On Bounded Depth Proofs for Tseitin Formulas on the Grid; Revisited

Johan Håstad and Kilian Risse
KTH Royal Institute of Technology
Stockholm, Sweden
johanh, kilianr@kth.se

Abstract—We study Frege proofs using depth-$d$ Boolean formulas for the Tseitin contradiction on $n \times n$ grids. We prove that if each line in the proof is of size $M$ then the number of lines is exponential in $n/(\log M)^{O(d)}$. This strengthens a recent result of Pitassi et al. [12]. The key technical step is a multi-switching lemma extending the switching lemma of Håstad [8] for a space of restrictions related to the Tseitin contradiction.

The strengthened lemma also allows us to improve the lower bound for standard proof size of bounded depth Frege refutations from exponential in $\Omega(n^{1/2d^2})$ to exponential in $\Omega(n^{1/(2d-1)})$.

Index Terms—proof complexity, bounded depth Frege

I. INTRODUCTION

Mathematicians like proofs, formal statements where each line follows by simple reasoning rules from previously derived lines. Each line derived in this manner, assuming that the reasoning steps are sound, can give us some insight into the initial assumptions of the proof. A particularly interesting consequence is contradiction. Deriving an obviously false statement allows us to conclude that the initial assumptions, also called axioms, are contradictory. We continue the study of Frege proofs of contradiction where each line in the proof is a Boolean formula of depth $d$. This subject has a long tradition, so let us start with a very brief history.

A very basic proof system is resolution: each line of such a proof simply consists of a disjunction of literals. The derivation rules of resolution are also easy to understand and simple to implement, but the proof system nevertheless gives rise to reasonably short proofs for some formulas. It is far from easy to give lower bounds for the size of proofs in resolution but it has been studied for a long time and by now many strong bounds are known.

An early paper by Tseitin [18] defined an important class of contradictions based on graphs that is central to this and many previous papers. For each edge there is a variable and the requirement is that the parity of the variables incident to any given node sum to a particular bit which is called the charge of that vertex. If the sum of the charges is one modulo two this is a contradiction. For a subsystem of resolution, called regular resolution, Tseitin proved exponential lower bounds on refutations of these formulas. After this initial lower bound it took almost another two decades before the first strong lower bound for general resolution was obtained by Haken [5], whose lower bound applied to the pigeonhole principle (PHP). Many other resolution lower bounds followed, but as we are not so interested in resolution and rather intend to study the more powerful proof system with formulas of larger, though still bounded, depth $d$ on each line, let us turn to such proof systems.

The study of proofs with lines limited to depth $d$ dates back several decades. A pioneering result was obtained by Ajtai [1] who showed that the PHP cannot be proved in polynomial size for any constant depth $d$. Developments continued in the 1990s and polynomial size proof were ruled out for values of $d$ up to $O(\log \log n)$ for both the PHP [11], [13] as well as the Tseitin contradiction defined over complete [19] and expander graphs [2].

These developments followed previous work where the computational power of the class of circuits$^1$ of depth $d$ was studied [4], [6], [15]–[17], [20]. It is not surprising that it is easier to understand the computational power of a single circuit rather than to reason about a sequence of formulas giving a proof. This manifested itself in that while the highest value of $d$ for which strong bounds were known for size of proofs remained at $O(\log \log n)$, the results for circuit size extended to almost logarithmic depth.

This gap was (essentially) closed in two steps. First

$^1$When the depth is small, there is no major difference between circuits and formulas so the reader should feel free to ignore this difference.
Pitassi et al. [14] proved superpolynomial lower bounds for $d$ up to $o(\sqrt{\log n})$ and then Håstad [8] extended this to depth $\Theta(\frac{n}{\log\log n})$ which, up to constants, matches the result for circuits.

The key technique used in most of the described results is the use of restrictions. These set most of the variables to constants which simplifies the circuit or formulas studied. If done carefully one can at the same time preserve the contradiction refuted or the function computed. Of course one cannot exactly preserve the contradiction and to be more precise a contradiction with parameter $n$ before the restriction turns into a contradiction of the same type but with a smaller parameter, $n/T$, after the restriction.

The simplification under a restriction usually takes place in the form of a switching lemma. This makes it possible to convert depth $d$ formulas to formulas of depth $d - 1$. A sequence of restrictions is applied to reduce the depth to (essentially) zero making the circuit or formula straightforward to analyze. The balance to be struck is to find a set of restrictions that leave a large resulting contradiction but at the same time allows a switching lemma to be proved with good parameters.

In proof complexity the most commonly studied measure is the total size of a proof. There are two components to this size, the number of reasoning steps needed and the size of each line of the proof. In some cases, such as resolution, each line is automatically bounded in size and hence any lower bound for proof size is closely related to the number of proof steps. In some other situation the line sizes may grow and an interesting question is whether this can be avoided.

This line of investigation for Frege proofs with bounded depth formulas was recently initiated by Pitassi et al. [12]. They consider the Tseitin contradiction defined over the grid of size $n \times n$, a setting where strong total size lower bounds for Frege refutations of bounded depth had previously been given by Håstad [8]. If each line of the refutation is limited to size $M$ and depth $d$, then Pitassi et al. [12] showed that the Frege proof must consist of at least $\exp(n/2^{O(d\sqrt{\log M})})$ many lines. For most interesting values of $M$ this greatly improves the bounds implied by the results for total proof size. In particular if $M$ is a polynomial the lower bounds are of the form $\exp(n^{1 - o(1)})$, as long as $d = o(\sqrt{\log n})$, in contrast to the total size lower bounds of the form $\exp(n^{\Omega(1/d)})$. Pitassi, Ramakrishnan, and Tan [12] rely on the restrictions introduced by Håstad [8] but analyze them using the methods of Pitassi et al. [14].

We study the same Tseitin contradiction on the grid and improve the lower bounds to $\exp(n/(\log M)^{O(d)})$, a bound conjectured by Pitassi et al. [12]. These bounds are the strongest bounds that can be proved by the present methods and even if we cannot match them by constructing actual proofs we can at least represent the intermediate results of a natural proof by such formulas. We discuss this in more detail below.

### A. Overview of proof techniques

The structure of the proof of our main result follows the approach of [12] but relies on proving much sharper variants of the switching lemma.

In a standard application of a switching lemma to proof complexity one picks a restriction and demands that switching happens to all depth two formulas in the entire proof. Each formula switches successfully with high probability and by an application of a union bound it is possible to find a restriction to get them all to switch simultaneously.

The key idea of [12] is that one need not consider all formulas in the proof at the same time. Rather one can focus on the sub-formulas of a given line. It is sufficient to establish that these admit what is called an $\ell$ partial common decision tree of small depth. This is a decision tree with the property that at each leaf, each of the formulas can be described by a decision tree of depth $\ell$. It turns out that this is enough to analyze the proof and establish that it cannot derive contradiction. The key property is that it is sufficient to only look at the constant number of formulas involved in each derivation step and analyze each such step separately.

The possibility to compute a set of formulas by an $\ell$ common partial decision tree after having been hit by a restriction is exactly what is analyzed by what has become known as a “multi-switching lemma” as introduced by [7], [10]. This concept was introduced in order to analyze the correlation of a small circuits of bounded depth with parity but turns out to also be very useful in the current context.

Even though there is no general method, it seems like when it is possible to prove a standard switching lemma there is good hope to also prove a multi-switching lemma with similar parameters. This happens when going from [6] to [7] and when going from [14] to [12]. We follow the same approach here and this paper very much builds on [8]. We need a slight modification of the space of restrictions and changes to some steps of the proof, but a large fraction of the proof remains untouched. Let us briefly touch on the necessary changes.

The switching lemma of Håstad [8] has a failure probability to not switch to a decision tree of depth $s$ of the form $(A/s)^{\Omega(s)}$ where $A$ depends on other
parameters. As a first step one needs to eliminate the factor $s$ in the base of the exponent. This triggers the above mentioned change in the space of restrictions. This change enables us to prove a standard switching lemma with stronger parameters. This results in an improvement of the lower bound for total proof size from $\exp(\Omega(n^{1/3d^2}))$ to $\exp(\Omega(n^{1/(2d-1)}))$. Even though the exponent’s exponent is probably still off by a factor of 2, this is a substantial improvement in the parameters.

The high level idea of the proof of the multi-switching lemma is that for each of the formulas analyzed we try to construct a decision tree of depth $\ell$. If this fails then we take the long branch in the resulting decision tree and instead query these variables in the common decision tree. A complication that arises is that the answers on the long path in the local decision tree and the answers on a potentially long branch in the common decision tree are different. This causes us to analyze a new combinatorial game on the grid, as defined in section III.

B. Constructing small proofs

Let us finally comment on a possible upper bound; how to construct efficient refutations. If we are allowed to reason with linear equations modulo two then the Tseitin contradiction has efficient refutations. In particular on the grid we can sum all equations in a single column giving an equation containing $O(n)$ variables that must be satisfied. Adding the corresponding equation for the adjacent column maintains an equation of the same size and we can keep adding equations from adjacent columns until we have covered the entire grid. We derive a contradiction and we never use an equation containing more than $O(n)$ variables.

If we consider resolution then it is possible to represent a parity of size $m$ as a set of clauses. Indeed, looking at the equation $\sum_{i=1}^{m} a_i = 0$ we can replace this by the $2^{m-1}$ clauses of full width where an odd number of variables appear in negative form. Now replace each parity in the above proof by its corresponding clauses. It is not difficult to check that Gaussian elimination can be simulated by resolution. Given linear equation $L_1 = b_1$ and $L_2 = b_2$ with $m_1$, and $m_2$ variables respectively, and both containing the variable $x$ we want to derive all clauses representing $L_1 \oplus L_2 = b_1 \oplus b_2$. We have $2^{m_1-1}$ clauses representing the first linear equation and the $2^{m_2-1}$ clauses representing the second linear equation. Now we can take each pair of clauses and resolve over $x$ and this produces a good set of clauses. If $L_1$ and $L_2$ do not have any other common variables we are done. If they do contain more common variables then additional resolution steps are needed but these are not difficult to find and we leave it to the reader to figure out this detail. We conclude that Tseitin on the grid allows resolution proofs of length $2^{O(n)}$.

Let us consider proofs that contain formulas of depth $d$ and let us see how to represent a parity. Given $\sum_{i=1}^{m} x_i = 0$ we can divide the variables in to groups of size $(\log M)^{d-1}$ and write down formulas of depth $d$ and size $M$ that represent the parity and the negation of the parity of each group. Assume that the output gate of each of these formulas is an or. We now use the above clause representation of the parity of the groups and get a set of $2^{m/(\log M)^{d-1}}$ formulas of size $mM/(\log M)^{d-1}$ that represent the linear equations. This means that we can represent each line in the parity proof by about $2^{n/(\log M)^{d-1}}$ lines of size about $M$. We do not know how to syntactically translate a Gaussian elimination step to some proof steps in this representation and thus we do not actually get a proof, only a representation of the partial results.

C. Organization

This is an extended abstract of the full version [9]. Many proofs and details are not present in this version. We refer the interested reader to the full version [9] for more details.

We start in section II with some preliminaries. We then describe in section III a combinatorial game, central to the multi-switching lemma. In section IV we recap the restrictions used and define the notion of $t$-evaluations in section V. Following this in section VI we state and prove our main theorems assuming the new switching lemmas. Finally in sections VII and VIII we explain the changes needed for the single-switching lemma and give a proof outline of the multi-switching lemma.

II. Preliminaries

We have a graph $G$ which we call “the grid” but to avoid problems at the perimeter we in fact use the torus. In other words we have nodes indexed by $(i,j)$, for $0 \leq i, j \leq n-1$ where $n$ is an odd integer and a node $(i,j)$ is connected to the four nodes at distance 1, i.e. where one coordinate is identical and the other moves up or down by 1 modulo $n$. For each node $v$ we have a charge $\alpha_v$ and for each edge $e$ in the graph we have a variable $x_e$. A Tseitin formula is given by a set of linear equalities modulo 2. That is, for each vertex $v$ in $G$ we have

$$\sum_{e \ni v} x_e = \alpha_v.$$  

The main case we consider, which we call “the Tseitin contradictions” is when $\alpha_v = 1$ for each $v$. We do use
more general charges in intermediate steps and hence the following lemma from [8] is useful for us.

Lemma II.1. Consider the Tseitin formulas with charges $\alpha_v$. If $\sum_v \alpha_v = 0$ this formula is satisfiable and has $2^n$ solutions where the positive integer $r_n$ depends only on $n$ and not on the value of $\alpha_v$.

As a converse to the above lemma, when $\sum_v \alpha_v = 1$ it is easy to see, by summing all equations, that the system is contradictory.

We are interested in proofs in the form of deriving the constant false from these axioms. The exact reasoning rules turn out not to be of central importance. The important properties of these rules are that they are sound and of constant size.

In order to prove that a Frege proof that consists of small and shallow lines is long we need the following notion. A decision tree $T$ is an $\ell$ common partial decision tree for $T_1, \ldots, T_m$ of depth $t$ if

1) $T$ is of depth $t$, and
2) for every $T_i$ and branch $\pi$ in $T$ there are decision trees $T(i, \pi)$ of depth $\ell$ such that the following holds. Let $T_i$ be the decision tree obtained from $T$ by appending the trees $T(i, \pi)$ at the corresponding leaf $\pi$ of $T$. Then, if a branch $\pi'$ in $T_i$ ends in a leaf labeled $b$, it holds that $T_i[\pi'] = b$.

III. A GAME ON THE GRID

As discussed in the introduction our new lower bound for the number of lines of a proof with short lines needs a multi-switching lemma and it turns out that the decision which variables to include is described by a combinatorial game. Let us discuss this game.

The game is played on the grid between an adversary $A$ and a player $P$. They take turns picking vertices and edges on the $n \times n$ grid. Once a vertex is picked it can never be picked again. The set of picked vertices is called $S$. The vertices outside $S$ are called “free”. The total number of picked nodes always remains less than $n/2$ and hence there is always a large connected component in the complement of $S$. Other connected components in the complement are called “small”. Some of the picked elements are called “active”.

The task of $P$ is to pick as few vertices as possible such that the following properties hold.

1) The number of picked nodes has the correct parity in some special components of $S$ described below.
2) The size of any small component in the complement of $S$ is even.

The game starts with an empty grid, and takes place in rounds where $A$ decides when to start the next round. $A$ can do two types of moves.

1) Pick an arbitrary new vertex $v$ and make it active. This is called a “simple” move.
2) Declare that a round is over. In this case $A$ can make any edge between an active vertex and a free vertex active. Each connected component must have an even number of activated edges leading in to it. This second type of move is called a completion move. When this move is completed all vertices become inactive and the next round starts.

After a simple move $P$ must pick some vertices to form a connected component of even size jointly with the just placed vertex. $P$ must also make sure that each connected component of the complement is of even size. Any vertex picked by $P$ in response to a simple move becomes active. Note that in this situation $P$ picks an odd number of vertices and hence at least one.

After a completion move $P$ must pick the free vertices with at least one adjacent active edge. It may pick some more vertices to achieve the following.

1) The parity of the size of each connected component of the just picked vertices must equal to the parity of active edges adjacent to it.
2) The number of vertices in any small connected component in the complement is even.

Although this looks complicated please note that if the there is only one active edge going in to the nodes $P$ must pick and these do not split any connected component of the complement, then these forced nodes is all that $P$ needs to select.

What forces $P$ to act in general is the creation of small odd size components in the complement of $S$ due to making the “obvious” choices. For any such component $C$, $P$ needs to add vertices to $S$ to make it of even size. It is also restricted to only adding vertices adjacent to a supplied starting vertex. This vertex is in $S$ but connected to at least some vertex in $C$. We call this “evenizing” with starting point $w$. All connected components of the complement created in this process must be made of to be of even size. It is simple to see that this can always be done, simply add any vertex adjacent to $w$. If this does not split $C$ in to at least two components then $P$ is done. Otherwise $P$ can simply recurse on any created component of odd size with the chosen vertex as the starting point. We must prove that, over the course of the entire game, $A$ cannot force $P$ to add too many vertices.

In order to prove this we set up a potential function. For each connected component of the complement con-
sider its edges to elements of $S$. For each edge to an active vertex we assign four points and for each other edge one point. Suppose the total number of points for component $C_i$ is $f_i$ and this number is called the score of $C_i$. We have a parameter $T$ and we say that each component of size at most $T$ is ultra small. We later fix $T$ to a suitable constant. A component that is not ultra small is called sizeable. This includes the large component. We now define the potential as

$$\sum_i f_i + G - D(F - 1)$$

where the sum is over components that are sizeable, $F$ the number of components that are sizeable, $D$ is a constant to be chosen suitably, and $G$ is the number of ultra small components. For $G$ we only count a component the first time it becomes ultra small. Further splitting of an ultra small component is ignored. The reason for using $(F - 1)$ is that we want to start the potential at 0 and hence not count the large component in this number.

We want to prove that this potential increases by at most a constant for each simple move and decreases by at least one half for other moves. By setting $T$ large enough (after we have chosen $D$) we make sure that $f_i \geq 2D$ for any component of size at least $T$.

Let us first analyze simple moves. When $A$ chooses a vertex it might increase $\sum_i f_i$ by at most 16. This might also cause a component of the complement of $S$ to split. To analyze the cost of such a split we first pay the increase by the addition of the extra vertex to $S$ in the form of increase to $f_i$. We then see how the splitting of a component of the complement affects the potential.

First note that splitting an ultra small component does not affect the potential (remember that we do not count this as an increase in $G$) and thus we are interested in splitting a sizeable component. We have sequence of simple lemmas.

**Lemma III.1.** If a sizeable component splits into ultra small components then the potential decreases by at least $D - 4$.

**Proof.** Suppose $C_i$ splits. This means that the term $f_i - D$ disappears in the potential. By construction this is at least $D$. We might have an increase of $G$ by 4 but no other increase. The lemma follows. 

Next we have.

**Lemma III.2.** If a sizeable component splits and the result contains at least two sizeable components then the potential decreases by at least $D$.

**Proof.** The creation of a sizeable component increases $F$. Any ultra small component created increases $G$ by one but at the same time its score is removed from the sum causing a decrease of that sum by at least 4.

Finally we analyze the third possibility.

**Lemma III.3.** If a sizeable component splits into a sizeable component and one or more ultra small components the potential decreases by at least three for each component split off.

**Proof.** The value of $F$ does not change. Any ultra small component created increases $G$ by one but its score of at least 4 is removed from the sum $\sum_i f_i$.

The above lemmas imply that the splitting of components only decreases the potential. What remains is to analyze the cost when $P$ is forced to evenize an odd size component. By “cost” we here mean increase in potential. We might have a negative cost which is a decrease in potential.

**Lemma III.4.** The cost of evenizing a component with an active starting point is at most $11 - m/2$ where $m$ is the number of moves made by $P$ in sizeable components. The cost of evenizing an ultra small component is 0.

**Proof.** Consult the full version of this paper.

The above takes care of all simple moves. Let us look at completion moves.

**Lemma III.5.** A completion decreases the potential by at least the number of active edges chosen by $A$. This includes the forced response by $P$.

**Proof.** The first that happens is that an edge which costs 4 is replaced by an inactive vertex next to it. This results in at most three edges of cost one and is hence a decrease of at least one in potential. If several active edges go to the same vertex $P$ has to add two vertices but this gives a decrease of at least two. Now unless this causes a split of a component we are done.

If it splits an ultra small component then there is no further change in the potential. If it splits a sizeable component then we might have to evenize two components and the following lemma is what we need.

**Lemma III.6.** The cost of evenizing a component with an inactive starting point is at most $3 - m$ where $m$ is the number of vertices added by $P$ to sizeable components. The cost of evenizing an ultra small component is at most 0.
Let us assume this lemma then finish the proof of lemma III.5. As many times previously unless we get exactly one non ultra small component it is easy to prove that there is a decrease so assume that this is the case. Each ultra small component decreases the potential by a least three and this is sufficient to pay for the evenizing of the component and this is demonstrated by lemma III.6.

The proof of lemma III.6 is surprisingly much simpler than the proof of lemma III.4. The key difference is that new edges added only cost one and not four. This makes it much easier to compensate the cost of new edges by the loss in potential due to the appearance of ultra small components.

**Proof of lemma III.6.** If the response of putting a vertex, \( v \), next to the starting vertex is sufficient then we have \( m = 1 \) and the potential increases by at most 2 as three edges are added and one is removed. The lemma is thus true in this case and let us analyze what happens to the potential if \( v \) causes the component of the complement to split. As before, unless it is a sizeable component that splits and the result is exactly one sizeable component and one or more ultra small components, we do have a substantial decrease in the potential due to the loss of a term \( D \).

As in the previous proof the worst case is when \( v \) splits the component into two components \( C_1 \) and \( C_2 \) where the first is sizeable and the second is ultra small and the third neighbor of \( v \) belongs to \( C_1 \). In this case we have added more edges of \( v \) into \( C_1 \). We have removed one edge (between \( v \) and the starting point) and lost the cost of at least three edges that are now part of \( C_2 \). This is a net loss of two to the potential. We need to evenize \( C_1 \) and this cost by induction at most \( 3 - m_1 \) if \( P \) picks \( m_1 \) vertices in this process. Finally we have one more ultra small component and thus the total cost is at most \( 2 - m_1 \). Since \( P \) picks \( m_1 + 1 \) vertices in total, the lemma follows. \( \square \)

We finally state the conclusion of this section.

**Lemma III.7.** If \( A \) makes \( s \) simple moves in the game, then the total number of moves is bounded by \( O(s) \).

**Proof.** The potential increases by \( O(1) \) for each simple move of \( A \). The evenizing of any odd component created costs at most \( O(1) \) but is decreased by \( 1/2 \) for any vertex chosen by \( P \) is a sizeable component. We conclude that the total number of moves in sizeable components is at most \( O(s) \).

As the number of ultra small component created is bounded by the potential, their number is \( O(s) \). In each such component there are \( O(1) \) moves. \( \square \)

**IV. Restrictions**

We use (essentially) the same space of random restriction as [8]. The only difference is the choice in the number of live centers in the partial restrictions. This value changes from \( Cs(n/T)^2 \) to \( C \log n(n/T)^2 \). For completeness we repeat all definitions from [8] but we keep the description brief and for intuition and motivation we refer to [8].

**A. Full restrictions**

In an \( n \times n \) grid we make sub-squares of size \( T \times T \) where \( T \) is odd. In each sub-square we choose \( \Delta = \sqrt{T}/2 \) of the nodes and call them centers. These are located evenly spaced on the diagonal of the \( 3T/4 \times 3T/4 \) central sub-square. This implies that they have separation \( 3\sqrt{T}/2 = 3\Delta \) in both dimensions.

The centers in neighboring sub-squares are connected by paths that are edge-disjoint except close to the endpoints. Let us describe how to connect a given center to a center in the sub-square on top. As there are \( T/4 = \Delta^2 \) rows between the two central areas, for each pair of centers (the \( j \)th center, \( c_j \) in the bottom sub-square and \( j \)th center \( c_j' \) in the top sub-square) we can designate a unique row, \( r_{ij} \) in this middle area.

To connect \( c_j \) to \( c_j' \) we first go \( i \) steps to the left and then straight up to the designated row \( r_{ij} \). This is completed by starting at \( c_j' \) and then going \( j \) steps to the right and down to the designated row. We finally use the appropriate segment from the designated row to complete the path (which might be in either direction).

We index the centers from 1 to \( \Delta \) and hence each path consists of 5 non-empty segments. The first and last segments are totally within the central area while the middle segment is totally in the area between the central areas. Segments two and four go from the central areas to the area in-between.

Connecting \( c_j \) to a center \( c_j' \) in a sub-square to the left is done in an analogous way. There is a unique column \( c_{ij} \) reserved for the pair and the path again consists of five non-empty segments. The first and last segments consist of \( i \) vertical edges up from \( c_j \), and \( j \) vertical edges down from \( c_j' \). We add horizontal segments connecting to the designated column \( c_{ij} \) and the middle segment is along this column. The below lemma is proved in [8].

**Lemma IV.1.** The described paths are edge-disjoint except for the at most \( \Delta \) edges close to an endpoint. For
each edge e, if there is more than one path containing e, these paths all have the same endpoint closest to e.

A restriction is defined by first choosing one center in each $T \times T$ sub-square and then the paths described above connecting these centers. Note that these paths are edge-disjoint. The chosen centers naturally form a $n/T \times n/T$ grid if we interpret the paths between the chosen centers as edges. We proceed to make the correspondence more complete by assigning values to variables.

We choose a solution to the Tseitin formula with charges 0 at the chosen centers and 1 at other nodes. As the number of chosen centers is odd, by lemma II.1, there are many such solutions. For variables not on the chosen paths these are the final values while for variables on the chosen paths we call them suggested values.

For each path $P$ between two chosen centers we have a new variable $x_P$ and for each variable $x_e$ on $P$ it is replaced by $x_P$ if the suggested value of $x_e$ is 0 and otherwise it is replaced by $x_P$.

We claim that with these substitutions we have reduced the Tseitin problem on an $n \times n$ grid to the same problem on an $n/T \times n/T$ grid. This is true in the sense that we have an induced grid when we interpret paths as new edges and we need to see what happens to the axioms.

Given a formula $F$ we can apply a restriction $\sigma$ to it in the natural way resulting in a formula denoted by $F|_\sigma$. Variables given constant values are replaced by constants while surviving variables are replaced by the appropriate negation of the corresponding path-variable.

These just defined restrictions are called full restrictions.

V. Basics for t-Evaluations

The concept of $t$-evaluations was introduced by Krajíček et al. [11] and is a very convenient tool for proving lower bounds on proof size. The content of this section is standard and we follow the presentation of Urquhart and Fu [19] while using the notation of Hästad [8]. We need a generalization of previous notions essentially as introduced by Pitassi et al. [12].

A tree $T$ represents $T_1 \lor \ldots \lor T_s$ if for every branch $\pi$ of $T$ ending in a leaf labeled 1 it holds that there is an $i \in [s]$ such that $T_i|_\pi = 1$, and if $\pi$ ends in a leaf labeled 0, then for all $i \in [s]$ it holds that $T_i|_\pi = 0$. The set of formulas $\Gamma$ has a $t$-evaluation $\varphi$, mapping formulas from $\Gamma$ to decision trees of depth at most $t$, if the following holds.

1) $\varphi$ maps constants to the appropriate decision tree of depth 0,
2) axioms are mapped by $\varphi$ to 1-trees,
3) if $\varphi(F) = T$ then $\varphi(\neg F)$ is a decision tree with the same topology as $T$ but where the value at each leaf is negated, and
4) if $F = \lor_{i \in [s]} F_i$, then $\varphi(F)$ represents $\lor_{i \in [s]} \varphi(F_i)$.

Each line of a proof has its own $t$-evaluation. In order to argue about the proof we need that these different $t$-evaluations are consistent, as explained next.

Let us first define what it means for decision trees to be consistent. Two decision trees $T_1, T_2$ are consistent if for every branch $\pi$ of $T_1$ ending in a leaf labeled $b$ it holds that $T_2|_\pi = b$ and vice-versa. Further, $T_1$ and $T_2$ are $\neg$-consistent, if for every branch $\pi$ of $T_1$ ending in a leaf labeled $b$, it holds that $T_2|_\pi = \neg b$ and vice-versa.

Let us say that two formulas are isomorphic if they only differ in the order of the or’s, and let us say that two formulas $F, G = \neg G'$ are $\neg$-isomorphic if $F$ and $G'$ are isomorphic.

Consider a $t$-evaluation $\varphi$ defined over a set of formulas $\Gamma$ and similarly let $\varphi'$ be a $t$-evaluation defined over the set of formulas $\Gamma'$. The two $t$-evaluations $\varphi$ and $\varphi'$ are consistent if

1) for all isomorphic formulas $F \in \Gamma$ and $F' \in \Gamma'$ it holds that $\varphi(F)$ and $\varphi'(F')$ are consistent, and
2) for all $\neg$-isomorphic formulas $F \in \Gamma$ and $F' \in \Gamma'$ it holds that $\varphi(F)$ and $\varphi'(F')$ are $\neg$-consistent.

We say that a Frege proof has a $t$-evaluation if for every line $\nu$ in the proof we have a $t$-evaluation $\varphi^\nu$ and for all lines $\nu, \nu'$ it holds that $\varphi^\nu$ and $\varphi'^{\nu'}$ are consistent.

Let us consider a Frege proof of depth $d$ and for a line $\nu$ in the proof let $\Gamma^\nu$ be the set of subformulas occuring on line $\nu$. In the following we construct a sequence of restrictions $\sigma_1, \sigma_2, \ldots, \sigma_d$ such that for every line and all formulas of depth at most $k$ we have consistent $t(k)$-evaluations if the formulas are hit by the concatenation $\sigma_k^\nu$ of the first $k$ restrictions in the sequence. When considering proof size we in fact have that all $t(k)$ are equal to the same value $t$, while in the proof when we lower bound the number of small lines, the value $t(k)$ grows as a function of $k$. In fact, in the latter situation, each line has a common part to all decision trees of that line and this common part increses in size with $k$.

Getting back to $t(k)$-evaluations, put different we build by induction on $k$ for every line $\nu$ a $t(k)$-evaluation for all formulas in

$$
\Gamma_k^\nu = \{F \sigma_k^\nu : F \in \Gamma^\nu \land \text{depth}(F) \leq k\}
$$

that are pairwise consistent and we look to extend these $t(k)$-evaluations to $\Gamma_{k+1}^\nu$. To make sure that the domain
of the \( t \)-evaluations does not decrease when we apply a restriction we use the lemma below from [8]. The fact that we allow consistent \( t(k) \)-evaluations, instead of a single \( t(k) \)-evaluation for the entire proof, does not change the proof which is a simple and fairly formal verification and hence omitted.

**Lemma V.1.** Let \( \varphi \) and \( \varphi' \) be two consistent \( t \)-evaluations respectively defined on the set of formulas \( \Gamma \) and \( \Gamma' \), and let \( \sigma \) be a full restriction whose output is a grid of size \( n \). Then, provided that \( t < n/4 \), \( \varphi(F)\sigma \) and \( \varphi'(F)\sigma \) are consistent \( t \)-evaluations whose domain includes \( \Gamma\sigma \), and \( \Gamma'\sigma \) respectively.

The important step of the argument is to use a switching lemma to extend the domain of the \( t(k) \)-evaluation from \( \Gamma_k \) to \( \Gamma_{k+1} \). We give that argument in the next section and here we turn to formulating the punch line once we have a \( t(k) \)-evaluation for a small Frege proof, where we think of \( t(k) \) as small.

It turns out that under these assumptions all lines in the proof are represented by 1-trees. As the the constant false is represented by a 0-tree we can thus not derive the desired contradiction. Hence in order to obtain the desired contradiction the Frege proof must be large, respectively long in the case of Frege proofs of bounded line size.

In order to formalize this argument we need to fix a Frege system so we can argue about the derivation rules. By a result of Cook and Reckhow [3] the precise choice of the Frege system is not important and we choose the same system as [8], [12], [14]. This system consists of the following rules.

- (Excluded middle) \( (p \lor \neg p) \)
- (Expansion rule) \( p \rightarrow (p \lor q) \)
- (Contraction rule) \( (p \lor p) \rightarrow p \)
- (Association rule) \( p \lor (q \lor r) \rightarrow (p \lor q) \lor r \)
- (Cut rule) \( p \lor q, \neg p \lor r \rightarrow q \lor r \)

These rules should be understood in the following manner: a depth \( d \) Frege proof can at any time, by excluded middle, write down a line of the form \( (p \lor \neg p) \) for any formula \( p \) if the line is of depth at most \( d \). Similarly the expansion rule says that if we have derived the formula \( p \), then we can write down the line \( (p \lor q) \) for any formula \( q \) such that the line is of depth at most \( d \). The crucial lemma is as follows.

**Lemma V.2.** Suppose we have a derivation using the above rules starting from the Tseitin axioms defined on the \( n \times n \) grid, that also has a \( t \)-evaluation. Then, if \( t \leq n/8 \), each line in the derivation is mapped to a 1-tree. This, in particular, implies that we cannot derive contradiction.

The proof in the standard case of this lemma is again a tedious and formal verification and can be found in full in [8]. The proof is by induction over the number of derivation steps and the key property is to take any path that leads to 0 in the derived formula and find a path that leads to a 0 in one of the assumptions. The fact that all decision trees are of depth less than \( n/8 \) ensures that it is possible to find a branch of any decision tree that is consistent with the given 0-branch.

In the current case, where each line has its own \( t \)-evaluation, due to consistency, not much is different. We can again take any 0-branch in the decision tree of a derived formula and find a 0-branch in one of the assumptions. Instead of repeating all cases let us do only the most interesting one: the cut rule.

We have \( F = (q \lor r) \) derived on line \( \nu \) and suppose \( \varphi''(F) \) is not a 1-tree. Take a supposed leaf with label 0 in \( \varphi''(F) \) and let \( \tau \) be the assignment leading to this leaf. We know that \( \varphi''(q)\tau \) and \( \varphi''(r)\tau \) are both 0-trees by the definition of a \( t \)-evaluation.

Now suppose \( (p \lor q) \) was derived on line \( \nu' \) less \( \nu \) and \( (\neg p \lor r) \) was derived on line \( \nu'' \) less \( \nu' \). By consistency of \( \nu \) and \( \nu' \) we know that \( \varphi''(q)\tau \) is a 0-tree and, as also \( \nu \) and \( \nu'' \) are consistent, so is \( \varphi''(r)\tau \).

Now, if any branch in \( \varphi''(p)\tau \) ends in a leaf labeled 0, then \( \varphi''(p \lor q)\tau \) can be extended to reach a 0-leaf. This is in contradiction to the inductive assumption. For similar reasons \( \varphi''(\neg p)\tau \) is a 1-tree. This contradicts the assumed consistency of \( \nu' \) and \( \nu'' \).

**VI. PROOFS OF THE MAIN THEOREMS**

We first reprove the main theorem of [8] with improved parameters.

**Theorem VI.1.** For \( d \leq O \left( \frac{\log n}{\log \log n} \right) \) the following holds. Any depth-\( d \) Frege refutation of the Tseitin contradiction defined on the \( n \times n \) grid requires size

\[
\exp \left( \Omega \left( n^{1/(2d-1)} (\log n)^{O(1)} \right) \right).
\]

In the following we construct a \( t \)-evaluation for all sub-formulas occurring in a short and shallow Frege proof to then conclude that all shallow Frege proofs of the Tseitin contradiction must be long. For the total size lower bound we in fact do not create distinct \( t \)-evaluations per line but rather a single one, used on each line. Such a \( t \)-evaluation is clearly consistent and hence satisfies our needs. Let \( \Gamma \) denote the set of sub-formulas occurring in the alleged proof. Our plan is to proceed as follows for \( i = 0, 1, 2, \ldots, d \).
We have a \( t \)-evaluation for all formulas of \( \Gamma \) that were originally of depth \( i \).

- Pick a random full restriction \( \sigma_i \) and extend the \( t \)-evaluation to all formulas of \( \Gamma[\sigma_i] \) of original depth at most \( i + 1 \).

At the starting point, \( i = 0 \), each formula is a literal which is represented by a natural decision tree of depth 1. In order to extend the \( t \)-evaluation to larger depth we use the following lemma, central to the argument.

**Lemma VI.2** (Switching Lemma). There is a constant \( A \) such that the following holds. Suppose there is a \( t \)-evaluation that includes \( F_i, 1 \leq i \leq m \) in its domain and let \( F = \lor_{i=1}^{m} F_i \). Let \( \sigma \) be a random full restriction. Then the probability that \( F[\sigma] \) cannot be represented by a decision tree of depth at most \( s \geq t \) and the number of live variables in each center is in the interval \([.99C \log n, 1.01C \log n]\) is at most

\[
(A(\log n)^{27} t \Delta^{-1})^{s/108}.
\]

We postpone the proof of this lemma to section VII and see how to use it when studying a refutation of size \( N \). We start with a \( t_1 \)-evaluation with \( t_1 = 1 \) for single literals and apply the lemma with \( s = \Omega(\log N) \) in the first step, while we choose \( t_i = s \) in later steps. We set \( \Delta_i = \Omega(t_i(\log n)^{27}) \) and hence have that \( T_i = 4\Delta_i^2 \) for each step.

We start with the original Tseitin contradiction on the \( n \times n \) grid. Start with \( n_0 = n \) and set \( n_{i+1} = n/T_i \) for \( i = 0, 1, \ldots, d - 1 \). We are going to choose a sequence of full restrictions \( \sigma_i \) mapping a grid of size \( n_i \) to a grid of size \( n_{i+1} \) randomly. Let \( \sigma_i^* \) be the composition of \( \sigma_0, \sigma_1, \ldots, \sigma_i \). Let \( \Gamma \) be the set of sub-formulas that appear in an alleged proof and we let

\[
\Gamma_i = \{ F[\sigma_i^*] \mid F \in \Gamma \land depth(F) \leq i \}.
\]

Let \( f_i \) be the number of sub-formulas of depth at most \( i \) in \( \Gamma_i \).

**Lemma VI.3.** With probability \( 1 - f_i 2^{-\Omega(s)} \) there is a \( t \)-evaluation \( \varphi_i \) whose domain includes \( \Gamma_i \).

**Proof.** This is essentially collecting the pieces. We prove the lemma by induction over \( i \). For \( i = 0 \) we have the \( t \)-evaluation that maps each literal to its natural decision tree of depth 1.

When going from depth \( i \) to depth \( i + 1 \) we need to define \( \varphi_{i+1} \) on all formulas originally of depth at most \( i + 1 \) and consider any such \( F \).

1) Each \( F \) of depth at most \( i \) is, by induction, in the domain of \( \varphi_i \) and it is readily verified that it is thus also in \( \varphi_{i+1} \).

2) If \( F \) is of depth \( i \) then \( \varphi_{i+1}(\neg F) \) is defined from \( \varphi_{i+1}(F) \) negating the labels at the leaves.

3) For \( F = \lor F_i \) where each \( F_i \) is of at most depth \( i \) we apply lemma VI.2.

The only place where the extension might fail is under step three but, by lemma VI.2, the probability of failure for any individual formula is at most \( 2^{-\Omega(s)} \) and as we have at most \( f_i - f_{i-1} \) formulas of depth exactly \( i \) the induction is complete.

Fixing parameters we reprove the main theorem from [8] with stronger parameters.

**Proof of theorem VI.1.** Suppose we have a refutation of size \( N \leq \exp(c_1(n^{1/(2d-1)}(\log n)^{-c_2})) \) for suitable positive constants \( c_1 \) and \( c_2 \). In the first iteration we use lemma VI.2 with \( t = 1 \) and \( \Delta = (2tA(\log n)^{27})^{-1} \) and \( s = 110\log N \). In later applications we use \( t = s \).

It is easy to see that with these numbers we have successful switching at each round with high probability. The number of live centers are in the desired interval and we are always able to construct the new \( t \)-evaluation.

Up to polylogarithmic factors we have that the final side length of the grid after all the restrictions is \( n(\log N)^{-2(2d-1)} \) and it is a \( t \)-evaluation with \( t = O(\log N) \). Thus if \( \log N \) is a polylogarithmic factor smaller than \( n^{1/(2d-1)} \) we get a contradiction.

Let us turn our attention to the main result of the present paper.

**Theorem VI.4.** For any Frege proof of the Tseitin principle defined over the \( n \times n \) grid graph the following holds. If each line of the proof is of size \( M \) and depth \( d \), then the number of lines in the proof is

\[
\exp \left( O \left( \frac{n}{((\log n)^{O(1)} \log M)^{2d}} \right) \right).
\]

The strategy of the proof is similar to the proof of theorem VI.1: we again build a \( t \)-evaluation for a supposed Frege proof. The main difference is that instead of creating a single \( t \)-evaluation for the entire proof we in fact independently create \( t \)-evaluations for each line. These \( t \)-evaluations turn out to be consistent and we thus obtain the claimed bounds.

Suppose we are given a Frege refutation of the Tseitin principle defined over the \( n \times n \) grid consisting of \( N \) lines, where each line is a formula of size \( M \) and depth \( d \). We denote by \( \Gamma^\nu \) the set of sub-formulas of line \( \nu \) in the proof and continue to construct a sequence of restrictions \( \sigma_1, \sigma_2, \ldots, \sigma_d \) such that all formulas of depth at most \( k \) have consistent \( t(k) \)-evaluations if hit
by the concatenation \(\sigma_k^*\) of the first \(k\) restrictions in the sequence, where \(t(k)\) is some function dependent on \(k\) to be fixed later. That is, for every line \(\nu\) we have a \(t(k)\)-evaluation \(\varphi_k^\nu\) for all formulas in the set

\[
\Gamma_k^\nu = \{ F[\sigma_k^*] \mid F \in \Gamma^\nu \land \text{depth}(F) \leq k \},
\]
and all these \(t(k)\)-evaluations are consistent. In addition to these \(t(k)\)-evaluations, for each line \(\nu\) we also maintain a decision tree \(T_k(\nu)\). We maintain the property that \(T_k(\nu)\) is a \(t\) common partial decision tree for all \(t(k)\)-evaluations \(\varphi_k^\nu(\Gamma_k^\nu)\) of bounded depth.

These partial common decision trees \(T_k(\nu)\) are useful to extend the \(t(k)\)-evaluations \(\varphi_k^\nu\) to larger depths. In each such step, increasing \(k\), we apply for each branch \(\pi\) from \(T_k(\nu)\) the following multi-switching lemma to the set of decision trees \(\varphi_k^\nu(\Gamma_k^\nu)\) of depth at most \(t\). We then extend \(T_k(\nu)\) in each leaf \(\pi\) by the partial common decision tree from the lemma to obtain \(T_{k+1}(\nu)\) of slightly larger depth.

**Lemma VI.5 (Multi-switching Lemma).** There are constants \(A, c_1,\) and \(c_2\) such that the following holds. Consider formulas \(F_i^j\), for \(j \in [M]\) and \(i \in [m_j]\), each associated with a decision tree of depth at most \(t\) and let \(F = \bigvee_{i=1}^m F_i^j\). Let \(\sigma\) be a random full restriction. Then the probability that the number of live variables in each center is in the interval \([.99C\log n, 1.01C\log n]\) and \((F_j|\sigma)_{j=1}^M\) cannot be represented by an \(\ell\) common partial decision tree of depth at most \(s\) is at most

\[
M^{s/\ell}(A(\log n)^{c_1}t\Delta^{-1})^{s/c_2}.
\]

We defer the proof of this lemma to section VIII. We apply lemma VI.5 with mostly the same parameters so let us fix these. We choose \(\ell = t = \log M\) and \(\Delta = D \cdot t \cdot (\log n)^{c_1}\), for a sufficiently large constant \(D\). The parameter \(s\) depends on \(k\) and is fixed to \(s = s_k = 2^{k-1}\log N\). With these parameters in place we can finally also fix \(t(k) = \sum_{i < k} s_i + \log M \leq 2^k \log N + \log M\).

**Lemma VI.6.** Suppose that for every line \(\nu \in [N]\) we have consistent \((k-1)\)-evaluations \(\varphi_{k-1}^\nu\) for formulas in \(\Gamma_k^\nu\) along with a \(t\) common partial decision tree \(T_{k-1}(\nu)\) for \(\varphi_{k-1}^\nu(\Gamma_k^\nu)\) of depth \(\sum_{i < k} s_i\). Then, with probability \(1 - N^{-1}\), there is a full restriction \(\sigma_k\) whose output grid is of dimension \(n\) and, assuming that \(t(k) \leq n/8\), for every line \(\nu \in [N]\) there is a consistent \(t(k)\)-evaluation \(\varphi_k^\nu\) for formulas in \(\Gamma_k^\nu\) and a \(t\) common partial decision tree \(T_k(\nu)\) for \(\varphi_k^\nu(\Gamma_k^\nu)\) of depth \(\sum_{i \leq k} s_i\).

**Proof.** Let us first extend the common partial decision trees and then explain how to obtain \(\varphi_k^\nu\) for different lines \(\nu \in [N]\).

The interesting formulas of original depth \(k\) to consider are the ones with a top \(\lor\) gate. Let us fix a line \(\nu \in [N]\) and consider all sub-formulas \(\{F^j = \bigvee_{i=1}^m F_i^j\}_{j=1}^M\) of line \(\nu\) of original depth \(k\) with a top \(\lor\) gate under the restriction \(\sigma_{k-1}\). As the original depth of every \(F^j\) is at most \(k - 1\), all these formulas are in the domain of \(\varphi_{k-1}^\nu\). Let us further fix a path \(\pi\) in \(T_{k-1}(\nu)\) and recall that all decision trees \(\varphi_{k-1}^\nu(F^j|\pi)\) are of depth at most \(t\).

For every \(\nu \in [N]\) and branch \(\pi\) of \(T_{k-1}(\nu)\) we apply lemma VI.5 to the set of formulas \(F^j|\pi\) with associated trees \(\varphi_{k-1}^\nu(F^j|\pi)\) of depth at most \(t\). The probability of failure of a single application is bounded by \(N^{-2k-1}\), assuming an appropriate choice of the constant \(D\). As we invoke lemma VI.5 at most \(N \cdot 2\sum_{i < k} s_i \leq N 2^k\) times, by a union bound, with probability at least \(1 - N^{-1}\), there is a full restriction \(\sigma_k\) such that for every line \(\nu \in [N]\) and every branch \(\pi \in T_{k-1}(\nu)\) we get a \(t\) common partial decision tree of depth at most \(s_k\) for the formulas \((F^j|\pi\sigma_k)_{j=1}^M\). Let us denote this common decision tree by \(T(\nu, \pi)\) and attach it to \(T_{k-1}(\nu)\) at the leaf \(\pi\) to obtain \(T_k(\nu)\). The trees \(T_k(\nu)\) are of depth at most \(\sum_{i \leq k} s_i\) as required.

Let us explain how to define \(\varphi_k^\nu\) for a fixed line \(\nu \in [N]\). Consider any formula \(F\) in \(\Gamma_k\).

- If \(F\) is of depth less than \(k\), then \(F\) is in the domain of \(\varphi_{k-1}^\nu\).
- If \(F\) is of depth \(k - 1\) then \(\varphi_k^\nu(\neg F)\) is defined from \(\varphi_k^\nu(F)\) negating the labels at the leaves.
- For \(F = \bigvee_i F_i\) of depth \(k\) we use the previously constructed common partial decision trees. We define \(\varphi_k^\nu(F)\) to be the decision tree whose first \(\sum_{i < k} s_i\) levels are equivalent to \(T_k(\nu)\) followed by \(t\) levels unique to \(F\) obtained from the multi-switching lemma.

Let us check that the decision trees \(T_k(\nu)\) are indeed \(t\) common partial decision trees for \(\varphi_k^\nu(\Gamma_k^\nu)\). By construction this clearly holds for formulas of depth \(k\) with a top \(\lor\) gate. As \(T_k(\nu)\) is equivalent to \(T_{k-1}(\nu)\) on the upper levels, and restrictions only decrease the depth of decision trees, by the initial assumptions this also holds for formulas of depth less than \(k\). As the \(t(k)\)-evaluations of formulas of depth \(k\) with a top \(\neg\) gate are defined in terms of formulas of depth less than \(k\), we also see that \(T_k(\nu)\) is a \(t\) common partial decision tree for such formulas.
Last we need to check that each \(\varphi_k^v\) is a \(t(k)\)-evaluation plus that these are pairwise consistent.

It is straightforward to check that all the properties hold for formulas of depth less than \(k\). Let us verify the \(t(k)\)-evaluation properties for formulas of depth \(k\).

Property 1 is immediate, as \(k > 0\). As we only consider consistent decision trees, property 2 also follows. Further, property 3 is satisfied by construction. Property 4 can be established by checking the property for each branch \(\pi\) in \(T_{k-1}(v)\) separately; for a fixed \(\pi\) we see by lemma VI.5 that this indeed holds.

Finally we need to establish that two \(t(k)\)-evaluations \(\varphi_k^v\) and \(\varphi_k^w\) are consistent for formulas of depth \(k\). By the inductive hypothesis we clearly have that \(\neg\)-isomorphic formulas are \(\neg\)-consistent. Further, isomorphic formulas with a top \(\neg\) gate are consistent. Hence we are only left with checking consistency for isomorphic formulas of depth \(k\) with a top \(\lor\) gate.

Let \(F = \lor_i F_i\) and \(F' = \lor_i F'_i\) be two isomorphic formulas from \(\Gamma'_k\) and \(\Gamma'_k\) respectively. For the sake of contradiction suppose \(\varphi_k^v(F)[\pi] = 1\) but \(\varphi_k^w(F')[\pi] = 0\) for some assignment \(\pi\). In the following we use that \(t(k) \leq n/8\) and hence there are consistent branches as claimed. By property 2 we know that for some \(F_i\) it holds that \(\varphi_k^v(F_i)[\pi] = 1\). As \(F\) and \(F'\) are isomorphic formulas we know that there is an \(F'_j\) such that \(F_i\) and \(F'_j\) are isomorphic formulas. As such formulas have consistent decision trees (by induction) we get that \(\varphi_k^w(F'_j)[\pi] = 1\).

But this cannot be as by property 4 of a \(t(k)\)-evaluation this implies that \(\varphi_k^v(F')[\pi] = 1\). This establishes that the different \(t(k)\)-evaluations are consistent, as required. \(\square\)

With all pieces in place we are ready to prove theorem VI.4.

**Proof of theorem VI.4.** Suppose we are give a proof of length \(N = \exp \left( n/((\log n)^c \log M)^{2d} \right)\), for some constant \(c\). We may assume that \(M \leq \exp(n^{1/2d - 1/2d(2d-1)})\), as otherwise we can apply theorem VI.1.

In order to create the consistent \(t(k)\)-evaluations \(\varphi^v\) for each line \(v \in [N]\) we consecutively apply lemma VI.6 \(d\) times. We start with \(\varphi_0^v\) which maps constants to the appropriate depth 0 decision tree and literals to the corresponding depth 1 decision trees. The partial common decision trees \(T_0(v)\) are all empty.

After applying lemma VI.6 \(d\) times we are left with a \(t(d)\)-evaluation for the proof. We need to ensure that \(t(d)\) is upper bounded by the dimension of the final grid: \(t(d) \leq 2^d \log N + \log M\), while the final side length of the grid is \(n \cdot (4\Delta^2)^{-d} = n \cdot (2D(\log n)^{c_1} \log M)^{-2d}\). For our choice of \(N\) and the assumption on \(M\) this indeed holds and the theorem follows. \(\square\)

**VII. The Improved Standard Switching Lemma**

The proof very much follows the proof of [8]. In fact large parts of the proof are the same.

For the benefit of the reader completely on top of [8] let us outline the differences in the following. For a full proof including a detailed proof outline we refer the interested reader to the full version of the present paper.

**A. Changes in the Argument**

The key number that has changed is the parameter \(k\), the total number of centers that are alive. In the definition of a partial restriction this parameter \(k\) has changed from \(C s(n/T)^{2}\) to \(C \log n(n/T)^{2}\). The fact that we had \(\Omega(s)\) live centers in each square was crucial in finding live centers to extend the information sets \(J_{s}\) to closed sets \(\gamma_{j}\). This process needed \(O(s)\) fresh centers from specific squares and there is nothing that prevents these from all being required to be in the same square. In the current proof we allow \(\gamma_{j}\) to be not closed and this implies that the restriction \(\rho^*\) is a generalized restriction where the Tseitin condition is violated at some vertices. This only happens when we have \(\Omega(\log n)\) exposed non-chosen centers in a sub-square and results in a single violating vertex. As the there are at most \(O(s)\) exposed centers over all we can have at most \(O(s/\log n)\) violating centers. The number of generalized restrictions with \(B\) violating centers is at most a factor \(n^{2B}\) more than the the number of ordinary restrictions. This number is \(2^{O(s)}\) and this factor can be absorbed in the constant \(A\) in the statement of the switching lemma.

**VIII. The Multi-Switching Lemma**

The proof of lemma VI.5 follows very much the proof of lemma VI.2. The strategy of the proof is essentially as follows.

If \(F^j\) is not turned in to a decision tree of depth \(\ell\), find the branch of in the extended canonical decision tree of length at least \(\ell\) and put the variables on this branch in the common decision tree. Query those variables and some extra variables and recurse.

We take any \(\sigma\) for which the lemma fails and with the aid of the formulas we transform it into a restriction \(\sigma^*\). This mapping can later be inverted by the use of some extra information. One complication to handle is that the answers to the variables found on the long branch in the extended decision tree of \(F^j\) and the answers on the long branch in the common decision tree to the same variables...
are different. This leads to the more complicated game analyzed in section III.

For further details we refer the interested reader to the full version of the present paper.

Acknowledgments. We are grateful to Mrinal Ghosh, Björn Martinsson and Aleksa Stanković for helpful discussions on the topic of this paper.

REFERENCES

[1] Miklós Ajtai. The complexity of the pigeonhole principle. Combinatorica, 14(4):417–433, 1994. Preliminary version in FOCS ’88.

[2] Eli Ben-Sasson. Hard examples for the bounded depth Frege proof system. Computational Complexity, 11(3-4):109–136, 2002.

[3] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. The Journal of Symbolic Logic, 44(1):36–50, 1979.

[4] M. Furst, J.B. Saxe, and M. Sipser. Parity, circuits and the polynomial-time hierarchy. Mathematical Systems Theory, 17:13–27, 1984.

[5] A. Haken. The intractability of resolution. Theoretical Computer Science, 39:297 – 308, 1985.

[6] J. Håstad. Almost optimal lower bounds for small depth circuits. In Proceedings of the eighteenth annual ACM symposium on Theory of computing, STOC ’86, pages 6–20, New York, NY, USA, 1986. ACM.

[7] J. Håstad. On the correlation of parity and small-depth circuits. SIAM Journal on Computing, 43:1699–1708, 2014.

[8] J. Håstad. On small-depth frege proofs for tseitin for grids. Journal of the ACM, 68:1–31, 2020.

[9] Johan Håstad and Kilian Risse. On bounded depth proofs for tseitin formulas on the grid; revisited. https://arxiv.org/abs/2209.05839, 2022.

[10] Russell Impagliazzo, William Matthews, and Ramamohan Paturi. A satisfiability algorithms for AC0. In Proceeding of the 23rd Annual ACM-SIAM Symposium on Discrete Algorithms, pages 961–972, 2012.

[11] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. Random Structures & Algorithms, 7(1):15–39, 1995.

[12] T. Pitassi, P. Ramakrishnan, and L. Tan. Tradeoffs for small-depth frege proofs. In 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS), pages 445–456, Los Alamitos, CA, USA, 2021. IEEE Computer Society.

[13] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. Computational Complexity, 3:97–140, 1993. Preliminary version in STOC ’92.

[14] Toniann Pitassi, Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan. Poly-logarithmic frege depth lower bounds via an expander switching lemma. In Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing, STOC ’16, page 644–657, New York, NY, USA, 2016. Association for Computing Machinery.

[15] A. Razborov. Bounded-depth formulae over the basis \{ AND,XOR \} and some combintorial problems (in russian). Problems of Cybernetics. Complexity Theory and Applied Mathematical Logic, pages 149–166, 1988.

[16] M. Sipser. Borel sets and circuit complexity. In Proceedings of the fifteenth annual ACM symposium on Theory of computing, STOC ’83, pages 61–69, New York, NY, USA, 1983. ACM.

[17] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In Proceedings of the nineteenth annual ACM symposium on Theory of computing, STOC ’87, pages 77–82, New York, NY, USA, 1987. ACM.

[18] G. S. Tseitin. On the complexity of derivation in the propositional calculus. In A. O. Slisenko, editor, Studies in constructive mathematics and mathematical logic. Part II, 1968.

[19] Alasdair Urquhart and Xudong Fu. Simplified lower bounds for propositional proofs. Notre Dame Journal of Formal Logic, 37(4):523–544, 1996.

[20] A. C-C. Yao. Separating the polynomial-time hierarchy by oracles. In Foundations of Computer Science, 1985., 26th Annual Symposium on, pages 1 –10, oct. 1985.