Annals of Pure and Applied Logic 157 (2009) 194–205

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

journal homepage: www.elsevier.com/locate/apal

On lengths of proofs in non-classical logics

Pavel Hrubeš

Department of Computer Science, University of Toronto, Canada

ARTICLE INFO

Article history:
Available online 12 December 2008

Keywords:
Proof complexity
Non-classical logics

ABSTRACT

We give proofs of the effective monotone interpolation property for the system of modal logic K, and others, and the system IL of intuitionistic propositional logic. Hence we obtain exponential lower bounds on the number of proof-lines in those systems. The main results have been given in [P. Hrubeš, Lower bounds for modal logics, Journal of Symbolic Logic 72 (3) (2007) 941–958; P. Hrubeš, A lower bound for intuitionistic logic, Annals of Pure and Applied Logic 146 (2007) 72–90]; here, we give considerably simplified proofs, as well as some generalisations.

1. Introduction

When investigating a proof system S, after the questions of its soundness and completeness have been settled, it is natural to consider the complexity of proofs in S. For a particular set of S tautologies, we want to determine the sizes of their shortest proofs, or to find examples of tautologies which require large proofs in S (where "large" depends on the nature of S). This problem can be interesting for at least two reasons. First, there is a well known connection between the complexity of propositional proof systems and some conjectures in computational complexity. Namely, we know that $NP \neq coNP$ iff for every propositional proof system S there exist propositional tautologies requiring superpolynomial size proofs in S. There is an analogous connection between $NP \neq PSPACE$ and the complexity of proof systems for intuitionistic logic and some modal logics, like K. The second motivation can have both a practical and a philosophical face, and it is the relative comparison of efficiency of proof systems. We can have two proof systems proving the same theorems (or at least equivalent with respect to some set of formulas), the proofs in one being considerably shorter than in the other. For example, in [6] we have been given examples of intuitionistic tautologies which require exponential size proofs in IL, but which have linear size classical proofs. If sizes of proofs can be taken as a measure of how difficult it is to prove theorems, this corresponds to the experience that many have had: it is more difficult to work intuitionistically than classically. In this way, proof complexity can study the function of concepts and tools used in mathematics and perhaps even in the natural language. How does the application of the excluded middle simplify arguments? Does the use of definitions simplify proofs? How are natural numbers useful? These are the questions that we can interpret as speed-up relations between proof systems.

Another remarkable aspect of the study of the complexity of intuitionistic proofs is that of determining their *computational content*. It is well known that from a proof of a formula $\forall x \exists y P(x, y)$ in intuitionistic predicate calculus one can extract a term s.t. $\forall x P(x, t(x))$ is a tautology, i.e. we can find a function which to every x assigns a y s.t. $P(x, y)$ is satisfied. This property is a basic aspect of the intended constructive nature of intuitionistic logic. Moreover, the term t may be understood as a programme for finding such a y. It has been shown in [3,4] that there even exists a close quantitative connection between sizes of intuitionistic *propositional* proofs and Boolean circuits.[1] They have shown that the system of intuitionistic logic enjoys *effective interpolation property*, which in general means that for a tautology of a certain form and with a proof of length n we can find a Boolean circuit of size polynomial in n which solves a certain problem. In this paper, we show that the

E-mail address: pahrubes@cs.toronto.edu.

[1] A circuit may be conceived as a programme computing a function from set of 0, 1-strings of length k to {0, 1}.

0168-0072/$ – see front matter © 2009 Published by Elsevier B.V.
doi:10.1016/j.apal.2008.09.013

connection between circuits and intuitionistic proofs is even tighter: we show that *IL* (and *K*) has even *effective monotone interpolation property*, i.e. for a suitable choice of tautologies we can guarantee that the circuit in question is monotone. Monotone Boolean circuits are a well-studied class of Boolean circuits. In [9,1] there were given examples of functions in *NP* which require superpolynomial resp. exponential size monotone circuits. This enables us to give examples of *IL* (and *K*) tautologies $A_1, A_2 \ldots$ s.t. every *IL* resp. *K* proof of A_i has an exponential number of proof-lines (in terms of the size of A_i).

The main theorems were already given in [5,6]. The proofs presented here are considerably simpler, more general, and use more elementary techniques. The original proof for *K* was based on a model-theoretic construction. The advantage, and, as it now appears, the only advantage, was in showing the affinity between the proof of the lower bound for *K*, and the proof of lower bound for monotone circuits (as formulated in [8]). The bound for *IL* was then obtained by means of a translation to *K*. In this paper, we reduce the monotone interpolation for both *K* and *IL* to the problem of satisfiability of a set of Horn clauses, which is shown to be decidable by a quadratic size monotone circuit. Hence the proof for *IL* is now direct and follows from the fact that in Gentzen style formalisation of *IL* the inferences can be represented by Horn clauses. We even present a lower bound on the sizes of generalisation axioms in *K*, the proof of which employs the simple technique used in [7] (and similar to [3]). The motivation for stating the proofs in a more standard fashion is, besides that of their simplification, the following: when the lower bound was first reached, it was believed (by the author at least) that it requires two components, the right choice of the hard tautologies, and the model theoretic construction. It was also hoped that a similar construction could be carried out in much stronger proof systems, perhaps even in classical logic. However, it is now clear that the proof requires no such extravagant approach, and that in fact the only non-trivial step is the choice of the tautologies. When they are stated, the proof of their hardness naturally follows.

Can some of the techniques be used to prove lower bounds for classical propositional logic? 'No' is then the conclusion of this paper. On the other hand, we can use intuitionistic logic as a background for the study of phenomena which are beyond our reach, or which do not occur in classical logic. Emil Jeřábek has recently proved a separation between extended and substitution intuitionistic calculi. In extended intuitionistic calculus we are allowed to use definitions in a proof.[2] In substitution calculus we are allowed to use the rule

$$\frac{\psi(p)}{\psi(\xi)},$$

where p is a variable and ξ a formula substituted in place of p. Extended and substitution systems for classical logic are well-known to be polynomially equivalent. In intuitionistic logic, the use of the substitution rule has an exponential speed-up over the extension rule. Hence, their equivalence in classical logic is, in a sense, merely accidental. A more fundamental problem that we could attack is:

Does extended intuitionistic calculus have a superpolynomial speed-up over intuitionistic calculus?

In other words, we ask whether the use of definitions can significantly shorten intuitionistic proofs. This problem, as far as I am aware, had not been completely solved for any proof system,[3] and perhaps even a reasonable conditional result would give an insight into the usefulness of abbreviations.

2. Modal logic

2.1. The system **K**

The system of modal logic *K* is obtained by adding the symbol $\Box$ to propositional logic. In addition to propositional rules and axioms, *K* contains *the rule of generalisation*

$$\frac{A}{\Box A}$$

and *the axiom of distributivity*

$$\Box(A \to B) \to (\Box A \to \Box B).$$

The generalisation rule and distributivity axiom will be called *modal rules of K*. We shall be interested in bounding the number of applications of modal rules in proofs of *K*, and hence the specific axiomatisation of the underlying propositional logic is immaterial.

2.2. Monotone interpolation for **K**

From the point of view of pure propositional logic, the symbol $\Box A$ is simply a new propositional variable. The modal rules of *K* can be seen as imposing additional structure on those variables. Let us ask *what* structure is imposed on the variables by modal axioms in a proof. We will see that the relations between those variables, as imposed by a *K* proof, can be represented in a simple way by means of Horn clauses.

[2] The so called extension rule has the form $q \equiv \psi$, where q occurs neither earlier in the proof nor in ψ, nor in the conclusion.

[3] Even in classical predicate calculus where we are allowed to define new predicates and terms the problem is tricky, see [2].

Let S be a K proof. We shall define *the characteristic set of clauses for* S, $\mathcal{C}_S$, as follows:

(1) if a generalisation rule

$$\frac{A}{\Box A}$$

occurs in S, we put the clause $\{\Box A\}$ in $\mathcal{C}_S$,
(2) if a distributivity axiom $\Box C \to (\Box A \to \Box B)$ occurs in S, where $C = A \to B$, we put the clause $\{\neg\Box C, \neg\Box A, \Box B\}$ in $\mathcal{C}_S$.

We can see that $\mathcal{C}_S$ is a set of Horn clauses and $\mathcal{C}_S$ never contains a negative clause (i.e. a clause of the form $\{\neg p_1, \dots \neg p_k\}$). $|\mathcal{C}_S|$ is equal to the number of applications of modal rules in S.

Let us first state a general property of a set of Horn clauses. For an assignment σ to variables V, V_σ will denote the set of clauses $\{\{v\}; v \in V, \sigma(v) = 1\}$. *The total size* of a set of clauses $\mathcal{C}$ is the sum of sizes of clauses in $\mathcal{C}$.

Proposition 1. (1) *Let $\mathcal{D}$ be a set of Horn clauses s.t. in $\mathcal{D}$ occurs no negative clause. Let Y be a set of negative singular clauses. Assume that $\mathcal{D}, Y$ is not satisfiable. Then there exists $C \in Y$ s.t. $\mathcal{D}, C$ is not satisfiable.*
(2) *Let $\mathcal{D}$ be a set of Horn clauses of total size n and not containing a negative clause. Let V be a set of variables and p a variable. Then there exists a monotone circuit C in variables V of size $O(n^2)$ s.t. for every assignment σ of V, $C = 1$ iff*

$$\mathcal{D}, V_\sigma, \{\neg p\}$$

is not satisfiable.

Proof. (1). Let us have a resolution refutation of $\mathcal{D} \cup Y$; it contains only Horn clauses. It is easy to see that we can transform the refutation to a tree-like refutation whose last step is a resolution of some clause in Y. i.e., the last step has the form

$$\frac{\{v\}, \quad \{\neg v\}}{\emptyset},$$

for some $\{\neg v\} \in Y$. When resolving a negative clause with a Horn clause, we obtain a negative clause. Hence in the resolution proof of the clause $\{v\}$ no clause of Y could have been used and $\mathcal{D} \cup \{\neg v\}$ is not satisfiable.

(2). Without loss of generality we can assume that $p \notin V$. For the definition of flowgraph and the relation between flowgraphs and monotone circuits see page 9. Let us represent a set of Horn clauses $\mathcal{D}$, containing no negative clauses, as a flowgraph F. (We stipulate that this implies that an empty clause is not in $\mathcal{D}$.) The vertices of F will be the variables in $\mathcal{D}$. Assume that $\mathcal{D}$ does not contain a clause of size one. If $\mathcal{D}$ is empty we let $C := 0$. If $\mathcal{D} \neq \emptyset$, for a clause $\{\neg q_1, \dots \neg q_k, q\}$ in $\mathcal{D}$ we shall put a gate from $q_1, \dots q_k$ to q in F. Let σ be an assignment to V. Clearly, $F_\sigma(p) = 1$ iff

$$\mathcal{D}, V_\sigma, \{\neg p\}$$

is unsatisfiable. By Proposition 5 there exists a monotone circuit C in variables V of size $O(n^2)$ s.t. $C(\sigma(V)) = F_\sigma(p)$. Then $C = 1$ iff $\mathcal{D}, V_\sigma, \{\neg p\}$ is unsatisfiable.

If $\mathcal{D}$ contains clauses of size one, let V_1 be the set of variables occurring as a singular clause in $\mathcal{D}$ and let $\mathcal{D}_{>1}$ be the set of clauses of size > 1 in $\mathcal{D}$. If $p \in V_1$ we set $C := 1$. Otherwise, let $C_{>1}$ be the circuit constructed from $\mathcal{D}_{>1}$ as above. The circuit C is then obtained from $C_{>1}$ by setting the variables V_1 to 1 in $C_{>1}$. □

For a formula α, $\Box A$ will be called *an immediate modal subformula of* α, if $\Box A$ has an occurrence in α not in a range of any modality. Then α can be uniquely written as

$$\beta(\Box A_1, \dots \Box A_k, s_1, \dots s_l),$$

where $\Box A_i$ are its immediate modal subformulas and $s_1, \dots s_l$ are variables having non-modalised occurrences in α, and β is a propositional formula. A truth assignment σ to all the immediate modal subformulas and variables occurring in α in a non-modal context induces a truth assignment Θ_σ to α. We define $\Theta_\sigma(\alpha)$ as the Boolean value of the formula

$$\beta(\sigma(\Box A_1), \dots \sigma(\Box A_k), \sigma(s_1), \dots \sigma(s_l)).$$

Lemma 2. *Let $S = A_1, \dots A_n$ be a K proof.*

(1) *Let $B_1, \dots B_k, B$ be formulas. Assume that*

$$\mathcal{C}_S, \{\Box B_1\}, \dots \{\Box B_k\}, \{\neg\Box B\}$$

is not satisfiable. Then

$$\bigwedge_{i=1,\dots k} \Box B_i \to \Box B$$

is a K tautology.
(2) *Assume that σ is an assignment to all immediate modal subformulas in S and the non-modalised variables in S. Assume that σ satisfies $\mathcal{C}_S$. Then*

$$\Theta_\sigma(A_i) = 1$$

for every $i = 1, \dots n$.

Proof. (1). Let F_S be the set of distributivity axioms and the conclusions $\Box A$ of generalisation rules used in S. The definition of $\mathcal{C}_S$ and Θ_σ directly implies the following:

($\star$) *Let σ be an assignment to the immediate modal subformulas in F_S. Then σ satisfies $\mathcal{C}_S$ iff the formulas in F_S are true in the assignment Θ_σ.*

The proof is then immediate. If $\mathcal{C}_S, \{\Box B_1\}, \ldots, \{\Box B_k\}, \{\neg\Box B\}$ is not satisfiable then the formula

$$\left(\bigwedge F_S \wedge \bigwedge_{i=1,\ldots k} \Box B_i\right) \to \Box B$$

is a tautology which is provable merely by propositional logic. Moreover, the formulas F_S are K tautologies and hence

$$\bigwedge_{i=1,\ldots k} \Box B_i \to \Box B$$

is a K tautology.

(2). By ($\star$) the formulas in F_S are satisfied by Θ_σ. Hence the modal rules in S are satisfied by Θ_σ. Since the definition of Θ_σ commutes with the definition of logical connectives, also the propositional axioms and rules are satisfied by Θ_σ. □

Let $\Box A_1, \ldots \Box A_k$ be the immediate modal subformulas of α. An assignment σ to the variables $V = \Box A_1, \ldots \Box A_k$ will be called *consistent with respect to* α, if there exists a K model M s.t. $M \models \alpha$ and $M \models \Box A_i$ iff $\sigma(\Box A_i) = 1$.

Lemma 3. *Let $\Box A_1, \ldots, \Box A_k$ be the immediate modal subformulas of α. Let S be a K proof of*

$$\alpha \to (\Box\beta_1 \vee \Box\beta_2).$$

Let $V = \Box A_1, \ldots \Box A_k$. Let σ be a consistent assignment to V with respect to α. Then the set of clauses

$$\mathcal{C}_S, V_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$$

is not satisfiable.

Proof. Let $Y_\sigma := \{\{\neg v\}; v \in V, \sigma(v) = 0\}$. Let us first show that

$$\mathcal{D} := \mathcal{C}_S, V_\sigma, Y_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$$

is not satisfiable. Assume, for the sake of contradiction, that ρ is an assignment satisfying $\mathcal{D}$. Then $\sigma \subseteq \rho$. Let M be a model s.t. $M \models \alpha$ and $M \models \Box A_i$ iff $\sigma(\Box A_i) = 1$. Let $\bar{s}$ be the list of variables occurring in a non-modal context in S. Let ρ' be the assignment to $\bar{s}$ s.t. $\rho'(s) = 1$ iff $M \models s$. Let $\sigma' := \rho \cup \rho'$. We can assume that σ' is defined on all immediate modal subformulas and non-modalised variables in S. By Lemma 2, the assignment $\Theta_{\sigma'}$ satisfies all the steps in S. Moreover, we can see that $\Theta_{\sigma'}(\alpha) = 1$, $\Theta_{\sigma'}(\Box\beta_1) = \Theta_{\sigma'}(\Box\beta_2) = 0$, and hence $\Theta_{\sigma'}(\alpha \to (\Box\beta_1 \vee \Box\beta_2)) = 0$, which is a contradiction.

Let us show that also $\mathcal{C}_S, V_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$ is not satisfiable. The clauses from $Y_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$ are the only negative clauses in $\mathcal{D}$. Hence, by Proposition 1, there exists $C \in Y_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$ s.t. $\mathcal{C}_S, X, C$ is not satisfiable. Let us show it is one of $\{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$. Assume the contrary. Then $C = \{\neg\Box A_j\}$ for some $A_j, j \in 1, \ldots k$. Then, by part (1) of Lemma 2,

$$K \vdash \bigwedge_{\Box A_i \in V_\sigma} \Box A_i \to \Box A_j.$$

But $M \models \bigwedge_{\Box A_i \in V_\sigma} \Box A_i$ and $M \models \Box A_j$ which is a contradiction. □

For a circuit C, $[C]$ will denote an equivalent Boolean formula, i.e., some formula defining the same Boolean function.

Theorem 4. *Let S be a K proof of the formula*

$$\alpha \to (\Box\beta_1 \vee \Box\beta_2).$$

Let $\Box A_1, \ldots \Box A_k$ be the immediate modal subformulas of α. Assume that S contains n modal rules. Then there exist monotone circuits C_1 and C_2 of size $O(n^2)$ in k variables s.t. the following are K tautologies:

(1) $\alpha(\Box A_1, \ldots \Box A_k, \bar{s}) \to [C_1](\Box A_1, \ldots \Box A_k) \vee [C_2](\Box A_1, \ldots \Box A_k)$,
(2) $[C_1](\Box A_1, \ldots \Box A_k) \to \Box\beta_1$, *and* $[C_2](\Box A_1, \ldots \Box A_k) \to \Box\beta_2$.

Proof. Let $\mathcal{C}_S$ be the characteristic set of clauses for S. The total size of $\mathcal{C}_S$ is $\leq 3n$, since every clause in $\mathcal{C}_S$ has size at most three. Let $V = \Box A_1, \ldots \Box A_k$. Let C_1 be the circuit of size $O(n^2)$ in variables V from Proposition 1 s.t. for any assignment σ to V, $C_1 = 1$ iff $\mathcal{C}_S, V_\sigma, \{\neg\Box\beta_1\}$ is unsatisfiable. Similarly for C_2 and β_2.

Let us show that $\alpha(\Box A_1, \ldots \Box A_k, \bar{s}) \to [C_1](\Box A_1, \ldots \Box A_k) \vee [C_2](\Box A_1, \ldots \Box A_k)$ is a K tautology. Let M be a K model s.t. $M \models \alpha$ and let σ be an assignment to V s.t. $\sigma(\Box A_i) = 1$ iff $M \models \Box A_i$. By Lemma 3, $\mathcal{C}_S, V_\sigma, \{\neg\Box\beta_1\}, \{\neg\Box\beta_2\}$ is unsatisfiable. Hence $C_1(\sigma(V)) = 1$ or $C_2(\sigma(V)) = 1$ and hence $M \models [C_1](\Box A_1, \ldots \Box A_k)$ or $M \models [C_2](\Box A_1, \ldots \Box A_k)$.

Let us show that (1) is a K tautology. Assume that $M \models [C_1](\Box A_1, \ldots \Box A_k)$ and let σ be as above. Then, by definition of C_1, $\mathcal{C}_S, V_\sigma, \{\neg\Box\beta_1\}$ is unsatisfiable. Hence, by Lemma 2 part (1)

$$\bigwedge_{\sigma(\Box A_i)=1} \Box A_i \to \Box\beta_1$$

is a K tautology. But the conjunction on the left hand side contains the formulas true in M and hence also $M \models \Box\beta_1$. □

Remark. Note that we do not restrict the formulas α, β_1 and β_2 in any way. In particular, α is allowed to contain non-modalised variables, negations of modal subformulas, and nested modalities. However, the important applications of the Theorem are in the case when the formulas have quite a simple form.

Corollary. *Let $\alpha(\Box p_1, \dots \Box p_k, \bar{s}) \to (\Box\beta_1(\bar{p}, \overline{r_1}) \vee \Box\beta_2(\bar{p}, \overline{r_2}))$ be a K tautology, where $\alpha(p_1, \dots p_k, \bar{s})$, β_1 and β_2 do not contain any modalities. Assume that S is a proof of the tautology with n modal rules. Then there exist monotone circuits C_1 and C_2 of size $O(n^2)$ in variables $\bar{p}$ with the following properties: for any assignment σ to the variables $\bar{p}$*

(1) *if $\alpha(\bar{p}, \bar{s})$ is true (for some assignment to $\bar{s}$) then $C_1(\bar{p}) = 1$ or $C_2(\bar{p}) = 1$,*
(2) *if $C_1(\bar{p}) = 1$ resp. $C_2(\bar{p}) = 1$ then β_1 resp. β_2 is true (for any assignment to $\overline{r_1}$ resp. $\overline{r_2}$.)*

Proof. Follows from the previous theorem and the fact that if A is a K tautology then the propositional formula A^0, obtained from A by deleting all the boxes, is a classical tautology. □

Flowgraphs and monotone circuits

A flowgraph F is a directed graph with edges uniquely labelled by subsets of vertices in the following fashion. For a vertex a of F, Pred(a) will denote the set of vertices b s.t. there is an edge from b to a. We than require that there exists a disjoint partition of Pred(a) into sets $X_1, \dots X_k$ s.t. for every $i = 1, \dots k$ and $b \in X_i$ the edge from b to a is labelled by X_i. The set of edges from X_i to a will be called *a gate from X_i to a.* The intended meaning of a gate from X_i to a is: if all the vertices in X are "true" then the vertex a is also "true".

Let us have a fixed subset V of the vertices of F. Let σ be a 0, 1-assignment to the vertices V. *A possible solution* of a flowgraph G is a 0, 1-assignment ρ to the vertices of G s.t.

(1) if $\sigma(v) = 1$ then $\rho(v) = 1$, for $v \in V$,
(2) for every a and a gate from X to a , if $\rho(b) = 1$ for every $b \in X$ then $\rho(a) = 1$.

The solution of F for σ is the 0, 1 - assignment F_σ to vertices of F s.t. for every vertex a, $F_\sigma(a) = 0$ iff there exists a possible solution ρ s.t. $\rho(a) = 0$. We can see that a vertex a is assigned 1 in F_σ iff there exists at least one gate from X to b s.t. $F_\sigma(b) = 1$ for all $b \in X$. Hence F_σ is the minimum possible solution of F for σ.

The following proposition shows that flowgraphs can be simulated by monotone circuits.

Proposition 5. *Let F be a flowgraph with n edges. Let a be a vertex in F. Then there exists a monotone circuit C in variables V of size $O(n^2)$ s.t. for every assignment σ to V*

$$C(\sigma(V)) = F_\sigma(a).$$

Proof. We will first show that we can find an acyclic flowgraph $F^\star$ of size $O(n^2)$ s.t. for any assignment σ to V, $F_\sigma(a) = F^\star_\sigma(a)$. Assume that F has k vertices $a_1, \dots a_k$. Hence $k \leq 2n$, as we can assume that F does not contain isolated vertices.

The construction is straightforward: for every vertex a of F, we introduce k copies $a^1, \dots a^k$. The flowgraph $F^\star$ will have k^2 vertices a^j, $a \in F, j = 1 \dots k$ and the gates will be defined as follows:

(1) For every $j = 1, \dots k-1$ and for every $a \in F$ we put in $F^\star$ a gate from a^j to a^{j+1}.
(2) For every $j = 1, \dots k-1$ and a gate from X to a in F, we add a gate from $X^j := \{b^j, b \in X\}$ to a^{j+1} in $F^\star$.

Finally, we identify the vertices v^1 of $F^\star$ with v for $v \in V$ and we identify the vertex a of M with its copy a^k in $F^\star$. Clearly, $F^\star$ contains $O(n^2)$ edges and $F_\sigma(a) = F^\star_\sigma(a)$ for any assignment.

The construction gives an acyclic flowgraph s.t. there are no edges leading to the vertices in V. It is now sufficient to prove that for such a flowgraph F with n edges and a vertex a of F there exists a monotone circuit C of size $O(n)$ s.t. $C(\sigma(V)) = F_\sigma(a)$ for any σ. To a vertex $v \in V$ we will assign the circuit v, and to a leaf of a different kind the constant 0. Assume that for a vertex $b \in F$ we have assigned circuits C_d to all $d \in$ Pred(b). For a gate from $X \subseteq$ Pred(b) to b, let C_X be the circuit $\bigwedge_{d \in X} C_d$. Then we assign to b the disjunction of C_X, for all gates from X to b. Such a circuit has size $O(n)$ and has the required property. □

2.3. Extension to other modal systems

In the proof of Theorem 4 we used only the fact that the characteristic set of clauses of a proof is a set of Horn clauses not containing negative clauses, and the clauses have a bounded size. These assumptions are equally satisfied in the systems K_4, Gödel-Löb's logic and some others (like the *NP* system $K + \Box\Box \bot$). For example, the K_4 axiom

$$\Box A \to \Box\Box A$$

receives the clause

$$\{\neg\Box A, \Box\Box A\}.$$

The characteristic set of clauses of S or $S4$ proof would be defined by transforming the proof into K resp. $K4$ proof by means of the translation $\Box A \to \Box A \wedge A$.

The theorem and its corollary[4] hold also for those systems without modification. Extending the result to S_5 is impossible, as observed in [5]. A deeper explanation follows from the fact there exists a kind of simulation between extended $S5$ and classical extended Frege systems. This, we hope, will one day appear in a paper by Emil Jeřábek.

[4] However, *the proof* of the corollary would need a modification in the case of Gödel-Löb's logic and $K + \Box\Box \bot$.

2.4. Counting the number of distributivity axioms and the number of generalisation rules in K

It will be noted that Theorem 4 is true also if we count only the number of *distributivity axioms* in a K proof. This would be achieved by assigning all singular clauses in the characteristic set of clauses of a proof (corresponding exactly to the conclusions of generalisation rules) to 1, and applying the argument to such a restricted characteristic set. This fact corresponds to the intuition that it is the distributivity axiom which is responsible for complexity of modal proofs. It may therefore be surprising that the same is true when the *size* of *generalisation rules* is considered, as we will show here.

Let $\mathcal{A}$ be a set of formulas. $cl(\mathcal{A})$ will denote the smallest set s.t.

(1) $\mathcal{A} \subseteq cl(\mathcal{A})$
(2) if $A,\ A \to B \in cl(\mathcal{A})$ then also $B \in cl(\mathcal{A})$.

In other words, $cl(\mathcal{A})$ is the closure of $\mathcal{A}$ under modus ponens.

For a proof S, *the set of generalised formulas of* S, G_S, will be the set of formulas A s.t. the rule

$$\frac{A}{\Box A}$$

occurs in S. The generalisation size of S will be the total size of G_S, i.e., the sum of sizes of formulas in G. For a formula A let us introduce a fresh variable $\langle A\rangle$.

Lemma 6. *Let G and $\mathcal{A} = \{A_1, \ldots A_k\}$ be sets of formulas, the total size of $G \cup \mathcal{A}$ being n. Let B be a formula. Then there exists a monotone circuit C in variables $V = \langle A_1\rangle, \ldots \langle A_k\rangle$ of size $O(n^2)$ s.t. for any assignment σ of V, $C = 1$ iff*

$$B \in cl(G, V_\sigma),$$

where $V_\sigma := \{A_i \in \mathcal{A}; \sigma(\langle A_i\rangle) = 1\}$.

Proof. Let us represent the set $G \cup \mathcal{A}$ by a flowgraph F of size n. Its vertices will be the subformulas of formulas in G and $\mathcal{A}$. For a vertex of F of the form $A \to B$ we connect A and $A \to B$ to B by a gate. Clearly, for an assignment σ to V, $B \in cl(G, V_\sigma)$ iff $F_\sigma(B) = 1$, and the statement then follows from Proposition 5. □

Lemma 7. (1) *Let G be a finite set of K tautologies. Let $\mathcal{A}$ be a finite set of formulas. Assume that $B \in cl(G \cup \mathcal{A})$. Then*

$$\bigwedge_{A \in \mathcal{A}} \Box A \to \Box B$$

is a K tautology.

(2) *Let $S = A_1, \ldots A_n$ be a K proof. Let $\mathcal{A}$ be a set of formulas. Let σ be a truth assignment to all immediate modal subformulas and variables occurring in non modal context in S s.t. $\sigma(\Box A) = 1$ iff $A \in cl(\mathcal{A}, G_S)$. Then*

$$\Theta_\sigma(A_i) = 1,$$

for $i = 1, \ldots n$ (Θ_σ is defined as in Lemma 2).

Proof. (1). Let X be a finite set of formulas. Define $cl_i(X)$, $i \in \omega$ as follows: $cl_0(X) := X$ and $cl_{i+1}(X)$ is the set of all formulas B for which there exists a formula C s.t. $C \to B$, $C \in cl_i(X)$. Then $cl(X) = \bigcup_{i\in\omega} cl_i(X)$. By induction with respect to i one can prove that if $B \in cl_i(X)$ then $\bigwedge_{A\in X} \Box A \to \Box B$ is a tautology. For $i = 0$ it is trivial. If $B \in cl_{i+1}(X)$ then there exists a C s.t. $C \to B$, $C \in cl_i(X)$, and hence $\bigwedge_{A\in X} \Box A \to \Box C$ and $\bigwedge_{A\in X} \Box A \to \Box(C \to B)$ are tautologies. Hence $\bigwedge_{A\in X} \Box A \to \Box B$ is a tautology, using the axiom of distributivity. If $X = G \cup \mathcal{A}$ where G is a set of K tautologies we obtain that also $\bigwedge_{A \in \mathcal{A}} \Box A \to \Box B$ is a K tautology.

(2). It is easy to see that Θ_σ satisfies all the axioms and rules S. The generalisation rule is satisfied trivially (all the conclusions are assigned 1 by definition). Distributivity axioms are satisfied by the definition of cl. Propositional rules and axioms are satisfied since Θ_σ commutes with propositional connectives. □

Lemma 8. *Let α be a formula and let $\mathcal{A} = A_1, \ldots, A_k$ be its immediate modal subformulas, let $V = \langle A_1\rangle, \ldots, \langle A_k\rangle$. Let S be a K proof of*

$$\alpha \to (\Box\beta_1 \vee \Box\beta_2).$$

Let σ be a consistent assignment to V with respect to α. Then either β_1 or β_2 is in $cl(G_S \cup V_\sigma)$.

Proof. As in Lemma 3. □

Theorem 9. *Let S be a K proof of the formula*

$$\alpha \to (\Box\beta_1 \vee \Box\beta_2).$$

Let $\Box A_1, \ldots \Box A_k$ be the immediate modal subformulas of α, having total size k. Assume that the total size of formulas generalised in S is n. Then there exist monotone circuits C_1 and C_2 in variables $v_1, \ldots v_k$ of size $O(n + k)^2$ s.t. the following are K tautologies:

(1) $\alpha(\Box A_1, \ldots \Box A_k, \vec{s}) \to [C_1](\Box A_1, \ldots \Box A_k) \vee [C_2](\Box A_1, \ldots \Box A_k)$,
(2) $[C_1](\Box A_1, \ldots \Box A_k) \to \Box\beta_1$, *and* $[C_2](\Box A_1, \ldots \Box A_k) \to \Box\beta_2$.

Proof. As in Theorem 4. □

2.5. Examples of hard **K** tautologies

We shall now use the corollary of Theorem 4 to give particular examples of hard K tautologies.

Example 1. - $\alpha(\Box\overline{p}, \overline{s}) \to \Box\beta$.

Assume that $\alpha(\overline{p}, \overline{s})$ and $\beta(\overline{p}, \overline{r})$ are formulas containing no $\Box$. We will say that a circuit C in variables $\overline{p}$ *interpolates* α and β, if for any assignment σ to $\overline{p}$

(1) if $\alpha(\overline{p}, \overline{s})$ is true (for some assignment to $\overline{s}$) then $C(\overline{p}) = 1$,
(2) if $C(\overline{p}) = 1$ then $\beta(\overline{p}, \overline{r})$ is true (for any assignment to $\overline{r}$.)

We will say that a formula α is *monotone in* $\overline{p}$, if it can be transformed to a DNF form where no negation is attached to a variable in $\overline{p}$.

Proposition 10. *Let $\alpha(\overline{p}, \overline{r})$ be a propositional formula monotone in $\overline{p}$ and let $\beta(\overline{p}, \overline{s})$ be a propositional formula.*

(1) *If $\alpha(\overline{p}, \overline{r}) \to \beta(\overline{p}, \overline{s})$ is a propositional tautology then $\alpha(\Box\overline{p}, \overline{r}) \to \Box\beta(\overline{p}, \overline{s})$ is a K-tautology.*
(2) *Assume that*

$$\alpha(\Box\overline{p}, \overline{r}) \to \Box\beta(\overline{p}, \overline{s})$$

is provable in K with n distributivity axioms. Then there exists a monotone circuit of size $O(n^2)$ which interpolates $\alpha(\overline{p}, \overline{r})$ and $\beta(\overline{p}, \overline{s})$.

Proof. (1). Note that if $\alpha(\overline{p}, \overline{s}) \to \beta(\overline{p}, \overline{s})$ is a classical tautology then there exists a monotone formula $\gamma(\overline{p})$ s.t. (i) $\alpha(\overline{p}, \overline{s}) \to \gamma(\overline{p})$ and (ii) $\gamma(\overline{p}) \to \beta(\overline{p}, \overline{s})$ are propositional tautologies. Hence also $\alpha(\Box\overline{p}, \overline{s}) \to \gamma(\Box\overline{p})$ and $\Box\gamma(\overline{p}) \to \Box\beta(\overline{p}, \overline{s})$ are K tautologies, the former by substituting $\Box\overline{p}$ for $\overline{p}$ in (i) and the latter by applying generalisation and distributivity to (ii). On the other hand, since γ is a monotone formula, then also $\gamma(\Box\overline{p}) \to \Box\gamma(\overline{p})$ can be proved in K by successive use of K tautologies $\Box A \circ \Box B \to \Box(A \circ B)$, where $\circ = \wedge, \vee$.

(2) is an immediate application of Corollary of Theorem 4 for $\beta_1 := \beta$, $\beta_2 := \bot$. □

Let

$$Clique_n^k(\overline{p}, \overline{r})$$

be the proposition asserting that $\overline{r}$ is a clique of size k on the graph represented by $\overline{p}$. Let

$$Color_n^k(\overline{p}, \overline{s})$$

be the proposition asserting that $\overline{s}$ is a k-coloring of the graph represented by $\overline{p}$.

Theorem 11. *Let Θ_n^k be the formula*

$$Clique_n^{k+1}(\Box\overline{p}, \overline{r}) \to \Box(\neg Color_n^k(\overline{p}, \overline{s})).$$

Then Θ_n^k is K tautology. Moreover, if $k := \sqrt{n}$ then every K-proof of the tautology Θ_n^k contains at least

$$2^{\Omega(n^{\frac{1}{4}})}$$

modal rules.

Proof. That Θ_n^k is a tautology follows from part (1) of the previous proposition. Let $k := \sqrt{n}$. Assume that Θ_n^k has a K-proof with m modal rules. By the previous proposition, there is a monotone interpolant C of $Clique_n^k(\overline{p}, \overline{r})$ and $\neg Color_n^k(\overline{p}, \overline{s})$ of size $O(m^2)$. By [1], every such circuit has size at least $2^{\Omega(n^{\frac{1}{4}})}$. Hence $m \sim \sqrt{2^{\Omega(n^{\frac{1}{4}})}} \sim 2^{\Omega(n^{\frac{1}{4}})}$. □

Example 2- $\bigwedge(\Box p \vee \Box q) \to (\Box\beta_1 \vee \Box\beta_2)$.

If β is a propositional formula in variables and $\overline{p} = p_1, \ldots p_n$, $\overline{q} = q_1, \ldots q_n$ then $\beta(\overline{p}/\neg\overline{q})$ will denote the formula obtained by substituting $\neg q_i$ for p_i, $i = 1, \ldots n$, in β. We may also write simply $\beta(\neg\overline{q})$ if the meaning is clear.

Lemma 12. *Let $\beta_1 = \beta_1(\overline{p}, \overline{r_1})$ and $\beta_2 = \beta_2(\overline{q}, \overline{r_2})$ be propositional formulas, $\overline{p}$, $\overline{q}$, $\overline{r_1}$, $\overline{r_2}$ disjoint. Let $\overline{p} = p_1, \ldots p_n$ and $\overline{q} = q_1, \ldots q_n$. Assume that β_1 is monotone in $\overline{p}$ or β_2 is monotone in $\overline{q}$. Assume that*

$$\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\neg\overline{p}, \overline{r_2})$$

is a classical tautology.

(1) *Then $\bigwedge_{i=1,\ldots n}(p_i \vee q_i) \to \beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\overline{q}, \overline{r_2})$ is a classical tautology.*
(2) *Let M, N be subsets of $\{1, \ldots n\}$ s.t. $M \cup N = \{1, \ldots n\}$. Then one of the following is a classical tautology:*

$$\bigwedge_{i\in M} p_i \to \beta_1(\overline{p}, \overline{r_1}), \qquad \text{or} \qquad \bigwedge_{i\in N} q_i \to \beta_2(\overline{q}, \overline{r_2}).$$

Proof. (1). Assume that, for example, β_2 is monotone in $\overline{q}$. Then

$$\bigwedge_{i=1,\dots n} (p_i \to q_i) \to (\beta_2(\overline{p}, \overline{r_2}) \to \beta_2(\overline{q}, \overline{r_2}))$$

is a tautology. Hence also

$$\bigwedge_{i=1,\dots n} (\neg p_i \vee q_i) \to (\beta_2(\overline{p}, \overline{r_2}) \to \beta_2(\overline{q}, \overline{r_2})),$$

$$\bigwedge_{i=1,\dots n} (p_i \vee q_i) \to (\beta_2(\neg\overline{p}, \overline{r_2}) \to \beta_2(\overline{q}, \overline{r_2}))$$

are tautologies. From the assumption that $\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\neg\overline{p}, \overline{r_2})$ is a tautology we obtain that also

$$\bigwedge_{i=1,\dots n} (p_i \vee q_i) \to (\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\overline{q}, \overline{r_2}))$$

is a tautology.

(2). Let M and N be fixed. Clearly,

$$\bigwedge_{i\in M} p_i \wedge \bigwedge_{i\in N} q_i \to \bigwedge_{i=1,\dots n} (p_i \vee q_i)$$

is a tautology and, by (1),

$$\bigwedge_{i\in M} p_i \wedge \bigwedge_{i\in N} q_i \to (\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\overline{q}, \overline{r_2}))$$

is a tautology. Since β_1 and β_2 contain no common variables, and β_1, resp. β_2 does not contain the variables $\overline{q}$, resp. $\overline{p}$ then either $\bigwedge_{i\in M} p_i \to \beta_1(\overline{p}, \overline{r_1})$ or $\bigwedge_{i\in N} q_i \to \beta_2(\overline{q}, \overline{r_2})$ is a tautology. □

Proposition 13. *Let $\beta_1 = \beta_1(\overline{p}, \overline{r_1})$ and $\beta_2 = \beta_2(\overline{q}, \overline{r_2})$ be propositional formulas, $\overline{p}$, $\overline{q}$, $\overline{r_1}$, $\overline{r_2}$ disjoint. Let $\overline{p} = p_1, \dots p_k$ and $\overline{q} = q_1, \dots q_k$. Assume that β_1 is monotone in $\overline{p}$ or β_2 is monotone in $\overline{q}$. Assume that*

$$\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\neg\overline{p}, \overline{r_2})$$

is a classical tautology.

(1) *Then*

$$\bigwedge_{i=1,\dots k} (\Box p_i \vee \Box q_i) \to (\Box\beta_1(\overline{p}, \overline{r_1}) \vee \Box\beta_2(\overline{q}, \overline{r_2}))$$

is K- tautology.

(2) *Moreover, if the tautology has a K-proof with n distributivity axioms then there exists a monotone circuit $C(\overline{p})$ of size $O(n^2)$ which interpolates $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ and $\beta_1(\overline{p}, \overline{r_1})$.*

Proof. Let us first show that the formula is a tautology. The assumption $\bigwedge_{i=1,\dots k}(\Box p_i \vee \Box q_i)$ can be transformed to a disjunction of conjunctions of the form

$$\bigwedge_{i\in M} \Box p_i \wedge \bigwedge_{i\in N} \Box q_i$$

such that $M \cup N = \{1, \dots k\}$. Hence it is sufficient to show that for such M and N

$$\bigwedge_{i\in M} \Box p_i \wedge \bigwedge_{i\in N} \Box q_i \to (\Box\beta_1 \vee \Box\beta_2) \qquad (\star)$$

is a tautology. By the previous Lemma either $\bigwedge_{i\in M} p_i \to \beta_1$ or $\bigwedge_{i\in N} q_i \to \beta_2$ is a classical tautology. In the first case $\bigwedge_{i\in M} \Box p_i \to \Box\beta_1$ is a tautology and hence also $(\star)$ is. Similarly in the latter case.

By the corollary of Theorem 4 there exist monotone circuits D_1 and D_2 in variables $\overline{p}$, $\overline{q}$ of size $O(n^2)$ s.t. for any assignment

$$(D_1(\overline{p}, \overline{q}) = 1) \to \beta_1, \qquad (1)$$

$$(D_2(\overline{p}, \overline{q}) = 1) \to \beta_2 \qquad (2)$$

and if the assignment satisfies $\bigwedge_{i=1,\dots k}(p_i \vee q_i)$ then

$$D_1(\overline{p}, \overline{q}) = 1 \vee D_2(\overline{p}, \overline{q}) = 1.$$

This in particular gives

$$D_1(\overline{p}, \neg\overline{p}) = 1 \vee D_2(\overline{p}, \neg\overline{p}) = 1. \qquad (3)$$

Let $C(\overline{p}) := D_1(\overline{p}, 1, \dots 1)$ and $C'(\overline{q}) := D_2(1, \dots 1, \overline{q})$. Since in (1) β_1 does not contain $\overline{q}$, we have

$$(C(\overline{p}) = 1) \to \beta_1(\overline{p}, \overline{r_1}). \tag{4}$$

Similarly, by replacing $\overline{q}$ by $\neg\overline{p}$ in (2) we have

$$(C'(\neg\overline{p}) = 1) \to \beta_2(\neg\overline{p}, \overline{r_2}). \tag{5}$$

Since D_1 and D_2 are monotone, (3) gives

$$D_1(\overline{p}, 1, \dots 1) = 1 \vee D_2(1, \dots 1, \neg\overline{p}) = 1$$

and hence

$$C(\overline{p}) = 1 \vee C'(\neg\overline{p}) = 1. \tag{6}$$

Let us show that the circuit C interpolates $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ and $\beta_1(\overline{p}, \overline{r_1})$. By (4) it is sufficient to prove that if for some assignment $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ is true then $C(\overline{p}) = 1$. But if $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ is true then by (5) $C'(\neg\overline{p}) = 0$ and, by (6), $C(\overline{p}) = 1$. □

Theorem 14. *Let*

$$\Theta_n^k := \bigwedge_{i=1,\dots n} (\Box p_i \vee \Box q_i) \to \Box\neg Color_n^k(\overline{p}, \overline{s}) \vee \Box\neg Clique_n^{k+1}(\neg\overline{q}, \overline{r}).$$

If $k := \sqrt{n}$ *then very K-proof of the tautology* Θ_n^k *contains at least*

$$2^{\Omega(n^{\frac{1}{4}})}$$

modal rules.

Proof. We shall apply Proposition 13 to the formulas $\beta_1 := \neg Color_n^k(\overline{p}, \overline{s})$ and $\beta_2 := \neg Clique_n^{k+1}(\neg\overline{q}, \overline{r})$. First, β_2 is monotone in $\overline{q}$ since $Clique(\overline{p}, \overline{r})$ is monotone in $\overline{p}$. Second, $\beta_1(\overline{p}, \overline{s}) \vee \beta_2(\overline{q}/\neg\overline{p}, \overline{r})$ is a classical tautology, since $\beta_2(\overline{q}/\neg\overline{p}, \overline{r}) = \neg Clique_n^{k+1}(\overline{p}/\neg\neg\overline{p}, \overline{r})$ is classically equivalent to $\neg Clique_n^{k+1}(\overline{p}, \overline{r})$ and

$$\neg Color_n^k(\overline{p}, \overline{s}) \vee \neg Clique_n^{k+1}(\overline{p}, \overline{r})$$

is a classical tautology. Hence Θ_n^k is a K tautology. Assume that it has a K proof with m modal rules. Then there exists a monotone circuit C in variables $\overline{p}$ of size $O(m^2)$ which interpolates $\neg\beta_2(\overline{q}/\neg\overline{p}, \overline{r})$ and β_1. Since $\neg\beta_2(\overline{q}/\neg\overline{p}, \overline{r})$ is classically equivalent to $Clique_n^{k+1}(\overline{p}, \overline{r})$, C interpolates $Clique_n^{k+1}(\overline{p}, \overline{r})$ and $\neg Color_n^k(\overline{p}, \overline{s})$. By the result in [1] every such circuit must have size at least $2^{\Omega(n^{\frac{1}{4}})}$. Hence $m \geq \sqrt{2^{\Omega(n^{\frac{1}{4}})}} \sim 2^{\Omega(n^{\frac{1}{4}})}$. □

3. Intuitionistic logic

3.1. The system IL

We will use a Gentzen style axiomatisation of intuitionistic logic. In a sequent $\Gamma \Rightarrow \Delta$, Γ and Δ are understood as sets of formulas. The axioms are $A \Rightarrow A$ and $\bot \Rightarrow A$. The inferences will be *the cut*

$$\frac{\Gamma \Rightarrow \Delta, A, \quad \Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta},$$

the weakening

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, \Sigma \Rightarrow \Delta, \Pi},$$

and the inferences

LEFT

$$\frac{\Gamma, A \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}, \quad \frac{\Gamma, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta} \qquad \frac{\Gamma, A \Rightarrow C, \quad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C}$$

$$\frac{\Gamma \Rightarrow A, \Delta, \quad \Gamma, B \Rightarrow \Delta}{\Gamma, A \to B \Rightarrow \Delta}$$

RIGHT

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}, \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B} \qquad \frac{\Gamma \Rightarrow A, \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B},$$

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \to B},$$

An *IL* proof of a formula A is a proof of the sequent $\Rightarrow A$. *The sequent size* of a proof S is the sum of $|\Gamma| + |\Delta|$ for sequents $\Gamma \Rightarrow \Delta$ in S. The sizes of formulas in S are not considered in the sequent size of S. The sequent size of a proof of A corresponds to the number of proof-lines in a Hilbert style proof of A.

3.2. Monotone interpolation for IL

As before, we shall now define *a characteristic set of clauses $\mathcal{C}_S$ for an IL proof S*. We shall consider only the right introduction rules of S. Recall that for a formula A, $\langle A\rangle$ denotes a new propositional variable. For any use of a right rule in S whose conclusion has the form

$$A_1, \dots A_k \Rightarrow B$$

we put in $\mathcal{C}_S$ the clause

$$\{\neg\langle A_1\rangle, \dots \neg\langle A_k\rangle, \langle B\rangle\}.$$

We can see that $\mathcal{C}_S$ is a set of Horn clauses, containing no negative clause. $|\mathcal{C}_S|$ is equal to the number of right inferences in S, and the total size of $\mathcal{C}_S$ is bounded by the sequent size of S.

We will now show that a truth assignment satisfying the set of characteristic clauses of a proof can be extended to a truth assignment satisfying the sequents in S. Let A be a formula. For the logical connectives $\circ = \wedge, \vee, \to$ the respective Boolean operations will be denoted $\circ_B = \wedge_B, \vee_B, \to_B$. Assume that σ is a truth assignment to variables $\langle B\rangle$ for all subformulas B of A. Then the assignment $\Theta_\sigma(A)$ will be defined as follows:

(1) $\Theta_\sigma(p) = \sigma\langle p\rangle$, for p a variable, $\Theta_\sigma(\bot) = 0$,
(2) $\Theta_\sigma(B \circ C) = \sigma\langle B \circ C\rangle \wedge_B (\Theta_\sigma(B) \circ_B \Theta_\sigma(C))$

We can see that for any σ

(i) $\Theta_\sigma(\bot) = 0$,
(ii) $\Theta_\sigma(A) = \sigma\langle A\rangle \wedge_B \Theta_\sigma(A)$, and
(iii) $\Theta_\sigma(A \circ B) \le \Theta_\sigma(A) \circ_B \Theta_\sigma(B)$.

Moreover, from (ii) we obtain that if σ satisfies the clause $\{\neg\langle A_1\rangle, \dots \neg\langle A_k\rangle, \langle A\rangle\}$ then

(iv) $\min_{i=1,\dots k} \Theta_\sigma(A_i) \le \sigma\langle A\rangle$.

We shall say that a sequent $\Gamma \Rightarrow \Delta$ *is satisfied* by Θ_σ iff $\min_{A\in\Gamma} \Theta_\sigma(A) \le \max_{A\in\Delta} \Theta_\sigma(A)$, where minimum of empty set is one and the maximum zero.

Lemma 15. *Let $S = \Pi_1, \dots \Pi_n$ be an IL proof.*

(1) *Let $B_1, \dots B_k$ and B be formulas. Let $\mathcal{C}_S, \{\langle B_1\rangle\}, \dots \{\langle B_k\rangle\}, \{\neg\langle B\rangle\}$ be unsatisfiable. Then*

$$\bigwedge_{i=1,\dots k} B_i \to B$$

is an IL tautology.

(2) *Let σ be an assignment to all variables $\langle B\rangle$ s.t. B is a subformula of some formula in S. Assume that σ satisfies $\mathcal{C}_S$. Then every Π_i in S is satisfied by Θ_σ.*

Proof. (1) is clear. (Compare with Lemma 2.)

(2). The axiom $A \Rightarrow A$ is satisfied trivially, and $\bot \Rightarrow A$ is satisfied because of the condition (i). Let us show that for a rule in S if its premise is satisfied by Θ_σ then so is its conclusion. For weakening and cut rule the statement holds trivially. As remarked in (iii), we have $\Theta_\sigma(A \circ B) \le \Theta_\sigma(A) \circ_B \Theta_\sigma(B)$. This implies that the left introduction rules are satisfied by Θ_σ, for any σ. Assume that σ satisfies $\mathcal{C}_S$ and let us have an instance of a right introduction rule in S. For example, let us take the rule

$$\frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \to B}.$$

Let $a := \min_{\gamma\in\Gamma} \Theta_\sigma(\gamma)$. By the assumption we have

$$\min(a, \Theta_\sigma(A)) \le \Theta_\sigma(B) \qquad (\star)$$

and we want to show that

$$a \le \Theta_\sigma(A \to B) = \sigma\langle A \to B\rangle \wedge_B (\Theta_\sigma(A) \to_B \Theta_\sigma(B)). \qquad (\star\star)$$

From $(\star)$ we have $a \le \Theta_\sigma(A) \to_B \Theta_\sigma(B)$. Since σ satisfies $\mathcal{C}_S$, it also satisfies the clause $\{\neg\langle\gamma\rangle, \gamma \in \Gamma, \langle A \to B\rangle\}$ and from (iv) we obtain that $a \le \sigma\langle A \to B\rangle$, which implies $(\star\star)$. The other rules are analogous. □

A formula α will be called *monotone*, if it contains only the connectives $\wedge$ and $\vee$.

Lemma 16. *Let S be an IL proof of the formula $\alpha \to (\beta_1 \vee \beta_2)$, where α is a monotone formula in variables $\overline{p}$. Let σ be a 0, 1-assignment to $\overline{p}$ s.t. α is true under σ. Let V_σ be the set of clauses of the form $\{\langle\gamma\rangle\}$, where γ is a subformula of α true under the assignment σ. Then*

$$\mathcal{C}_S, V_\sigma, \{\neg\langle\beta_1\rangle\}, \{\neg\langle\beta_2\rangle\}$$

is not satisfiable.

Proof. Assume that ρ is an assignment which satisfies $\mathcal{C}_S, V_\sigma, \{\neg\langle\beta_1\rangle\}, \{\neg\langle\beta_2\rangle\}$. We can assume that ρ is defined on all subformulas of formulas in S. From the definition of Θ_ρ we obtain that $\Theta_\rho(\alpha) = 1$, $\Theta_\rho(\beta_1) = \Theta_\rho(\beta_2) = 0$ and $\Theta_\rho(\alpha \to (\beta_1 \vee \beta_2)) = 0$. But that contradicts the previous Lemma. □

Theorem 17. *Let α be a monotone formula in variables $\overline{p}$ and of size k. Assume that S is an IL proof of the tautology*

$$\alpha \to \beta_1 \vee \beta_2.$$

Assume that the sequent size of S is n. Then there exist monotone circuits C_1 and C_2 of size $O(n^2 + k)$ in variables $\overline{p}$ s.t. the following are IL tautologies:

(1) $\alpha \to [C_1] \vee [C_2]$,
(2) $[C_1] \to \beta_1$, *and* $[C_2] \to \beta_2$.

Proof. Let V be the set of variables of the form $\langle\gamma\rangle$, where γ is a subformula of α. Let $q := \langle\beta_1\rangle$, $r := \langle\beta_2\rangle$. The total size of $\mathcal{C}_S$ is $\leq n$. Let C_q be a monotone circuit in variables V of size $O(n^2)$ s.t. for any assignment σ to V, $C_q = 1$ iff $\mathcal{C}, V_\sigma, \{\neg q\}$ is unsatisfiable, where $V_\sigma = \{\{v\} \in V; \sigma(v) = 1\}$. Let C_1 be the circuit obtained by substituting γ for $\langle\gamma\rangle$ in C_q. It is a monotone circuit in variables $\overline{p}$, and we can assume that it has size $O(n^2 + k)$. Similarly for C_r and C_2. The proof then proceeds like that of Theorem 4. □

3.3. A hard IL tautology

As in Section 2.5 we now use Theorem 17 to obtain hard *IL* tautologies.

Proposition 18. *Let $\beta_1 = \beta_1(\overline{p}, \overline{r_1})$ and $\beta_2 = \beta_2(\overline{q}, \overline{r_2})$ be propositional formulas, $\overline{p}$, $\overline{q}$, $\overline{r_1}$, $\overline{r_2}$ disjoint. Let $\overline{p} = p_1, \ldots p_k$ and $\overline{q} = q_1, \ldots q_k$. Assume that β_1 is monotone in $\overline{p}$ or β_2 is monotone in $\overline{q}$. Assume that*

$$\beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\neg\overline{p}, \overline{r_2})$$

is a classical tautology.

(1) *Then*

$$\bigwedge_{i=1,\ldots k} (p_i \vee q_i) \to (\neg\neg\beta_1 \vee \neg\neg\beta_2)$$

is IL-tautology.

(2) *If the tautology has IL proof of sequent size n then there exists a monotone circuit $C(\overline{p})$ of size $O((n^2 + k)$ which interpolates $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ and $\beta_1(\overline{p}, \overline{r_1})$.*

Proof. Let us first show that the formula is a tautology. The assumption $\bigwedge_{i=1,\ldots k}(p_i \vee q_i)$ can be transformed to an intuitionistically equivalent disjunction of conjunctions of the form

$$\bigwedge_{i\in M} p_i \wedge \bigwedge_{i\in N} q_i$$

such that $M \cup N = \{1, \ldots k\}$. Hence it is sufficient to show that for such M and N

$$\bigwedge_{i\in M} p_i \wedge \bigwedge_{i\in N} q_i \to (\neg\neg\beta_1 \vee \neg\neg\beta_2) \qquad (\star)$$

is an intuitionistic tautology. By Lemma 12 either $\bigwedge_{i\in M} p_i \to \beta_1$ or $\bigwedge_{i\in N} q_i \to \beta_2$ is a classical tautology. In the first case

$$\left(\bigwedge_{i\in M} p_i \to \neg\neg\beta_1\right)$$

is an intuitionistic tautology, since the double negation enables one to reproduce the classical proof in *IL*. The latter case is similar.

Part (2) follows from Theorem 17 in a similar way to the proof of Proposition 13. □

Corollary. *Let $\overline{p} = p_1 \ldots p_n$ and $\overline{q} = q_1, \ldots q_n$ and let $\overline{p}$, $\overline{q}$, $\overline{r}$, $\overline{s}$ be disjoint. Let*

$$\Theta_n^k := \bigwedge_{i=1,\ldots n} (p_i \vee q_i) \to (\neg \mathit{Color}_n^k(\overline{p}, \overline{s}) \vee \neg \mathit{Clique}_n^{k+1}(\overline{p}/\neg\overline{q}, \overline{r})).$$

Then Θ_n^k is an IL-tautology. If $k := \sqrt{n}$ then every IL-proof of the tautology Θ_n^k contains at least

$$2^{\Omega(n^{\frac{1}{4}})}$$

proof-lines.

Proof. As in Corollary of Proposition 14. Note that we omit the double negation in front of $\neg$*Clique* resp. $\neg$*Color*, since $\neg A$ and $\neg\neg\neg A$ are intuitionistically equivalent. □

Acknowledgment

Written at Mathematical Institute of the Czech Academy of Sciences, and with support from the grant IAA1019401.

References

[1] N. Alon, R. Boppana, The monotone circuit complexity of Boolean functions, Combinatorica 7 (1) (1987) 1–22.
[2] J. Avigad, Eliminating definitions and Skolem functions in first-order logic, ACM Transactions of Computational Logic V (N) (2002) 1–14.
[3] S.R. Buss, G.G. Mints, The complexity of the disjunction and existence properties in intuitionistic logic, Annals of Pure and Applied Logic 99 (1999) 93–104.
[4] S.R. Buss, P. Pudlák, On the computational content of intuitionistic propositional proofs, Annals of Pure and Applied Logic 109 (2001) 46–94.
[5] P. Hrubeš, Lower bounds for modal logics, Journal of Symbolic Logic 72 (3) (2007) 941–958.
[6] P. Hrubeš, A lower bound for intuitionistic logic, Annals of Pure and Applied Logic 146 (2007) 72–90.
[7] E. Jeřábek, Frege systems for extensible modal logics, Annals of Pure and Applied Logic 142 (2006) 366–379.
[8] M. Karchmer, On proving lower bounds for circuit size, in: Proceedings of Structure in Complexity, 8th Annual Complexity Conference, 1993, pp. 112–119.
[9] A.A. Razborov, Lower bounds on the monotone complexity of some Boolean functions, Soviet Mathematics Doklady 31 (1985) 354–357.

Further reading

[1] S.R. Buss, Polynomial size proofs of the propositional pigeonhole principle, Journal of Symbolic Logic 52 (1987) 916–927.
[2] J. Krajíček, Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, Journal of Symbolic Logic 62 (2) (1997) 457–486.
[3] G. Mints, A. Kojevnikov, Intuitionistic Frege systems are polynomially equivalent, Zapisky Nauchnych Seminarov POMI 316 (2004) 129–146.
[4] P. Pudlák, On the complexity of intuitionistic propositional calculus, Sets and Proofs, in: Logic Colloquium' 97, 1999, pp. 197–218.