Charles University in Prague
Faculty of Mathematics and Physics

Some problems concerning lengths of proofs

Pavel Hrubeš

Ph.D. Thesis
Prague, 2007

Abstract

In the thesis, we address two issues (Part I and Part II) connected with lengths of proofs: Kreisel's conjecture, and the complexity of several systems of non-classical propositional logics. Kreisel's conjecture is a long open problem concerning the number of steps in proofs in Peano arithmetic. The problem is not solved here, but we present natural modifications of PA where Kreisel's conjecture is false. Namely the theory $PA(-)$, obtained by extending PA with a new function symbol minus, the theory of integers $\mathcal{Z}$, and others. The exposition closely follows the paper [9]. We then apply a similar reasoning to propositional logic. We construct a natural yet startling propositional proof system, FI, a systems in which many tautologies are provable in a constant number of steps. More exactly, for every n there exists c s.t. every tautology with at most n variables is provable in FI in c proof-lines. We proceed to prove non-constant lower bounds for FI and to analyse similar phenomena in other logics.

In the second part, we prove lower bounds on the sizes of proofs in certain systems of modal logic, namely K_4, S_4, Gödel-Löb's logic, and intuitionistic propositional calculus. For those systems, we give examples of tautologies $A_1, A_2, \ldots$ s.t. every proof of A_i in the system must be of exponential size (in terms of the size of A_i). We also give various speed-up relations between systems of modal logic, and between classical and intuitionistic propositional calculi. Speed-up between intuitionistic and classical propositional calculus illustrates how the excluded middle principle simplifies propositional proofs. The main results were given in [10] and [11], but we give independent and simpler proofs here.

Acknowledgements

I would like to thank my supervisor Pavel Pudlák for his advice, help, and infinite patience in listening to all my great ideas which for the most part turned not to be so. I thank Stefano Cavagnetto and Joost Joosten, the former for introducing me to the problem of Kreisel's conjecture, the latter for introducing me to modal logic; Emil Jeřábek for being an often - exploited source of information; and Olga Neumanová for linguistic and typographic support. Section 2 was motivated by discussions with Matthias Baaz. I received financial help from the grant IAA1019401.

Contents

Introduction

The traditional topics of mathematical logic are the study of *provability* and *definability*. In the former case we want to know which sentences are provable in a proof system, in the latter, which concepts are expressible in a language. The purpose of the inquiry is to establish the strength and limits of the tools we use in science and mathematics, as well as to compare strength of different logical systems. The questions can be refined: we may ask how difficult it is to prove or define something in a proof system or a language. As the basic measure of the complexity of a proof we take its size. Instead of asking whether a sentence is provable or not, we take a provable sentence and ask what is the size of its shortest proof in the proof system. One motivation for such an investigation is the comparison of efficiency of proof systems. For we can have two proof systems P and Q which prove the same theorems, but in P the proofs are much shorter than in Q. From a *logical* point of view the systems are equivalent, but not so from the practical one. Similarly, we may consider sizes of definitions in various languages.

The practical aspect conveys a philosophical point. For the meaning of words is to be explained from their *use* better than their denotation, especially if, as in mathematics, the denotation is obscure or dubious. And the use of many words and language tools is not only to express new facts, but to make communication more efficient. There are even concepts whose main purpose is such: abbreviations and definitions. To explain those by merely stating the definiens would be missing their purpose. Their function is to shorten expressions and arguments. The function can be formally described by comparing the efficiency of the system which does and that which does not allow definitions. I believe that in this way the study of complexity of proofs and expressions can help to explain and describe the use of concepts in mathematics and natural language.

Example 1 - Grandmother and the use of definitions.

We often use concepts that can be defined from other concepts, or which are even introduced by explicit definitions. *"Grandmother"*, for example. Whenever we use the word *"grandmother"* we could equivalently use the phrase *"a mother of ones' father or ones' mother"*. That, however, would be too cumbersome. We should also note that in our language we are allowed to iterate the definition, and speak about *"greatgrandmother"*, *"greatgreatgrandmother"* etc. How much can expression or proofs be shortened by the use of definitions? Mathematically, we can investigate the following questions:

1. Let us have a language L and we extend it to the language L_+ equipped with the possibility to introduce new words by means of definitions. How much shorter can be the expressions in L_+ than in L?

2. Let us have a proof system P and we extend it to the system P_+ equipped with the possibility to introduce new words by means of definitions. How much shorter can be the proofs in P_+ than in P?

Mathematically, the problems are of a special interest when L is taken as the language of propositional logic, $\wedge, \vee, \neg$, and P as the basic proof system axiomatising classical propositional logic, the so called *Frege system.* 1) then corresponds to the problem of separating Boolean circuits from Boolean formulas, and 2) to separating Frege and extended Frege system. The former problem is a basic open problem of Boolean complexity, and the latter a basic open problem of propositional proof complexity (see [25] and [15]). If L resp. P is a first-order language resp. the usual system of classical predicate logic, the answers to the problems will depend on whether identity "$=$" is present, whether function symbols are allowed, as well as on some extralogical assumptions.

Example 2 - natural numbers.

Do numbers, and in what sense, exist? is a question which obscures the far more interesting question *How are numbers used?* It cannot be maintained that natural numbers are logically redundant, for there are contexts where the use of natural numbers cannot be eliminated. On the other hand, there are contexts, and perhaps the principal ones, where this is possible, such as *"John has two sheep"* or *"the third king of Bohemia"*[1]. In elementary contexts, natural numbers behave like certain logical abbreviations; this has lead some to the belief that they are ontologically redundant - they do not denote an object, and do not express a new fact[2]. Nevertheless they are used, by physicists, architects, carpenters, and all who ever counted or measured anything. One of their many functions, even in contexts where they are logically redundant, is to shorten expressions and arguments. This is achieved in at least two ways. First, in the direct shortening of formulas, as in the case *"John has three hundred sheep"*. Second, when one discerns a numerical structure in a real life problem, the problem can often be solved more efficiently on the abstract level, as a problem about natural numbers. A purely mathematical problem, say $3+5=?$, can be identified in a concrete situation, the equation

$$3+5=8$$

can be computed by mathematical means and applied again to the situation.

I believe that even if all other uses of natural numbers were lost and forgotten, their aforementioned application would still give an excellent justification for their presence in language.

Proof complexity and computational complexity

A different motivation for the study of lengths of proofs is the connection with *computational complexity*; and perhaps it is for this reason that the problem has attracted so much attention. Computability theory has provided an exact mathematical definition of the concept of *algorithm.* We can meaningfully ask

[1] We can say "There exist sheep A and B, $A \neq B$, which belong to John"

[2] Namely Wittgenstein in *Tractatus.* However, *Tractatus* contains one of the most penetrating analysis of the use of natural numbers.

which problems are solvable by an algorithm, and which are not. This question, too, can be refined: we can ask whether a problem is solvable *efficiently.* An efficient algorithm is usually understood as an algorithm which requires polynomial time to find the answer (polynomial in terms of the size of its input). The purpose of computational complexity is to delimit the class of efficiently solvable problems. This is the heart of the fundamental *P versus NP problem.* One of the many formulations of the problem is the following:

($\star$) *Does there exist an algorithm which would decide in a polynomial time whether a classical propositional formula is a tautology?*

On the other hand, the basic open question of proof complexity is the following:

($\star\star$) *Does there exist a propositional proof system in which all classical propositional tautologies have polynomial size proofs?*

The expected answer to both of these questions is *"no"* and the connection is that if ($\star\star$) has a negative answer then also ($\star$) has. Hence to solve the problem ($\star\star$) would imply the solution to the P versus NP problem.

However, it is not very likely that P versus NP problem would be solved by means of proof complexity. So far the interaction between proof and computational complexity was mainly one way: the results and methods of computational complexity were applied in proof complexity. The connection between the fields rather shows that the problems of proof complexity are not artificial questions of solitary logicians, and it gives an explanation why the questions in proof complexity are difficult. Moreover, the study of complexity of particular proof systems gives a certain evidence for believing our computability conjectures. We can also hope that one day some techniques of proof complexity would be applicable also in computational complexity, and proof complexity would finally repay its debt to computational complexity.

PART I

1 Kreisel's conjecture

There are two main measures of complexity of a proof: its *size*, i.e., the total number of symbols, and *the number of proof-lines*. From the computational point of view, size is the more important of the two characteristics, for it is the size which determines how difficult it is for a machine (and presumably for the human mind) to verify the correctness of the proof. The number of proof lines is also an important measure, if only because in this perspective we meet new, interesting and often very surprising phenomena. Moreover, the number of proof lines is a lower bound on the size of a proof and hence the number of proof lines can give an information about the size of a proof.

A famous problem connected to the number of proof-lines is *Kreisel's Conjecture (KC)* (as quoted in [8]):

Let $\forall_n \psi(n)$ be a sentence of PA. Assume that there is some k s.t. for every n $\psi(\overline{n})$ is provable in PA in k steps. Then $\forall_n \psi(n)$ is provable in PA.

Similarly, we could formulate KC for any formal system S related to arithmetic. The peculiarity of KC lies in the fact that it depends not so much on the logical strength of S, i.e., on how many propositions are provable in S, but on the length of proofs in S and, in particular, on the structure of terms in S. So far, it has been shown that for some theories obtained by weakening[3] of PA, KC is true. Parikh [21] has shown that KC is true in the theory obtained by replacing the binary function symbols for multiplication and addition by ternary predicates in PA; the result has been extended by Miyatake [19] to the case where also $+$ is present as a function symbol. Baaz and Pudlák [1993] proved KC for the theory $I\Sigma_1$.[4] Krajíček and Pudlák [14] proved that KC holds for any finitely axiomatised theory. On the other hand, we can find trivial examples of theories where KC is false, e.g., one obtained by adding every instance of an undecidable Π_1-sentence as an axiom. Yukami [26] has shown, using the Matyasievich theorem, that KC is false when we add to PA all the true equations of the form $\overline{n}\cdot\overline{m} = \overline{n \cdot m}$. We will present more natural theories where KC is false: the system $PA(-)$ differs from PA only in containing an additional function symbol, minus. The theory $\mathcal{Z}$ has exactly the same language as PA but it is a natural axiomatisation of the theory of integers. We will show that in those systems we can find k s.t. every sentence of the form $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$ is provable in k steps, which implies that KC is false (as follows from Yukami's argument). The systems $PA(q)$ and $PA(N)$ will be obtained by weakening the systems $PA(-)$ and $\mathcal{Z}$ respectively. Here, KC will be disproved without determining such an upper bound for multiplication, i.e., without bounding proof lengths of the equation $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$.

[3] In the sense of having longer proofs.

[4] However, only with the scheme of minimum and the axioms of identity.

Kreisel's conjecture is a problem which significantly depends on the function of terms in proofs. Our inability to decide KC (and many related problems, as illustrated in Section 1.3) highlights the fact how little we understand this function. Our construction in $PA(-)$ and $\mathcal{Z}$ shows that function symbols can be much more powerful than one would expect. This also hints at the possibility that KC is false even in PA. If, after all, KC is true then the results show that the proof must concentrate on the specific properties of PA. In the proof it must be relevant that the functions definable by terms in PA are provably increasing, polynomial etc. We cannot hope for a proof that would work independently on the function symbols used, and thus we cannot hope to solve KC by some clever general argument.

Let us first introduce some notation:

1. PA will denote the usual Peano arithmetic.

2. Let T be a theory, ψ a formula and k a number. Then

   $$T \vdash_k \psi$$

   states that ψ is provable in T in k steps.

3. We assume that identity is formalised using *the schemes of identity*, i.e., infinitely many axioms

   $$x = y \rightarrow t(z/x) = t(z/y)$$

   for every term of PA and

   $$x = y \rightarrow (\psi(z/x) \equiv \psi(z/y))$$

   for every formula of PA [5].

4. We shall be dealing with terms recursively defined by a given rule. Those terms will be denoted Q^n, $Q^n_m, \ldots$ where the indices range over natural numbers. For example, $S^n(0)$ will denote the term $S(S(\ldots S(0)))$ where the S's occur n times (this term will be also denoted by $\overline{n}$). If $\psi(Q^n)$ is a formula containing the depicted recursive term then

   $$T \vdash_b \psi(Q^n)$$

   is an abbreviation for the statement *'there exists k such that for every n, $T \vdash_k \psi(Q^n)$'*. Similarly for a greater number of terms possibly with a greater number of indices. As an example we state the following important lemma (see [26]):

[5] On the other hand, for the purposes of our construction it would be sufficient to axiomatise identity with the finite list of axioms of the type $x = y \rightarrow S(x) = S(y)$, and similarly for the other function and predicate symbols. The reason is that an important fragment of the identity schema is derivable from the scheme of induction in a fixed number of steps.

Lemma 1 *$PA \vdash_b S^n(y) + x = S^n(y + x)$ and hence $PA \vdash_b x + S^n(y) = S^n(x + y)$.*

`Proof.` Let $\psi(y, x)$ denote the formula $S^n(y)+x = S^n(y+x)$. The proof is by induction with respect to x. If $x = 0$ then $\psi(y, 0) = S^n(y) + 0 = S^n(y + 0)$ and $PA \vdash_b \psi(y, 0)$. Let us show that $PA \vdash_b \psi(y, x) \to \psi(y, S(x))$. Assume $\psi(y, x)$. Then we have $S^n(y) + S(x) = S(S^n(y) + x) = S(S^n(y + x)) = S^n(S(y + x)) = S^n(y + S(x))$ and hence also $\psi(y, S(x))$. `QED`

The following can be obtained from [26] and so we just sketch the proof:

Theorem 2 *Let T be a consistent recursively axiomatised theory which contains the language of PA and extends PA. Assume that there is $k \in \omega$ s.t. for every $n, m \in \omega$ the formula*

$$\overline{n} \cdot \overline{m} = \overline{n \cdot m}$$

is provable in T in k steps. Then KC is false in T.

`Proof.` By the Matyasievich theorem we can find terms of PA, $t_1(x, y_1, \ldots y_l)$ and $t_2(x, y_1, \ldots y_l)$ s.t. the formula

$$\psi(x) := \forall x \exists y_1, \ldots \exists y_l \; t_1(x, y_1, \ldots y_l) = t_2(x, y_1, \ldots y_l)$$

is true and undecidable in T. From Lemma 1 every equation of the form $\overline{n} + \overline{m} = \overline{n + m}$ is provable in a bounded number of steps. This, together with the assumption of the theorem, gives an upper bound for the proofs of the instances $\psi(\overline{n})$. `QED`

1.1 The theory $PA(-)$

The theory $PA(-)$ is obtained by adding to PA a new binary function symbol '$-$' and the axiom

$$\forall x \forall y \forall z \; (x - y = z) \equiv (x = y + z \vee (x < y \wedge z = 0)),$$

and extending the scheme of induction to the language of $PA(-)$. We are going to prove the following theorem:

Theorem 3 *There exists $k \in \omega$ such that for every n, m,
$PA(-) \vdash_k S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$, or shortly*

$$PA(-) \vdash_b S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$$

Corollary *There is a number k and a formula $\psi(x)$ in the language of PA such that for every n $PA(-) \vdash_k \psi(S^n(0))$ but $PA(-) \nvdash \forall x \; \psi(x)$.*

The point of the construction is the following. For a large term T we are sometimes able to decide in a small number of steps whether it is equal to zero or one, as will be seen below. The information whether a term equals zero or not does not seem very useful. It may become so if we have a term $q(x, y)$ s.t. $q(x, y) = 0$ iff $x \neq y$. For then if we show that $q(t_1, t_2) \neq 0$, in a small number of steps, then we also have $t_1 = t_2$ in a small number of steps. Minus, as introduced here, enables us to find a term with such a property.

Let the expression $t_1 \bigtriangleup t_2$ be an abbreviation for $((t_1 - t_2) + (t_2 - t_1))$. We observe the following:

Lemma 4 *The following is provable in $PA(-)$:*

1. $(x + z) \bigtriangleup (y + z) = x \bigtriangleup y$,
2. $(x \bigtriangleup y = 0) \equiv (x = y)$,
3. $(\overline{1} - (x \bigtriangleup y) = 0) \equiv (x \neq y)$.

Let $T^n_m(x)$ denote the term

$$S^m(0) \cdot S^n(x) \bigtriangleup S^{n \cdot m}(S^m(0) \cdot x).$$

We will show that $PA(-) \vdash_b \overline{1} - T^n_m(0) \neq 0$, which immediately implies $PA(-) \vdash_b S^m(0) \cdot S^n(0) = S^{n \cdot m}(0)$.

For terms t_1 and t_2 we shall write $t_1 \sim t_2$, if the terms t_1 and t_2 are identical. $t[t_1/t_2]$ will denote the term obtained by replacing all the occurrences of t_1 in t by t_2.

Lemma 5 *1. $PA(-) \vdash_b S^m(0) \cdot S(x) = S^m(S^m(0) \cdot x)$.*

2. $T^n_m(S(x))[S^m(0) \cdot S(x)/S^m(S^m(0) \cdot x)] \sim T^{n+1}_m(x)$, for every n.

3. $PA(-) \vdash_b \forall x\ T^n_m(x) = T^n_m(0)$ and hence
$PA(-) \vdash_b T^n_m(0) \neq 0 \rightarrow \forall x T^n_m(x) \neq 0$.

`Proof.` 1) With the use of Lemma 1 we obtain $S^m(0) \cdot S(x) = S^m(0) \cdot x + S^m(0) = S^m(S^m(0) \cdot x + 0) = S^m(S^m(0) \cdot x)$.

2) By inspection.

3) It is sufficient to prove $T^n_m(S(x)) = T^n_m(x)$ in a bounded numbers of steps, the statement then follows by induction. The following equivalences are proved in a bounded number of steps by the use of Lemma 1 and the statement 1).

$$\begin{aligned}
T^n_m(S(x)) = &\quad S^m(0) \cdot S^n(S(x)) &\bigtriangleup&\quad S^{n \cdot m}(S^m(0) \cdot S(x)) \\
= &\quad S^m(0) \cdot S(S^n(x)) &\bigtriangleup&\quad S^{n \cdot m}(S^m(S^m(0) \cdot x)) \\
&= (S^m(0) \cdot S^n(x) + S^m(0)) &\bigtriangleup&\quad S^{n \cdot m}(S^m(S^m(0) \cdot x)) \\
&= (S^m(0) \cdot S^n(x) + S^m(0)) &\bigtriangleup&\quad S^{n \cdot m}(S^m(S^m(0) \cdot x) + 0) \\
&= (S^m(0) \cdot S^n(x) + S^m(0)) &\bigtriangleup&\quad (S^{n \cdot m}(S^m(0) \cdot x) + S^m(0))
\end{aligned}$$

By Lemma 4 part 1) we conclude

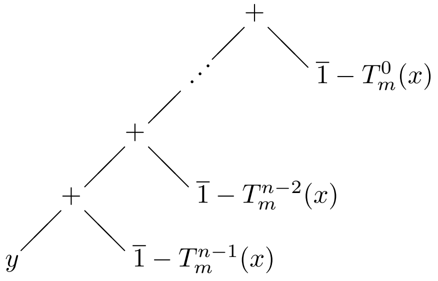
$$T^n_m(S(x)) \quad = \quad S^n(x)\cdot S^m(0) \bigtriangleup S^{n\cdot m}(S^m(0)\cdot x)$$

QED

Lemma 6 *Let t, t_1, t_2 be terms. Then the implication $t_1 = t_2 \to t = t[t_1/t_2]$ is provable in $PA(-)$ in three steps.*

Proof. Let z be a variable not occurring in t and let $t' := t[t_1/z]$. Let x_1, x_2 be variables not occurring in t'. The implication $x_1 = x_2 \to t'[z/x_1] = t'[z/x_2]$ is an axiom of identity. Applying substitutions x_1/t_1 and x_2/t_2 we obtain $t_1 = t_2 \to t'[z/t_1] = t'[z/t_2]$. But $t'(z/t_1) \sim t$ and $t'(z/t_2) \sim t[t_1/t_2]$. QED

Let $Q(y, x)$ denote the term



Lemma 7

$$PA(-) \vdash_b Q(y + (\bar{1} - T^n_m(x)), x) = Q(y, S(x)) + (\bar{1} - T^0_m(x))$$

and hence

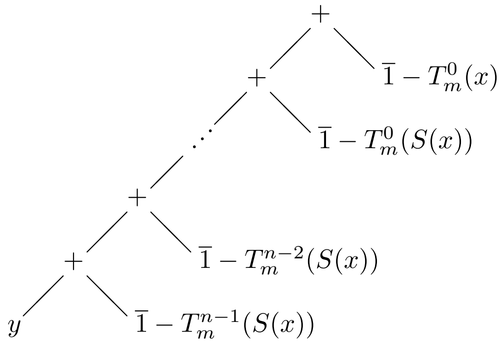
$$PA(-) \vdash_b Q(y + (\bar{1} - T^n_m(x)), x) = Q(y, S(x)) + \bar{1}$$

Proof. Let t_1 be the term $S^m(0)\cdot S(x)$ and t_2 be the term $S^m(S^m(0)\cdot x)$. Let us show that

$$(\star) \qquad (Q(y, S(x)) + (\bar{1} - T^0_m))[t_1/t_2] \sim Q(y + (\bar{1} - T^n_m(x), x).$$

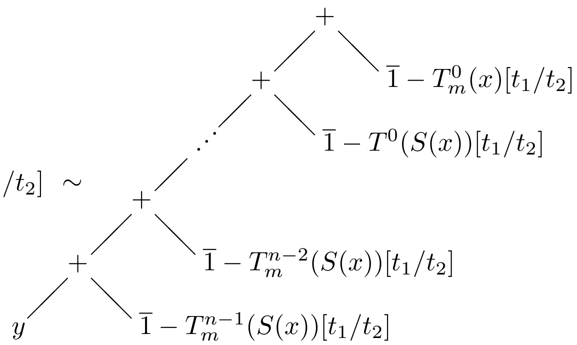
We have

$Q(y, S(x)) + (\bar{1} - T^0_m(x)) \qquad \sim$



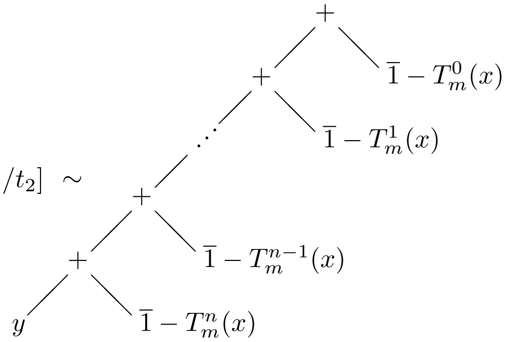
Hence

$(Q(y,S(x)) + (\overline{1} - T_m^0(x)))[t_1/t_2] \;\sim$


$+$
$+$
$\overline{1} - T_m^0(x)[t_1/t_2]$
$\overline{1} - T^0(S(x))[t_1/t_2]$
$+$
$+$
$\overline{1} - T_m^{n-2}(S(x))[t_1/t_2]$
y
$\overline{1} - T_m^{n-1}(S(x))[t_1/t_2]$

But $T_m^0(x)$ does not contain t_1 and by Lemma 5, $T_m^k(S(x))[t_1/t_2] \sim T_m^{k+1}(x)$. Hence

$(Q(y,S(x)) + (\overline{1} - T_m^0(x)))[t_1/t_2] \;\sim$


$+$
$+$
$\overline{1} - T_m^0(x)$
$\overline{1} - T_m^1(x)$
$+$
$+$
$\overline{1} - T_m^{n-1}(x)$
y
$\overline{1} - T_m^n(x)$

which is the term $Q(y + (\overline{1} - T_m^n(x)), x)$ and hence $(\star)$ is verified.

By the previous Lemma and Lemma 5, part 1, we finally obtain

$$PA(-) \vdash_b Q(y + (\overline{1} - T_m^n(x)), x) = Q(y, S(x)) + (\overline{1} - T_m^0(x))$$

The other part of the proposition follows from the fact that $PA(-) \vdash_b T_m^0(x) = 0$. QED

Proof of Theorem 3: We reason in $PA(-)$. Assume that $S^m(0) \cdot S^n(0) \neq S^{m \cdot n}(0)$. Then $T_m^n(0) \neq 0$ and, by Lemma 5, for every x, $T_m^n(x) \neq 0$. Then, by Lemma 4, part 3, $\overline{1} - T_m^n(x) = 0$ for every x. The previous lemma then gives the equality

$$(\star) \qquad Q(y,x) = Q(y, S(x)) + \overline{1}.$$

Let $y := 0$. By induction we can prove that for every z,

$$(\star\star) \qquad Q(0,0) = Q(0,z) + z.$$

If $z = 0$ we have $Q(0,0) = Q(0,0) + 0$ which is true. Assume that the statement holds for z, i.e., $Q(0,0) = Q(0,z) + z$. From $(\star)$ we have $Q(0,z) = Q(0,S(z)) + \overline{1}$ and hence $Q(0,0) = Q(0,S(z)) + \overline{1} + z = Q(0,S(z)) + S(z)$.

But the proposition $(\star\star)$ implies that $Q(0,0) \geq z$ for every z, which is impossible. QED

1.1.1 The theory $PA(q)$

Let q be a function symbol of arity ≥ 1. The theory $PA(q)$ will be the theory obtained by adding the symbol q to the language of PA and extending the scheme of induction to the language of $PA(q)$. Hence the only axioms describing the properties of q in $PA(q)$ are those given in the induction and the identity schemes.

Theorem 8 *There is a number k and a formula $\psi(x)$ in the language of $PA(q)$ such that for every n $PA(q) \vdash_k \psi(S^n(0))$ but $PA(q) \not\vdash \forall x\ \psi(x)$.*

Proof. Assume that q is a binary function. The sentence

$$\forall x \forall y \forall z\ (q(x,y) = z) \equiv (x = y + z \vee (x < y \wedge z = 0))$$

will be denoted as $SUBTR[q]$. As in Theorem 2 we can find a formula $\psi'(x)$ in the language of PA such that $\forall x\ \psi(x)$ is not provable in PA (and hence in $PA(q)$), but the instances are provable in a bounded number of steps, if we have an upper bound on proof-lengths for the equations $\overline{n} \cdot \overline{m} = \overline{n \cdot m}$. Let $\psi(x)$ be the formula

$$SUBTR[q] \rightarrow \psi'(x)$$

In every instance of the formula we can assume $SUBTR[q]$ and use q in place of minus as in the previous section. Hence we obtain $PA(q) \vdash_b \psi(S^n(0))$. The sentence $\forall x\ \psi(x)$ is not provable in $PA(q)$, since $PA(q)$ is a conservative extension of PA and the formula $SUBTR[q]$ is satisfiable (i.e., every model of PA can be expanded to the model of $PA(q) + SUBTR[q]$).

If q has an arity bigger than two, we can use the term $q(x, y, 0, \ldots 0)$ instead.

Assume that q is a unary function symbol. In PA we have a binary term OP coding pairs of natural numbers. The previous argument can be applied to the term $q(OP(x,y))$. QED

1.2 The theory of integers

The function minus, as introduced in section 1.1, is quite different from the functions definable by terms in PA. Not only it is not increasing but it is also very 'discontinuous'. Note that with minus we have definitions by cases on terms: if we have functions f_1, f_2, g_1, g_2 defined by terms then we also have a term in $PA(-)$ which defines the function h such that $h(x) = f_1(x)$, if $g_1(x) \leq g_2(x)$, and $h(x) = f_2(x)$ otherwise.[6] We defined minus in this way because we wanted to have a theory with the same universe as PA. However, this property of minus is not essential in the proof of Theorem 3. We will now show that a similar argument can be applied to the theory of integers, where minus is definable in the natural way.

The theory of integers, $\mathcal{Z}$, is the theory with constant 0, function symbols $S, +, \cdot$ and predicates $<, \leq, =$. The axioms are the following[7]:

[6] Observe that $h(x) = f_1(x)(1 - (g_1(x) - g_2(x))) + f_2(x)(1 - ((g_2(x) + 1) - g_1(x)))$.

[7] We take the leisure to write $x > y$ ($\geq y$) instead of $y < x$ ($\leq x$) and abbreviate the bounded quantifiers in the usual way

$Q1:$ $\forall x \forall y (S(x) = S(y)) \to x = y$

$Q3':$ $\forall x \exists y \; S(y) = x$

$Q4:$ $\forall x \; x + 0 = x$

$Q5:$ $\forall x \forall y \; x + S(y) = S(x + y)$

$Q6:$ $\forall x \; x \cdot 0 = 0$

$Q7:$ $\forall x \forall y \; x \cdot S(y) = x \cdot y + x$

$R8:$ $\forall x < 0 \exists y > 0 \; x + y = 0$

$D9:$ $\forall x \forall y \; x \leq y \equiv x < y \vee x = y$

$L10:$ $\forall x \geq 0 \; S(x) > 0$

$L11:$ $\forall x \; x < 0 \equiv \neg(x \geq 0))$

$L12:$ $\forall x \forall y \; (x < y \equiv \exists z > 0 \; y = x + z)$

and the scheme of induction

IND: $(\psi(0) \wedge (\forall x \geq 0 \; \psi(x) \to \psi(S(x))) \to \forall x \geq 0 \; \psi(x)$

The axioms Q1 -Q7 determine the behaviour of $S, +$ and $\cdot$; they are the axioms of PA except for the modified axiom $Q3'$. $R8$ is the key axiom relating positive and negative numbers. $D9$ is a definition of $\leq$. The axioms $L10$-$L11$ can be equivalently replaced by axioms asserting that $<$ is a linear ordering and that $x < S(x)$. The motivation for choosing our axiomatisation is the following: axioms preceding $L12$, except for the definition $D9$, use the relations $<, \leq$ only in the context $x < 0$, $x \leq 0$ etc., i.e., we employ only the property 'to be a positive (non-negative) number'. The axiom $L10$ asserts that the successor of a non-negative number is positive, the axiom $L11$ says that every number is either positive or non-positive and not both. It is just the last axiom which determines the exact properties of $<$. Note that there is no function symbol for minus in $\mathcal{Z}$ and that the scheme of induction applies only to positive numbers.

Lemma 9 *Let ψ be a formula in the language of $\mathcal{Z}$. Then the following are provable in $\mathcal{Z}$:*

IND1 $(\psi(0) \wedge \forall x \geq 0(\psi(x) \to \psi(S(x)) \wedge \forall x < 0(\psi(S(x)) \to \psi(x))) \to \forall x \psi(x)$

IND2 $((\psi(0) \wedge (\forall x \psi(x) \equiv \psi(S(x))) \to \forall x \psi(x)$

`Proof.` It is sufficient to prove part one, the other follows immediately. Reason within $\mathcal{Z}$. Assume that i) $\psi(0)$, ii) $(\forall x \geq 0 \; \psi(x) \to \psi(S(x))$ and iii) $\forall x < 0 \; \psi(S(x)) \to \psi(x)$. From i), ii) and IND we obtain $\forall x \geq 0 \; \psi(x)$. By $L11$ it is sufficient to show that $\forall x < 0 \; \psi(x)$. The following can be easily proved by induction (and the axioms $Q4$, $Q5$):

Claim. $\forall x \forall y \geq 0\ x + S(y) = S(x) + y$
Let $\psi'(x)$ be the formula

$$\forall z < 0\ z + x = 0 \rightarrow \psi(z),$$

where z does not occur freely in ψ. Let us show that $\forall x \geq 0\ \psi'(x)$. If $x = 0$ then then there is no $z < 0$ s.t. $z + x = 0$, and the statement holds. Assume that $\psi(x)$ is true for $x \geq 0$. Let us show that $\psi(Sx)$ is true. Let $z < 0$ be such that $z + S(x) = 0$. Then $S(z) + x = 0$ and, by the inductive assumption, we have $\psi(S(z))$ (if $S(z) \geq 0$, use the first part of the proposition, and if $S(z) < 0$, use the inductive assumption) . From iii) we have $\psi(z)$. Hence $\psi'(S(x))$ is true and therefore also $\forall x \geq 0\ \psi'(x)$. This, together with axiom $R8$, gives $\forall x < 0\ \psi(x)$. QED

The next proposition serves mainly to convince the reader of the soundness of the system $\mathcal{Z}$.

Proposition 10 *The following formulae are provable in $\mathcal{Z}$:*

1. *i)* $x \neq S(x)$, *ii)* $x + y = y + x$, *iii)* $(x + y) + z = x + (y + z)$, *iv)* $y + z = x + z \equiv y = x$, *v)* $x \cdot (y + z) = x \cdot y + x \cdot z$, *vi)* $x \cdot y = y \cdot x$, *vii)* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. *i)* $\forall x \forall y \exists ! z\ x = y + z$, *ii)* $(x \geq 0 \wedge y \geq 0) \rightarrow x + y \geq 0$, *iii)* $(x \leq 0 \wedge y \leq 0) \rightarrow x + y \leq 0$
3. *i)* $\neg x < x$, *ii)* $x < y \vee y < x \vee x = y$, *iii)* $(x < y) \wedge (y < z) \rightarrow (x < z)$, *iv)* $\neg(x < y \wedge y < x)$
4. *i)* $\forall x \forall y (x > 0 \wedge y > 0 \vee x < 0 \wedge y < 0) \rightarrow x \cdot y > 0$, *ii)* $x \cdot x \geq x$.
5. $\exists ! z \forall x\ x \cdot z + x = 0$

Proof. For 1) proceed as in PA but use IND2 where appropriate. We will prove part ii), the rest is similar. (In order to prove i) note that the statement $S(0) \neq 0$ follows from $L10$ and $L11$.) Let us first prove that for all x, $0 + x = x$. Let $\psi(x)$ be the formula $0 + x = x$. If $x = 0$ the formula holds because of $Q4$. Let us show that $\psi(x)$ iff $\psi(S(x))$, for every x. Assume $\psi(x)$. Then $0 + S(x) = S(0 + x) = S(x)$ and $\psi(S(x))$ holds. Assume $\psi(S(x))$. Then $0 + S(x) = S(x)$ and so $S(0 + x) = S(x)$. By $Q1$ we have $0 + x = x$ and $\psi(x)$ holds. By IND2 we then obtain $\forall x \psi(x)$. Let now $\psi(x)$ be the formula $\forall y\ x + y = y + x$. If $x = 0$, the formula holds as shown. As in the previous case we can prove that $\psi(x)$ iff $\psi(S(x))$, for every x and hence $\forall x \psi(x)$ holds.

2) The first proposition is straightforward, the second one requires the axiom $L10$. The next one uses the axiom $L11$.

3) If $x < x$ then there is $z > 0$ such that $x = x + z$. But then $(x = x + 0 = x + z)$ and by 1), iv) we have $z = 0$. But that is impossible, by axiom $L11$. The rest follows from the statements already proved.

4) Easy.

5) Let z_0 be such that $S(z_0) = 0$. Then $x \cdot S(z_0) = 0$. But $x \cdot S(z_0) = x \cdot z_0 + x$. If on the other hand $x \cdot z + x = 0$ for every x then also $S(0) \cdot z + S(0) = 0$ and hence $S(0) \cdot S(z) = 0$. But $S(0) \cdot S(z) = S(z)$ and hence $S(z) = 0$. Therefore $z = z_0$. QED

We are now going to prove the following theorem:

Theorem 11 *There is k such that for every n, m, $\mathcal{Z} \vdash_k S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$, or shortly*

$$\mathcal{Z} \vdash_b S^n(0) \cdot S^m(0) = S^{n \cdot m}(0)$$

Corollary *There is a number k and a formula $\psi(x)$ in the language of $\mathcal{Z}$ such that for every n $\mathcal{Z} \vdash_k \psi(S^n(0))$ but $\mathcal{Z} \not\vdash \forall x \geq 0 \ \psi(x)$.*

Lemma 12 *Let T be a theory such that $\exists z \psi(z)$ is provable in T. Let T' be the extension of T by a new constant c and the axiom $\psi(c)$. Then there exists a function $p : \omega \to \omega$ with the following property: if ξ is a formula in the language of T such that $T' \vdash_k \xi$ then $T \vdash_{p(k)} \xi$.*

Hence if S is a set of formulae in the language of T and $k \in \omega$ is such that $T' \vdash_k \xi$ for every $\xi \in S$ then there is $j \in \omega$ s.t. $T \vdash_j \xi$, for every $\xi \in S$.

Proof. The first part is easy and the other follows. QED

The lemma shows that we can, without significantly shortening the proofs, extend the language of $\mathcal{Z}$ by new constant symbols. By Proposition 10 part 5 we can thus work in the system $\mathcal{Z}$(-1) obtained by adding a new constant -1 to the language of $\mathcal{Z}$ together with the axiom

$$\forall x \ x \cdot (\text{-}1) + x = 0$$

The expression $t_1 - t_2$ will be an abbreviation for $t_1 + (\text{-}1).t_2$ The expression $t_1 \oplus t_2$ will be an abbreviation for $t_1 \cdot t_1 + t_2 \cdot t_2$.

Lemma 13 *The following formulae are provable in $\mathcal{Z}$:*

1. $(x + z) - (x + z) = x - y$
2. $x - y = 0 \ \equiv \ x = y$
3. $(0 \oplus 0) = 0$.
4. $(x \oplus y) \geq 0$
5. $x \neq 0 \to (y \oplus x > y)$.

`Proof.` 1)-3) are easy.

4) and 5) follow from Proposition 10, part 4. `QED`

Let $T^n_m(x)$ denote the term

$$S^m(0) \cdot S^n(x) - S^{n \cdot m}(S^m(0) \cdot x).$$

We will show that $\mathcal{Z} \vdash_b T^n_m(0) = 0$, which immediately implies $\mathcal{Z} \vdash_b S^m(0) \cdot S^n(0) = S^{n \cdot m}(0)$.

The proof proceeds similarly to the one in Section 1.1.

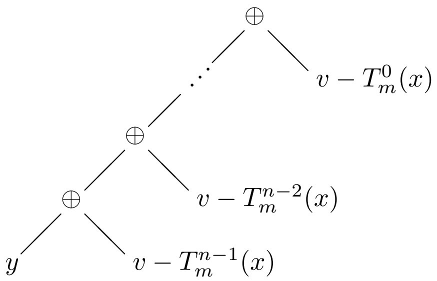
Lemma 14 *1. $\mathcal{Z} \vdash_b S^m(0) \cdot S(x) = S^m(S^m(0) \cdot x)$*

2. $T^n_m(S(x))[S^m(0) \cdot S(x)/S^m(S^m(0) \cdot x)] \sim T^{n+1}_m(x)$, for every n.

3. $\mathcal{Z} \vdash_b \forall x \; T^n_m(x) = T^n_m(0)$.

`Proof.` As in Lemma 5 `QED`

Let $Q(y, v, x)$ denote the term



The following is proved as in Lemma 7:

Lemma 15

$$\mathcal{Z} \vdash_b Q(y \oplus (v - T^n_m(x)), v, x) = Q(y, v, S(x)) \oplus (v - T^0_m(x))$$

and hence

$$\mathcal{Z} \vdash_b Q(y \oplus (v - T^n_m(x)), v, x) = Q(y, v, S(x)) \oplus v.$$

Proof of Theorem 9: We reason in $\mathcal{Z}$. Assume that $S^m(0) \cdot S^n(0) \neq S^{m \cdot n}(0)$. Therefore $T^n_m(0) \neq 0$. Let $v_0 := T^n_m(0)$. We have $v_0 - T^n_m(0) = 0$ and $v_0 \neq 0$. By Lemma 14 part 3, $v_0 - T^n_m(x) = 0$ for every x.

The previous lemma then gives

$$Q(y \oplus 0, v_0, x) = Q(y, v_0, S(x)) \oplus v_0.$$

Let $y := 0$. Then we obtain (Lemma 13, part 3)

$$(\star) \qquad Q(0, v_0, x) = Q(0, v_0, S(x)) \oplus v_0.$$

By induction with respect to z we can prove that for every $z \geq 0$ and for every x

$$Q(0, v_0, x) \geq z.$$

If $z = 0$, the proposition follows from Lemma 13, part 4 (since $Q(0, v_0, x)$ has the form $t_1 \oplus t_2$.) Assume the statement holds for $z \geq 0$. From $(\star)$ and Lemma 13, part 5, and the fact that $v_0 \neq 0$ we have $Q(0, v_0, x) > Q(0, v_0, S(x))$. By the inductive assumption $Q(0, v_0, x) \geq z$ for every x and hence $Q(0, v_0, S(x)) \geq z$. Hence $Q(0, v_0, x) > Q(0, v_0, S(x))$ implies $Q(0, v_0, x) > z$ and $Q(0, v_0, x) \geq S(z)$. But that is impossible. QED

1.2.1 The theory $PA(N)$

Let $N(x)$ be a unary predicate. The expressions $\forall x \in N\ \psi(x)$, $\exists x \in N\ \psi(x)$ will abbreviate the formulae $\forall x\ N(x) \rightarrow \psi(x)$, $\exists x\ N(x) \wedge \psi(x)$ respectively. Let ψ be a formula of PA. Then *the relativisation* of ψ will be the formula obtained by replacing the quantifiers $\forall x$, $\exists x$ by $\forall x \in N$, $\exists x \in N$ respectively. The theory $PA(N)$ will be the theory obtained by adding the unary predicate N to the language of PA. Its axioms - besides induction - will be the relativisations of axioms of PA, and the induction being replaced by the scheme

$$(\psi(0) \wedge (\forall x \in N\ (\psi(x) \rightarrow \psi(S(x)) \rightarrow \forall x \in N\ \psi(x),$$

where ψ is any formula of $PA(N)$.

The intended meaning of the predicate N is *'is a natural number'*. In this reading, PA is equivalent to the theory $PA(N)$ plus the axiom $\forall x\ N(x)$. At the same time the theory $PA(N)$ can be extended to a theory equivalent to $\mathcal{Z}$, by adding only a finite number of axioms. This fact is used in the following theorem.

Theorem 16 *There is a formula $\psi(x)$ in the language of $PA(N)$ and a number k such that for every n, $PA(N) \vdash_k \psi(S^n(0))$ but $PA(N) \not\vdash \forall x \in N\ \psi(x)$.*

Proof. The proof is similar to the proof of Theorem 8. Let κ be the conjunction of the axioms of $\mathcal{Z}$, apart from induction, and the sentence $\forall x\ N(x) \equiv x \geq 0$. Let $\psi'(x)$ be as in Theorem 8 and let $\psi(x)$ denote the formula

$$\kappa \rightarrow \psi'(x).$$

The theory $PA(N) + \kappa$ is equivalent to $\mathcal{Z}$. This is true even in the sense of conserving the lengths of proofs: the lengths of proofs in $\mathcal{Z}$ and $PA(N)+\kappa$ differ at most by a constant. As shown above $\mathcal{Z} \vdash_b \psi'(S^n(0))$ and hence $PA(N) \vdash_b \psi(S^n(0))$. The formula $\forall x \in N(x)\ \psi(x)$ is not provable in $PA(N)$, for $PA(N)$ is conservative over PA. QED

1.3 A weakening of KC and the structure of constant terms

A weakening of Kreisel's conjecture, which we call *'The Very Weak Kreisel's Conjecture'*, VWKC, can be obtained as follows:

Let $k \in \omega$. Assume that for every constant term C of PA the formula $\psi(C)$ is provable in PA in k steps. Then the formula $\forall x \psi(x)$ is provable in PA.

The VWKC immediately follows from KC, and it seems very straightforward. However, we are unable to prove (or disprove) even such a weak statement. This highlights the fact how little we know about the possible use of terms in PA. A related problem of this kind is the following:

Are all true equations of the form $C_1 = C_2$, where C_1 and C_2 are constant terms, provable in PA in a bounded number of steps?

This problem, too, seems quite straightforward: it seems enough to take for C a sufficiently large and chaotic term. But this is not the case. It can be shown that true equations of the form $C = 0$, $\neg(C = 0)$, $C = 1$, $\neg(C = 1)$, for a constant term C, can be proved for even 'very large' and 'very chaotic' terms in a bounded number of steps.[8] Hence we cannot easily rule out the alternative that all true formulas of the form $C = 0$, $\neg(C = 0)$, $C = 1$, $\neg(C = 1)$, and even all true equations, can be proved in a bounded number of steps.

To end on a happier note, there is at least something that can be proved easily:

Observation. For every k there are (non constant) terms t_1 and t_2 s.t. the equation $t_1 = t_2$ is true but cannot be proved in PA in k steps. An example of such equation is

$$(\dots((x + y_1) + y_2) \dots + y_n) = x + (\dots((y_1 + y_2) + y_3) \dots + y_n),$$

for a sufficiently large n. In other words, the equation asserts commutativity of a large sum. The proof of this fact would proceed like the proof in Section 2.2.

[8] Namely, for terms C s.t. every subterm of C has value 0 or 1. This will be apparent from Section 2.

2 Propositional proof systems with identity

We have seen that in arithmetic, many non-trivial propositions are provable even in a constant number of steps, if we are granted a sufficiently rich term structure. A similar phenomenon can occur in propositional logic, if are allowed to use the *identity axiom*

$$\xi \equiv \xi' \to \psi(p/\xi) \equiv \psi(p/\xi'),$$

or the *identity rule*

$$\frac{\xi \equiv \xi'}{\psi(p/\xi) \equiv \psi(p/\xi')}.$$

For in this case, formulas behave in a similar way like terms. We will investigate propositional proof system with the identity axiom, FI, and with the identity rule, FIr. We will prove quite a surprising result, that in the systems all tautologies with a bounded number of variables are provable in a bounded number of steps[9]. However, the identity rule is much weaker than the identity axiom, and we will show that FI has an unbounded speed-up over FIr (with respect to the number of proof-lines). In fact, FI is an optimal system in a certain class of systems, called generalised Frege systems (see Section 2.3). On the other hand, identity axiom may seem more natural because it is sound in most logics. Non-classical logics with identity rule will be considered in Section 2.2.2.

2.1 Constant upper bounds on number of proof-lines

Let us have a fixed language L of propositional logic. We can assume that it contains the constants 0 and 1, and the usual logical connectives $\to, \neg, \wedge, \vee, \equiv$. We assume that F is a particular propositional proof system having the form of a *Frege system.* The usual textbook axiomatisation of propositional logic is a kind of Frege system. In general, Frege system is defined as follows. *Frege rule* is an inference of the form

$$\frac{\psi_1(p_1, \dots p_k), \dots \psi_n(p_1, \dots p_k)}{\psi(p_1, \dots p_k)}$$

s.t. for any truth assignment to the variables $p_1, \dots p_k$, if $\psi_1, \dots \psi_n$ are true then so is ψ. *An application* of a Frege rule is a substitution of formulas for the variables $p_1, \dots p_k$, i.e. the inference

$$(Fr) \qquad \frac{\psi_1(\xi_1, \dots \xi_k), \dots \psi_n(\xi_1, \dots \xi_k)}{\psi(\xi_1, \dots \xi_k)}$$

Frege system is a finite list of Frege rules which is complete, i.e., every tautology is derivable in the system.

The identity axiom is a formula of the form

[9] This result has been first proved in [3].

$$(Id) \qquad\qquad \xi \equiv \xi' \to \psi(p/\xi) \equiv \psi(p/\xi'),$$

where ξ, ξ' and ψ are arbitrary formulas. The system F augmented with the identity axiom will be called *Frege system with identity*, FI. Frege system with identity is *not* a Frege system.

A formula ψ will be called *a closed formula*, if it does not contain propositional variables; hence ψ contains only logical connectives and 0 or 1.

Lemma 17 *If $F \vdash_c \xi(p)$ then $F \vdash_c \xi(p/\psi)$. In particular, there are c_1, c_2 s.t. for any formula ψ, $F \vdash_{c_1} \psi \equiv \psi$, $F \vdash_{c_2} ((\neg\psi \to 0) \to \psi$ etc.*

`Proof.` It is sufficient to replace every formula $\xi_i(p)$ in the F-proof of ξ by the formula $\xi_i(p/\psi)$. We thus obtain an F-proof of $\xi(p/\psi)$ of equal length. `QED`

Lemma 18 *Let $p \oplus q$ be the abbreviation for $p \equiv \neg q$. Then*

$$F \vdash p \oplus 1 \ \equiv\ \neg p \quad \textit{and} \quad F \vdash \neg p \to (q \oplus p \ \equiv\ q).$$

`Proof.` Trivial. `QED`

Theorem 19 *There exists $c \in \omega$ s.t. for every closed formula ψ, if ψ is a tautology then $FI \vdash_c \psi$. The c is determined by the particular properties of FI.*

`Proof.` Let the language of F be formed by the connectives $\lambda_1, \ldots \lambda_k$ with arities $r_1, \ldots r_k$ respectively. We will imagine closed formulas as trees in the usual way. The depth of a formula is the length of the longest branch; hence 0 and 1 have depth zero. Every formula of depth one has the form

$$\lambda_i(a_1, \ldots a_{r_i}), \quad i = 1, \ldots k$$

where $a_1, \ldots a_{r_i} = 0, 1$. Those formulas will be denoted $\mu_1, \ldots \mu_m$ (note that $m = \sum_{i=1,\ldots k} 2^{r_i}$). For $i = 1, \ldots m$, $\mu_i^\star$ will be either the formula 0 or 1, 0 if the truth value of μ_i is zero and 1 if the truth value is one.

Let ψ be a given closed formula. We shall construct a proof of ψ of length c s.t. the c does not depend on the choice of ψ. Instead of the phrase *'there is a c s.t. $FI \vdash_c \xi$ and c is independent on ψ'*, we shall write simply

$$FI \vdash_b \xi,$$

where ξ is assumed to be determined by ψ in a particular way (as will be clear later).

Assume that ψ is a tautology and ψ has depth n. Let us construct a sequence of formulas $\psi_n, \psi_{n-1}, \ldots \psi_0$ s.t. ψ_i has depth i. First, $\psi_n := \psi$. Assume that ψ_l, $l = n, \ldots 1$, has been constructed. Then ψ_{l-1} is obtained from ψ_l by replacing all the formulas μ_i in ψ_l by $\mu_i^\star$, $j = 1, \dots m$. We see that for every $l = 1, \dots n$, if ψ_l has truth value one then ψ_{l-1} has truth value one. Since ψ is a tautology, we have $\psi_0 = 1$.

For every ψ_i, $i = n \dots 1$, let us define the formula θ_i with m propositional variables $p_1, \dots p_m$ as follows: θ_i is obtained from ψ_i by replacing all the occurrences of μ_j in ψ_i by p_j, $j = 1, \dots m$.

Thus we immediately obtain

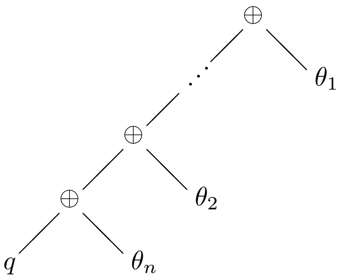
$$\theta_i(p_1/\mu_1, \dots p_m/\mu_m) = \psi_i, \quad i = n, \dots 1 \tag{1}$$

But also, from the definition of ψ_i,

$$\theta_i(p_1/\mu_1^\star, \dots p_m/\mu_m^\star) = \psi_{i-1}, \quad i = n, \dots 1 \tag{2}$$

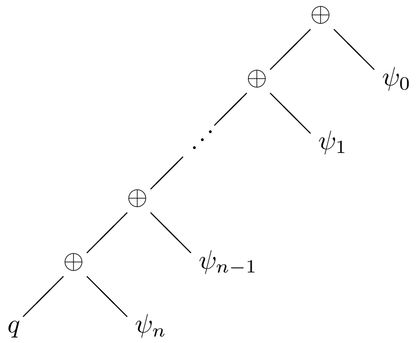
Let us now have the formula

$\Delta(q, p_1, \dots p_m) :=$



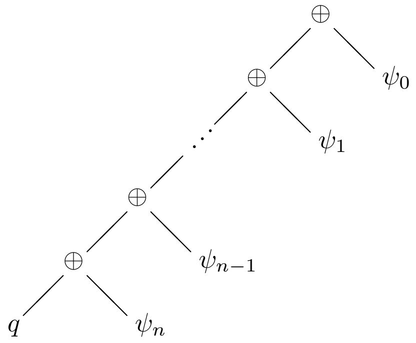
From the equation (1) we obtain

$\Delta(q/(q \oplus \psi_n), p_1/\mu_1^\star, \dots p_m/\mu_m^\star) \;=$



From the equation (2) we obtain

$\Delta(q, p_1/\mu_1, \dots p_m/\mu_m) \oplus \psi_0 \qquad =$



which together gives

(3) $$\Delta(q/(q \oplus \psi_n), p_1/\mu_1^\star, \dots p_m/\mu_m^\star) = \Delta(q, p_1/\mu_1, \dots p_m/\mu_m) \oplus \psi_0.$$

By Lemma 17 we have

(4) $$FI \vdash_b \Delta(q/(q \oplus \psi_n), p_1/\mu_1^\star, \dots p_m/\mu_m^\star) \equiv \Delta(q, p_1/\mu_1, \dots p_m/\mu_m) \oplus \psi_0,$$

Every formula of the form $\mu_j \equiv \mu_j^\star, j = 1, \dots m$ is provable in FI. Hence, applying the identity axioms m times, we obtain

(5) $$FI \vdash_b \Delta(q, p_1/\mu_1, \dots p_m/\mu_m) \equiv \Delta(q, p_1/\mu_1^\star, \dots p_m/\mu_m^\star),$$

Combining (4) and (5), we have

(6) $$FI \vdash_b \Delta(q/(q \oplus \psi_n), p_1/\mu_1^\star, \dots p_m/\mu_m^\star) \equiv \Delta(q, p_1/\mu_1^\star, \dots p_m/\mu_m^\star) \oplus \psi_0,$$

Hiding the occurrences of $p_i/\mu_i^\star$ and using the fact that $\psi_n = \psi$ and $\psi_0 = 1$, we can write that

(7) $$FI \vdash_b \Delta(q \oplus \psi) \equiv \Delta(q) \oplus 1.$$

By Lemma 18

(8) $$FI \vdash_b \Delta(q \oplus \psi) \equiv \neg\Delta(q).$$

From Lemma 18 $\neg\psi \to (q \oplus \psi \equiv q)$ is provable in a bounded number of steps. Hence, by the axiom of identity, we have

(9) $$FI \vdash_b \neg\psi \to (\Delta(q \oplus \psi) \equiv \Delta(q)).$$

But (8) and (9) yields

(10) $$FI \vdash_b \neg\psi \to (\neg\Delta(q) \equiv \Delta(q)),$$

and hence

$$FI \vdash_b \psi,$$

since $\Delta(q) \equiv \neg\Delta(q)$ is a contradiction (Lemma 17). QED

Lemma 20 *There exists a constant d s.t. for every ψ if $FI \vdash_c \psi(p/0)$ and $FI \vdash_c \psi(p/1)$, then*

$$FI \vdash_{c.d} \psi(p).$$

Proof. The axioms of identity state

$$(p \equiv 1) \to (\psi(p) \equiv \psi(p/1))$$

and

$$(p \equiv 0) \to (\psi(p) \equiv \psi(p/0)).$$

Since $(p \equiv 1) \vee (p \equiv 0)$ is a tautology then

$$(\psi(p) \equiv \psi(p/0)) \vee (\psi(p) \equiv \psi(p/1))$$

is a tautology provable in a number of steps independent on ψ. Assuming that both $\psi(p/1)$ and $\psi(p/0)$ are provable in c steps, then we can find a k independent on ψ s.t.

$$FI \vdash_{2c+k} \psi(p).$$

It is now sufficient to take $d := 2 + k$. QED

Theorem 21 *There exists $c \in \omega$ s.t. for every tautology ψ with n variables*

$$FI \vdash_{c^{n+1}} \psi.$$

Proof. Let c be the constant from Theorem 19 and d the constant from the previous Lemma. By induction with respect to n let us prove that ψ is provable in $c.d^n$ steps in *FI*. If $n = 0$ the proposition holds by the Theorem 19. Let ψ be a tautology with $n+1$ variables. Assume that ψ contains a variable p. If ψ is a tautology then both $\psi(p/0)$ and $\psi(p/1)$ are tautologies with n variables. By the inductive assumption

$$FI \vdash_{c.d^n} \psi(p/0) \qquad \text{and} \qquad FI \vdash_{c.d^n} \psi(p/1).$$

Then, by the previous Lemma

$$FI \vdash_{c.d^{n+1}} \psi(p).$$

Finally, we set $c := \max(c, d)$. QED

The statement can be proved also in FIr; we give the following version:

Theorem 22 *For every n there exists c s.t.*

$$FIr \vdash_c \psi,$$

for any tautology ψ with n variables.

Proof. The proof is analogous to that for FI. Let us just state the main points. In FIr we do not have Lemma 20, and the procedure of Theorem 19 must be repeated directly for the n-variable case. Let the variables $p_1, \dots p_n$ be fixed. Let $A = \alpha_1, \dots \alpha_m$, $m = 2^n$, be the set of DNF formulas that can be formed from the variables, s.t. any formula in variables $p_1, \dots p_n$ is equivalent to some α_i. For any connective λ of arity r and $\beta_1, \dots \beta_m \in A$ we can find $\alpha \in A$ s.t.

$$\lambda(\beta_1, \dots \beta_r) \equiv \alpha$$

is a tautology. Moreover, there is a c s.t. all such tautologies are provable in c steps. The argument of Theorem 19 can be repeated with $\alpha_1, \dots \alpha_m$ in place of the truth-values $0, 1$, using identity rules in place of axioms where appropriate. (Note that this requires writing the formulas $\theta_1 \dots \theta_n$ in reverse order in Δ.) QED

2.2 Non-constant lower bounds

It is now apparent that proving even non-constant lower bounds in FI and FIr may not be a trivial matter. Not too difficult, though. We want to apply the results of this section to a variety of systems, and hence we state the theorems in quite a general form. The reader may want first to have a look at the applications in 2.2.1 and 2.2.2.

Let us first introduce several definitions.

1. *A language* L is a finite list of *logical connectives* and infinitely many propositional variables. *Formulas of* L are defined in the usual way,

2. *A logic* P is a set of formulas in a fixed language L s.t. the set is closed under substitutions of formulas for propositional variables. Formulas in P are P*-tautologies.* We shall also assume that P is non-degenerate, that not all formulas are P-tautologies. The term *"logic"* is intended to include classical and intuitionistic propositional logic, and modal logic.

3. L^+ is obtained by adding to L an infinite list of *second-order variables* $X, Y, Z \ldots$, infinitely many for every arity. Hence *variables* will be either propositional variables $p, q, r \ldots$(1-variables) or second-order variables (2-variables) $X, Y, Z \ldots$. *Second-order formula (2-formula)* is defined inductively as follows:

   (a) Every 1-variable is a 2-formula,

   (b) if f is a logical connective or 2-variable of arity n and $\xi_1 \ldots \xi_n$ are 2-formulas then $f(\xi_1, \ldots \xi_n)$ is 2-formula.

   A substitution is a function σ from variables to 2-formulas s.t. for a 2-variable X of arity n, $\sigma(X)$ has arity $\geq n$. For a 2-formula ψ, ψ^σ is defined by induction as follows:

   (a) $p^\sigma = \sigma(p)$ for a 1-variable p.

   (b) if $\psi = X(\xi_1, \ldots \xi_n)$, X is n-ary variable and $\sigma(X) = \mu(p_1, \ldots p_m)$, where μ is a formula and $m \geq n$, then $\psi^\sigma = \mu(\xi_1^\sigma, \ldots \xi_n^\sigma, p_{n+1}, \ldots p_m)$.[10]

   (c) if $\psi = \beta(\xi_1, \ldots \xi_n)$, β is n-ary logical connective then $\psi^\sigma = \beta(\xi_1^\sigma, \ldots \xi_n^\sigma)$.

   A 2-formula ξ will be called *a substitution instance of a 2-formula* ψ, if there exists a substitution σ s.t. $\xi = \psi^\sigma$.

4. *Generalised Frege rule for* P is a rule of the form

$$\frac{A_1(X_1, \ldots X_k), \ldots A_m(X_1, \ldots X_k)}{B(X_1, \ldots X_k)},$$

   where $A_1, \ldots A_m, B$ are 2-formulas not containing 1-variables, s.t. the rule is sound. That is, for any substitution of 1-formulas for 2-variables, if

[10] Some fixed ordering on the 1-variables must be assumed in this case.

$A_1, \dots A_n$ are P-tautologies then B is also a 2-tautology. *An application of the rule* is a substitution of 1-formulas for the 2-variables in the rule, an inference of the form

$$(GFr) \qquad \frac{A_1(\sigma(X_1), \dots \sigma(X_k)) \dots A_m(\sigma(X_1), \dots \sigma(X_k))}{B(\sigma(X_1), \dots \sigma(X_k))},$$

Frege rule for P is a generalised Frege rule which contains 2-variables of zero arity only.

5. *Frege system for P* is a finite list of Frege rules which is complete, i.e., every P-tautology is derivable by means of the rules. Similarly, *generalised Frege system for P* is a finite complete set of generalised Frege rules. FI and FIr are examples of generalised Frege systems for classical logic (other examples are given in 2.3). Note that generalised Frege system can prove only the formulas in L; second order variables appear only in the formulation of rules and not in their application.

6. Let S be a generalised Frege system. Then S^+ is the extension of S to 2-formulas. S^+ has the same rules like S except that they can be applied to 2-formulas as well. *S^+-tautology* is a 2-formula derivable in S^+. Hence S^+, as opposed to S, does prove 2-formulas. Note that two different generalised Frege systems for the same logic can produce different sets of 2-tautologies (see 2.2.1).

We are now to prove the following theorem:

Theorem 23 *Let S be a generalised Frege system. Then there exists $c \in \omega$ s.t. for every tautology ψ if $S \vdash_k \psi$ then ψ is a substitution instance of a S^+-tautology χ which contains at most $c.k$ variables.*

Lemma 24 *1. Let ψ be a S^+-tautology and δ a variable of arity m which occurs in ψ. Then there exists a connective or 2-variable f different from δ of arity $n \geq 1$ s.t. in ψ occurs a formula of the form $f(\mu_1, \dots, \mu_j, \delta(\lambda_1, \dots \lambda_m), \mu_{j+1}, \dots \mu_{n-1})$. Formulas of this particular form will be written as $f\delta(\mu_1 \dots \mu_{n-1}, \lambda_1, \dots \lambda_m)$.*

2. Let f and δ be as in part 1). Let ξ be a formula and Y a variable of arity $n - 1 + m$ not occurring in ξ. Then there exists a unique *formula $\overline{\xi}$ with the following properties*

(a) $\xi = \overline{\xi}(Y/f\delta)$.

(b) $\overline{\xi}$ does not contain a subformula of the form $f\delta(\mu_1 \dots \mu_{n-1}, \lambda_1, \dots \lambda_m)$.

`Proof.` 1) It is sufficient to take an uppermost occurrence of δ in ψ, when ψ is understood as a tree growing from the root downwards. Since ψ is a S^+-tautology, it cannot have the form $\psi = \delta(\lambda_1, \dots \lambda_m)$, for otherwise the logic would be degenerate.

2) Existence of $\overline{\xi}$ satisfying the properties is clear. Uniqueness follows from the fact that f and δ are different. `QED`

Let δ be a variable. We shall say that δ is *critical* in an S^+ application of generalised Frege rule of the form (GFr), if $\sigma(X_i)$ has the form $\delta(\mu_1, \dots \mu_m)$ for some $i = 1, \dots k$. A variable will be called critical in S^+-proof K if it is critical in some step of the proof.

Lemma 25 *1. There exists d s.t. every S^+ proof K with k proof-lines contains at most $d.k$ critical variables.*

2. Let K be a S^+ proof of ψ with k proof-lines. Assume that a variable X occurs in ψ and is not critical in K. Let $\overline{\psi}$ be as in Lemma 24, part 2). Then $S^+ \vdash_k \overline{\psi}$.

`Proof.` 1) is clear. 2). Let $K = \xi_1 \dots \xi_k$, $\xi_k = \psi$. It is sufficient to verify that $\overline{K} = \overline{\xi_1}, \dots \overline{\xi_k}$ is a $FI2$ proof. But that is easy. `QED`

Proof of Theorem 23. We will prove a more general statement, that there exists $c \in \omega$ s.t. for every 2-formula ψ if $S^+ \vdash_k \psi$ then ψ is a substitution instance of a S^+-tautology χ which contains at most $c.k$ variables. Let d be the constant from Lemma 25, part 1). We will proceed by induction with respect to the size of ψ, where size is simply the number of symbols in ψ. Assume that $\vdash_k \psi$. If ψ has at most $d.k$ variables, or is of size at most $d.k$, the proposition is true trivially. Assume that ψ contains more than $d.k$ variables and K be a proof of ψ with k proof-lines. By Lemma 25, part 1), there is a variable δ occurring in ψ which is not critical in K. By part 2) of the Lemma, $\overline{\psi}$ has a proof with k proof lines. But $\overline{\psi}$ has a smaller size than ψ and by the inductive assumption there exists a tautology χ with $d.k$ variables s.t. $\overline{\psi}$ is a substitution instance of χ. Since ψ is a substitution instance of $\overline{\psi}$ then ψ is also a substitution instance of χ. This completes the proof.`QED`

Theorem 23 is intended to give lower bounds for tautologies containing many propositional variables. It is quite powerless if the tautology contains, say, one variable, for then the tautology itself satisfies the conclusion of the Theorem. This does not matter, if we are interested in the systems FI and FIr (Theorems 21 and 22). However, in the case of systems like intuitionistic or modal logic a different consideration is necessary.

Let S be a Frege system for a logic P. We will assume that the language of S contains the symbol $\equiv$ which has some basic properties: $p \equiv p$ is a P-tautology, and S contains the rules

$$\frac{X \equiv Y}{Y \equiv X}, \qquad \frac{X \equiv Y, Y \equiv Z}{X \equiv Z}, \qquad \frac{X, X \equiv Y}{Y},$$

or some rules with the same function. Moreover, assume that the identity rule is sound over P. Then SIr will be the system S plus the identity rule. If T is a set of formulas we will write that $T \vdash \psi$, if ψ is provable in SIr using the formulas in T as axioms. In particular, if T contains $\xi \equiv \xi'$ than the formula can be used as a premiss of an identity rule.

Let $\xi_i, i \in I$ be a list of formulas s.t. $\xi_i \equiv \xi_j$ is not a P tautology for any $i, j \in I, i \neq j$, and let $p_i, i \in I$ be a list of variables. Then $\psi(\xi_i/p_i, i \in I)$ will be defined as follows (we abbreviate $\psi(\xi_i/p_i, i \in I)$ by $\psi^\star$):

1. if $S \vdash \psi \equiv \xi_i$ for some $i \in I$ then $\psi^\star := p_i$.
2. Otherwise, if ψ has the form $\lambda(\psi_1, \ldots \psi_n)$ for a logical connective λ, we let $\psi^\star := \lambda(\psi_1^\star, \ldots \psi_n^\star)$. If ψ is a variable or a constant we let $\psi^\star = \psi$.

Proposition 26 *Let S be a Frege system for logic P. Then there exists $c \in \omega$ with the following properties: let $SIr \vdash_k \psi$. Let $\xi_i, i \in I$ and $p_i, i \in I$ be as above, where the variables p_i do not occur in ψ. Let T be the theory containing all formulas of the form $p_j \equiv \theta(\xi_i/p_i, i \in (I \setminus \{j\}))$, for $j \in I$ and θ provably equivalent to ξ_j in S. Then*

$$T \vdash_{c \cdot k} \psi(\xi_i/p_i, i \in I).$$

`Proof.` For a formula γ, let $\gamma^\star$ be an abbreviation for $\gamma(\xi_i/p_i, i \in I)$. First, let us note the following:

Claim. *For a formula $\alpha(q_1, \ldots q_m)$ of size n and $\beta_1, \ldots \beta_m$ arbitrary formulas*

$$T \vdash_{O(n)} (\alpha(\beta_1, \ldots \beta_m))^\star \equiv \alpha(\beta_1^\star, \ldots \beta_m^\star)$$

The claim is proved easily by induction over the depth of α.

We must show that if $K = \gamma_1 \ldots \gamma_l$ is a SIr proof then every $\gamma_1^\star \ldots \gamma_l^\star$ can be proved over T using at most $c \cdot l$ steps, for a constant c whose size will be clear from the following. Proceed by induction with respect to l.

Assume that the last inference in K is an application of a Frege rule

$$\frac{A_1(\sigma(X_1), \ldots \sigma(X_k)), \ldots A_m(\sigma(X_1), \ldots \sigma(X_k))}{B(\sigma(X_1), \ldots \sigma(X_k))}.$$

By the assumption the formulas $(A_1(\sigma(X_1), \ldots \sigma(X_k)))^\star, \ldots (A_m(\sigma(X_1), \ldots \sigma(X_k))^\star$ are provable in $c \cdot (l-1)$ steps. From the Claim also the formulas $(A_1(\sigma(X_1)^\star, \ldots \sigma(X_k)^\star)), \ldots, A_m(\sigma(X_1)^\star, \ldots \sigma(X_k)^\star)$ are provable over T using additional inferences whose number depends only on the size of $A_1, \ldots A_m$. Hence we are allowed to use the inference

$$\frac{A_1(\sigma(X_1)^\star, \ldots \sigma(X_k)^\star), \ldots A_m(\sigma(X_1)^\star, \ldots \sigma(X_k)^\star)}{B(\sigma(X_1)^\star, \ldots \sigma(X_k)^\star)}.$$

The statement then follows by another application of the Claim to the formula B. Altogether, we proved $\gamma_l^\star$ in $c \cdot (l-1) + s$ steps, where s depends on the used Frege rule only.

Assume that the last inference was an identity rule

$$\frac{\theta_1 \equiv \theta_2}{\Delta(q/\theta_1) \equiv \Delta(q/\theta_2)}.$$

As above, it is sufficient to simulate the inference

$$\frac{\theta_1^\star \equiv \theta_2^\star}{(\Delta(q/\theta_1))^\star \equiv (\Delta(q/\theta_2))^\star}.$$

From the definition of $\Delta(q/\theta_1))^\star$ and $(\Delta(q/\theta_2))^\star$ and the fact that $S \vdash \theta_1 \equiv \theta_2$ we can find a formula $\Gamma(q)$ s.t.

$$(\Delta(q/\theta_1))^\star = \Gamma(q/\theta_1^\star) \qquad \text{and} \qquad (\Delta(q/\theta_1))^\star = \Gamma(q/\theta_2^\star).$$

Hence it is sufficient to apply the rule

$$\frac{\theta_1^\star \equiv \theta_2^\star}{(\Gamma(q/\theta_1^\star) \equiv \Gamma(q/\theta_2^\star)}.$$

Again, the inference requires only a bounded number of additional steps. QED

2.2.1 *FI* and *FIr*

We shall now apply Theorem 23 to give specific examples of tautologies not provable in FI and FIr in a bounded number of steps. This requires to give a semantic specification of FI^+ and FIr^+ tautologies. Although the systems FI and FIr are formalisations of the same logic, the sets FI^+ and FIr^+ are different. This fact will be used to separate the systems. We will also see that the system FI^+ is complete with respect to the natural interpretation of 2-formulas. This fact will be used in Section 2.3 to show that FI is an optimal generalised Frege system for classical propositional logic.

The system FI^+ is obtained by extending the language of propositional logic by second-order variables. Its tautologies can be defined as the formulas derivable by means of propositional logic, and the axioms

$$\xi \equiv \xi' \to X(\ldots,\xi,\ldots) \equiv X(\ldots,\xi',\ldots),$$

for any 2-variable X and any 2-formulas ξ and ξ'.

Similarly, the system FIr^+ can be characterised by the rule

$$\frac{\xi \equiv \xi'}{X(\ldots,\xi,\ldots) \equiv X(\ldots,\xi',\ldots)}.$$

Proposition 27 *1. A 2-formula is FI^+ tautology iff it is a propositional tautology for any interpretation of 2-variables as truth-functions.*

2. If a 2-formula is FIr^+ tautology then it is K tautology for any interpretation of 2-variables as K formulas.

`Proof.` It is easy to see that FI^+-tautologies are true in the interpretation. For the converse, assume that we have a 2-formula Γ which is a propositional tautology for any interpretation of 2-variables as truth-functions. Assume, for simplicity, that Γ contains only a single 2-variable X. Let X have arity n. There are 2^n possible truth-functions of arity n. Let $\alpha_1, \dots \alpha_{2^n}$ be some L-formulas in variables $p_1, \dots p_n$ defining the Boolean functions. Then for every $i = 1, \dots 2^n$ the formula $\Gamma(X/\alpha_i)$ is a 1-tautology. Let $\alpha_i \sim X$ be an abbreviation for the conjunction of 2^n formulas

$$\alpha_i(\sigma(p_1), \dots \sigma(p_k)) \equiv X(\sigma(p_1), \dots \sigma(p_k)),$$

for every assignment σ to the variables $p_1, \dots p_n$. Using the identity axiom, one can prove

$$(\alpha_i \sim X) \to (\Gamma(X/\alpha_i) \equiv \Gamma(X))$$

for every $i = 1, \dots 2^n$. Since $\Gamma(X/\alpha_i)$ is 1-tautology, we also obtain

$$FI^+ \vdash (\alpha_i \sim X) \to \Gamma(X).$$

Finally,

$$FI^+ \vdash \bigvee_{i=1,\dots 2^n} \alpha_i \sim X$$

is a tautology. This, together with the previous formula, completes the proof.

Part 2) is easy. `QED`

Theorem 28 *Let $\xi^n(q)$ be the formula*

$$(\dots((q \wedge p_1) \wedge p_2) \dots) \wedge p_n.$$

Then

1. *there is no $c \in \omega$ s.t. $FI \vdash_c \xi^n(q) \to q$ for every n.*
2. *there is no $c \in \omega$ s.t. $FIr \vdash_c q \equiv q' \to \xi^n(q) \equiv \xi^n(q')$ for every n.*

`Proof.` For part 1) assume the opposite. Then, by Theorem 23, for a sufficiently large n $\xi^n(q) \to q$ is a substitution instance of an FI^+ tautology θ_1 with $< n$ variables. Inspecting the form of $\xi^n(q) \to q$, we can conclude that it is a substitution instance of FI^+ tautology of the form

$$(\dots((X(\xi^m) \wedge p_{m+1}) \wedge p_{m+2}) \dots) \wedge p_n \to q,$$

for some $0 \leq m \leq n$. Setting the variables $p_1, \dots p_n$ to 1, and applying the identity axiom, we obtain that

$$X(q) \to q$$

is an FI^+ tautology. But that is not the case, for the formula is not a propositional tautology if we interpret X as the constant function 1.

The argument for part 2) is similar. We then obtain that

$$q \equiv q' \to X(q) \equiv X(q')$$

is an FIr^+ tautology. But if we interpret X as $\Box$ of the logic, the formula is not K tautology. QED

2.2.2 Some non-classical logics

We will now show that Theorem 22 is false, if we add the identity rule to modal logic K or intuitionistic propositional logic. We will give examples of tautologies with only two propositional variables which cannot be proved in a bounded number of steps in the systems. The reason is the following: in classical logic we can form only finitely many non-equivalent formulas from a finite list of variables. That is the essence of Theorem 22. In K, however, the formulas $\Box p, \Box\Box p \ldots$ are not equivalent. Similarly, by the result in [20] there are infinitely non-equivalent intuitionistic formulas in one variable.

The system K of modal logic will be introduced in Section 3, and for IL we take the Hilbert style axiomatisation of intuitionistic logic given in Section 4. The system KIr resp. ILr is the system K resp. IL plus the identity rule.

Theorem 29 *1. Let $\eta^n(q)$ be the formula*

$$(\ldots((q \wedge \Box p) \wedge \Box\Box p) \ldots) \wedge \Box^n p.$$

Then there is no $c \in \omega$ s.t. $KIr \vdash_c \eta^n(q) \to q$ for every n.

2. Let $\alpha_i, i \in \omega$ be a sequence of IL formulas with one variable s.t. $IL \not\vdash \alpha_i \equiv \alpha_j$ for $i \neq j$. Let $\eta^n(q)$ be the formula

$$(\ldots((q \wedge \alpha_1) \wedge \alpha_2) \ldots) \wedge \alpha_n.$$

Then there is no $c \in \omega$ s.t. $ILr \vdash_c \eta^n(q) \to q$ for every n.

Proof. Part 1). We shall apply Proposition 26. Assume that the formulas are provable in a bounded number of steps. Let ξ_i be the formula $\Box^i p$ and let $p_i, i \in \omega$ and T be as in the Proposition. Let $\delta_n(q)$ be the formula $(\ldots((q \wedge p_1) \wedge p_2) \ldots) \wedge p_n$. By the Proposition, the formulas $\delta^n(q) \to q$ can be proved in a bounded number of steps from the theory T. For a modal formula A, let A_0 denote the formula obtained by deleting all the boxes in A. We can see that if $KIr \vdash_k A$ then $FI \vdash_k A_0$. Let T_0 be the theory $\{A_0, A \in T\}$. Since $\delta^n(q) \to q$ does not contain modalities, it is provable from T_0 in FI in a bounded number of steps. Since a bounded length proof can use only a bounded number of formulas from T, for every n there exists a subset F_n of T of a bounded size s.t.

$$F_n \vdash \delta^n(q) \to q$$

in a bounded number of steps. Since we now work in FI, we have also

$$\bigwedge F_n \to (\delta^n(q) \to q).$$

By Theorem 23 the formula is then a substitution instance of a FI^+ tautology with a bounded number of variables. As in Theorem 28 we can show that this is impossible.

Part 2) is similar. QED

2.3 Speed-up and Generalised Frege systems

In Section 2.2 we have defined the notion of a generalised Frege system for a logic P. We will now briefly consider generalised Frege systems for classical propositional logic, or simply generalised Frege systems. Let us first give few examples.

Examples of generalised Frege systems.

1. Frege system with identity, FI, with the axiom

$$X \equiv X' \to Z(X) \equiv Z(X').$$

2. *FIr, Frege system with identity rule*

$$\frac{X \equiv X'}{Z(X) \equiv Z(X')}$$

3. *Frege system with generalisation axiom, Fg,* i.e., F plus the axiom

$$(Y(0) \wedge Y(1)) \to Y(X)$$

and also *Frege system with generalisation rule Fgr*, i.e., the rule

$$\frac{Y(0) \wedge Y(1)}{Y(X)}.$$

Substitution Frege system. Substitution Frege system SF is defined as a Frege system F plus the rule

$$\frac{\psi(p)}{\psi(p/\xi)}.$$

Strictly speaking, SF is not a generalised Frege system. This is because we forbid the occurrence of first-order variables in the formulation of a generalised Frege rule. This could be remedied by modifying the definition of generalised Frege system by allowing propositional variables, while requiring that in an application of a rule we are allowed to substitute for 1-variables only 1-variables.

However, such a modification is not necessary, for any such "generalised" generalised Frege rule can be simulated by a generalised Frege rule. In the specific case of SF we will see in Proposition 31 that SF is equivalent to F (in the sense of the Proposition).

Let P_1 and P_2 be generalised Frege systems (in the same language L).

1. We say that P_1 *l-simulates* P_2, if there exists a function $g : \omega \to \omega$ s.t. for every formula ψ if $P_2 \vdash_k \psi$ then $P_1 \vdash_{g(k)} \psi$.
2. We say that P_1 and P_2 are *l-equivalent*, if P_1 l-simulates P_2 and P_2 l-simulates P_1.
3. If P_1 l-simulates P_2 and P_1 and P_2 are not l-equivalent, we say that P_1 *has an unbounded speed-up over* P_2.

The notion of l-simulation relates to number of proof lines and not to size of proofs in the respective systems. Note that in the definition of l-simulation we make no assumption concerning the growth of g: the function may very well be exponential or faster.

In the sense of l-simulation, the system FI is optimal in the class of generalised Frege systems:

Theorem 30 *FI l-simulates any generalised Frege system.*

Proof. Let us say that a generalised Frege system is *proper*, if the only rule with a non-empty assumption is modus ponens. In other words, it consists of modus ponens and a finite list of axioms.

Claim 1. *Every generalised Frege system is l-simulated by some proper generalised Frege system.*

Assume that we have a generalised Frege rule

$$(\star) \qquad \frac{A_1, \ldots A_m}{B}.$$

Let us show that

$$(\star\star) \qquad \bigwedge_{i=1,\ldots m} A_i \to B$$

is a tautology for any substitution σ of 1-formulas for the 2-variables. Without loss of generality we can assume that for any 2-variable X of arity r the arity of $\sigma(X)$ is r. In particular, if X has arity zero then $\sigma(X)$ is the constant 0 or 1. Assume that we have such a substitution and that $(\star\star)$ is not a tautology. Then there is a truth assignment to propositional variables s.t. $\sigma(\bigwedge_{i=1,\ldots m} A_i)$ is true and $\sigma(B)$ is false. However, since we do not allow propositional variables in the formulation of a generalised Frege rule, and by the property of σ, the formulas $\sigma(\bigwedge_{i=1,\ldots m} A_i)$ and $\sigma(B)$ do not contain any propositional variables.

Hence $\sigma(\bigwedge_{i=1,\dots m} A_i)$ is a tautology. But that contradicts the assumption that the rule $(\star)$ was sound. Hence every generalised Frege rule can be replaced by a generalised Frege axiom, without significantly increasing lengths of proofs.

Claim 2. *Every proper generalised Frege system is l-simulated by FI.*

Let S be a proper generalised Frege system. By Proposition 27 every generalised Frege axiom, as being a tautology for any substitution of 1-formulas for 2-variables, is an FI^+ tautology. Let c be a constant s.t. every generalised Frege axiom of S is provable in at most c steps in FI^+. Clearly, if $FI^+ \vdash_c A$ and σ is a substitution of 1-formulas for 2-variables then $FI \vdash_c \sigma(A)$. Hence also every instance of an axiom in S is provable in FI in c steps. This completes the proof of the proposition. QED

The other speed-up relations can be summarised as follows:

Proposition 31 *1. SF and F are l-equivalent.*

2. FIr has an unbounded speed-up over F.

3. FI has an unbounded speed-up over FIr.

4. The systems FI, Fg and Fgr are l-equivalent.

Proof. 1). We can transform a SF proof into a tree-like form, with an exponential increase of the number of proof-lines. In a tree-like proof, we can eliminate the substitution p/ξ by replacing all preceding occurrences of p by ξ.

2). It is a well-known fact that there are closed tautologies which do not have bounded length proofs in F. (E.g., $\neg \dots \neg 1$, where the number of negations is even. See [16]) However, all closed tautologies are provable in FI in a bounded number of steps.

3). Consider the formulas from Theorem 28, part 2). The formulas are instance of the identity axiom and hence they can be proved in FI in one step. By the Theorem, they cannot be proved in a bounded number of steps in FIr.

4). It is sufficient to prove that Fgr l-simulates FI. Hence we must show that the scheme of identity is provable in Fgr in a bounded number of steps. Consider the formula $\Gamma(p, q)$

$$p \equiv q \to \psi(p) \equiv \psi(q).$$

Then every substitution of $0, 1$ for the variables p, q in Γ results in a tautology which is provable in F in a bounded number of steps. (Either the consequent is trivially true or the antecedent trivially false.) We can apply twice the generalisation rule to obtain

$$\xi \equiv \xi' \to \psi(\xi) \equiv \psi(\xi').$$

QED

PART II

3 Modal logic

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 $g : \omega \rightarrow \omega$ find (or decide whether it exists) a sequence of Q-tautologies $\psi_1, \psi_2, \dots$ such that for every $i \in \omega$ every Q-proof of ψ_i must have size at least $g(|\psi_i|)$.[11]

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 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 for it is 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 $NP \neq coNP$.

We will prove an exponential lower bound on the number of proof lines in the basic system of modal logic, K. We will then extend the result to other systems of modal logic, as well as to intuitionistic propositional calculus (in Section 4). The lower bound 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 [23], 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

[11] $|\psi_i|$ 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.

of size polynomial in n separating $Color_{k+1}$ and $Clique_k$. This approach has been first applied by Krajíček [16] 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 Theorems 7 and 10 for the exact formulation), and we show that every 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.

3.1 Monotone interpolation for 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.

The characteristic set of clauses of a K proof.
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.

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

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

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 37. 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 $C_{>1}$. `QED`

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.` 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 $\mathcal{C}_S, \{\Box B_1\}, \dots \{\Box B_k\}, \{\neg \Box B\}$ is not satisfiable then the formula

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

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

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

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. `QED`

Let $\Box A_1, \dots \Box A_k$ be the immediate modal subformulas of α. An assignment σ to the variables $V = \Box A_1, \dots \Box A_k$ 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 $\Box A_1, \dots \Box A_k$ be the immediate modal subformulas of α. Let S be a K proof of*

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

Let $V = \Box A_1, \dots \Box A_k$. 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 $\overline{s}$ be the list of variables occurring in a non-modal context in S. Let ρ' be the assignment to $\overline{s}$ 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, $j \in 1, \dots k$. 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. `QED`

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

`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 $V = \Box A_1, \dots \Box A_k$. 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 $\alpha(\Box A_1, \dots \Box A_k, \overline{s}) \to [C_1](\Box A_1, \dots \Box A_k) \vee [C_2](\Box A_1, \dots \Box A_k)$ 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 $M \models [C_1](\Box A_1, \dots \Box A_k)$ or $M \models [C_2](\Box A_1, \dots \Box A_k)$.

Let us show that 1) is a K tautology. Assume that $M \models [C_1](\Box A_1, \dots \Box A_k)$ 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 $M \models \Box\beta_1$. `QED`

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 $\alpha(\Box p_1, \dots \Box p_k, \overline{s}) \to (\Box\beta_1(\overline{p}, \overline{r_1}) \vee \Box\beta_2(\overline{p}, \overline{r_2}))$ be a K tautology, where $\alpha(p_1, \dots p_k, \overline{s})$, 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 $\overline{p}$ with the following properties: for any assignment σ to the variables $\overline{p}$*

1. *if $\alpha(\overline{p}, \overline{s})$ is true (for some assignment to $\overline{s}$) then $C_1(\overline{p}) = 1$ or $C_2(\overline{p}) = 1$,*
2. *if $C_1(\overline{p}) = 1$ resp. $C_2(\overline{p}) = 1$ 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. `QED`

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 function of a gate from X_i to a is that 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 $d \in \mathrm{Pred}(b)$. For a gate from $X \subseteq \mathrm{Pred}(b)$ 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. QED

3.1.1 Model theoretic reading of the proof

The original proof of monotone interpolation for K was based on a model theoretic construction (see [10]). Let us here sketch the main points. We want to count only the applications of distributivity axioms in a K proof, hence we can work in the theory K_5^0 which does not contain the distributivity axiom. 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 Razborov's proof of lower bound on monotone circuit size, see [13].

The theory $\mathbf{K_5^0}$. The theory K_5^0 will have, in addition to the propositional rules, the rules of *generalisation* and *transparency*

$$(G) \quad \frac{A}{\Box A}, \qquad\qquad (T) \quad \frac{A \equiv B}{\Box A \equiv \Box B}$$

and the axiom scheme

$$(V) \qquad \Box((A_1 \wedge \Box B) \vee (A_2 \wedge \neg\Box B)) \equiv (\Box A_1 \wedge \Box B) \vee (\Box A_2 \wedge \neg \Box B)$$

By means of the strange looking axiom (V) every formula of K_5^0 can be transformed to a formula of modal depth one. Its role is to simplify models of K_5^0, and in principle it is dispensable.

The relevant connection between K_5^0 and K is following:

Proposition 1. *Let A be a K tautology. and let Γ be the set of distributivity axioms occurring in a K proof of A. Then $\bigwedge \Gamma \to A$ is a K_5^0 tautology.*

Models for $\mathbf{K_5^0}$. Let U denote the set of all possible truth assignments to propositional variables (i.e., U is infinite). Let $\mathcal{G} \subseteq P(U)$ be fixed. For $v \in U$ and a modal formula A we define that

$$v \Vdash A$$

by induction as follows:

1. For a variable p, $v \Vdash p$, if p is assigned 1 in v.

2. We let $v \Vdash A_1 \wedge A_2$ iff $v \Vdash A_1$ and $v \Vdash A_2$. We let $v \Vdash \neg A$ iff not $v \Vdash A$, and similarly for other connectives.

3. Finally, assume that the relation $u \Vdash A$ has been defined for any $u \in U$. Let
$$[A] := \{u \in U; u \Vdash A\}\,.$$
Then let $v \Vdash \Box A$ iff $[A] \in \mathcal{G}$.

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.)

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

$\mathcal{G}$ and distributivity axioms. Note that, using the transparency rule, the distributivity axiom $\Box(A \to B) \to (\Box A \to \Box B)$ can be replaced by a pair of axioms of the form

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

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

If A and B do not contain modalities then the axioms impose the following conditions on $\mathcal{G}$:

1. $X, Y \in \mathcal{G} \to X \cap Y \in \mathcal{G}$

2. $X \in \mathcal{G}, X \subseteq Y \to Y \in \mathcal{G}$

In other words, distributivity axioms require $\mathcal{G}$ to be a filter.

3.2 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 $\overline{p}$, and that the sets of variables $\overline{p},\overline{s},\overline{r}$.

Proposition 6 *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 $\beta_1 := \beta$, $\beta_2 :=\perp$.
`QED`

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 $\overline{p}$. To be exact, $\overline{p}=p_{i_1i_2}, i_1,i_2=1,\dots n$, $\overline{r}=r_{ij}, \overline{s}=s_{ij}, i=1,\dots n, j=1,\dots k$. $Clique_n^k(\overline{p},\overline{r})$ is the formula

$$\bigwedge_j \bigvee_i r_{ij} \wedge \bigwedge_i \bigwedge_{j_1\neq i_2} (\neg r_{ij_1} \vee \neg r_{ij_2}) \wedge \bigwedge_{i_1\neq i_2, j_1, j_2} (r_{i_1j_1} \wedge r_{i_2j_2} \to p_{i_1i_2})$$

and $Color^k_n(\overline{p},\overline{s})$ 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 indices i range over $1,\dots n$ and j over $1,\dots k$.

Theorem 7 *Let*

$$\Theta^k_n := Clique^{k+1}_n(\Box\overline{p},\overline{r}) \rightarrow \Box(\neg Color^k_n(\overline{p},\overline{s})).$$

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

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

modal rules.

`Proof.` Assume that Θ^k_n has a K-proof with m modal rules. By the previous proposition, there is a monotone interpolant C of $Clique^k_n(\overline{p},\overline{r})$ and $\neg Color^k_n(\overline{p},\overline{s})$ 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. One could obtain a hard K tautology of the form $\alpha(\Box\overline{p},\overline{s}) \rightarrow \Box\beta$ also by exploiting the gap between monotone and general circuits, as in Section 4. The same applies to the tautologies of the form offered in Example 2.

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

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

Lemma 8 *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 $\overline{p} = p_1,\dots p_n$ and $\overline{q} = q_1,\dots q_n$. 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 $\bigwedge_{i=1,\dots n}(p_i \vee q_i) \rightarrow \beta_1(\overline{p},\overline{r_1}) \vee \beta_2(\overline{q},\overline{r_2})$ is a classical tautology.

(2) Let M, N be subsets of $\{1,\dots n\}$ s.t. $M \cup N = \{1,\dots n\}$. Then one of the following is a classical tautology:

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

`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

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

and

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

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. `QED`

Proposition 9 *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

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

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

From 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

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

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

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

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

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

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

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

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

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

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

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), $C(\overline{p})=1$. QED

Theorem 10 *Let*

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

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 9 on the formulas $\beta_1 := \neg\mathit{Color}_n^k(\overline{p},\overline{s})$ and $\beta_2 := \neg\mathit{Clique}_n^{k+1}(\neg\overline{q},\overline{r})$. First, β_2 is monotone in $\overline{q}$ since $\mathit{Clique}(\overline{p},\overline{r})$ 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 $\beta_2(\overline{q}/\neg\overline{p},\overline{r}) = \neg\mathit{Clique}_n^{k+1}(\overline{p}/\neg\neg\overline{p},\overline{r})$ is classically equivalent to $\neg\mathit{Clique}_n^{k+1}(\overline{p},\overline{r})$ and

$$\neg\mathit{Color}_n^k(\overline{p},\overline{s}) \vee \neg\mathit{Clique}_n^{k+1}(\overline{p},\overline{r})$$

is a classical tautology. Hence Θ_n^k is a K tautology. Assume that it has an 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 $\mathit{Clique}_n^{k+1}(\overline{p},\overline{r})$, C interpolates $\mathit{Clique}_n^{k+1}(\overline{p},\overline{r})$ and $\neg\mathit{Color}_n^k(\overline{p},\overline{s})$. By the result in [1] every such circuit must have size at least $2^{\Omega(n^{\frac{1}{4}})}$. Hence $m \geq \sqrt{2^{\Omega(n^{\frac{1}{4}})}} \sim 2^{\Omega(n^{\frac{1}{4}})}$. QED

3.3 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 seem 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 $A,\ A \rightarrow B \in cl(\mathcal{A})$ 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 11 *Let G and $\mathcal{A} = \{A_1, \dots A_k\}$ 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 $V = \langle A_1\rangle, \dots \langle A_k\rangle$ 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. `QED`

Lemma 12

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 $S = A_1, \dots A_n$ 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 $i = 1, \dots n$ (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 $\bigwedge_{A \in \mathcal{A}} \Box A \rightarrow \Box B$ 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. QED

Lemma 13 *Let α be a formula and let $\mathcal{A} = A_1, \dots A_k$ be its immediate modal subformulas, let $V = \langle A_1 \rangle, \dots \langle A_k \rangle$. Let S be a K proof of*

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

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. QED

Theorem 14 *Let S be a K proof of the formula*

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

Let $\Box A_1, \dots \Box A_k$ 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 $v_1, \dots v_k$ of size $O(n+k)^2$ s.t. the following are K tautologies:

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

Proof. As in Theorem 4. QED

3.4 Applications to other modal systems

3.4.1 K$_4$ and Gödel-Löb's logic

The system K_4 is the system K plus the axiom

$$\Box A \rightarrow \Box\Box A.$$

Gödel-Löb's logic is obtained by extending K_4 by one more axiom

$$\Box(\Box A \rightarrow A) \rightarrow \Box A.$$

In the proof of Theorem 4 we used only the fact that the characteristic set of clauses of a modal 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 and Gödel-Löb logic and some others. For example, the K_4 axiom

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

receives the clause

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

The theorem and its corollary[12] hold also for those systems without modification. The same argument applies also to the system

$$K + \Box\Box \perp .$$

That is remarkable since the system is in NP.

However, let us here reduce lower bounds for those systems to the lower bound for K. The following Proposition is also remarkable for other reasons: it shows that in a K proof of a tautology of modal depth one we can assume, as far as the number of applications of modal rules is concerned, that in the proof we use only formulas of modal depth one. Second, it shows that there is no speed-up between K_4, Gödel-Löb's logic and K on tautologies of modal depth one, when the number of modal rules is considered.

Proposition 15 *Let A be a tautology of K, K_4, or Gödel-Löb's logic of modal depth one. If A has has a proof with n modal rules than A has a K proof with $O(n)$ modal rules. Moreover, the proof is such that all the formulas in the proof have modal depth one.*

`Proof.` For a formula A, let $A^\star$ denote the formula obtained by deleting all the boxes in A which are in a range of another $\Box$, and let A^0 be the formula obtained by deleting all the boxes. Then B^0 is a propositional formula and $B^\star$ is a formula of modal depth one. First note that if A is a K_4 tautology then A^0 is a propositional tautology. Second, let us prove the following:

Claim. *If A has K_4 proof with n modal rules then $A^\star$ has a K proof with n modal rules, all of which have modal depth one.*

Let $S = A_1, \ldots A_k$, $A_k = A$ be a proof of A with n modal rules. Let Γ be the set of distributivity axioms, the K_4 axioms and the conclusions of generalisation rules used in S. Then $|\Gamma| = n$. Let $S^\star = A_1^\star, \ldots A_k^\star$ and $\Gamma^\star = \{\gamma^\star, \gamma \in \Gamma\}$. Then $|\Gamma^\star| \leq n$. It is easy to see that every formula in $S^\star$ is provable from $\Gamma^\star$ by means of propositional logic only. Moreover, if B is an axiom of distributivity then $B^\star$ is also an axiom of distributivity. The translation od a K_4 axiom $(\Box B \to \Box\Box B)^\star$ is the propositional tautology $\Box B^0 \to \Box B^0$. If $\Box B$ is a conclusion of generalisation rule then B is K_4 tautology and $(\Box B)^\star = \Box B^0$, where B^0 is a propositional tautology. Hence $\Box B^0$ is provable by the single modal inference

$$\frac{B^0}{\Box B^0}.$$

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

Altogether, every formula in $\Gamma^\star$ is provable in K using at most one modal rule, each of modal depth one.

The statement for K and K_4 follows from the Claim and the fact that $A^\star = A$ for a modal depth one formula. For Gödel-Löb's logic the translation must be slightly modified. We let A^0 be the formula obtained by replacing all the immediate modal subformulas in A by the constant 1. $A^\star$ is then obtained by replacing every immediate modal subformula $\Box B$ of A by $\Box B^0$. Then B^0 is a propositional formula and $B^\star$ is a formula of modal depth one. Note that if A is a Gödel-Löb's tautology then A^0 is a propositional tautology. The proof then proceeds in a similar way. `QED`

Corollary *The theorems 4, 7 and 10 are true also in K_4 and Gödel-Löb's logic.*

3.4.2 S and S_4

S resp. S_4 is the logic K resp. K_4 plus the modal rule

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

As will be shown in Theorem 20 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 the systems are equivalent (as far as the number of modal rule modal rules is concerned).

For a formula ψ, 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 16 *Let ψ be S resp. S_4 tautology. Then ψ^s is K resp. K_4 tautology. Furthermore, if ψ has a S-proof resp. S_4 proof with n modal rules then ψ^s has a K resp. K_4 proof with at most $O(n)$ modal rules.*

`Proof.` The part for S is easy. For S_4 observe that the S_4 modal rule $\Box A \to \Box\Box A$ translates to

$$(\Box A^s \wedge A^s) \to (\Box(\Box A^s \wedge A^s) \wedge \Box A^s \wedge A^s),$$

which is provable in K_4 using no more than, say, ten modal rules. `QED`

Proposition 17 *Let α be a propositional formula monotone in $\overline{p} = p_1, \ldots p_n$ and β_1, β_2 propositional formulas. Let*

$$\Theta := \alpha(\Box p_1, \ldots, \Box p_n) \to (\Box\beta_1 \vee \Box\beta_2).$$

Then if Θ has a S-proof resp. S_4 proof with n modal rules then Θ has K-proof with $O(n)$ modal rules. (α may contain non-modalised variables,) `Proof.` We will prove the proposition for S, the part for S_4 follows similarly from the previous Lemma and Proposition 15.

Assume that Θ has S-proof with n modal rules. Then Θ^s has K-proof with $O(n)$ modal rules, where

$$\Theta^s = \alpha(\Box p_1 \wedge p_1, \ldots, \Box p_n \wedge p_n) \rightarrow (\Box\beta_1 \wedge \beta_1 \vee \Box\beta_2 \wedge \beta_2).$$

Hence also

$$\Theta_2 := \alpha(\Box p_1 \wedge p_1, \ldots, \Box p_n \wedge p_n) \rightarrow (\Box\beta_1 \vee \Box\beta_2)$$

has a K-proof with $O(n)$ modal rules. Substituting throughout the proof $\Box p_i$ for p_i, $i = 1, \ldots n$, we obtain that also

$$\Theta_3 := \alpha(\Box\Box p_1 \wedge \Box p_1, \ldots, \Box\Box p_n \wedge \Box p_n) \rightarrow (\Box\beta_1(\overline{p}/\Box\overline{p}) \vee \Box\beta_2(\overline{p}/\Box\overline{p})$$

has a K proof with $O(n)$ modal rules. From the Claim in the proof of Proposition 15, the formula $\Theta_3^\star$ is K-tautology and has a K-proof with at most n modal rules. However,

$$\Theta_3^\star = \alpha(\Box p_1 \wedge \Box p_1, \ldots, \Box p_n \wedge \Box p_n, \overline{r}) \rightarrow (\Box\beta_1 \vee \Box\beta_2).$$

Hence $\Theta_3^\star$ is equivalent to Θ using just propositional rules. Therefore Θ has K-proof with $O(n)$ modal rules. `QED`

Corollary *The theorems 7 and 10 are true also in K_4 and Gödel-Löb's logic.*

3.4.3 K$_{4.5}$ and some speed-up relations

The theory $K_{4.5}$ is the theory K_4 plus the axiom

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

Our results do not apply to $K_{4.5}$ (and hence to S_5). It can be shown that tautologies of Theorems 7 and 10 a) require only a polynomial number of modal rules in $K_{4.5}$ and b) have a polynomial size proof assuming that certain classical tautologies have polynomial size Frege proofs. The same applies to all other hard tautologies mentioned above. This is no coincidence; it can be shown there exists a certain simulation between $K_{4.5}$ and classical Frege system. Namely, to every $K_{4.5}$ tautology A one can in polynomial time assign a classical propositional tautology A^c s.t. A has a $K_{4.5}$ proof with a polynomial number of proof-lines iff A^c has a classical Frege proof with a polynomial number of proof-lines. (See [12]). Hence to prove a lower bound on the number of proof-lines in $K_{4.5}$ is as difficult as to prove lower bound in extended Frege system.

We will show that a variant of the tautology of Theorem 7 has a polynomial-size proof in $K_{4.5}$. Since this variant has only exponential proofs in K or K_4, this implies that there is an exponential speed-up between $K_{4.5}$ and K resp. K_4 on tautologies of modal-depth one.

Lemma 18 *Let A be a K-tautology of modal depth one. Assume that the variables $\overline{r} = r_1, \dots r_k$ do not occur in A in a modal context. Assume that $A(\Box\overline{r})$ has a K-proof with n modal rules. Then A has a K-proof with $O(n+k)$ modal rules.*

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

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

Let $S = A_1, \dots A_m$ be the proof of $A(\Box\overline{r})$. As in Proposition 15 we can easily show that $A^\star_m = (A(\Box\overline{r}))^\star$ is provable in K using $O(n)$ modal rules. However,

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

and $\Box 1$ is provable using only one generalisation, and hence $(\Box r_i)^\star \equiv r_i$ is provable using only one generalisation rule. Hence also the equivalence

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

using only k modal rules. Altogether, A is provable with $O(n+k)$ modal rules.
`QED`

Theorem 19 *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 $K_{4.5}$.*

`Proof.` Let Θ be the tautology

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

Hence Θ differs from the tautology of Theorem 7 only by the substitution $\overline{r}/\Box\overline{r}$. 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 $K_{4.5}$.

The proposition *Clique* is written in such a way that all the negations in *Clique* are attached to variables $\overline{r}$. Note that in $K_{4.5}$ we can prove

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

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

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

can be proved by a linear-size proof in $K_{4.5}$. However, the propositional implication

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

can be proved by a polynomial size proof in a classical Frege system, as shown in [5]. 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 $K_{4.5}$. QED

The importance of the Theorem 19 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, K_4 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 20 *Let P be K, K_4, 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 $A_1,\ A_2,\ A_3,\ldots$ which have only exponential-size proofs in P. Let λ be the formula $\Box p \rightarrow p$, for a variable p not occurring in A_i, $i = 1, 2, \ldots$. Let us have the sequence

$$A_1 \vee \lambda,\ A_2 \vee \lambda,\ A_3 \vee \lambda, \ldots.$$

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. As in Proposition 15 we can show that if η has a proof in P with n modal rules then $\eta^\star$ has a proof in P with n modal rules. But

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

which is - using just one generalisation - equivalent to A_i. QED

4 Intuitionistic logic

In this section we prove an exponential lower bound for intuitionistic propositional calculus IL. The presentation is closely related to that for modal logic. In particular, we prove that IL has a form of *effective monotone interpolation property.* Weaker results in this direction were reached earlier by Buss, Mints and Pudlák (see [6], [7] and [22]). The results presented here were first proved in [11], via translation of IL to K (see Section 4.1.1). The proof given here is direct, and it resembles the traditional methods.

As a remarkable consequence we obtain an exponential speed-up between intuitionistic and classical propositional calculus. We present relatively natural examples of IL tautologies which have polynomial size classical proofs, but only exponential size IL proofs. This can be taken as a nice illustration of how the law of excluded middle simplifies proofs. The other side of the coin is that our results cannot be extended to classical logic. So far, lower bounds for systems of classical propositional logic were achieved for artificial proof systems only, like resolution and bounded-depth Frege. The problem of proving lower bounds for the usual axiomatisation of classical propositional logic, the so called Frege system, is one of the basic open problems of proof complexity. And we leave it unchallenged. From the formulation of the proof of lower bound for IL, it is apparent that the method does not generalise to classical logic. (See also Section 4.3.)

4.1 Monotone interpolation for IL

We will use a Gentzen style axiomatisation of intuitionistic logics. 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*

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

the weakening

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

and the inferences

LEFT	RIGHT
$\dfrac{\Gamma, A \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}, \qquad \dfrac{\Gamma, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}$	$\dfrac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}, \qquad \dfrac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$
$\dfrac{\Gamma, A \Rightarrow C, \qquad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C}$	$\dfrac{\Gamma \Rightarrow A, \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B},$
$\dfrac{\Gamma \Rightarrow A, \Delta, \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \to B \Rightarrow \Delta}$	$\dfrac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \to B},$

An IL proof of a formula A is a proof of the sequent $\Rightarrow A$. *The total 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 total sequent size of S.

Let us also state the usual Hilbert style axiomatisation of IL. The only rule of inference is modus ponens

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

The axioms are the following:

Ax1	$A \to (B \to A)$
Ax2	$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
Ax3	$\bot \to A$
Ax4, Ax5	$A \wedge B \to B, \quad A \wedge B \to A$
Ax6	$(A \to (B \to C)) \to (A \wedge B \to C)$
Ax7, Ax8	$A \to A \vee B, \quad B \to A \vee B$
Ax9	$(B \to A) \to ((C \to A) \to (B \vee C \to A))$

The relation between Hilbert style and Gentzen style axiomatisation is the following:

Proposition 21 *Let A be a formula. Then the sequent $\Rightarrow A$ has a proof in the Gentzen style calculus for IL iff A is provable in Hilbert style calculus for IL. Moreover, if A has a Hilbert style proof with n proof lines then $\Rightarrow A$ has a proof of total sequent size $O(n)$, and vice versa.*

Characteristic set of clauses of IL proof.
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

$$A_1, \ldots A_k \Rightarrow B$$

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

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

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 $\mathcal{C}_S$ corresponds to the total 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). $\Theta_\sigma(A \circ B) \leq \Theta_\sigma(A) \circ_B \Theta_\sigma(B)$

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

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

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

Lemma 22 *Let $S = \Pi_1, \ldots \Pi_n$ be an IL proof.*

1. *Let $B_1, \ldots B_k$ and B be formulas. Let $\mathcal{C}_S, \{\langle B_1\rangle\}, \ldots \{\langle B_k\rangle\}, \{\neg\langle B\rangle\}$ be unsatisfiable. Then*
$$\bigwedge_{i=1,\ldots k} B_i \to B$$
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 premiss 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 $\Theta_\sigma(A \circ B) \leq \Theta_\sigma(A) \circ_B \Theta_\sigma(B)$. 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

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

and we want to show that

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

From $(\star)$ we have $a \leq \Theta_\sigma(A) \to_B \Theta_\sigma(B)$. 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 $a \leq \sigma\langle A \to B\rangle$, which implies $(\star\star)$. The other rules are analogous. QED

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

Lemma 23 *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. QED

Theorem 24 *Let α be a monotone formula in variables $\overline{p}$ of size k. Assume that S is an IL proof of the tautology*

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

Assume that the total 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. QED

4.1.1 Translating IL to K

Another way how to prove lower bound for IL would be to reduce it to the lower bound for K. We can give a translation of intuitionistic logic to K s.t. for any intuitionistic tautology A its translation A^t is a K tautology. The translation is not in general faithful, it may happen that A^t is a tautology without A being so. Also, the translation is not polynomial. However, there is a polynomial (linear) relation between the number of proof-lines in an intuitionistic proof of A and number of *modal rules* in K-proof of A^t.

For an intuitionistic formula A of IL, its translation A^t to K is defined as follows:

1. $p^t = \Box p$ and $\bot^t = \bot$.
2. $(A \to B)^t = \Box A \wedge A^t \to \Box B \wedge B^t$.
3. $(A \vee B)^t = (\Box A \wedge A^t) \vee (\Box B \wedge B^t)$.
4. $(A \wedge B)^t = A^t \wedge B^t$.

We can think of the translation as a combination of three different translations: a) the Gödel translation from IL to $S4$, b) the translation from $S4$ to $K4$, i.e., $(\Box A)^t = \Box A^t \wedge A^t$, and c) the translation from $K4$ to K which was employed in [10] and Proposition 15, based on deleting all boxes which are in a scope of another $\Box$. In the following proposition we think about Hilbert style axiomatisation of IL (for a proof see [11]):

Proposition.

(1) If A is IL-tautology then A^t is K-tautology.

(2) If A has IL-proof with n proof-lines then A^t has a K-proof with $O(n)$ modal rules.

Let us show how the proposition can be used to prove Theorem 25. The translation of the IL tautology of the form

$$(\star) \qquad \bigwedge_{i=1,\dots k} (p_i \vee q_i) \to \beta_1 \vee \beta_2$$

is the K formula (1)

$$(\Box(\bigwedge_{i=1,\dots k} (p_i \vee q_i)) \wedge \bigwedge_{i=1,\dots k} (\Box p_i \vee \Box q_i)) \to \Box(\beta_1 \vee \beta_2) \wedge (\Box\beta_1 \wedge \beta_1^t \vee \Box\beta_2 \wedge \beta_2^t).$$

This implies, using no modal rules,

$$(2) \qquad (\Box(\bigwedge_{i=1,\dots k} (p_i \vee q_i)) \wedge \bigwedge_{i=1,\dots k} (\Box p_i \vee \Box q_i)) \to (\Box\beta_1 \vee \Box\beta_2).$$

However,

$$\bigwedge_{i=1,\dots k}(\Box p_i \vee \Box q_i) \to \Box(\bigwedge_{i=1,\dots k}(p_i \vee q_i))$$

is provable in K with $O(k)$ distributivity axioms. Hence from (1) we can prove

$$(3) \qquad \bigwedge_{i=1,\dots k}(\Box p_i \vee \Box q_i) \to (\Box\beta_1 \vee \Box\beta_2).$$

using $O(k)$ modal rules. Applying the proposition, we obtain that if $(\star)$ is provable in IL with n proof-lines then (3) is provable in K with $O(n+k)$ modal rules. This allows us to reduce the hard IL tautology to the hard K tautology, given in Example 2, in Section 3.2.

4.2 Hard IL tautologies

4.2.1 Interpolation style tautologies

Proposition 25 *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*

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

   is IL-tautology.

2. *If the tautology has a Hilbert style IL proof with n proof lines 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 $\bigwedge_{i=1,\dots k}(p_i \vee q_i)$ 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 $M \cup N = \{1, \dots k\}$. Hence it is sufficient to show that for such M and N

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

is an intuitionistic tautology. By Lemma 8 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

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

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

Part 2) follows from Theorem 24 in a similar way to the proof of Proposition 9. QED

As in Section 3.2 we now apply the proposition to the formulas *Clique* and *Color*.

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

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

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 10. Note that we omit the double negation infront of $\neg$*Clique* resp. $\neg$*Color*, since $\neg A$ and $\neg\neg\neg A$ are intuitionistically equivalent. QED

4.2.2 Tautologies based on the gap between monotone and general circuits

We are now going to present a different kind of a hard IL tautology. The basis is still the possibility of extracting a monotone circuit from an intuitionistic proof, but the construction no longer deserves the title "monotone interpolation". Assume that we have a classical formula $\alpha(\overline{p})$ which defines a monotone Boolean function f, where α itself is allowed to be non-monotone (i.e., may contain negations). In classical propositional logic we can find a tautology asserting that α does indeed define a monotone function. The most transparent formulation is the tautology

$$(\star) \qquad \bigwedge_{i=1,\dots n} (p_i \to q_i) \to (\alpha(\overline{p}) \to \alpha(\overline{q})).$$

One might conjecture that a proof of $(\star)$ must have size at least $C_m(f)$, the size of a smallest monotone circuit C computing f. This seems likely because the first-hand strategy for proving $(\star)$ is by constructing a monotone circuit computing f. Furthermore, if $NP \neq coNP$ then some tautologies of the form

($\star$) are hard also in F, for the problem of deciding whether a circuit (or even a formula) defines a monotone function is *coNP*-complete.[13] Hence in order to obtain a hard tautology of the form ($\star$) it would be sufficient to find a formula α s.t. i) α defines a monotone Boolean function f, ii) α has a polynomial size, and iii) $C_m(f)$ is exponential. It should not deter us that an example of such a formula is not known, for there are examples of *circuits* with such properties, and it is only a technical detail to rephrase ($\star$) for a circuit. Whether this strategy can give hard tautologies for classical Frege systems will be discussed in Section 4.3.2. On the other hand, the approach is successful in intuitionistic logic. It is sufficient to formulate ($\star$) with disjunctions rather than implications and we obtain tautologies with exponential lower bounds on the number of proof lines in IL.

The major difference between this approach and that of monotone interpolation is the following: if we want to obtain a lower bound on proofs by means of monotone interpolation, we need more than just the fact that a monotone function f cannot be computed by a small monotone circuit. We must employ the full statement of Razborov's theorem that for given monotone functions g, h s.t. $g \leq h$ (i.e., $g(x) \leq h(x)$ on every input) there is no small monotone circuit defining a function f s.t. $g \leq f \leq h$.[14] In the setting of this section, it is sufficient to assume that f is not computable by a small monotone circuit. The additional, also non-trivial, fact required is that f is computable by a small general circuit.

Proposition 26 *Assume that $\alpha(\overline{p})$ is a propositional formula which defines a monotone Boolean function $f(\overline{p})$. Let $\overline{p} = p_1, \dots p_k$ and $\overline{q} = q_1, \dots q_k$. Then the formula*

$$\bigwedge_{i=1,\dots k} (p_i \vee q_i) \rightarrow (\neg\neg\alpha(\overline{p}) \vee \neg\alpha(\neg\overline{q}))$$

is an IL-tautology. Moreover, if the tautology has a Hilbert style IL proof with n proof-lines then there exists a monotone circuit of size $O(n^2+k)$ which computes f.

`Proof.` We shall apply Proposition 25. Let us check the assumptions of the Theorem for $\beta_1 := \alpha(\overline{p})$ and $\beta_2 := \neg\alpha(\overline{p}/\neg\overline{q})$. Since α defines a monotone function then β_1 is monotone in $\overline{p}$. (Recall that β_1 is monotone in $\overline{p}$ if it can be transformed, classically, to a DNF form with no negations attached to $\overline{p}$.) Since

$$(\star) \qquad \beta_2(\overline{q}/\neg\overline{p}) = \neg\alpha(\neg\neg\overline{p})$$

then $\beta_1(\overline{p}) \vee \beta_2(\overline{q}/\neg\overline{p}))$ is classically equivalent to $\alpha(\overline{p}) \vee \neg\alpha(\overline{p})$ which is a classical tautology. Hence $\Gamma := \bigwedge_{i=1,\dots k}(p_i \vee q_i) \rightarrow (\neg\neg\beta_1 \vee \neg\neg\beta_2)$ is IL-tautology and

[13] To see that the problem is in *coNP* is easy. For *coNP*-completeness note that the formula $\neg p \wedge A(\overline{q})$ is monotone iff $A(\overline{q})$ is a contradiction.

[14] On the other hand, note that if $f \in NP \cap coNP$, as is the case of the perfect matching function, then a bound on $C_m(f)$ is indeed sufficient.

if Γ has a proof in IL with n proof-lines then then there exists a monotone circuit C of size $O(n^2+k)$ which interpolates $\neg\beta_2(\overline{q}/\neg\overline{p})$ and $\beta_1(\overline{p})$. But since $\beta_1(\overline{p}) = \alpha(\overline{p})$ and from $(\star)$ $\neg\beta_2(\overline{q}/\neg\overline{p})$ is equivalent to $\alpha(\overline{p})$ then C interpolates $\alpha(\overline{p})$ and $\alpha(\overline{p})$, and hence it computes f. In the statement of the proposition we write $\neg\alpha(\neg\overline{q})$ instead of $\neg\neg\neg\alpha(\neg\overline{q})$. QED

As remarked above, Proposition 26 does not yet give a lower bound for IL for we do not have an example of a function f definable by a small Boolean formula but not by a small monotone circuit. In order to avoid this obstacle, we will now code circuits with formulas. Let C be a circuit in variables $\overline{p}$ s.t. the $\wedge$- and $\vee$-gates have fan-in two. We shall define a formula $[C(\overline{p})]^{15}$ which asserts that C outputs 1 on variables $\overline{p}$. For any gate a of C let us have a variable r_a. If a is a leaf (i.e., a variable in $\overline{p}$) we let $r_a := a$. Otherwise we assume that the variables $r_a, a \in C$ and $\overline{p}$ are mutually different. *The condition for a* will be the formula M_a s.t.

1. if $a = \neg b$ then $M_a :=\ (r_a \equiv \neg r_b)$,
2. if $a = b \wedge c$ then $M_a :=\ (r_a \equiv (r_b \wedge r_c))$ and
3. if $a = b \vee c$ then $M_a :=\ (r_a \equiv (r_b \vee r_c))$

Let c be the output gate of C. Then $[C(\overline{p})]$ will be the formula

$$\bigwedge_{a\in C} M_a \to r_c,$$

where the conjunction ranges over the gates in C. When we write e.g. $[\neg C(\neg\overline{q})]$ as below, we mean the result of application of a similar procedure to the circuit $\neg C(\neg\overline{q})$ (the gates being coded by different variables then those of $C(\overline{p})$.)

Proposition 27 *Assume that $C(\overline{p})$ is a circuit which defines a monotone Boolean function $f(\overline{p})$. Let $\overline{p} = p_1, \dots p_k$ and $\overline{q} = q_1, \dots q_k$. Then the formula*

$$\Gamma := \bigwedge_{i=1,\dots k} (p_i \vee q_i) \to (\neg\neg[C(\overline{p})] \vee \neg\neg[\neg C(\neg\overline{q})])$$

is an IL tautology. Moreover, if the tautology has an IL proof with n distributivity axioms then there exists a monotone circuit of size $O((n^2+k)$ which computes f.

Proof. To show that the formula is IL tautology follows by an analogous argument as in Proposition 25. Let us assume that Γ has an IL-proof S with n proof-lines. Let $\alpha(\overline{p})$ be a formula defining f. For a gate a of C, let $\gamma_a(\overline{p})$ be a formula equivalent to the circuit C_a. Similarly for a formula $\delta_a(\overline{q})$ and a gate a of the circuit $D(\overline{q}) := \neg C(\neg\overline{q})$. If c resp. d are the output gates of C resp. D,

[15] The $[C]$ here is different from $[C]$ in Theorem 24

we can assume that $\gamma_c = \alpha(\overline{p})$ and $\delta_d = \neg\alpha(\neg\overline{q})$. Substituting throughout S γ_a for r_a, $a \in C$, and δ_a for r_a, $a \in D$, we obtain an IL-proof of

$$\Delta := \Gamma(r_a/\gamma_a)_{a\in C}(r_a/\delta_a)_{a\in D}$$

with n proof-lines. Let

$$\lambda_1(\overline{p}) := \bigwedge_{a\in C} M_a(r_a/\gamma_a)_{a\in C}$$

and

$$\lambda_2(\overline{q}) := \bigwedge_{a\in D} M_a(r_a/\delta_a)_{a\in D}.$$

Then Δ is equal to

$$\bigwedge_{i=1,\ldots k}(p_i \vee q_i) \to (\neg\neg(\lambda_1(\overline{p}) \to \alpha(\overline{p}))) \vee (\neg\neg(\lambda_2((\overline{q})) \to \neg\alpha(\neg\overline{q}))).$$

Clearly, λ_1 and λ_2 are classical tautologies and hence the formulas

$$\beta_1(\overline{p}) := \lambda_1(\overline{p}) \to \alpha(\overline{p})$$

and

$$\beta_2(\overline{q}) := \lambda_2(\overline{q}) \to \neg\alpha(\overline{q})$$

satisfy the assumptions of Proposition 24 (compare with Proposition 26). Hence there is a monotone circuit $E(\overline{p})$ of size $O((n^2 + k)$ which interpolates $\neg\beta_2(\neg\overline{p})$ and $\beta_1(\overline{p})$. Since λ_1 and λ_2 are classical tautologies then both $\beta_1(\overline{p})$ and $\neg\beta_2(\neg\overline{p})$ are equivalent to $\alpha(\overline{p})$ and hence E computes f. QED

Corollary *There exists a sequence $\gamma_n, n \in \omega$ of IL tautologies of size n s.t. every IL-proof of γ_n has at least $2^{\Omega(n^{\frac{1}{4}})}$ proof-lines.*

Proof. By [24] and [17] there exists a monotone function f computable by a polynomial circuit C s.t. every monotone circuit computing f has at least the size $2^{\Omega(n^{\frac{1}{4}})}$. Apply the Proposition to the circuit C. QED

4.3 Classical logic

In this section we state what is now obvious, that there is an exponential speed-up between classical and intuitionistic systems of propositional logic. This follows from the fact that the tautology of Corollary of Proposition 25 has a polynomial-size classical proof. We also prove something less obvious, that tautologies of the form of Proposition 27 have polynomial-size classical proofs, if C is taken as a particular circuit computing the perfect matching function.

4.3.1 Speed-up between classical and intuitionistic propositional calculi

We will define the system of classical propositional logic, the Frege system F, as the system IL, in the Hilbert style axiomatisation, plus the axiom

$$\neg\neg A \to A.$$

Theorem 28 *Let Θ_n^k be the IL tautology of Corollary of Proposition 25. If $k := \sqrt{n}$ then every IL-proof of the tautology Θ_n^k contains an exponential number of proof-lines but Θ_n^k has a polynomial size classical proof.*

`Proof.` In order to show that Θ_n^k has a polynomial size classical proof it is sufficient to prove that

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

has a polynomial-size Frege proof. But that follows from [5]. `QED`

Remark. Now that we have an exponential lower bound for intuitionistic calculus, a speed up between classical and intuitionistic logic could be trivially obtained as follows: let $\Theta_i, i \in \omega$ be any sequence of IL-tautologies s.t. Θ_i have only exponential proofs in IL. Let us consider the sequence

$$\Gamma_i := (\neg\neg p \to p) \vee \Theta_i.$$

Then Γ_i have linear size classical proofs. Moreover, by [6], if $IL \vdash A \vee B$ then $IL \vdash A$ or $IL \vdash B$, and the proof of A resp. B has a polynomial size with respect to the size of the proof of $A \vee B$. Since $IL \not\vdash \neg\neg p \to p$ then Γ_i have only exponential size proofs in IL. In this way one can obtain speed up between IL and any stronger proof system. However, such a speed-up is not very informative. Let us now show that a more natural speed-up occurs also between IL and Gödel-Dummet's logic.

Fuzzy logic. Gödel-Dummett's logic is the system IL plus the axiom

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

It is one of the basic systems of fuzzy logic. We can find polynomial size proofs of tautologies of Corollary of Theorem 25. The tautology in the corollary has the form

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

and

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

has a polynomial classical proof. In Gödel-Dummett logic

$$(\neg\neg(A \vee B)) \to (\neg\neg A \vee \neg\neg B)$$

is a tautology. Hence it is sufficient to prove

$$\bigwedge_{i=1,\dots n} (p_i \vee q_i) \to \neg\neg(\beta_1(\overline{p}, \overline{s}) \vee \beta_2(\overline{q}, \overline{r})).$$

The tautology has a polynomial size proof since the double negation enables to reproduce the classical proof even in IL.

4.3.2 Short Frege proofs of tautologies based on the gap between monotone and general circuits

One might conjecture that we could employ classical analogies of the tautologies in Proposition 27, i.e., tautologies of the form[16]

$$(\star) \qquad \bigwedge_{i=1,\dots n} (p_i \to q_i) \to (C(\overline{p}) \to C(\overline{q}))$$

for a circuit C computing a monotone Boolean function f, to find lower bounds for classical propositional systems. However, we will show that the tautology asserting monotonicity of a particular circuit defining the perfect matching function has a polynomial size Frege proof. Since we have a quasipolynomial lower bound for monotone circuits computing the perfect matching function, we conclude that there is no polynomial function relating the size of Frege proof of $(\star)$ and $C_m(f)$. In order to completely frustrate the possibility of finding lower bounds for F by means of $(\star)$, we would like to find polynomial size Frege proofs for a circuit defining a monotone function f s.t. the gap $C_m(f)/C(f)$ is exponential. Unfortunately, we know only one example of such a function (namely the one obtained from [24]), and the complexity of the algorithm does not invite formalisation.

The perfect matching problem. Let $G \subseteq U \times V$ be a bipartite graph on $U = u_1, \dots u_n$, $V = v_1, \dots v_n$. *A matching* M is a set of vertex disjoint edges of G. M is *a perfect matching*, if $|M| = n$. G will be represented by propositional variables p_{ij}, $i, j = 1, \dots n$ s.t. there is an edge in G connecting u_i and v_j iff $p_{ij} = 1$. *The perfect matching function* f_{PM} is the function in variables $\overline{p} = p_{ij}, i, j = 1, \dots n$, s.t. $f_{PM}(\overline{p}) = 1$ iff the graph represented by $\overline{p}$ has a perfect matching. f_{PM} is a monotone function. By the result of Razborov [23] every monotone circuit computing f_{PM} must have a superpolynomial size. On the other hand, there is a polynomial time algorithm deciding whether a bipartite graph G has a perfect matching, and hence there are polynomial size circuits computing f_{PM}.

Recall the coding of circuits from Section 4.2.2. For circuits $C_1, \dots C_n$ and a formula A

$$A(C_1, \dots C_n)$$

[16] In F we would understand $(\star)$ as containing the conditions M_a for gates of $C(\overline{p})$ and $C(\overline{q})$ in the assumption.

will be an abbreviation for

$$\bigwedge_{a\in C_i, i=1,\dots n} M_a \to A(r_1,\dots r_n),$$

where $r_1,\dots r_n$ are variables representing the outputs of $C_1,\dots C_n$. Hence the gate definitions are always placed in the assumption of the whole proposition. For a list of variables $\overline{q}$, $C_{\overline{q}}$ will denote the list of circuits indexed by the formulas $\overline{q}$. Let $A = A(\overline{p},\overline{q})$ be a formula. We will say that circuits $C_{\overline{q}}$ in variables $\overline{p}$

1. *solve the problem A*, if

   $$(\star) \qquad A(\overline{p},\overline{q}) \to A(\overline{p}, C_{\overline{q}})$$

   is a tautology, and

2. *solve the problem A polynomially in F*, if the circuits have polynomial size and $(\star)$ has a polynomial size Frege proof.

Moreover, the function $f_A(\overline{p})$ will be the Boolean function s.t. for any assignment to the variables $\overline{p}$, $f_A(\overline{p}) = 1$ iff there exists an assignment to $\overline{q}$ s.t. $A(\overline{p},\overline{q})$ is true.

As opposed to the previous notation, we shall say that $A(\overline{p},\overline{q})$ is *monotone in $\overline{p}$* if A contains only the binary connectives $\wedge$, $\vee$, and negations do not occur in front of variables $\overline{p}$.

Lemma 29 *Let $A = A(\overline{p},\overline{q})$ be a formula, $\overline{r} = r_1,\dots r_k$, $\overline{p} = p_1,\dots p_k$. Assume that circuits $C_{\overline{q}}$ in variables $\overline{p}$ solve the problem A. Then*

(1) the circuit $C(\overline{p}) := A(\overline{p}, C_{\overline{q}}(\overline{p}))$ computes the function $f_A(\overline{p})$.

(2) Assume in addition that $C_{\overline{q}}$ solve the problem A polynomially in F and that A is monotone in $\overline{p}$. Then the tautology

$$(\star) \qquad \bigwedge_{i=1,\dots n} (p_i \to r_i) \to (C(\overline{p}) \to C(\overline{r}))$$

has a polynomial size Frege proof in F.

`Proof.` (1) is clear.

(2) We must show that

$$(\star) \qquad \bigwedge_{i=1,\dots n} (p_i \to r_i) \to (A(\overline{p}, C_{\overline{q}}(\overline{p})) \to A(\overline{r}, C_{\overline{q}}(\overline{r}))$$

has a polynomial size Frege proof . Since $A(\overline{p},\overline{q})$ is monotone in $\overline{p}$, we obtain a linear Frege proof of

$$(i) \qquad \bigwedge_{i=1,\dots n} (p_i \to r_i) \to (A(\overline{p}, C_{\overline{q}}(\overline{p})) \to A(\overline{r}, C_{\overline{q}}(\overline{p})).$$

Since the circuits $C_{\overline{q}}$ solve the problem A polynomially in F, we have a polynomial Frege proof of

$$(ii) \qquad A(\overline{r}, C_{\overline{q}}(\overline{p})) \to A(\overline{r}, C_{\overline{q}}(\overline{r})),$$

which together with (i) gives a polynomial size Frege proof of $(\star)$. (Note that $(\star)$ contains all the circuit gate conditions in its assumption.) QED

Let $\overline{p} = p_{ij},\ i,j = 1,\dots n$ and $\overline{q} = q_{ij},\ i,j = 1,\dots n$. Then the formula

$$\mathrm{MATCH}(\overline{p}, \overline{q})$$

is the formula asserting that $\overline{q}$ is a matching on the graph represented by $\overline{p}$, i.e., the formula

$$\bigwedge_{i,j}(\neg q_{ij} \vee p_{ij}) \wedge \bigwedge_{i,j_1 \neq j_2}(\neg q_{ij_1} \vee \neg q_{ij_2}) \wedge \bigwedge_{i_1 \neq i_2, j}(\neg q_{i_1 j} \vee \neg q_{i_2 j}),$$

where the indices range over $1,\dots n$. The formula

$$\mathrm{PMATCH}(\overline{p}, \overline{q}) := \bigwedge_i \bigvee_j q_{ij} \wedge MATCH(\overline{p}, \overline{q})$$

is the formula asserting that $\overline{q}$ is a perfect matching. In the Appendix, we will sketch the construction of circuits $C_{\overline{q}}$ which polynomially solve the problem PMATCH in F. This will give the following theorem:

Theorem 30 *There is a circuit C which computes the perfect matching function s.t. the tautology*

$$\bigwedge_{i,j=1,\dots n} (p_{ij} \to q_{ij}) \to (C(\overline{p}) \to C(\overline{q}))$$

has a polynomial size Frege proof. Hence (to match the formulation of Proposition 27) also the tautology

$$\bigwedge_{i,j=1,\dots n} (p_{ij} \vee q_{ij}) \to ([C(\overline{p})] \vee [\neg C(\neg \overline{q})])$$

has a polynomial size Frege proof.

Proof. Follows from the previous lemma and the fact that there exist circuits $C_{\overline{q}}$ which solve the problem PMATCH$(\overline{p}, \overline{q})$ polynomially in F, as will be shown in the Appendix. QED

Appendix

The algorithm

Let us first outline the algorithm for finding a perfect matching in a graph. For a matching M and a vertex v, we will say that v *is matched* if $v \in Vert(M)$. Similarly, an edge e is matched if $e \in M$. A path P in G will be called *alternating* if it alternates between matched and unmatched edges and the first vertex is unmatched. An alternating path will be called *augmenting* if it ends by an unmatched vertex, too.

The algorithm constructs a sequence of matchings $M_0, \dots M_n$, M_i having size i. Let $M_0 := \emptyset$. At the stage $i+1$, find an augmenting path P for M_i and let $M_{i+1} := (M_i \setminus P) \cup (P \setminus M_i)$.

An augmenting path for a matching M in G can be found as follows. Let $u \in U$ be an unmatched vertex in G and define a sequence of sets of vertices $U_0^u, U_1^u, \dots U_n^u \subseteq U$, $V_1^u, \dots V_n^u \subseteq V$.

$$\begin{aligned} U_0^u &:= \{u\} \\ V_{i+1}^u &:= \{a \in Vert(G), \exists b \in U_i^u \ \langle a, b\rangle \in G \setminus M\}, \qquad i = 0, \dots n-1 \\ U_{i+1}^u &:= \{a \in Vert(G), \exists b \in V_i^u \ \langle a, b\rangle \in M\}, \qquad i = 1, \dots n-1. \end{aligned}$$

Clearly, for every $a \in V_k^u$ resp. $a \in U_k^u$ there exists an alternating path of length $2k-1$ resp. $2k$ from u to a. Hence if we find a and $k = 1, \dots n$ s.t. $a \in V_k^u$ and a is unmatched, then there is an augmenting path from u to a. Moreover, we can easily construct the path: we can find $a' \in U_{k-1}^u$ s.t. $\langle a', a\rangle \in G$ is unmatched. Again there is an alternating path of length $2k-2$ from u to a', and we can find some $a'' \in V_{k-2}^u$ s.t. $\langle a'', u\rangle \in G$ is matched etc. until we reach u.

A set $X \subseteq U$ will be called *critical in* G, if $|X| > |G(X)|$, where $G(X) \subseteq V$ is the image of X over the graph G. The correctness of the algorithm can be proved using

Hall's theorem:
G has a perfect matching iff G does not have a critical set.

It can be easily shown that the sets U_i^u, V_i^u constructed above either define an augmenting path, or

$$X := \bigcup_{i=0,\dots n} U_i^u$$

is a critical set. For if $Y := \bigcup_{i=0,\dots n} V_i^u$ then i) $Y = G(X)$, from the definition, and ii) $|Y| = |(X \setminus \{u\})| = |X| - 1$, since every vertex of Y is matched to some vertex in $X \setminus \{u\}$.

Therefore if G has a perfect matching then there is no critical set, and the algorithm extends the matching M_i to M_{i+1}, $i < n$.

The formalisation

There exist polynomial formulas $Count_n^k(p_1, \dots p_n)$ asserting that exactly k of the variables $\overline{p} = p_1, \dots p_n$ are true s.t. their expected properties have polysize

Frege proofs in F (see [5]). This enables the formalisation of basic counting arguments in F.

The formula $\mathrm{MATCH}^k(\overline{p},\overline{q})$ will be an abbreviation for

$$MATCH(\overline{p},\overline{q}) \wedge Count^k_n(\bigvee_{j=1,\dots n} q_{ij},\ i=1,\dots n).$$

For a vertex a, the formula $\mathrm{MATCHED}_a(\overline{q})$ will be an abbreviation for $\bigvee_{j=1,\dots n} q_{ij}$, if $a=u_i \in U$, and $\bigvee_{j=1,\dots n} q_{ji}$, if $a=v_i\in V$.

A path of odd length $2k-1$ in a bipartite graph on U and V which starts in some $a_1 \in U$ can be represented by a sequence $a_1,\dots a_k \in U$ and $b_1,\dots b_k \in V$ s.t. the path contains edges $\langle a_l, b_l\rangle$ and $\langle b_l, a_{l+1}\rangle$. Let $\overline{f}=f_{ij},\ i,j=1,\dots n$ and $\overline{g}=g_{ij},\ i,j=1,\dots n$ be fresh variables. Let $a=u_i,\ b=v_j$ be vertices. Then the formula

$$\mathrm{PATH}^{2k-1}_{ab}(\overline{p},\overline{f},\overline{g})$$

will be the formula asserting that $\overline{f}$ and $\overline{g}$ represent a path from a to b of length $2k-1$, i.e., the assertion that i) $\overline{f}$ and $\overline{g}$ are onto one-to-one partial functions from $1,\dots n$ to $1,\dots k$, and $f_{1i}=1$, $g_{kj}=1$, and ii) for every $i',j'=1,\dots n$, and $l=1,\dots k-1$, if $f_{i'l}=1$ and $g_{j'l}=1$, or $g_{j'l}=1$ and $f_{i'l+1}=1$, then $p_{i'j'}=1$.

In a similar fashion, we can introduce the formulas $\mathrm{PATH}^k_{ab}(\overline{p},\overline{f},\overline{g})$ for k even, and hence in general

$$\mathrm{PATH}^k_{ab}(\overline{p},\overline{f},\overline{g})$$

is a formula asserting that $\overline{f}$ and $\overline{g}$ represent an odd path from a to b of length k. Similarly, we introduce the formula

$$\mathrm{ALTPATH}^k_{ab}(\overline{p},\overline{q},\overline{f},\overline{g}),$$

asserting that $\overline{f}$ and $\overline{g}$ represent an alternating path of odd length from a to b w.r. to the matching $\overline{q}$. By means of $\mathrm{MATCHED}_a(\overline{q})$ we can introduce

$$\mathrm{AUGPATH}^k_{ab}(\overline{p},\overline{q},\overline{f},\overline{g}),$$

a formula asserting that $\overline{f}$ and $\overline{g}$ represent an augmenting path from a to b w.r. to the matching $\overline{q}$. Finally,

$$\mathrm{AUGPATH}(\overline{p},\overline{q},\overline{f},\overline{g})$$

is the disjunction of all $\mathrm{AUGPATH}^k_{ab}(\overline{p},\overline{q},\overline{f},\overline{g})$.

For a list of formulas $\overline{A}=A_{ij}, i,j=1,\dots n$ $\mathrm{Dom}(\overline{A})$, will be the list of n formulas $\bigwedge_i A_{i1},\dots \bigwedge_i A_{in}$.

$$\mathrm{CRIT}(\overline{p},\overline{r}),$$

will be the formula asserting that the set $X := \{u_i \in U; r_i=1\}$ is a critical set in the graph represented by $\overline{p}$. More exactly, if $\overline{r}=r_1,\dots r_n$, it is a disjunction of conjunctions of the form $\mathrm{Count}^k_n(r_1,\dots r_n)\wedge \mathrm{Count}^j_n(\mathrm{Dom}(r_i \wedge p_{ij}))$, for $j<k$.

Lemma 1 shows that the easy direction of Hall's theorem has a short F-proof:

Lemma 1 *The formula*

$$PMATCH(\overline{p}, \overline{q}) \to \neg CRIT(\overline{p}, \overline{r})$$

has a polynomial size Frege proof.

`Proof.` Assume PMATCH$(\overline{p}, \overline{q})$ and CRIT$(\overline{p}, \overline{r})$. Then we obtain a negation of pigeonhole principle which has a short Frege refutation. `QED`

Lemma 2 *There are polynomial circuits $C_{\overline{f}}$ and $D_{\overline{g}}$ in variables $\overline{p}, \overline{q}$ s.t. the following has polynomial size Frege proof:*

$$MATCH(\overline{p}, \overline{q}) \to (AUGPATH(\overline{p}, \overline{q}, C_{\overline{f}}, D_{\overline{g}}) \vee CRIT(\overline{p}, Dom(C_{\overline{f}}))).$$

`Proof.` Recall the sets $U_0^a, \dots U_n^a$ and $V_0^u, \dots V_n^a$. For $a \in U$, we can find polynomial size circuits E_{au}^s, $s = 0, \dots n$, $u \in U$, and F_{av}^s, $s = 1, \dots n$, $v \in U$, s.t. $E_{au}^s = 1$ iff $u \in U_s^a$ and $E_{av}^s = 1$ iff $v \in V_s^a$, and moreover, the analogons of the defining relations between U_i^a and V_i^a have polynomial Frege proofs. The proof is then a straightforward formalisation of the above informal argument. `QED`

Lemma 3 *There exist circuits $C_{\overline{q}}$ in variables $\overline{p}, \overline{q}, \overline{f}, \overline{g}$ s.t. the following has polynomial size Frege proof:*

$$MATCH^k(\overline{p}, \overline{q}) \to (MATCH^{k+1}(\overline{p}, C_{\overline{q}}) \vee CRIT(\overline{p}, Dom(C_{\overline{q}}))).$$

`Proof.` The following is a simple counting argument in F: if M is a matching of size k and P is an augmenting path then $(P \setminus M) \cup (M \setminus P)$ is a matching of size $k+1$. The statement of the Lemma then follows from the previous one. `QED`

Let us recall the matchings $M_0, \dots M_n$ from our description of the algorithm. Using the circuits from Lemma 2 and Lemma 3, we can find polynomial circuits $C_{\overline{q}}^k(\overline{p})$ s.t. there are short Frege proofs of

$$\mathrm{MATCH}^k(\overline{p}, C_{\overline{q}}^k) \vee \mathrm{CRIT}(\overline{p}, \mathrm{Dom}(C_{\overline{q}}^k))),$$

i.e., they either define a matching of size k, or a critical set. Since MATCH$^n(\overline{p}, \overline{q})$ is equivalent to PMATCH$(\overline{p}, \overline{q})$, we also have circuits $C_{\overline{q}}$ and polynomial Frege proofs for

$$\mathrm{PMATCH}(\overline{p}, C_{\overline{q}}) \vee \mathrm{CRIT}(\overline{p}, \mathrm{Dom}(C_{\overline{q}}))).$$

Finally, from Lemma 1 it follows that

$$\mathrm{PMATCH}(\overline{p}, \overline{q}) \to \mathrm{PMATCH}(\overline{p}, C_{\overline{q}})$$

has a polynomial size Frege proof, and hence the circuits $C_{\overline{q}}$ solve the problem PMATCH$(\overline{p}, \overline{q})$ polynomially in F.

References

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

[2] Baaz, M., Pudlák, P. (1993) Kreisel's conjecture for $L\exists_1$, *Arithmetic, Proof Theory, and Computation Complexity*, Papers from the Conference Held in Prague, July 2-5, 1991, New York: Oxford University Press, 30-60

[3] Baaz, M., Zach, R. (1994) Short proofs of tautologies using the schema of equivalence, *Selected papers from CSL'93 workshop*, Berlin: Springer, 33-35.

[4] Bílková, M. (2003) Feasible disjunction and interpolation properties in modal logic $S4$, LC 2002 Muenster, abstract in *The Bulletin of Symbolic Logic*, **9(1)**.

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

[6] Buss, S. R., Mints, G. (1999) The complexity of the disjunction and existence properties in intuitionistic logic, *Annals of Pure and Applied Logic*, **99**: 93 - 104.

[7] Buss, S. R., Pudlák, P. (2001) On the computational content of intuitionistic propositional proofs, *Annals of Pure and Applied Logic*, **109**: 46 - 94.

[8] Friedman, H. (1975) One hundred and two problems in mathematical logic, *The Journal of Symbolic Logic*, **40**: 113-129.

[9] Hrubeš, P. (2007) Theories very close to PA where Kreisel's conjecture is false, *Journal of Symbolic Logic*, **72**: 123-137.

[10] Hrubeš, P. (2007) Lower bounds for modal logics, *Journal of Symbolic Logic*, **72, 3**: 941-958.

[11] Hrubeš, P. (2007) A lower bound for intuitionistic logic, *Annals of Pure and Applied Logic*, **146**: 72 - 90.

[12] Jeřábek, E. (200?) Substitution Frege and extended Frege proof system in non-classical logics, preprint.

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

[14] Krajíček, J., Pudlák, P. (1988) The number of proof lines and the size of proofs in first order logic, *Arch. Math. Logic*, **27**: 69-84.

[15] Krajíček, J. (1995) Bounded arithmetic, propositional logic, and complexity theory, Cambridge University Press, USA.

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

[17] Grötschler, M., Lovász, L., Schrijver, A., The ellipsoid method and its consequences in combinatorial optimisation, *Combinatorica*, **1(2)**: 169 - 197.

[18] Mints, G., Kojevnikov, A. (2004) Intuitionistic Frege systems are polynomially equivalent, *Zapisky Nauchnych Seminarov POMI*, **316**: 129 - 146.

[19] Miyatake, T. (1980) On the lengths of proofs in formal systems, *Tsukuba Journal of Mathematics*, **4**: 115-125.

[20] Nishimura, I. (1960) On formulas of one variable in intuitionistic propositional calculus, *Journal of Symbolic Logic*, **25(4)**: 327 - 331.

[21] Parikh, R. (1973) Some results on the length of proofs, *TAMS* **177**: 29-36.

[22] Pudlák, P. (1999) On the complexity of propositional calculus, Sets and proofs, *Logic Colloquium'97*, Cambridge University Press, 197 - 218.

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

[24] Tardos, É. (1987), The gap between monotone and non-monotone circuit complexity is exponential, *Combinatorica*, **7(4)**: 141 - 142.

[25] Wegener, I. (1987) The Complexity of Boolean Functions, John Willey et Sons Ltd, and B. G. Teubner, Stuttgart.

[26] Yukami, T. (1978) A note on a formalised arithmetic with function symbols and +, *Tsukuba Journal of Mathematics*, **7**: 69-73.

[27] Yukami, T. (1984) Some results on speed-up, *Ann. Jap. Assoc. Philos. Sci.*, **6**: 195-205.

1.

2.

3.

4.

5.

6.