Manuscript version: *October 1, 1996*
*DIMACS workshop on Feasible Arithmetics and Proof Complexity* (Submitted)

# Exponential Lower Bounds on the Size of Clause Based Semantic Derivations

Stasys Jukna*

Department of Computer Science †
University of Trier, D-54286, Trier, GERMANY
and
Department of Mathematical Logic
Institute of Mathematics, Vilnius, LITHUANIA

## Abstract

We consider the clause–based version of the general model of *semantic derivations* proposed by Krajíček. Resolution refutation proof is a special deterministic version of fanin-2 clause–based derivation. We prove the following combinatorial lower bound on the length of such derivations. Let $\mathcal{F}$ be a $k$-partite hypergraph, with at most $b$ points in each part such that no point belongs to more than $d$ edges and any two edges share at most $\lambda$ points. If $|\mathcal{F}| \geq k(d+1)/2$ then no CNF containing such a hypergraph among its clauses, can have a fanin-$l$ semantic derivation of length smaller than $\exp\left(\Omega\left(\frac{k^2}{b(l+\lambda)}\right)\right)$. When applied to the generalized pigeonhole principle $PHP_n^m$ and to blocking principles for finite geometries, this directly yields exponential lower bounds on the length of their semantic derivations, including the $\exp\left(\Omega(n^2/(lm))\right)$ lower bound for the length of fanin-$l$ clause–based semantic derivation of $PHP_n^m$.

*Research supported by a DFG grant Me 1077/10–1.

†E-mail: jukna@ti.uni-trier.de

# 1. Introduction

The pigeonhole principle asserts that every arrangement of $n$ pigeons among $m$ $(m > n)$ holes must leave at least one of the holes empty. A natural search problem associated with this principle is to find such a hole. Many other problems have a similar flavor: Given an unsatisfiable CNF formula and an assignment to its variables, find a clause which is not satisfied. Given a hypergraph $\mathcal{F}$ and a set of points $A$ which does not intersect all the edges of $\mathcal{F}$, find an edge $E \in \mathcal{F}$ such that $E \cap A = \emptyset$. In general, given a set $H$ of Boolean functions and a set $A \subseteq \{0,1\}^n$ of binary strings, the *search problem* for $H$ over the set $A$ is the following: given an input $a \in A$ (a query), find a function $h \in H$ (an answer) such that $h(a) = 0$. The problem is *valid* (or well-defined) if every query has at least one answer; the problem is to find it.

How hard it is to solve such search problems? The answer depends of course on their representation and the computational model. A general situation is captured by the model of 'semantic derivations' introduced by Krajíček [17]. This is a kind of a standard model of straight-line program, and is defined in [17] as follows. Let $F$ be a set of Boolean functions. A semantic $F$-derivation of a Boolean function $f$ from the functions in $H$ is a sequence of functions $f_1, \ldots, f_t$ such that $f_t = f$, and each $f_i$ is either one of the functions in $H$ or belongs to $F$ and is derived from previous functions by the *semantic rule*, which allows to infer a function $f_i$ from the functions $f_{i_1}, \ldots, f_{i_l}$ if and only if $f_i \geq \prod_{j=1}^{l} f_{i_j}$. As noted in [17], proofs in any of the usual propositional calculi translate into semantic derivations: simply replace a sequent (a formula, an equation, etc) by the corresponding Boolean function. We are going to look semantic derivations as searching algorithms, so we slightly extend their definition.

A *semantic $F$-derivation* for a search problem $(H, A)$ is a directed acyclic graph $G$ with one distinguished node $v_0$, called the *root*, and a set of out–degree 0 nodes, called the *leaves*. Every node $v$ of $G$ is labeled by a Boolean function $f_v \in F \cup H$ (called a *test function*) in such a way that $f_v \in H$ for every leaf $v$, and $f_{v_0}(A) \equiv 0$ for the root $v_0$. The only restriction is that the labeling $v \mapsto f_v$ must fulfill the following *consistency* condition: if $v_1, \ldots, v_l$ are immediate successors of a node $v$ in $G$ then

$$f_v(a) \geq \prod_{i=1}^{l} f_{v_i}(a) \quad \text{for all} \quad a \in A.$$

The consistency ensures that for every $a \in A$ there must be at least one path $v_0, v_1, \ldots, v_t$ in $G$ from the root $v_0$ to a leaf $v_t$ such that $f_{v_0}(a) = f_{v_1}(a) = \ldots = f_{v_t}(a) = 0$. Since the last function $f_{v_t}$ belongs to $H$, we have found a desired answer for the query $a$. Note that, for

$A = \{0,1\}^n$, the sequence of all test functions in semantic $F$-derivation for a search problem $(H, A)$ is exactly the semantic $F$-derivation of the function $f_{v_0}$ from $H$ in the sense of [17] (and vice versa). Thus, the only difference is that we represent the derivation as a graph and relax the consistency condition to subsets $A \subseteq \{0,1\}^n$.

The *size* (or *length*) of a derivation is the number of nodes in it. The *fanin* is the maximal out–degree [1] of its node. Given a search problem, the goal is to estimate the minimum possible size of a derivation for it.

If we allow arbitrary fanin then the problem becomes trivial: take $|F|$ leaves and connect the root with each of them. Moreover, if we put no other restrictions on the labeling $v \mapsto f_v$, except for consistency, then the search procedure is, in general, non-deterministic. It can be made deterministic by the following restriction: require that every node $v$ in $G$ has only two successors $v_1$ and $v_2$, and that the corresponding test functions satisfy the inequality $f_v \geq (x_i \vee f_{v_1}) \wedge (\neg x_i \vee f_{v_2})$ for some variable $x_i$. It is easy to see that then every input induces exactly one path from the root to a leaf, i.e. the search is deterministic. The class of such semantic derivations is the familiar model of (deterministic) *branching programs.*

The fanin in branching programs is restricted to 2 but there is no restriction on the form of test functions. On the other hand, the most restrictive case would be to require each test function $f_v$ to be a *clause*, i.e. a disjunction of some variables or their negations. If we add the additional requirement that $f_v = (x_i \vee f_{v_1}) \wedge (\neg x_i \vee f_{v_2})$ then we obtain the classical model of *resolution refutation proof.* If we add one more restriction - require the graph be a tree - then we obtain the familiar Boolean *decision tree* model. Search problems in this model were studied by Lovász *et al.* [18] where a drastic difference between nondeterministic, probabilistic and deterministic variants of this model was shown.

In this paper we concentrate on an intermediate computational model: we restrict possible test functions $f_v$ to clauses only (as in resolution) but allow large fanin and do not put any other restrictions on the the labeling $v \mapsto f_v$, except the consistency (hence, the resulting derivation needs not be deterministic). We call such derivations *clause-based semantic derivation.* Formally, these are semantic $F$-derivations where $F$ is the set of all clauses. Our main result is a general combinatorial lower bound for this model (Theorem 1 below) and the simplicity of its proof.

[1] Not the in-degree, it can be arbitrary. Fanin $l$ means that every conclusion must be derived (by the semantic rule) from at most $l$ hypotheses.

# 2. A general lower bound

In this section we state our main result and describe several its applications. We first need to setup some notation. A *hypergraph* over a set $X$ is a family $\mathcal{F}$ of its subsets; elements of $X$ are *points*, and sets in $\mathcal{F}$ are *edges*. The *cover number* $\tau(\mathcal{F})$ is the minimal possible number of points in a set, intersecting all the edges of $\mathcal{F}$. By an *edge-search problem for* $\mathcal{F}$ we will mean the following: given a set $A$ with $|A| < \tau(\mathcal{F})$, find an edge $E$ of $\mathcal{F}$ such that $A \cap E = \emptyset$. There can be several such edges in $\mathcal{F}$; our goal is to find at least one of them.

We will be interested in the size of clause-based semantic derivation for this problem. Recall that any such derivation is a digraph, each node of which is labeled by a clause. Leaves are labeled by (positive) clauses $\{x_i : i \in E\}$, one for each edge $E \in \mathcal{F}$. All the remaining nodes can be labeled by clauses in an arbitrary way; consistency is the only requirement. Note that if $C = \{x_i : i \in I\} \cup \{\neg x_j : j \in J\}$ is a clause then $C(A) = 0$ if and only if $A \cap I = \emptyset$ and $A \supseteq J$. Thus, in clause-based derivations we allow tests of the form "Does $A$ separates a given pair of disjoint sets?".

We will consider only special $k$-partite hypergraphs. Let $S_1, \ldots, S_k$ be mutually disjoint subsets of $X$, called *blocks*. A *partial transversal* is a set $B \subseteq X$ which intersects each block in at most one point; $B$ is a *transversal* if $|B| = k$ (in this case $B$ intersects each block in exactly one point).

**Definition.** We call a hypergraph $\mathcal{F}$ a $(k, b, \lambda, d)$-*design* if there exist $k$ mutually disjoint blocks $S_1, \ldots, S_k$ such that:

1. Every edge of $\mathcal{F}$ is a transversal for $S_1, \ldots, S_k$;
2. $|S_i| \leq b$ for all $i = 1, \ldots, k$;
3. $|E \cap F| \leq \lambda$ for all edges $E \neq F \in \mathcal{F}$;
4. Every point belongs to at most $d$ edges of $\mathcal{F}$.

Such a design $\mathcal{F}$ is *large* if every transversal of $S_1, \ldots, S_k$ avoids at least one edge of $\mathcal{F}$. Note that any design, with more than $kd$ edges, is large, but there also are large designs with smaller number of edges.

Our main result is the following general lower bound on the size of clause–based semantic derivations.

**Theorem 1.** *Let $\mathcal{F}$ be a large $(k, b, \lambda, d)$-design, and $G$ be a clause-based semantic derivation of fanin at most $l$. Let $s$ and $t$ be integers satisfying*

$$ls \leq \min\{|\mathcal{F}| - dt, k - t\} \text{ and } t \geq k/2 \tag{1}$$

*If $G$ solves the edge-search problem for $\mathcal{F}$ then $|G| \geq 2^{M/b}$ where*

$$M = \frac{s(k - t - ls + 1)^2}{k + \lambda \cdot (s - 1)} \tag{2}$$

*In particular, if $|\mathcal{F}| \geq k(d + 1)/2$ then*

$$|G| \geq \exp\left(\Omega\left(\frac{k^2}{b(l + \lambda)}\right)\right). \tag{3}$$

**Remark.** Note that Theorem 1 gives also the same lower bound for the size of any clause-based semantic derivation of the following statement $Cover(\mathcal{F})$: "for any set of points $A$, either $|A| \geq \tau(\mathcal{F})$ or $A$ does not intersect some edge of $A$". This statement can be written as a propositional formula in different ways. For example, one can take an unsatisfiable CNF formula $\Phi(x) \wedge \Psi(x, y)$ where $\Phi(x)$ consists of $|\mathcal{F}|$ clauses $\{x_i : i \in E\}$, one for each edge $E \in \mathcal{F}$, and $\Psi(x, y)$ consist of the clauses $\{y_{i,1}, \ldots, y_{i,|X|}\}$, $\{\neg y_{i,j}, \neg y_{i',j}\}$, $\{\neg y_{i,j}, \neg x_j\}$ where $1 \leq i \neq i' \leq |X| - \tau(\mathcal{F}) + 1$ and $1 \leq j \leq |X|$. The meaning of this last formula is the following: given a set of points $A \subseteq X$, the formula $\Psi(A, y)$ is satisfiable if and only if there is an injection from $\{1, \ldots, |X| - \tau(\mathcal{F}) + 1\}$ to $X \setminus A$, which in turn can happen iff $|A| < \tau(\mathcal{F})$. The whole formula $Cover(\mathcal{F})$ has $O(|\mathcal{F}| + |X|^2)$ clauses. Note that any semantic derivation of $Cover(\mathcal{F})$ also solves the edge-search problem for $\mathcal{F}$: associate with each set $A$ of less than $\tau(\mathcal{F})$ points, a string $y_A$ such that $\Psi(A, y_A) = 1$, and fix this injection. (Recall that in clause–based derivation we allow *arbitrary* clauses; besides main '$x$-variables' they can have any auxiliary '$y$-variables'). Thus, a lower bound on the size of a semantic derivation for the edge-search problem for $\mathcal{F}$ is also a lower bound on the size of a semantic derivation of an empty clause from the clauses in $Cover(\mathcal{F})$. The complexity of the search problem itself is, however, interesting in its own right.

To motivate the rest of the paper, let us mention several applications of Theorem 1.

**Example 1 (Pigeonhole principle).** The pigeonhole principle $PHP_n^m$ $(m \geq n + 1)$ says that if each of $n$ pigeons sits in one of the $m$ holes (and, by the low of nature, no one sits in two holes) then there must be an empty hole. The corresponding search problem is the following: given an $n \times m$ $(0,1)$-matrix $M$ with $m > n$ and exactly one 1 in each row, find an all-0 column. In this case we have a hypergraph $\mathcal{F}$ with $m$ edges, corresponding to columns, and $n$ blocks, corresponding to rows. Since $|\mathcal{F}| = m > n$, this hypergraph is a large $(k, b, \lambda, d)$-design with $k = n$, $b = m$, $\lambda = 0$ and $d = 1$. Since $|\mathcal{F}| = m > n = k(d+1)/2$, we can apply (3), which yields the lower bound $2^{\Omega\left(n^2/(ml)\right)}$. Recall that $2^{\Omega(n^2/m)}$ is the best known lower bound for the minimal length of a Resolution refutation proof of $PHP_n^m$ [13, 23, 9, 11]. So, the reason why $PHP_n^m$ is hard for Resolution, seems to lie not in the weakness of the resolution rule itself, but rather in the impossibility to keep enough information about possible outcomes, using small (up to $l$) sets of clauses.

**Example 2 (Affine planes).** Take an affine plane $\mathrm{AG}(2, q)$ of order $q$. Every point lies on $q+1$ lines, and there are $q(q+1)$ lines, each two of which intersect in at most one point. It is known (see [15, 5]) that every set of less than $2q-1$ points misses at least one line of $\mathrm{AG}(2,q)$. This result leads to the following *line search problem for* $\mathrm{AG}(2,q)$. We have $n = q(q+1)$ variables $x_1, \ldots, x_n$ corresponding to points, and $n$ leaves, labeled by clauses $C_L = \bigvee_{i \in L} x_i$, corresponding to lines $L$. Given a set of at most $2(q-1)$ points, the problem is to find a line with no point in this set. By the result, mentioned above, this problem is well defined. Any semantic derivation for this problem solves the edge-search problem for the following design $\mathcal{F}$. Take any set $\mathcal{L}' = \{L_1, \ldots, L_q\}$ of $q$ parallel (i.e. mutually disjoint) lines, and consider the hypergraph $\mathcal{F}$, the edges of which are all the remaining $q^2$ lines. Since every such line intersects each of the lines $L_1, \ldots, L_q$ in exactly one point, the hypergraph $\mathcal{F}$ is a $(k, b, \lambda, d)$-design with $k = b = d = q$ and $\lambda = 1$. To verify the largeness, let $B$ be any transversal. Since $B$ intersects all the lines $L_1, \ldots, L_q$, we have that $B$ must avoid at least one line of $\mathcal{F}$, since otherwise $B$ would intersect *all* the lines of $\mathrm{AG}(2,q)$. Thus $\mathcal{F}$ is large. Since $|\mathcal{F}| = q^2 > q(q+1)/2 = k(d+1)/2$, we we can apply (3), which yields the lower bound $2^{\Omega(q/l)} = \exp\left(\sqrt{|\mathcal{F}|}/l\right)$ on the size of any clause–based semantic derivation of fanin $\leq l$, solving the edge-search problem for $\mathcal{F}$, and hence, for any such derivation solving the line search problem for $\mathrm{AG}(2,q)$.

**Example 3 (Projective planes).** Take a projective plane $\mathrm{PG}(2,q)$ of order $q$. It has the same number $n = q^2 + q + 1$ of lines and points; each line has $q+1$ points and every point lies in $q+1$ lines; any two lines share exactly one point. It is known (see [6, 7]) that any set of at most $q + \sqrt{q}$ points must either contain a line or must avoid a line. This result leads to the following *line search problem for* $\mathrm{PG}(2,q)$. We have $n = q^2 + q + 1$ variables $x_1, \ldots, x_n$ corresponding to points, and and $2n$ leaves, labeled by clauses $C_L^+ = \bigvee_{i \in L} x_i$ and $C_L^- = \bigvee_{i \in L} \neg x_i$. Given a set of at most $q + \sqrt{q}$ points, the problem is to find a line which lies entirely either in this set or in its complement. This problem reduces to the line search problem in affine planes. The idea is to use the well-known fact that deletion of any one line $L_0$ from $\mathrm{PG}(2,q)$ (together with all its points) gives us affine plane $\mathrm{AG}(2,q)$; the lines of this new plane are sets $L \setminus L_0$ where $L \neq L_0$ are lines of the projective plane. Let now $G$ be a fanin-$l$ clause–based semantic derivation solving the line search problem for $\mathrm{PG}(2,q)$. Fix an arbitrary line $L_0$ of $\mathrm{PG}(2,q)$ and set to 0 all the variables $x_i$ with $i \in L_0$. This restriction kills (evaluates to 1) all negative leaves of $G$ and deletes (i.e. evaluates to 0) exactly one variable from each positive leaf. The restriction $L_0 \mapsto 0$ corresponds to deletion of $L_0$ from $\mathrm{PG}(2,q)$, and hence, leads to $\mathrm{AG}(2,q)$. Thus, we obtain a derivation which solves the line search problem for $\mathrm{AG}(2,q)$. As shown in the previous example, this derivation (and hence the original derivation $G$) must have at least $2^{\Omega(q/l)}$ clauses.

# 3. The proofs

The proof of Theorem 1 consists of two steps: the 'killing large clauses' step and the 'forcing large clauses' step. The goal of the first step is to show that, if the graph $G$ would have less than $2^{M/b}$ clauses, with $M$ defined by (2), then it would be possible to set some $t$ variables to constants so that all long clauses in $G$ are killed (i.e. are evaluated to 1). The goal of the second step is to show that no graph can solve the desired search problem, using only short clauses as tests. Hence, the size of $G$ cannot be smaller than $2^{M/b}$, as desired.

The approach itself is not new. Similar ideas appear (more or less explicitly) in different lower bounds proofs. The 'killing' (large clauses/monomials) idea is a standard trick in circuit complexity (cf. the famous Switching Lemma for depth-2 AND/OR circuits). The 'forcing' (large clauses) idea was used by Chvátal and Szemerédi [10] to generate hard examples for resolution. In a recent work [2], Beame and Pitassi accumulated both ideas into a direct and elegant proof of Haken's [13] lower bound for the pigeonhole principle $PHP_n^{n+1}$. Our work is motivated by the exposition in [2].

All the combinatorics we need is accumulated in two lemmas: the 'killing large clauses' lemma (Lemma 1) and the 'forcing large clause' lemma (Lemma 2)

## 3.1. Combinatorics

**Lemma 1. (Killing Lemma)** *Let $\mathcal{A}$ be a hypergraph over a set $X$, and $S_1, \ldots, S_k$ be a partition of $X$ into sets of cardinality at most $b$. If $|\mathcal{A}| < \left(\frac{k}{k-t}\right)^{r/b}$ and each edge of $\mathcal{A}$ has* *more than $r$ points then there is a partial transversal $T$ of $S_1, \ldots, S_k$ such that $|T| \leq t+1$ and $T$ intersects all the edges of $\mathcal{A}$.*

**Proof.** Let $n = |X|$. We construct the set $T$ via the following "greedy" procedure. Let $\mathcal{A}^1 = \mathcal{A}$ and $X^1 = X$. For each $i$, $1 \leq i \leq t$, include in $T$ the element $x_i \in X^i$ which occurs in the largest number of sets of $\mathcal{A}^i$. Then remove from $X^i$ all the points of that block, which contains $x_i$, to obtain $X^{i+1}$, and remove all the sets containing $x_i$ from $\mathcal{A}^i$ to obtain $\mathcal{A}^{i+1}$. Sets deleted after $t+1$ steps intersect the set $\{x_1, \ldots, x_{t+1}\}$. Since $n \leq kb$, the number of remaining sets in $\mathcal{A}$ is bounded from above by $\alpha \cdot |\mathcal{A}|$ where

$$\begin{aligned} \alpha &= \left(1 - \frac{r}{n}\right)\left(1 - \frac{r}{n-b}\right) \cdots \left(1 - \frac{r}{n-bt}\right) \leq e^{-\frac{r}{n} - \frac{r}{n-b} - \cdots - \frac{r}{n-bt}} \\ &\leq e^{-\frac{r}{b}\left[\frac{1}{k} + \frac{1}{k-1} + \cdots + \frac{1}{k-t}\right]} \leq \left(\frac{k}{k-t}\right)^{-r/b}. \end{aligned}$$

Since $\mathcal{A}$ has less than $\alpha^{-1}$ sets, all the sets of $\mathcal{A}$ are already intersected by $T$, as desired. ▯

Let $T$ be a partial transversal of $S_1, \ldots, S_k$, and let $\mathcal{H} \subseteq \mathcal{F}$. We say that $\mathcal{H}$ is a *$T$-witness* for a set of points $A$ if, for every transversal $B$ containing $T$, we have that either $B \cap A \neq \emptyset$ or $B \cap E = \emptyset$ for at least one $E \in \mathcal{H}$ (or both). Put otherwise, every extension of $T$, intersecting all the edges of $\mathcal{H}$, must intersect the set $A$. Given a set of points $A \subseteq X$, define its *weight* $w_T(A)$ as the minimum number $|\mathcal{H}|$ of edges in a $T$-witness $\mathcal{H}$ for $A$. Note that the largeness of $\mathcal{F}$ ensures that the weight function $w_T(\cdot)$ is well-defined for every partial transversal $T$

**Lemma 2. (Forcing Lemma)** *Let $T$ be a partial transversal, $t = |T|$, and let $A \subseteq X$ be a set of points of weight $s = w_T(A)$. Then*

$$|A| \geq \frac{s(k-t-s+1)^2}{k + \lambda(s-1)}. \tag{4}$$

Lemma 2 follows directly from the following two lemmas.

**Lemma 3.** *Let $\mathcal{H}$ be a minimal $T$-witness for a set $A$. Let $s = |\mathcal{H}|$ and $t = |T|$. Then $|A \cap E| \geq k - t - s + 1$ for every edge $E \in \mathcal{H}$.*

**Proof.** Take an arbitrary edge $E \in \mathcal{H}$. Since $\mathcal{H}$ is minimal, there must be a transversal $B \supseteq T$ such that the set $B$ intersects all the edges of $\mathcal{H}' = \mathcal{H} \setminus \{E\}$ but $B \cap (E \cup A) = \emptyset$. For each edge $E' \in \mathcal{H}'$ choose any one point from the intersection $B \cap E'$, and let $I$ be the set of these choosed $\leq |\mathcal{H}'| = s-1$ points. Let $\tilde{E}$ denote the set of all points in $E$, which belong to no of the blocks intersecting $I \cup T$. Since every edge $E$ is a transversal, every block contains only one point of $E$, and hence, $|\tilde{E}| \geq |E| - |T| - |I| \geq k - t - s + 1$. It remains therefore to prove that $A \supseteq \tilde{E}$ for every edge $E \in \mathcal{H}$.

To prove this, take an edge $E \in \mathcal{H}$ and an arbitrary point $x \in \tilde{E}$. Our goal is to show that $x$ belongs to $A$. Let $S$ be the (unique) block containing this point $x$. The fact that point $x$ belongs to $\tilde{E}$ implies that this block $S$ is disjoint from both $T$ and $I$. Since $B$ is a partial transversal and $B \cap \tilde{E} = \emptyset$, the block $S$ intersects $B$ in some other point $y \neq x$. Remove from $B$ the point $y$ and add the point $x$. The resulting set $(B \setminus \{y\}) \cup \{x\}$ intersects the edge $E$. Moreover, $B \setminus \{y\} \supseteq I \cup T$, because $y \in S$ and $S \cap (I \cup T) = \emptyset$. Therefore, the set $(B \setminus \{y\}) \cup \{x\}$ contains $T$ and intersects all the remaining edges in $\mathcal{H}'$ (since $I$ intersects them). Since $\mathcal{H}$ is a witness for $A$, we have that $A \cap ((B \setminus \{y\}) \cup \{x\}) \neq \emptyset$. This together with $A \cap B = \emptyset$, implies that $x \in A$. ▯

**Lemma 4.** *Let $\mathcal{F} = \{E_1, \ldots, E_s\}$ be a family of sets such that $u \leq |E_i| \leq v$ and $|E_i \cap E_j| \leq \lambda$ for all $i \neq j$. Then*

$$|E_1 \cup \cdots \cup E_s| \geq \frac{u^2 s}{v + (s-1)\lambda}.$$

**Proof.** The proof is a slight modification of a similar counting argument used by K. Corrádi [12] in the case when $u = v$. Let $X = \cup_{i=1}^{s} E_i$. For a point $x \in X$, let $d(x)$ be the number of sets in $\mathcal{F}$ containing $x$. Then, for each set $E \in \mathcal{F}$, $\sum_{x \in E} d(x) = \sum_{F \in \mathcal{F}} |E \cap F| \leq v + (s-1)\lambda$. Summing over all sets $E \in \mathcal{F}$ we obtain

$$\sum_{E \in \mathcal{F}} \sum_{x \in E} d(x) = \sum_{x \in X} d(x)^2 \geq \frac{1}{|X|} \left( \sum_{x \in X} d(x) \right)^2 = \frac{1}{|X|} \left( \sum_{E \in \mathcal{F}} |E| \right)^2 \geq \frac{(us)^2}{|X|}.$$

Using the previous estimate we obtain $(us)^2 \leq s \cdot |X| \left(v + (s-1)\lambda\right)$, which gives the desired lower bound on $|X|$. ▯

**Proof of Lemma 2.** Let $\{E_1, \ldots, E_s\} \subseteq \mathcal{F}$ be a minimal set of edges witnessing the weight of $A$. By Lemma 3 there exist subsets $\tilde{E}_i \subseteq E_i$ such that $A \supseteq \tilde{E}_1 \cup \cdots \cup \tilde{E}_s$ and $u \leq |\tilde{E}_i| \leq v$ with $u = k - t - s + 1$ and $v = k$. Lemma 4 yield the desired lower bound (4). ▯

## 3.2. Proof of Theorem 1

Let $G$ be a clause-based semantic derivation of fanin at most $l$ and suppose that $G$ solves the edge-search problem for $\mathcal{F}$. The largeness of $\mathcal{F}$ ensures that all the transversals of $S_1, \ldots, S_k$ are legal inputs for $G$. We will use this property to re-label the nodes of $G$ so that all the test are *positive* clauses, i.e. clauses without negated literals. The idea of this transformation is similar to that used by Buss [8] in case of the pigeonhole principle. For a point $i$, let $S(i) = S \setminus \{i\}$ where $S$ is the (unique) block containing this point $i$. Replace every clause $C$ of $G$ by the clause $C^+$ which is obtained from $C$ by replacing each negated literal $\neg x_i$ by the set of positive literals $\{x_j : j \in S(i)\}$. Since for any transversal $B$ we have that $i \in B \iff B \cap S(i) = \emptyset$, it follows that $C^+(B) = C(B)$, and hence, the resulting graph $G^+$ still solves the edge-search problem for $\mathcal{F}$, restricted to transversals.

The graph $G^+$ has at most $\ell = |G|$ clauses. Let $r$ be the smallest number for which

$$\ell < \left(\frac{k}{k-t}\right)^{r/b} \tag{5}$$

By Lemma 1, there is a partial transversal $T$ such that $|T| \leq t+1$ and every clause in $G^+$, with $\geq r$ variables, has at least one variable $x_i$ with $i \in T$. Assign now constant 1 to all the variables $x_i$ with $i \in T$. This kills (i.e. evaluates to 1) all clauses with $r$ or more variables, and hence, the resulting graph $G'$ can have only clauses, with less than $r$ variables each.

Since every leaf of $G$ corresponds to an edge of $\mathcal{F}$ and each point belongs to no more than $d$ edges of $\mathcal{F}$, at least $|\mathcal{F}| - dt$ of the leaves survive the restriction. These leaves correspond to exactly those edges of $\mathcal{F}$, that do not intersect $T$. Thus, $G'$ solves the edge-search problem for $\mathcal{F}$, restricted to transversals $B$ such that $B \supseteq T$. If $C = \bigvee_{i \in A} x_i$ is a clause in $G'$ then $A \cap T = \emptyset$ (since $C$ survived the restriction $T \mapsto 1$). We can therefore define the weight of $C$ as the weight $w_T(A)$ of the corresponding set of points $A$. This way, each leaf of $G'$ gets weight 1. On the other hand, the root must have weight larger than $\min\{|\mathcal{F}| - dt, k-t\}$, since we have at least $|\mathcal{F}| - dt$ leaves, for any $k-t$ of them we can find a transversal $B \supseteq T$ such that $B \setminus T$ intersects all of them (recall that $|B| = k$ and $|T| = t$). Since (by soundness) the weight of every clause is at most the sum of the weights of the (at most $l$) clauses from which it is derived, we can find a clause $C$ such that $s \leq w(C) \leq ls$, as long as $ls$ does not exceed the weight of the root, which is ensured by (1). By Lemma 2 this clause has at least

$$M = \frac{s(k-t-ls+1)^2}{k + \lambda(s-1)}$$

variables. Since $G'$ does not have clauses with more than $r-1$ variables, $M$ must be strictly smaller than $r$. Since $r$ was minimal for which (5) holds, we have

$$|G| = \ell \geq \left(\frac{k}{k-t}\right)^{M/b}, \tag{6}$$

which is $\geq 2^{M/b}$ since $t \geq k/2$, as desired. This completes the proof of Theorem 1. ▯

# 4. Concluding remarks

The input size of an edge-search problem for a hypergraph $\mathcal{F}$ is the number $|\mathcal{F}|$ of edges. It is interesting to compare the lower bounds which we obtain for searching problems, resulting from the generalized pigeonhole principle and from the line search problem in finite geometries. By Theorem 1, the general lower bound is exponential in $\Omega(k^2/b)$ if $\mathcal{F}$ is $k$-partite with block size $b$. Thus, in case of $PHP_k^b$, the bound is $\exp(k^2/|\mathcal{F}|)$, which is super-polynomial only if $|\mathcal{F}| = o(k^2/\log k)$, and it is still not known if it remains such for $|\mathcal{F}| \geq k^2$. (Recall that $k$ is the number of pigeons and $|\mathcal{F}| = b$ is the number of holes). In this sense, the lower bound for $\mathrm{AG}(2,q)$ is better: here we have $|\mathcal{F}| = k^2$ (with $k = q$) and the bound is $\exp\left(\sqrt{|\mathcal{F}|}\right)$. The reason, why our argument (as well as previous arguments, based on Haken's "bottlenecks counting" idea [13, 23, 9, 11]) does not work for $PHP_k^b$ with $b \geq k^2$, is that we *a priori* restrict our search domain to transversals only. This makes possible the transformation $G \mapsto G^+$ but binds our hands when trying to kill long clauses, since now our killing set $T$ must be (partial) transversal. Note that without this last restriction, we could replace the bound $\left(\frac{k}{k-t}\right)^{r/b}$ in Lemma 1 by $\left(\frac{n}{n-t}\right)^{r}$, which does not depend on the block size $b$ at all (!). The overall conclusion is that, in order to get lower bounds for $PHP_k^b$ with $b \geq k^2$, one should learn more on how to force large clauses which are not assumed be positive.

The approach based on 'effective interpolation theorems' is now one of most successful schemes for proving lower bounds in different proof systems (see [22] for a survey). The main idea is to reduce the original problem to that for (monotone) Boolean circuits or communication protocols, where large lower bounds are known. Although powerful, this approach fails in the situations where the corresponding problems (like all three examples in Section 2) *have* small circuits or small communication complexity. In such situations we need some direct 'combinatorial' lower bounds argument. Theorem 1 gives such an argument for clause–based semantic derivations. Next logical step could be to understand the combinatorics of cutting planes proofs. All the known superpolynomial lower bounds for the length of such proofs follow from the corresponding lower bounds on the size of monotone Boolean [20, 1] and monotone real circuits [14, 19, 16] via appropriate interpolation theorems [21, 4, 17, 19]. Thus, known bounds capture the weakness of corresponding circuits rather than the weakness of cutting planes themselves. To get more insight in their structure, it would be interesting to understand the cutting plane complexity of blocking principles for finite geometries. These geometries have more structure then the pigeonhole principle, and the corresponding principles have very natural formulation in terms of linear inequalities. The Jamison-Brower-Schrijev's theorem [15, 5] for $\mathrm{AG}(2,q)$ is given by the system of $2n+1$

inequalities:

$$\begin{aligned}&\sum_{i\in L_j} x_i \geq 1, \qquad j=1,\dots,n\\&\sum_{i=1}^{n} x_i \leq 2(q-1)\\&0\leq x_i\leq 1, \qquad i=1,\dots,n.\end{aligned}$$

Bruen's theorem [6] for PG$(2,q)$ also can be stated as a system of $3n+1$ inequalities:

$$\begin{aligned}&1\leq \sum_{i\in L_j} x_i \leq q-1, \qquad j=1,\dots,n\\&\sum_{i=1}^{n} x_i \leq q+\sqrt{q}\\&0\leq x_i\leq 1, \qquad i=1,\dots,n.\end{aligned}$$

What is the cutting plane complexity of these systems? The "quadratic counting" trick used in Bruen's proof makes plausible the conjecture that this system does *not* have a short cutting planes proof, unless we allow quadratic inequalities and/or multiplication of two inequalities. Both answers - a short cutting planes proof of Bruen's theorem or the absence of such proof - would be interesting.

# Acknowledgment

I would like to thank Alexander Razborov for turning my attention to resolution proofs and very interesting discussions.

# References

[1] N. Alon and R.B. Boppana, The monotone circuit complexity of boolean functions. *Combinatorica*, **7** (1987), 1–22.

[2] P. Beame and T. Pitassi, Simplified and improved resolution lower bounds. In: *Proc. of 37th FOCS'96* (to appear)

[3] A. Blokhuis, On the size of a blocking set in PG$(2,p)$, *Combinatorica* **14** (1994), 111–114.

[4] M. Bonet, T. Pitassi and R. Raz, Lower bounds for cutting planes with small coefficients. In: *Proc. 27th ACM STOC* (1995), 575–584.

[5] A.E. Brower and A. Schrijev, The blocking number of an affine space. *J. Comb. Theory (A)* **24** (1978), 251–253.

[6] A. A. Bruen, Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.* **76** (1970), 342-344.

[7] A. A. Bruen, Blocking sets in finite projective planes. *SIAM J. Appl. Math.* **21** (1971), 380–392.

[8] S. Buss, Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, **52** (1987), 916–927.

[9] S. Buss and G. Turán, Resolution proofs of generalized pigeonhole principles. *Theor. Comp. Sci.*, **62** (1988) 311–317.

[10] V. Chvátal and E. Szemerédi, Many hard examples for resolution. *J. ACM* **35** (4) (1988), 759–768.

[11] S. Cook and T. Pitassi, A feasibly constructive lower bound for resolution proofs. *Information Processing Letters* **34** (1990), 81–85.

[12] K. Corrádi, Problem at the Schweitzer competition. *Mat. Lapok*, 20 (1969), 159–162.

[13] A. Haken, The intractability of resolution. *Theor. Comp. Sci.,* **39** (1985), 297–308.

[14] A. Haken and S. Cook, An exponential lower bound for the size of monotone real circuits. Manuscript, 1995.

[15] R. Jamison, Covering finite fields with cosets of subspaces. *J. Comb. Theory (A)* **22** (1977), 253–266.

[16] S. Jukna, Finite limits and monotone computations over the reals. Submitted to *Combinatorica*, 1996.

[17] J. Krajíček, Interpolation theorems, lower bounds for proof systems and independency results for bounded arithmetic. *J. Symbolic Logic*, (to appear)

[18] L. Lovász, M. Noar, I. Newman and A. Wigderson, Search problems in the decision tree model. In: *Proc. of 32th FOCS*, (1991), 576–585. Journal version: *SIAM J. Discr. Math.,* **21** (1995).

[19] P. Pudlák, Lower bounds for resolution and cutting planes proofs and monotone computations. Submitted to *Journal of Symbolic Logic*, 1995.

[20] A.A. Razborov, Lower bounds on the monotone circuit complexity of some Boolean functions. *Soviet Mathem. Doklady*, **31** (1985), 354–357.

[21] A.A. Razborov, Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic. *Izvestia: Mathematics* **59**:1 (1995), 205–227.

[22] A.A. Razborov, Lower bounds for propositional proofs and independence results in bounded arithmetic. In: *Proc. of 23rd Int. Colloq. Automata, Languages and Programming, ICALP'96*, (Paderborn, Germany, 1996).

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