Записки научных
семинаров ПОМИ
Том 316, 2004 г.

G. Mints, A. Kojevnikov

INTUITIONISTIC FREGE SYSTEMS ARE POLYNOMIALLY EQUIVALENT

ABSTRACT. As shown in [3], any two classical Frege systems polynomially simulate each other. The same proof does not work for the intuitionistic Frege systems, since they can have non-derivable admissible rules. (The rule A/B is *derivable* if formula $A \to B$ is derivable. The rule A/B is *admissible* if for all substitutions σ if $\sigma(A)$ is derivable then $\sigma(B)$ is derivable). In this paper we polynomially simulate a single admissible rule and show that any two intuitionistic Frege systems polynomially simulate each other.

1. Introduction

One of the important open problems in the neighborhood of P=NP is obtaining superpolynomial lower bounds for the size of derivations in propositional calculus stated in a standard way with axiom schemata and modus ponens (*Frege systems*). No results of this kind are known for a classical propositional calculus CPC where satisfiability problem is NP-complete. Under the assumption NP$\cap$co-NP$\not\subseteq$ P/poly and for factoring it is shown in [2] that the intuitionistic propositional calculus Int does not always have polynomial size proofs. Derivability problem for Int is PSPACE-complete.

Recall that in the classical case *a proof system* for a language L is defined in [3] as a polynomial-time computable function f mapping strings in some finite alphabet (proof candidates) onto L (the set of theorems). If $y = f(\pi)$, then we will say that π is a *proof* of y. The notation $\pi : y$ means that y is proved by π. An *inference system* is defined there as a finite set of *schematic axioms* and *inference rules*. An *inference rule* is an $(n+1)$-tuple of formulas $A_1, \ldots, A_n/B$, where B is a logical consequence of $A_1, \ldots, A_n$. This rule is written

$$\frac{A_1 \ \ldots \ A_n}{B} \tag{1.1}$$

The research described in this publication was made possible in part by Award No. RM1-2409-ST-02 of the U.S. Civilian Research & Development Foundation for the Independent States of the Former Soviet Union (CRDF).

An inference system S is called in [3] *implicationally complete* if B is derivable in S from $A_1, \dots, A_n$ whenever B is a logical consequence of $A_1, \dots, A_n$. A *Frege system* is defined as an implicationally complete inference system.

It is well known ([17, 3]) that any two classical Frege systems polynomially simulate each other. The proofs given there used the fact that all admissible rules of CPC are derivable. Let us remind that a rule (1.1) is *derivable* in a system S if there is a deduction of the formula B from assumptions $A_1, \dots, A_n$ by the rules of the system S. For all systems we consider here the deduction theorem holds, hence the rule (1.1) is derivable iff a formula

$$(A_1 \to \dots \to (A_n \to B) \dots) \tag{1.2}$$

is derivable in the system S. By completeness theorem this is equivalent to B being a logical consequence of $A_1, \dots, A_n$.

A rule (1.1) is *admissible* in S if for all substitutions σ of formulas for propositional variables, if all formulas $\sigma(A_1), \dots, \sigma(A_n)$ are derivable in S, then $\sigma(B)$ is derivable in S. The following result is well-known.

Lemma 1.1. *Every admissible rule of* CPC *is derivable.*

Proof. Note that if a formula (1.2) is not derivable in CPC, it is not a Boolean tautology according to classical truth-tables. Hence there is an assignment

$$v : \{x_1, \dots, x_k\} \to \{0, 1\}$$

of truth values to propositional variables that makes the formula (1.2) false:

$$v(A_1) = \dots = v(A_n) = 1, \quad \text{but} \quad v(B) = 0. \tag{1.3}$$

Consider a following substitution:

$$\sigma(x_i) := \begin{cases} \top, & \text{if } v(x_i) = 1, \\ \bot, & \text{if } v(x_i) = 0, \end{cases}$$

where the truth values $\top, \bot$ are present in the language or defined, say $\top := (\bot \to \bot)$.

From (1.3), we see by a standard Kalmar proof of completeness theorem for CPC that formulas

$$\sigma(A_1), \dots, \sigma(A_n) \text{ and } \neg\sigma(B)$$

are derivable in CPC. This refutes admissibility of the rule (1.1). $\square$

The same proof does not work for the intuitionistic propositional systems, since they can have non-derivable admissible rules. An example for the standard formulation of Int ([8, 11]) is

$$\frac{\neg A \to B \vee C}{(\neg A \to B) \vee (\neg A \to C)}. \tag{1.4}$$

This fact led to a question: can adding an admissible rule to a standard formulation of Int lead to a dramatic reduction in the size of proofs. In the present paper we provide a negative answer.

A problem of the existence of an algorithm recognizing admissibility of a rule in Int was posed in [5]. The solution was found by V. V. Rybakov in 1984. Rybakov also showed that admissible rules of Int do not have a finite basis and constructed a semantic criterion for admissibility [18]. In [9], a nice r.e. set of rules was proved to be a basis for the admissible rules of Int. The latter result is based on a result from [6]: the variety of Heyting algebras has finitary unification type. This means that for every satisfiable formula A in Int there are effectively computable substitutions $\sigma_1, \dots, \sigma_n$ such that $\sigma_i(A), 1 \leqslant i \leqslant n$ is a theorem of Int, and if some substitution instance $\tau(A)$ of A is a theorem, then τ is less general then some of the σ_i. The intuitionistic unification problem was posed by N. Shanin at the end of 1960s and some partial results were obtained by his Ph.D. student [7].

Definition 1.2. *A Frege system S for Int is a finite set of schematic axioms derivable in Int and schematic inference rules admissible in Int, provided S contains up to a polynomial translation a standard axiomatization* **H***:*

Axiom schemata:

$$A \to (B \to A)$$
$$A \to (B \to C) \to ((A \to B) \to (A \to C))$$
$$(A \& B) \to A; (A \& B) \to B$$
$$A \to (B \to (A \& B))$$
$$A \to (A \vee B); B \to (A \vee B)$$
$$(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$$
$$\bot \to A$$

Inference rule:

$$\frac{A \quad A \to B}{B} \; \textit{Modus Ponens}.$$

We consider formulas in the standard language $L = \{\&, \vee, \rightarrow, \bot\}$, but everything works for a language polynomially translatable into L. Important example used below is the language of *sequents* $A_1, \ldots, A_n \Rightarrow B$ translated by formula (1.2).

In the present paper, we provide a polynomial method of extracting from a proof of the premise of arbitrary admissible rule some proof of its conclusion. Therefore the following Theorem holds.

Theorem 1.3. *Any two Frege systems over $\{\&, \vee, \rightarrow, \bot\}$ for Int are polynomially equivalent.*

Remark 1.4. Our treatment covers all connectives explicitly definable from the standard set $\{\&, \vee, \rightarrow, \bot\}$. This covers all connectives considered in the Prawitz-style approach by ([19, 20]), that is connectives given by introduction rules plus corresponding (in the sense of Gentzen) elimination rules. The general notion of an intuitionistic connective was a subject of further discussion [10]. A kind of a Sheffer stroke for Int was defined in [12].

The paper is organized as follows. In Sec. 2, we restate a complete *proof system AR for admissible rules* from [9]. Arbitrary admissible rule of Int has a finite proof in AR. In Sec. 4, we provide a polynomial time algorithm for modeling each of the rules of AR. It is essentially the polynomial disjunction property algorithm from [1] extended as in the Lemma 2 of [2] to cover the rules of AR and streamlined along the lines of a polynomial Kleene slash of [4].

An article extending these results will be published in LC'2004.

2. A system AR complete for admissible rules

The system **AR** in [9] has

Axiom schemata:

$$V: \ (A \rightarrow r \vee s) \vee t \triangleright (A)(r, s, p_1, \ldots, p_n) \vee t,$$

where

$$A = \&_{i=1}^{n}(p_i \rightarrow q_i),$$

$$(A)(r, s, p_1, \ldots, p_n) = (A \rightarrow r) \vee (A \rightarrow s) \vee \bigvee_{i=1}^{n}(A \rightarrow p_i)$$

and

$$A \triangleright B \quad \text{where} \quad \text{Int} \vdash (A \rightarrow B).$$

Inference rules:

$$\frac{C \rhd A \quad C \rhd B}{C \rhd A \& B}\ Conj \qquad \frac{A \rhd B \quad B \rhd C}{A \rhd C}\ Cut$$

We introduce an equivalent Hilbert style system.

System AR

Axioms: all derivable formulas of Int [a derivation in Int is supposed to be given explicitly]

Two inference rules:

$$\frac{(A \to r \vee s) \vee t}{(A)(r, s, p_1, \dots, p_n) \vee t} V \qquad \frac{A \quad A \to B}{B}\ ModusPonens$$

Lemma 2.1. $\mathtt{AR} = AR$, *that is*

$$A \rhd B \text{ in } \mathtt{AR} \text{ iff } B \text{ is derivable from } A \text{ in } AR.$$

Hence AR *is complete for admissible rules of Int.*

Proof. Easy induction on derivations. □

Theorem 2.2 [9]. *A rule* F/G *is admissible in* **H** *iff there is a proof of* B *from* A *in the system* AR.

3. Natural Deduction

This section expands some material from Sec. 3 of [3] and adjusts it to the intuitionistic framework.

3.1. The System NJ. Derivable objects in a natural deduction system NJ are *sequents*

$$A_1, \dots, A_n \Rightarrow B \ (n \geqslant 0)$$

written also $\Gamma \Rightarrow A$, where Γ is a finite ordered sequence of formulas.

The system has axioms

$$\Gamma, A \Rightarrow A \quad \text{and} \quad \Gamma, \bot \Rightarrow A \quad \text{for any formula } A$$

and inference rules (standard elimination and introduction rules for &, $\vee$, $\to$ plus structural rules):

$$\frac{\Gamma \Rightarrow A \& B}{\Gamma \Rightarrow A}\ \&E \qquad \frac{\Gamma \Rightarrow A \& B}{\Gamma \Rightarrow B}\ \&E \qquad \frac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \& B}\ \&I$$

$$\frac{\Gamma \Rightarrow A \vee B \qquad \Gamma, A \Rightarrow C \qquad \Gamma, B \Rightarrow C}{\Gamma \Rightarrow C}\ \vee E \quad \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}\ \vee I \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}\ \vee I$$

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

$$\frac{\Gamma \Rightarrow B}{A, \Gamma \Rightarrow B}\ \text{Weak} \quad \frac{\Gamma, A, A \Rightarrow B}{\Gamma, A \Rightarrow B}\ \text{Contr} \quad \frac{\Gamma, A, B, \Sigma \Rightarrow C}{\Gamma, B, A, \Sigma \Rightarrow C}\ \text{Perm},$$

where Γ, Σ are arbitrary finite sequences of formulas.

This version of NJ is obviously equivalent to other versions where an *antecedent* (the part at the left of $\Rightarrow$) of a sequent is a finite set or a finite multiset of formulas.

Definition 3.1. *A natural deduction is a sequence of sequents where each member is an axiom or is obtained from the previous ones by an inference rule.*

NJ_w ($w \geq 2$) denotes the restriction of NJ where only sequents $A_1, \dots, A_n \Rightarrow B$ with $n \leq w$ are allowed.

$$(A_1, \dots, A_n \Rightarrow B)^* :=$$
$$:= \begin{cases} (A_1 \& (A_2 \& \dots \& (A_{n-1} \& A_n) \dots)) \to B, & \text{if } n > 0, \\ B, & \text{if } n = 0. \end{cases}$$

We use notation $\lambda(\pi)$ and $\rho(\pi)$ [3] for number of lines and maximal number of occurrences of atoms in a formula in a derivation π.

Theorem 3.2. *There are polynomial time functions g_1, g_2 such that*

$$\text{if } \pi : \Gamma \vdash_{\mathbf{H}} B, \text{ then } g_1(\pi) : \Gamma \Rightarrow B \text{ in } NJ_3$$

with

$$\lambda(g_1(\pi)) \leq c\lambda(\pi), \quad \rho(g_1(\pi)) \leq c\rho(\pi); \tag{3.1}$$

$$\text{and if } \kappa : \Gamma \Rightarrow B \text{ in } NJ_w, \text{ then } g_2(\kappa) : \Gamma \vdash_{\mathbf{H}} B$$

with

$$\lambda(g_2(\kappa)) \leq c\lambda(\kappa), \quad \rho(g_2(\kappa)) \leq c\rho(\kappa), \tag{3.2}$$

where c depends only on w.

Proof. Every axiom schema of **H** is provable in NJ_3 and modus ponens is modeled by $\to I$ providing (3.1).

For any natural deduction κ of a sequent $\Gamma \Rightarrow B$ let $g_2(\kappa)$ be the **H**-proof of of the formula $(\Gamma \Rightarrow B)^*$ obtained by replacing every sequent

S by S^* and inserting additional formulas to complement every rule of natural deduction:

$$(X \to (A\&B)) \to (X \to A),\ (X \to (A\&B)) \to (X \to B),$$

$$(X \to A) \to ((X \to B) \to (X \to A\&B)), \ldots$$

$$(A\&X \to B) \to (X \to (A \to B),\ (X \to B) \to (A \to (X \to B)),$$

$$(A\&(A\&X) \to B) \to (A\&X \to B)$$

$$(\Gamma, A, B, \Sigma \Rightarrow C)^* \to (\Gamma, B, A, \Sigma)^* \tag{3.3}$$

where the antecedent Γ, A, B, Σ has at most w terms. **H**-proofs of all formulas except (3.3) are bounded by a constant independent of w. Parameters of **H**-proofs of (3.3) depend on w in an essential way [15, Chapter I, Section 5]. This provides estimates (3.2). □

4. Polynomial approximation property

Definition 4.1. *Let*

$$A = \&_{i\leq m}(A_i \to B_i), \tag{4.1}$$

and

$$\Pi : A \Rightarrow C_1 \vee C_2, \tag{4.2}$$

be a natural deduction.

Notation $\pi : A \vdash E$ means that π is a proof of a sequent $A' \Rightarrow E$ for $A' = A$ or $A' = \emptyset$.

Let $[\Pi]_A$ be the closure of the set of all subproofs of Π under the following rules:

Proofs of all sequents

$$A \Rightarrow A, \quad A \Rightarrow (A_i \to B_i), \quad (i \leq m) \tag{4.3}$$

are in $[\Pi]_A$.

If $\pi : \Gamma \Rightarrow C$ is a subproof of π, then $\pi \in [\Pi]_A$.

If $\pi_1, \ldots, \pi_k \in [\Pi]_A$, π_{k+1} is a subproof of Π (the major premise), then $R_A(\pi_1, \ldots, \pi_{k+1}) \in [\Pi]_A$, where

$$\frac{\pi_1 : A \vdash E_1 \ \ldots \ \pi_k : A \vdash E_k \quad \pi_{k+1} :\ E_1, \ldots, E_k, A \vdash E}{R(\pi_1, \ldots, \pi_{k+1}) :\ A \vdash E}\ R_A.$$

The symbol $R_\emptyset$ denotes the modification of the rule R_A with $A = \emptyset$:

$$\frac{\pi_1 : \Rightarrow E_1 \ \ldots \ \pi_k : \Rightarrow E_k \ \pi_{k+1} : \ E_1, \ldots, E_k \Rightarrow E}{R_\emptyset(\pi_1, \ldots, \pi_{k+1}) : \Rightarrow E} \ R_\emptyset$$

$[\Pi]_\emptyset$ means a closure of the deduction Π with respect to the rule $R_\emptyset$.

Define a relation $\Pi|_A C$ for formulas C by induction on C.

Definition 4.2. $\Pi|_A C$ *if either*
one of the sequents

$$A \Rightarrow A_j \ (j = 1, \ldots, m), \quad A \Rightarrow \bot, \quad A \Rightarrow C_i \ (i = 1, 2) \tag{4.4}$$

(possibly with an empty antecedent instead of A) is in Π; or

$$A \Rightarrow C \in \Pi \tag{4.5}$$

(possibly with an empty antecedent instead of A) and one of the following conditions is satisfied:

1. *C is a propositional variable or*
2. *$C = D\&E$ and $\Pi|_A D$ and $\Pi|_A E$ or*
3. *$C = D \vee E$ and ($\Pi|_A D$ or $\Pi|_A E$) or*
4. *$C = D \rightarrow E$ and ($\Pi|_A D$ implies $\Pi|_A E$).*

The relation $|_A$ is extended to sequents:

$$\pi|_A \ E_1, \ldots, E_k, A' \Rightarrow C, \ \ \textit{iff} \ \ \pi|_A E_1, \ldots, \pi|_A E_k \ \ \textit{imply} \ \ \pi|_A C$$

The relation $\Pi|_\emptyset$ is defined similarly to $\Pi|_A C$ for proofs

$$\Pi : \Rightarrow C_1 \vee C_2 \tag{4.6}$$

instead of (4.2), requiring presence in Π one of the sequents

$$\Rightarrow C_1, \ \Rightarrow C_2 \tag{4.7}$$

instead of (4.4) and $\Rightarrow C \in \Pi$ instead of (4.5).

$$\pi|_\emptyset \ E_1, \ldots, E_k \Rightarrow C, \ \ \textit{iff} \ \ \pi|_\emptyset E_1, \ldots, \pi|_\emptyset E_k \ \ \textit{imply} \ \ \pi|_\emptyset C.$$

If $\Gamma = E_1, \ldots, E_k$, then $\pi|_\emptyset \Gamma$ means $(\pi|_\emptyset E_1, \ldots, \pi|_\emptyset E_k)$, and similarly for $\pi|_A \Gamma$.

Remark 4.3. The closure is essentially the same as reasoning with Horn clauses using unit resolution.

Note that the rule R is derivable in NJ. For example

$$\frac{A \Rightarrow E_1 \; A \Rightarrow E_2 \; A, E_1, E_2 \Rightarrow E}{A \Rightarrow E} R$$

is inferred as follows (leaving out Weak, Perm, Contr):

1. $A, E_1, E_2 \Rightarrow E$
2. $A, E_2 \Rightarrow E_1 \rightarrow E$ $(\rightarrow I)$
3. $A \Rightarrow E_1$
4. $A, E_2 \Rightarrow E$ $(\rightarrow E)$
5. $A \Rightarrow E_2 \rightarrow E$ $(\rightarrow I)$
6. $A \Rightarrow E_2$
7. $A \Rightarrow E$ $(\rightarrow E)$

Definition 4.4. *NJR is the result of adding rules $R_\emptyset, R_A$ to NJ.*

Definition 4.5. *Let π be an NJR-deduction. Denote by $\lambda_1(\pi)$ the number of different succedents G in sequents $\Gamma \Rightarrow G$ occurring in π with a nonempty Γ.*

Theorem 4.6. *Let π be an NJR-deduction and π' be a natural deduction of a sequent $\Rightarrow F$, where*

$$F = \quad (A \rightarrow (C_1 \vee C_2)) \vee D, \text{ and } A = \&_{i \leq m}(A_i \rightarrow B_i)$$

from some sequent in π. Then the deduction $\pi \cup \pi'$ can be extended to an NJR-deduction Π of a sequent $\Rightarrow F'$, where

$$F' = \quad ((A \rightarrow C_1) \vee ((A \rightarrow C_2) \vee \bigvee_{i \leq m} (A \rightarrow A_i))) \vee D \tag{4.8}$$

such that

$$\lambda_1(\Pi) = \lambda_1(\pi \cup \pi') + m; \quad \rho(\Pi) = \max(\rho(\pi \cup \pi'), \rho(F')), \tag{4.9}$$

$$\lambda(\Pi) \leq \lambda(\pi \cup \pi') + (3m + 2) + 2\lambda_1(\pi \cup \pi'). \tag{4.10}$$

Proof. Step 1. Form the closure π^+ of $\pi \cup \pi'$ under the rule $R_\emptyset$.

Claim 1. For every sequent $\Gamma \Rightarrow E \in \pi \cup \pi'$ one has $\pi^+|_\emptyset \; \Gamma \Rightarrow E$. In particular one of the sequents

$$\Rightarrow (A \rightarrow C_1 \vee C_2), \quad \Rightarrow D \tag{4.11}$$

is in π^+.

Proof. The second part follows by $\pi^+|_\emptyset(A \to C_1 \vee C_2) \vee D$, so we prove the first part by induction on the proof $\pi \cup \pi'$.

If one of the sequents (4.11) is in π^+, then we have $\pi^+|_\emptyset S$ for every sequent S, and the claim is proved. Assume that

$$\text{none of the sequents (4.11) is in } \pi^+. \tag{4.12}$$

Consider possible cases.

Induction base: axiom.

Case $\perp \Rightarrow C$. Since $\pi^+|_\emptyset\perp$, is impossible, we are done.

Case $C \Rightarrow C$. Then $\pi^+|_\emptyset C$ by assumption.

Induction step. Consider cases depending of the last rule L of $\pi \cup \pi'$.

1. L is $\&I$, $\vee I$ or $\&E$. Straightforward using inductive definition of $\pi^+|_\emptyset C$.
2. L is $\vee E$
$$\frac{\Gamma \Rightarrow D \vee F \;\; \Gamma, D \Rightarrow G \;\; \Gamma, F \Rightarrow G}{\Gamma \Rightarrow G}.$$
Assume $\pi^+|_\emptyset\Gamma$. By IH for the left premise $\pi^+|_\emptyset D \vee F$, that is $\pi^+|_\emptyset D$ or $\pi^+|_\emptyset F$ by definition of $|_\emptyset$. Apply IH to one of remaining premises to get $\pi^+|_\emptyset G$.
3. L is $\to I$
$$\frac{\Gamma, D \Rightarrow F}{\Gamma \Rightarrow D \to F}.$$
Assume $\pi^+|_\emptyset\Gamma$, $\pi^+|_\emptyset D$. By $\pi^+|_\emptyset\Gamma$ all sequents $\Rightarrow \Gamma$ are in π^+. By closure for the rule $R_\emptyset$, $\Rightarrow D \to F$ is in π^+. By IH applied to the premise of $\to I$, $\pi^+|_\emptyset F$ as needed for $\pi^+|_\emptyset D \to F$.
4. $\to E$:
$$\frac{\Gamma \Rightarrow D \to F \;\; \Gamma \Rightarrow D}{\Gamma \Rightarrow F}.$$
Assume $\pi^+|_\emptyset\Gamma$. By IH, $\pi^+|_\emptyset(D \to F)$, $\pi^+|_\emptyset D$, hence $\pi^+|_\emptyset F$ as required.
5. For some formula B we have $\pi^+|_\emptyset B$, and a sequent $B \Rightarrow E$ in $\pi \cup \pi'$ is obtained by the inference:
$$\frac{B \Rightarrow \Gamma \;\; \ldots \;\; B, \Gamma \Rightarrow E}{B \Rightarrow E} \; R_B.$$
Assumption B may be absent in some of the premises. By IH we get
$$\pi^+|_\emptyset \; B \Rightarrow \Gamma, \;\; \pi^+|_\emptyset \; B, \Gamma \Rightarrow E.$$

Together with an assumption $\pi|_\emptyset B$ this implies $\pi^+|_\emptyset\Gamma$ by definition of $|_\emptyset$. Applying this to $\pi^+|_\emptyset B, \Gamma \Rightarrow E$, we get $\pi^+|_\emptyset E$ as required for $\pi^+|_\emptyset(B \Rightarrow E)$.

□ Claim 1.

Step 2. If $\Rightarrow D$ is in π^+, we are done. Add $\Rightarrow F$ derived by $\vee$I. The result $\Pi = \pi^+ \cup \{\Rightarrow F\}$ is a deduction of $\Rightarrow F$.

Step 3. It remains to treat the case when $\Rightarrow (A \rightarrow C_1 \vee C_2)$ is in π^+. We repeat the step 1 relative to the formula A. Extend π^+ by including the sequents (4.3). Form the closure π^* of $\pi^+ \cup (4.3)$ under the rule R_A with a restriction: *the main premise $E_1, \dots, E_k \Rightarrow A$ is not a conclusion of an R-rule.*

Finally put $\Rightarrow F'$ as an end sequent.

Claim 2. For every sequent $\Gamma \Rightarrow E \in \pi^+ \cup$ (4.3) one has $\pi^*|_A\ \Gamma \Rightarrow E$. In particular one of the sequents

$$A \Rightarrow A_j\ (j = 1, \dots, m), \quad A \Rightarrow \bot, \quad A \Rightarrow C_i\ (i = 1, 2) \tag{4.13}$$

is in π^*.

Proof. The second part follows by $\pi^*|_A(A \rightarrow C_1 \vee C_2)$, so we prove the first part by induction on the proof $\pi^+ \cup$ (4.3).

If one of the sequents (4.13) is in π^*, then we have $\pi^*|_A S$ for every sequent S, and the claim is proved. Assume that

$$\text{none of the sequents (4.13) is in } \pi^*. \tag{4.14}$$

We have

$$\pi^*|_A(A_i \rightarrow B_i)$$

for all $i \le m$ since $\pi^*|_A A_i$ is excluded by (4.14), but $A \Rightarrow (A_i \rightarrow B_i)$ is included into π^* by (4.3). Hence we have

$$\pi^*|_A A \tag{4.15}$$

by definition of $|_A$.

Induction base: axiom.

Case $\bot \Rightarrow C$. Since $\pi^*|_A\bot$, is impossible by (4.14), we are done.

Case $C \Rightarrow C$. Then $\pi^*|_A C$ by assumption (and we are done) except $C = A$, when (4.15) works.

Induction step. Consider cases depending of the last rule L of $\pi^+ \cup$(4.3).

1. L is $\&, \vee I$ or $\& E$. Straightforward using inductive definition of $\pi^*|_A C$.

2. L is $\vee E$
$$\frac{\Gamma \Rightarrow D \vee F \;\; \Gamma, D \Rightarrow G \;\; \Gamma, F \Rightarrow G}{\Gamma \Rightarrow G}.$$
Assume $\pi^*|_A \Gamma$. By IH for the left premise $\pi^*|_A D \vee F$, that is $\pi^*|_A D$ or $\pi^*|_A F$ by definition of $|_A$. Apply IH to one of remaining premises to get $\pi^*|_A G$.

3. L is $\rightarrow I$
$$\frac{\Gamma, D \Rightarrow F}{\Gamma \Rightarrow D \rightarrow F}.$$
Assume $\pi^*|_A \Gamma$, $\pi^*|_A D$. By $\pi^*|_A \Gamma$ all sequents $A \Rightarrow \Gamma$ are in π^+. By closure for the rule R_A, the sequent $A \Rightarrow D \rightarrow F$ is in π^+. By IH applied to the premise of $\rightarrow I$, $\pi^*|_A F$ as needed for $\pi^*|_A D \rightarrow F$.

4. $\rightarrow E$:
$$\frac{\Gamma \Rightarrow D \rightarrow F \;\; \Gamma \Rightarrow D}{\Gamma \Rightarrow F}.$$
Assume $\pi^*|_A \Gamma$. By IH, $\pi^*|_A (D \rightarrow F)$, $\pi^*|_A D$, hence $\pi^*|_A F$ as required.

5. For some formula B we have $\pi^*|_A B$, and a sequent $B \Rightarrow E$ in $\pi \cup (4.3)$ is obtained by the inference:
$$\frac{B \Rightarrow \Gamma \;\; \ldots \;\; B, \Gamma \Rightarrow E}{B \Rightarrow E}\, R_B$$
Assumption B may be absent in some of the premises. By IH we get
$$\pi^*|_A \; B \Rightarrow \Gamma, \quad \pi^*|_A B, \Gamma \Rightarrow E$$
Together with an assumption $\pi^*|_A B$ this implies $\pi^*|_A \Gamma$ by definition of $|_A$. Applying this to $\pi^*|_A B, \Gamma \Rightarrow E$, we get $\pi^*|_A E$ as required for $\pi^*|_A \; B \Rightarrow E$.

$\square$ Claim 2.

Step 4. Required NJR-deduction Π of $\Rightarrow F'$ is obtained by $\rightarrow I$ (and maybe $\Rightarrow \bot \rightarrow A_1$) and a series of $\vee I$ from the sequent in the list (4.13) which is a member of π^*.

Let us estimate the parameters of the deduction Π.

λ_1	ρ	λ
$\lambda_1(\pi \cup \pi')$	$\rho(\pi \cup \pi')$	$\lambda(\pi \cup \pi') + \lambda_1(\pi \cup \pi')$
	$\max \rho(F')$	$+1$
$+m$		$+2\lambda_1(\pi \cup \pi') + 2m$
	$\max \rho(F')$	
		$+m+2.$

Step 1 adds to $\pi \cup \pi'$ only sequents $\Rightarrow G$ (with empty antecedents) coming from sequents $\Gamma \Rightarrow G$ with non-empty succedents Γ occurring in $\pi \cup \pi'$. Therefore λ_1, ρ are not changed; the contribution to λ is $\leq \lambda_1(\pi \cup \pi')$.

Step 2 preserves λ_1, changes ρ taking $\rho(F')$ into consideration and adds at most 1 to λ. In that case there are no steps 3, 4.

Step 3 adds sequents $A \Rightarrow G$ and/or $\Rightarrow G$ coming from sequents $\Gamma \Rightarrow G$ (with nonempty $\Gamma \neq G$) occurring in $\pi \cup \pi'$. The contribution of this step to λ_1 comes from the sequents (4.3), hence bounded by m. Indeed all other succedents G of the sequents with nonempty antecedents are the same as in $\pi \cup \pi'$. The contribution to ρ is 0 (all formulas A, G are already present in $\pi \cup \pi'$), the contribution to λ is at most $2\lambda_1(\pi \cup \pi') + 2m$. Indeed each sequent $\Gamma \Rightarrow G$ in the result of the Step 1 with Γ nonempty (all of them come from $\pi \cup \pi'$) or (4.3) can generate at most two new sequents: $A \Rightarrow G$ and $\Rightarrow G$. $A \Rightarrow A$ does not generate anything new. Since the sequents $\Rightarrow G$ added at the Step 1 are not added again, the term $2\lambda_1(\pi \cup \pi')$ of Step 3 absorbs the term $\lambda_1(\pi \cup \pi')$ of the Step 1. Finally, Step 4 updates ρ by $\rho(F')$ and adds at most $m + 2$ intermediate sequents. All of them except at most two: $A \Rightarrow \bot$, $\bot \Rightarrow C_1$, have empty antecedent. Possible additions during Step 4 are shown below, with D' denoting $\bigvee_{i \leq m}(A \to A_i)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow A_1}{\Rightarrow (A \to A_1)} \quad \cdots}{\Rightarrow D'}}{\Rightarrow (A \to C_2) \vee D'}}{\Rightarrow (A \to C_1) \vee ((A \to C_2) \vee D')}}{\Rightarrow ((A \to C_1) \vee ((A \to C_2) \vee D')) \ \vee D}$$

or

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow \bot \quad \dfrac{\bot \Rightarrow C_2}{\Rightarrow \bot \to C_2}}{A \Rightarrow C_2}}{\Rightarrow A \to C_2}}{\dfrac{\Rightarrow (A \to C_2) \vee D'}{\Rightarrow (A \to C_1) \vee ((A \to C_2) \vee D')}}}{\Rightarrow ((A \to C_1) \vee ((A \to C_2) \vee D')) \ \vee D}$$

where $A \Rightarrow C_2$ may be given instead of being derived from $A \to \bot$.

Lemma 4.7. *Assume that NJV deduction P contains n V-inferences*

$F_1/F_1', \ldots, F_n/F_n'$ *with*

$$F_j = \quad (A^j \to (C_1^j \vee C_2^j)) \vee D^j, \quad \text{and} \quad A^j = \&_{i \le m_j}(A_i^j \to B_i^j)$$

$$F_j' = \quad ((A^j \to C_1^j) \vee ((A^j \to C_2^j) \vee \bigvee_{i \le m} (A^j \to A_i^j))).$$

Then P can be transformed into an NJR deduction P' of the same formula with

$$\rho(P') = \rho(P); \quad \lambda(P') \le (2n+1)\lambda(P) + (2n+4)(m_1 + \ldots + m_n). \quad (4.16)$$

Proof. V-inferences determine a partition of P:

$$P = \pi_1 \cup \pi_2 \cup \ldots \cup \pi_n \cup \pi_{n+1},$$

where F_j, F_j' go to π_j, π_{j+1}, respectively.

$$\begin{array}{c} \pi_1 \\ \dfrac{F_1}{F_1'}\ V_1 \\ \pi_2 \\ \dfrac{F_2}{F_2'}\ V_2 \\ \vdots \\ \pi_n \\ \dfrac{F_n}{F_n'}\ V_n \\ \pi_{n+1} \end{array}$$

Let Π_1 be the result of applying Lemma 4.6 to $\emptyset$ as π and π_1 as π'. For $j \ge 1$ NJR-deduction Π_{j+1} is obtained by the same lemma with Π_j as π and π_{j+1} as π'. We have by induction on j that Π_j derives F_j' and

$$\lambda_1(\Pi_j) \le \lambda_1(\pi_1 \cup \ldots \cup \pi_j) + (m_1 + \ldots + m_j);$$

$$\lambda(\Pi_j) \le \lambda(\pi_1 \cup \ldots \cup \pi_j) + 3(m_1 + \ldots + m_j) + 2j + 2j\lambda_1(\Pi_j)$$

$$\rho(\Pi_j) \le \max(\rho(\pi_1 \cup \ldots \cup \pi_j), \rho(F_j'))$$

Induction base is (4.9, 4.10). Induction step is similar:

$$\lambda_1(\Pi_{j+1}) \le \lambda_1(\Pi_j) + \lambda_1(\pi_{j+1}) + m_{j+1} \le$$

$$\lambda_1(\pi_1 \cup \ldots \cup \pi_{j+1}) + (m_1 + \ldots + m_{j+1})$$

$$\lambda(\Pi_{j+1}) \le \lambda(\Pi_j \cup \pi_{j+1}) + 3m_{j+1} + 2 + 2\lambda_1(\Pi_j \cup \pi_{j+1}) \le$$

$$\lambda(\pi_1 \cup \ldots \cup \pi_j) + 3(m_1 + \ldots + m_j) + 2j +$$

$$2j\lambda_1(\Pi_j) + \lambda(\pi_{j+1}) + 3m_{j+1} + 2 + 2\lambda_1(\Pi_{j+1})$$

$$\leq \lambda(\pi_1 \cup \ldots \cup \pi_{j+1}) + 3(m_1 + \ldots + m_{j+1}) + 2(j+1) + 2(j+1)\lambda_1(\Pi_{j+1})$$

$$\rho(\Pi_j) \leq \max(\rho(\pi_1 \cup \ldots \cup \pi_{j+1}), \rho(F'_j), \rho(F'_{j+1})) =$$

$$\max(\rho(\pi_1 \cup \ldots \cup \pi_j), \rho(F'_{j+1})),$$

since F'_j occurs in π_{j+1}. Adding π_{n+1} to Π_n, we get required proof P' with the estimates:

$$\lambda(P') \leq \lambda(\Pi_n) + \lambda(\pi_{n+1}) \leq$$

$$\lambda(\Pi) + 3(m_1 + \ldots + m_n) + 2n + 2n\lambda_1(\Pi_n) \leq$$

$$\lambda(P) + 3(m_1 + \ldots + m_n) + 2n + 2n\lambda(P) + 2n(m_1 + \ldots + m_n) \leq$$

$$(2n+1)\lambda(P) + (2n+4)(m_1 + \ldots + m_n)$$

$$\rho(\Pi') \leq \rho(\pi).$$

□

5. Polynomial modeling of admissible rules

If π is a derivation $S_1, \ldots, S_p$ and σ is a substitution of formulas for propositional variables, then $\sigma(\pi)$ means $\sigma(S_1), \ldots, \sigma(S_p)$.

Lemma 5.1. *If π is a derivation of a sequent S from a sequent T in a system AR, then $\sigma(\pi)$ is a derivation of a sequent σS from σT in AR with*

$$\lambda(\sigma(\pi)) = \lambda(\pi),\ \rho(\sigma(\pi)) \leq c\rho(\pi)$$

with c depending only on σ.

Proof. The proof proceeds by induction on π. If $\sigma = (C_1/x_1, \ldots, C_n/x_n)$, then $c = \max\{\rho(C_1), \ldots, \rho(C_n)\}$. □

Lemma 5.2. *Let* $\mathbf{H}$ *be a Frege system, and*

$$\mathbf{H}^{+} = \mathbf{H} + \{R_1, \dots, R_r\}$$

be its extension with admissible rules

$$R_i \cong F_i/G_i, \; i = 1, \dots, r.$$

Then there is a constant c *depending on* $R_1, \dots, R_r$ *and a polynomial-time function* f *such that for all proofs*

$$\pi :\vdash_{\mathbf{H}^+} B$$

one has:

$$f(\pi) :\vdash_{\mathbf{H}} B, \; \lambda(f(\pi)) \leqslant c(\lambda(\pi))^2, \; \rho(f(\pi)) \leqslant c\rho(\pi).$$

Proof. By Theorem 2.2, the $\mathbf{H}$-derivation π is transformed into an NJ_3V-deduction of the same formula by replacing each of the rules R_i by its derivation in AR. By Theorem 3.2 we can assume that the axioms of AR that are $\mathbf{H}$-derivable formulas are replaced by their NJ_3-deductions. If π had r_1 applications of rules $R_1, \dots, R_r$, this adds $\leq c_1 r_1$ sequents with formulas of the size $\leq c_1\rho(\pi)$. The deduction P has $n \leq c_1 r_1$ applications of the rule V. Here c_1 depends only on $R_1, \dots, R_n$. We assume c_1 to be big enough, in particular $c_1 > 1$. We have

$$\rho(P) \leq \max(\rho(\pi), c_1\rho(\pi)) = c_1\rho(\pi)$$

$$\lambda(P) \leq \lambda(\pi) + c_1 r_1 \leq (c_1 + 1)\lambda(\pi)$$

Each of the numbers $m_1, \dots, m_n$ in(4.16) for P is bounded by a constant (say the same c_1) depending only of $R_1, \dots, R_r$, hence $m_1 + \dots + m_n \leq c_1 n$. By Lemma 4.7, there exists an NJ_3-deduction P' of the same sequent as before such that

$$\rho(P') \leq \rho(P) \leq c_1\rho(\pi),$$

$$\lambda(P') \leq (2n+1)\lambda(P) + (2n+4)(m_1 + \dots + m_n) \leq (2n+4)(\lambda(P) + c_1 n)$$

$$\leq (2\lambda(P) + 4)(c_1 + 1)\lambda(P) \leq c(\lambda(\pi))^2.$$

□

Theorem 5.3. *For any two intuitionistic Frege systems* $\mathfrak{F}_1$ *and* $\mathfrak{F}_1$ *over* $\{\&, \vee, \rightarrow, \bot\}$ *there is a function* f *and constant* c *such that for all derivations* $\pi : \vdash_{\mathfrak{F}_1} B$, *we have* $f(\pi) : \vdash_{\mathfrak{F}_2} B$, *and* $\lambda(f(\pi)) \leqslant c(\lambda(\pi))^2$, $\rho(f(\pi)) \leqslant c\rho(\pi)$.

Proof. Lemma 5.2 provides a proof in $\mathbf{H} \subseteq \mathfrak{F}_2$. □

Theorem 1.3 is a corollary of Theorem 5.3.

We thank E. A. Hirsch who drew our attention to the problem of the equivalence of the intuitionistic propositional proof systems and helped to clarify related problems. The authors are grateful to Yu. Matiyasevich, V. V. Rybakov, and V. Orevkov for useful discussions.

References

1. S. Buss, G. Mints, *The complexity of the disjunction and existential properties in intuitionistic logic.* — Annals of Pure and Applied Logic **99**, Nos. 1–3 (1999), 93–104.
2. S. Buss, P. Pudlak, *On the computational content of intuitionistic propositional proofs.* — Annals of Pure and Applied Logic **109**, Nos. 1–2 (2001), 49–64.
3. S. A. Cook, A. Reckhow, *The relative efficiency of propositional proof systems.* — The Journal of Symbolic Logic **44**, No. 1 (1979), 36–50.
4. M. Ferrari, C. Fiorentini, G. Fiorino, *On the complexity of disjunction and explicit definability properties in some intermediate logics.* — in: Proceedings of LPAR'02, Lect. Notes in Computer Science **2514** (2002), 175–189.
5. H. Friedman, *One Hundred and Two Problems in Mathematics Logic.* — The Journal of Symbolic Logic **40**, No. 2 (1975), 113–129.
6. S. Ghilardi, *Unification in intuitionistic logic.* — The Journal of Symbolic Logic **64**, No. 2 (1999,)859–880.
7. Ja. Ja. Golota, *Nets of Marks and Deducibility in the Intuitionistic Propositional Calculus.* — Zap. Nauchn. Semin. LOMI **40** (1974), 4–9.
8. R. Harrop, *Concerning formulas of the types* $A \rightarrow B \vee C$, $A \rightarrow (Ex)B(x)$ *in intuitionistic formal systems.* — The Journal of Symbolic Logic **25**, No. 1 (1960), 27–32.
9. R. Iemhoff, *On the admissible rules of intuitionistic propositional logic.* — The Journal of Symbolic Logic **66**, No. 1 (2001), 281–243.
10. G. Kreisel, *Constructivist approaches to logic.* — In: *Modern Logic–A Survey: Historical, Philosophical, and Mathematical Aspects of Modern Logic and Its Applications* (E. Agazzi, ed.) **149** (1981), 67–91.
11. G. Kreisel, H. Putnam, *Eine Unableitbarkeitsbeweismethode für den intuitionistischen Aussagenkalkül.* — Archiv für mathematische Logic und Grundlagenforschung, **3**, Nos. 3–4 (1957), 74–78.
12. A. V. Kuznetsov, *Analogs of the 'Sheffer stroke' in constructive logic.* — Dokl. Akad. Nauk SSSR **160** (1965), 274–277.
13. G. Mints, *Derivability of admissible rules.* — Zap. Nauchn. Semin. LOMI **32** (1972) 85–99.

14. G. Mints, *A Short Introduction to Intuitionistic Logic.* — Kluwer Academic/Plenum Publishers (2000).
15. V. P. Orevkov, *Complexity of Proofs and their Transformations in Axiomatic Theories.* — Translations of Mathematical Monographs 128, American Mathematical Society (1993).
16. P. Pudlák, *On the complexity of the propositional calculus.* — In: *Sets and Proofs: Invited papers from Logic Colloquium'* 97, Cambridge University Press (1999), pp. 197–218.
17. R. A. Reckhow, *On the lengths of proofs in the propositional calculus.* — PhD thesis, Department of Computer Science, University of Toronto (1976).
18. V. V. Rybakov, *Admissibility of Logical Inference Rules.* — Elsevier, Amsterdam (1997).
19. P. Schroeder-Heister, *A natural extension of natural deduction.* — The Journal of Symbolic Logic **49**, No. 4 (1984), 1284–1300.
20. J. I. Zucker, R. S. Tragesser, *The adequacy problem for inferential logic.* — Journal of Philosophical Logic **7** (1978), 501–516.

Department of Philosophy,
Stanford University
URL: www-philosophy.stanford.edu/fss/gm.html

Поступило 5 декабря 2004 г.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
URL: logic.pdmi.ras.ru/~arist/