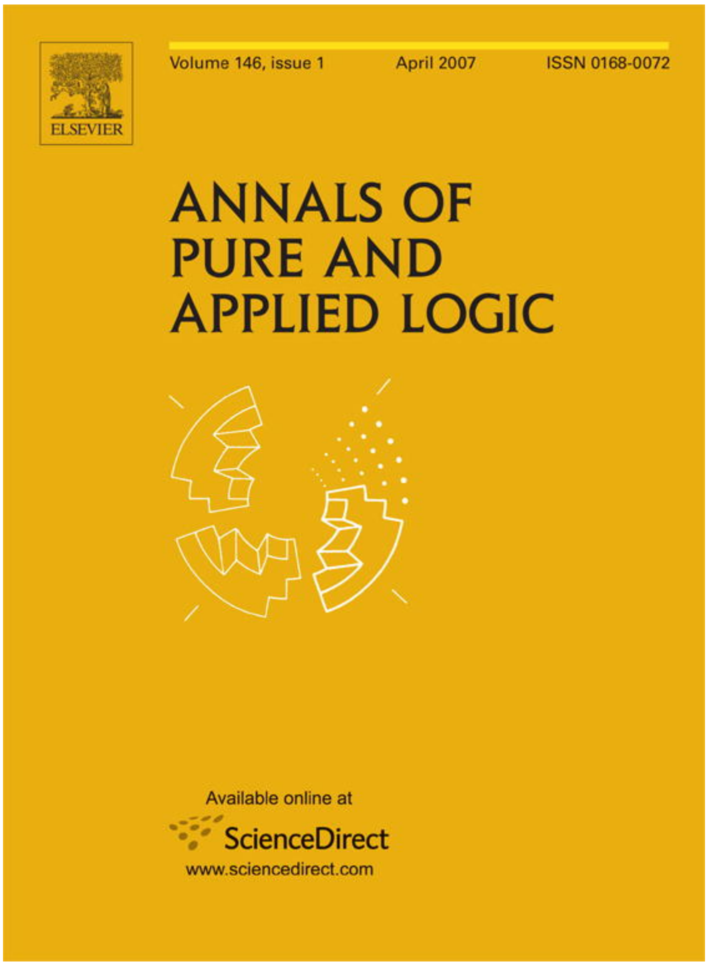
Volume 146, issue 1
April 2007
ISSN 0168-0072
ELSEVIER
ANNALS OF PURE AND APPLIED LOGIC
Available online at
ScienceDirect
www.sciencedirect.com

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Annals of Pure and Applied Logic 146 (2007) 72–90
ANNALS OF PURE AND APPLIED LOGIC
www.elsevier.com/locate/apal

A lower bound for intuitionistic logic

Pavel Hrubeš

Mathematical Institute, Czech Academy of Sciences, Prague, Czech Republic

Received 23 October 2006; received in revised form 2 January 2007; accepted 11 January 2007
Available online 25 January 2007
Communicated by U. Kohlenbach

Abstract

We give an exponential lower bound on the number of proof-lines in intuitionistic propositional logic, IL, axiomatised in the usual Frege-style fashion; i.e., we give an example of IL-tautologies $A_1, A_2, \ldots$ s.t. every IL-proof of A_i must have a number of proof-lines exponential in terms of the size of A_i. We show that the results do not apply to the system of classical logic and we obtain an exponential speed-up between classical and intuitionistic logic.

Keywords: Proof complexity; Intuitionistic logic; Modal logic

1. Introduction

One of the basic problems of proof complexity is to find lower bounds on sizes of proofs in various proof systems. The general form of the problem is the following:

For a proof system S and a function $g : \omega \rightarrow \omega$ find a sequence of S-tautologies (determine whether it exists) A_i, $i \in \omega$, s.t. every S-proof of A_i must have size at least $g(|A_i|)$.[1]

For weak proof systems, such as those formalising propositional logic, the problem is interesting when g is an exponential or a superpolynomial function. Recently, an exponential lower bound on the number of proof-lines was reached in [6] for the system K of modal logic. In this paper, we extend the result to the system of intuitionistic propositional logic, IL. We will present examples of IL-tautologies A s.t. every IL-proof of A must contain an exponential number of proof-lines. Exact axiomatisation of IL will be given in Section 3. The axiomatisation is a particular kind of a *Frege system* for intuitionistic propositional logic. In [8] it has been shown that all such systems are polynomially equivalent, and hence our proof is not sensitive to the choice of axiomatisation, as far as it remains Frege-style.

The method of proof of this paper is simple. We show that there is a sound translation of IL to K preserving the number of proof-lines.[2] This enables us to reduce the lower bound for IL to that of K. Since the basic tool of [6] was that of *monotone interpolation*, here too we obtain a form of monotone interpolation for IL. For a better exposition

E-mail address: pahrubes@centrum.cz.

[1] $|A_i|$ denotes the size of A_i. The size of a tautology or of a proof is the number of symbols it contains.

[2] For exact formulation see Proposition 3.

0168-0072/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.apal.2007.01.001

of the concept see [6], or for example [7]. However, we shall present two different types of hard IL-tautologies, the first having the traditional interpolation style, the latter being based on the gap between monotone and non-monotone circuits. The latter form is a formalisation of the assertion "$C(\overline{p})$ *defines a monotone function*" for a general circuit C defining a monotone Boolean function (see Section 5).[3] I believed that such a tautology could give a lower bound even for classical propositional systems. In Section 6 it is shown that this is in general not the case.

It has been proved earlier by Pavel Pudlák [9] that intuitionistic propositional calculus has an effective interpolation property. (See also [4].) This was based on the result of Buss and Mints [3] who have shown that intuitionistic disjunction has a constructive behaviour even in the sense of complexity of proofs, i.e., that from an intuitionistic proof of a disjunction $A \vee B$ one can extract a proof of A or B in a polynomial time. These results, though revealing a close connection between the complexity of intuitionistic proofs and Boolean circuits, and illuminating a new aspect of constructivity in intutionistic logic, are not sufficient to give a concrete lower bound on sizes of IL proofs. This is because by means of effective interpolation we reduce the problem of finding a proof size lower bound to that of finding a circuit lower bound, a substantially more difficult problem. In this paper we show that IL has even *monotone* effective interpolation property and hence we can apply the classical results in monotone circuit complexity to IL.

2. A different form of monotone interpolation for K

The proof system K is obtained by adding the symbol $\Box$ to the language of propositional logic. The underlying propositional logic is formalised by means of a Frege system (the axiomatisation of classical logic given in Section 6 is adequate). In addition, K has the *rule of generalisation* and the *distributivity axiom*

$$\frac{A}{\Box A}, \qquad \Box(A \to B) \to (\Box A \to \Box B).$$

We are going to reduce monotone interpolation for IL to the monotone interpolation for K. However, the form of monotone interpolation offered in [6] is not suitable for this purpose, and we will first prove a different kind of monotone interpolation for K. The following theorem can be found in [6]:

Theorem 0. *Let α, β_1 and β_2 be propositional formulas. Assume that α is a monotone formula (i.e., containing only the connectives $\wedge$ and $\vee$) and that it contains only the variables $\overline{p}$, and that β_1 resp. β_2 contain only the variables $\overline{p}, \overline{s_1}$ resp $\overline{p}, \overline{s_2}$. Assume that*

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

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

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

A propositional formula β will be called *monotone in* $\overline{p}$ if the formula, when transformed to a DNF form, does not contain negation in front of any variable in $\overline{p}$. If β is a general 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 1. *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 $\bigwedge_{i=1,\dots n}(p_i \vee q_i) \to \beta_1(\overline{p}, \overline{r_1}) \vee \beta_2(\overline{q}, \overline{r_2})$ is a classical tautology.*
(2) *Let M, N be subsets of $\{1, \dots n\}$ s.t. $M \cup N = \{1, \dots n\}$. Then one of the following is a classical tautology:*

[3] The lower bound was first reached for the tautologies in Section 5. It was Pavel Pudlák who reminded the author that the same argument applies also to the more natural tautologies of Section 4.

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

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

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

is a tautology. Hence also

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

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. $\square$

Let $\alpha = \alpha(\overline{p}, \overline{r})$ and $\beta = \beta(\overline{p}, \overline{s})$ be propositional formulas, $\overline{r}$, $\overline{s}$ disjoint. We will say that a circuit C in variables $\overline{p}$ *interpolates* α *and* β if for every assignment σ of the variables $\overline{p}$

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

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

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

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

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

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

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

From Theorem 0 there exist monotone circuits D_1 and D_2 in variables $\overline{p}$, $\overline{q}$ of size $O(n^2)$ s.t. for any assignment

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

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

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

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

This in particular gives

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

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

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

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

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

Since D_1 and D_2 are monotone, (3) gives

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

and hence

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

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

3. Translation of IL to K

The language of intuitionistic propositional logic, IL, contains the connectives $\to$, $\vee$, $\wedge$ and a fixed variable symbol $\perp$. 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	$\perp \to A$
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	$(B \to A) \to ((C \to A) \to (B \vee C \to A))$.

We give a translation of intuitionistic logic to K s.t. for any intuitionistic tautology A its translation A^t is K-tautology. The translation is not in general faithful, it may happen that A^t is a tautology without A being so.[4] 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 the number of *distributivity axioms* in a K-proof of A^t.

For an intuitionistic formula A of IL, its translation A^t to K will be defined as follows[5]:

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. $(A \wedge B)^t = A^t \wedge B^t$.

Note that A^t is always a formula of K of modal-depth one, i.e., A^t does not contain nested modalities. 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 [6], based on deleting all boxes which are in a scope of another $\Box$. Routinely, but laboriously, we can verify the following:

Proposition 3. (1) *If A is an IL-tautology then A^t is a K-tautology.*
(2) *If A has an IL-proof with n proof-lines then A^t has a K-proof with $O(n)$ axioms of distributivity.*

Proof. We proceed by induction on the number of proof-lines in an IL-proof. Let us first show that the translation of an axiom is K-tautology. It will be apparent that the proofs do not require more than, say, five distributivity axioms. Note that we can use a form of deduction theorem in K, i.e., in order to prove $A \to B$ it is sufficient to prove B from the assumption A provided we do not apply generalisiation to a consequence of A in the proof. For an IL-formula A, $A^\star$ will be an abbreviation for $\Box A \wedge A^t$.

Ax1.

$$(A \to (B \to A))^t = A^\star \to \Box(B \to A) \wedge (B^\star \to A^\star).$$

But $\Box A \to \Box(B \to A)$ and hence $A^\star \to \Box(B \to A)$ is a K-tautology and $A^\star \to (B^\star \to A^\star)$ is a propositional tautology.

Ax2. The translation of A2 is an implication s.t. on its left hand side we have the conjunction of

$$\Box(A \to (B \to C)) \tag{a}$$

and

$$A^\star \to \Box(B \to C) \wedge (B^\star \to C^\star), \tag{b}$$

and on the right hand side we have the conjunction of

$$\Box((A \to B) \to (A \to C)) \tag{c}$$

and

$$(\Box(A \to B) \wedge (A^\star \to B^\star) \to (\Box(A \to C) \wedge (A^\star \to C^\star)). \tag{d}$$

By applying distributivity twice to the tautology

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

we obtain that the following are K-tautologies:

$$\Box(A \to (B \to C)) \to \Box((A \to B) \to (A \to C)), \tag{$\star$}$$

$$\Box(A \to (B \to C)) \to (\Box(A \to B) \to \Box(A \to C)). \tag{$\star\star$}$$

[4] Consider the formula $\neg\neg p \to p$.
[5] Hence the symbol $\bot$ is assumed also in K. If not, $\bot$ can be simulated by any fixed contradiction in K.

Hence (c) follows from (a) by ($\star$). In order to prove (d) from (a) and (b), let us show that $\Box(A \to C)$ and $A^\star \to C^\star$ follow from (a), (b),

$$\Box(A \to B) \tag{e}$$

and

$$A^\star \to B^\star. \tag{f}$$

Again, from (a), (e) and ($\star\star$) we obtain $\Box(A \to C)$. (b) implies, in particular,

$$A^\star \to (B^\star \to C^\star).$$

This, together with (f), gives $A^\star \to C^\star$ by means of propositional logic only.

Ax3, Ax4–5 and Ax7–8 are easy.

The translation of Ax6 is an implication which contains

$$\Box(A \to (B \to C)), \tag{a}$$

$$A^\star \to \Box(B \to C) \wedge (B^\star \to C^\star) \tag{b}$$

on the left hand side and

$$\Box(A \wedge B \to C), \tag{c}$$

$$\Box(A \wedge B) \wedge A^t \wedge B^t \to C^\star \tag{d}$$

on the right hand side. (c) follows from (a) by applying distributivity to the tautology

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

In order to prove (d) from (b), let us show that $C^\star$ follows from (b) and

$$\Box(A \wedge B) \wedge A^t \wedge B^t. \tag{e}$$

Since $\Box(A \wedge B)$ implies $\Box A \wedge \Box B$, (e) implies $\Box A \wedge \Box B \wedge A^t \wedge B^t$ and hence $A^\star \wedge B^\star$. (b) gives, in particular, $A^\star \to (B^\star \to C^\star)$ which together with $A^\star \wedge B^\star$ implies $C^\star$, by means of propositional logic only.

The translation of Ax9 is an implication with

$$\Box(B \to A) \tag{a}$$

$$B^\star \to A^\star \tag{b}$$

on the left hand side, and

$$\Box((C \to A) \to (B \vee C \to A)), \tag{c}$$

$$\Box(C \to A) \wedge (C^\star \to A^\star) \to \Box(B \vee C \to A) \wedge (\Box(B \vee C) \wedge (B^\star \vee C^\star) \to A^\star) \tag{d}$$

on the right hand side. By applying distributivity twice to the tautology

$$\Box((B \to A) \to ((C \to A) \to (B \vee C \to A)))$$

we obtain that the following are tautologies:

$$\Box(B \to A) \to \Box((C \to A) \to (B \vee C \to A)) \tag{$\star$}$$

$$\Box(B \to A) \to (\Box(C \to A) \to \Box(B \vee C \to A)). \tag{$\star\star$}$$

By means of ($\star$), (c) follows from (a). In order to prove (d) from (a) and (b), it is sufficient to prove $\Box(B \vee C \to A)$ from (a) and

$$\Box(C \to A), \tag{e}$$

and to prove $A^\star$ from (b) and

$$C^\star \to A^\star, \tag{f}$$

$$B^\star \vee C^\star. \tag{g}$$

But $\Box(B \vee C \to A)$ follows from (a) and (e) by means of ($\star\star$) and $A^\star$ follows from (b), (f) and (g) by means of propositional logic only.

Let us consider modus ponens. Assume that $IL \vdash A$ and $IL \vdash A \to B$. We must show that $K \vdash B^t$. By the inductive assumption $K \vdash A^t$ and $K \vdash (A \to B)^t = \Box A \wedge A^t \to \Box B \wedge B^t$. Since $IL \vdash A$ then A is a classical tautology and $K \vdash \Box A$ by generalisation. In the proof of $\Box A$, no distributivity is required. But hence $K \vdash \Box A \wedge A^t$. Hence $K \vdash \Box B \wedge B^t$ and $K \vdash B^t$, using no additional distributivity axiom. $\Box$

Lemma 4. *Let $\alpha(\overline{p})$ be a formula in CNF form of size k containing no negations. Assume that*

$$\Gamma := \alpha(\overline{p}) \to \beta_1 \vee \beta_2$$

has an intuitionistic proof with n proof-lines. Then

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

has a K-proof with $O(n+k)$ distributivity axioms.

Proof. For simplicity, let us assume that $\alpha = \bigwedge_i (p_1^i \vee p_2^i)$. In the general case the argument is similar. Then

$$\begin{aligned} \alpha^t &= \left(\bigwedge_i (p_1^i \vee p_2^i)\right)^t = \bigwedge_i (p_1^i \vee p_2^i)^t = \bigwedge_i ((\Box p_1^i \wedge (p_1^i)^t) \vee (\Box p_2^i \wedge (p_2^i)^t)) \\ &= \bigwedge_i ((\Box p_1^i \wedge \Box p_1^i) \vee (\Box p_2^i \wedge \Box p_2^i)). \end{aligned}$$

But $\bigwedge_i ((\Box p_1^i \wedge \Box p_1^i) \vee (\Box p_2^i \wedge \Box p_2^i))$ is, using no distributivity, equivalent to $\bigwedge_i (\Box p_1^i \vee \Box p_2^i)$. Hence $\alpha(\overline{p})^t$ is equivalent to $\alpha(\Box\overline{p})$, using no distributivity. We have

$$\begin{aligned} \Gamma^t &= (\alpha \to \beta_1 \vee \beta_2)^t \\ &= \Box\alpha \wedge \alpha^t \to (\Box(\beta_1 \vee \beta_2) \wedge (\beta_1 \vee \beta_2)^t) \\ &= \Box\alpha \wedge \alpha^t \to (\Box(\beta_1 \vee \beta_2) \wedge ((\Box\beta_1 \wedge \beta_1^t) \vee (\Box\beta_2 \wedge \beta_2^t))). \end{aligned}$$

Hence Γ^t is, using no distributivity, equivalent to

$$\Box\alpha(\overline{p}) \wedge \alpha(\Box\overline{p}) \to \Box(\beta_1 \vee \beta_2) \wedge ((\Box\beta_1 \wedge \beta_1^t) \vee (\Box\beta_2 \wedge \beta_2^t)). \tag{$\star$}$$

Assume that Γ has an intuitionistic proof with n proof-lines. Hence Γ^t and ($\star$) have K-proofs with $O(n)$ distributivity axioms. Hence also

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

has a K-proof with $O(n)$ distributivity axioms. Since α is a monotone formula then $\alpha(\Box\overline{p}) \to \Box\alpha(\overline{p})$ is provable with $O(k)$ distributivity axioms. Therefore

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

has a K-proof with $O(n+k)$ distributivity axioms. $\Box$

4. Monotone interpolation for *IL*

The formula $Clas(p)$ will be the formula $p \vee \neg p$ and $Clas(p_1, \ldots p_n)$ will be an abbreviation for

$$\bigwedge_{i=1,\ldots n} Clas(p_i).$$

Theorem 5. *Let $\beta_1 = \beta_1(\overline{p}, \overline{r_1})$ and $\beta_2 = \beta_2(\overline{q}, \overline{r_2})$ be propositional formulas, $\overline{p}$, $\overline{q}$, $\overline{r_1}$, $\overline{r_2}$ disjoint. Let $\overline{p} = p_1, \ldots p_k$ and $\overline{q} = q_1, \ldots q_k$ and $\overline{v} := \overline{p}, \overline{q}, \overline{r_1}, \overline{r_2}$. 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. Then

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

is an IL-tautology. Moreover, if the tautology has an IL-proof with n proof lines then there exists a monotone circuit $C(\overline{p})$ of size $O((n+k)^2)$ 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 $\bigwedge_{i=1,\ldots k}(p_i \vee q_i)$ can be transformed to an intuitionistically equivalent disjunction of conjunctions of the form

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

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

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

is an intuitionistic tautology. By Lemma 1 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

$$Clas(\overline{v}) \to \left(\bigwedge_{i\in M} p_i \to \beta_1\right)$$

is an intuitionistic tautology, since the assumption $Clas(\overline{v})$ enables us to reproduce the classical proof in IL. But then also

$$\bigwedge_{i\in M} p_i \to (Clas(\overline{v}) \to \beta_1)$$

and hence $(\star)$ are IL tautologies. The latter case is similar.

Assume that the formula

$$\Gamma := \bigwedge_{i=1,\ldots n} (p_i \vee q_i) \to (Clas(\overline{v}) \to \beta_1) \vee (Clas(\overline{v}) \to \beta_2)$$

has an intuitionistic proof with n proof-lines. By Lemma 4 the formula

$$\bigwedge_{i=1,\ldots k} (\Box p_i \vee \Box q_i) \to (\Box(Clas(\overline{v}) \to \beta_1) \vee \Box(Clas(\overline{v}) \to \beta_2))$$

has a K-proof with $O(n+k)$ distributivity axioms. However, $Clas(\overline{v})$ is a classical tautology. Hence

$$\Box(Clas(\overline{v}) \to \beta_1) \to \Box\beta_1$$

and

$$\Box(Clas(\overline{v}) \to \beta_2) \to \Box\beta_2$$

can be proved in K using one axiom of distributivity each. Hence

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

has a K-proof with $O(n+k)$ distributivity axioms. Hence, by Theorem 2 there exists a monotone circuit of size $O((n+k)^2)$ which interpolates $\neg\beta_2(\neg\overline{p}, \overline{r_2})$ and $\beta_1(\overline{p}, \overline{r_1})$. $\Box$

Let

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

be the proposition asserting that $\overline{r}$ is clique of size k on the graph represented by $\overline{p}$.[6]

Let

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

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

Theorem 6. *Let $\overline{p} = p_1, \ldots, p_n$ and $\overline{q} = q_1, \ldots q_n$ and let $\overline{p}, \overline{q}, \overline{r}, \overline{s}$ be disjoint, $\overline{v} := \overline{p}, \overline{q}, \overline{r}, \overline{s}$. Let*

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

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. We shall apply Theorem 5 to the formulas $\beta_1 := \neg Clique_n^{k+1}(\overline{p}, \overline{s})$ and $\beta_2 := \neg Color_n^k(\neg\overline{q}, \overline{r})$. First, β_2 is monotone in $\overline{q}$ since $Color(\overline{p}, \overline{r})$ 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 $\beta_2(\overline{q}/\neg\overline{p}, \overline{r}) = \neg Color_n^k(\overline{p}/\neg\neg\overline{p}, \overline{r})$ is classically equivalent to $\neg Color_n^k(\overline{p}, \overline{r})$ and

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

is a classical tautology. Hence Θ_n^k is an IL-tautology. Assume that it has an IL-proof with m proof-lines. Then, by Theorem 5, there exists a monotone circuit C in variables $\overline{p}$ of size $O((m+n)^2)$ 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 $Color_n^k(\overline{p}, \overline{r})$, C interpolates $Color_n^k(\overline{p}, \overline{r})$ and $\neg Clique_n^{k+1}(\overline{p}, \overline{s})$. By the result in [1] every such circuit must have size at least $2^{\Omega(n^{\frac{1}{4}})}$. Hence $m \geq \sqrt{2^{\Omega(n^{\frac{1}{4}})}} \sim 2^{\Omega(n^{\frac{1}{4}})}$. $\square$

An extension to IL_{Har}

A formula A will be called a *Harrop formula* if every disjunction in A occurs in the context

$$B \vee C \to D.$$

The system IL_{Har} will be obtained by adding the axiom

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

to IL for any Harrop formula A. ($\neg A$ is an abbreviation for $A \to \bot$.) Hence IL_{Har} restricted to Harrop formulas is equivalent to classical logic, in the sense that a Harrop formula A is provable in IL_{Har} iff A is a classical tautology. However, the disjunction retains non-classical behaviour in IL_{Har} and we can extend the lower bound to IL_{Har}. Recall the translation from intutionistic to K-formulas from Section 3.

Lemma 7. *Let A be a Harrop formula. Then*

$$\neg\Box\bot \to (\Box A \to A^t)$$

is a K-tautology. Moreover, the tautology has a K-proof with $O(|A|)$ distributivity axioms.

Proof. Straightforward induction on the size of A. The assumption $\neg\Box\bot$ is required at the basis step $\Box\bot \to \bot^t$. $\square$

6 An explicit formulation of *Clique* and *Color* can be found in [7], for example. However, the only important feature of the formulas is that the formula *Clique* is monotone in variables $\overline{p}$.

Lemma 8. 1. *If A is an IL_{Har}-tautology then $\neg\Box\perp\to A^t$ is K-tautology.*
2. *If A has an IL_{Har}-proof of size*[7] *n then $\neg\Box\perp\to A^t$ has a K-proof with $O(n)$ axioms of distributivity.*

Proof. The proof would proceed by induction as the proof of Proposition 3. It is sufficient to show that for any Harrop formula A,

$$\neg\Box\perp\to(\neg\neg A\to A)^t$$

is a K-tautology with a proof with $O(|A|)$ distributivity axioms. But

$$(\neg\neg A\to A)^t=\Box\neg\neg A\wedge(\neg\neg A)^t\to\Box A\wedge A^t$$

is, using two axioms of distributivity, equivalent to

$$\Box A\wedge(\neg\neg A)^t\to\Box A\wedge A^t$$

and hence it is sufficient to find a K-proof for

$$\neg\Box\perp\to(\Box A\wedge(\neg\neg A)^t\to\Box A\wedge A^t),$$

resp. for

$$\neg\Box\perp\to(\Box A\to\Box A\wedge A^t),$$

with $O(|A|)$ distributivity axioms. But that follows from the previous Lemma. □

The following theorem implies an exponential lower bound on sizes of proofs in IL_{Har}:

Theorem 9. *Let $\beta_1=\beta_1(\overline{p},\overline{r_1})$ and $\beta_2=\beta_2(\overline{q},\overline{r_2})$ be Harrop 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. Then

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

is an IL_{Har}-tautology. Moreover, if the tautology has an IL_{Har} proof of size n then there exists a monotone circuit $C(\overline{p})$ of size $O((n+k)^2)$ which interpolates $\neg\beta_2(\neg\overline{p},\overline{r_2})$ and $\beta_1(\overline{p},\overline{r_1})$.

Proof. The proof is similar to that of Theorem 5. Note that if we prove a tautology of the form

$$\neg\Box\perp\to(A\to\Box B\vee\Box C)$$

in K using n axioms of distributivity than we can prove

$$(A\to\Box B\vee\Box C)$$

using $n+1$ axioms of distributivity. □

Remark. Since the $\to,\neg$-fragment of IL_{Har} is equivalent to classical logic formalised using implication and negation, we also have a translation from a $\to,\neg\wedge$-fragment of classical logic to K, where classical logic is axiomatised as a Frege system (e.g., the system F offered in Section 6 restricted to $\to,\neg$-language). However, the translation cannot be used to find a lower bound on classical proofs. From Lemma 7 it follows that for every Harrop formula A of size n, if A is a classical tautology then $\neg\Box\perp\to A^t$ has a K-proof with $O(n)$ distributivity axioms.

[7] Note that here *size* of a proof means the number of its symbols.

5. Tautologies based on the gap between monotone and general circuits

We are now going to present a different kind of a hard tautology in IL. Again, the idea is still possibility of extracting a monotone circuit from an intutionistic 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 propositional logic we can find a tautology asserting that α does indeed define a monotone function. The most transparent formulation is the tautology

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

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.[8] 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 the next section. 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. $g \leq f \leq h$.[9] 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.

Theorem 10. *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 $\overline{q} = q_1, \dots q_k$, $\overline{v} := \overline{p}, \overline{q}$. Then the formula*

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

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

Proof. We shall apply Theorem 5. 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 to a DNF form with no negations attached to $\overline{p}$.) Since

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

then

$$\beta_1(\overline{p}) \vee \beta_2(\overline{q}/\neg\overline{p})) \equiv \alpha(\overline{p}) \vee \neg\alpha(\overline{p})$$

is a classical tautology. Hence $\Gamma := \bigwedge_{i=1,\dots k}(p_i \vee q_i) \to ((Clas(\overline{v}) \to \beta_1) \vee (Clas(\overline{v}) \to \beta_2)$ is IL-tautology and if Γ has a proof in IL with n proof-lines then there exists a monotone circuit C of size $O((n+k)^2)$ 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. □

[8] 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.

[9] 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.

As remarked above, Theorem 10 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 $[C(\overline{p})]$ 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 than those of $C(\overline{p})$.)

Lemma 11. *Let $C(\overline{p})$ be a circuit defining a monotone Boolean function. Let $\overline{p} = p_1, \dots p_n$ and $\overline{q} = q_1, \dots q_n$. 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:*

1. $\bigwedge_{i \in M} p_i \to [C(\overline{p})]$ *or*
2. $\bigwedge_{i \in N} q_i \to [\neg C(\neg\overline{q})]$.

Proof. Let $\alpha(\overline{p})$ be a propositional formula defining f. As we have checked in the proof of the previous Theorem, the formulas $\beta_1(\overline{p}) := \alpha(\overline{p})$ and $\beta_2(\overline{q}) := \neg\alpha(\neg\overline{p})$ satisfy the assumptions of Lemma 1. Hence either $\bigwedge_{i \in M} p_i \to \alpha(\overline{p})$ or $\bigwedge_{i \in N} q_i \to \neg\alpha(\neg\overline{q})$ is a tautology. Assume the first alternative. Let c be the output gate of C. Clearly

$$\bigwedge_{a \in C} M_a \to (r_c \equiv \alpha(\overline{p}))$$

is a tautology and hence also

$$\bigwedge_{i \in M} p_i \to \left(\bigwedge_{a \in C} M_a \to r_c\right) = \bigwedge_{i \in M} p_i \to [C(\overline{p})]$$

is a tautology. In the latter case the argument is identical. $\square$

Theorem 12. *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 $\overline{q} = q_1, \dots q_k$. Let $\overline{v}$ be the list of variables $\overline{p}, \overline{q}$ plus the variables occurring in $[C(\overline{p})]$ or $[\neg C(\neg\overline{q})]$. Then the formula*

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

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

Proof. To show that the formula is IL-tautology follows from Lemma 11 by an analogous argument as in Theorem 5. 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, 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

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

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

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

and

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

satisfy the assumptions of Theorem 10. Hence there is a monotone circuit $E(\overline{p})$ of size $O((n+k)^2)$ which interpolates $\beta_1(\overline{p})$ and $\neg\beta_2(\neg\overline{q})$. Since λ_1 and λ_2 are classical tautologies then both $\beta_1(\overline{p})$ and $\neg\beta_2(\neg\overline{q})$ are equivalent to $\alpha(\overline{p})$ and hence E computes f. $\square$

Corollary. *There exists a sequence γ_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 [13] and [5] 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 Theorem to the circuit C. $\square$

6. 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 Theorem 6 has a polynomial-size classical proof. We also prove something less obvious, that the tautology of Theorem 12 has a polynomial-size classical proof, if C is taken as a particular circuit computing the perfect matching function.

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

$$\neg\neg A \to A,$$

where $\neg A$ is understood as $A \to \perp$.

Speed-up between classical and intuitionistic propositional calculi

Theorem 13. *Let Θ_n^k be the IL-tautology of Theorem 6. 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 [2]. $\square$

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 Θ_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

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

Then Γ_i have linear size classical proofs. Moreover, by [3] 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 $IL \nvdash p \vee \neg p$ then Γ_i have only exponential size proofs in IL. (A similar argument can be found in [12].)

A quasi-polynomial speed-up between IL and F on tautologies of the form of Theorem 12 will follow from the argument in the next part of this section.

Fuzzy logic. Gödel–Dummett 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 obtain speed-up between Gödel–Dummett and intuitionistic logic in the same way as in the previous remark. More interestingly, we can find polynomial size proofs of tautologies of the form of Theorem 6. The tautology in Theorem 6 has the form

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

where $\overline{v}$ is the list $\overline{p}, \overline{q}, \overline{r}, \overline{s}$ 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

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

is a tautology. Hence it is sufficient to prove

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

or

$$Clas(\overline{v}) \to \left(\bigvee_{i=1,\dots n} (p_i \vee q_i) \to (\beta_1(\overline{p}, \overline{s}) \vee \beta_2(\overline{q}, \overline{r})) \right).$$

However, the last tautology has a polynomial size proof since the assumption $Clas(\overline{v})$ enables us to reproduce the classical proof in Gödel–Dummett logic.

Short proofs of tautologies based on monotonicity of the perfect matching problem

One might conjecture that we could employ classical analogies of the tautologies in Theorem 12, i.e., tautologies of the form[10]

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

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 F-proof. Since we have a quasi-polynomial lower bound for monotone circuits

[10] 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.

computing the perfect matching function, we conclude that there is no polynomial function relating the size of F-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 F-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 [13]), and the complexity of the algorithm does not invite formalisation.

The perfect matching problem

Let G be a bipartite graph on U and V, $U = u_1, \ldots u_n$, $V = v_1, \ldots v_n$. *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}, $i, j = 1, \ldots n$ 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 $\overline{p} = p_{ij}, i, j = 1, \ldots n$, variables s.t. $f_{PM}(\overline{p}) = 1$ iff the graph represented by $\overline{p}$ has a perfect matching. Clearly, f_{PM} is a monotone function. By the result of Razborov [10] 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 5. For circuits $C_1, \ldots C_n$ and a formula A

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

will be an abbreviation form

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

where $r_1, \ldots r_n$ are variables representing the outputs of $C_1, \ldots C_n$. 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
$$A(\overline{p}, \overline{q}) \to A(\overline{p}, C_{\overline{q}}) \qquad (\star)$$
is a tautology, and
2. *solve the problem A polynomially in F*, if the circuits have polynomial size and $(\star)$ has a polynomial size F-proof.

Moreover, the function $f_A(\overline{p})$ will be the Boolean function s.t. for any assignment of the variables $\overline{p}$, $f_A(\overline{p}) = 1$ iff there exists an assignment of $\overline{q}$ 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 14. *Let $A = A(\overline{p}, \overline{q})$ be a formula, $\overline{r} = r_1, \ldots r_k$, $\overline{p} = p_1, \ldots p_k$. 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*
$$\bigwedge_{i,j=1,\ldots n} (p_i \to r_i) \to (C(\overline{p}) \to C(\overline{r})) \qquad (\star)$$
has a polynomial size proof in F.

Proof. (1) is clear.

(2) We must show that

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

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

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

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

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

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

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

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

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 15. *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 F-proof. Hence (to match the formulation of Theorem 12) 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 F-proof.

Acknowledgement

The paper was written in Prague, Mathematical Institute of the Czech Academy of Sciences, with support from grant IAA1019401.

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 $U_0^u, U_1^u, \dots U_n^u \subseteq U$, $V_1^u, \dots V_n^u \subseteq V$.

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

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 $a' \in U^u_{k-1}$ 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 $a'' \in V^u_{k-2}$ 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^u_i, V^u_i constructed above either define an augmenting path, or

$$X := \bigcup_{i=0,\dots n} U^u_i$$

is a critical set. For if $Y := \bigcup_{i=0,\dots n} V^u_i$ 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, since there is no critical set, the algorithm finds an augmenting path for M_i and hence it extends the matching M_i to M_{i+1}, until a perfect matching is reached.

The formalisation

There exist polynomial formulas $Count^k_n(p_1, \dots p_n)$ asserting that exactly k of the variables $\overline{p} = p_1, \dots p_n$ are true s.t. their expected properties have polysize proofs in F (see [2]). This enables the formalisastion of basic counting arguments in F.

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

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

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 in a bipartite graph on U and V which starts in some $u_{i_1} \in U$ can be represented by a sequence $u_{i_1}, \dots u_{i_k} \in U$ $v_{j_1}, \dots v_{j_k} \in V$ s.t. the path contains edges $\langle u_{i_l}, v_{j_l}\rangle$ and $\langle v_{i_l}, u_{j_{l+1}}\rangle$. 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

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

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

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

will be the formula asserting that $\overline{f}$ and $\overline{g}$ represent an alternating path of odd length from a to b w.r.t. to the matching $\overline{q}$, i.e., the conjunction of i) $\mathrm{ODDPATH}^k_{ab}(\overline{p}, \overline{f}, \overline{g})$, ii) $\neg\mathrm{MATCHED}_a(\overline{q})$ and iii) $\bigwedge_{i,j}(f_{il} \wedge g_{jl} \to \neg q_{ij})$, for odd l, and $\bigwedge_{i,j}(f_{il} \wedge g_{jl} \to \neg q_{ij})$ for l even. Similarly for an odd path which starts in some $a \in U$ and for even length paths. Let

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

be the formulas asserting that $\overline{f}$ and $\overline{g}$ represent a path resp. alternating path from a to b of length k.

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

will be the formula asserting that $\overline{f}$ and $\overline{g}$ represent an augmenting path from u to v w.r.t. to the matching $\overline{q}$, i.e., an alternating path from a to b s.t. b is unmatched. 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 $\overline{A} = A_{ij}, i, j = 1, \ldots n$, $\mathrm{Dom}(\overline{A})$ will be the list of n formulas

$$\bigwedge_i A_{i1}, \ldots \bigwedge_i A_{in}.$$

The formula

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

$\overline{r} = r_1, \ldots r_n$, 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, it is a disjunction of conjunctions of the form $\mathrm{Count}_n^k(r_1, \ldots r_n) \wedge \mathrm{Count}_n^j(\mathrm{Dom}(r_i \wedge p_{ij}))$, for $j < k$.

The following lemma shows that the easy direction of Hall's theorem is shortly provable in F:

Lemma 16. *The formula*

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

has a polynomial-size Frege proof.

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

Lemma 17. *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:*

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

Proof. Recall the sets $U_0^a, \ldots U_n^a$ and $V_0^u, \ldots V_n^a$. For $a \in U$, we can find polynomial-size circuits E_{au}^s, $s = 0, \ldots n$, $u \in U$, and F_{av}^s, $s = 1, \ldots n$, $v \in U$, 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 anologons of the defining relations between U_i^a and V_i^a have polynomial proofs in F. The proof is then a straightforward formalisation of the above informal argument. □

Lemma 18. *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:*

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

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. □

Let us recall the matchings $M_0, \ldots M_n$ from our description of the algorithm. Using the circuits from Lemma 17 and Lemma 18, we can find polynomial circuits $C_{\overline{q}}^k(\overline{p})$ s.t. there are short Frege proofs of

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

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

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

Finally, from Lemma 16 it follows that

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

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

References

[1] N. Alon, R. Boppana, The monotone circuit complexity of Boolean functions, Combinatorica 7 (1) (1987) 1–22.
[2] S.R. Buss, Polynomial size proofs of the propositional pigeonhole principle, Journal of Symbolic Logic 52 (1987) 916–927.
[3] S.R. Buss, G. Mints, The complexity of the disjunction and existence properties in intuitionistic logic, Annals of Pure and Applied Logic 99 (1999) 93–104.
[4] S.R. Buss, P. Pudlaák, On the computational content of intuitionistic propositional proofs, Annals of Pure and Applied Logic 109 (2001) 46–94.
[5] M. Grötschler, L. Lovász, A. Schrijver, The ellipsoid method and its consequences in combinatorial optimization, Combinatorica 1 (2) 169–197.
[6] P. Hrubeš, Lower bounds for modal logics, Journal of Symbolic Logic (in press).
[7] J. Krajíček, Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, Journal of Symbolic Logic 62 (2) (1997) 457–486.
[8] G. Mints, A. Kojevnikov, Intuitionistic Frege systems are polynomially equivalent, Zapisky Nauchnych Seminarov POMI 316 (2004) 129–146.
[9] P. Pudlák, On the complexity of intuitionistic propositional calculus, Sets and proofs, in: Logic Colloquium'97, Cambridge University Press, 1999, pp. 197–218.
[10] A.A. Razborov, Lower bounds on the monotone complexity of some Boolean functions, Soviet Mathematics Doklady 31 (1985) 354–357.
[11] R. Statman, Intuitionistic propositional logic is polynomial-space complete, Theoretical Computes Science 9 (1979) 67–72.
[12] R. Statman, Speedup by theories with infinite models, Proceedings of American Mathematical Society 81 (3) (1981) 465–469.
[13] É. Tardos, The gap between monotone and non-monotone circuit complexity is exponential, Combinatorica 7 (4) (1987) 141–142.