Preprint, Institute of Mathematics, AS CR, Prague. 2007-12-15

Lower bounds for modal logics

Pavel Hrubeš*

January 2, 2007

Abstract

We give an exponential lower bound on number of proof-lines in the proof system K of modal logic, i.e., we give an example of K-tautologies $\psi_1, \psi_2, \ldots$ s.t. every K-proof of ψ_i must have a number of proof-lines exponential in terms of the size of ψ_i. The result extends, for the same sequence of K-tautologies, to the systems $K4$, Gödel-L'ob's logic, S and $S4$. We also determine some speed-up relations between different systems of modal logic on formulas of modal-depth one.

Keywords: proof complexity, modal logic, lower bound, monotone interpolation.

1 Introduction

The object of proof complexity is to determine how efficient various proof systems are in proving their theorems. This leads to the basic problem of finding lower bounds on sizes of proofs in the systems, which can be formulated as follows:

For a proof system Q and a function $g : \omega \to \omega$ find (or decide whether it exists) a sequence of Q-tautologies $\psi_1, \psi_2, \ldots$ such that for every $i \in \omega$ every Q-proof of ψ_i must have size at least $g(|\psi_i|)$.[1]

The answer to the problem, as well as its importance, will of course depend on the particular system Q and function g. For example, in the case of predicate calculus the problem has an affirmative solution for any recursive function g, and the lower bounds are even more radical if Q contains some arithmetic. In the case of weak proof systems, like propositional calculus, the problem is more subtle and much more difficult. For such systems, the question is to find an exponential (or at least superpolynomial) lower bound. Until now, such a lower

*The proof was obtained in Prague, Mathematical Institute of the Czech Academy of Science, under grant IAA1019401. The paper was completed in Munich, Ludwig-Maximilian University, under Marie-Curie scholarship

[1] $|\psi_i|$ means the size of ψ_i, i.e., the number of symbols in ψ_i. Likewise, the size of a proof is the total number of symbols in the proof.

bound has been proved only for artificial proof systems, namely resolution and Frege systems of bounded depth. The difficulty of the problem has the same reason which makes it particularly interesting: its connection to computational complexity and the question whether $NP = coNP$ (resp. $PSPACE = coNP$.) By the theorem of Cook and Reckhow, if we show that *every* propositional system has a superpolynomial lower bound then $NP \neq coNP$.

The proof system

In the main part of the paper we construct an exponential lower bound for the system of modal logic K. The system is obtained by adding the symbol for necessity, $\Box$, to propositional logic. Propositional logic is assumed to be formalised by the usual rules and axioms, having the general form of Frege rules. More precisely, a Frege rule is the rule

$$\frac{\psi_1(\overline{p}), \ldots \psi_k(\overline{p})}{\xi(\overline{p})},$$

where the formulas $\psi_1, \ldots \psi_k, \xi$ are propositional formulas (i.e., not containing $\Box$) s.t. every truth assignement of the propositional variables which satisfies all of $\psi_1(\overline{p}), \ldots \psi_k(\overline{p})$ satisfies also $\xi(\overline{p})$. An application of the rule is a substitution of formulas for the variables $\overline{p}$, the substituted formulas being arbitrary modal formulas. The specific set of Frege rules chosen will not affect the proof of lower bound. In addition, K has *the rule of generalisation*

$$\frac{\psi}{\Box\psi},$$

and the *axiom of distributivity*

$$\Box(\psi \rightarrow \xi) \rightarrow (\Box\psi \rightarrow \Box\xi).$$

The distributivity axiom has the key role in constructing the lower bound. In fact, we will show that every proof of the given tautology requires an exponential number of applications of the distributivity axiom in K. The other proof systems to which the result applies are extensions of K by other modal axioms, which will be specified in Section 6. The same lower bound is valid also in the case of $K4$, Gödel-Löb's logic, S and $S4$, by showing that the additional axioms do not lead to shortening of proofs on tautologies of modal depth one (as far as the number of distributivity axioms is concerned). The result does not apply to $K5$ and $S5$. In this case, it is shown that $K5$ and $S5$ have exponential speed-up over K on tautologies of modal-depth one (see Section 6.6). A recent application of the lower bound for K is a lower bound on the lengths of proofs in intuitionistic propositional logic, which will be given elsewhere.

All the logics to which the result applies are $PSPACE$-complete, while we are short of proving the same for $K5$ or $S5$ which are in NP. However, this is a mere coincidence. The hard tautologies which will be presented are tautologies of modal depth one. But the system K restricted only to formulas of modal depth one is also NP-complete.

The method of proof

The general strategy of the proof is the following: as we are not attempting to find lower bounds for Frege systems, we shall count only the applications of modal axioms in a proof. In fact, we will consider only the *number* of *axioms of distributivity* in a proof. In order to be able to find a lower bound on the number of applications of distributivity in a K-proof, we will work in the theory K_5^0 (introduced on page 4) which does not contain the distributivity axiom. We show that if Γ is the set of distributivity axioms used in K-proof of ψ then

$$\bigwedge \Gamma \to \psi$$

is a K_5^0-tautology. Hence, in order to show that n is a lower bound on the number of applications of distributivity in a proof of ψ, it is sufficient to show that for every set Γ of distributivity axioms s.t. $|\Gamma| < n$, $\bigwedge \Gamma \to \psi$ is not K_5^0-tautology. The theory K_5^0 has a very simple model theory, and this question is then resolved model-theoretically. In models of K_5^0 we interpret $\Box$ over a set $\mathcal{G}$, which is a set of sets of truth assignments. Distributivity axioms impose $\mathcal{G}$ to be closed on intersections and supersets, i.e., they require $\mathcal{G}$ to be a filter. In order to find a model in which $\bigwedge \Gamma \to \psi$ is false, it is sufficient to find $\mathcal{G}$ which looks like a filter enough to make the axioms in Γ true without making true ψ. It should be observed that the model construction is intimately related to Karchmer's formulation of the Razborov proof of lower bound on monotone circuit size, see [3].[2] (However, the proof was obtained without knowing Karchmer's approach.)

Monotone interpolation

The bound itself is not reached directly, but rather by showing that K has a form of *monotone interpolation*. The idea of monotone interpolation is to apply the seminal results in circuit complexity of Razborov [5], and Alon-Boppana [1] and others, to proof-complexity. Alon and Boppana have shown that every monotone circuit C (i.e., a circuit which contains only $\wedge$-gates, $\vee$-gates and no $\neg$-gates) which separates the set of $k+1$-colorable graphs, $Color_{k+1}$, and graphs with clique of size k, $Clique_k$, (i.e., it is a circuit which outputs 1, if the graph is $k+1$-colorable, 0, if the graph has k-clique, and anything if neither applies) must be of exponential size. The implication

($\star$) *"if a graph has a clique of size $k+1$ then it is not k-colorable"*

can be formulated as a propositional tautology. Hence in order to find an exponential lower bound for a propositional proof system P, it is sufficient to show that from a P-proof of ($\star$) of size n one can extract a monotone circuit of size polynomial in n separating $Color_{k+1}$ and $Clique_k$. This approach has been first applied by Krajíček [4] to obtain a lower bound for resolution. In the case of K, we rephrase ($\star$) by inserting $\Box$ here and there to obtain a modal tautology (see Theorem 14 for the exact formulation), and we show that every

[2] This connection is made more explicit in Remark on page 7.

K-proof of the modified $(\star)$ with n distributivity axioms gives a monotone circuit separating $Color_{k+1}$ and $Clique_k$ of size approximately n^2. This is achieved by representing the model-theoretic content of distributivity axioms used in a proof by a so called *flowgraph*, and by observing that flowgraphs can be simulated by monotone circuits.

As remarked above, the proof of monotone interpolation for K employs the same general approach as the proof of monotone lower bound for circuits. The proof could hence be carried out directly, by repeating the proof of Alon and Boppana, without an explicit reference to it.

I worked on the problem of lower bounds for modal logic with Pavel Pudlák and Joost Joosten, to whom I am thankful for introducing me to the problematics as well as for invaluable help.

2 Theory K_5^0

Theory K_5^0

The theory K_5^0 will have, in addition to the propositional rules, the rules of *generalisation* and *transparency*

$$(G) \qquad \frac{\psi}{\Box\psi}, \qquad\qquad (T) \qquad \frac{\psi \equiv \xi}{\Box\psi \equiv \Box\xi}$$

and the axiom scheme

$$(V) \qquad \Box((\psi_1 \wedge \Box\xi) \vee (\psi_2 \wedge \neg\Box\xi)) \equiv (\Box\psi_1 \wedge \Box\xi) \vee (\Box\psi_2 \wedge \neg\Box\xi)$$

The axiom scheme expresses the $K5$ property that modalised formulas have truth-values independent on a possible world - thence the notation K_5^0.[3] The axiom allows us to transform any formula to a formula of modal depth one, i.e., with no nested modalities:

Proposition 1 *For any formula ψ there exists a formula ψ' of modal-depth one s.t.*

$$K_5^0 \vdash \psi \equiv \psi'.$$

`Proof.` Assume, for simplicity, that $\psi = \Box\xi$ and that there is a propositional formula η s.t. every $\Box$ occurring in ξ occurs as $\Box\eta$. ξ is, by means of propositional rules only, equivalent to

$$(\lambda_1 \wedge \Box\eta) \vee (\lambda_2 \wedge \neg\Box\eta)$$

for some propositional formulas λ_1, λ_2. By transparency

$$K_5^0 \vdash \Box\xi \equiv \Box((\lambda_1 \wedge \Box\eta) \vee (\lambda_2 \wedge \neg\Box\eta)).$$

[3]Note that we cannot use the usual $K5$ formulation because we do not have distributivity.

Hence, by (V),

$$K_5^0 \vdash \Box\xi \equiv (\Box\lambda_1 \wedge \Box\eta) \vee (\Box\lambda_2 \wedge \neg\Box\eta),$$

where $(\Box\lambda_1 \wedge \Box\eta) \vee (\Box\lambda_2 \wedge \neg\Box\eta)$ has modal-depth one. The general proof is carried out easily by induction. `QED`

Models for K_5^0

Let U denote the set of all possible truth assignments of propositional variables (i.e., U is infinite). Let $\mathcal{G} \subseteq P(U)$ be fixed. For $v \in U$ and a modal formula ψ we define that

$$v \Vdash \psi$$

by induction as follows:

1. For a variable p, $v \Vdash p$, if p is assigned 1 in v.
2. We let $v \Vdash \psi_1 \wedge \psi_2$ iff $v \Vdash \psi_1$ and $v \Vdash \psi_2$. We let $v \Vdash \neg\psi$ iff not $v \Vdash \psi$, and similarly for other connectives.
3. Finally, assume that the relation $u \Vdash \psi$ has been defined for any $u \in U$. Let
$$[\psi] := \{u \in U; u \Vdash \psi\}.$$
Then let $v \Vdash \Box\psi$ iff $[\psi] \in \mathcal{G}$.

Let $v \in U$, $\mathcal{G} \subseteq P(U)$. The pair $\langle v, \mathcal{G}\rangle$ is *a model for* K_5^0, if $U \in \mathcal{G}$. (The requirement $U \in \mathcal{G}$ corresponds to the rule of generalisation.) We write that $\langle v, \mathcal{G}\rangle \models \psi$, if $v \Vdash \psi$. Note that if every variable in ψ occurs only in modal context (for such a formula we say it is *purely modal*), the fact whether $\langle v, \mathcal{G}\rangle \models \psi$ is independent on v and we may also write simply $\mathcal{G} \models \psi$.

Theorem 2 *K_5^0 is sound and complete with respect to K_5^0 models, i.e., for every formula ψ, $K_5^0 \vdash \psi$ iff for every K_5^0 model M, $M \models \psi$.*

`Proof.` The soundness part is easy. For the completeness part it is sufficient to prove that for every consistent formula ψ (i.e., $K_5^0 \nvdash \psi$) there exists a model M s.t. $M \models \psi$.

STEP 1. By Proposition 1 we can assume that ψ has modal-depth one.

STEP 2. Let $r_1, \ldots r_n$ be the list of variables which occur in ψ in non-modal context. For an assignment σ of the variables $r_1, \ldots r_n$, let ψ^σ denote the formula obtained by replacing every non-modal occurrence of r_i by $\sigma(r_i)$, $i = 1, \ldots n$. Since ordinary propositional rules are in K_5^0, there exists some assignment σ s.t. ψ^σ is consistent. Clearly, if we have $\mathcal{G}$ s.t. $\mathcal{G} \models \psi^\sigma$ then $\langle \sigma, \mathcal{G}\rangle \models \psi$. Therefore we can assume that ψ is a purely modal formula.

STEP 3. Assume that ψ is a purely modal formula of modal depth one. By means of propositional logic only, we can transform it to an equivalent DNF formula, i.e. a formula which is a disjunction of formulas of the form

$$\Box\psi_1 \wedge \Box\psi_n \wedge \neg\Box\xi_1 \wedge \dots \neg\Box\xi_m.$$

Since ψ is consistent then at least one of the disjuncts is consistent. For such a disjunct η of the depicted form, we let $\mathcal{G} := \{[\psi_i]; i = 1, \dots n\} \cup \{U\}$. Let us show that $\mathcal{G} \models \eta$. From the definition of $\mathcal{G}$, $\mathcal{G} \models \Box\psi_i$, $i = 1, \dots n$. Assume that $\mathcal{G} \not\models \neg\Box\xi_j$ for some $j = 1, \dots m$. Then $[\xi_j] \in \mathcal{G}$. But then either $[\xi_j] = U$ or there is $i = 1, \dots n$ s.t. $[\xi_j] = [\psi_i]$. In the former case ξ_i is a propositional tautology and in the latter $K_5^0 \vdash \xi_j \equiv \psi_i$. In both cases $K_5^0 \vdash \Box\psi_i \to \Box\xi_j$, which contradicts the assumption that η is consistent. `QED`

3 An approach to lower bounds

The theory K is the theory which, in addition to the propositional rules, has a) the rule of generalisation, and b) the axiom of distributivity

$$\Box(\psi \to \xi) \to (\Box\psi \to \Box\xi).$$

Proposition 3 *Let ψ be K-tautology.*

(1) Let Γ be the set of distributivity axioms occurring in a proof of ψ. Then

$$\bigwedge\Gamma \to \psi$$

is a K_5^0-tautology.

(2) Assume that for every set Γ of distributivity axioms s.t. $|\Gamma| < k$, the formula

$$\bigwedge\Gamma \to \psi$$

is not a K_5^0-tautology. Then every K proof of ψ contains at least k axioms of distributivity.

`Proof.` (1) Assume the opposite. Then, by completeness of K_5^0, we have a model $M = \langle v, \mathcal{G}\rangle$ s.t. $M \models \bigwedge\Gamma$ but $M \not\models \psi$. Let S be the proof of ψ. It is sufficient to prove by induction that

for every $u \in U$ and a formula η in S, $u \Vdash \eta$.

Consider the possible alternatives. a) For an axiom of propositional logic the statement holds, and an application of a propositional rule retains the property. b) An element of Γ is true in M by the assumption. Since distributivity axioms are purely modal formulas then they are true in every $u \in U$ as well. c) Assume

that generalisation is applied to ψ. By the assumption, for every $u \in U$, $u \Vdash \psi$. Hence $[\psi] = U$ and therefore $\mathcal{G} \models \Box\psi$. d) Similarly for the transparency rule.

(2) trivially follows. QED

Note that if $\psi \equiv \xi$ is a K_5^0 tautology then in general we need two distributivity axioms to prove $\Box\psi \equiv \Box\xi$ in K. But those distributivity axioms, as following straight from the transparency rule, will be omitted in Proposition 3.

In terms of $\mathcal{G}$, distributivity axiom corresponds to the condition

$$(\star) \qquad -X \cup Y \in \mathcal{G},\ X \in \mathcal{G} \ \rightarrow \ Y \in \mathcal{G}.$$

A set

$$\Lambda \subseteq P(U)^2$$

will be called a *set of distributivity conditions*. We shall say that $\mathcal{G}$ is *distributive on* Λ iff every $\langle X, Y\rangle \in \Lambda$ satisfies the condition $(\star)$.

If Γ is a set of distributivity axioms of modal depth one, the set of corresponding conditions Λ is defined as follows: for every distributivity axiom of the form

$$\Box(\psi \rightarrow \xi) \rightarrow (\Box\psi \rightarrow \Box\xi)$$

we put

$$\langle [\psi], [\xi]\rangle$$

in Λ.

Clearly, if $\mathcal{G}$ is distributive on Λ, then every distributivity axiom in Γ is true in $\langle v, \mathcal{G}\rangle$, v arbitrary. For if $\mathcal{G} \models \Box(\psi \rightarrow \xi)$ and $\mathcal{G} \models \Box\psi$ then $[\psi \rightarrow \xi] = -[\psi] \cup [\xi] \in \mathcal{G}$ and $[\psi] \in \mathcal{G}$. Then, by $(\star)$, $[\xi] \in \mathcal{G}$ and hence $\mathcal{G} \models \Box\xi$.

Remark. Note that the condition $(\star)$ can be replaced by an equivalent pair of conditions of the form

$$(\star\star) \qquad X, Y \in \mathcal{G} \ \rightarrow \ X \cap Y \in \mathcal{G}, \qquad\qquad X \in \mathcal{G},\ X \subseteq Y \ \rightarrow \ Y \in \mathcal{G}.$$

Hence distributivity axioms can be seen as requiring $\mathcal{G}$ to be a filter. In our lower-bound we shall construct $\mathcal{G}$ which is a filter enough to satisfy the distributivity axioms used in a (hypothetical) proof of a tautology ψ without making ψ true.

If we demand $\mathcal{G}$ to be distributive on the whole $P(U)^2$ then $\mathcal{G}$ is a filter. Restricting U to a set $U_{\overline{p}}$ of assignments of a finite set of variables $\overline{p}$ then $U_{\overline{p}}$ is finite and $\mathcal{G}$ restricted to $U_{\overline{p}}$ is a trivial filter, i.e., generated by a single set $M \subseteq U_{\overline{p}}$. In that case the K_5^0 model $\langle v, \mathcal{G}\rangle$ coincides with the $K5$ model $\langle v, M\rangle$.

The following is a simple but nevertheless a very important lemma:

Lemma 4 *For a formula η, let η' denote the formula obtained by deleting all boxes in η. Furthermore, let $\eta^\star$ be the formula obtained by deleting every $\Box$ in η which is in a range of another box. Then:*

(1) If ψ is K-tautology then ψ' is a propositional tautology.

(2) If ψ is K-tautology then $\psi^\star$ is K-tautology. Moreover, if ψ has K-proof S with n distributivity axioms then $\psi^\star$ has K-proof S' s.t. i) S' contains at most n distributivity axioms and ii) all formulas in S' have modal-depth one.

`Proof.` (1) is clear.

(2) Let $S = \eta_1 \dots \eta_n$, $\eta_n = \psi$, be K-proof of ψ and let Γ be the set of distributivity axioms occurring in S. We see that if η is an axiom of distributivity then $\eta^\star$ is also such. Hence $\Gamma^\star := \{\gamma^\star; \gamma \in \Gamma\}$ is also a set of distributivity axioms. Let $S^\star = \eta_1^\star \dots \eta_n^\star$. We must show by induction that every $\eta_i^\star$, $i = 1, \dots n$, is provable in K by a proof with formulas of modal depth one using just the distributivity axioms in $\Gamma^\star$. Clearly, the only non-trivial step is when η_j is obtained from η_i, $i < j$ by generalisation. Assume then that $\eta_j = \Box\eta_i$ has been obtained as

$$\frac{\eta_i}{\Box\eta_i}.$$

We have $(\eta_j)^\star = (\Box(\eta_i)^\star) = \Box\eta_i'$. Since η_i is K-tautology then by part (1) η_i' is a propositional tautology. Therefore we can prove $\Box\eta_i'$ first by proving η_i', using just propositional rules, and then applying generalisation

$$\frac{\eta_i'}{\Box\eta_i'}.$$

Hence no distributivity is needed to prove $\Box\eta_i' = (\eta_j)^\star$. `QED`

Proposition 5 *Let ψ be a K-tautology of modal depth one. Assume that it has K-proof S with n distributivity axioms. Then ψ has a K-proof S' s.t. i) S' contains n distributivity axioms ii) all the distributivity axioms in S' have modal depth one.*

`Proof.` Immediately follows from the previous lemma. `QED`

The following is then an easy consequence of Proposition 3:

Theorem 6 *Let ψ be a K-tautology of modal depth one. Assume that for every set of distributivity conditions Λ s.t $|\Lambda| < k$ there exists $\mathcal{G}$ distributive on Λ and a corresponding model s.t. $\langle v, \mathcal{G}\rangle \not\models \psi$. Then every K proof of ψ contains at least k axioms of distributivity.*

`Proof.` Assume the contrary. Then we have a K-proof S of ψ with less than k axioms of distributivity. By the previous proposition, we can assume that all the formulas in ψ, and hence also the distributivity axioms, have modal-depth one. Let Λ be the set of conditions corresponding to Γ, the distributivity axioms in S. By the assumption, we can find $\langle v, \mathcal{G}\rangle$ s.t. $\mathcal{G}$ is distributive on Λ and $\langle v, \mathcal{G}\rangle \not\models \psi$. But hence $\langle v, \mathcal{G}\rangle \models \bigwedge\Gamma$ and $\langle v, \mathcal{G}\rangle \not\models \bigwedge\Gamma \to \psi$ which contradicts Proposition 3. `QED`

4 Monotone interpolation for K

For a propositional formula $\alpha(\overline{p}, \overline{r})$, $\alpha(\Box\overline{p}, \overline{r})$ will denote the formula obtained from α by replacing all variables $p \in \overline{p}$ by $\Box p$. A modality-free formula α will be called *monotone*, if the only logical connectives occurring in α are $\wedge$ and $\vee$. If we have a monotone formula α containing exactly the variables $\overline{p}$ and a modality-free formula β s.t. $\alpha \to \beta$ is a tautology then also

$$(\star) \qquad \alpha(\Box\overline{p}) \to \Box\beta$$

is a modal tautology. The obvious strategy for proving $(\star)$ is to start with the atoms of α and then expand the boxes in α upwards by changing $\Box\psi_1 \wedge \Box\psi_2$ resp. $\Box\psi_1 \vee \Box\psi_2$ to $\Box(\psi_1 \wedge \psi_2)$ resp. $\Box(\psi_1 \vee \psi_2)$. Hence we have obtained $\Box\alpha$ and we proceed by one application of distributivity on $\Box(\alpha \to \beta)$. In this way, we needed at least as many distributivity axioms as there are connectives in α (when the circuit size of α is considered.) This process could be made - with respect to the distributivity axioms - more efficient if we first transformed $\alpha(\Box\overline{p})$ to a formula of a smaller monotone circuit size by means of pure propositional logic and applied the described procedure to the simplified formula. For example, we can transform $\alpha(\Box\overline{p})$ either to a CNF or a DNF form which may have very different sizes. We will now prove that such a strategy is the most efficient in proving the implication, that any proof of $(\star)$ contains at least as many axioms of distributivity as is the size of the smallest monotone interpolant of α and β.

We shall say that a circuit $C(\overline{p})$ *interpolates* $\alpha(\overline{p})$ and $\beta(\overline{p}, \overline{r})$ iff for any assignment σ of $\overline{p}$

1. if $\alpha(\overline{p})$ is true then $C(\overline{p}) = 1$ and
2. if $C(\overline{p}) = 1$ then for every assignment of $\overline{r}$ $\beta(\overline{p}, \overline{r})$ is true.

The size of a circuit is the number of its gates.

It is easy to show that if there is a monotone interpolant of α and β of size n, then $\alpha(\Box\overline{p}) \to \Box\beta$ has a proof with $o(n)$ distributivity axioms. We are now going to prove the following:

Theorem 7 *Let α be a monotone formula containing exactly the variables $\overline{p}$ and let β be a modality-free formula. Assume that*

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

has an K proof with n distributivity axioms. Then there is a monotone circuit of size $\leq o(n^2)$ which interpolates α and β.

Note: we do not restrict the variables occurring in β in any way.

We first introduce some concepts:

Flowgraphs

A flowgraph M is a directed labeled graph with the following properties:

1. The labels of vertices are unique and some vertices are labeled by variables $p_1, \dots p_n$ and the constant 1.
2. for every edge $\langle a, b\rangle$ in M there exists a vertex a' s.t. $\langle a', b\rangle$ is also an edge in M and both the edges are labeled $\wedge\{a, a'\}$. Such a pair will be called a $\wedge$-*gate* and we shall write that $b = a \wedge a'$.

A flowgraph will be called *acyclic*, if the underlying graph is acyclic.
The size of M will be the number of gates in M.

For an assignment σ of variables $\overline{p}$, *a possible solution* of a flowgraph M is an assignment v of the vertices of M by $0, 1$ s.t.

1. $v(1) = 1$, and if $\sigma(p_i) = 1$ then $v(p_i) = 1$, $i = 1, \dots n$,
2. for every $\wedge$-gate $\langle a, b\rangle$ $\langle a', b\rangle$, if $v(a) = 1$ and $v(a') = 1$ then $v(b) = 1$.

The solution of M for σ is the assignment V_σ^M of M s.t. for every vertex a, $V_\sigma^M(a) = 0$, if there exists a possible solution v s.t. $v(a) = 0$, and $V_\sigma^M(a) = 1$ otherwise. I.e. V_σ^M is the minimum possible solution of M for σ. (Where no confusion is possible, the superscript M will be omitted.)

Hence a vertex b (which is not a variable or 1) is assigned 1 in V_σ iff there exists at least one $\wedge$-gate $b = a \wedge a'$ such that $V_\sigma(a) = 1$ and $V_\sigma(a') = 1$. Thus there is an immediate connection between acyclic flowgraphs and monotone circuits: a circuit $b = \bigvee_{i=1,\dots n} a_i \wedge a_i'$ corresponds to the flowgraph in which there are n $\wedge$-gates $b = a_i \wedge a_i'$. I.e., a circuit $\wedge$-gate corresponds to a flowgraph $\wedge$-gate, and an $\vee$-gate has its counterpart in the multiplicity of $\wedge$-gates with a single output.

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

Proposition 8 *Let M be a flowgraph of size n. Let a be a vertex in M. Then there exists a monotone circuit C_a of size $o(n^2)$ s.t. for every assignement σ of $\overline{p}$*

$$C_a(\sigma(\overline{p})) = 1 \qquad \equiv \qquad V_\sigma(a) = 1.$$

`Proof.` STEP 1. For flowgraphs M and N and a vertex a, which is vertex both in M and N, we say that N *simulates M on a* if for every assignement σ of $\overline{p}$, $V_\sigma^M(a) = V_\sigma^N(a)$. First, it must be shown that for every flowgraph M of size n and a vertex a of M there exists an acyclic flowgraph M' of size $o(n^2)$ s.t. M' simulates M on a.

The construction proceeds as follows: let M have k vertices $a_1, \dots a_k$ and n gates (so $k \leq 2n$, as we can assume that there are no isolated vertices in M.) For every vertex a_j $j = 1, \dots k$, we introduce k copies $a_j^1, \dots a_j^k$. The flowgraph M' will have k^2 vertices a_j^i, $i, j = 1, \dots k$ and the gates will be defined as follows:

1. For every $j = 1, \ldots k$ label a^1_j by $p \in \overline{p}$ resp. 1 provided a_j was labelled by p resp. 1 in M.

2. For every $j = 1, \ldots k$ and for every i, $1 \leq i < k$ we put in M' a double edge from a^i_j to a^{i+1}_j s.t. it forms $\wedge$-gate $a^{i+1}_j = a^i_j \wedge a^i_j$.

3. For every $i = 1, \ldots k-1$ and $j_1, j_2 = 1, \ldots k$, we connect $a^i_{j_1}$ and $a^i_{j_2}$ by $\wedge$-gate to a^{i+1}_j, provided there is $\wedge$-gate from a_{j_1}, a_{j_2} to a_j in M.

Finally, we identify vertices the vertex $a = a_j$ of M with its copy a^k_j in M'. It is easy to see that M' simulates M on a. The size of M' is $n.k \sim o(n^2)$.

STEP 2. Second, it is sufficient to prove that for an acyclic flowgraph M of size n and a vertex a of M there is a monotone circuit C_a of the desired properties of size $2n$. The above construction automatically gives a flowgraph s.t. every node labelled by a p or 1 is a leaf and we shall assume also this property in M. To a leaf which is labeled by a variable p or 1 assign the circuit p resp. 1 and to a leaf of a different kind an empty circuit. Assume that for a vertex b we have assigned circuits to source nodes of all gates with an output node b. First, delete all gates s.t. at least one of their source nodes has been assigned empty circuit. If there is no gate left, assign b an empty circuit. Otherwise, let $\langle c_1, d_1\rangle, \ldots \langle c_n, d_n\rangle$ be the input nodes of $\wedge$-gates with output b. Then assign to b the circuit $(c_1 \wedge d_1) \vee \ldots \vee (c_n \wedge d_n)$.

QED

Flowgraphs for distributivity axioms.

For a set Γ of distributivity axioms of modal-depth one let $\Lambda \subseteq P(U)^2$ be the corresponding set of distributivity conditions (see page 7). *A flowgraph for* Λ (or Γ) is a flowgraph whose vertices are labeled by subsets of U and defined as follows:

1. put all $[p_1], \ldots [p_n]$, U to M,

2. put the vertices a, a', b in M and form a gate $b = a \wedge a'$ iff there exists $\langle X, Y\rangle \in \Lambda$, $a = X$, $a' = -X \cup Y$ and $b = Y$.

In the definition, we identify variables $p_1, \ldots p_n$ with their extensions $[p_1], \ldots [p_n]$ and the constant 1 with U.

The following two lemmas give the key properties of flowgraphs for distributivity axioms.

Lemma 9 *Let Λ be a set of conditions and M a flowgraph for Λ. Let ψ be a modality-free formula. Assume that a vertex in M is labeled by $[\psi]$. Let σ be an assignement of $\overline{p}$ and assume that $V_\sigma([\psi]) = 1$. Then*

$$K \vdash \bigwedge_{\sigma(p_i)=1} \Box p_i \to \Box\psi$$

`Proof.` Straight from the definition. `QED`

Lemma 10 *Let Λ be a set of conditions and M a flowgraph for Λ. Let ψ be a modality-free formula. Assume that a vertex in M is labeled by $[\psi]$. Let σ be an assignement of $\overline{p}$ and assume that $V_\sigma([\psi]) = 0$. Then there exists $\mathcal{G}$ distributive on Λ s.t. $\mathcal{G} \models \Box p_i$, for every p_i s.t. $\sigma(p_i) = 1$, and $\mathcal{G} \not\models \Box\psi$.*

`Proof.` It is sufficient to define $\mathcal{G} := \{X \subseteq U; V_\sigma(X) = 1\} \cup \{U\}$. `QED`

Note that by virtue of Lemma 9, in Lemma 10 we have that also $\mathcal{G} \models \neg\Box p_i$, if $\sigma(p_i) = 0$.

Proof of Theorem 7.

Let Γ be the set of distributivity axioms used in the proof of

$$\alpha(\Box\overline{p}) \to \Box\beta.$$

Let $|\Gamma| = n$. By Proposition 5 we can assume that formulas in Γ are of modal depth one. Let Λ be the corresponding set of conditions. Then $|\Lambda| \leq n$. Let M be the flowgraph for Λ. Again, the size of the flowgraph is $\leq n$. We can assume that there is a vertex in M labeled $[\beta]$, otherwise no distributivity has been applied to β in the proof, β is a propositional tautology and the statement is trivial. By the Proposition 8 we can find a monotone circuit C of size $\leq o(n^2)$ s.t. for any assignement σ

$$C(\sigma(\overline{p})) = 1 \quad \equiv \quad V_\sigma([\beta]) = 1.$$

Let us show that C interpolates α and β. Let σ be an assignement s.t. $\alpha(\sigma(\overline{p}))$ is true. Assume that $C(\sigma(\overline{p})) = 0$. Then also $V_\sigma([\beta]) = 0$ and so by Lemma 10 we can find a model $\mathcal{G}$ s.t. $\mathcal{G} \models \Gamma$, $\mathcal{G} \not\models \Box\beta$ and for every p_i, if $\sigma(p_i) = 1$ then $\mathcal{G} \models \Box(p_i)$. But if σ satisfies α then $\mathcal{G} \models \alpha(\Box\overline{p})$. Hence

$$\mathcal{G} \not\models \bigwedge\Gamma \to (\alpha(\Box\overline{p}) \to \Box\beta),$$

which is impossible since $\bigwedge\Gamma \to (\alpha(\Box\overline{p}) \to \Box\beta)$ is K_5^0-tautology.

Assume that σ is an assignement s.t $C(\sigma(\overline{p})) = 1$. Then $V_\sigma([\beta]) = 1$ and by Lemma 9

$$\bigwedge_{\sigma(p_i)=1} \Box p_i \to \Box\beta$$

is a K-tautology. But hence also

$$\bigwedge_{\sigma(p_i)=1} p_i \to \beta$$

is a propositional tautology. Therefore $\beta(\sigma(\overline{p}), \overline{r})$ is a propositional tautology and satisfied by any assignement of $\overline{r}$.

Hence C interpolates α and β. `QED`

A generalisation of Theorem 7

For the purpose of a later reference we state here a generalisation of Theorem 7. The proposition will not be used elsewhere in this paper.

Proposition 11 *Let α, β_1 and β_2 be propositional formulas. Assume that α is a monotone formula and that it contains exactly the variables $\overline{p}$, and that β_1 resp. β_2 contain variables $\overline{p}, \overline{s_1}$ resp $\overline{p}, \overline{s_2}$. Assume that*

$$\alpha(\Box\overline{p}) \rightarrow \Box\beta_1 \vee \Box\beta_2$$

has a K-proof with n distributivity axioms. Then there exist monotone circuits $C_1(\overline{p})$ and $C_2(\overline{p})$ of size $o(n^2)$ s.t. for any assignement σ of $\overline{p}$

(1) if α is true then $C_1(\overline{p}) = 1$ or $C_2(\overline{p}) = 1$,

(2) if $C_1(\overline{p}) = 1$ then β_1 is true (for any assignement of the variables $\overline{s_1}$), and if $C_2(\overline{p}) = 1$ then β_2 is true (for any assignement of the variables $\overline{s_2}$).

`Proof.` The proof is a straightforward generalisation of the proof of Theorem 7. Part (1) follows from Lemma 9 and part (2) from Lemma 10. `QED`

A different modification of Theorem 7 could be obtained by weakening the monotonicity assumption of α. The monotonicity requirement demands that neither $\neg\Box p$ nor $\Box\neg p$ occur in α. However, no substantial modification of the proof would be required if the later assumption was dropped. In that case of course, the circuit obtained would no longer be monotone.

5 The hard tautology

A propositional formula α in variables $\overline{p}, \overline{r}$ will be called *monotone in* $\overline{p}$, if the formula when transformed to a DNF form does not contain a negation of any variable in $\overline{p}$.

For a propositional formula $\psi(\overline{p}, \overline{r})$, $\bigvee_{\overline{r}} \psi(\overline{p}, \overline{r})$ will denote the disjunction of all formulas of the form $\psi(\overline{p}, \sigma(\overline{r}))$, where σ is an assignement of the variables $\overline{r}$.

Lemma 12 *Let ψ be K-tautology and let the variables $\overline{r} = r_1, \ldots r_j$ not occur in ψ in a modal context. Assume that ψ has a K-proof S with n distributivity axioms. Then there exists a K-proof $S^\star$ of ψ with n distributivity axioms s.t. the variables $\overline{r}$ do not occur in S in a modal context.*

`Proof.` Let $S = \psi_1, \ldots \psi_k$, where $\psi_k = \psi$. Let the set of distributivity axioms in S be Γ, $|\Gamma| = n$. Let $\overline{q} = q_1, \ldots q_j$ be a set of auxiliary variables. For a formula η, let $\eta^\star$ denote the formula obtained by replacing the modalised occurrences of variables $\overline{r}$ by $\overline{q}$ in the respective order. Hence $\psi^\star = \psi$. Let $\Gamma^\star := \{\gamma^\star, \gamma \in \Gamma\}$.

It should be proved by induction with respect to i, $i = 1, \dots k$, that $\psi_i^\star$ has K-proof S_i s.t. a) the variables $\overline{r}$ do not occur in S_i in a modal context and b) all distributivity axioms in the proof are elements of $\Gamma^\star$. Clearly, the only non-trivial steps are when ψ_i was obtained from ψ_l, $l < i$, by generalisation rule. Assume that $\psi_i = \Box\psi_l$ was obtained as

$$\frac{\psi_l}{\Box\psi_l}.$$

Assume that $\psi_l^\star$ has a proof S_l of the desired properties. Let us show that also $\psi_i^\star = (\Box\psi_l)^\star$ has such a proof. Let $\eta := \psi_l(\overline{r}/\overline{q})$. Then $\psi_i^\star = \Box\eta$. Let T be the proof obtained by replacing $\overline{r}$ by $\overline{q}$ in S_i. Hence T is a proof of η with no occurrence of $r \in \overline{r}$ and therefore with all distributivity axioms in $\Gamma^\star$. The proof S_i of $\psi_i^\star = \Box\eta$ can then be obtained by adding generalisation

$$\frac{\eta}{\Box\eta}$$

to T. QED

Theorem 13 *Let $\alpha(\overline{p}, \overline{r})$ be a monotone formula 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 $\bigvee_{\overline{r}} \alpha(\overline{p}, \overline{r})$ and $\beta(\overline{p}, \overline{s})$.

Proof. (1) Clearly, it is sufficient to prove that for every assignement σ of variables $\overline{r}$, $\alpha(\Box\overline{p}, \sigma(\overline{r})) \to \Box\beta$ is a K-tautology. Hence it is sufficient to prove that if α is a monotone formula and

$$\alpha \to \beta$$

is a propositional tautology then also

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

is a K-tautology. But that has been explained on page 9.

(2) Let $\gamma(\overline{p}) := \bigvee_{\overline{r}} \alpha(\overline{p}, \overline{r})$. Let us show that γ and β have an interpolant C of size $o(n^2)$. By Theorem 7, it is sufficient to prove that

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

has a proof with at most n axioms of distributivity.

Let S be a proof of $\alpha(\Box\overline{p},\overline{r}) \rightarrow \Box\beta(\overline{p},\overline{s})$ and Γ the set of distributivity axioms occurring in it, $|\Gamma| = n$. By the previous Lemma we can assume that the variables $\overline{r}$ do not occur in Γ. For an assignement σ of $\overline{r}$, let S^σ denote the proof obtained by replacing $\overline{r}$ by $\sigma(\overline{r})$ in S. Then for any such σ, S^σ is a proof of $\alpha(\Box\overline{p},\sigma(\overline{r})) \rightarrow \Box\beta(\overline{p},\overline{s})$ and all the distributivity axioms it contains are in Γ (for elements of Γ do not contain $\overline{r}$). All the proofs S^σ can be joint to a proof of

$$\gamma(\Box\overline{p}) \rightarrow \Box\beta(\overline{p},\overline{s}).$$

The set of distributivity axioms in the proof is again Γ. QED

Let

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

be the proposition asserting that $\overline{r}$ is 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 $\overline{p}$. To be exact, $\overline{p} = p_{i_1 i_2}, i_1, i_2 = 1,\ldots n$, $\overline{r} = r_{ij}, \overline{s} = s_{ij}, i = 1,\ldots n, j = 1,\ldots k$. $Clique_n^k(\overline{p},\overline{r})$ is the formula

$$\bigwedge_j \bigvee_i r_{ij} \wedge \bigwedge_i \bigwedge_{j_1 \neq i_2} (\neg r_{ij_1} \vee \neg r_{ij_2}) \wedge \bigwedge_{i_1 \neq i_2, j_1, j_2} (r_{i_1 j_1} \wedge r_{i_2 j_2} \rightarrow p_{i_1 i_2})$$

and $Color_n^k(\overline{p},\overline{s})$ is the formula

$$\bigwedge_i \bigvee_j s_{ij} \wedge \bigwedge_{i_1, i_2, j} (p_{i_1 i_2} \rightarrow (\neg s_{i_1 j} \vee \neg s_{i_2 j})),$$

where the indeces i range over $1,\ldots n$ and j over $1,\ldots k$.

Theorem 14 *Let*

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

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

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

distributivity axioms.

Proof. Assume that Θ_n^k has a K-proof with m distributivity axioms. By the previous lemma, there is a monotone interpolant C of $\bigvee_{\overline{r}} Clique_n^k(\overline{p},\overline{r})$ 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 $m \sim \sqrt{2^{\Omega(n^{\frac{1}{4}})}} \sim 2^{\Omega(n^{\frac{1}{4}})}$. QED

Remark. A hard tautology of quite a different form could be obtained from the following proposition (which is an immediate corollary of Theorem 7):

Assume that $\alpha(\overline{p})$ is a modality-free formula which defines a monotone Boolean function f (but α is not necessarily monotone itself). Then

$$(\star) \qquad \alpha(\Box\overline{p}) \rightarrow \Box\alpha(\overline{p})$$

is a K-tautology. If $(\star)$ has a proof in K with n axioms of distributivity then there exists a monotone circuit of size $o(n^2)$ computing f.

This proposition would give us a lower-bound, had we had an example of a monotone function f such that i) f is defined by a small Boolean *formula* ii) every monotone circuit which defines f must be large. However, by introducing new variables for gates of C, we can express also the proposition $C(\Box\overline{p}) \rightarrow \Box C(\overline{p})$, where C is a circuit. Such a modified tautology gives a lower bound if we have monotone f such that i) f is defined by a small Boolean *circuit* ii) every monotone circuit which defines f is large. Examples of such functions are well-known.

6 Applications to other modal systems.

In this section we prove that the tautology given in Theorem 14 is a hard tautology also in the systems of modal logic $K4$, Gödel-Löb's logic, S and $S4$. For $K5$ (and hence $S5$) this is probably not the case and we show that there is an exponentialm speed-up between $K5$ and K on tautologies of modal-depth one.

1. The system K4

$K4$ is the system K plus the axiom

$$\Box\psi \rightarrow \Box\Box\psi.$$

The application to $K4$ is immediate:

Theorem 15 *Let ψ be a K-tautology of modal depth one. Assume that ψ has a proof in $K4$ with n axioms of distributivity. Then ψ has a proof in K with at most n axioms of distributivity.*

`Proof.` It is easy to show that Lemma 4 is true also in the case of $K4$. The point is that

$$(\Box\psi \rightarrow \Box\Box\psi)^\star = \Box\psi' \rightarrow \Box\psi'$$

is a propositional tautology. We thus obtain $K4$-proof with at most n distributivity axioms and formulas of modal depth one, i.e., a K-proof. `QED`

Corollary *Let Θ_n^k be the tautology of Theorem 14, for the same choice of k. Then every $K4$ proof of Θ_n^k contains an exponential number of distributivity axioms.*

The following lemma will be used in the proof of Theorem 19. We shall say that an axiom of distributivity of the form $\Box(\psi \to \xi) \to (\Box\psi \to \Box\xi)$ is *a proper axiom of distrivutivity,* if $K_5^0 \not\vdash \psi \equiv \xi$. As remarked on page 3, the bound of Theorem 14 applies when only the number of proper distributivity axioms is considered.

Lemma 16 *Let $K4^+$ be the logic $K4$ plus the axiom*

$$\Box\psi \to \Box(\psi \wedge \Box\psi).$$

Let ψ be K-tautology of modal depth one. Assume that ψ has a proof in $K4^+$ with n axioms of distributivity. Then ψ has a proof in K with at most n proper axioms of distributivity.

`Proof.` The proof is parallel to the proof of Theorem 15. The only modification is that

$$(\Box\psi \to \Box(\psi \wedge \Box\psi))^\star = \Box\psi' \to \Box(\psi' \wedge \psi').$$

But $\psi' \equiv \psi' \wedge \psi'$ is a propositional tautology and hence no proper distributivity axiom is required. `QED`

Remark. The argument of the proof of Theorem 15 can be applied to the system $K4$ plus the axiom

$$\Box\Box\psi \to \Box\psi.$$

2. Gödel - Löb's logic

GL is the system $K4$ plus the Löb axiom

$$\Box(\Box\psi \to \psi) \to \Box\psi.$$

Theorem 17 *Let ψ be K-tautology of modal depth one. Assume that ψ has a proof in GL with n axioms of distributivity. Then ψ has a proof in K with at most n proper axioms of distributivity.*

`Proof.` The proof is similar to that of Lemma 4. Let η' be defined as follows: for every subformula of η of the form $\Box\xi$ which is not in a range of further modality, replace $\Box\xi$ by 1.

Claim. *Assume that $GL \vdash \psi$. Then ψ' is a propositional tautology.*

The claim is proved easily by induction: the $K4$ axiom and Löb axiom change to $1 \to 1$, distributivity to $1 \to (1 \to 1)$ and generalisation to

$$\frac{\eta}{1}.$$

Let $\eta^\star$ be defined as follows: for every subformula of η of the form $\Box\xi$ which is not in a range of further modality, replace $\Box\xi$ by $\Box\xi'$. We can see that if η is a distributivity axiom then $\eta^\star$ is a distributivity axiom. Again, we can show that if $S = \eta_1 \dots \eta_k$ is GL-proof of ψ and Γ is the set of distributivity axioms in S, then every $\eta_i^\star$, $i = 1, \dots k$, is provable in K using just distributivity from $\Gamma^\star := \{\gamma^\star; \gamma \in \Gamma\}$. The $K4$ axiom changes to $\Box\psi' \to \Box 1$, which is provable in K without using any distributivity, and Löb axiom becomes

$$(1) \qquad \Box(1 \to \psi') \to \Box\psi'.$$

But $(1 \to \psi) \equiv \psi$, is a propositional tautology and so (1) is provable in K using no proper distributivity. For the generalisation use the above claim. `QED`

Corollary *Let Θ_n^k be the tautology of Theorem 14, for the same choice of k. Then every proof of Θ_n^k in Gödel-Löb's logic contains an exponential number of distributivity axioms.*

Remark. The argument of the proof applies also to the system $K4$ plus the axiom

$$\Box\Box\psi \vee \Box\neg\Box\psi.$$

This is interesting because this system together with the axiom from the previous remark is equivalent to $K5$ for which the lower-bound does not work.

3. S, S4

S resp. $S4$ is the logic K resp. $K4$ plus the axiom

$$\Box\psi \to \psi.$$

As will be shown in Theorem 22 there is an exponential speed-up between S and K. However, in the case of monotone formulas such as the ones needed in the lower bound there is indeed no speed-up between S and K (as far as the number of distributivity axioms is concerned).

For a formula ψ of modal-depth one, ψ^s will be the usual translation of S to K, i.e. $p^s := p$, $(\psi_1 \wedge \psi_2)^s := {\psi_1}^s \wedge {\psi_2}^s$ and similarly for other connectives, and mainly

$$(\Box\psi)^s := \Box\psi \wedge \psi^s.$$

Lemma 18 *Let ψ be S-tautology of modal-depth one. Then ψ^s is K-tautology. Furthermore, if ψ has a S-proof resp. $S4$ proof with n distributivity axioms then ψ^s has a K-proof with at most n distributivity axioms resp. n proper distributivity axioms.*

`Proof.` Straightforward. `QED`

Theorem 19 *Let $\alpha(p_1, \ldots p_n, \overline{r})$ be a monotone formula in $p_1, \ldots p_n$. Let*

$$\Theta := \alpha(\Box p_1, \ldots, \Box p_n, \overline{r}) \rightarrow \Box\beta(p_1, \ldots p_n, \overline{s}).$$

Then if Θ has a S-proof resp. $S4$ proof with n distributivity axioms then Θ has K-proof with at most n distributivity axioms resp. n proper distributivity axioms.

`Proof.` We will prove the proposition for S, the part for $S4$ follows similarly from the previous Lemma and Lemma 16.

Assume that Θ has S-proof with n distributivity axioms. Then $\Theta_1 := \Theta^s$ has K-proof with at most n distributivity axioms,

$$\Theta_1 = \alpha(\Box p_1 \wedge p_1, \ldots, \Box p_n \wedge p_n, \overline{r}) \rightarrow \Box\beta(p_1, \ldots p_n, \overline{s}) \wedge \beta(p_1, \ldots p_n, \overline{s}).$$

Hence also

$$\Theta_2 := \alpha(\Box p_1 \wedge p_1, \ldots, \Box p_n \wedge p_n, \overline{r}) \rightarrow \Box\beta(p_1, \ldots p_n, \overline{s})$$

has a K-proof with at most n distributivity axioms. Substituting throughout the proof $\Box p_i$ for p_i, $i = 1, \ldots n$, we obtain that also

$$\Theta_3 := \alpha(\Box\Box p_1 \wedge \Box p_1, \ldots, \Box\Box p_n \wedge \Box p_n, \overline{r}) \rightarrow \Box\beta(\Box p_1, \ldots \Box p_n, \overline{s})$$

has a K proof with at most n distributivity axioms. By Lemma 4, the formula $\Theta_3^\star$ is K-tautology and has a K-proof with at most n distributivity axioms. However,

$$\Theta_3^\star = \alpha(\Box p_1 \wedge \Box p_1, \ldots, \Box p_n \wedge \Box p_n, \overline{r}) \rightarrow \Box\beta(p_1, \ldots p_n, \overline{s}).$$

Hence $\Theta_3^\star$ is equivalent to Θ using just propositional rules. Therefore Θ has K-proof with at most n distributivity axioms. `QED`

Corollary *Let Θ_n^k be the tautology of Theorem 14, for the same choice of k. Then every S resp. $S4$ proof of Θ_n^k contains an exponential number of distributivity axioms.*

3. K5 and some speed-up relations

The theory $K5$ is the theory $K4$ plus the axiom

$$\neg\Box\psi \to \Box\neg\Box\psi.$$

The result of Theorem 14 does not apply to $K5$ (and hence to $S5$). It can be shown that the tautology of the Theorem a) requires only a polynomial number of distributivity axioms in $K5$ and b) it has a polynomial-size proof assuming that certain classical tautologies have poly-size Frege proofs. The same applies to the hard tautology mentioned in Remark on page 16. Those observations will be left without a proof here. We will rather prove that a variant of the tautology of Theorem 14 has a polynomial-size proof in $K5$. Since this variant has only exponetial proofs in K or $K4$, this implies that there is an exponential speed-up between $K5$ and K resp. $K4$ on tautologies of modal-depth one.

Lemma 20 *Let ψ be a K-tautology of modal depth one. Assume that the variables $\overline{r}$ do not occur in ψ in a modal context. Assume that $\psi(\Box\overline{r})$ has a K-proof with n distributivity axioms. Then ψ has a K-proof with at most n distributivity axioms.*

`Proof.` Let $\xi(\overline{r}/1)$ be an abbreviation for $\xi(r_1/1,\ldots r_k/1)$ for $\overline{r} = r_1,\ldots r_k$. For a formula η of modal depth one, let $\eta^\star$ denote the formula obtained by replacing every $\Box\xi$ by

$$\Box\xi(\overline{r}/1) \wedge \xi(\overline{r}).$$

Let $S = \eta_1,\ldots\eta_m$, $\eta_m = \psi$ be the proof of $\psi(\Box\overline{r})$. By Lemma 4 we can assume that the proof of ψ contains only formulas of modal depth one. As in Lemma 4 we can easily show that $\eta_m^\star = (\psi(\Box\overline{r}))^\star$ is provable in K using n distributivity axioms. However,

$$(\Box r_i)^\star = \Box 1 \wedge r_i$$

and $\Box 1$ is provable only using generalisation, and hence $(\Box r_i)^\star \equiv r_i$ is provable using no distributivity rule. Hence also the equivalence

$$(\psi(\Box\overline{r}))^\star \equiv \psi(\overline{r})$$

is provable with no distributivity axioms. Altogether, ψ is provable with n distributivity axioms. `QED`

Theorem 21 *There exists a K-tautology Θ of modal depth one s.t. every K-proof of Θ contains exponential number of proof-lines, but Θ has a polynomial-size proof in $K5$.*

`Proof.` Let Θ' be the tautology

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

of Theorem 14. Let $\Theta := \Theta'(\Box\overline{r})$. By the previous Lemma, the tautology has only proofs with exponential number of proof-lines in K. Let us show that it has a polynomial-size proof in $K5$.

The proposition *Clique* is written in such a way that all the negations in *Clique* are attached to variables $\overline{r}$. Note that in $K5$ we can prove

$$\begin{array}{rcl}(\neg)\Box r_i \wedge (\neg)\Box r_j & \rightarrow & \Box((\neg)\Box r_i \wedge (\neg)\Box r_j) \\ \Box\eta \wedge (\neg)\Box r_j & \rightarrow & \Box(\eta \wedge (\neg)\Box r_j)\end{array}$$

where $(\neg)$ means that the negation may be absent. Similarly when exchanging $\wedge$ for $\vee$. This implies that

$$(\star) \qquad Clique_n^{k+1}(\Box\overline{p}, \Box\overline{r}) \rightarrow \Box Clique_n^{k+1}(\overline{p}, \Box\overline{r})$$

can be proved by a linear-size proof in $K5$. However, the propositional implication

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

can be proved by a polynomial size proof in Frege system, as shown in [2]. Hence also

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

has a polynomial-size proof. Using one distributivity, also

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

has a polynomial-size proof. This, together with $(\star)$ gives a polynomial-size proof of Θ in $K5$. `QED`

The importance of the Theorem 21 lies in the fact that it gives speed-up on formulas of modal-depth one. A speed-up on formulas of modal-depth one can be obtained also between S on the one hand, and the systems K, $K4$ and Gödel-Löb's logic on the other. The same trick can probably be applied to show speed-up relations between the other systems on general modal formulas.

Theorem 22 *Let P be K, $K4$, or Gödel-Löb's logic. Then S has an exponential speed-up over P on formulas of modal-depth one. More exactly, there exists a sequence of formulas provable both in P and S s.t. they have linear-size proofs in S but every proof in P must be exponential.*

`Proof.` We know that there exists a sequence of K-tautologies $\psi_1,\ \psi_2,\ \psi_3, \ldots$ which have only exponential-size proofs in P. Let λ be the formula

$$\Box p \rightarrow p,$$

for a variable p not occurring in ψ_i, $i = 1, 2, \ldots$. Let us have the sequence

$$\psi_1 \vee \lambda,\ \psi_2 \vee \lambda,\ \psi_3 \vee \lambda, \ldots.$$

Clearly, the formulas have linear-size proofs in S. It is easy to show that the sequence has only exponential-size proofs in P: for a formula η, let $\eta^\star$ denote the formula obtained by replacing every occurrence of the variable p in a modal context by 1, and every occurrence of p in a non-modal context by 0 in η. It is easy to see that if η of modal-depth one has a proof in P with n distributivity axioms then $\eta^\star$ has also a proof in P with n distributivity axioms. But

$$(\psi_i \vee \lambda)^\star = \psi_i \vee (\Box 1 \rightarrow 0),$$

which is - using no distributivity - equivalent to ψ_i. `QED`

References

[1] Alon, N., Boppana, R. (1987) The monotone circuit complexity of Boolean functions, *Combinatorica*. **7(1)**:1-22.

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

[3] Karchmer, M. (1993), On Proving Lower Bounds for Circuit Size, in: Proceedings of Structure in Complexity, 8th Annual Complexity Conference, pp. 112-19, IEEE Computer Science Press

[4] Krajíček, J. (1997), Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *Journal of Symbolic Logic*, **62(2)**: 457 - 486

[5] Razborov, A. A. (1985), Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathematics Doklady*, **31**: 354-357