \leq 11$). Fortunately, in this regime our bound degenerates into a traditional exponential bound, and for that purpose we can utilize several existing results like (4).

2. PRELIMINARIES

In this section we give necessary definitions and state some useful facts.

A literal is either a Boolean variable $x$ or its negation $\bar{x}$; we will sometimes use the uniform notation $x^\epsilon \overset{\text{def}}{=} \begin{cases} x & \text{if } \epsilon = 1 \\ \bar{x} & \text{if } \epsilon = 0. \end{cases}$

A clause $C$ is either a disjunction of literals in which no variable appears along with its negation, or 1. The latter is a convenient technicality (e.g. with this convention the set of all clauses makes a lattice in which $\lor$ is the join operator etc.); 1 should be thought of as a placeholder for all trivially true clauses. $C$ is a sub-clause of $D$, also denoted by $C \subseteq D$ if either $D = 1$ or $C, D \neq 1$ and every literal appearing in $C$ also appears in $D$. Two clauses $C$ and $D$ are simultaneously falsifiable if $C \lor D \neq 1$, that is both $C$ and $D$ are not 1 and do not contain conflicting literals. The empty clause $C$ will be denoted by 0. The set of variables occurring in a clause $C$ (either positively or negatively) will be denoted by $\text{Vars}(C)$ ($\text{Vars}(1) \overset{\text{def}}{=} \emptyset$). The width of a clause $C$ is defined as $w(C) \overset{\text{def}}{=} |\text{Vars}(C)|$.

A CNF $\tau$ is a conjunction of clauses, often identified with the set of clauses it is comprised of. A CNF is a $k$-CNF if all clauses in it have width at most $k$. Unsatisfiable CNFs are traditionally called contradictions. For CNFs $\tau, \tau'$, $\tau \models \tau'$ is the semantical implication meaning that every truth assignment satisfying $\tau$ also satisfies $\tau'$. Thus, $\tau$ is a contradiction if and only if $\tau \models 0$. Also, for clauses $C$ and $D$, $C \leq D$ if and only if $C \models D$. A clause $C$ is simultaneously falsifiable with a CNF $\tau$ if $C \lor \tau \neq 1$. Note that $C$ is simultaneously falsifiable with $\tau$ if and only if it is simultaneously falsifiable with at least one clause $D \in \tau$. The subscript $n$ in $\tau_n$ always stands for the number of variables in the CNF $\tau_n$.

The resolution proof system operates with clauses and it consists of the single resolution rule

$$\frac{C \lor x \quad D \lor \bar{x}}{C \lor D}.$$  \hfill (7)

A tree-like$^3$ resolution proof $\Pi$ is a binary rooted tree in which all nodes are labelled by clauses, and such that the clause assigned to every internal node can be deduced from clauses sitting at its two children via a single application of the resolution rule. A tree-like resolution proof of a clause $C$ from a CNF $\tau$ is a tree-like resolution proof $\Pi$ in which all leaves are labelled by clauses from $\tau$, and the root is labelled by a clause $\tilde{C}$ such that $\tilde{C} \leq C$ (the latter technicality is necessary since we did not include the weakening rule). A refutation of a contradiction is a proof of 0 from it. The depth $D(\Pi)$ of a proof $\Pi$ is the height (the number of edges in the longest path) of its underlying tree, and it will be convenient to define its size $|\Pi|$ as the number of leaves (which is

$^3$DAG-like proofs are not considered in this paper.
within a factor of two from the overall number of vertices anyway). The width \( w(\Pi) \) is the maximum width of a clause appearing in \( \Pi \).

For a CNF \( \tau \) and a clause \( C \), we let \( D(\tau \vdash C) \), \( S_T(\tau \vdash C) \) and \( w(\tau \vdash C) \) denote the minimum possible value of \( D(\Pi), |\Pi| \) and \( w(\Pi) \), respectively, taken over all tree-like resolution proofs \( \Pi \) of \( C \) from \( \tau \) (if \( \tau \not\vdash C \), we let all three measures be equal to \( \infty \)).

The following result will be one of the starting points for our construction.

**Proposition 2.1 ([Ben-Sasson et al. 2004]).** There exists an increasing sequence \( \{\tau_n\} \) of 4-CNF contradictions such that \( w(\tau_n \vdash 0) \leq 6 \), but \( S_T(\tau_n \vdash 0) \geq \exp(\Omega(n/\log n)) \).

Let \( A \) be a \( m \times n \) 0-1 matrix. For \( i \in [m] \), let \( J_i(A) \defeq \{ j \in [n] \mid a_{ij} = 1 \} \). For a clause \( E \) in the variables \( \{y_1, \ldots, y_m\} \), by \( E[A] \) we will denote the CNF obtained from \( E \) by the \( \mathbb{F}_2 \)-linear substitution \( y_i \mapsto \bigoplus_{j \in J_i(A)} x_j \ (i \in [m]) \) followed by converting the resulted Boolean function to a CNF in such a way that every clause \( C \) in \( E[A] \) contains all relevant variables:

\[
\text{Vars}(C) = \bigcup_{y_i \in \text{Vars}(E)} \{x_j \mid j \in J_i(A) \}.
\]

For a CNF \( \tau = E_1 \land E_2 \land \ldots \land E_t \), we let \( \tau[A] \defeq E_1[A] \land \ldots \land E_t[A] \). If \( \tau \) is a contradiction then evidently \( \tau[A] \) is a contradiction, too. The converse need not be true in general, of course.

For \( I \subseteq [m] \), the boundary of this set of rows is defined as

\[
\partial_A(I) \defeq \{ j \in [n] \mid \{ i \in I \mid j \in J_i(A) \} = 1 \},
\]

i.e., it is the set of columns that have precisely one 1 in their intersections with \( I \). \( A \) is an \((r, s, c)\)-boundary expander\(^5\) if \( |J_i(A)| \leq s \) for any \( i \in [m] \) and \( |\partial_A(I)| \geq c|I| \) for every set of rows \( I \subseteq [m] \) with \( |I| \leq r \). An \((r, n, c)\)-boundary expander (i.e., a \( m \times n \) matrix satisfying only the second of these conditions) will be simply called an \((r, c)\)-boundary expander.

For a set of columns \( J \subseteq [n] \), we let

\[
\text{Ker}(J) \defeq \{ i \in [m] \mid J_i(A) \subseteq J \}
\]

be the set of rows completely contained in \( J \). Let \( A \setminus J \) be the sub-matrix of \( A \) obtained by removing all columns in \( J \) and all rows in \( \text{Ker}(J) \).

We need two properties of boundary expanders whose analogues were used, in one or another form, in almost all their applications in proof complexity. The first one, proven by a simple probabilistic argument, says that good expanders exist in the range \( m \gg n \) (note that it becomes sub-optimal in the frequently used setting \( s, c = O(1), m = O(n) \)).

**Lemma 2.2.** Let \( n \to \infty \) and \( m, s, c, r \) be arbitrary integer parameters possibly depending on \( n \) such that \( c \leq \frac{3}{4} s \) and

\[
r \leq o(n/s) \cdot m^{-\frac{c}{s}}.
\]

Then for sufficiently large \( n \) there exist \( m \times n \) \((r, s, c)\)-boundary expanders.

The second property says that in every good expander, the class of small sets of rows whose removal leads to a relatively good expander is in a sense everywhere dense.

---

\(^4\)[\( [m] \defeq \{1, \ldots, m\} \).  
\(^5\)In [Alekhnovich et al. 2004] such matrices were simply called expanders.

---

**Lemma 2.3.** Let $A$ be an $m \times n$ $(r, 2)$-boundary expander. Then for every $J \subseteq [n]$ with $|J| \leq r/4$ there exists $\tilde{J} \supseteq J$ such that $|\text{Ker}(\tilde{J})| \leq 2|J|$ and $A \setminus \tilde{J}$ is an $(r/2, 3/2)$-boundary expander.

We, however, have not been able to recover these statements from the literature in a referrable form, and for this reason their simple proofs are included in the Appendix.

### 3. Main Results

In this brief section we formulate our main results.

**Theorem 3.1.** Let $k = k(n) \geq 4$ be any parameter, and let $\epsilon > 0$ be an arbitrary constant. Then there exists a sequence of $k$-CNF contradictions $\{\tau_n\}$ in $n$ variables such that $w(\tau_n \vdash 0) \leq O(k)$ but for any tree-like refutation $\Pi$ with $w(\Pi) \leq n^{1-\epsilon}/k$ we have the bound

$$|\Pi| \geq \exp\left(n^{\Omega(k)}\right).$$

As we noted in Introduction, our main technique is hardness compression, and since the corresponding statement might be of independent interest, we formulate it here as a separate result.

**Theorem 3.2.** Let $\tau_m$ be an arbitrary contradiction in the variables $y_1, \ldots, y_m$, and let $A$ be an $m \times n$ $(r, 2)$-boundary expander for some $r$. Then every tree-like refutation $\Pi$ of $\tau_m[A]$ with $w(\Pi) \leq r/4$ must satisfy

$$|\Pi| \geq 2^{2D(\tau_m \vdash 0)/r}.$$

### 4. Proofs

In this section we prove Theorems 3.1 and 3.2, and we begin with the latter. We present our proof as a plain inductive argument since, in our view, it is often more instructive than various top-down approaches (cf. the recent simplification of the Atserias-Dalmau bound [Atserias and Dalmau 2008] obtained by Filmus et al. [Filmus et al. 2014] and independently by Razborov (unpublished)).

Fix an $m \times n$ $(r, 2)$-boundary expander $A$, where $r$ is an arbitrary parameter. Let us say that a set of columns $J$ is closed if $A \setminus J$ is an $(r/2, 3/2)$-boundary expander (cf. Lemma 2.3). Fix now an arbitrary CNF $\tau_m$ (that need not necessarily be a contradiction) in the variables $y_1, \ldots, y_m$. We are going to prove the following.

**Claim 4.1.** Assume that $C$ is a clause in the variables $x_1, \ldots, x_n$ that possesses a tree-like proof $\Pi$ from $\tau[A]$ with $w(\Pi) \leq r/4$. Let $J \subseteq [n]$ be an arbitrary closed set with $J \supseteq \{j \mid x_j \in \text{Vars}(C)\}$, and let $E$ be any clause in $y$-variables with

$$\text{Vars}(E) = \{y_i \mid i \in \text{Ker}(J)\}$$

such that $E[A]$ and $C$ are simultaneously falsifiable. Then

$$D(\tau \vdash E) \leq \frac{r}{2} \cdot \log_2 |\Pi|. $$

**Proof.** (of Claim 4.1) Let $C, \Pi, J$ and $E$ satisfy the assumptions of our claim. The argument proceeds by induction on $|\Pi|$.

**Base** $|\Pi| = 1$, i.e. $C$ contains a sub-clause $\bar{C}$ that appears in $E[A]$ for some $\bar{E} \in \tau$. Since $\text{Vars}(\bar{C}) = \bigcup_{y_j \in \text{Vars}(E)} \{x_j \mid j \in J_i(A)\}$ and $\{x_j \mid j \in J\} \supseteq \text{Vars}(C) \supseteq \text{Vars}(\bar{C})$, we conclude that $\{i \in [m] \mid y_i \in \text{Vars}(E)\} \subseteq \text{Ker}(J)$, that is $\text{Vars}(\bar{E}) \subseteq \text{Vars}(E)$. Also,
Since only remains to show that falsifiable by our assumption (and simply by setting additionally corresponding sub-proof Case 1, Fix arbitrarily an assignment \( \alpha \) to \( \{ x_k \mid k \in J \} \) falsifying both \( E[A] \) and \( C \). Assume that the last application of the resolution rule has the form

\[
\begin{array}{c}
C_0 \lor x_j \\
C_0 \lor \bar{x}_j \\
\end{array}
\]

Thus we can apply the inductive assumption to the clause \( C \), to the child labeled by \( \text{Vars}(E) = \{ y_i \mid i \in \text{Ker}(\tilde{J}) \} \) and simultaneously falsifiable with \( E \). We conclude that \( D(\tau \vdash E) \leq r \cdot \log_2 |\Pi| \leq r \cdot \log_2 |\Pi| \).

Case 2, \( j \notin J \).

One of the two sub-trees \( \Pi_0, \Pi_1 \) (say, \( \Pi_0 \)) determined by the children of the root has size \( \leq |\Pi|/2 \), and we assume w.l.o.g. that it corresponds to the child labeled by \( C \). Since \( w(C \lor x_j) \leq r/4 \) by our assumption, we can apply Lemma 2.3 to the set \( J' \equiv \{ j' \mid x_{j'} \in \text{Vars}(C \lor x_j) \} \). This will give us a closed \( \tilde{J} \supseteq \{ j' \mid x_{j'} \in \text{Vars}(C \lor x_j) \} \) with \( |\tilde{J}| \leq r/2 \), and our goal is to prove that every clause \( \tilde{E} \) with \( \text{Vars}(\tilde{E}) = \{ y_i \mid i \in \text{Ker}(\tilde{J}) \} \) and simultaneously falsifiable with \( E \) satisfies the assumptions of Claim 4.1 with \( C := C \lor x_j \), \( J := \tilde{J} \) and \( E := \tilde{E} \) (the rest will be easy). For that we only have to extend our original assignment \( \alpha \) to the variables \( \{ x_j \mid j \in J \cup \tilde{J} \} \) in such a way that it will falsify both \( \tilde{E}[A] \) and \( C \lor x_j \).

Since \( C \leq C \lor C_1 \leq C \) is already falsified by \( \alpha \), the latter task can be achieved simply by setting additionally \( \alpha(x_j) \overset{\text{def}}{=} 0 \) (\( x_j \notin \text{dom}(\alpha) \) since \( j \notin J \)). Also, every literal \( y_i' \) of a variable \( y_i \in \text{Vars}(E) \lor \text{Vars}(\tilde{E}) \) maps to \( y_i'[A] = \bigoplus_{j \in J(A)} x_j \oplus 0 \oplus 1 \) and, since \( J(A) \subseteq J \), it has been already decided by \( \alpha \). As \( E \) and \( \tilde{E} \) are simultaneously falsifiable by our assumption (and \( \alpha \) falsifies \( y_i'[A] \)), \( \alpha(y_i[A]) \) is actually equal to \( \tilde{\epsilon} \). It only remains to show that \( \alpha' \) can be extended in such a way that it sets all \( y_i[A] \) for \( i \in \text{Ker}(\tilde{J}) \setminus \text{Ker}(J) \) to fixed values predetermined to falsify the formula \( \tilde{E}[A] \).

Let \( A' \) be the matrix obtained from \( A \setminus J \) by additionally removing the column \( j \) from it. Since \( A \setminus J \) is an \( (r/2, 3/2) \)-boundary expander, \( A' \) is an \( (r/2, 1/2) \)-boundary expander. Also, \( \text{Ker}(\tilde{J}) \setminus \text{Ker}(J) \) is a set of rows of cardinality \( \leq r/2 \), therefore \( \partial_{A'}(I) \neq \emptyset \) for every non-empty subset \( I \subseteq \text{Ker}(\tilde{J}) \setminus \text{Ker}(J) \). Applying reverse induction, we can write \( \text{Ker}(\tilde{J}) \setminus \text{Ker}(J) \) as an ordered set: \( \text{Ker}(\tilde{J}) \setminus \text{Ker}(J) = \{ i_1, \ldots, i_{\ell} \} \) in such a way that for every \( \nu \in [\ell] \) the set of columns \( J_{i_{\nu}}(A') \setminus \bigcup_{\mu=1}^{\nu-1} J_{i_{\mu}}(A') \) is not empty. Fix arbitrarily \( j_{\nu} \in J_{i_{\nu}}(A') \setminus \bigcup_{\mu=1}^{\nu-1} J_{i_{\mu}}(A') \). Now, we first extend \( \alpha' \) to \( \{ x_j \mid j \in (J \cup J') \setminus \{ j_1, j_2, \ldots, j_{\ell} \} \} \)
arbitrarily (say, by zeros) and then consecutively extend it to $x_{j_1}, \ldots, x_{j_k}$ so that the linear forms $\bigoplus_{j \in J_i(A)} x_j, \ldots, \bigoplus_{j \in J_i(A)} x_j$ are set to the right values.

In conclusion, $E$ satisfies the assumptions of Claim 4.1 with $C := C_0 \lor x_j$. Since $C_0 \lor x_j$ has a proof from $\tau[A]$ of width $\leq r/4$ and size $\leq |\Pi|/2$, $D(\tau \vdash E) \leq 4 (\log_2 |\Pi| - 1)$. This conclusion holds for an arbitrary clause $E$ in the variables $\{ y_i \mid i \in \text{Ker}(J) \}$ simultaneously falsifiable with $E$. Now we resolve all these clauses in the brute-force way along all the variables $\{ y_i \mid i \in \text{Ker}(J) \setminus \text{Ker}(J) \}$. Since the depth of this added brute-force proof is at most $r/2$, we get a proof of $E$ in depth $\frac{r}{2} \log_2 |\Pi|$.

This completes the analysis in case 2 of the inductive step. Claim 4.1 is proved. □

Theorem 3.2 is now immediate. If $\tau$ is a contradiction and $\Pi$ is a refutation of $\tau[A]$ with $w(\Pi) \leq r/4$, we simply apply Claim 4.1 with $C := 0$, $J := \emptyset$ and $E := 0$.

For Theorem 3.1, we are going to apply Theorem 3.2 to $\tau[A]$, where $\tau$ is the contradiction from Proposition 2.1 and $A$ is the (random) matrix guaranteed by Lemma 2.2.

**Proof of Theorem 3.1.**

First of all we can assume that $k \geq 12$ since otherwise already the contradictions from Proposition 2.1 will do. Set $w := n^{1-\epsilon}/k$, $r := 4w$, $s := [k/4] \geq 3$, $c := 2$ and choose the parameter $m$ as the smallest value for which (8) is satisfied. Clearly, $m \geq (n/kw)^{\Omega(k)} \geq n^{\Omega(k)}$. It turns out that $m \leq n^2$ then, as before, we simply take the 4-CNF contradiction $\tau_n$ provided by Proposition 2.1. Otherwise we take the formula $\tau_m$ provided by that proposition and compose it with an $m \times n (r, s, 2)$-expander $A$ guaranteed by Lemma 2.2.

Recall that $D(\tau_m \vdash 0) \geq \Omega(m/\log m)$. Hence Theorem 3.2 implies that every tree-like refutation $\Pi$ of the $k$-CNF contradiction $\tau_m[A]$ with $w(\Pi) \leq w$ must have size at least

$$|\Pi| \geq \exp \left( \Omega \left( \frac{m}{r \log m} \right) \right) \geq \exp \left( \Omega \left( \frac{m}{n \log m} \right) \right) \geq \exp(m^{\Omega(1)}) \geq \exp(n^{\Omega(k)}).$$

It only remains to remark that the width 6 refutation of $\tau_m$ stipulated by Proposition 2.1 can be converted into a width $O(k)$ refutation of $\tau_m[A]$ simply by applying the operator $E \mapsto E[A]$ to its lines and filling in the blanks by naive brute-force derivations.

5. OPEN PROBLEMS

Our first (vaguely defined) open question is clear from the context: identify or prove more “supercritical” tradeoffs. At this point it is already clear that this peculiar phenomenon is rare, but is it extremely rare? One natural place to look for more examples (given the abundance of traditional tradeoffs) is propositional space complexity.

Our result is a bit incomplete since the lower bound is doubly exponential only in the number of variables, not in the size of the contradiction. We remark that by contrast, in [Berkholz 2012] the size of the contradiction stays polynomial even when the minimum refutation width is unbounded. Is there any way to combine the small size of contradictions provided by Berkholz’s method with a larger interval $[\mu_{\min}, \mu]$ in which the lower bound holds, as in our paper? Even more ambitiously, perhaps tradeoffs of this kind can be proved for contradictions that not only have small size, but also small (say, constant) width? Attempting a rigorous formulation (there are many other ways to pinpoint this question), do there exist contradictions $\tau_n$ that possess constant width refutations (and hence in particular $w(\tau_n) \leq O(1)$), but such that any such refutation must necessarily have tree-like size $\exp(n^2)$?
Acknowledgement
I am greatly indebted to Jakob Nordström and the anonymous referee for extensive and very useful comments on an earlier version of this paper.

REFERENCES

A. APPENDIX
Here we give self-contained proofs of Lemmas 2.2 and 2.3.
Lemma 2.2. Let \( n \to \infty \) and \( m, s, c \) be arbitrary integer parameters possibly depending on \( n \) such that \( c \leq \frac{3}{4}s \) and
\[
r \leq o(n/s) \cdot m^{c/2}.
\]
Then for sufficiently large \( n \) there exist \( m \times n \) \((r, s, c)\)-boundary expanders.

Proof. This lemma and its proof is identical to [Alekhnovich et al. 2004, Theorem 5.1], except that we relax some restrictions on the parameters. We construct a random \( m \times n \) matrix \( A \) by picking independently in each row \( s \) uniformly random entries with repetitions (the latter feature is not crucial, but it does make calculations neater).

That is, we let \( J_i(A) \stackrel{\text{def}}{=} \{j_{i1}, \ldots, j_{is}\} \), where \( \{j_{i\nu}\} \ (i \in [m], \nu \in [s]) \) is a collection of \( ms \) independent random \([n]\)-valued variables.

Recall that a matrix \( A \) is an (ordinary) \((r, s, c)\)-expander if, again, \(|J_i(A)| \leq s\) for all \( i \in [m] \), and for every \( I \subseteq [m] \) with \(|I| \leq r \) we have \( |\bigcup_{i \in I} J_i(A)| \geq c \cdot |I| \). Thus, the only difference from boundary expanders consists in replacing \( \partial_A(I) \) with \( \bigcup_{i \in I} J_i(A) \).

Claim A.1. Every \((r, s, \frac{c+2}{2})\)-expander is an \((r, s, c)\)-boundary expander.

Proof. (of Claim A.1) Since every column \( j \in \bigcup_{i \in I} J_i(A) \setminus \partial_A(I) \) belongs to at least two sets \( J_i(A) \) \((i \in I) \), we have the bound
\[
|\bigcup_{i \in I} J_i(A)| \leq |\partial_A(I)| + \frac{1}{2} \left( \sum_{i \in I} |J_i(A)| - |\partial_A(I)| \right) \leq \frac{1}{2} (s|I| + |\partial_A(I)|).
\]
On the other hand, \(|\bigcup_{i \in I} J_i(A)| \geq \frac{s+c}{2}|I|\) since \( A \) is an \((r, s, \frac{c+2}{2})\)-expander. The required inequality \(|\partial_A(I)| \geq c \cdot |I|\) follows.

Thus, it remains to prove that \( A \) is an \((r, s, c')\)-expander with probability \( 1 - o(1) \), where \( c' \stackrel{\text{def}}{=} \frac{c+2}{2} \). Let \( p_\ell \) be the probability that any given \( \ell \) rows of the matrix \( A \) violate the expansion property. By the union bound,
\[
P[A \text{ is not a } (r, s, c')\text{-expander}] \leq \sum_{\ell=1}^{r} p_\ell \cdot m^\ell.
\]
On the other hand,
\[
p_\ell = P[|\{j_{i\nu}| i \in I, \nu \in [s]\}| \leq c'|I|] \leq \left( \frac{n}{c'|I|} \right)^{\ell} \cdot \left( \frac{c'|I|}{n} \right)^{s|I|}
\]
\[\leq O(1)^{c'|I|} \cdot \left( \frac{c'|I|}{n} \right)^{s|I|} \cdot \left\{ O((s|I|)/n) \right\}^{(s-c')|I|},\]
where for the last inequality we used that \( c' \leq \frac{5}{8} c \leq \frac{7}{8} s \) and hence \( c' \leq O(s-c) \). Thus,
\[
P[A \text{ is not a } (r, s, c')\text{-expander}] \leq \sum_{\ell=1}^{r} O((s|I|)/n)^{(s-c')|I|} m^\ell \leq \sum_{\ell=1}^{r} \left( O((sr)/n) \right)^{(s-c')|I|} m^\ell,
\]
and since \( m(sr/n)^{s-c'} = m(sr/n)^{(s-c)/2} \leq o(1) \) by our assumption, we obtain a decaying geometric progression. Lemma 2.2 follows.

Lemma 2.3. Let \( A \) be an \( m \times n \) \((r, 2)\)-boundary expander. Then for every \( J \subseteq [n] \) with \(|J| \leq r/4\) there exists \( \tilde{J} \supseteq J \) such that \(|\text{Ker} (\tilde{J})| \leq 2|J|\) and \( A \setminus \tilde{J} \) is an \((r/2, 3/2)\)-boundary expander.
We define a strictly increasing sequence of sets of columns $J_0 \subset J_1 \subset \ldots \subset J_t \subset \ldots$ as follows. Let $J_0 \overset{\text{def}}{=} J$. For $t > 0$, we first let $S_t$ be an arbitrary set of rows of size $\leq r/2$ violating the $(r/2, 3/2)$-boundary expansion condition in $A \setminus J_{t-1}$ if such a set exists; otherwise, the construction terminates. Then we let

$$J_t \overset{\text{def}}{=} J_{t-1} \cup \bigcup_{i \in S_t} J_i(A).$$

Note that since the chain $J_0 \subset J_1 \subset \ldots \subset J_t \subset \ldots$ is strictly increasing, the process does terminate at some point; let $J_T$ be the final set in this chain. We claim that $b_{J_T} := J_T$ has the required properties, and the only thing that has to be checked is that $|\ker(J_T)| \leq 2|J|$. For that we prove by induction on $t = 0, \ldots, T$ that $|\ker(J_t)| \leq 2|J|$. 

**Base case** $|\ker(J)| \leq 2|J|$ immediately follows from the fact that $A$ is an $(r, 2)$-boundary expander and $|J| \leq r/4$.

**Inductive step.** Assume that $|\ker(J_{t-1})| \leq 2|J|$ for some $1 \leq t \leq T$, and let us prove that $|\ker(J_t)| \leq 2|J|$.

Since $|S_t| \leq r/2$, $|\ker(J_{t-1})| \leq 2|J| \leq r/2$ and $\ker(J_{t-1}) \cup S_t \subseteq \ker(J_t)$, we can choose a set of rows $I$ such that $\ker(J_{t-1}) \cup S_t \subseteq I \subseteq \ker(J_t)$ and

$$|I| = \min(r, |\ker(J_t)|). \quad (9)$$

Applying to $I$ the expansion condition, we get

$$|\partial_A(I)| \geq 2|I|.$$ 

On the other hand, $I \subseteq \ker(J_t)$ implies that

$$\partial_A(I) \subseteq J \cup \bigcup_{s=1}^t \partial_A\setminus J_{s-1}(S_s).$$

Since $S_s$’s violate the $(r/2, 3/2)$-boundary expansion conditions in respective matrices, we conclude that

$$|\partial_A(I)| \leq |J| + \frac{3}{2} \sum_{s=1}^t |S_s| \leq |J| + \frac{3}{2}|I|,$$

where for the latter inequality we used the fact $I \supseteq S_1 \cup S_2 \cup \ldots \cup S_t$. Comparing these two inequalities, we find that $|I| \leq 2|J| \leq r/2$. Now (9) implies that in fact $|I| = |\ker(J_t)|$ that completes the inductive step in the proof of Lemma 2.3.  
