Electronic Colloquium on Computational Complexity, Report No. 22 (2021)

Depth lower bounds in Stabbing Planes for combinatorial principles

Stefan Dantchev
Department of Computer Science
Durham University, UK
s.s.dantchev@durham.ac.uk

Nicola Galesi
Department of Computer Science
Sapienza Università di Roma, IT
nicola.galesi@uniroma1.it

Abdul Ghani
Department of Computer Science
Durham University, UK
abdul.ghani@durham.ac.uk

Barnaby Martin
Department of Computer Science
Durham University, UK
barnaby.d.martin@durham.ac.uk

February 20, 2021

Abstract

We prove logarithmic depth lower bounds in *Stabbing Planes* for the classes of combinatorial principles known as the *Pigeonhole principle* and the *Tseitin* contradictions. The depth lower bounds are new, obtained by giving almost linear length lower bounds which do not depend on the bit-size of the inequalities and in the case of the Pigeonhole principle are tight.

The technique known so far to prove depth lower bounds for Stabbing Planes is a generalization of that used for the *Cutting Planes* proof system. In this work we introduce two new approaches to prove length/depth lower bounds in Stabbing Planes: one relying on *Sperner's Theorem* which works for the Pigeonhole principle and Tseitin contradictions over the complete graph; a second proving the lower bound for Tseitin contradictions over a grid graph, which uses a result on *essential coverings* of the boolean cube by linear polynomials, which in turn relies on *Alon's combinatorial Nullenstellensatz*.

ISSN 1433-8092

1 Introduction

Finding a satisfying assignment for a propositional formula (SAT) is a central component for many computationally hard problems. Despite being older than 50 years and exponential time in the worst-case, the DPLL algorithm [6, 7, 17] is the core of essentially all high performance modern SAT-solvers. DPLL is a recursive boolean method: at each call one variable x of the formula $\mathcal{F}$ is chosen and the search recursively branches into the two cases obtained by setting x respectively to 1 and 0 in $\mathcal{F}$. On UNSAT formulas DPLL performs the worst and it is well-known that the execution trace of the DPLL algorithm running on an unsatisfiable formula $\mathcal{F}$ is nothing more than a treelike refutation of $\mathcal{F}$ in the proof system of *Resolution* [17] (Res).

Since SAT can be viewed as an optimization problem the question whether Integer Linear Programming (ILP) can be made feasible for satisfiability testing received a lot of attention and is considered among the most challenging problems in local search [18, 10]. One proof system capturing ILP approaches to SAT is *Cutting Planes*, a system whose main rule implements the *rounding* (or *Chávtal cut*) approach to ILP. Cutting planes works with integer linear inequalities of the form $\mathbf{a}\mathbf{x} \leq b$, with $\mathbf{a}, b$ integers, and, like resolution, is a sound and complete refutational proof system for CNF formulas: indeed a clause $C = (x_1 \vee \ldots \vee x_r \vee \neg y_1 \vee \ldots \vee \neg y_s)$ can be written as the integer inequality $\mathbf{y} - \mathbf{x} \leq s - 1$.

Beame et al. [2], extended the idea of DPLL to a more general proof strategy based on ILP. Instead of branching only on a variable as in resolution, in this method one considers a pair $(\mathbf{a}, b)$, with $\mathbf{a} \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$, and branches limiting the search to the two half-planes: $\mathbf{a}\mathbf{x} \leq b - 1$ and $\mathbf{a}\mathbf{x} \geq b$. A *path* terminates when the LP defined by the inequalities in $\mathcal{F}$ and those forming the path is infeasible. This method can be made into a refutational treelike proof system for UNSAT CNF's called *Stabbing planes* (SP) ([2]) and it turned out that it is polynomially equivalent to the treelike version of Res(CP), a proof system introduced by Krajíček [12] where clauses are disjunction of linear inequalities.

In this work we consider the complexity of proofs in SP focusing on the *length*, i.e. the number of queries in the proof; the *depth* (called also *rank* in [2]), i.e. the length of the longest path in the proof tree; and the *size*, i.e. the bit size of all the coefficients appearing in the proof.

1.1 Previous works and motivations

Lower bounds for size can be obtained in SP, but in a limited way: in [2] it is proven that size S and depth D SP refutations imply treelike Res(CP) proofs of size $O(S)$ and width $O(D)$; Kojevnikov [11], improving the *interpolation method* introduced for Res(CP) by Krajíček [12], gave exponential lower bounds for treelike Res(CP) when the width of the clauses (i.e. the number of linear inequalities in a clause) is bounded by $o(n/\log n)$. Hence these lower bounds are applicable only to very specific classes of formulas (whose hardness comes from boolean circuit hardness) and only to SP refutations of low depth.

Nevertheless SP appears to be a strong proof system. Firstly notice that the condition terminating a path in a proof is not a trivial contradiction like in resolution, but is the infeasibility of an LP, which is only a polynomial time verifiable condition. Hence linear size SP proofs might be already a strong class of SP proofs, since they can hide a polynomial growth into one final node whence to run the verification of the terminating condition. At present we know that:

1. SP polynomially simulates CP (Theorem 4.5 in [2]). Hence in particular the PHP^m_n can be refuted in SP by a proof of size $O(n^2)$ ([5]). Furthermore it can be refuted by a $O(\log n)$ depth proof since polynomial size CP proofs, by Theorem 4.4 in [2], can be balanced in SP [1].

[1] Another way of proving this result is using Theorem 4.8 in [2] stating that if there are length L and space S CP refutations of a set of linear integral inequalities, then there are depth $O(S \log L)$ SP refutations of the same set of linear integral inequalities; and then use the result in [9] (Theorem 5.1) that PHP^m_n has polynomial length and constant space CP refutations.

2. Beame et al. in [2] proved the surprising result that the class of Tseitin contradictions $\mathsf{Ts}(G, \omega)$ over any graph G of maximum degree D, with an odd charging ω, can be refuted in SP in size quasipolynomial in $|G|$ and depth $O(\log^2 |G| + D)$.

Depth lower bounds for SP are proved in [2]:

1. a $\Omega(n/\log^2 n)$ lower bound for the formula $\mathsf{Ts}(G, w) \circ \mathsf{VER}^n$, composing $\mathsf{Ts}(G, \omega)$ (over an expander graph G) with the gadget function VER^n (see Theorem 5.7 in [2] for details); and

2. a $\Omega(\sqrt{n \log n})$ lower bound for the formula $\mathsf{Peb}(G) \circ \mathsf{IND}_l^n$ over $n^5 + n \log n$ variables obtained by lifting a pebbling formula $\mathsf{Peb}(G)$ over a graph with high pebbling number, with a *pointer function* gadget IND_l^n (see Theorem 5.5. in [2] for details).

Similarly to size, these depth lower bounds are also applicable only to very specific classes of formulas. In fact they are obtained by extending to SP the technique introduced by Krajíček [13] for CP of reducing shallow proofs of a formula $\mathcal{F}$ to efficient *real* communication protocols computing a related search problem and then proving that such efficient protocols cannot exist.

Despite the fact that SP is at least as strong as CP, in SP the known lower bounds techniques are derived from those of treelike CP. Hence finding other techniques to prove depth and size lower bounds for SP is important to understand its proof strength. For instance, unlike CP where we know tight $\Theta(\log n)$ rank bounds for the PHP_n^m [3, 16] and $\Omega(n)$ rank bounds for Tseitin contradictions [3], for SP no depth lower bound is at present known for purely combinatorial statements.

In this work we address such problems.

1.2 Contributions and techniques

The main original motivation of this work was to prove depth lower bounds in SP for truly combinatorial statements, like $\mathsf{Ts}(G, w)$ or PHP_n^m, which we know to be efficiently provable, but on which we cannot use methods reducing to the complexity of boolean functions, like the ones mentioned above. We present two new methods for proving depth lower bounds in SP which in fact are the consequence of proving length lower bounds. Our bounds are numerically weak (almost linear for the length and logarithmic for the depth), but for the PHP_n^m they give optimal depth lower bounds from length lower bounds that do not depend on the bit-size of the coefficients. We prove:

1. an optimal $\Omega(\log n)$ lower bound for the depth of SP proofs of the PHP_n^m.

2. an $\Omega(\log n)$ lower bound for the depth of SP proofs of $\mathsf{Ts}(G, \omega)$, when G is a $n \times n$ grid graph H_n or the complete graph K_n. These last results must be compared with the $O(\log^2 n)$ upper bound for $\mathsf{Ts}(H_n, \omega)$ given in [2].

Our results are derived from the following initial geometrical observation: let $\mathbb{S}$ be a space of *admissible points* in $\{0, 1, 1/2\}^n$ satisfying a given unsatisfiable system of integer linear inequalities $\mathcal{F}(x_1, \ldots, x_n)$. In a SP proof for $\mathcal{F}$, at each branch $Q = (\mathbf{a}, b)$ the set of points in the $\mathsf{slab}(Q) = \{\mathbf{s} \in \mathbb{S} : b - 1 < \mathbf{ax} < b\}$ does not survive in $\mathbb{S}$. At the end of the proof on the leaves, where we have infeasible LP's, no point in $\mathbb{S}$ can survive the proof. So it is sufficient to find conditions such that, under the assumption that a proof of $\mathcal{F}$ is "small", even one point of $\mathbb{S}$ survives the proof. In pursuing this approach we use two methods.

The *antichain method*. Here we use a well-known bound based on Sperner's Theorem [4, 20] to upper bound the number of points in the slabs where the set of non-zero coefficients is sufficiently large. Trading between the number of such slabs and the number of points ruled out from the space $\mathbb{S}$ of admissible points, we obtain the lower bound.

We initially present the method and the $\Omega(\log n)$ lower bound on a set of unsatisfiable integer linear inequalities - the *Simple Pigeonhole Principle* (SPHP) - capturing the core of the counting argument used to prove efficiently the PHP in CP. Since SPHP_n has rank 1 CP proofs, it entails a strong separation between CP rank and SP depth. We then apply the method to PHP_n^m and to $\mathsf{Ts}(K_n, \omega)$.

The *covering method*. The antichain method appears too weak to prove size and depth lower bounds on $\mathsf{Ts}(G, w)$, when G is for example a grid or a pyramid. To solve this case, we consider another approach that we call the *covering method*: we reduce the problem of proving that one point in $\mathbb{S}$ survives from all the $\mathsf{slab}(Q)$ in a small proof of $\mathcal{F}$, to the problem that a set of polynomials which *essentially covers* the boolean cube $\{0,1\}^n$ requires at least n polynomials, which is a well-known problem [1, 14]. For this reduction to work we have to find a high dimensional projection of $\mathbb{S}$ covering the boolean cube and defined on variables effectively appearing in the proof. We prove that matchings in G work properly to this aim on $\mathsf{Ts}(G, \omega)$. Since the grid H_n has large matchings, we can obtain the lower bound on $\mathsf{Ts}(H_n, \omega)$.

The paper is organized as follows: We give the preliminary definitions in the next section and then we move to other sections: one on the lower bounds by the antichain method and the other on lower bounds by the covering method.

2 Preliminaries

We use $[n]$ for the set $\{1, 2, \ldots, n\}$, $\mathbb{Z}/2$ for $\mathbb{Z} \cup (Z + \frac{1}{2})$ and $\mathbb{Z}^+$ for $\{1, 2, \ldots\}$.

2.1 Proof systems

Here we recall the definition of the Stabbing Planes proof system from [2].

Definition 1. *A* linear integer inequality *in the variables $x_1, \ldots, x_n$ is something of the form $\sum_{i=1}^n a_i x_i \geq b$, where each a_i and b are integral. A set of such inequalities is said to be* unsatisfiable *if there are no $0/1$ assignments to the x variables satisfying each inequality simultaneously.*

Note that we reserve the term infeasible, in contrast to unsatisfiable, for (real or rational) linear programs.

Definition 2. *Fix some variables $x_1, \ldots, x_n$. A* Stabbing Planes (SP) *proof of a set of integer linear inequalities $\mathcal{F}$ is a binary tree $\mathcal{T}$, with each node labeled with a* query $(\mathbf{a}, b)$ *with $\mathbf{a} \in \mathbb{Z}^n, b \in \mathbb{Z}$. Out of each node we have an edge labeled with $\mathbf{a}x \geq b$ and the other labeled with its integer negation $\mathbf{a}x \leq b - 1$. Each leaf ℓ is labeled with a* LP *system P_ℓ made by a nonnegative linear combination of inequalities from $\mathcal{F}$ and the inequalities labelling the edges on the path from the root of $\mathcal{T}$ to the leaf ℓ.*

If $\mathcal{F}$ is an unsatisfiable *set of integer linear inequalities, $\mathcal{T}$ is a* Stabbing Planes (SP) refutation *of $\mathcal{F}$ if all the* LP*'s P_ℓ on the leaves of $\mathcal{T}$ are infeasible.*

Definition 3. *The* slab *corresponding to a query $Q = (\mathbf{a}, b)$ is the set $\mathsf{slab}(Q) = \{\mathbf{x} \in \mathbb{R}^n : b - 1 < \mathbf{a}\mathbf{x} < b\}$ satisfying neither of the associated inequalities.*

Since each leaf in a SP refutation is labelled by an infeasible LP, throughout this paper we will actually use the following geometric observation on SP proofs $\mathcal{T}$: the set of points in $\mathbb{R}^n$ must all be ruled out by a query somewhere in $\mathcal{T}$. In particular this will be true for those points in $\mathbb{R}^n$ which satisfy a set of integer linear inequalities $\mathcal{F}$ and which we call *feasible points* for $\mathcal{F}$.

Fact 1. *The slabs associated with a* SP *refutation must cover the feasible points of $\mathcal{F}$. That is,*

$$\{\mathbf{y} \in \mathbb{R}^n : \mathbf{a}\mathbf{y} \geq b \text{ for all } (\mathbf{a}, b) \in \mathcal{F}\} \subseteq \bigcup_{(\mathbf{a},b)\in\mathcal{F}} \{\mathbf{x} \in \mathbb{R}^n : b - 1 < \mathbf{a}\mathbf{x} < b\}$$

The *length* of a SP refutation is the number of queries in the proof tree. The *depth* of a SP refutation $\mathcal{T}$ is the longest root-to-leaf path in $\mathcal{T}$. The size (respectively depth) of refuting $\mathcal{F}$ in SP is the *minimum* size (respectively depth) over all SP refutations of $\mathcal{F}$. We call *bit-size* of a SP refutation $\mathcal{T}$ the total number of bits needed to represent every inequality in the refutation.

Definition 4 ([5])**.** *The* Cutting Planes (CP) *proof system is equipped with boolean axioms and two inference rules:*

$$\begin{array}{c|c|c} \textit{Boolean Axioms} & \textit{Linear Combination} & \textit{Rounding} \\ \hline \dfrac{}{x\geq 0} \quad \dfrac{}{-x\geq -1} & \dfrac{\mathbf{ax}\geq c \qquad \mathbf{bx}\geq d}{\alpha\mathbf{ax}+\beta\mathbf{bx}\geq \alpha c+\beta d} & \dfrac{\alpha\mathbf{ax}\geq b}{\mathbf{ax}\geq \lceil b/\alpha\rceil} \end{array}$$

where $\alpha, \beta, b \in \mathbb{Z}^+$ and $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$. A CP refutation of some unsatisfiable set of integer linear inequalities is a derivation of $0 \geq 1$ by the aforementioned inference rules from the inequalities in $\mathcal{F}$.

A CP refutation is *treelike* if the directed acyclic graph underlying the proof is a tree. The *length* of a CP refutation is the number of inequalities in the sequence. The *depth* is the length of the longest path from the root to a leaf (sink) in the graph. The *rank* of a CP proof is the maximal number of rounding rules used in a path of the proof graph. The *size* of a CP refutation is the bit-size to represent all the inequalities in the proof.

2.2 Restrictions

Let $V = \{x_1, \ldots, x_n\}$ be a set of n variables and let $\mathbf{ax} \leq b$ be a linear integer inequality. We say that a variable x_i *appears in*, or is *mentioned by* a query $Q = (\mathbf{a}, b)$ if $a_i \neq 0$ and *does not appear* otherwise.

A *restriction* ρ is a function $\rho : D \to \{0, 1\}$, $D \subseteq V$. A restriction acts on a half-plane $\mathbf{ax} \leq b$ setting the x_i's according to ρ. Notice that the variables $x_i \in D$ do not appear in the restricted half-plane.

By $\mathcal{T}\restriction_\rho$ we mean to apply the restriction ρ to all the queries in a SP proof $\mathcal{T}$. The tree $\mathcal{T}\restriction_\rho$ defines a new SP proof: if some $Q\restriction_\rho$ reduces to $0 \leq -b$, for some $b \geq 1$, then that node becomes a leaf in $\mathcal{T}\restriction_\rho$. Otherwise in $\mathcal{T}\restriction_\rho$ we simply branch on $Q\restriction_\rho$. Of course the solution space defined by the linear inequalities labelling a path in $\mathcal{T}\restriction_\rho$ is a subset of the solution space defined by the corresponding path in $\mathcal{T}$. Hence the leaves of $\mathcal{T}\restriction_\rho$ define an infeasible LP.

We work with linear integer inequalities which are a translation of families of CNFs $\mathcal{F}$. Hence when we write $\mathcal{F}\restriction_\rho$ we mean the applications of the restriction ρ to the set of linear integer inequalities defining $\mathcal{F}$.

3 The antichain method

This method is based on Sperner's theorem. Using it we can prove depth lower bounds in SP for PHP^m_n and for Tseitin contradictions $\mathsf{Ts}(K_n, \omega)$ over the complete graph. To motivate and explain the main definitions, we use as an example a simplification of the PHP^m_n, the *simplified Pigeonhole principle* SPHP_n, which has some interest since, as we will show it exponentially separates CP rank from SP depth.

3.1 Simplified Pigeonhole Principle

As mentioned in the Introduction, the SPHP_n intends to capture the core of the counting argument used to prove efficiently the PHP in CP.

Definition 5. *The SPHP_n is the following unsatisfiable family of inequalities:*

$$\begin{array}{ll} \sum_{i=1}^n x_i \geq 2 & \\ x_i + x_j \leq 1 & \textit{(for all } i \neq j \in [n]\textit{)} \end{array}$$

Lemma 1. SPHP_n *has a rank* 1 *CP refutation, for* $n \geq 3$.

Proof. Let $S := \sum_{i=1}^{n} x_i$ (so we have $S \geq 2$). We fix some $i \in [n]$ and sum $x_i + x_j \leq 1$ over all $j \in [n] \setminus \{i\}$ to find $S + (n-2)x_i \leq n-1$. We add this to $-S \leq -2$ to get

$$x_i \leq \frac{n-3}{n-2}$$

which becomes $x_i \leq 0$ after a single cut. We do this for every i and find $S \leq 0$ - a contradiction when combined with the axiom $S \geq 2$. □

It is easy to see that SPHP_n has depth $O(\log n)$ proofs in SP, either by a direct proof or appealing to the polynomial size proofs in CP of the PHP_n^m ([5]) and then using the Theorem 4.4 in [2] informally stating that "CP proofs can be balanced in SP".

Corollary 1. *The* SPHP_n *has Stabbing Planes refutations of depth* $O(\log n)$.

We will prove that this depth is tight.

3.2 Sperner's Theorem

Let $\mathbf{a} \in \mathbb{R}^n$. The *width* $w(\mathbf{a})$ of $\mathbf{a}$ is the number of non-zero coordinates in $\mathbf{a}$. The width of a query $(\mathbf{a}, b)$ is $w(\mathbf{a})$.

Let $n \in \mathbb{N}$. Fix $W \subseteq [0,1] \cap \mathbb{Q}^+$ of finite size $k \geq 2$ and insist that $0 \in W$. We also insist that, if w_m is the maximal element in W, that W is closed under the map $x \to w_m - x$. The W's we work with in this paper are $\{0, 1/2\}$ and $\{0, 1/2, 1\}$. We disallow (for example) $\{0, 1/3, 1\}$ as it is not closed under $x \to 1 - x$.[2]

Definition 6. *A* (n, W)*-word is an element in* W^n.

We consider the following extension of Sperner's theorem.

Theorem 1 ([15, 4])**.** *Fix some* $t \geq 2, t \in \mathbb{N}$. *For the pointwise ordering of* $[t]^f$*, any antichain has size at most* $t^f \sqrt{\frac{6}{\pi(t^2-1)f}}(1 + o(1))$.

We will use the simplified bound that any antichain $\mathcal{A}$ has size $|\mathcal{A}| \leq \frac{t^f}{\sqrt{f}}$.

Lemma 2. *Let* $\mathbf{a} \in \mathbb{Z}^n$ *and* $|W| = k \geq 2$. *The number of* (n, W)*-words* $\mathbf{s}$ *such that* $\mathbf{as} = b$*, where* $b \in \mathbb{Q}$ *is at most* $\frac{k^n}{\sqrt{w(\mathbf{a})}}$.

Proof. Assume for a moment that the a_i's are non-negative. Let $I_{\mathbf{a}} = \{i \in [n] : a_i \neq 0\}$. Notice that $|I_{\mathbf{a}}| = w(\mathbf{a})$. For a (n, W)-word $\mathbf{s}$, let $\tilde{\mathbf{s}} = \mathsf{proj}_{\restriction I_{\mathbf{a}}}(s)$ be the projection of $\mathbf{s}$ on the set of coordinates $I_{\mathbf{a}}$. $\tilde{\mathbf{s}}$ is a $(w(\mathbf{a}), k)$-word and we claim that the set of such $\tilde{\mathbf{s}}$ forms an antichain on $[k]^{w(\mathbf{a})}$. Let $J_{\tilde{\mathbf{s}}} = \{i \in I_{\mathbf{a}} | \tilde{s}_i \neq 0\}$. Since $\mathbf{as} = b$, then $\sum_{i \in J_{\tilde{\mathbf{s}}}} a_i \tilde{s}_i = b$. By the non-negativity of the a_i's it follows that if $J_{\tilde{\mathbf{s}}} \subset J_{\tilde{\mathbf{t}}}$, then $\sum_{i \in J_{\tilde{\mathbf{s}}}} a_i \tilde{s}_i < \sum_{i \in J_{\tilde{\mathbf{t}}}} a_i \tilde{t}_i$. Hence the set of $J_{\tilde{\mathbf{s}}}$ forms an antichain on $[k]^{w(\mathbf{a})}$ induced from the $\tilde{\mathbf{s}}$. That is, we have at most $k^{w(\mathbf{a})}/\sqrt{w(\mathbf{a})}$ such $J_{\tilde{\mathbf{s}}}$, each the result of projecting at most $2^{n-w(\mathbf{a})}$ solution (n, W)-words.

To justify the assumption that all a_i's are non-negative, we show how to repeatedly replace the pair $\mathbf{a}, b$ with a new pair $\mathbf{a}', b'$, where $w(\mathbf{a}') = w(\mathbf{a})$ and the number of (n, W)-words $\mathbf{s}$ such that $\mathbf{as} = b$ is the same as those with $\mathbf{a}'\mathbf{s} = b'$. We do this until $\mathbf{a}$ is nonnegative and the upper bound applies.

[2] Although we note that the following proofs can be modified to work without this demand of closure.

Let w_m be the maximum element in W and write $\mathbf{as} = \sum_{i\in 1}^{n} a_i s_i$. Say that $a_1 < 0$. Then we simply replace s_1 with $w_m - s_1$, and replace $\mathbf{a}$ and b with the result of rearranging

$$a_1(w_m - s_1) + \sum_{1=2}^{n} a_i s_i = b \text{ which is } -a_1 s_1 + \sum_{1=2}^{n} a_i s_i = b - a_1 w_m.$$

So let $\mathbf{a}' = (-a_1, a_2, \ldots, a_n)$ and $b' = b - a_1 w_m$. It is important to note that the pairs $\mathbf{a}, b$ and $\mathbf{a}', b'$ have the same number of solutions in W^n. This can be seen by mirroring the first coordinate around w_m: the vector $\mathbf{x} = (x_1, \ldots, x_n)$ is a solution to $\sum_{i\in 1}^{n} a_i x_i = b$ if and only if $\mathbf{x}' = (x'_1 = w_m - x_1, x'_2 = x_2 \ldots, x'_n = x_n)$ is a solution for

$$-a_1 x'_1 + \sum_{1=2}^{n} a_i x'_i = -a_1(w_m - x_1) + \sum_{1=2}^{n} a_i x_i = \sum_{1=1}^{n} a_i x_i - a_1 w_m = b - a_1 w_m = b'.$$

□

3.3 Large admissibility

A (n, W)-word s is *admissible* for an unsatisfiable set of integer linear inequalities $\mathcal{F}$ over n variables if s satisfies all constraints of $\mathcal{F}$. A set of (n, W)-words is admissible for $\mathcal{F}$ if all its elements are admissible. $\mathcal{A}(\mathcal{F}, W)$ is the set of all admissible (n, W)-words for $\mathcal{F}$.

The interesting sets W for an unsatisfiable set of integer linear inequalities $\mathcal{F}$ are those such that almost all (n, W)-words are admissible for $\mathcal{F}$. We will apply our method on sets of integer linear inequalities which are a translation of unsatisfiable CNF's generated over a given domain. Typically these formulas on a size n domain have a number of variables which is not exactly n but a function of n, $\nu(n) \geq n$. Hence for the rest of this section we consider $\mathscr{F} := \{\mathcal{F}_n\}_{n\in\mathbb{N}}$ as a family of sets of unsatisfiable integer linear inequalities, where $\mathcal{F}_n$ has $\nu(n) \geq n$ variables. We call $\mathscr{F}$ an *unsatisfiable family*.

Consider then the following definition recalling that we denote $k = |W|$:

Definition 7. *$\mathscr{F}$ is* almost full *if* $|\mathcal{A}(\mathcal{F}_n, W)| \geq k^{\nu(n)} - o(k^{\nu(n)})$.

Notice that, because of the o notation, Definition 7 might be not necessarily true for all $n \in \mathbb{N}$, but only starting from some $n_{\mathscr{F}}$.

Definition 8. *Given some almost full family $\mathscr{F}$ (over $\nu(n)$ variables) we let $n_{\mathscr{F}}$ be the natural number with*

$$\frac{k^{\nu(n)}}{|\mathcal{A}(\mathcal{F}_n, W)|} \leq 2 \quad \textit{for all} \quad n \geq n_{\mathscr{F}}.$$

As an example we prove SPHP is almost full (notice that in the case of SPHP_n, $\nu(n) = n$).

Lemma 3. *SPHP_n is almost full.*

Proof. Fix $W = \{0, 1/2\}$ so that $k = |W| = 2$. Let U be the set of all (n, W)-words with at least four coordinates set to $1/2$. U is admissible for SPHP_n since inequalities $x_i + x_j \leq 1$ are always satisfied for any value in W and inequalities $x_1 + \ldots + x_n \geq 2$ are satisfied by all points in U which always contain four $1/2$. By a simple counting argument, in U there are $2^n - 4n^3 = 2^n - o(2^n)$ admissible (n, W)-words. Hence the claim. □

Lemma 4. *Let $\mathscr{F} = \{\mathcal{F}_n\}_{n\in\mathbb{N}}$ be an almost full unsatisfiable family, where $\mathcal{F}_n$ has $\nu(n)$ variables. Further let $\mathcal{T}$ be a* SP *refutation of $\mathcal{F}$ of minimal width ω. If $n \geq n_{\mathscr{F}}$ then $|\mathcal{T}| = \Omega(\sqrt{w})$.*

Proof. We estimate at what rate the slab of the queries in $\mathcal{T}$ rule out admissible points in U.

Since all the queries in $\mathcal{T}$ have width at least w, according to Lemma 2, each query in $\mathcal{T}$ rules out at most $\frac{k^{\nu(n)}}{\sqrt{w}}$ admissible points. By Fact 1 no point survives at the leaves, in particular the admissible points. Then it must be that

$$|\mathcal{T}|\frac{k^{\nu(n)}}{\sqrt{w}} \geq |\mathcal{A}(\mathcal{F}_n, W)| \quad \text{which means} \quad |\mathcal{T}| \cdot \frac{k^{\nu(n)}}{|\mathcal{A}(\mathcal{F}_n, W)|} \geq \sqrt{w}$$

We finish by noting that, by the assumption $n \geq n_{\mathscr{F}}$, and then by Definition 8, we have $2 \geq \frac{k^{\nu(n)}}{|\mathcal{A}(\mathcal{F}_n, W)|}$. □

3.4 Main theorem

We focus on restrictions ρ that after applied on an unsatisfiable family $\mathscr{F} = \{\mathcal{F}_n\}_{n\in\mathbb{N}}$, reduce the set $\mathcal{F}$ to another set in the same family.

Definition 9. *Let $\mathscr{F} = \{\mathcal{F}_n\}_{n\in\mathbb{N}}$ be an unsatisfiable family and c a positive constant. $\mathscr{F}$ is* c-self-reducible *if for any set V of variables, with $|V| = t < n/c$, there is a restriction ρ with domain $V' \supseteq V$, such that $\mathcal{F}_n\restriction_\rho = \mathcal{F}_{n-ct}$ (up to renaming of variables).*

Let us motivate the definition with an example.

Lemma 5. SPHP_n *is* 1*-self-reducible.*

Proof. Whatever set of variables x_i, $i \in I \subset [n]$ we consider, it is sufficient to set x_i to 0 to fulfill Definition 9. □

Theorem 2. *Let $\mathscr{F} := \{\mathcal{F}_n\}_{n\in\mathbb{N}}$ be a unsatisfiable set of integer linear inequalities which is almost full and c-self-reducible. If $\mathcal{F}_n$ defines a feasible* LP *whenever $n > n_{\mathscr{F}}$, then for n large enough, the shortest* SP *proof of $\mathcal{F}_n$ is of length $\Omega(\sqrt[4]{n})$.*

Proof. Take any SP proof $\mathcal{T}$ refuting $\mathcal{F}_n$ and fix $t = \sqrt[4]{n}$.

The proof proceeds by stages $i \geq 0$ where $\mathcal{T}_0 = \mathcal{T}$. The stages will go on while the invariant property (which at stage 0 is true since $n > n_{\mathscr{F}}$ and c a positive constant)

$$n - ict^3 > \max\{n_{\mathscr{F}}, n(1 - 1/c)\}$$

holds.

At the stage i we let $\Sigma_i = \{(\mathbf{a}, b) \in \mathcal{T}_i : w(\mathbf{a}) \leq t^2\}$ and $s_i = |\Sigma_i|$. If $s_i \geq t$ the claim is trivially proven. If $s_i = 0$, then all queries in $\mathcal{T}_i$ have width at least t^2 and by Lemma 4 (which can be applied since $n - ict^3 > n_{\mathscr{F}}$) the claim is proven (for n large enough).

So assume that $0 < s_i < t$. Each of the queries in Σ_i involves at most t^2 nonzero coefficients, hence in total they mention at most $s_i t^2 \leq t^3$ variables. Extend this set of variables to some V' in accordance with Definition 9 (which can be done since, by the invariant, $ict^3 < n/c$). Set all these variables according to self-reducibility of $\mathcal{F}$ in a restriction ρ_i and define $\mathcal{T}_{i+1} = \mathcal{T}_i\restriction_{\rho_i}$. Note that by Definition 9 and by that of restriction, $\mathcal{T}_{i+1}$ is a SP refutation of $\mathcal{F}_{n-ict^3}$ and we can go on with the next stage. (Also note that we do not hit an empty refutation this way, due to the assumption that $\mathcal{F}_n$ defines a feasible LP.)

Assume that the invariant does not hold. If this is because $n - ict^3 < n_{\mathscr{F}}$ then, as each iteration destroys at least one node,

$$|\mathcal{T}| \geq i > \frac{n - n_{\mathscr{F}}}{ct^3} \in \Omega(n^{1/4}).$$

If this is because $n - ict^3 < n - n/c$, then again for the same reason it holds that

$$|\mathcal{T}| \geq i > \frac{n}{c^2 n^{3/4}} \in \Omega(n^{1/4}).$$

□

Using Lemmas 3 and 5 and the previous Theorem we get:

Corollary 2. *The length of any* SP *refutation of* SPHP_n *is* $\Omega(\sqrt[4]{n})$. *Hence the minimal depth is* $\Omega(\log n)$.

3.5 Lower bounds for the Pigeonhole principle

Definition 10. *The* Pigeonhole Principle PHP_n^m, $m > n$, *is the family of unsatisfiable integer linear inequalities defined over the variables* $\{P_{i,j} : i \in [m], j \in [n]\}$ *consisting of the following inequalities:*

$$\begin{array}{lll} \sum_{j=1}^{n} P_{ij} \geq 1 & \forall j \in [m] & \textit{(every pigeon goes into some hole)} \\ P_{ik} + P_{jk} \leq 1 & \forall k \in [n], i \neq j \in [m] & \textit{(at most one pigeon enters any given hole)} \end{array}$$

We present a lower bound for PHP_n^m closely following that for SPHP_n, in which we largely ignore the diversity of different pigeons (which makes the principle rather like SPHP_n).

In this subsection we fix $W = \{0, 1/2\}$, and for the sake of brevity refer to (n, W)-words as *biwords*.

Lemma 6. *The* PHP_n^m *is almost full.*

Proof. We show that there are at least 2^{mn-1} admissible biwords (for sufficiently large n). For each pigeon i, there are admissible valuations to holes so that, so long as at least two of these are set to $1/2$, the others may be set to anything in $\{0, 1/2\}$. This gives at least $2^n - (n+1)$ possibilities. Since the pigeons are independent, we obtain at least $(2^n - (n+1))^m$ biwords. Now this is $2^{mn}\left(1 - \frac{n+1}{2^n}\right)^m$ where $\left(1 - \frac{n+1}{2^n}\right)^m \sim e^{\frac{-(n+1)m}{2^n}}$ whence, $\left(1 - \frac{n+1}{2^n}\right)^m \geq e^{\frac{-(n+2)m}{2^n}}$ for sufficiently large n. It follows there is a constant c so that:

$$2^{mn}\left(1 - \frac{n+1}{2^n}\right)^m \geq 2^{mn - \frac{c(n+2)m}{2^n}} \geq 2^{mn-1}$$

for sufficiently large n. □

Lemma 7. *The* PHP_n^m *is* 1*-self-reducible (with respect to the subscript* n*).*

Proof. We are given some set I of variables from PHP_n^m. Let $H := \{j : P_{i,j} \in I \text{ for some i}\}$ be the holes mentioned by I. We simply forbid these holes with the restriction setting $P_{i,j}$ to 0 for every pigeon $i \in [m]$ and every hole $j \in H$. □

Theorem 3. *The length of any* SP *refutation of* PHP_n^m *is* $\Omega(n^{1/4})$.

Proof. Note that the all $1/2$ point is feasible for PHP_n^m. Then with Lemma 6 and Lemma 7 in hand we meet all the prerequisites for Theorem 2.

□

By simply noting that a SP refutation is a binary tree, we get the following corollary.

Corollary 3. *The SP depth of the* PHP_n^m *is* $\Omega(\log n)$.

3.6 Lower bounds for Tseitin contradictions over the complete graph

Definition 11. *For a graph $G = (V, E)$ along with a charging function $\omega : V \to \{0, 1\}$ satisfying $\sum_{v \in V} \omega(v) = 1 \mod 2$. The* Tseitin contradiction $\mathsf{Ts}(G, \omega)$ *is the set of linear inequalities which translate the CNF encoding of*

$$\sum_{\substack{e \in E \\ e \ni v}} x_e = \omega(v) \mod 2.$$

for every $v \in V$, where the variables x_e range over the edges $e \in E$.

In this subsection we consider $\mathsf{Ts}(K_n, \omega)$ and ω will always be an odd charging for K_n. We let $N := \binom{n}{2}$ and we fix $W = \{0, 1/2, 1\}$, $k = 3$ and for the sake of brevity refer to (n, W)-words as *triwords*. We will abuse slightly the notation of Section 3.3 and consider the family $\{\mathsf{Ts}(K_n, \omega)\}_{n \in \mathbb{N},\ \omega \text{ odd}}$ as a single parameter family in n. The reason we can do this is because the following proofs of almost fullness and self reducibility do not depend on ω at all (so long as it is odd, which we will always ensure).

Lemma 8. $\mathsf{Ts}(K_n, \omega)$ *is almost full.*

Proof. We show that $\mathsf{Ts}(K_n, \omega)$ has at least $c3^N$ admissible triwords, for any constant $0 < c < 1$ and n large enough. We define the assignment ρ setting all edges (i.e. x_e) to a value in $W = \{0, 1, 1/2\}$ independently and uniformly at random, and inspecting the probability that some fixed constraint for a node v is violated by ρ.

Clearly if at least 2 edges incident to v are set to $1/2$ its constraint is satisfied. If none of its incident edges are set to $1/2$ then it is satisfied with probability $1/2$. Let $A(v)$ be the event "*no edge incident to v is set to $1/2$ by ρ*" and let $B(v)$ be the event that "*exactly one edge incident to v is set to $1/2$ by ρ*". Then:

$$\Pr[v \text{ is violated}] \leq \frac{1}{2}\Pr[A(v)] + \Pr[B(v)] = \frac{1}{2}\frac{2^{n-1}}{3^{n-1}} + \frac{(n-1)2^{n-2}}{3^{n-1}} = n\frac{2^{n-2}}{3^{n-1}}.$$

Therefore, by a union bound, the probability that there exists a node with violated parity is bounded above by $n^2\frac{2^{n-2}}{3^{n-1}}$, which approaches 0 as n goes to infinity. □

Lemma 9. $\mathsf{Ts}(K_n, \omega)$ *is 2-self-reducible.*

Proof. We are given some set of variables I. Each variable mentions 2 nodes, so extend these mentioned nodes arbitrarily to a set S of size exactly $2|I|$, which we then hit with the following restriction: if S is evenly charged, pick any matching on the set $\{s \in S : w(s) = 1\}$, set those edges to 1, and set any other edges involving some vertex in S to 0. Otherwise (if S is oddly charged) pick any $l \in \{s \in S : w(s) = 1\}$ and $r \in [n] \setminus S$ and set x_{lr} to 1. $\{s \in S : w(s) = 1\} \setminus l$ is now even so we can pick a matching as before. And as before we set all other edges involving some vertex in S to 0. In the first case the graph induced by $[n] \setminus S$ must be oddly charged (as the original graph was). In the second case this induced graph was originally evenly charged, but we changed this when we set x_{lr} to 1. □

Lemma 10. *For any oddly charged ω and n large enough, all* SP *refutations of* $\mathsf{Ts}(K_n, \omega)$ *have length* $\Omega(\sqrt[4]{n})$.

Proof. We have that the all $1/2$ point is feasible for $\mathsf{Ts}(K_n, \omega)$. Then we can simply apply Theorem 2. □

Corollary 4. *The depth of any SP refutation of* $\mathsf{Ts}(K_n, \omega)$ *is* $\Omega(\log n)$.

4 The covering method

In [14] Linial and Radhakrishnan considered the problem of the minimal number of hyperplanes covering all the points of the cube $\{0,1\}^n$. To make the problem meaningful they defined the notion of an *essential covering* of $\{0,1\}^n$.

Definition 12 ([14])**.** *A set L of linear polynomials with real coefficients is said to be an* essential cover *of the cube $\{0,1\}^n$ if*

(E1) for each $v \in \{0,1\}^n$, there is a $p \in L$ such that $p(v) = 0$,

(E2) no proper subset of L satisfies (E1), that is, for every $p \in L$, there is a $v \in \{0,1\}^n$ such that p alone takes the value 0 on v, and

(E3) every variable appears (in some monomial with non-zero coefficient) in some polynomial of L.

They also prove the following theorem:

Theorem 4 ([14], Theorem 2)**.** *Any essential cover L of the cube with n coordinates satisfies $|L| \in \Omega(\sqrt{n})$.*

4.1 Turning a refutation of Tseitin contradictions into an essential cover of the hypercube

Fix some $\mathsf{Ts}(G,\omega)$ and a SP refutation $\mathcal{T}$, thought of as a set of queries $(\mathbf{a}, b)$. We say that an edge of G is *mentioned* in $\mathcal{T}$ if the variable x_e appears with non-zero coefficient in some query in $\mathcal{T}$.

Lemma 11. *For any matching M on the edges of G mentioned in $\mathcal{T}$, where all matched vertices have degree at least 3, there is an essential cover L of the $|M|$ coordinate hypercube with $|L| \leq |R|$.*

Proof. Let M be any matching on the edges mentioned in $\mathcal{T}$. Let H' be the set of the $2^{|M|}$ admissible points for $\mathsf{Ts}(G,\omega)$ gotten by giving the edges in M any $\{0,1\}$ value and setting the rest of the edges to $1/2$. (That these are admissible for $\mathsf{Ts}(G,\omega)$ comes from the fact that, given the degree of G is at least 3, all vertices, including matched ones, are incident to at least two edges set to $1/2$.) By Fact 1 all of these points must have been killed in some query $(\mathbf{a}, b)$ in $\mathcal{T}$ (i.e. $x \in \mathsf{slab}(\mathbf{a}, b)$)). Hence

$$x \text{ is killed by } (\mathbf{a}, b) \Leftrightarrow \sum_{e \in E(G)} a_e x_e = b + 1/2 \Leftrightarrow \sum_{e \in M} a_e x_e = b + 1/2 - (1/2)\left(\sum_{e \in E(G)\setminus M} a_e\right)$$

This just means that the set

$$L := \left\{ \left((a_e)_{e \in M}, b + \frac{1}{2}\left(1 - \sum_{e \in E(G)\setminus M} a_e\right)\right) : (a,b) \in R \right\}$$

covers the hypercube $H = \{0,1\}^{|M|}$ defined over variables $x_e, e \in M$. It remains to show that this cover is essential:

- (E1) i.e. for each $x \in H$, there is some $p \in L$ with $p(x) = 0$. This is clear and just talked about.
- (E2) i.e. no proper subset satisfies E1. As we are interested in the lower bound, we can just take subsets if we need to.
- (E3) i.e. every variable appears with non-zero coefficient somewhere in L. This just follows from M being a subset of the edges mentioned by $\mathcal{T}$.

□

Lemma 12. *Pick some set S of vertex-disjoint unit squares (4-cycles) in H_n. Any refutation R of any $\mathsf{Ts}(H_n, \omega)$ must mention at least one edge in each square.*

Proof. We will use a couple times the following idea due to A. Urquhart in [19]: starting from some binary assignment to the edges in G, take a path from two vertices u and v, and flip all the edges on this path. If u and v are distinct, we flip their polarities (as they are incident to exactly one edge that gets flipped) and no other vertex has its incident charge changed (because they have zero or two incident edges flipped.) If $u = v$, then nothing gets its polarity changed. In this way we can find a binary assignment to the edges of any graph falsifying exactly the parity constraint for a single node v.

So suppose some square $s := \{a, b, c, d\} \subseteq V(H_n)$ fails to have a single edge mentioned. Find a binary assignment to the edges falsifying (say) only the parity constraint for a. Modify this assignment by setting every edge in s to $1/2$. This point is admissible - a is incident to two $1/2$ edges and so is any other vertex that has had its incident edges touched. But this admissible point can never be ruled out in a slab, as it is only fractional on edges not mentioned by R. □

Theorem 5. *Let ω be an odd charging of H_n. $\mathsf{Ts}(H_n, \omega)$ requires length $\Omega(n)$ to refute in SP.*

Proof. Fix some refutation R. We work in the inner $(n-2) \times (n-2)$ grid - in this grid every node has degree 4 so we may use Lemma 11. In this grid we can find $d := (\lfloor \frac{n-2}{2} \rfloor)^2$ vertex-disjoint squares, and in each such square we can choose (Lemma 12) an edge mentioned in R. As these squares are vertex disjoint the chosen edges form a matching and Lemma 11 tells us there is some essential cover R of the d-dimensional hypercube with $|R| \geq |L|$. Now due to Theorem 4 we have $|L| \in \Omega(n)$ and we are done. □

Corollary 5. *$\mathsf{Ts}(H_n, \omega)$ requires depth $\Omega(\log(n))$ to refute in SP.*

5 Conclusions and acknowledgements

The $\Omega(\log n)$ depth lower bound for $\mathsf{Ts}(H_n, \omega)$ is not optimal since [2] proved an $O(\log^2 n)$ upper bound for $\mathsf{Ts}(G, \omega)$, for any bounded-degree G. Even to apply the covering method to prove a depth $\Omega(\log^2 n)$ lower bound on $\mathsf{Ts}(K_n, \omega)$ (notice that it would imply a superpolynomial length lower bound), the polynomial covering of the boolean cube should be improved to work on general cubes. To this end the algebraic method used in [14] should be improved to work with generalizations of multilinear polynomials.

While finishing the writing of this manuscript we learned about [8] from Noah Fleming. We would like to thank him for answering some questions on his paper [2], and sending us the manuscript [8] and for comments on a preliminary version of this work.

References

[1] Noga Alon and Zoltán Füredi. Covering the cube by affine hyperplanes. *Eur. J. Comb.*, 14(2):79–83, 1993.

[2] Paul Beame, Noah Fleming, Russell Impagliazzo, Antonina Kolokolova, Denis Pankratov, Toniann Pitassi, and Robert Robere. Stabbing planes. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference, ITCS 2018, January 11-14, 2018, Cambridge, MA, USA*, volume 94 of *LIPIcs*, pages 10:1–10:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[3] Joshua Buresh-Oppenheim, Nicola Galesi, Shlomo Hoory, Avner Magen, and Toniann Pitassi. Rank bounds and integrality gaps for cutting planes procedures. *Theory of Computing*, 2(4):65–90, 2006.

[4] Teena Carroll, Joshua Cooper, and Prasad Tetali. Counting antichains and linear extensions in generalizations of the boolean lattice, 2009.

[5] W. Cook, C. R. Coullard, and G. Turán. On the complexity of cutting-plane proofs. *Discrete Appl. Math.*, 18(1):25–38, 1987.

[6] Martin Davis, George Logemann, and Donald W. Loveland. A machine program for theorem-proving. *Commun. ACM*, 5(7):394–397, 1962.

[7] Martin Davis and Hilary Putnam. A computing procedure for quantification theory. *J. ACM*, 7(3):201–215, 1960.

[8] Noah Fleming, Mika Göös, Russell Impagliazzo, Toniann Pitassi, Robert Robere, Li-Yang Tan, and Avi Wigderson. On the power and limitations of branch and cut. Technical report, 2021.

[9] Nicola Galesi, Pavel Pudlák, and Neil Thapen. The space complexity of cutting planes refutations. In David Zuckerman, editor, *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, volume 33 of *LIPIcs*, pages 433–447. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.

[10] Henry A. Kautz and Bart Selman. Ten challenges redux: Recent progress in propositional reasoning and search. In Francesca Rossi, editor, *Principles and Practice of Constraint Programming - CP 2003, 9th International Conference, CP 2003, Kinsale, Ireland, September 29 - October 3, 2003, Proceedings*, volume 2833 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2003.

[11] Arist Kojevnikov. Improved lower bounds for tree-like resolution over linear inequalities. In João Marques-Silva and Karem A. Sakallah, editors, *Theory and Applications of Satisfiability Testing - SAT 2007, 10th International Conference, Lisbon, Portugal, May 28-31, 2007, Proceedings*, volume 4501 of *Lecture Notes in Computer Science*, pages 70–79. Springer, 2007.

[12] Jan Krajícek. Discretely ordered modules as a first-order extension of the cutting planes proof system. *J. Symb. Log.*, 63(4):1582–1596, 1998.

[13] Jan Krajícek. Interpolation by a game. *Math. Log. Q.*, 44:450–458, 1998.

[14] Nathan Linial and Jaikumar Radhakrishnan. Essential covers of the cube by hyperplanes. *Journal of Combinatorial Theory, Series A*, 109(2):331–338, 2005.

[15] Lutz Mattner and Bero Roos. Maximal probabilities of convolution powers of discrete uniform distributions. *Statistics & probability letters*, 78(17):2992–2996, 2008.

[16] Mark Nicholas Charles Rhodes. On the chvátal rank of the pigeonhole principle. *Theor. Comput. Sci.*, 410(27-29):2774–2778, 2009.

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

[18] Bart Selman, Henry A. Kautz, and David A. McAllester. Ten challenges in propositional reasoning and search. In *Proceedings of the Fifteenth International Joint Conference on Artificial Intelligence, IJCAI 97, Nagoya, Japan, August 23-29, 1997, 2 Volumes*, pages 50–54. Morgan Kaufmann, 1997.

[19] Alasdair Urquhart. Hard examples for resolution. *J. ACM*, 34(1):209–219, 1987.

[20] Jacobus Hendricus van Lint and Richard Michael Wilson. *A Course in Combinatorics*. Cambridge University Press, Cambridge, U.K.; New York, 2001.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il