Lower bounds to the size of constant-depth propositional proofs

Jan Krajíček

Abstract

[1] LK is a natural modification of Gentzen sequent calculus for propositional logic with connectives $\neg$ and $\bigwedge, \bigvee$ (both of unbounded arity). Then for every $d \geq 0$ and $n \geq 2$, there is a set T_n^d of depth d sequents of total size $O(n^{3+d})$ which are refutable in LK by depth $d+1$ proof of size $\exp(O(log^2 n))$ but such that every depth d refutation must have the size at least $\exp(n^{\Omega(1)})$. The sets T_n^d express a weaker form of the pigeonhole principle.

It is a fundamental problem of mathematical logic and complexity theory whether there exists a proof system for propositional logic in which every tautology has a short proof, where the *length* (equivalently the *size*) of a proof is measured essentially by the total number of symbols in it and *short* means polynomial in the length of the tautology. Equivalently one can ask whether for every theory T there is another theory S (both first order and reasonably axiomatized, e.g. by schemes) having the property that if a statement does not have a short proof in T then there is a short verification of it in S.[2]

This problem is, with a general notion of a proof system, equivalent to a principal question of complexity theory, namely whether the class of predicates acceptable in non-deterministic polynomial time is closed under complementation, [8]. One can show that if there exists such an optimal proof system it can be formed by augmenting the usual text-book calculus (called a *Frege system* in the terminology of [8]) by the extension rule (allowing to abbreviate formulas by new propositional variables) and by an additional, polynomial time recognizable, set of tautologies as extra axioms. Equivalently, for such an optimal proof system one could take a fragment T of true arithmetic (finitely axiomatizable and Π_1^0, in fact) where for a proof of the tautology φ is a taken a T-proof of the arithmetization $Taut(\lceil\varphi\rceil)$ of "φ is a tautology", see [14] for more details.

[1] 1991 *Mathematical Subject Classification* . Primary 03F20;
Secondary 03F07,68Q15,68R99.
Key words and phrases :Lengths of proofs, propositional calculus, Frege systems, pigeonhole principle.

[2] This problem was mentioned in a similar form in *K. Gödel's* letter to *J. von Neumann* in 1956. One can restrict to T=predicate calculus.

A trivial method for verifying that a formula is tautology is to list all possible truth assignments to its atoms and check that none of them makes the formula false. The length of such a verification is exponential in the number of atoms. It appears however, that this is actually the most efficient algorithm known: there is no proof system for which a subexponential upper bound would be established.

For a few particular systems some *lower bounds* to the size of proofs are known. *Haken* [10] established exponential lower bound for the resolution system, preceeded by *Cejtin* [7] who showed a similar lower bound for regular resolution. *Ajtai* [1] then proved that there is no universal polynomial upper bound for proofs in a Frege system when the logical depth of all formulas in proofs is bounded by an independent constant. Analyzing that argument *Bellantoni, Pitassi* and *Urquhart* [4] extracted a specific superpolynomial lower bound to the length of such constant-depth Frege proofs. [3]

In this paper we establish exponential lower bounds for these systems and a superpolynomial speed-up between them, in the sense of the *Abstract.*[4]

1 The proof system LK

For technical reasons we shall work with a particular formulation of the sequent calculus but this inessential as all such systems (with cut rule) are equivalent and they are equivalent to any Frege system, meaning that their proofs mutually translate with only polynomial increase in size and linear in depth (hence a constant depth in one system is constant in the others as well), [8]. The system we shall use is a modification of Gentzen's calculus LK, cf. [22] or [23], and we shall use the name LK for our system too.

LK has atoms $x, y, \ldots$, constants $0, 1$, connectives: negation $\neg$, disjunction $\bigvee$ and conjunction $\bigwedge$ (both of unbounded arity), and some auxilliary symbols (commas, brackets). Formulas are defined inductively: constants, atoms and negated atoms are formulas, and if φ_i are formulas so are $\bigwedge_i \varphi_i$ and $\bigvee_i \varphi_i$. $\neg\varphi$ is an abbreviation of the formula formed from φ by interchanging $\bigwedge$ and $\bigvee$, 0 and 1, and atoms and their negations. *The logical depth* , or just *depth* , $dp(\varphi)$ of formula φ is the maximal nesting of $\bigwedge, \bigvee$ in it.[5] In particular, constants and

[3] Their bound is of the form $\exp(\Omega(\log n \cdot \log^{(O(1))} n))$, where $\log^{()}$ is the iterated logarithm and the number of iterations depends on the depth.

[4] Soon after results of this paper were obtained, *P. Pudlák, A. Woods* and myself [15] (and independently *P. Beame, R. Impagliazzo* and *T. Pitassi* [3]) improved bounds for tautologies considered in [1] and [4] to an exponential one.

[5] There are two other reasonable definitions of the depth: the maximal number of alternations of $\bigwedge, \bigvee$ (considered e.g. in [6]) and a notion of the depth based on a hierarchy of constant-depth circuits in boolean complexity (cf.Section 3). The notion of $\Sigma - depth$ of a proof in Section 4 is based on this latter notion, and it seems to be relevant for present purposes, and also for its relation to the hierarchy of bounded arithmetic formulas. All propositions in this section are valid for either of these definitions.

atoms have depth 0 and the depths of φ and $\neg\varphi$ are equal. *The length* $|\varphi|$ of φ is the total number of occurences of constants, atoms and connectives in it.

Cedents $\Gamma, \Delta, \ldots$ are finite (possibly empty) sequences of formulas. A cedent is true if at least one its formula is true.

LK has the following seven inference rules: three structural rules (weakening, exchange and contraction), cut-rule, initial cedent rule (the following are initial cedents: $(1), (\neg x, x)$) and two introduction rules:

$$\bigvee : \ introduction \qquad \frac{\Gamma, \varphi}{\Gamma, \bigvee_i \varphi_i}, \quad provided\ \varphi\ is\ among\ \varphi_i,$$

$$\bigwedge : \ introduction : \qquad \frac{\Gamma, \varphi_1 \quad \Gamma, \varphi_2, \quad \ldots \quad \Gamma, \varphi_n}{\Gamma, \bigwedge_i \varphi_i}.$$

An LK-proof is *a sequence* of cedents, each either an initial one or derived from previous ones by one of the inference rules. A proof is *tree-like* if every cedent in it is a hypothesis of at most one inference.

The length of a proof is the sum of the lengths of all formulas in it, its depth is the maximum depth of a formula in it.

A proof is a proof of a formula φ if its end-cedent is the one element sequence (φ). A *refutation proof* of set T of cedents is a proof of the empty cedent $()$ in LK augmented by cedents from T as additional initial cedents (axioms).

Note that any unsatisfiable set of depth d cedents has a depth d refutation. (This is seen as follows: if $T = \{(A^i_1, \ldots, A^i_{k_i}) | 1 \leq i \leq n\}$ then any cedent $(\neg A^1_{j_1}, \ldots, \neg A^n_{j_n})$ is a tautology for any choice of $1 \leq j_i \leq k_i$ and thus has - by the cut-elimination - a depth d proof. These $k_1 \cdot k_2 \cdot \ldots k_n$ proofs can be combined by cuts with axioms from T to yield a proof of $()$.)

Also note that resolution refutations and depth 0 refutations are mutually translatable with only polynomial increase in the length.

Next two propositions clarify the relation between sequence-like and tree-like proofs.

Proposition 1.1 Let Π be a depth d proof of length $|\Pi|$. Then there is depth $d{+}1$ tree-like proof Π^* with the same end-cedent and with length $|\Pi^*| = O(|\Pi|^2)$. The same holds for refutations of sets of depth d cedents.

Proof: Let $\Pi = (\Gamma_1, \ldots, \Gamma_k)$, where the cedent Γ_l has the form $(\varphi^l_1, \ldots, \varphi^l_{n_l})$, and denote by $\neg\Gamma_l$ the cedent $(\neg\varphi^l_1, \ldots, \neg\varphi^l_{n_l})$ and by $\bigwedge \neg\Gamma_l$ (*resp.* $\bigvee \Gamma_l$) the conjunction $\bigwedge_{i=1}^{n_l} \neg\varphi^l_i$ (resp. the disjunction $\bigvee_{i=1}^{n_l} \varphi^l_i$).

Obviously for all $l \leq k$ either Γ_l is an initial cedent or there are $l_1 < l_2 < l$ such that one of the cedents: $(\bigvee \Gamma_l, \bigwedge \neg\Gamma_{l_2}, \bigwedge \neg\Gamma_{l_1})$ or $(\bigvee \Gamma_l, \bigwedge \neg\Gamma_{l_2})$, is valid (depending on by which rule Γ_l was inferred). Let Δ_l denote such a cedent. It is easy to see that each Δ_l has depth $d+1$, tree-like (and cut-free, in fact) proof of length $O\big(|\Gamma_l| + |\Gamma_{l_2}| + |\Gamma_{l_1}|\big)$.

By fewer than k cuts (and some contractions) we get from the Δ_l's the cedent $\Delta = (\bigvee \Gamma_k, \bigwedge \neg\Gamma_{u_1}, \ldots, \bigwedge \neg\Gamma_{u_r})$ where $\Gamma_{u_1}, \ldots, \Gamma_{u_r}$ are certain initial cedents.

This part of the constructed proof is also tree-like as in every step one cuts out $\bigwedge \neg\Gamma_v$ with maximal possible v, and every v is treated at most once. The length of this part is at most $k \cdot O(|\Pi|)$.

Clearly, Δ yields by several simple inferences of a total length $O(|\Delta|^2)$ cedent Γ_k. Hence the length of the constructed tree-like, depth $d+1$ proof Π^* is $|\Pi^*| = O(|\Pi|^2)$.

■

Proposition 1.2 Let Π^* be a tree-like, depth $d+1$ proof of a depth d cedent Γ. Then there is a depth d proof Π of Γ, not necessarily tree-like, of length $|\Pi| = O(|\Pi^*|^4)$. The same holds for refutations of a set of depth d cedents.

Proof-sketch: Write each cedent Δ in Π^* as $\Delta_0, \Delta_1, \Delta_2$ where Δ_0 is formed from depth d formulas, Δ_1 from depth d+1 conjunctions $\bigwedge_{i_1} A^1_{i_1}, \ldots, \bigwedge_{i_l} A^l_{i_l}$ and Δ_2 from depth d+1 disjunctions $\bigvee_{j_1} B^1_{j_1}, \ldots, \bigvee_{j_k} B^k_{j_k}$. By induction on the number of inferences above Δ show that the cedent $(\Delta_0, \ldots, B^1_{j_1}, \ldots, B^k_{j_k}, \ldots)$ has a depth d proof of length $O(S^2)$ from the cedents $(\ldots, \neg A^1_{i_1}, \ldots), \ldots, (\ldots, \neg A^l_{i_l}, \ldots)$, where S is the length of a subproof of Π^* yielding Δ. This is straightforward except for the estimate of the length, which is established by showing that the new proof has $O(S^2)$ cedents, each of length $O(S^2)$. For the former the assumption that Π^* is tree-like is needed, the latter is obvious as every formula in the new proof occurs already in the original subproof.

■

We end this section by a proposition analogous to the theorem of *Spira* [20] about the relation between the size and the depth of boolean formulas. A *special* $\bigwedge$: *introduction* is a derived rule of LK: from $(\psi_1, \ldots, \psi_r, \neg\eta)$ derive $(\psi_1, \ldots, \psi_r, \neg\psi_1 \wedge \ldots \wedge \neg\psi_r \wedge \neg\eta)$. A *path* through a proof is a sequence of cedents $(\Gamma_0, \ldots, \Gamma_u)$ such that Γ_o is the end-cedent, Γ_{i+1} is a hypothesis of a rule giving Γ_i and Γ_u is an axiom or an initial cedent.

Proposition 1.3 Let Π be tree-like, depth d refutation of T of length N. Then there are a set T_0 of tautological cedents and a tree-like, depth $d+1$ refutation Π' of $T \cup T_0$ of length $|\Pi'| = O(N^2)$ which uses special $\bigwedge$: *introduction* rule but does not use $\bigwedge$: *introduction*, and such that the maximum number h of cuts on any path through Π' satisfies: $h \leq 1 + 2\lceil \log_{3/2}(N) \rceil$.

Proof: The proof follows the argument of *Spira* [20]. Construct a refutation Π'' by replacing every $\bigwedge$: *introduction* with a principal formula $\bigwedge_i \varphi_i$ by repeated cuts with the cedent $(\neg\varphi_1, \ldots, \neg\varphi_n, \bigwedge_i \varphi_i)$, and let all these new cedents form the set T_0. Let H be the number of cuts in Π''. Clearly $H \leq |\Pi''| \leq N^2$. By induction on u prove

Claim: Let $(3/2)^{u-1} < H \leq (3/2)^u$. Then there exists Π' with $h \leq 1 + u$.

For the induction step, with $(3/2)^u < H \leq (3/2)^{u+1}$ note that we can find subproof Π_0 of Π'' ending with the cut-rule and two maximal subproofs Π_1, Π_2

such that $\frac{1}{2}(3/2)^u \leq H(\Pi_1) \leq (3/2)^u$ and also $H - H(\Pi_1) \leq (3/2)^u$; $H(\Pi_1)$ denotes the number of cuts in Π_1.

Let the end-cedent of Π_1 be $(\psi_1, \ldots, \psi_r, \eta)$ and that of $\Pi_2 : (\psi_1, \ldots, \psi_r, \neg\eta)$. Insert in $\Pi'' - \Pi_1$ a special $\bigwedge$: *introduction* after $(\psi_1, \ldots, \psi_r, \neg\eta)$ to infer $(\psi_1, \ldots, \psi_r, \neg\psi_1 \wedge \ldots \wedge \neg\psi_r \wedge \neg\eta)$, getting from $\Pi'' - \Pi_1$ a proof Π_3 of $(\neg\psi_1 \wedge \ldots \wedge \neg\psi_r \wedge \neg\eta)$. By the induction hypothesis applied to Π_1 and Π_3 we get two proofs of $\psi_1 \vee \ldots \vee \psi_r \vee \eta$ and $\neg\psi_1 \wedge \ldots \wedge \neg\psi_r \wedge \neg\eta$, both with a maximum of $1+u$ cuts on each path and of lengths $O(|\Pi_1|^2)$ and $O((|\Pi''|-|\Pi_1|)^2)$ respectively. Joining these two proofs by a cut yields the required proof Π'.

■

Note that one can easily get a refutation Π' with only one cut and of depth $d+2$.

2 The pigeonhole principle

Let D, R be two non-empty sets, where $R = \{1, \ldots, n\}$. Consider the set $\neg PHP(D, R)$ of cedents: $(\neg x_{ij}, \neg x_{ik})$, one for each $i \in D$ and $j \neq k \in R$, $(\neg x_{ik}, \neg x_{jk})$, one for each $i \neq j \in D$ and $k \in R$, and $(x_{i1}, \ldots, x_{in})$, one for each $i \in D$. Thinking about x_{ik} as saying $f(i) = k$, the cedents from $\neg PHP(D, R)$ assert that f is an injective function from D into R. Hence for $|D| > n$ the set $\neg PHP(D, R)$ is refutable.

The argument from *Haken* [10] was generalized by *Buss* and *Turán* to yield the following lower bound which we restate for our system (*Haken* had $m = n + 1$).

Proposition 2.1 (*S. Buss - G. Turán* [6])

Let $|D| = m > n$. Then every depth 0 refutation of $\neg PHP(D, R)$ must have length at least $\exp\left(\Omega\left(\frac{n^2}{m}\right)\right)$.

■

Note that for $m = n^{1+\varepsilon}, 0 < \varepsilon < 1$, this bound is of the form $\exp(n^{\Omega(1)})$. For this case we also have an upper bound.

Proposition 2.2

Let $|D| = n^{1+\varepsilon}$ for $0 < \varepsilon < 1$. Then there is a refutation of $\neg PHP(D, R)$ of length $\exp(O(\log^2 n))$ in which every formula is either a conjunction of size $O(\log n)$ or a disjunction of size $O(\log n)$.

Proof-sketch: *J. Paris, A. Wilkie,* and *A. Woods* [17] showed that $I\Delta_0(f) + \Omega_1$ proves that f cannot be an injection of $n^{1+\varepsilon}$ into n. Their proof can be used (employing also a conservation result of [5]) to prove in the bounded arithmetic fragment $T_2^2(\alpha)$ that α cannot be a graph of an injection of $n^{1+\varepsilon}$ into n. Moreover, all quantifiers in such a proof are bounded by $\exp(O(\log^2 n))$, cf. [13].

For any fixed n, a propositional translation (translating bounded quantifiers by conjuctions and disjunctions and $\alpha(i,j)$ by p_{ij}, see [16]) yields a depth 3, tree-like refutation of $\neg PHP(D,R)$ of length $\exp(O(\log^2 n))$ in which all depth 1 subformulas have size at most $O(\log n)$ and, in addition, the number of formulas in any cedent of the refutation is bounded by a constant independent of n.

Using this additional information it is straightforward to show that if a subproof Π of the refutation ends with the cedent

$$(\bigwedge_{i_1} A^1_{i_1}, \ldots, \bigwedge_{i_l} A^l_{i_l}, \bigvee_{j_1} B^1_{j_1}, \ldots, \bigvee_{j_k} B^k_{j_k}, \Delta)$$

where the formulas $\bigwedge_{i_1} A^1_{i_1}, \ldots, \bigwedge_{i_l} A^l_{i_l}, \bigvee_{j_1} B^1_{j_1}, \ldots, \bigvee_{j_k} B^k_{j_k}$ are of depth 3 and the formulas in Δ are of depth at most 2, then for any choice of $i_1, \ldots, i_l$ the cedent $(A^1_{i_1}, \ldots, A^l_{i_l}, B^1_1, \ldots, B^1_{j_1}, \ldots, B^k_1, \ldots, B^k_{j_k}, \Delta)$ has a depth 2, tree-like proof $\Pi_{i_1,\ldots,i_l}$ whose total size $\Sigma_{i_1,\ldots,i_l} |\Pi_{i_1,\ldots,i_l}|$ is at most $\exp(O(\log^2 n))$. Hence there is also a depth 2, tree-like refutation of $\neg PHP(D,R)$ in which all depth 1 subformulas are of size $O(\log n)$.

Applying to this refutation (the proof of) Proposition 1.2 yields a refutation with the required properties.

■

3 Random partial truth evaluations

In the lower bound proof we will apply a boolean complexity technique developed for the construction of an oracle separating levels of the polynomial time hierarchy, see [18, 25] and [11]. This section introduces the method and recalls relevant combinatorial results, all due essentially to *J. Hastad* [11].

A formula φ is $\sum_d^{S,t}$, $d \geq 0$, if it is equivalent to a formula ψ having the properties:
(a) $dp(\psi) \leq d+1$,
(b) if $dp(\psi) = d+1$ then the outmost connective of ψ is $\bigvee$,
(c) ψ has $\leq S$ subformulas of depth ≥ 2 and
(d) all depth 1 subformulas are (conjunctions or disjunctions) of arity at most t.

A formula is $\Pi_d^{S,t}$ iff its negation is $\sum_d^{S,t}$.

A formula φ is Δ_1^t if both φ and $\neg\varphi$ are expressible as disjunctions of conjunctions of arity at most t. For $d, n \geq 1$ arbitrary and any atom $x_{ij} (i \in D, j \in R)$ let $f_{ij}^{d,n}$ be depth d formula in n^d new atoms $x_{ij}^{i_1,\ldots,i_d}$:

$$f_{i,j}^{d,n} := \bigwedge_{i_1 < n} \ \bigvee_{i_2 < n} \ldots Q_{i_d < n} \ x_{ij}^{i_1,\ldots,i_d},$$

where Q is $\bigwedge$ iff d is odd. For $d = 0$, let $f_{i,j}^{d,n}$ be just x_{ij}.

For a formula φ with atoms $y_1, y_2, \ldots, y_k$ and a map $\varrho : \{y_1, \ldots, y_k\} \to \{0, 1, z_1, \ldots, z_v\}$, $\varphi|\varrho$ denotes the formula φ with y_i replaced by $\varrho(y_i)$. All atoms in $\varphi|\varrho$ are among $z_1, \ldots, z_v$.

In next section we will make essential use of the following proposition.

Proposition 3.1 Let $d \geq 1, n$ be sufficiently large and $|D| \leq n^2, |R| = n$. Let V be the set of all variables occuring in one of $f_{i,j}^{d,n}$, *let* $\varphi_1, \ldots, \varphi_u$ be some $\Sigma_d^{N,logN}$ or $\Pi_d^{N,logN}$ formulas with variables from V of total length $\sum_{i=1}^{u} |\varphi_i| \leq N$, and let $U_1, \ldots, U_r \subseteq D \times R$ be arbitrary sets with $r \leq n^c$, where c is any fixed constant (independent of n). Assuming $N \leq \exp(n^{1/3})$ the following holds:

there exists map $\varrho : V \to \{0, 1\} \cup \{x_{ij} | i \in D, j \in R\}$ such that:

- (i) all formulas $\varphi_1|\varrho, \ldots, \varphi_n|\varrho$ are $\Delta_1^{\log N}$
- (ii) every $f_{i,j}^{d,n}|\varrho, i \in D$ and $j \in R$, is equivalent to either 0 or x_{ij},
- (iii) for every $U_s, 1 \leq s \leq r$, for at least $|U_s| \cdot n^{-1/2}$ pairs $(i, j) \in U_s$ the formula $f_{i,j}^{d,n}|\varrho$ is equivalent to x_{ij}.

Proof-sketch: The proposition is a combination of *Hastad's* two "switching lemmas" (4 and 8 of Section 5 of [11]) with minor modifications. We give here enough details to explain these two lemmas and we infer the proposition from them. The reader should consult [11] for details.

- (1) For fixed $x_{ij}, (B_u)_u$ is a partitioning of the variables occuring in $f_{i,j}^{d,n}$ into n^{d-1} classes B_u of the form $\{x_{ij}^{i_1,\ldots,i_{d-1},t} | t < n\}$, one for each choice of $i_1, \ldots, i_{d-1} < n$.
- (2) For $0 < p < 1$, $R_+^{d,n}(p, x_{ij})$ is a probability space of random restrictions ϱ of atoms of $f_{i,j}^{d,n}$, i.e. partial maps with values $0, 1$, determined by the process:
  (a) to each class B_u assign independently a value s_u with: $Prob[s_u = *] = p$ and $Prob[s_u = 0] = 1 - p$.
  (b) To each variable $y \in B_u$ assign independently a value $\varrho(y)$ with: $Prob[\varrho(y) = s_u] = p$ and $Prob[\varrho(y) = 1] = 1 - p$.
  The space $R_+^{d,n}(p)$ is formed of restrictions defined on all variables from V which are disjoint independent unions of restrictions from spaces $R_+^{d,n}(p, x_{ij}), i \in D$ and $j \in R$. The space $R_-^{d,n}(p)$ is defined analogically exchanging roles of 0 and 1 in (a) and (b) above.
- (3) For $\varrho \in R_+^{d,n}(p)$, the map $g(\varrho)$ is defined by:
  (a) $g(\varrho)(x_{ij}^{i_1,\ldots,i_{d-1},t}) = x_{ij}^{i_1,\ldots,i_{d-1}}$, provided for no $s < t$ is

$\varrho(x_{ij}^{i_1,\ldots,i_{d-1},s}) = *$,

(b) $g(\varrho)(x_{ij}^{i_1,\ldots,i_{d-1},t}) = 1$, otherwise.

For $\varrho \in R_-^{d,n}(p)$, $g(\varrho)$ is defined identically using 0 instead of 1 in (b).

- (4) **Lemma** (cf. 4, Sect.5, [11]) Let φ be a $\Sigma_d^{S,t}$ or a $\Pi_d^{S,t}$-formula with atoms from V and suppose $0 < p < 1$. Let ϱ_{d-k} be choosen independently and at random from $R_+^{d-k,n}(p)$ or $R_-^{d-k,n}(p)$, for $k = 0, \ldots, d-1$. Then with probability at least $1 - S(6pt)^t$ the restricted formula $\varphi|\varrho_d|g(\varrho_d)|\varrho_{d-1}|g(\varrho_{d-1})\ldots|\varrho_1|g(\varrho_1)$ is in Δ_1^t.

  ■

- (5) A lemma like the one above can be proved for simpler probability spaces, see [11], but the importance of this version is that we have a more control of how restricted the formulas $f_{i,j}^{d,n}$ are.

  Lemma (cf. 8, Sect. 5, [11]). Let $p = (2lm^{-1}\log(m))^{1/2}$ (where l is large enough w.r.t. d and c) and let ϱ_{d-k} be chosen at random from $R_+^{d-k,n}(p)$, if $d-k$ is odd or from $R_-^{d-k,n}(p)$ if $d-k$ is even, $k = 0, \ldots, d-1$. Then with probability at least 1/2 none of $f_{i,j}^{d,n}$ collapses by $\varrho_d|g(\varrho_d)|\ldots|\varrho_1|g(\varrho_1)$ to 1 and for every U_s for at least $|U_s|n^{-1/2}$ pairs $(i,j) \in U_s$ $f_{i,j}^{d,n}$ is equivalent to x_{ij}.

  ■

  Comment: By Lemma 8 of Section 5 of [11], slightly modified by adding a parameter l into p, each $f_{i,j}^{d-k,n}|\varrho_{d-k}|g(\varrho_{d-k})$ contains $f_{i,j}^{d-k-1,n}$ with probability at least $1 - (\frac{1}{3})n^{-l+d-k+1}$. Hence with probability at least $1 - n^{-l+d+5}$ this happens for all of at most n^3 formulas $f_{i,j}^{d,n}, i \in D$ and $j \in R$, and all $k = 0, \ldots, d-1$.

  With probability at least $1 - (\frac{1}{6})n^{-l+3}$ all $f_{i,j}^{1,n}$ collapse by $|\varrho_1|g(\varrho_1)$ to either x_{ij} or 0 (this is directly computed).

  Finally, the expected number of $f_{i,j}^{1,n}$ collapsing to $x_{i,j}$ and not to 0 for $(i,j) \in U_s$ is at least $(\log(n) \cdot n^{-1})^{1/2} \cdot |U_s|$ and one can get at least $n^{-1/2}|U_s|$ of such (i,j) with arbitrarily high probability ($\geq 1 - n^{-c-1}$) by the well-known estimate to the tail of the binomial distribution. Hence this holds for all $U_1, \ldots, U_r$ with probability at least $1 - \frac{1}{n}$.

  Combining all these probabilities together, with $l > d+5$, gives the lemma. The reader may consult [12] where a similar computation is done in detail.

- (6) Now having lemmas of (4) and (5), we see that a random $|\varrho_d|g(\varrho_d)|\ldots|\varrho_1|g(\varrho_1)$ will have the property required in the propostion as long as $N(6pt)^t = N(6(2ln^{-1}\log n)^{1/2}\log N)^{\log N} < \frac{1}{2}$. This inequality is true whenever e.g. $N \leq \exp(n^{1/3})$, for n sufficiently large.

■

4 The lower bound

Now we are ready to prove the lower bound, the main result of this paper. The $\Sigma - depth$ of a proof Π of length $N = |\Pi|$ is the minimal d such that every formula in Π is either $\Sigma_d^{N,logN}$ or $\Pi_d^{N,logN}$.

Theorem Let $d \geq 0$ and $\varepsilon > 0$ be arbitrary and let $|D| = n^{1+\varepsilon}$ and $|R| = n$. Let $\neg PHP(D,R)(f_{i,j}^{d,n})$ denote the set $\neg PHP(D,R)$ with formulae $f_{i,j}^{d,n}$ substituted for variables x_{ij}. Then for sufficiently large n the following two conditions hold:

- (i) every Σ-depth d, tree-like refutation of $\neg PHP(D,R)(f_{i,j}^{d,n})$ must have length at least $\exp(n^{1/5})$,
- (ii) there are Σ-depth d, sequence-like and Σ-depth $d+1$, tree-like refutations of $\neg PHP(D,R)(f_{i,j}^{d,n})$ of length at most $\exp(O(\log^2 n))$.

■

Corollary For any $d \geq 0$ there is a superpolynomial speed-up (m versus $\exp(\exp(\Omega(\log^{1/2} m)))$) between sequence-like and tree-like Σ-depth d refutations of sets of depth d cedents.

■

Proof of the theorem: The proof will occupy the rest of this section. Fix $d \geq 0, n \geq 1$ and $\varepsilon > 0$. Consider the following modification of the pigeonhole principle. Let D, R be as stated in the assumptions and let $r : D \rightarrow P(R)$ be a function assigning to each $i \in D$ a subset $r(i)$ of R such that:

- (a) $|r(i)| \geq n^{1/2}$, for all $i \in D$,
- (b) $|\{i | j \in r(i)\}| \geq n^{1/2+\varepsilon}$, for all $j \in R$.

Then *modified* PHP, $\neg MPHP(D,R,r)$, is the set of cedents of $\neg PHP(D,R)$ in which we replace the variables x_{ik} for which $k \notin r(i)$ by 0.

That is, $\neg MPHP(D,R,r)$ is:

$$(\neg x_{ij}, \neg x_{ik}),\ \ for\ i \in D\ and\ j \neq k \in r(i),$$

$$(\neg x_{ik}, \neg x_{jk}),\ \ for\ i \neq j \in D\ and\ k \in r(i) \cap r(j),$$

$$(x_{ij_1}, \ldots, x_{ij_r}),\ \ for\ i \in D\ and\ r(i) = \{j_1, \ldots, j_r\}.$$

Part (i) of the theorem follows from two claims:

Claim 1 (depth reduction): Let $d \geq 1$ and n be sufficiently large, and assume Π is a Σ-depth d, tree-like refutation of $\neg PHP(D,R)(f^{d,n}_{i,j})$ with length $|\Pi| = N \leq \exp(n^{1/3})$. Then there exists a function $r : D \to P(R)$ satisfying conditions (a) and (b) above, and a tree-like refutation Π_0 of $\neg MPHP(D,R,r)$ of length $|\Pi_0| \leq N + n^{O(d)}$ in which every formula is $\Delta_1^{\log N}$.

Claim 2 (base case): For n sufficiently large and any $r : D \to P(R)$ satisfying (a) and (b), every tree-like refutation Π_0 of $\neg MPHP(D,R,r)$ in which every formula is $\Delta_1^{\log(|\Pi_0|)}$ must have the length at least $|\Pi_0| \geq \exp(n^{1/4}/2)$.

Proof of Claim 1: Let $d \geq 1$ and Π satisfy the hypothesis of the claim. Let $\varphi_1, \ldots, \varphi_u$ list all formulas of Π (so $\sum_{i=1}^{u} |\varphi_i| \leq |\Pi| \leq N$) and $U_1, \ldots, U_r$ list all $n + n^{1+\varepsilon}$ subsets of $D \times R$ of the form either $\{i\} \times R$ or $D \times \{j\}$, $i \in D$ and $j \in R$.

By Proposition 3.1 there is a map ϱ assigning to the variables occuring in $f^{d,n}_{i,j}$ either $0, 1$ or x_{ij} s.t.

- (i) all $\varphi_1|\varrho, \ldots, \varphi_u|\varrho$ are $\Delta_1^{\log N}$,
- (ii) $f^{d,n}_{i,j}|\varrho$ is equivalent to either 0 or x_{ij}, and
- (iii) $|\{(i,j) \in U_s | f^{d,n}_{i,j}|\varrho \not\equiv 0\} \geq n^{-1/2}|U_s|$.

Define the map r: $j \in r(i)$ iff $f^{d,n}_{i,j}|\varrho \not\equiv 0$. Then r satisfies conditions (a) and (b) above by (ii) and (iii). Clearly $\Pi|\varrho$ (that is Π with all φ_i replaced by $\varphi_i|\varrho$) is a refutation of $(\neg PHP(D,R)(f^{d,n}_{i,j}))|\varrho$.

Finally observe that from the axioms of $\neg MPHP(D,R,r)$ follow all axioms $(\neg PHP(D,R)(f^{d,n}_{i,j}))|\varrho$ by a proof of size $n^{O(d)}$ in which every formula is a subformula of $(\neg PHP(D,R)(f^{d,n}_{i,j}))|\varrho$, i.e. $\Delta_1^{\log N}$. This is because each $f^{d,n}_{i,j}|\varrho$ can be proved to be equivalent to either x_{ij} or 0 depending on whether $j \in r(i)$ or $j \notin r(i)$. q.e.d. (Claim 1)

Proof of Claim 2: Let Π_o be a tree-like refutation of $\neg MPHP(D,R,r)$ in which every formula is Δ_1^t for $t = log(S)$, $S = |\Pi_o|$. By an obvious analogy to Proposition 1.3 for Σ-depth there is set T_0 of tautological cedents and a tree-like refutation Π_1 of $T_0 \cup \neg MPHP(D,R,r)$ of length $|\Pi| \leq S^2$ using special $\bigwedge :$ *introduction* instead of the ordinary one, and such that on every path through Π_1 there is at most $1 + 2log_{3/2}(S) \leq 4t$ cuts, and all formulas in Π_1 are either $\Sigma_1^{S,t}$ or $\Pi_1^{S,t}$.

Pair (α^+, α^-) of disjoint subsets of $D \times R$ determines a partial truth evaluation α of atoms x_{ij} : α assigns 1 to those x_{ij} with $(i,j) \in \alpha^+$, and 0 to those with $(i,j) \notin \alpha^-$. The evaluation α is total if (α^+, α^-) is a partition of $D \times R$. We say that α extends β if $\alpha^+ \supseteq \beta^+$ and $\alpha^- \supseteq \beta^-$. For total α there is a unique path $(\Gamma_o, \ldots, \Gamma_u)$ in Π_1 such that all Γ_i receive value 0 by α. As the cedents in

T_0 are tautological, Γ_u must be an axiom from $\neg MPHP(D,R,r)$. We say that α *determines* this path $(\Gamma_o,\ldots,\Gamma_u)$.

Call those partial evaluations β for which β^+ is a graph of a partial $1-1$ function from D into R and such that $(i,j)\in\beta^+$ implies $j\in r(i)$ *good* .

We claim that there is a good partial evaluation β such that $|\beta^+\cup\beta^-|\le 4t^2$ and such that all good total evaluations extending β determine the same path. To show this we construct by induction on l good partial evaluations β_l and a partial path $(\Gamma_o,\ldots,\Gamma_{u_l})$ such that:

- (i) $|\beta_l^+\cup\beta_l^-|\le t\cdot l$,
- (ii) $(\Gamma_o,\ldots,\Gamma_{u_l})$ contains at least l cuts,
- (iii) $(\Gamma_o,\ldots,\Gamma_{u_l})$ is an initial part of any path determined by any good total evaluation extending β_l.

Note that in Π_1 all rules are unary except the cut-rule. Put $\beta_0:=(\emptyset,\emptyset)$ and let $(\Gamma_o,\ldots,\Gamma_{u_{l_0}})$ be the unique maximal path on which all inferences are only unary. Assume we have β_l and $(\Gamma_o,\ldots,\Gamma_{u_l})$ and that Γ_{u_l} is the lower cedent of a cut rule with cut formula ϕ, and w.l.o.g. assume ϕ is $\Sigma_1^{S,t}$. Consider two cases: (a) there is a total good evaluation α extending β_l which makes ϕ true, (b) there is no such evaluation. In Case (a) , as ϕ is $\Sigma_1^{S,t}$, we can find a good extension β_{l+1} of β_l , β_{l+1} included in α, such that $|(\beta_{l+1}^+\cup\beta_{l+1}^-)\setminus(\beta_l^+\cup\beta_l^-)|\le t$ and such that any total good extension of β_{l+1} makes ϕ true. In this case let $(\Gamma_o,\ldots,\Gamma_{u_{l+1}})$ be a prolongation of $(\Gamma_o,\ldots,\Gamma_{u_l})$ containing the upper cedent of the rule in which $\neg\phi$ occurs. In Case (b) put $\beta_{l+1}:=\beta_l$ and let $(\Gamma_o,\ldots,\Gamma_{u_{l+1}})$ be a prolongation of $(\Gamma_o,\ldots,\Gamma_{u_l})$ containing the upper cedent in which ϕ occurs.

Since on every path through Π_1 there are at most $4t$ cuts, for some $l_o\le 4t$ $(\Gamma_o,\ldots,\Gamma_{u_{l_0}})$ is a complete path. Put $\beta:=\beta_{l_0}$.

Let Γ be the unique axiom of $\neg MPHP(D,R,r)$ occuring in the path determined by β. As β is good this axiom must be of the form $(x_{i,j_1},\ldots,x_{i,j_r})$ for $r\ge n^{1/2}$. We want to show that $4t^2\ge r$. Assume otherwise and let x_{ij} be an atom from Γ such that $(\beta^+\cup\{(i,j)\},\beta^-)$ is good. Such x_{ij} must exist as β gives values to at most $4t^2$ atoms. Define a good total evaluation α by $\alpha^+:=\beta^+\cup\{(i,j)\}$. By the construction this α determines the same path as β but makes Γ true. This is a contradiction, hence $4t^2\ge r\ge n^{1/2}$ which entails $|\Pi_0|\ge exp(n^{1/4}/2)$. q.e.d. (Claim 2)

As part (ii) of the theorem follows from the observation that, substituting $f_{i,j}^{d,n}$ for x_{ij} in the proof guaranteed by Proposition 2.2, gives a Σ-depth d refutation of size $exp(O(log^2 n))$, the theorem is proved. ■

The following appears to be an open problem.

Open problem:[6] Is there $c\ge 0$ such that for every $d\ge c$ there is a sequence of

[6] In [3] and [15], for any $d\ge 0$ and any n sufficiently large, a lower bound $\exp(n^{\Omega(1)})$ to the size of depth d refutations of $\neg PHP(D,R)$ is proved , where $|D|=n+1, |R|=n$. I don't

sets $(T_n^d)_n$ of depth $\leq c$ cedents of total length $n^{O(1)}$ satisfying (i) and (ii) of the theorem, that is: (i) any Σ-depth d, tree-like refutation of T_n^d must have the size $\exp(n^{\Omega(1)})$, and (ii) T_n^d have much shorter Σ-depth, tree-like $d+1$ refutations? I expect that the answer is affirmative with $c = 0$.

5 Connections to bounded arithmetic

In this final section I shall discuss two topics inspired by a relation of propositional logic to bounded arithmetic. I do not enter into the details of bounded arithmetic so parts might be intelligible only to readers familiar with that subject.

That the study of constant-depth proofs is relevant to bounded arithmetic is shown by a result of *Paris* and *Wilkie* [16]. They observed that propositional translations (obtained analogously to $\neg PHP(D, R)$ in Section 2) of a combinatorial principle, which can be formulated by a first order formula over finite structures (or as arithmetic Δ_0 formula) and which is provable in bounded arithmetic, have constant depth proofs of polynomial length (in the size of the structure). In particular, a superpolynomial lower bound to the length of such proofs implies unprovability of the principle in bounded arithmetic. [7]

Many important open problems in bounded arithmetic deal with counting, see [16, 2]. While the questions from [16] about explicit counting in the hierarchy of bounded predicates were to a large extent answered in [24] (assuming that the polynomial time hierarchy does not collapse), questions about the relations between various simple principles of counting (such the pigeonhole principle and the parity principle considered in [2]) remain open. Let me give an example of such a problem formulated for propositional logic. Let $p, n \geq 1$ and let $x_{ij}, 1 \leq i, j \leq n$ be n^2 atoms. For any $m \geq 1$ and any m^2 formulas $\varphi_{uv}, 1 \leq u, v \leq m$, with atoms x_{ij} let the formula $\Phi_p[(\varphi_{uv})|m]$ say that the relation $\{(u, v)|\varphi_{uv}\ is\ true\}$ is not a partition of $\{1, \ldots, m\}$ into p-element classes. The problem is: Is there d and k such that, for and odd n, the formula $\Phi_2[x_{ij}|n]$ has a depth d proof of the length at most n^k from some formulas of the form $\Phi_3[\varphi_{uv}|m], m \not\equiv 0(3)$?

A corresponding problem in boolean complexity, namely whether there are constant-depth, polynomial size formulas with MOD_3 gates computing MOD_2 (i.e. parity) was answered in the negative, see [19]. The difficulty of the problem from our example lies in the fact that one does not deal with counting directly but rather with its properties. A standard vehicle how to move from properties of a relation or a function to its explicit definition is *Beth's* definability theorem or, equivalently, *Craig's* interpolation theorem, and we would need a version of

see how to combine the techniques of those proofs and this paper to answer the problem.

[7] If bounded arithmetic is augmented by the function $f(x)$ one needs a lower bound majorizing any fixed iteration of f on n.

it with strong upper bounds to the depth and to the length of an interpolant of an implication in terms of the depth and the length of a proof of the implication to be able to reduce problems like the one above to complexity theory. Unfortunately, such effective interpolation is valid only for cut-free LK-proofs. The following statement is obtained by modifying *Craig's* original argument, see [9].

Proposition 5.1 Assume Π is a tree-like, cut-free proof of the cedent $(\Gamma(\bar{x},\bar{y}),\Delta(\bar{x},\bar{z}))$. Then there is a formula $I(\bar{x})$ such that both cedents (Γ, I) and $(\neg I, \Delta)$ are valid, and which satisfies: (i)$|I| \leq |\Pi|$, (ii) $dp(I) \leq 1 + 2min(dp(\Gamma), dp(\Delta))$.

Proof-sketch: Let $\Omega = (\Omega_0(\bar{x},\bar{y}),\Omega_1(\bar{x},\bar{z}))$ be a cedent in Π where $\Omega_0 = (A_1,\ldots,A_k)$ and $\Omega_1 = (B_1,\ldots,B_l)$ are ancestors of Γ resp. of Δ. By induction on the number of inferences above Ω show that there are formulas $U_i^j, 1 \leq i \leq k, 1 \leq j \leq k_i$, and $V_r^s, 1 \leq r \leq l, 1 \leq s \leq l_r$, in which only the variables $\bar{x}$ appear and which satisfy:

- (a) the cedent $(\ldots,\neg U_i^j,\ldots,V_r^s,\ldots)$ is valid,
- (b) the cedents (Ω_0, U_i^j) and $(\neg V_r^s, \Omega_1)$ are valid for all i,j,r,s,
- (c) $dp(U_i^j) \leq 2dp(A_i)$ and $dp(V_r^s) \leq 2dp(B_r)$ for all i,j,r,s,
- (d) $\sum_{1\leq j\leq k_i} |U_i^j| \leq an(A_i)$ and $\sum_{1\leq s\leq l_r} |V_r^s| \leq an(B_r)$ where $an(C)$ denotes the sum of the lengths of all ancestors of C (including C).

Note that both $\bigwedge_{i,j} U_i^j$ and $\bigvee_{r,s} V_r^s$ are interpolants for (Ω_0,Ω_1).

■

To see that a similar statement does not hold for proofs with cuts, even of constant depth, note that any boolean function $f(x_1,\ldots,x_n)$ computable by a circuit C of size m is also computed by any interpolant to a particular depth 4 and length $O(n+m)$ implication having depth 4 and length $O((n+m)^2)$ proof: to every gate in C assign variable y_i and let formula (of depth 4) $\phi(\bar{x},y_1,\ldots,y_m)$ be a conjuction of local conditions how C computes, i.e. of the conditions of the form $y_i = x_j, y_i = \neg y_j, y_i = y_j \wedge y_k$, and $y_i = y_j \vee y_k$ saying that the gate y_i is computed as the input x_i, the negation of y_j, the conjuction of y_j and y_k, or the disjunction of y_j and y_k, respectively. Obviously for any k the cedent $(\neg\phi(\bar{x},\bar{y}),\neg y_k,\neg\phi(\bar{x},\bar{z}),z_k)$ is valid and it is not difficult to see that it has actually a depth 4 proof of length $O((n+m)^2)$; construct the proofs in the order in which C computes the gates. But any interpolant to such a cedent computes y_k, so interpolants for k_0 corresponding to the output of C compute $f(\bar{x})$.

In particular, all functions computable by polynomial size circuits are also definable by interpolants of polynomial length implications with constant-depth polynomial length proofs.[8]

There is a close similarity between the proof of Claim 2 in Section 4 and the proof of the independence of the weak pigeonhole principle on $S_2^2(\alpha)$ from [13]; we shall consider this in a detail now. Let Π be a Σ-depth d (not necessarily tree-like) refutation of a set T of cedents, and let α be a truth evaluation of all atoms of T. As T is unsatisfiable there must be a cedent $\Gamma \in T$ which is given the value 0 by α. We can find such Γ by the following search in Π.

Construct a path $(\Gamma_1, \Gamma_2, \ldots, \Gamma_u)$ through Π such that all Γ_i are given the value 0 by α. Then, necessarily, $\Gamma_u \in T$. Finding Γ_{i+1}, given Γ_i is non-trivial only in the cases of the cut-rule and of $\bigwedge$:introduction (we avoided this case in Claim 2 by considering special $\bigwedge:$ *introduction* instead of the ordinary one). In the case of the cut-rule we ask an oracle whether α makes the cut-formula true or false and choose Γ_{i+1} to be the unique false hypothesis of the rule. In the case of $\bigwedge$:introduction with the principal formula $\bigwedge_{i \leq u} \varphi_i$ we will consider two algorithms:

- (a) either we can find false φ_i by binary search asking queries of the form $\bigwedge_{a \leq i \leq b} \varphi_i$,
- (b) or we simply request the oracle to give us some false φ_i.

Let $N = |\Pi|$, let H be the number of cuts in Π and let h resp. k be the maximum number of cuts resp. of $\bigwedge:$ *introductions* on a path. Then estimates to the complexity of the two algorithms are:

- (A) the algorithm using (a) asks at most $h + klog(N)$ queries about the validity of $\Sigma_d^{N,logN}$ formulas (from Π),
- (B) the algorithm using (b) asks at most h queries about $\Sigma_d^{N,logN}$ formulas and at most k special queries of type (b).

Let $\exists y \leq x\varphi(x,y)$ be a bounded $\Sigma_{d+1}^b(R)$ formula, $\varphi(x,y) = \forall z \leq x\varphi'(x,y,z)$ with $\varphi' \in \Sigma_{d-1}^b(R)$, and assume it is provable in $S_2^d(R)$ or $T_2^d(R)$. Then by analogy to Proposition 2.2 we have refutations of the sets

$$T_n^d = \{\neg\hat{\varphi}(n,0), \ldots, \neg\hat{\varphi}(n,n)\}, n = 0, 1, \ldots$$

(here $\neg\hat{\varphi}(n,u)$ denotes a cedent of propositional translations of $\neg\varphi'(n,u,v)$ for $v = 0, \ldots, n$), which are in both cases tree-like, Σ-depth d of the length $N = 2^{\log(n)^{O(1)}}$, but in case of $S_2^d(R)$ the refutation will have only $\log(n)^{O(1)}$ cuts

[8]Note that this observation together with Proposition 5.1 (and with some lower bound results from [25], [11] or [19]) offers a new proof of exponential lower bound for cut-elimination in LK, cf. [21].

while in case of $T^d_2(R)$ there will be possibly $2^{\log(n)^{O(1)}}$ cuts. However, in both cases is h proportional to $log(H)$ and k is a constant independent from n.

Hence the algorithm (A) searching for a false axiom in a refutation formed from a $T^d_2(R)$-proof asks at most $\log(n)^{O(1)}$ queries about $\Sigma^{N,logN}_d$ formulas, and the algorithm (B) searching a refutation formed from an $S^d_2(R)$-proof needs at most $O(\log(\log n))$ queries on $\Sigma^{N,logN}_d$ formulas and and $O(1)$ special queries. As a search for a false axiom from set T^d_n is just a search for a witness to the existential quantifier in $\exists y \leq n\varphi(n,y)$, these two algorithms can be seen as (nonuniform) versions of witnessing theorems for $\Sigma^b_{d+1}(R)$-consequences of $T^d_2(R)$ ad $S^d_2(R)$ respectively, as proved in [5] and [12] resp.. (Note that the proof of Proposition 1.3 also produces a tree-like Σ-depth $d-1$ refutation of T^d_n, but in this refutation h is proportional only to N).

A natural question is then what is the necessary increase in the depth when arranging that h is proportional to $\log(H)$ while enlarging the proof only polynomially. For tree-like proofs, increase by 1 is sufficient by Proposition 1.1 and also necessary as the example of the obvious refutation of $\{(x_1),\ldots,(x_n),(\neg x_1,\ldots,\neg x_n)\}$ shows. For sequence-like proofs, increase by 2 is sufficient (by Propositions 1.1 and 1.3) and it is also necessary even if the new proof is allowed to be sequence-like (this follows from Proposition 2.2: if we could get from the proof there a Σ-depth 1 proof with balanced cuts then the proof of Claim 2 would imply that the size of the original proof had to be $exp(n^{\Omega(1)})$, contradicting 2.2).

If the formulas in Π have small complexity we can add extra information about the search problem. For example, if Π is balanced (i.e. h,k are proportional to $log(N)$) and all formulas in it are Δ^t_1, $t = logN$, then the search problem is solvable by a simple decision tree of height $O(t^4)$; this is because truth of a Δ^t_1-formula can be decided by a simple decision tree of the height $O(t^2)$.

Acknowledgement: Most results of this paper were obtained while I was visiting the Department of Mathematics of the University of Illinois at Champaign-Urbana (90/91) and presented during the workshop "Arithmetic: Proof Theory and Complexity" held in Prague June 15 - July 15, 1991. I thank *Gaisi Takeuti* for valuable discussions on this topic.

References

[1] *M. Ajtai:* "The complexity of the pigeonhole principle", in: Proc. IEEE 29^{th} Annual Symp. on Foundation of Computer Science, (1988), pp. 346-355.

[2] ——:"Parity and the pigeonhole principle", in: Feasible Mathematics, Eds. S.R.Buss and P.J.Scott, Birkhauser, (1990), pp.1-24.

[3] *P. Beame, R. Impagliazzo and T. Pitassi:* "Exponential lower bounds for the pigeonhole principle", Univ. of Toronto TR 257/91, (1991).

[4] *S. Bellantoni, T. Pitassi and A. Urquhart* : "Approximation and small depth Frege proofs", SIAM J. of Computing, 21(6), (1992), pp.1161-1179.

[5] *S. R. Buss* : Axiomatizations and conservations results for fragments of bounded arithmetic", in: Contemporary Mathematics Vol.106, Proc. of Workshop in Logic and Computation, A.M.S., (1990), pp.57-84.

[6] *S. R. Buss and G. Turán* :"Resolution proofs of generalized pigeonhole principles", Theoretical Computer Science 62, (1988), pp.311-317.

[7] *G. C. Cejtin* :"On the complexity of derivations in propositional calculus", in: Studies in mathematics and mathematical logic, Part II, ed. A.O.Slisenko, (1968), pp.115-125.

[8] *S.A. Cook and A.R. Reckhow:* "The relative efficiency of propositional proof systems", J. Symbolic Logic 44(1), (1979), pp. 36-50.

[9] *W. Craig* :"Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory", Journal of Symbolic Logic 22(3), (1957), pp.269-285.

[10] *A. Haken:* "The intractability of resolution", Theoretical Computer Science 39, (1985), pp. 297-308.

[11] *J. Hastad* :"Almost optimal lower bounds for small depth circuits", in: Advances in Comput. Research, Vol.5, JAI Press, (1989), pp.143-170.

[12] *J. Krajíček* :" Fragments of bounded arithmetic and bounded query classes", Transactions of the A.M.S., to appear.

[13] ——:"No counter-example interpretation and interactive computation", in: Logic from Computer Science, Ed.Y. N. Moschovakis, Mathematical Sciences Research Institute Publication 21, Berkeley, (1992), pp.287-293.

[14] *J. Krajíček and P. Pudlák:* "Propositional proof systems, the consistency of first order theories and the complexity of computations", J. Symbolic Logic 54(3), (1989), pp. 1063-1079

[15] *J. Krajíček, P. Pudlák and A. Woods* : "Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle", Journal of the AMS, submitted.

[16] *J. Paris and A. Wilkie:* "Counting problems in bounded arithmetic", in: Methods in Mathematical Logic, LNM 1130, Springer (1985), pp. 317-340.

[17] *J. Paris, A. Wilkie and A. Woods:* "Provability of the pigeonhole principle and the existence of infinitely may primes", Journal of Symbolic Logic 53 (4), (1988), pp. 1235-1244.

[18] *M. Sipser:* "Borel sets and circuit complexity", Proc. 15th Annual ACM Symp. on Th. of Computing, (1983), pp. 61-69.

[19] *R. Smolensky:* "Algebraic methods in the theory of lower bounds for Boolean circuit complexity", in: Proc. 19th Ann. ACM Symp. on Th. of Computing, (1987), pp. 77-82.

[20] *P.M. Spira:* "On time-hardware complexity of tradeoffs for Boolean functions", in: Proc. 4^{th} Hawaii Symp. System Sciences, Western Periodicals Co., North Hollywood (1971), pp. 525-527.

[21] *R. Statman:* "Proof search and speed-up in the predicate calculus", Ann. Math. Logic 15, (1978), pp. 225-287.

[22] *W.W. Tait:* "Normal derivability in classical logic", in: "The syntax and semantics of Infinitary Languages", ed. J. Barwise, Springer, (1968), pp. 204-236.

[23] *G. Takeuti:* "Proof theory", North-Holland, (1975).

[24] *S. Toda:* "On the computational power of PP and $\oplus P$", Proc. 30th IEEE Symp. on the Found. of Computer Science, (1989), pp. 514-519.

[25] *A. Yao:* "Separating the polynomial-time hierarchy by oracles", Proc. 26th Ann. IEEE Symp. on Found. of Comp. Sci., (1985), pp. 1-10.

Mathematical Institute
Academy of Sciences
Žitná 25, Praha 1
11567 Czech Republic
E.mail: krajicek at csearn.bitnet