Order Number 9325075

On logical flow graphs

Carbone, Alessandra, Ph.D.

City University of New York, 1993

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

ON LOGICAL FLOW GRAPHS

by

Alessandra Carbone

A dissertation submitted

to the Graduate Faculty in Mathematics

in partial fulfillment of the requirements

for the degree of Doctor of Philosophy,

The City University of New York.

1993

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the requirement for the degree of Doctor of Philosophy.

5/3/93 — **Rohit Parikh**

Date — Chair of Examining Commitee

5/3/93 — **Jozeph Dodziuk**

Date — Executive Officer

Rohit Parikh

Melvin Fitting

Kenneth McAloon

Supervisory Committee

The City University Of New York

Abstract

ON LOGICAL FLOW GRAPHS

by

Alessandra Carbone

Adviser: Professor Rohit Parikh

The key topic of this thesis is the notion of *proof*. This research considers proofs as objects, measures their complexity with the number of lines and studies the logical relations among the occurrences of formulas in them. We develop a theory of how the influence of a formula spreads through a proof, based on the notion of *logical flow graph* (introduced by S. Buss in 1991) and we study how the logical flow graph of a proof behaves with respect to two basic results in proof theory: the Cut Elimination Theorem and the Craig Interpolation Theorem.

The results are used to obtain lower bounds on the number of lines in a proof. Namely, we applied them to the following context of Peano Arithmetic: postulating that large numbers are not finite leads to an inconsistent extension of arithmetic which is, however, conservative for proofs of low complexity. Thus an inconsistent theory can prove true results, as long as the proofs are not too long. This was first proved by Parikh in 1971. In 1985, Dragalin improves Parikh lower bounds on the complexity of the proofs of true sentences. In this work we improve Parikh's statement showing that if a sentence is proved using the fact that large numbers are not finite by means of a proof with low complexity, then one can find a

proof of it with *lower* complexity and not using the postulate on large numbers. Our lower bounds are the best possible bounds and considerably improve the ones obtained by both Parikh and Dragalin. We then consider the consistent theory of large numbers asserting the *existence* of some large number and show that not only is a conservative extension of Peano Arithmetic but also that there is no speed-up by this theory over arithmetic.

Results on the complexity (intended as number of symbols) of the interpolant C for a given sequent $A \rightarrow B$ and on the complexity (intended as number of lines) of the proofs $A \rightarrow C$ and $C \rightarrow B$ are also studied and proofs of the classical and intuitionistic Craig's Interpolation Theorem based on logical flows are given.

Acknowledgements

I would like to express my heartly thanks to my adviser Rohit Parikh. Many times, talking to him, simple thoughts were revealing their beauty and what appeared as small to me, was becoming suddenly meaningful. He offered to me his understanding of the questions of logic, stimulated my own thoughts and intuitions. I am profoundly gratitude to him for these reasons, in equal manner. I would also like to say that my interest in proof theory and arithmetic was greatly encouraged by his work and thank him again for the financial support he supplied along two years of my studies.

I wish to express my thanks to Melvin Fitting for having been always stimulating to me. The content of chapter 4 has been developed because of his remarks in one of my seminars. Many more suggestions have been pointed out by both Melvin Fitting and Kenneth McAloon. Those are not content of this thesis but they will hopefully be of my future work.

I wish to thank Peter Clote for addressing me to the literature at the start of my dissertation and encouragment in pursuing my ideas; Sam Buss for pointing out to me a mistake in a paper (not included in this thesis but involving the ideas developed here) and encouragement; Franco Montagna and Dick deJongh for introducing me to my first research experience.

Thanks to Rohit Parikh, Melvin Fitting, Kenneth McAloon for serving in my committee and jointly to Sam Buss, Peter Clote, Dick deJongh and Franco Montagna for being my references when applying for a job.

Last, I would like to acknowledge the presence of Konstantinos Georgatos, as a friend as well as a collegue, for continuous conversations and moral support all along my graduate studies.

Contents

Chapter 1

Introduction

The key topic of this thesis is the notion of *proof*. The concept of *provability* has been fairly well understood in logic, but still the concept of *proof* is not. This research considers proofs as objects, measures their complexity in number of lines and studies the logical relations among the occurrences of formulas in them.

Namely, we will develop further some ideas introduced by Sam Buss in [Bus91]. In his paper, Buss uses the notion of ***logical flow graph*** to prove that the k-provability problem (i.e. given a formula A and an integer k, to determine if A has a proof with k or fewer lines) for a particular first order theory is undecidable.

Concepts similar to Buss definition of logical flow graphs have been independently and previously introduced by Jean-Yves Girard who discusses tracing the flow of formulas through linear logic proofs ([Gir87]).

We will develop a theory and study how the logical flow graph of a proof behaves with respect to two basic results in proof theory: Gentzen's Cut Elimination Theorem and

Craig's Interpolation Theorem. The third and fourth chapters in this thesis are respectively devoted to them.

The Cut Elimination Theorem says that any proof in the sequent calculus can be transformed into a proof with good structural properties, where "good" roughly means that one can actually understand the relations between formulas in it. We can ask, what is the information content of the original proof kept by the transformation? Or analogously, what is the "effective" contribution of a proof to the validity of a sequent? We show that what matters in a proof are all formulas occurring in it having some precisely formalized logical link to the formulas of the end-sequent. Nothing more. In terms of logical flow graphs, the structure that counts turns out to be a subgraph of the complete logical flow graph describing the proof. In chapter 3 we develop and apply this idea to the context of arithmetic.

The Craig Interpolation Theorem speaks about the relations between formulas in the end-sequent of a sequent calculus proof. Roughly speaking, given a sequent $A \rightarrow B$ there is a formula C, called the interpolant, that is made up of subformulas "common" to A and B and such that $A \rightarrow C$ and $C \rightarrow B$ are provable sequents. We can ask what the proof of $A \rightarrow B$ says about such "common" subformulas. We show that "common" simply means logically linked in the logical flow graph of the proof.

These are the main ideas on which the thesis is based. Let us now introduce in more detail the content of each chapter.

Chapter 2 PRELIMINARIES

A version of Gentzen's sequent calculus is presented; the notion of logical flow graph is reviewed and examples are given. In a subsection we present a proposition involving the concept of *similarity* of proofs.

Chapter 3 FEASIBLE NUMBERS AND NO SPEED-UP FOR NON-STANDARD THEORIES

Postulating that large numbers are not finite leads to an inconsistent extension of arithmetic which is, however, conservative for proofs of low complexity (intended as number of lines). Thus an inconsistent theory can prove true results, as long as the proofs are not too long. This was first proved by Parikh in 1971. In 1985, Dragalin improves Parikh's lower bounds on the complexity of the proofs of true sentences. Our result improves Parikh's statement by showing that if a sentence is proved using the fact that large numbers are not finite, by means of a proof with low complexity, then one can find a proof of it with *lower* complexity and not using the postulate on large numbers. Our lower bounds are the best possible bounds and considerably improve the ones obtained by both Parikh and Dragalin. We then consider the consistent theory of large numbers asserting the *existence* of some large number and show that not only is it a conservative extension of Peano Arithmetic but also that there is no speed-up by this theory over arithmetic. The whole argument is proof-theoretical and based on the analysis of the relations between occurrences of formulas. It points out the correspondence between the number of formulas in a proof and the existence of non-standard numbers in models of arithmetic.

Chapter 4 INTERPOLANTS AND FLOW GRAPHS

We investigate the relations between interpolants of a sequent and the logical flow of the formulas in a proof of it. We present the proofs of both classical and intuitionistic version of the Craig Interpolation Theorem based on considerations on logical flow of formulas. We also prove two results concerning the logical complexity (i.e. the number of symbols) of the interpolants.

It is a well known fact that the logical complexity of the interpolants for a given sequent $A \to B$ is in general not linear in the logical complexity of A and B (see [Mun93]). It seems that the reason is connected with the logical flow of the formulas in a proof. We show that whenever A (respectively, B) does not contain pairs of subformulas *logically* linked (in a precise sense defined by flow graphs) one to each other, then there is an interpolant with logical complexity bounded by the logical complexity of A (respectively, B).

The second fact we point out concerns sequents $A \to B$ with no logical links between formulas occurring both in A and B. Given a proof (possibly *with* cuts) of $A \to B$ we "extract" a proof either of $A \to$ or of $\to B$ with smaller complexity than the complexity of the original proof for $A \to B$.

Note that these two facts *cannot* be shown as a consequence of the usual construction used to prove the Craig Interpolation Theorem because the latter is based on the Cut Elimination Theorem which increases the length of proofs very substantially.

Chapter 2

Preliminaries

2.1 The Sequent Calculus

This section contains a brief review of the *the sequent calculus*, the formulation of first order logic due to Gentzen. For a detailed exposition the reader can refer to [Tak75] or [Gir87] or [Kle88].

The sequent calculus is formulated in a first order language (possibly containing the equality symbol) with logical symbols $\wedge, \vee, \neg, \supset, \exists$ and $\forall$; it has *free* variables denoted $a, b, c, \ldots$ and *bound* variables denoted $x, y, z, \ldots$. As usual, *terms* are formed from constant symbols, free variables and function symbols; *semi-terms* are like terms but may contain bound variables as well. *Formulas* are defined as usual with the condition that only bound variables may be quantified and only free variables may appear free. *Semi-formulas* are defined as formulas except for both bound and free variables that may appear free in it; one can observe that a subformula of a formula is a semi-formula and in fact a subformula of a semi-formula is a semi-formula.

A *sequent* is a line of the form

$$A_1, \ldots, A_k \to B_1, \ldots, B_l$$

where the A_i's and B_j's are formulas; its intended meaning is $\bigwedge_i A_i \supset \bigvee_j B_j$. We permit k and l to be zero. A sequence of formulas separated by commas is a *cedent*; in the sequent above, $A_1, \ldots, A_k$ is the *antecedent* and $B_1, \ldots, B_l$ is the *succedent*. We will often refer to antecedents and succedents in a sequent using capital letters of the Greek alphabet. For instance $\Gamma \to \Delta$ denotes a sequent. In the following we will intend a sequence $A_1, \ldots, A_k$ to be a *multiset* of formulas, i.e. finite (possibly empty) set of formulas, in which repetitions of some formulas are admitted; the order of formulas in a multiset is not essential but for every member of the multiset the number of its occurrences is important. By the symbol Γ, Δ we denote the union of the multisets Γ and Δ (i.e. the multiset containing all formulas in Γ and Δ so that if n_1 and n_2 are the number of occurrences of a formula A in Γ and Δ respectively, then $n_1 + n_2$ is the number of occurrences of A in the union Γ, Δ.) The multiset A, Γ is obtained from Γ by adjoining the formula A. For short we will denote Γ_1, Γ_2 as $\Gamma_{1,2}$.

It should be pointed out that a proof in the sequent calculus is intended to be a *tree* of sequents; each sequent must either be an axiom (in this case the sequent is labeling a leaf of the tree) or be derived by one of the rules of inference we will give below (the sequent is a label for an internal node of the tree). In a sequent calculus proof every occurrence of a sequent in the proof other than the end-sequent is used exactly once as a premise of an inference. Notice that a proof could be defined as sequence of sequents; but obviously any proof defined as such can be transformed into a tree-like proof by duplicating subproofs to derive intermediate results multiple times.

The axioms for our sequent calculus are the following

(i) logical axioms of the form $A, \Gamma \to \Delta, A$;

(ii) equality axioms of the form

- $\Gamma \to \Delta, t = t$;
- $t_1 = s_1, \ldots, t_k = s_k, P(t_1, \ldots, t_k), \Gamma \to \Delta, P(s_1, \ldots, s_k)$ where P is a k-ary predicate symbol;
- $t_1 = s_1, \ldots, t_k = s_k, \Gamma \to \Delta, f(t_1, \ldots, t_k) = f(s_1, \ldots, s_k)$ where f is a k-ary function symbol.

The formulas occurring in the cedents Γ, Δ of the above axioms are referred to as *non-distinguished* formulas of the sequent. All others are called *distinguished.*

The rules of inference are divided into two groups: the *logical rules* that introduce logical connectives to the left and to the right side of a sequent, and the *structural rules* (note that cut rule and contraction rule will be the only structural rules of the calculus.)

The *logical rules* are the following:

$\neg$: *left* $\dfrac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}$ $\qquad$ $\neg$: *right* $\dfrac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}$

$\wedge$: *right* $\dfrac{\Gamma_1 \to \Delta_1, A \quad \Gamma_2 \to \Delta_2, B}{\Gamma_{1,2} \to \Delta_{1,2}, A \wedge B}$

$$\wedge : \textit{left} \qquad \frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \qquad \frac{A, \Gamma \to \Delta}{B \wedge A, \Gamma \to \Delta}$$

$$\vee : \textit{left} \qquad \frac{A, \Gamma_1 \to \Delta_1 \quad B, \Gamma_2 \to \Delta_2}{A \vee B, \Gamma_{1,2} \to \Delta_{1,2}}$$

$$\vee : \textit{right} \qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B} \qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, B \vee A}$$

$$\supset : \textit{left} \qquad \frac{\Gamma_1 \to \Delta_1, A \quad B, \Gamma_2 \to \Delta_2}{A \supset B, \Gamma_{1,2} \to \Delta_{1,2}}$$

$$\supset : \textit{right} \qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, A \supset B} \qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, B \supset A}$$

$$\exists : \textit{left} \qquad \frac{A(b), \Gamma \to \Delta}{(\exists x)A(x), \Gamma \to \Delta} \qquad \exists : \textit{right} \qquad \frac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, (\exists x)A(x)}$$

$$\forall : \textit{left} \qquad \frac{A(t), \Gamma \to \Delta}{(\forall x)A(x), \Gamma \to \Delta} \qquad \forall : \textit{right} \qquad \frac{\Gamma \to \Delta, A(b)}{\Gamma \to \Delta, (\forall x)A(x)}$$

In the $\exists$: *left* and $\forall$: *right* inferences the free variable b is called the *eigenvariable* and must not appear in the lower sequent. The variable x must be freely substitutable into A for all four quantifier inferences. Note that in the $\vee$: *right* and $\supset$: *right* inferences, the formula B is not logically connected to the upper sequent of the rule.

The *structural rules* are

$$\textit{Cut} \qquad \frac{\Gamma_1 \to \Delta_1, A \quad A, \Gamma_2 \to \Delta_2}{\Gamma_{1,2} \to \Delta_{1,2}}$$

$$\textit{Contraction} \qquad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A} \qquad \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}$$

The formula occurrence, which is introduced explicitly into the lower sequent of a given rule of inference is called the *main* formula of the inference, and the formula(s), which are distinguished in the upper sequent(s) are the *auxiliary* formula(s). For example in the $\vee$:*left* rule the formula $A \vee B$ is the main formula and the formulas A and B are the auxiliary formulas. The other formulas of a sequent (i.e. the formulas in Γ, Δ) are called *side formulas.*

The cut rule has no main formulas; its auxiliary formulas are also called *cut-formulas.* An application of the cut rule will simply be called a *cut.*

The auxiliary formulas of a contraction rule are also called *contracting formulas.*

We do not need the usual Weakening and Exchange rules in our calculus (as they appear in Gentzen's original formalization), because it uses multisets of formulas instead of sequences. The reader familiar with Gentzen's original formulation may like to notice that non-distinguished formulas appearing in logical axioms and equality axioms play the role of formulas introduced by Weakening.

Our formalization will be referred to as LK_e, ignoring the slight differences from Gentzen's classical formalization. The symbol LK denotes the system LK_e when the equality axioms are dropped.

2.2 The logical flow graph

In [Bus91], Sam Buss introduces the notion of *logical flow graph* to study how the influence of a formula spreads through a proof in LK_e. Following his introduction, we present the notion of logical flow graph formulated for our sequent theory. We will then prove that a logical flow graph is always acyclic and we will introduce the notion of *inner* proof based on subgraphs of a logical flow graph.

Let Π be a proof. An *s-formula* is an *occurrence* of a subformula of a formula in Π (here, '*s*-' stands for '*semi*-' or '*sub*-'). It has to be emphasized that an *s*-formula is an *occurrence* of a subformula in the proof as opposed to the subformula itself which may occur many times in the proof. A formula A is a *variant* of B if A can be obtained from B by changing some of the terms in B. The *logical flow graph* (formally defined below) is a directed graph whose nodes are *s*-formulas in Π; two *s*-formulas will be connected by an edge only if they are variants of each other; any two *s*-formulas connected by an edge will be in (distinct) sequents of some inference or will both be in an axiom on opposite sides of the sequent arrow.

We define the logical flow graph by specifying the edges.

First, in an axiom $A, \Gamma \rightarrow \Delta, A$ there is an edge directed from the left-hand A to the right-hand A. In an equality axiom

$$t_1 = r_1, \ldots, t_k = r_k, P(t_1, \ldots, t_k), \Gamma \rightarrow \Delta, P(r_1, \ldots, r_k)$$

there is an edge directed from $P(t_1, \ldots, t_k)$ to $P(r_1, \ldots, r_k)$. In all other equality axioms (and when P is an equality in the axiom displayed above), there is an edge from all distinguished equations in the antecedent to the distinguished equation in the succedent.

Second, in any logical and structural inferences listed above, there is an edge directed from each side formula in the antecedent Γ in the *lower* sequent to the corresponding side formula of Γ in the *upper* sequent(s). There is an edge directed from each formula in the succedent Δ in the *upper* sequent to the corresponding formula of Δ in the *lower* sequent.

Third, in any logical inference or in a contraction rule if A (or B) is an auxiliary formula which appears in the succedent of an upper sequent of an inference then there is an edge directed from that A (or B) to the corresponding s-formula in the lower sequent. If A (or B) is an auxiliary formula which appears in the antecedent of an upper sequent of an inference then there is an edge directed towards that A (or B) from the corresponding s-formula in the lower sequent.

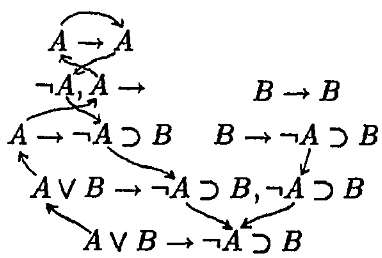
Fourth, in a cut inference there is an edge directed from the cut formula A in the succedent of the left-hand upper sequent to the occurrence of A in the antecedent of the right-hand upper sequent.

Fifth, suppose there is a directed edge from an s-formula A_1 to A_2 and suppose B_1 is a subformula of A_1. Since A_1 and A_2 are variants there is a subformula B_2 of A_2 which corresponds to the subformula B_1 of A_1; the s-formulas B_1 and B_2 are, of course, variants. If B_1 occurs positively in A_1 then there is an edge from B_1 to B_2. If B_1 occurs negatively in A_1 then there is an edge from B_2 to B_1. Recall that B occurs positively (negatively) in A if B occurs an even (odd) number of times in the scope of a negation or in the left-hand operand of an implication. Clearly B_1 occurs positively in A_1 if and only if B_2 occurs positively in A_2. This concludes the definition of logical flow graph.

As an example consider the following proof

$$\dfrac{\dfrac{\dfrac{\dfrac{A \rightarrow A}{\neg A, A \rightarrow}}{A \rightarrow \neg A \supset B} \quad \dfrac{B \rightarrow B}{B \rightarrow \neg A \supset B}}{A \vee B \rightarrow \neg A \supset B, \neg A \supset B}}{A \vee B \rightarrow \neg A \supset B}$$

with logical flow graph restricted to the formula A (edges for $\neg A$, B and $\neg A \supset B$ are not indicated)



A formula B occurs positively (negatively) in a sequent $\Gamma \rightarrow \Delta$ if B occurs negatively (positively) in a formula of Γ or positively (negatively) in a formula of Δ. If not otherwise indicated, in the following we will intend a positive or negative occurrence of a formula to be defined relatively to sequents. Notice that in a logical flow graph there are four kinds of edges: edges connecting positive occurrences, that are directed downwards; edges connecting negative occurrences, that are directed upwards; edges defined on axioms, that are directed from negative occurrences towards positive occurrences; edges defined on cut-formulas, that are directed from positive occurrences towards negative occurrences.

If a proof is cut-free, its logical flow graph will contain only three kinds of edges.

We call any sequence of connected edges in the logical flow graph of $\Pi : S$ a *path*; we call any path starting and ending with two (distinct) s-formulas occurring in S a *bridge*.

A logical flow graph is *acyclic* when there is no path starting from an occurrence of a formula and going back to it.

Proposition 1 *Let $\Pi : S$ be a LK-proof. The logical flow graph of Π is acyclic.*

To show this proposition we need first the definition of *weak occurrence* of a formula in a proof. Let $\Pi : S$ be a proof and $\mathcal{L}$ be a logical flow graph. An occurrence of a formula A

in S is *non-weak* if there exists a variant linked to it (by a path in $\mathcal{L}$) that is a main formula of some logical inference or a distinguished occurrence in some axiom of Π. A formula that is *not* non-weak, is called *weak*.

The following two lemmas will also be used in the proof of the proposition. Their proofs are by induction on the height of Π and we will skip them.

Lemma 2 *Let* $\Pi : \Gamma \rightarrow \Delta, A$ *be a deduction and* A *be a weak occurrence in* Π. *A deduction* $\Pi' : \Gamma \rightarrow \Delta$ *can be constructed such that, if* Π *is acyclic then* Π' *is acyclic.*

Lemma 3 *Let* $\Pi : \Gamma \rightarrow \Delta$ *be a deduction and* Λ, Θ *be multisets. A deduction* $\Pi' : \Gamma, \Lambda \rightarrow \Delta, \Theta$ *can be constructed where* Λ, Θ *are weak occurrences in* Π', *such that if* Π *is acyclic then* Π' *is acyclic.*

Proof. (Proposition 1) Suppose first that Π is a cut-free proof. Then there are only three kinds of edges connecting positive and negative occurrences of formulas in it, as remarked above. Notice that if all occurrences of formulas in a path are positive (negative) then the edges of the path should always go upwards (downwards), and therefore the path cannot be a cycle. Suppose there is a cycle in Π. By the latter observation, both negative and positive occurrences of formulas must occur in it. In particular we should have a way to connect positive occurrences to negative occurrences but there are no such edges in a logical flow graph of a cut-free proof. Therefore a cut-free proof cannot have cycles.

If Π contains cuts and there is a cycle in it then the cycle must pass through a cut-formula, because of our last observation. To show that Π is acyclic, we apply the cut-elimination procedure to Π, to transform it in a cut-free proof Π'. Let $\Pi_1, \ldots, \Pi_k$ be the intermediate proofs obtained applying the procedure of cut elimination, where Π_1 is Π and Π_k is Π'. We will show that the cut-formula in Π_i (to which the procedure is applied) does not have a cycle passing through it, for all $i = 1 \dots k$.

We will consider only two steps of the cut elimination procedure. All others can be handled following the same ideas.

Take Π_i be of the form

$$\cfrac{\begin{array}{cc} \Pi_1' & \Pi_2' \\ \Gamma_1 \rightarrow \Delta_1, A & A, \Gamma_2 \rightarrow \Delta_2 \end{array}}{\begin{array}{c}\Gamma_{1,2} \rightarrow \Delta_{1,2} \\ \vdots \lambda \end{array}}$$

where A in Π_1' is weak, and Π_{i+1} be of the form

$$\begin{array}{c} \Pi_1'' \\ \Gamma_{1,2} \rightarrow \Delta_{1,2} \\ \vdots \lambda \end{array}$$

where Π_1'' is obtained from Π_1' eliminating the weak occurrence A (using Lemma 2) and adding the weak occurrences Γ_2, Δ_2 to the sequent $\Gamma_1 \rightarrow \Delta_1$ (using Lemma 3). Since A is weak, all paths in the logical flow graph of Π_1' arriving at A originate in axioms and therefore there cannot be cycles in Π_i passing through such an occurrence of A.

Let Π_i be of the form

$$\cfrac{\cfrac{\begin{array}{cc} \Pi_1' & \Pi_2' \\ B, \Gamma_1 \rightarrow \Delta_1, A & C, \Gamma_2 \rightarrow \Delta_2 \end{array}}{B \vee C, \Gamma_{1,2} \rightarrow \Delta_{1,2}, A} \quad \begin{array}{c} \Pi_3' \\ A, \Gamma_3 \rightarrow \Delta_3 \end{array}}{\begin{array}{c} B \vee C, \Gamma_{1,2,3} \rightarrow \Delta_{1,2,3} \\ \vdots \lambda \end{array}}$$

and Π_{i+1} be of the form

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1' \\ B, \Gamma_1 \rightarrow \Delta_1, A\end{array} \quad \begin{array}{c}\Pi_3' \\ A, \Gamma_3 \rightarrow \Delta_3\end{array}}{B, \Gamma_{1,3} \rightarrow \Delta_{1,3}} \qquad \begin{array}{c}\Pi_2' \\ C, \Gamma_2 \rightarrow \Delta_2\end{array}}{B \vee C, \Gamma_{1,2,3} \rightarrow \Delta_{1,2,3}}$$
$$\vdots \lambda$$

By induction hypothesis Π_{i+1} does not contain cycles passing through the cut-formula A. Moreover notice that the logical flow graph of Π_{i+1} is essentially the same as the logical flow graph of Π_i; in fact, the only difference concerning the paths passing through A, consists in the extension of such paths with one more occurrence of A in Π_i. Therefore the transformation could not have eliminated cycles. □

The direction of the edges in a logical flow graph can be justified by the usual notion of soundness for axioms and logical rules. For instance, consider the edge connecting the occurrences of a formula A in the upper and lower sequents of a $\neg$: *left* rule

$$\begin{array}{c}\Gamma \rightarrow \Delta, A \\ \neg A, \Gamma \rightarrow \Delta\end{array}$$

and suppose that $A \rightarrow A'$ is a valid sequent. The rule obtained substituting A with A' in the lower sequent (as the direction of the logical edge suggests), i.e.

$$\frac{\Gamma \rightarrow \Delta, A}{\neg A', \Gamma \rightarrow \Delta}$$

is a sound rule. On the other hand

$$\frac{\Gamma \rightarrow \Delta, A'}{\neg A, \Gamma \rightarrow \Delta}$$

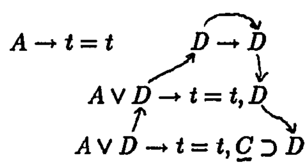
is not sound.

In the following, we focus on the logical relations between *atomic* formulas and we study *when* their presence in the proof is relevant to the validity of the end-sequent. More formally, we will work with the subgraph of a logical flow graph whose nodes are atomic formulas; whenever we refer to s-formulas we will intend them to be atomic.

If one decides not to look at the whole logical flow graph for a proof Π but at subgraphs of it, one may observe that there are subgraphs tracing *proofs* involving only certain occurrences of formulas in Π. We will refer to them as *inner* proofs in Π. Let us illustrate the idea with an example. Consider the following proof

$$\frac{\dfrac{A \rightarrow t = t \quad D \rightarrow D}{A \vee D \rightarrow D, t = t}}{A \vee D \rightarrow t = t, C \supset D}$$

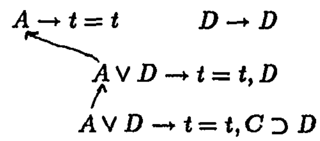
and the portion of the logical flow graph not relying on equality



It is easy to see that it describes the inner proof

$$\frac{D \rightarrow D}{D \rightarrow C \supset D}$$

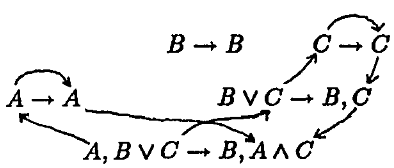
On the other hand, not all subgraphs of Π induce a proof. For instance, consider the subgraph

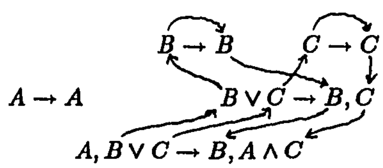


Notice that a given proof may contain more than one inner proof. For instance, consider the following very simple proof

$$\frac{A \to A \qquad \dfrac{B \to B \quad C \to C}{B \vee C \to B, C}}{A, B \vee C \to B, A \wedge C}$$

and the two logical flows for it





describing respectively the inner proofs

$$\frac{A \to A \quad C \to C}{A, C \to A \wedge C} \qquad \text{and} \qquad \frac{B \to B \quad C \to C}{B \vee C \to C, B}.$$

One can notice that in general the antecedent and consequent of the end-sequent of the original proof are not necessarily implied nor do they imply the antecedent and consequent of the end-sequent in the inner proof. For instance, consider the latter example and its logical flow represented on the left. The antecedent of $A, B \vee C \to B, A \wedge C$ does not imply the consequent of $A, C \to A \wedge C$, namely $A, B \vee C \to A \wedge C$ is not a valid sequent. Notice that this observation, brings to light a *sense* in which the informational content of a proof is lost in the logical form of its end-sequent.

The idea of *inner* proof is a basic intuition for what follows. It will be formally defined by means of the notion of *flow* in chapter 3. Properties of logical flow graphs are presented and motivated in chapters 3 and 4. In chapter 3 we will consider them in the context of Peano Arithmetic, while in chapter 4 we will refer to the pure sequent calculus LK.

2.2.1 Validity and Similarity of proofs

The directionality of the edges in a logical flow graph will not usually be relevant to the proofs of the results in this thesis. To illustrate the meaning of the directionality of a flow graph though, we will prove a property of the structure of the proofs for the propositional sequent system LK_P (defined as LK but with no quantifier rules). Under suitable conditions the result can be extended to the system LK.

A statement may have several *similar* proofs and of course, several non-*similar* ones. Also different statements can be proved in a *similar* way. If one wants to generalize the notion of proof, one should look for a notion characterizing *similar* proofs of *similar* conclusions. There are different approaches to this question already in the literature (see [Kre71], [Pra71], [Sza77]) and it seems that a definite mathematical concept capturing the intuition of *similarity* has not been obtained yet. In the following we will consider the notion of *proof-analysis* as a possible approximation of the informal notion of similarity. This concept has been introduced by Parikh in [Par73] and appears in works by the following: Farmer (see [Far84]; he calls this notion a *skeleton*), Krajicek (see [Kra89]; he calls it the *type of proof*), Orevkov (see [Ore84], [Ore87]; he calls it a *schema of proof*). For an overview of results in this area see [Kra87].

A *proof-analysis* is a tree of sequents together with information associated to all nodes of a tree about which inference rule or which axiom schema has been used to derive a given sequent (i.e. the label of the node).

We say that a proof Π and a tree of sequents Π' are *weakly isomorphic* if they have the same proof-analysis and there exists a map f that is a homomorphism on the structure of the formulas (with respect to the structure of the proof), i.e. f is a map from formula occurrences of Π into formulas, and for each logical rule R applied in Π, the main formula of R and its image under f have the same principal connective.

If A, B are premises of a rule in Π and $A \wedge B$ is the main formula then f should map the occurrence of $A \wedge B$ as main formula, into a conjunction of the form $f(A) \wedge f(B)$, where $f(A), f(B)$ may be different from the images under f of the auxiliary occurrences A and B in the premises. Notice that a distinguished occurrence of a formula in an axiom can be mapped by f into an arbitrary formula of the language. We call f a *weak isomorphism*.

One can observe that a proof-analysis can be associated to any tree of sequents; in fact such a tree might be *not* a proof in the conventional sense. We will use this fact to show the following:

Proposition 4 *Let* $\Pi : S$ *be a proof in* LK_P *and* $\Pi' : S'$ *be a tree of sequents weakly isomorphic to* Π *with weak isomorphism* f. *Suppose that for all edges from* A *to* B *of the logical flow graph of* Π, *where either* A *is a positive occurrence of a formula and* B *an s-formula, or* A *is a s-formula and* B *a negative occurrence of a formula, the sequent* $f(A) \rightarrow f(B)$ *is valid. Then* S' *is valid.*

Proof. Take Π be a proof and Π' be a tree of sequents satisfying the conditions of the statement. By induction on the height of Π we show that S' is valid.

Let Π be of the form $A^1, \Gamma \rightarrow \Delta, A^2$ (note that the superscripts indicate the occurrences of A in Π) and Π' be of the form $B, \Gamma' \rightarrow \Delta', C$, where $f(A^1) = B$ and $f(A^2) = C$. Since by hypothesis, $B \rightarrow C$ is valid, then S' is valid.

Let R be the last rule of Π. Suppose R is a $\wedge$:*right* rule applied to the subproofs $\Pi_1 : \Gamma_1 \rightarrow \Delta_1, A$ and $\Pi_2 : \Gamma_2 \rightarrow \Delta_2, B$ to obtain the sequent $\Gamma_{1,2} \rightarrow \Delta_{1,2}, A \wedge B$. The tree of sequents Π' will be of the form

$$\frac{\begin{array}{cc} \Pi'_1 & \Pi'_2 \\ \Gamma_1 \rightarrow \Delta_1, C & \Gamma_2 \rightarrow \Delta_2, D \end{array}}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, E \wedge F}$$

where Π'_1 and Π'_2 are trees of sequents. We know by hypothesis that $C \rightarrow E$ and $D \rightarrow F$ are valid sequents, therefore $\Gamma_1 \rightarrow \Delta_1, E$ and $\Gamma_2 \rightarrow \Delta_2, F$ are valid sequents, and in particular S' is a valid sequent (this is because $f(A \wedge B)$ is $f(A) \wedge f(B)$, i.e. $E \wedge F$.)

All other rules are treated in a similar way. □

The proposition points out that to claim a sequent to be valid, all we need is to exhibit a proof-analysis and suitable valid sequents so that a tree structure weakly isomorphic to a proof can be built.

Chapter 3

No Speed-up for Non-Standard Theories

3.1 Introduction

It appears already in philosophical works by Mannoury ([Man09]), Poincaré ([Poi13]) and Wittgenstein ([Wit78]) that there is a genuine difference between our understanding of say the number 10 and the number $67^{257^{729}}$.

In [Ber35], Bernays observes that intuitionism as well as ordinary mathematics contains a strong idealization in the facts that numbers such as 10 and $67^{257^{729}}$ are treated as objects of the same kind, even though arithmetical operations do not have a *concrete* meaning for very large numbers. He suggests strict-finitism as a conceivable position in philosophy of mathematics.[1]

[1] Strict-finitist philosophy of mathematics insists that the meanings of all terms appearing in mathematical

In [EV61], Esenin-Volpin declares his adherence to strict-finitism and starts some attempts in the reconstruction of mathematics along the new lines (see also [EV70]). He refuses the conception that natural numbers are closed under simple arithmetical operations, such as exponentiation and develops a rich and complicated theory of 'concrete' mathematical activity (leading for instance, as he claims, to a 'concrete' proof of the consistency of Zermelo-Fraenkel set theory). He introduces the concept of a set of *feasible* numbers closed under successor but bounded by a given natural number, say 10^{12}. The notion he introduces appears to be paradoxical and indeed it is an abstract form of the classical paradoxes of the bald man (adding one hair at a time can never turn a bald man into a non-bald man) and the heap (by removing a single grain at a time you will still have a heap).

The first precise proof-theoretical result about the 'concrete' correctness of the notion of feasible numbers was given by Parikh ([Par71]) that proves the 'concrete' consistency of the theory defined adding to Peano Arithmetic the above mentioned properties of feasible numbers. This result has been refined by Gavrilenko (unpublished work) and Dragalin ([Dra85]). In the present paper we will give a more natural statement of Parikh's result and we will show optimal complexity bounds improving the work by Dragalin.

statements must be given in relation to *constructions* which we can effectively carry out, and of our capacity to recognize *in practice* such constructions as providing proofs of those statements. No construction that is too complex or too lengthy to effect in practice, is accepted by strict-finitism. In addition to the one discussed in this introduction, several attempts to develop a formal strict-finitist theory have been made. The most developed is the *Alternative Set Theory* by Vopenka ([Vop79]) and his school in Prague. See also [Saz90], the *Predicative Arithmetic* by Nelson ([Nel86]) and the theory of *Vague Predicates* by Dummett ([Dum78b], [Dum78a]) and Parikh ([Par83]). For a general discussion on the strict-finitist program see [Gan82] and for its relations with intuitionism see [Tro90].

The theory of feasible numbers seems to be useful for constructive investigations in non-standard model theory. In the last section we consider a consistent theory asserting the *existence* of a non-feasible number and we present a proof-theoretical argument showing that such a theory not only is a conservative extension of Peano Arithmetic, but in fact has no speed-up over it. The proof points out the correspondence between the number of formulas in a proof and the existence of non-standard numbers in models of arithmetic.

3.2 The theory of feasible numbers

In this section we will work with Peano Arithmetic, denoted PA. Actually, the following results hold for arbitrary theories (including the Predicate Calculus). This is because no assumption is needed on the strength of the theory[2].

To the language of PA (defined by the symbols $0, s, +, *, <, =$) add the symbol F and to PA add the axioms[3]

(i) $F(0)$

(ii) $F(x) \rightarrow F(s(x))$

(iii) $F(x) \wedge F(y) \rightarrow F(x+y)$

(iv) $F(x) \wedge F(y) \rightarrow F(x*y)$

(v) $x = y \rightarrow (F(x) \rightarrow F(y))$

[2]Note that both Parikh and Dragalin's results need a theory to contain a rather modest portion of PA. Namely, it is sufficient that the theory be strong enough to prove or refute any closed numerical equality or inequality.

[3]Note that with the symbol PA we indicate the Hilbert style formalization of Peano Arithmetic, where tautologies are axioms. In particular, observe that axiom (iii) can be derived from (iv),(vi) and the axioms of PA; axiom (v) can be derived from (ii) and (vi).

(vi) $F(x) \wedge y < x \rightarrow F(y)$

(vii) $\neg F(\theta)$

where θ is some fixed variable-free term in the language of PA. The value of θ will be indicated as $val(\theta)$. Call this theory PA_F. Any formula containing the symbol F will be called an *F-formula* and a formula not containing any occurrence of F will be referred to as *F-free*.

The theory PA_F is clearly inconsistent (because of the presence of axiom (vii)) but we will show that proofs with a "small" number of formulas cannot prove inconsistency. In fact, such proofs can only establish truths in the original language of PA.

Let a proof be a *tree* of formulas (i.e. each occurrence of a formula in the proof can be used at most once as premise of a rule) and let $N(\Pi)$ denote the number of all formulas in the PA_F-proof Π. Our main result can be formulated as follows

Theorem 5 *Let Π be a proof in PA_F of the closed formula B. The formula B does not contain F. Suppose that the number of axioms of the form (ii) – (iv) occurring in Π is n and that $val(\theta) > 2^n$. Then there is a proof $\Pi' : B$ in PA such that $N(\Pi') \leq N(\Pi)$.*

The lower bound 2^n depends on the fact that proofs are considered in their tree-like form. If proofs are linear (i.e. if a formula can be used more than once in the proof) then the theorem holds with 2^{2^n} as a lower bound for $val(\theta)$.

A lower bound on the value $val(\theta)$ of the term θ (relative to the theory PA_F) is computed by Parikh using the Hilbert-Ackermann's ϵ-substitution method and by Dragalin using a cut-elimination technique. Both proofs give a primitive recursive lower bound for $val(\theta)$

but much higher than 2^n. If we define the function $exp_t(n,0) = n$, $exp_t(n, i+1) = t^{exp_t(n,i)}$ (for some natural number $t > 1$) then

- Parikh's bound can be expressed as $val(\theta) > exp_2(1, exp_2(r, \frac{1}{2} \cdot k \cdot (k+1)) \cdot n)$, where k is the number of axioms of the form $A(t) \supset \exists x A(x)$ occurring in the proof and such that A contains the F symbol, r is the number of quantifiers occurring in formulas A of the form described above and n is the number of occurrences of the special axioms of the form *(ii)-(iv)* in Π;[4]

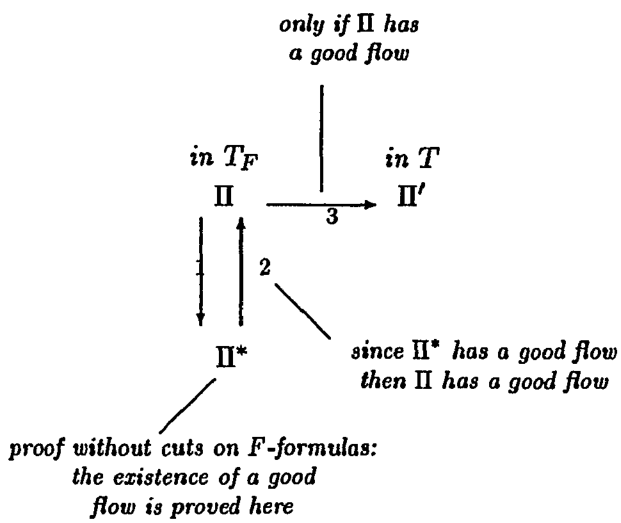
- Dragalin's bound is expressed as $val(\theta) > exp_2(1, exp_4(39 \cdot N(\Pi), 39 \cdot N(\Pi)))$.

As one can see, Parikh's bound depends on the complexity of F-formulas in the deduction Π and on the number of some special axioms in it, while Dragalin's bound depends essentially only on the number of formulas in Π. Our result improves both bounds and is sensitive only to the number of occurrences of special axioms in the proof. It can be shown that it is the best possible bound (namely, for all $\alpha < 1$, we show that 2^{n^α} is not a bound.)

Moreover, both Parikh and Dragalin claim the existence of a proof in PA of the F-free formula B but their construction produces a proof of very large complexity. Our result, instead, ensures that one can construct a PA-proof with smaller or equal complexity than the original proof Π. In addition, the complexity of the formulas (intended as number of symbols) occurring in the PA-proof turns out to be no greater than the complexity of the formulas in Π.

[4]For the theory of feasible numbers defined as PA_F but not containing the axioms (iii) and (iv), Parikh improves the lower bound to $val(\theta) > n \cdot exp_2(r, \frac{1}{2} \cdot k \cdot (k+1))$, while Dragalin obtains $exp_2(1, exp_4(30 \cdot N(\Pi), 30 \cdot N(\Pi)))$. Our Theorem 25 refines these results to $val(\theta) > n$.

In section 3.3 below we introduce the *sequent theory* of feasible numbers T_F associated to PA_F (we call T the part of T_F associated to PA); in section 3.4 we review Buss' notion of logical flow graph and define the notion of "good flow" of formulas in a T_F-proof; in section 3.5, a number of properties of good flows of formulas in T_F-proofs are studied. Among them we show that if a T_F-proof Π^* is obtained applying a cut elimination procedure to all F-formulas in a proof Π, then whenever Π^* has a good flow of formulas then Π must have a good flow as well; moreover, we give general conditions on the existence of a good flow for T_F-proofs containing only cuts on F-free formulas. In section 3.6, we show that a T_F-proof Π can be transformed into a suitable F-free proof Π' of the same complexity (i.e. number of sequents), whenever Π has a flow. This suffices to show the version of our Theorem 5 for the sequent theory T_F. The idea of the proof can roughly be represented by the following diagram (where the arrows represent transformations of proofs and the numbering represents the order of performance of the transformations)



In section 3.7 we convert this result (formalized for T_F) to the original theory PA_F.

Finally we consider the consistent theory of feasible numbers asserting the *existence* of some non-feasible number, we show it is a conservative extension of PA and that there is no speed-up by this theory over PA. In section 3.8 we consider different directions in which Theorem 5 can be generalized.

3.3 The sequent theory of feasible numbers T_F

We will work with a theory of sequents T_F (resp. T) associated to PA_F (resp. PA) and we will "translate" afterwards the results into PA_F. In this theory, the special axioms will be replaced by special rules: *F-successor*, *F-plus*, *F-times*, and so on.

Let $N(\Pi)$ denote the number of all sequents in the T_F-proof Π. We will prove the following

Theorem 6 *Let Π be a proof in T_F of the closed formula B. The formula B does not contain F. Suppose that the number of special rules F-successor, F-plus and F-times applied in Π is n and that $val(\theta) > 2^n$. Then there is a proof $\Pi' : B$ in T such that $N(\Pi') \leq N(\Pi)$.*

As already remarked for Theorem 5, note that a proof in T_F is a tree of sequents (see section 2.1) and, the lower bound 2^n in our theorem depends on the fact that proofs are considered in their tree-like form. If proofs are linear, then the theorem still holds, but with 2^{2^n} as a lower bound for $val(\theta)$. In this case also, the bound turns out to be the best possible.

The axioms and the rules of inference for our sequent theory T_F are formalized (without loss of generality) for the logical connectives $\neg, \vee, \exists$. The full predicate calculus is obtained by taking the other connectives as being defined in terms of $\neg, \vee, \exists$. The theory PA_F can clearly be formalized in terms of this restricted set of logical connectives together with the non-logical symbols $0, s, +, *, =, <, F$. There are four kind of axioms

(i) logical axioms of the form $A, \Gamma \rightarrow \Delta, A$ (note that A may be an F-formula);

(ii) equality axioms of the form

- $\Gamma \rightarrow \Delta, t = t$;
- $t_1 = s_1, \ldots, t_k = s_k, P(t_1, \ldots, t_k), \Gamma \rightarrow \Delta, P(s_1, \ldots, s_k)$ where P is a k-ary predicate symbol (distinct from F);
- $t_1 = s_1, \ldots, t_k = s_k, \Gamma \rightarrow \Delta, f(t_1, \ldots, t_k) = f(s_1, \ldots, s_k)$ where f is a k-ary function symbol.

(iii) PA-axioms of the form $\Gamma \rightarrow \Delta, A$, where A is an arbitrary non-logical axiom of PA (note that the formula A is F-free);

(iv) a *special axiom* of the form $\Gamma \rightarrow \Delta, F(0)$.

The rules of inference are divided into three groups: the *logical rules* and *structural rules* (as in section 2.1), and the *special rules* concerning the predicate F.

The *special rules* are

$$F - equality \qquad \frac{\Gamma_1 \rightarrow \Delta_1, r = t \quad \Gamma_2 \rightarrow \Delta_2, F(r)}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t)}$$

$$F - inequality \qquad \frac{\Gamma_1 \rightarrow \Delta_1, t < r \quad \Gamma_2 \rightarrow \Delta_2, F(r)}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t)}$$

$$F - successor \qquad \frac{\Gamma \rightarrow \Delta, F(t)}{\Gamma \rightarrow \Delta, F(s(t))}$$

$$F - plus \qquad \frac{\Gamma_1 \rightarrow \Delta_1, F(r) \quad \Gamma_2 \rightarrow \Delta_2, F(t)}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(r+t)}$$

$$F - times \qquad \frac{\Gamma_1 \rightarrow \Delta_1, F(r) \quad \Gamma_2 \rightarrow \Delta_2, F(t)}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(r*t)}$$

$$F - elimination \qquad \frac{\Gamma \rightarrow \Delta, F(\theta)}{\Gamma \rightarrow \Delta}$$

The F – *elimination* rule is also called the *critical rule* because of the special role it plays in the theory (i.e. it makes the theory inconsistent).

The part of T_F (corresponding to PA) which does not refer to F will be denoted just T.

3.4 Logical flow graphs for T_F

In the following we will use the definition of logical flow graph given in section 2.2. Since the calculus T_F is an extension of the sequent calculus of section 2.1, we need to extend the definition of logical flow graph as well.

First, in a PA-axiom as well as in the special axiom, there are no edges that are defined. Second, in any special rule there is an edge directed from each auxiliary F-formula in the upper sequent(s) to the main F-formula in the lower sequent. There is no outgoing edge from the equality and inequality auxiliary formulas in the upper sequent of F-*equality* and F-*inequality*, respectively.

This concludes the definition of logical flow graph for T_F-proofs. As we have already observed in section 2.2, we will focus on the logical relations between *atomic* formulas occurring in a proof, therefore whenever we refer to s-formulas we will intend them to be atomic.

We now define the noton of *full path.*

Definition 7 Let Π be a proof in T_F, $\mathcal{L}$ its logical flow graph, and f be a sequence of edges in $\mathcal{L}$ between s-formulas that are *not* F-atomic; let C_1 be the formula of f with no incoming edges (belonging to f) and C_2 be the one with no outcoming edges (belonging to f); f may be empty in which case C_1 is C_2. The sequence f is called a *full path* if

a. for each $i = 1, 2$ one of the following conditions is satisfied

1. C_i occurs in the endsequent of Π;
2. C_i is an s-formula occurring in some non-distinguished formula of the axioms of Π (i.e. in the cedents Γ, Δ);
3. C_i is an s-formula occurring in A of a PA-axiom $\Gamma \rightarrow \Delta, A$;
4. C_i is an equation (inequality) and occurs as an auxiliary formula in the *F-equality* (*F-inequality*) rule;
5. C_i is an s-formula occurring in B of the main formula $A \vee B$ or $B \vee A$ in a $\vee$:*right* application in Π;

b. the formula C_1 (C_2) does not have incoming (outgoing) edges in $\mathcal{L}$.

Notice that the formula C_i in $a.2, a.5$ does not give any logical contribution to the proof, in the sense that the validity of the sequent in which C_i appears, resides on the logical relations concerning formulas other than C_i.

F-free atomic formulas that are nodes of a path are called *active* formulas in the path. More generally we say that a formula (not necessarily atomic) is active in a set of paths whenever some (possibly all) of its F-free s-formulas are active.

Definition 8 Let $\Pi : S$ be a proof and $\mathcal{F}$ be a set of paths in Π. The 'forgetful' map $H_{\mathcal{F}}$ from occurrences of formulas in Π to formulas (possibly none) is defined as follows

1. if A is an atomic formula then $H_{\mathcal{F}}(A) = \begin{cases} A & \textit{if } A \textit{ is active in } \mathcal{F} \\ \emptyset & \textit{otherwise} \end{cases}$

2. $H_{\mathcal{F}}(\neg A) = \begin{cases} \neg H_{\mathcal{F}}(A) & \textit{if } H_{\mathcal{F}}(A) \neq \emptyset \\ \emptyset & \textit{otherwise} \end{cases}$

3. $H_{\mathcal{F}}(A \vee B) = \begin{cases} H_{\mathcal{F}}(A) \vee H_{\mathcal{F}}(B) & \textit{if } H_{\mathcal{F}}(A), H_{\mathcal{F}}(B) \neq \emptyset \\ H_{\mathcal{F}}(A) & \textit{if } H_{\mathcal{F}}(B) = \emptyset \\ H_{\mathcal{F}}(B) & \textit{if } H_{\mathcal{F}}(A) = \emptyset \\ \emptyset & \textit{if } H_{\mathcal{F}}(A), H_{\mathcal{F}}(B) = \emptyset \end{cases}$

4. $H_{\mathcal{F}}((\exists x)A(x)) = \begin{cases} (\exists x)H_{\mathcal{F}}(A(x)) & \textit{if } H_{\mathcal{F}}(A(x)) \neq \emptyset \\ \emptyset & \textit{otherwise} \end{cases}$

Let A be a formula. The formula $H_{\mathcal{F}}(A)$ when defined, is not necessarily a subformula of A. On the other hand, not all subformulas of A can be images of some forgetful map $H_{\mathcal{F}}$. Take for instance A to be $(\exists x)(P(x) \vee Q(x))$; the subformula $P(x)$ cannot be the image of any forgetful map and the formula $(\exists x)Q(x)$ is not a subformula of A but it can be obtained from A by forgetting $P(x)$. Because of these properties, we will call $H(A)$ an *inner formula of* A.

Let Γ be a multiset of formulas $A_1 \dots A_n$; with the symbol $H(\Gamma)$ we denote the multiset $H(A_1) \dots H(A_n)$. If Γ, Δ are two multisets of formulas then $H(\Gamma \rightarrow \Delta)$ denotes the sequent $H(\Gamma) \rightarrow H(\Delta)$ where $H(\Gamma), H(\Delta)$ are multisets. We will call $H(\Gamma \rightarrow \Delta)$ an *inner sequent of* $H(\Gamma \rightarrow \Delta)$.

Notice that the map $H_{\mathcal{F}}$ is $\mathcal{F}$-dependent (whenever confusion cannot arise, we will denote the map $H_{\mathcal{F}}$ with the symbol H). In particular, observe that each image of a formula in Π under H is a F-free formula (this follows from the definition of active formulas), when defined.

For any two sets of paths $\mathcal{F}_1, \mathcal{F}_2$ let $H_{\mathcal{F}_1} \preceq H_{\mathcal{F}_2}$ if $H_{\mathcal{F}_1}(A) = \emptyset$ whenever $H_{\mathcal{F}_2}(A) = \emptyset$. Then define the map G to be the maximal forgetful map with respect to the order $\preceq$. Namely, the map G will forget all F-atomic occurrences in a formula and only those. Notice that the map G is $\mathcal{F}$-independent.

Definition 9 Let $\Pi : S$ be a proof of height greater than 1 with last rule R. Let R be either a binary rule applied to $\Pi_1 : S_1$, $\Pi_2 : S_2$ or a unary rule applied to $\Pi_1 : S_1$.

1. Let f be a path in Π_i with an active s-formula C occurring positively (negatively) in S_i (where i is either 1 or 2 in case R is binary, and 1 in case R is unary). If R is a binary logical rule or R is a unary rule or C occurs in some side formula of a cut rule, then a path f' in Π is the ***natural extension*** of f if it is defined by extending f with the outgoing (incoming) edge from (to) C to (from) the variant C' in S (in the sense of the logical flow graph);

2. let R be a cut rule, f_1 be a path in Π_1 with active subformula C occurring positively

(negatively) in the cut-formula A of S_1, f_2 be a path in Π_2 with the same active subformula C of A occurring negatively (positively) in the cut-formula of S_2. Then, a path f' in Π is the ***natural extension*** of f_1, f_2 if it is defined by connecting f_1, f_2 with the outgoing (incoming) edge from (to) C in Π_1 to (from) C in Π_2 (in the sense of the logical flow graph).

The following definition describes sets of paths we will work with in the next section. They will be called *flows* and they will be used to bring out the intuition of *inner* proof. The definition is split in two cases. First we consider a proof Π to be an axiom, second we examine the last rule of inference in Π and define the flow with respect to flows existing for immediate subproof(s) of it.

Definition 10 Let $\Pi : S$ be a proof in T_F with last rule R (if any).

1 Suppose Π is an axiom; the set of paths $\mathcal{F}$ for Π is called a *flow* if it is a set of full paths and the following conditions are satisfied

1. if Π has the form $A, \Gamma \rightarrow \Delta, A$, then $\mathcal{F}$ contains at least an edge linking two variants in the distinguished occurrences of A (i.e. $H_{\mathcal{F}}(A)$ is not empty), and
2. if Π is a PA-axiom $\Gamma \rightarrow \Delta, A$, then A is active in $\mathcal{F}_1$ and $H_{\mathcal{F}_1}(A) = A$, and
3. if Π is an equality axiom then all its distinguished formulas are active in $\mathcal{F}_1$.

2.a Suppose R is a $\vee$-*left*, or *F-plus* or *F-times* applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$ of Π. A set of paths $\mathcal{F}$ for Π is called a *flow* if the following conditions are satisfied

1. there exist flows $\mathcal{F}_1, \mathcal{F}_2$ such that the auxiliary formulas in S_1, S_2 are both active, and exactly the natural extensions of paths in $\mathcal{F}_1$, $\mathcal{F}_2$ are in $\mathcal{F}$, or

2. there exists a flow $\mathcal{F}_1$ such that all natural extensions of paths in $\mathcal{F}_1$ are in $\mathcal{F}$ and any other (possibly none) path in $\mathcal{F}$ is a F-free s-formula of S with a logical edge to/from some side formula in S_2. Similarly for Π_2.

2.b Suppose R is a *cut* rule applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$ of Π. A set of paths $\mathcal{F}$ for Π is called a *flow* if

1. there exist flows $\mathcal{F}_1, \mathcal{F}_2$ for Π_1, Π_2 such that $H_{\mathcal{F}_1}(A)$ and $H_{\mathcal{F}_2}(A)$ are the same non-empty inner formulas and $\mathcal{F}$ is exactly the set of natural extensions of paths in $\mathcal{F}_1, \mathcal{F}_2$, or

2. there exists a flow $\mathcal{F}_1$ for Π_1 where $H_{\mathcal{F}_1}(A)$ is empty, the flow $\mathcal{F}$ is the natural extension of $\mathcal{F}_1$ and any other (possibly none) path in $\mathcal{F}$ is a F-free s-formula of S with a logical edge to/from some side formula in S_2. Similarly for Π_2.

2.c Suppose R is a *F-equality* or *F-inequality* applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$ of Π. A set of paths $\mathcal{F}$ for Π is called a *flow* if

1. there exists a flow $\mathcal{F}_2$ for Π_2 such that all natural extensions of paths in $\mathcal{F}_2$ are in $\mathcal{F}$ and any other (possibly none) path in $\mathcal{F}$ is a F-free s-formula of S with a logical edge to/from some side formula in S_1, or

2. there exists a flow $\mathcal{F}_1$ for Π_1 with non-active auxiliary formula, such that all natural extensions of paths in $\mathcal{F}_1$ are in $\mathcal{F}$ and any other (possibly none) path in $\mathcal{F}$ is a F-free s-formula of S with a logical edge to/from some side formula in

S_2.

2.d Suppose R is a *unary* rule applied to the subproof $\Pi_1 : S_1$ of Π. A set of paths $\mathcal{F}$ for Π is called a *flow* if there exists a flow $\mathcal{F}_1$ for Π_1 such that all the natural extensions of paths in $\mathcal{F}_1$ are in $\mathcal{F}$ and in case R is $\vee$:*right* applied to a sequent $\Gamma \rightarrow \Delta, A$ to obtain $\Gamma \rightarrow \Delta, A \vee B$ or $\Gamma \rightarrow \Delta, B \vee A$, any other path in $\mathcal{F}$ is a F-free s-formula in B.

2.e Suppose R is a *contraction* rule applied to $\Pi_1 : S_1$. A set of paths $\mathcal{F}$ is called a *flow* if there exists a flow $\mathcal{F}_1$ for Π_1 such that the following conditions are satisfied

1. both images of contracting formulas in Π_1 are the same under $H_{\mathcal{F}_1}$, and
2. exactly all natural extensions of paths in $\mathcal{F}_1$ are in $\mathcal{F}$.

This concludes the definition of *flow*. Notice that a flow $\mathcal{F}$ on Π with a binary rule R as last rule of inference, is sometimes passing only through one of the immediate subproofs of Π. Moreover, notice that the images under $H_{\mathcal{F}}$ of the auxiliary formulas for R being a cut rule or a contraction rule, are the same, whenever not empty.

The flow $\mathcal{F}$ obtained from $\mathcal{F}_1, \mathcal{F}_2$ (possibly only $\mathcal{F}_1$) is also referred to as *natural extension* of $\mathcal{F}_1, \mathcal{F}_2$.

Proposition 11 *Let $\Pi : S$ be a proof in T_F and $\mathcal{F}$ a flow for Π. Then there exists a proof Π' in T of $H_{\mathcal{F}}(S)$ such that $N(\Pi') \leq N(\Pi)$.*

To show this proposition we need a lemma on the structure of proofs. We will state it here but prove it in section 3.5 together with other results of the same nature. Its proof is of independent interest and not linked to this particular application.

Lemma 12 (Addition of weak occurrences) *Let* $\Pi : \Gamma \rightarrow \Delta$ *be a deduction and* Λ, Θ *be multisets. A deduction* $\Pi' : \Gamma, \Lambda \rightarrow \Delta, \Theta$ *can be constructed such that* $N(\Pi') = N(\Pi)$ *and if* Π' *has a flow* $\mathcal{F}'$ *then there exists a flow* $\mathcal{F}$ *for* Π *with base* $H_{\mathcal{F}}(\Gamma \rightarrow \Delta) = H_{\mathcal{F}'}(\Gamma \rightarrow \Delta)$.

Proof. (Proposition 11) By induction on the height of Π.

$h(\Pi) = 1$: the proof Π must be an axiom of one of the following forms:

- $A, \Gamma \rightarrow \Delta, A$: if $\mathcal{F}$ exists then $H(A) \neq \emptyset$. Since $H(A), H(\Gamma) \rightarrow H(\Delta), H(A)$ is an axiom then let Π' be $H(A), H(\Gamma) \rightarrow H(\Delta), H(A)$;

- an equality axiom or a PA-axiom: in this case the image under H of the axiom is an axiom as well. Define Π' to be this image;

- $\Gamma \rightarrow \Delta, F(0)$: a flow $\mathcal{F}$ cannot exist. Hence Proposition 11 holds vacuously.

$h(\Pi) = k + 1$: assume that $\mathcal{F}$ is a flow for Π; we can proceed by inspecting the form of the last rule of inference R.

- $\neg$: *left*: let Π be of the form

$$\frac{\begin{array}{c}\Pi_1 \\ \Gamma_1 \rightarrow \Delta_1, A\end{array}}{\neg A, \Gamma_1 \rightarrow \Delta_1}$$

  Apply the induction hypothesis to Π_1 and obtain Π'_1 such that $N(\Pi'_1) \leq N(\Pi_1)$. If A is active in $\mathcal{F}$ then apply to Π'_1 a $\neg$: *left*; if not, notice that $H_{\mathcal{F}}(S_1)$ is $H_{\mathcal{F}}(S)$ and therefore Π' can be taken to be Π'_1. Clearly $N(\Pi') \leq N(\Pi)$.

  The $\neg$: *right*, $\exists$:*left*, $\exists$:*right* cases are handled similarly.

- $\vee$: *left*: let Π be of the form

$$\frac{\begin{matrix}\Pi_1 & \Pi_2 \\ A, \Gamma_1 \rightarrow \Delta_1 & B, \Gamma_2 \rightarrow \Delta_2\end{matrix}}{A \vee B, \Gamma_{1,2} \rightarrow \Delta_{1,2}}$$

If $\mathcal{F}$ is defined in both Π_1 and Π_2 then A and B are both active and the induction hypothesis can be applied to Π_1, Π_2 to find proofs Π'_1, Π'_2 to combine with a $\vee$: *left* and obtain Π'. Clearly $N(\Pi') = N(\Pi'_1) + N(\Pi'_2) + 1 \leq N(\Pi_1) + N(\Pi_2) + 1 = N(\Pi)$. If $\mathcal{F}$ is defined only in Π_1 (respectively in Π_2) then apply the induction hypothesis to it to obtain Π'_1 and Lemma 12 to add all weak occurrences $H_{\mathcal{F}}(C)$ for C in Γ_2, Δ_2 (respectively Γ_1, Δ_1). Call the resulting proof Π'. Clearly $N(\Pi'_1) \leq N(\Pi_1)$ and by Lemma 12 $N(\Pi') \leq N(\Pi'_1) \leq N(\Pi)$.

- $\vee$:*right*: let Π be of the form

$$\frac{\begin{matrix}\Pi_1 \\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix}}{\Gamma_1 \rightarrow \Delta_1, A \vee B}$$

If A and B are active in $\mathcal{F}$ then apply the induction hypothesis to Π_1 to obtain Π'_1 and the $\vee$:*right* to $H_{\mathcal{F}}(B)$. In case A is active and B is not, let Π'_1 be the result of the induction hypothesis applied to Π_1. In case A is not active but B is then apply Lemma 12 to Π'_1 (obtained by induction hypothesis) to add the weak occurrence $H_{\mathcal{F}}(B)$. Clearly $N(\Pi'_1) \leq N(\Pi_1)$ and therefore $N(\Pi') \leq N(\Pi)$.

The *contraction* rule is handled similarly.

- *cut*: let Π be of the form

$$\frac{\begin{matrix}\Pi_1 & \Pi_2\\ \Gamma_1 \to \Delta_1, A & A, \Gamma_2 \to \Delta_2\end{matrix}}{\Gamma_{1,2} \to \Delta_{1,2}}$$

If the cut formulas are active in $\mathcal{F}$ then apply the induction hypothesis to Π_1, Π_2 to obtain the sequents $H_{\mathcal{F}}(\Gamma_1) \to H_{\mathcal{F}}(\Delta_1), H_{\mathcal{F}}(A)$ and $H_{\mathcal{F}}(A), H_{\mathcal{F}}(\Gamma_2) \to H_{\mathcal{F}}(\Delta_2)$, where both distinguished occurrences of $H_{\mathcal{F}}(A)$ are the same inner formula of A. Then apply a cut rule to these sequents.

If $\mathcal{F}$ is active in Π_1 (or similarly Π_2) but not in the cut formula A of $\Gamma_1 \to \Delta_1, A$ (respectively, $A, \Gamma_1 \to \Delta_1$), we can apply the induction hypothesis to obtain Π_1' and Lemma 12 to add the weak occurrences $H_{\mathcal{F}}(B)$ for B in Γ_2, Δ_2 (respectively Γ_1, Δ_1).

- *F-plus*: let Π be of the form

$$\frac{\begin{matrix}\Pi_1 & \Pi_2\\ \Gamma \to \Delta, F(s) & \Gamma \to \Delta, F(t)\end{matrix}}{\Gamma \to \Delta, F(s+t)}$$

The flow $\mathcal{F}$ must be the natural extension of a flow in Π_1 or Π_2; say Π_1. Apply the induction hypothesis to Π_1 and obtain Π_1'; let Π' be Π_1'. Clearly $N(\Pi') \leq N(\Pi)$.

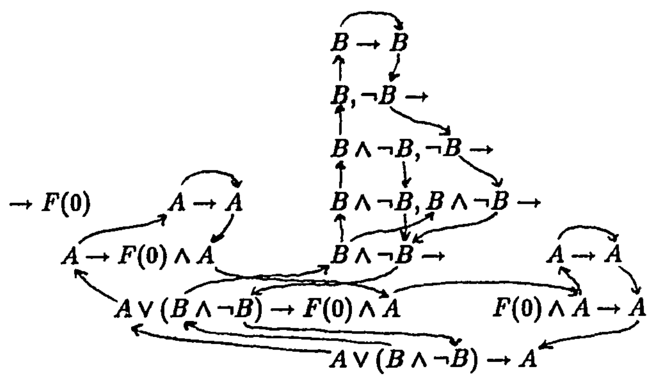
The other F-rules are handled similarly.

□

The definition of *flow* of formulas in a T_F-proof together with Proposition 11 will play a crucial role in the following. We illustrate this intuition with an example. Consider the following T_F-proof

$$\dfrac{\dfrac{\dfrac{\rightarrow F(0) \quad A \rightarrow A}{A \rightarrow F(0) \wedge A} \quad \dfrac{\dfrac{\dfrac{\dfrac{B \rightarrow B}{B, \neg B \rightarrow}}{B \wedge \neg B, \neg B \rightarrow}}{B \wedge \neg B, B \wedge \neg B \rightarrow}}{B \wedge \neg B \rightarrow}}{A \vee (B \wedge \neg B) \rightarrow F(0) \wedge A} \qquad \dfrac{A \rightarrow A}{F(0) \wedge A \rightarrow A}}{A \vee (B \wedge \neg B) \rightarrow A}$$

and the flow



generating the *inner* proof

$$\dfrac{\dfrac{A \rightarrow A \quad \dfrac{\dfrac{\dfrac{\dfrac{B \rightarrow B}{B, \neg B \rightarrow}}{B \wedge \neg B, \neg B \rightarrow}}{B \wedge \neg B, B \wedge \neg B \rightarrow}}{B \wedge \neg B \rightarrow}}{A \vee (B \wedge \neg B) \rightarrow A} \qquad A \rightarrow A}{A \vee (B \wedge \neg B) \rightarrow A}$$

Notice that this latter proof does not contain the symbol F. Given a short T_F-proof of a F-free sequent we will look for a suitable flow to prove the existence of a T-proof for that sequent.

Before concluding this section, let us give two more definitions regarding flows.

Definition 13 Let $\Pi : \Gamma \to \Delta$ be a T_F-proof. A flow $\mathcal{F}$ for Π is *good* if for all axioms S in Π, if $H(S)$ is not empty then $H(A)$ is $G(A)$ for all distinguished occurrences A in S.

For instance, consider the sequent $C \vee (\neg B \wedge F(t)), \Gamma \to \Delta, C \vee (\neg B \wedge F(t))$ where A is $C \vee (\neg B \wedge F(t))$ and $G(A)$ is $C \vee \neg B$. The flow

$$C \vee (\neg B \wedge F(t)), \Gamma \to \Delta, C \vee (\neg B \wedge F(t))$$

is good since $H(A)$ has the form $C \vee \neg B$, while

$$C \vee (\neg B \wedge F(t)), \Gamma \to \Delta, C \vee (\neg B \wedge F(t))$$

is not because $H(A)$ is C.

Intuitively a *good* flow is a flow where all logical axioms are either completely active (i.e. all F-free s-formulas of their distinguished occurrences are active) or completely non-active (i.e. there is no path in the flow passing through the axiom). Remember that special axiom's are completely non-active because the distinguished occurrence is a F-formula, and PA-axioms are either completely active or completely non-active by definition of flow.

Given two flows one can define the ***union*** of them. The notion of union will be used in subsection 3.5 to prove Lemma 21.

Definition 14 Given two flows $\mathcal{F}_1, \mathcal{F}_2$ for a proof $\Pi : S$, the *union* $\mathcal{F}_1 \sqcup \mathcal{F}_2$ is defined by induction on the height of Π as follows.

Suppose Π is an axiom, then $\mathcal{F}_1 \sqcup \mathcal{F}_2$ is the flow where an s-formula A is active if and only if it is active in $\mathcal{F}_1$ or $\mathcal{F}_2$.

Suppose the last rule of inference R in Π is a $\vee$-*left*, or *F-plus* or *F-times* applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$; let $\mathcal{F}_{1,1}, \mathcal{F}_{1,2}, \mathcal{F}_{2,1}, \mathcal{F}_{2,2}$ be the flows associated to Π_1, Π_2.

1. if both auxiliary formulas in S_1, S_2 are active, exactly the natural extensions of paths in $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$ and $\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}$ are in $\mathcal{F}_1 \sqcup \mathcal{F}_2$;
2. if the auxiliary formula in S_1 (respectively, S_2) is not active and $\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}$ (respectively, $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$) is not empty, all natural extensions of paths in $\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}$ (respectively, $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$) are in $\mathcal{F}_1 \sqcup \mathcal{F}_2$; and any formula of S with a logical edge to some side-formula active in S_1 (respectively, S_2) is forced to be active in $\mathcal{F}_1 \sqcup \mathcal{F}_2$.

Suppose R is a *cut* rule applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$ of $\Pi : S$; let $\mathcal{F}_{1,1}, \mathcal{F}_{1,2}, \mathcal{F}_{2,1}, \mathcal{F}_{2,2}$ be the flows associated to Π_1, Π_2.

1. If $H_{\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}}(A)$ is not empty (notice that $H_{\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}}(A)$ is $H_{\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}}(A)$) then let $\mathcal{F}_1 \sqcup \mathcal{F}_2$ be the natural extension of $H_{\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}}(A)$ and $H_{\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}}(A)$;
2. if $H_{\mathcal{F}_{1,i} \sqcup \mathcal{F}_{2,i}}(A)$ (for some $i = 1, 2$) is empty then all natural extensions of paths in $H_{\mathcal{F}_{1,i} \sqcup \mathcal{F}_{2,i}}(A)$ are in $\mathcal{F}_1 \sqcup \mathcal{F}_2$; any other formula of S with a logical edge to some formula active in S_j (for $j \neq i$ and $j = 1, 2$) is forced to be active in $\mathcal{F}_1 \sqcup \mathcal{F}_2$.

Suppose R is a *F-equality* or *F-inequality* applied to the subproofs $\Pi_1 : S_1$ and $\Pi_2 : S_2$ of Π; let $\mathcal{F}_{1,1}, \mathcal{F}_{1,2}, \mathcal{F}_{2,1}, \mathcal{F}_{2,2}$ be the flows associated to Π_1, Π_2.

1. If $\mathcal{F}_{1,2} \sqcup \mathcal{F}_{2,2}$ is not empty, define $\mathcal{F}_1 \sqcup \mathcal{F}_2$ to be the natural extension of it; moreover, any other formula of S with a logical edge to some formula active in S_1 is forced to be active in $\mathcal{F}_1 \sqcup \mathcal{F}_2$;

2. if $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$ is not empty and the auxiliary formula in S_1 is not active, all natural extensions of paths in $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$ are in $\mathcal{F}_1 \sqcup \mathcal{F}_2$ and moreover,any other formula of S with a logical edge to some formula active in S_2 is forced to be active in $\mathcal{F}_1 \sqcup \mathcal{F}_2$.

Suppose R is a *unary* rule applied to the subproof $\Pi_1 : S_1$ of Π; let $\mathcal{F}_{1,1}, \mathcal{F}_{2,1}$ be the flows associated to Π_1. Define $\mathcal{F}_1 \sqcup \mathcal{F}_2$ to be the natural extension of $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$. If R is a $\vee$:*right* rule applied to a sequent $\Gamma \rightarrow \Delta, A$ to obtain $\Gamma \rightarrow \Delta, A \vee B$ or $\Gamma \rightarrow \Delta, B \vee A$, any s-formula C in B is active in $\mathcal{F}_1 \sqcup \mathcal{F}_2$ if it is active in either $\mathcal{F}_1$ or $\mathcal{F}_2$.

Suppose R is a *contraction* rule applied to $\Pi_1 : S_1$ and $\mathcal{F}_{1,1}, \mathcal{F}_{2,1}$ are the flows associated to Π_1 then let $\mathcal{F}_1 \sqcup \mathcal{F}_2$ be the natural extension of $\mathcal{F}_{1,1} \sqcup \mathcal{F}_{2,1}$.

This concludes the definition of union of flows.

3.5 Some properties of the theory T_F

To prove Theorem 6 we need to study the logical paths of F-formulas as well as the logical paths of F-free formulas occurring in a T_F-proof. In fact, given a T_F-proof, the analysis of the logical graph of F-formulas in it will induce the bound 2^n we are looking for, and the analysis of the logical graph of F-free formulas will lead to find a suitable flow for the proof from which we will generate an inner proof of the same sequent with no occurrence of symbols F in it.

In this section, we will first discuss few properties on paths of F-formulas, and then some lemmas concerning the relations between flows and structure of T_F-proofs.

3.5.1 Paths of F-formulas

We start with some definitions concerning the logical flow graph of the F-formulas. Let Π be a T_F-proof and $\mathcal{L}$ its logical flow graph. An *F-path* is a sequence of edges in $\mathcal{L}$ between F-atomic formulas of Π.

Definition 15 Let $F(t)$ be a s-formula occurring positively in Π and f be a F-path of Π where $F(t)$ is the formula with no outgoing edges (belonging to f); let C be the formula of f with no incoming edges in $\mathcal{L}$. The F-path f is called a *full F-path associated to $F(t)$* if one of the following conditions is satisfied

1. C occurs in the endsequent of Π, or
2. C is an s-formula occurring in some non-distinguished formula of the axioms of Π (i.e. in the cedents Γ, Δ), or
3. C is $F(0)$ and appears as a distinguished occurrence in a special axiom of Π, or
4. C is an s-formula occurring in B of the main formula $A \vee B$ or $B \vee A$ in a $\vee$:*right* application in Π.

Let $F(t)$ be a s-formula occurring positively in Π; the *F-flow associated to $F(t)$* is the set of *all* full F-paths in Π that are associated to $F(t)$.

Definition 16 A F-flow associated to $F(t)$ is called *complete* if one of the following condition is satisfied

a. t is the term 0, or

b. there exists a variant $F(s)$ of $F(t)$ (possibly $F(t)$ itself) belonging to the F-flow such that

1. $F(s)$ is a main formula of a *F-successor*, *F-plus*, *F-times* rule application, and
2. $F(s)$ is the closest variant with an incoming path to $F(t)$ satisfying property 1 (i.e. the variants in the F-flow lying between $F(s)$ and $F(t)$ do not satisfy the property), and
3. the F-flows associated to the parents of $F(s)$ (i.e. the auxiliary formulas from which $F(s)$ is derived) are complete.

Given a T_F-proof, the only way in which a F-atomic formula $F(t)$ can be linked by a F-path to a variant $F(s)$ with $val(s) > val(t)$ is by means of a *F-successor*, *F-plus*, *F-times* rule application to $F(t)$ in the proof. This fact is captured by the notion of complete F-flow and pointed out in the following lemma.

Lemma 17 *Let t be any closed primitive recursive term in the language of PA. Suppose $F(t)$ has a complete F-flow in a T_F-proof Π. Then $val(t) \leq 2^n$, where n is the number of F-successor, F-plus, F-times rules in Π. Moreover, 2^n is the best possible upper bound for $val(t)$ in the sense that for all $\alpha < 1$, 2^{n^α} is not an upper bound.*

Proof. By definition of complete F-flow it is enough to check what is the maximum value that can be assigned to the root of a binary tree (not necessarily complete) with n nodes (denoted $max(n)$ for short), where leaves have value 1 and the value of an internal node is obtained applying successor, plus or times functions to the values of the parent(s). By induction we have:

$n = 1$: $max(1) = 1 \leq 2^0 = 1$;

$n + 1$: there are *two* cases. We may have a tree where the root has only one parent which is a root of a subtree of n nodes. In this case we apply the induction hypothesis to the subtree and obtain that $max(n+1) = max(n) + 1 \leq 2^n + 1 \leq 2^{n+1}$ (note that the value of the root can increase only by 1 because there is only one parent).

Or we may have a root with two parents that are respectively roots for a subtree of k nodes and a subtree of $n - k$ nodes. In this case we apply the induction hypothesis to the subtrees and obtain that $max(n+1) = max(k) \cdot max(n-k) \leq 2^k \cdot 2^{n-k} \leq 2^n \leq 2^{n+1}$. Notice that the hightest value of a root with two parents is obtained by multiplying the values of the parents (for $n > 2$). If $n = 2$ then the values must be added.

To show that 2^n is the best possible upper bound for $val(t)$ given n, we can proceed observing that in our proof, we used the fact that the number of nodes and the value of the nodes of a binary tree, are respectively described by the functions f, g defined as follows:

$$f(0) = 15 \qquad f(k+1) = 2 \cdot f(k) + 1$$

and

$$g(k) = 2^{4 \cdot 2^k}$$

We will show that for all α such that $0 < \alpha < 1$ and $k \to \infty$ the inequality $g(k) > 2^{f(k)^\alpha}$ holds, i.e.

$$\frac{log_2 log_2 g(k)}{log_2 f(k)} > \alpha$$

from where we derive that $2^{f(k)} \geq g(k)$ (for all k) is the best possible bound. Notice that $f(k)$ can be written as $15 \cdot 2^k + \sum_{i=1}^{k-1} 2^i$, that is $16 \cdot 2^k - 1$. Therefore

$$\begin{aligned}
\lim_{k\to\infty} \frac{log_2 log_2 2^{4\cdot 2^k}}{log_2(16\cdot 2^k - 1)} &= \lim_{k\to\infty} \frac{2+k}{log_2(16\cdot 2^k - 1)} = \\
\lim_{k\to\infty} \frac{1}{\frac{1}{ln2}\cdot\frac{1}{16\cdot 2^k - 1}\cdot 16\cdot 2^k \cdot ln2} &= \lim_{k\to\infty} \frac{16\cdot 2^k - 1}{16\cdot 2^k} = \\
\lim_{k\to\infty} 1 - \frac{1}{16\cdot 2^k} &= 1 > \alpha
\end{aligned}$$

□

Note that if the rule *F-times* is not a special rule of T_F then the lemma holds for $val(t) \leq n$.

3.5.2 Flow graphs and T_F-proofs

A number of lemmas concerning the structure of a T_F-proof and its flows are proved. The main result of this section is Lemma 21. Let us start with a definition.

Definition 18 Let $\Pi : S$ be a proof in T_F with endsequent S; let $\mathcal{F}$ be a flow in Π. The sequent $H(S)$ induced by $\mathcal{F}$ is called a *base for* $\mathcal{F}$.

We say that an occurrence of the formula A in S does not belong to the base whenever it is not active (i.e. $H(A) = \emptyset$).

Lemma 19 (Substitution into a deduction) *Let t be a term. Let $\Gamma(a) \to \Delta(a)$ be a T_F-provable sequent in which the variable a is fully indicated*[5], *and let $\Pi(a)$ be a proof of*

[5]Let B be a formula containing k distinct free variables $b_1, \ldots, b_k$; let $t_1, \ldots, t_k$ be a k-tuple of terms. Consider A to be the formula obtained replacing all free variables b_i's with the terms t_i's. We say that a term t_i is *fully indicated* in A if all occurrences of t_i in A are obtained by such a replacement (Cf. [Tak75]).

$\Gamma(a) \rightarrow \Delta(a)$ in which every eigenvariable is different from a and not contained in t. Then $\Pi(t)$ (i.e. the result of replacing all a's in $\Pi(a)$ by t) is a proof of $\Gamma(t) \rightarrow \Delta(t)$. Moreover $N(\Pi(t)) = N(\Pi(a))$ and if $\Pi(t)$ has a flow $\mathcal{F}_t$ with base $H_{\mathcal{F}_t}(\Gamma(t) \rightarrow \Delta(t))$ then $\Pi(a)$ has a flow $\mathcal{F}_a$ with base $H_{\mathcal{F}_a}(\Gamma(a) \rightarrow \Delta(a)) = H_{\mathcal{F}_t}(\Gamma(t) \rightarrow \Delta(t))(t/a)$.

Proof. By induction on the height of Π. If $\Pi(a)$ is an axiom then $\Pi(t)$ is an axiom as well. We must consider now the case in which Π ends with a rule of inference R. It is enough to apply the induction hypothesis to the premise(s) of R and apply to the result the rule R again. Note that the proof $\Pi(t)$ is obtained by replacing all occurrences of a in $\Pi(a)$ with t, hence the structure of the proof remains the same and therefore its logical flow. This implies that $N(\Pi(a)) = N(\Pi(t))$ and that the flows of Π' are flows for Π as well (and vice versa). □

We give now the proof of Lemma 12 (stated in section 3.4). The result essentially says that to each sequent we can always add new weak formulas without augmenting the complexity of the proof. In other words, the weakening rule can be simulated by the system.

Proof. (Lemma 12 - Addition of weak occurrences) By induction on the height of Π. If Π is an axiom then Π' is an axiom as well. If Π ends with a rule of inference R then apply the induction hypothesis to one of the premises whenever R is binary, or to the only one premiss whenever R is unary; apply again the rule R to the result. Notice that lemma 19 may have to be used to handle the case $\exists$:*left*.

Since the structure of Π' is essentially the same as the structure of Π (the only difference consists on the presence of weak occurrences Λ, Θ in Π') then $N(\Pi') = N(\Pi)$ and any flow of Π' is a flow of Π as well whenever it is restricted to formulas of Π (notice that the formulas in Λ, Θ are weak occurrences, hence they do not interfere with the logical structure of Π). □

Lemma 20 (Elimination of weak occurrences) *Let $\Pi : S$ be a deduction and A a weak occurrence of a formula in S. Let S' be the result of omitting A from S. Then a deduction $\Pi' : S'$ can be constructed such that $N(\Pi') = N(\Pi)$, and Π' has a flow $\mathcal{F}'$ if and only if Π has a flow $\mathcal{F}$. Moreover, if $\mathcal{F}'$ exists then $\mathcal{F}$ can be defined so that $H_{\mathcal{F}}(S) = H_{\mathcal{F}'}(S')$.*

Proof. By induction on the height of Π. If S is an axiom then S' is an axiom as well (since A is a non-distinguished occurrence). The induction step is proved deleting the weak occurrence A from a premise of the last rule of inference R of Π and applying R again to the resulting proof(s). This can be done because a weak occurrence cannot be a main formula in Π.

Since the structure of Π' is the same as the structure of Π then $N(\Pi') = N(\Pi)$. Notice that if Π has a flow $\mathcal{F}^*$ with A active in it, then there is a flow $\mathcal{F}$ where A is not active defined as $\mathcal{F}^*$ except on the variants linked to A (in the logical flow graph): let each s-formula of A be not active. The claim follows easily from this observation. □

We remind the reader that the *degree of a formula* is defined inductively as follows: $d(P) = 1$ if P is atomic, $d(A \vee B) = sup\{d(A)+1, d(B)+1\}$ and $d(\neg A) = d((\exists x)A) = d(A)+1$. The *degree of a cut* is the degree of its cut-formulas.

Lemma 21 (Cut Elimination) *There exists an effective procedure that transforms every T_F-proof $\Pi : S$ into a derivation $\Pi' : S$ with no cuts on F-formulas. Moreover if Π' has a good flow with base $H'(S)$ then Π has a good flow with base $H(S) = H'(S)$.*

Proof. If Π does not contain cuts on F-formulas then the claim holds.

In the following we will describe a procedure that transforms any cut on F-formulas of degree ≥ 1 in Π into a cut(s) of lower degree, possibly no cuts. This operation must be repeated until every cut on F-formulas of degree ≥ 1 has systematically been eliminated. The proof Π' will be obtained from Π by a finite number ($k > 0$) of steps of reduction transforming Π_i into Π_{i+1} and where Π_1 is Π and Π_k is Π'. We say that Π_{i+1} has been obtained by Π_i if a step of the reduction procedure is applied to a cut on a F-formula in the proof Π_i.

Assume that Π_{i+1} has a good flow with base $H_{i+1}(S)$; we want to show that Π_i has a good flow with base $H_i(S) = H_{i+1}(S)$. Notice that this suffices to show the claim.

There are six kinds of reduction we must discuss:

1. the reducibility of the complexity of a cut when at least one of the cut-formulas is weak;
2. the elimination of a cut when both cut formulas are distinguished occurrences in axioms;

3. the elimination of a cut when the cut formulas are F-atomic and one of them is a distinguished formula (occurring negatively) in a logical axiom;

4. the permutation of the cut upward in case a cut-formula is passive (and not weak) on the right (similarly, on the left);

5. the reducibility of the complexity of a cut when both cut-formulas are main formulas;

6. the reducibility of the complexity of a cut in case one of the cut-formulas is the main formula of a contraction rule.

The reduction of kind 6 is the most problematic one; to study the flow of formulas passing through contraction-formulas we will need to show some general properties of cut-formulas and logical flows. This will be done in a subclaim at the end of the proof.

Let us start to discuss reductions of kind 1. Let Π_i be of the form

$$\dfrac{\begin{array}{c}\Pi_1'\\ \Gamma_1 \to \Delta_1, A\end{array} \quad \begin{array}{c}\Pi_2'\\ A, \Gamma_2 \to \Delta_2\end{array}}{\Gamma_{1,2} \to \Delta_{1,2}} \\ \vdots\lambda$$

In this case apply Lemma 20 to the subproof where the cut-formula is weak, say for instance Π_1'. Then apply Lemma 12 to the result, to add the weak occurrences Γ_2, Δ_2 to the sequent $\Gamma_1 \to \Delta_1$. Call Π_1'' the resulting proof and define Π_{i+1} as

$$\begin{array}{c}\Pi_1''\\ \Gamma_{1,2} \to \Delta_{1,2}\\ \vdots\lambda\end{array}$$

By Lemma 20 if Π_1'' has a good flow then Π_1' has it and its base is $H_{\mathcal{F}_{i+1}}(\Gamma_1 \to \Delta_1)$. Define $\mathcal{F}_i$ as such flow on Π_i' and activate Γ_2, Δ_2 in the sequent $\Gamma_{1,2} \to \Delta_{1,2}$ of Π_i' as in Π_i''.

Define the flow in λ of Π_i as in λ of Π_{i+1}.

Reductions of kind 2 are treated as follows. Let Π_i be of the form described in case 1, where Π'_1, Π'_2 are axioms and both cut-formulas are distinguished occurrences in the axioms. The case when both Π_1, Π_2 are logical axioms and the case when Π_1 is a special axiom and Π_2 a logical axiom, are the only ones can arise (here, the fact that the equality axiom for predicates cannot be applied to the predicate F plays a crucial role). It is easy to see that the sequent $\Gamma \rightarrow \Delta$ is an axiom itself. Therefore, define Π_{i+1} to be

$$\begin{array}{c} \Gamma \rightarrow \Delta \\ \vdots\lambda \end{array}$$

Moreover, for every bridge (if any) from/to a formula in Γ to/from a formula in Δ of the sequent $\Gamma \rightarrow \Delta$ in Π_i define a corresponding edge in the axiom $\Gamma \rightarrow \Delta$ of Π_{i+1}. A logical flow is obtained. This means that if $\Gamma \rightarrow \Delta$ in Π_{i+1} has a good flow then $\Gamma \rightarrow \Delta$ in Π_i has a good flow with the same base. Define the flow on λ of Π_i as in λ of Π_{i+1}.

Reductions of kind 3 are treated as follows. Let Π_i be of the form

$$\begin{array}{c} \dfrac{\begin{array}{c}\Pi'_1 \\ \Gamma_1 \rightarrow \Delta_1, F(t)\end{array} \quad F(t), \Gamma_2 \rightarrow \Delta_2, F(t)}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t)} \\ \vdots\lambda \end{array}$$

Define Π_{i+1} as

$$\begin{array}{c} \Pi''_1 \\ \Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t) \\ \vdots\lambda \end{array}$$

where Π_1'' has been obtained applying Lemma 12 to Π_1', to add the weak occurrences Γ_2, Δ_2 to the sequent $\Gamma_1 \rightarrow \Delta_1, F(t)$. By Lemma 20, if Π_1'' has a good flow then Π_1' has it and its base is $H_{\mathcal{F}_{i+1}}(\Gamma_1 \rightarrow \Delta_1)$. Define $\mathcal{F}_i$ as such flow on Π_i' and activate Γ_2, Δ_2 in the sequent $\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t)$ of Π_i' as in Π_i''.

We consider now the case in which cuts are not acting on main formulas (i.e. the reductions of kind 4). Suppose we have the cut formula passive on the right (the case in which it is passive on the left is handled similarly).

Let Π_i be of the form

$$\dfrac{\dfrac{\begin{matrix}\Pi_1' \\ B, \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \begin{matrix}\Pi_2' \\ C, \Gamma_2 \rightarrow \Delta_2\end{matrix}}{B \vee C, \Gamma_{1,2} \rightarrow \Delta_{1,2}, A} \quad \begin{matrix}\Pi_3' \\ A, \Gamma_3 \rightarrow \Delta_3\end{matrix}}{\begin{matrix}B \vee C, \Gamma_{1,2,3} \rightarrow \Delta_{1,2,3} \\ \vdots \lambda\end{matrix}}$$

and Π_{i+1} of the form

$$\dfrac{\dfrac{\begin{matrix}\Pi_1' \\ B, \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \begin{matrix}\Pi_3' \\ A, \Gamma_3 \rightarrow \Delta_3\end{matrix}}{B, \Gamma_{1,3} \rightarrow \Delta_{1,3}, A} \quad \begin{matrix}\Pi_2' \\ C, \Gamma_2 \rightarrow \Delta_2\end{matrix}}{\begin{matrix}B \vee C, \Gamma_{1,2,3} \rightarrow \Delta_{1,2,3} \\ \vdots \lambda\end{matrix}}$$

The flow $\mathcal{F}_i$ is defined as the natural extension of the flow $\mathcal{F}_{i+1}$ in Π_1, Π_2, Π_3 respectively. Define the flow on λ of Π_i as in λ of Π_{i+1}.

All remaining cases of right (left, respectively) subproof having a logical rule as last rule of inference, are treated similarly. In an analogous way we also treat the permutation of cuts upwards.

We consider now reductions of kind 5. Suppose Π_i has the following form

$$\dfrac{\dfrac{\begin{matrix}\Pi'_1\\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix}}{\Gamma_1 \rightarrow \Delta_1, A \vee B} \quad \dfrac{\begin{matrix}\Pi'_2\\ A, \Gamma_2 \rightarrow \Delta_2\end{matrix} \quad \begin{matrix}\Pi'_3\\ B, \Gamma_3 \rightarrow \Delta_3\end{matrix}}{A \vee B, \Gamma_{2,3} \rightarrow \Delta_{2,3}}}{\begin{matrix}\Gamma_{1,2,3} \rightarrow \Delta_{1,2,3}\\ \vdots\lambda\end{matrix}}$$

and Π_{i+1} is defined as follows

$$\dfrac{\begin{matrix}\Pi'_1\\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \begin{matrix}\Pi''_2\\ A, \Gamma_{2,3} \rightarrow \Delta_{2,3}\end{matrix}}{\begin{matrix}\Gamma_{1,2,3} \rightarrow \Delta_{1,2,3}\\ \vdots\lambda\end{matrix}}$$

where Π''_2 has been obtained by applying Lemma 12 to Π'_2.

By Lemma 20 if Π''_2 has a good flow then Π'_2 has it and its base is $H_{\mathcal{F}_{i+1}}(A, \Gamma_2 \rightarrow \Delta_2)$. Define $\mathcal{F}_i$ as such flow on Π'_i and activate Γ_3, Δ_3 in the sequent $A \vee B, \Gamma_{2,3} \rightarrow \Delta_{2,3}$ of Π'_i as in Π''_i. Define $\mathcal{F}_i$ to be the natural extension of $\mathcal{F}_{i+1}$ on Π'_1, with both occurrences of B not active in the auxiliary formulas $A \vee B$. The flow must also be naturally extended to the sequent $\Gamma \rightarrow \Delta$ and to λ. Notice that $H_{i+1}(\Gamma \rightarrow \Delta) = H_i(\Gamma \rightarrow \Delta)$ (therefore $H_{i+1}(S) = H_i(S)$) and that the flow so defined is good since $\mathcal{F}_{i+1}$ is good. Since by hypothesis $\mathcal{F}_{i+1}$ is essential, $\mathcal{F}_i$ turns out to be essential as well by the construction.

The cases where $\neg A$ and $(\exists x)A(x)$ are main formulas in the upper sequents, are treated similarly (the proof Π_{i+1} relative to these cases is defined following the usual cut-elimination procedure described in [Tak75]). Notice that Lemma 19 has to be used together with the hypothesis that Π is regular (and therefore Π_i by construction), for the $(\exists x)A(x)$ case.

The last transformation we must discuss concerns the cuts on a contracted formula (i.e. reductions of kind 6). Let Π_i be of the form

$$\dfrac{\begin{matrix}\Pi_1' \\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \dfrac{\begin{matrix}\Pi_2' \\ A, A, \Gamma_2 \rightarrow \Delta_2\end{matrix}}{A, \Gamma_2 \rightarrow \Delta_2}}{\Gamma_{1,2} \rightarrow \Delta_{1,2}}$$
$$\vdots \lambda$$

and Π_{i+1} be of the form

$$\dfrac{\begin{matrix}\Pi_1' \\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \dfrac{\begin{matrix}\Pi_1' \\ \Gamma_1 \rightarrow \Delta_1, A\end{matrix} \quad \begin{matrix}\Pi_2' \\ A, A, \Gamma_2 \rightarrow \Delta_2\end{matrix}}{A, \Gamma_{1,2} \rightarrow \Delta_{1,2}}}{\Gamma_{1,1,2} \rightarrow \Delta_{1,1,2}}$$
$$\vdots \text{Contractions}$$
$$\Gamma_{1,2} \rightarrow \Delta_{1,2}$$
$$\vdots \lambda$$

This case has a non-trivial definition of good flow $\mathcal{F}_i$ based on a good flow $\mathcal{F}_{i+1}$. We will show that

Claim *If there is a good flow $\mathcal{F}_2'$ associated to Π_2' in Π_{i+1} then there is a good flow $\mathcal{F}_2^*$ associated to Π_2' in Π_i, where the images of the contraction formulas A are the same (whenever both not empty) and they are exactly defined as the union of the images of A induced by the flow $\mathcal{F}_{i+1}$ on the occurrences of Π_1'.*

Notice that if the claim is shown then one can define the flow in $\mathcal{F}_i$ to be the natural extension of the union of the flows (in $\mathcal{F}_{i+1}$) on the occurrences Π_1', and of the flow $\mathcal{F}_2^*$ for Π_2.

To show the claim we need to present some general properties of cut-formulas in the cut-elimination procedure. Let $\Pi_1 \ldots \Pi_k$ be the sequence of proofs obtained by applying the cut-elimination procedure; by induction on $j = 1, \ldots, k$ we define the notion of *unjustified* s-formula in Π_i, knowing which formulas are unjustified in Π_{i+1}. Our notation will refer back to the figures we used to describe the steps of reduction. If a reduction of kind 1 is applied to Π_i we call the s-formula A in Π'_2 unjustified; if a reduction of kind 5 is applied we call the s-formula B in the right cut-formula $A \vee B$ in Π_i unjustified; if a reduction of kind 6 is applied we have that the two occurrences of the proofs Π'_1 in Π_{i+1} are identified in Π_i and in this case whenever a s-formula B is unjustified in one occurrence but not unjustified in the other, let the corresponding occurrence of Π'_i in Π_i be not unjustified; if a s-formula B is unjustified in Π_{i+1}, then its corresponding s-formula B in Π_i is unjustified. This concludes the definition of unjustified formula.

Notice that by construction, given two subproofs $\Pi_1 : \Gamma_1 \rightarrow \Delta_1, A$ and $\Pi_2 : A, \Gamma_2 \rightarrow \Delta_2$ to which a cut is applied, if B occurs as unjustified s-formula in A of Π_2 (resp. Π_1) then the corresponding B in the cut-formula A of Π_1 (resp. Π_2) cannot be unjustified.

We want to show that two contraction formulas A^1, A^2 in a reduction step 6 are always *compatible*, i.e. for all corresponding pairs of s-formulas B occurring in the contraction formulas, either both occurrences are unjustified or both are not unjustified.

We proceed by induction on the reduction steps of the cut-elimination procedure. Assume that on step i transforming Π_i into Π_{i+1} the claim is false. Formally, call A^1, A^2 the two occurrences of A in Π_2 and Π_1^1, Π_1^2 the two occurrences of Π'_1 in Π_{i+1} which auxiliary formulas A cut respectively A^1 and A^2; assume that there is a s-formula B^2 in A^2 that is unjustified while the corresponding B^1 in A^1 is not.

$$\dfrac{\begin{array}{c}\Pi_1^2\\ \Gamma_1 \rightarrow \Delta_1, A^2\end{array} \quad \dfrac{\begin{array}{c}\Pi_1^1\\ \Gamma_1 \rightarrow \Delta_1, A^1\end{array} \quad \begin{array}{c}\Pi_2'\\ A^1, A^2, \Gamma_2 \rightarrow \Delta_2\end{array}}{A, \Gamma_{1,2} \rightarrow \Delta_{1,2}}}{\dfrac{\Gamma_{1,1,2} \rightarrow \Delta_{1,1,2}}{\begin{array}{c}\vdots \text{Contractions}\\ \Gamma_{1,2} \rightarrow \Delta_{1,2}\\ \vdots \lambda\end{array}}}$$

We consider three cases.

First, suppose that in Π_1^2 we have two logical paths f_1, f_2 from a variant B^* (occurring in the cut-formula of Π_1^2) logically linked to B^2; one is a bridge to the end-sequent of Π_1^2 and the other is not.

Notice that we have to have a path that is not a bridge because B^2 is an unjustified formula. This means that Π_1^2 contains a contraction application on a pair of variants C's (where C is a subformula of A containing B^*, and possibly C is B^* itself) such that the path f_1 pass through one of them while f_2 pass through the other. Since C is a cut-formula, the only way the contraction application could have been introduced in Π_1^2 is by means of an application of step 6 in the cut-elimination procedure generating Π_i, say step j (where $j < i$) transforming Π_j into Π_{j+1}. By induction it turns out that both contraction formulas C in Π_j are compatible and moreover, their cut-formulas C should be not unjustified (hence the s-formula B^* occurring in it). This is because at least one of the contraction-formulas has a bridge to the end-sequent. Therefore (by construction) the s-formula A^2 in Π_2 has to have B not unjustified. Contradiction.

Second, suppose that in Π_1^2 we have only one logical path f_1 from the variant B^* logically linked to B^2 and that f_1 is not a bridge. This means that B^* has been introduced in Π_1^2 by an $\vee$-*right* application or by a reduction of kind 1 (i.e. B^* is a weak occurrence in Π_1^2). But then, both occurrences of B in A^1, A^2 respectively should be unjustified. Contradiction.

Third, suppose that in Π_1^2 we have two logical paths f_1, f_2 from the variant B^* logically linked to B^2 and both of them are not bridges. This means that in Π_1^2 there exists a contraction of some pair of formulas C as discussed in the first case. Since both paths are not bridges we have that B has been introduced in Π_1^2 by an $\vee$-*right* application or a reduction of kind 1 in the cut-elimination procedure. Arguing as in the previous case, we deduce a contradiction.

This concludes the proof of our claim.

Now it is enough to observe that given a proof Π and a good flow $\mathcal{F}$ for it, whenever a not unjustified s-formula B is not active in an active occurrence A in Π, one can always define an extension of $\mathcal{F}$ to $\mathcal{F}'$ where B is active. Notice that if B is not unjustified, then it has been introduced by an $\vee$:*right* application or it is a weak occurrence (this is because the flow is good by hypothesis; notice that this assumption is crucial at this step of the proof).

This concludes the proof. □

Corollary 22 *Let* $\Pi : S$ *be a proof with* n *applications of* F*-successor,* F*-plus and* F*-times. Let* Π' *be the result of a cut-elimination procedure applied to* F*-formulas. If* $F(t)$ *is some occurrence in* Π' *and* $\Pi' : S$ *has a complete* F*-flow associated to it then* $F(t)$ *also has an occurrence in* Π *and* $val(t) \leq 2^n$.

Proof. For each step of the cut-elimination procedure described in Lemma 21 (transforming a proof Π_i into a proof Π_{i+1}, where $i = 1 \dots k$ for some k) it can be shown that if there exists a complete F-flow associated to some $F(t)$ in Π_{i+1} then there exists a complete F-flow associated to some occurrence of $F(t)$ in Π_i. This is because each flow in Π_{i+1} is "preserved" in Π_i.

Since by hypothesis there exists a complete F-flow associated to some $F(t)$ in Π', then there exists a complete F-flow in Π associated to some $F(t)$ (note that Π is Π_1 and Π' is Π_k). By Lemma 17 applied to Π, it follows that $val(t) \leq 2^n$. Notice that Lemma 17 cannot be applied directly to Π' because Π' is the cut-free proof associated to Π and the number of *F-successor*, *F-plus* and *F-times* applications in it is generally greater than n (since the complexity of Π' is much bigger than the complexity of Π). □

Definition 23 Let $\Pi : A_1, \dots, A_n \rightarrow B_1, \dots, B_n$ be a proof in T_F. A sequent $\Gamma' \rightarrow \Delta'$ is a *good base* for Π if Γ', Δ' are subcollections of $A_1, \dots, A_n$ and $B_1, \dots, B_n$ (respectively), and there exists a good flow $\mathcal{F}$ in Π such that

1. $H_{\mathcal{F}}(A_1, \dots, A_n \rightarrow B_1, \dots, B_n)$ is $\Gamma' \rightarrow \Delta'$, and
2. for all formulas A_i in $A_1, \dots, A_n \rightarrow B_1, \dots, B_n$, either $H_{\mathcal{F}}(A_i)$ is $G(A_i)$ or $H_{\mathcal{F}}(A_i)$ is empty. Similarly for B_i.

Intuitively, for all atomic (that are not F-formulas) occurrences C in a formula A of S, if $H(A)$ is not empty then C must belong to the base (i.e. $H(C)$ is not empty).

Lemma 24 *Let $\Pi : S$ be a proof in T_F and $val(\theta) > 2^n$ where n is the number of applications of F-successor, F-plus and F-times in Π. At least one of the following holds*

a. there exists a good base for S;

b. there exists an s-formula $F(t)$ in S

1. with a complete F-flow, or

2. with a bridge to a variant in S, or

3. with a path to an auxiliary occurrence $F(\theta)$ in some application of a critical rule in Π.

In particular, if S is F-free then S has a good base.

Proof. This proof is a consequence of Lemma 21 for which it follows that for all proofs (possibly containing cuts on F-formulas of arbitrary degree), condition a holds whenever b does not.

If Π satisfies one of the conditions in b, we are done. Suppose it does not then we must show that condition a holds, and for this it is enough to prove the proposition on proofs Π not containing cuts on F-formulas (and possibly containing cuts on F-free formulas). In fact, if Π is a proof with arbitrary cuts then by Lemma 21 we know that there exists an effective procedure transforming Π into a proof Π' (with no cuts on F-formulas) such that, if Π' satisfies a then Π satisfies a as well. Moreover, it is easy to see that if Π does not satisfy $b.i$ (for $i = 1, 2, 3$) then Π' does not (to show it, it is enough to check that if $b.i$ holds for Π_{i+1} then it holds for Π_i as well, where Π_i and Π_{i+1} are two successive steps on the cut-elimination procedure described in Lemma 21).

Let us suppose that there are no cuts on F-formulas in Π. We proceed by induction on the height of Π.

$h(\Pi) = 1$: Π must be an axiom of one of the following forms

- $A, \Gamma \rightarrow \Delta, A$: if A does not contain only F-atomics as atomic subformulas, then condition a is satisfied with $G(A) \rightarrow G(A)$ as good base; otherwise *b.2* holds;
- it is an *equality axiom* or a *PA-axiom*: in this case condition a holds.
- $\Gamma \rightarrow \Delta, F(0)$: condition *b.1* holds.

$h(\Pi) = k + 1$: we proceed by inspecting the form of the last rule of inference R.

- $\neg$: *left*: let S_1 be the upper sequent of R. If S_1 satisfies a then S satisfies a; in fact, if the good base of S_1 is defined with respect to the good flow $\mathcal{F}_1$, then the base of S defined as the natural extension of $\mathcal{F}_1$ must be good.

  If S_1 satisfies *b.i* then S satisfies *b.i* (for $i = 1, 2, 3$); in fact, all positive occurrences of an s-formula in S, have an incoming edge from a positive occurrence of an s-formula in S_1, and all negative occurrences of formulas in S have an outgoing edge to a negative occurrence of an s-formula in S_1. Moreover, no new bridges are created or old bridges deleted.

  The $\neg$: *right*, $\exists$: *left* and $\exists$: *right* cases are treated similarly;

- $\vee$: *left*: let S_1, S_2 be the (left and right, respectively) upper sequents of R. If one of them satisfies *b.i* (for $i = 1, 2, 3$) then S satisfies *b.i*. Suppose that *b.i* is not satisfied by S_1 and by S_2 then by induction hypothesis *a* holds for both. This means that there exist good bases $H(S_1), H(S_2)$ and in particular, there exist good flows $\mathcal{F}_1$, $\mathcal{F}_2$.

If the auxiliary occurrence of A (resp. B) is not active then let $H(S)$ be $H(S_1)$ (resp. $H(S_2)$) and $\mathcal{F}$ be the natural extension of $\mathcal{F}_1$ (resp. $\mathcal{F}_2$). If both auxiliary occurrences A and B are active then let $\mathcal{F}$ be the natural extension of $\mathcal{F}_1$ and $\mathcal{F}_2$; since $\mathcal{F}_1, \mathcal{F}_2$ are good then $\mathcal{F}$ is good. The base $H(S)$ is a good base because $H(S_1)$ and $H(S_2)$ are good bases and $\mathcal{F}$ is good.

- $\vee$: *right* : let S_1 be the upper sequent of R. If S_1 satisfies *b.i* (for $i = 1, 2, 3$) then S satisfies *b.i*; if it satisfies *a* then the formula A may or may not be active in $\mathcal{F}_1$. If it is not active then let $\mathcal{F}$ be the natural extension of $\mathcal{F}_1$; $H(S)$ is a good base because $\mathcal{F}$ is good and $H(S_1)$ is a good base.

  If A is active, then let $\mathcal{F}$ be the natural extension of $\mathcal{F}_1$ and let all F-free s-formulas of B be active in $\mathcal{F}$; $H(S)$ is a good base because $\mathcal{F}$ is good, $H(S_1)$ is a good base and all atomic F-free subformulas of A are active in $\mathcal{F}$ (i.e. $H(A) = G(A)$).

- *Cut*: let Π be of the form

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma_1 \to \Delta_1, A & A, \Gamma_2 \to \Delta_2 \end{array}}{\Gamma_{1,2} \to \Delta_{1,2}}$$

  By hypothesis, the formula A is F-free therefore $\Gamma_{1,2} \to \Delta_{1,2}$ satisfies *b.i* (for $i = 1, 2, 3$) whenever at least one of $\Gamma_1 \to \Delta_1, A$ or $A, \Gamma_2 \to \Delta_2$ satisfies *b.i*. Otherwise $\Gamma_1 \to \Delta_1, A$ and $A, \Gamma_2 \to \Delta_2$ satisfy *a*. In particular, if the image of one of the cut formulas A is empty, say the one relative to Π_1, then let $\mathcal{F}$ be the natural extension of $\mathcal{F}_1$. If both images are not empty they should be the same (i.e. $G(A)$). Define $\mathcal{F}$ as the natural extension on $\mathcal{F}_1, \mathcal{F}_2$ with suitable edges between the cut-formulas.

- *F-plus*: let Π be of the form

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma_1 \rightarrow \Delta_1, F(t_1) & \Gamma_2 \rightarrow \Delta_2, F(t_2) \end{array}}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t_1 + t_2)}$$

If there exists a good base in Π_1 or Π_2 we are done; in fact the natural extension would define a good base for Π. If not then by induction hypothesis, some of the $F(t)$'s in $\Gamma \rightarrow \Delta, F(t_1)$ or $\Gamma \rightarrow \Delta, F(t_2)$ may satisfy *b.i* (for some $i = 1, 2, 3$) and therefore $\Gamma \rightarrow \Delta, F(t_1 + t_2)$ satisfies *b.i*. Notice that if *b.1* is satisfied by the auxiliary occurrences $F(t_1), F(t_2)$ in Π_1, Π_2 then $F(t_1 + t_2)$ has a F-complete flow as well, and it is associated to $F(t_1 + t_2)$.

The *F-times* and *F-successor* cases are handled similarly;

- *F-equality*: let Π be of the form

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ \Gamma_1 \rightarrow \Delta_1, t = s & \Gamma_2 \rightarrow \Delta_2, F(s) \end{array}}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, F(t)}$$

If there exists a good base in $\Gamma_1 \rightarrow \Delta_1$ or $\Gamma_2 \rightarrow \Delta_2$ of the endsequent of Π_1 or Π_2 we are done. If not then by induction hypothesis, the condition *b.i* (for some $i = 1, 2, 3$) must hold in Π_2 and therefore in Π.

The *F-inequality* and *F-contraction* cases are handled similarly.

- *F-elimination*: let Π be of the form

$$\frac{\begin{array}{c} \Pi_1 \\ \Gamma \rightarrow \Delta, F(\theta) \end{array}}{\Gamma \rightarrow \Delta}$$

If there exists a good base for Π_1 then Π has a good base as well. If not then $\Gamma \rightarrow \Delta, F(\theta)$ must satisfy a condition *b.i* for some $i = 1, 2, 3$. If some $F(t)$ in $\Gamma \rightarrow \Delta$ satisfies *b.i* then we are done. If the auxiliary occurrence satisfies *b.i* then it can be observed that *b.2* is the only condition can hold. In fact, condition *b.3* cannot be satisfied by $F(\theta)$ because both occurrences of the formula $F(\theta)$ have to be *ending* formulas of an F-flow; therefore they cannot be linked. Condition *b.1* cannot be satisfied because by hypothesis $val(\theta) > 2^n$ and an F-complete flow requires $val(\theta) \leq 2^n$ by Lemma 17.

Notice that, if *b.2* is satisfied then the variant in the endsequent $\Gamma \rightarrow \Delta$ of Π will satisfy *b.3*.

□

3.6 From T_F-proofs to T-proofs

Using Lemma 24, we are now ready to show Theorem 6.

Proof. (Theorem 6) By Lemma 24 there exists a good base for $\Pi : S$ and by Proposition 11 there exists $\Pi' : H(S)$ where $N(\Pi') \leq N(\Pi)$. Notice that if a formula A occurs in $H(S)$ then $H(A) = A$ because $H(S)$ is a good base and S is F-free.

If $H(S) \neq S$, by Lemma 12 we can introduce weak formulas and obtain $\Pi'' : S$ from Π', where $N(\Pi'') \leq N(\Pi)$. □

Call T_F^- the theory T_F without *F-times*. Similarly to Theorem 2 we can derive the following, using the observation to Lemma 17 instead of Lemma 17 itself.

Theorem 25 *Let* Π *be a proof in* T_F^- *of the closed formula* B. *The formula* B *does not contain* F. *Suppose that the number of* F*-successor and* F*-plus applications in* Π *is* n *and that* $val(\theta) > n$. *Then there is a proof* $\Pi' : B$ *in* T *such that* $N(\Pi') \leq N(\Pi)$.

3.7 Non-standard elements and feasible numbers

Since we shall be talking about structure of proofs in PA_F (resp. PA), we shall remark on the formalization of the calculus we use. We shall assume that this formalization is constituted by the axioms of PA_F (resp. PA) together with tautologies, axioms for equality, quantifier axioms

- $\exists x A(x) \vee \neg A(t)$, where t is free for x in A;
- $(\exists x(\neg A \vee B) \vee \exists x A) \vee \neg \exists x B$;
- $A \vee \neg \exists x A$, where x does not occur free in A

and modus ponens as only rule of inference.

We remind the reader that a proof in PA_F is a tree where each formula except the end-formula, is used in the proof only once as premise of a modus ponens application.

Proposition 26 *If* $\Pi : A$ *is a proof in* PA_F *with* n *occurrences of the axioms (ii)-(iv) in it then there exists a proof* $\Pi' : \rightarrow A$ *in* T_F *with* n *applications of* F*-successor,* F*-plus,* F*-times.*

Proof. The proof $\Pi' : \to A$ can be easily built from $\Pi : A$

1. by substituting all axioms of PA_F with T_F-proofs of a sequent of suitable form (for instance $(\exists x(\neg A \vee B) \vee \exists x A) \vee \neg\exists x B$ may be transformed in the sequent $\exists x B \to \exists x(\neg A \vee B), \exists x A$), and

2. by transforming all modus ponens applications in cut applications.

Notice that each occurrence of an axiom of the form *(ii)-(iv)* can be translated in T_F with a proof of it using exactly *one* occurrence of the rules *F-successor*, *F-plus*, *F-times* respectively. □

We are now ready to show our main theorem.

Proof. (Theorem 5) Consider the proof $\Pi : B$ in PA_F and apply to it Proposition 26 to obtain $\Pi^* : \to B$ in T_F. Then, apply Theorem 6 to Π^* and build $\Pi^{**} : \to B$ in T, where $N(\Pi^{**}) \leq N(\Pi^*)$. The proofs Π^* and Π^{**} are essentially the same proof except for the F-formulas that have been "deleted" in Π^{**} (in particular, all subproofs of Π^* associated to special axioms occurring in Π have been deleted). An easy transformation will produce Π' in PA with $N(\Pi') \leq N(\Pi)$ (note that Π' is obtained from Π essentially by "deleting" all F-formulas).

A more precise argument would be tedious. □

Remark. The analogue of Theorem 5 for the theory T_F^- (i.e. the theory defined as T_F without axiom *(iv)*) or for theories with many feasibilities can be proved.

As a corollary of Theorem 5 we can show

Corollary 27 *Let T_0 be the theory PA plus the special axioms (i)-(vi) and (vii) $\exists x \neg F(x)$. Let B be a closed formula in the language of PA. If $\Pi : B$ is a T_0-proof then there exists a PA-proof $\Pi' : B$ such that $N(\Pi') \leq 2 \cdot N(\Pi)$.*

Proof. Call T_0^- the theory T_0 without *(vii)*; let B be any F-free formula such that $\exists x \neg F(x) \vdash_k^{T_0^-} B$. Then $\forall \theta.(\neg F(\theta) \vdash_{2 \cdot k}^{T_0^-} B)$ and taking a large enough value $val(\theta)$ (with respect to k), by Theorem 5 we have $\vdash_{2 \cdot k}^{PA} B$. □

In [Kre69] and [Par69] it is shown by model-theoretic arguments that results proved using non-standard analysis can also be proved by standard methods. Namely, Kreisel ([Kre69]) shows that there is a recursive formal system in which the existing practice of non-standard analysis can be codified and it is a conservative extension of the current system of analysis. Parikh ([Par69]) shows that the Robinson's enlargement of any first order theory T (i.e. T is expanded to include some non-standard apparatus) is *always* a conservative extension of the standard version. Notice that T_0 is an enlargement (in Robinson's sense) of PA and our corollary not only implies that T_0 is a conservative extension of PA but that there is not even speed-up by T_0 over PA.

The fact that T_0 is a consistent extension of PA is easily proved using non-standard models of PA and interpreting $F(x)$ as "x is a non-standard number" (see [Par71]). Nevertheless our proof is syntactic and points out a correspondence between length of proofs (intended as number of steps) and non-standard numbers.

3.8 A generalization

In [Dra85], the concrete consistency of a theory of feasible numbers is shown in a generalized version. Namely, Dragalin suggests to extend Parikh's result by extending the language $0, s, +, *, <, =, F$ with a finite number of primitive recursive function symbols Q, say $f_1, \ldots, f_p$ and the theory PA_F with the axioms

(viii) $F(x_1) \ldots F(x_k) \rightarrow F(f_i(x_1, \ldots, x_k))$, for all $i = 1 \ldots p$.

for all $i = 1 \ldots p$. Call PA_F^s such theory (where s stands for "strong".) Assume that the smallest class of the Grzegorczyk Hierarchy where such functions belong is $\mathcal{E}_n$ (for $n \geq 2$). Theorem 5 can then be stated in the following stronger version

Theorem 28 *Suppose that the functions $f_1, \ldots, f_p$ occurring in PA_F^s-axioms of type (viii) belong to the Grzegorczyk class $\mathcal{E}_n$, for $n \geq 2$, then there exists a function g in $\mathcal{E}_{n+1}$ such that the following holds. Let Π be a proof in PA_F^s of the closed formula B. The formula B does not contain F. Suppose that the number of axioms of the form $(ii), (iii), (iv), (viii)$ occurring in Π is n and that $val(\theta) > g(n)$. Then there is a proof $\Pi' : B$ in PA such that $N(\Pi') \leq N(\Pi)$.*

We will not describe the proof. It essentially follows the steps the one we gave.

Chapter 4

Interpolants and Flow Graphs

4.1 Introduction

We give a proof of the well known Craig's Interpolation Theorem based on logical flow graphs

Theorem 29 (Craig's Interpolation Theorem for LK) *Let A and B be two formulas such that the sequent $A \rightarrow B$ is LK-provable. If A and B have at least one predicate letter in common, then there exists a formula C (called the interpolant of $A \rightarrow B$), such that C contains only those individual constants, predicate constants and free variables that occur in both A and B, and such that $A \rightarrow C$ and $C \rightarrow B$ are LK-provable. If A and B contain no predicate constant in common, then either $A \rightarrow$ or $\rightarrow B$ is LK-provable.*

The interpolant will be built by steps on the complexity of the subproofs using some easy considerations on the logical flows of the formulas in the proof. The method points out the logical relations between the s-formulas occurring in the interpolant and the ones occurring in A and B. Based on considerations concerning such relations, in subsection 4.1.2 we study a case of "easy" to prove sequents, where the interpolant is linearly bounded; in subsection 4.1.3 we prove that in case A and B are *not* "logically related" (in the sense of the logical flow graph) then one can find either a proof of $A \rightarrow$ or a proof of $\rightarrow B$ bounded by the complexity of the proof of $A \rightarrow B$; in section 4.2 we present the intuitionistic sequent calculus LJ and give the proof of the Interpolation Theorem for it. To simplify the exposition we will work only with the connectives $\land, \lor, \neg, \exists, \forall$.

4.1.1 The Interpolation Theorem

The theorem will be derived as a consequence of Gentzen's cut-elimination theorem. In fact, given a proof $\Pi : A \rightarrow B$ (possibly with cuts) we apply first the cut-elimination theorem to it and obtain a cut-free proof $\Pi_* : A \rightarrow B$. We will then build the interpolant C_* for $A \rightarrow B$ associated to Π_* together with the proofs $\Pi_*^A : A \rightarrow C_*$ and $\Pi_*^B : C_* \rightarrow B$, by stages on the subproofs of Π_*. The idea consists of "extracting" from the proof Π_*, two proofs associated to A and B respectively. As a consequence, each part of the original proof Π_* that "contributes" to the construction of the formula A (B respectively) will appear in the proof Π_*^A (Π_*^B respectively).

Proposition 30 *Let Π_* : S be a cut-free proof in LK. For all positive (negative) occurrences of a s-formula D in Π_*, there is exactly one positive (negative) occurrence of a s-formula D' in S with a logical path from (to) D.*

Proof. By induction on the height of the proof Π_*. The result follows because all logical and structural rules have the property that the incoming and outgoing logical paths to the premises are naturally extended to the conclusion. For instance consider $\wedge$:*right* be the last rule of inference in Π_* and the proof Π_* be of the form

$$\frac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ \Gamma_1 \rightarrow \Delta_1, A & \Gamma_2 \rightarrow \Delta_2, B\end{array}}{\Gamma_{1,2} \rightarrow \Delta_{1,2}, A \wedge B}$$

Suppose D is a positive (negative) occurrence in Π_*. If D is in Π_1, then by induction hypothesis, there is exactly one positive (negative) occurrence of a s-formula D_1' in $\Gamma_1 \rightarrow \Delta_1, A$ with logical path from D. The natural extension of such path activates exactly one formula D' in $\Gamma_{1,2} \rightarrow \Delta_{1,2}, A \wedge B$, variant of D_1'. If D is in $\Gamma_{1,2} \rightarrow \Delta_{1,2}, A \wedge B$, the claim is obviously satisfied for D' being D. □

In the sequel we will refer to the unique path described in the above statement as the *direct logical path from (to)* the positive (negative) s-formula D to the endsequent.

The property is the formulation in terms of logical paths of the well known *subformula property* (i.e. each s-formula in Π_* is a subformula of some formula in S. See [Tak75].)

Notice that if there is a positive (negative) s-formula D in Π_* linked to a negative (positive) s-formula D' in S, then there must be an axiom in Π_* through which a logical path passes, inducing the change of sign for the variants D and D'. In particular, we may have more than one negative (positive) s-formula D' in S linked to the positive (negative) s-formula D. This is because we have the contraction rule on our calculus that can be applied to two variants of D occurring positively (negatively) in Π_* and linked to D by logical paths.

If this is the case, notice that two different paths are actually passing through D. Since it may happen that both of them are linked to some negative (positive) variants in the end-sequent, the assertion follows. As a consequence of this observation we have that all weak occurrences in a cut-free proof Π_* are linked to only one variant in the end-sequent, and such a variant must be of the same sign.

Proof. (Theorem 29) Extend the first order language L with the atomic formulas $\top$, $\bot$ and the system LK with the new axioms $\Gamma \to \Delta, \top$ and $\bot, \Gamma \to \Delta$. Call the new language and the new system L^+ and LK^+, respectively. We will build a formula C_* and proofs $\Pi_*^A : A \to C_*, \Pi_*^B : C_* \to B$, first in the language L^+ and system LK^+. We will then map them into the language L and system LK. To indicate that the language of C_* (i.e. the set of symbols occurring in C_*) is contained in the intersection of the language of A with the language of B extended with $\top, \bot$, we will use the symbol $L(C_*) \subset^+ L(A) \cap L(B)$ (namely to say that $L(C_*) \subset (L(A) \cap L(B)) \cup \{\top, \bot\}$).

The proof is by induction on the height of Π. For each subproof Π of Π_* with end-sequent $\Gamma_\Pi \to \Delta_\Pi$ we show that

1. there exist subcollections $\Gamma_\Pi^A, \Delta_\Pi^A$ and $\Gamma_\Pi^B, \Delta_\Pi^B$ of Γ_Π, Δ_Π such that

   a. each formula occurrence in $\Gamma_\Pi^A, \Delta_\Pi^A$ ($\Gamma_\Pi^B, \Delta_\Pi^B$, respectively) has a direct path to A (B, respectively), and

   b. Γ_Π is $\Gamma_\Pi^A \Gamma_\Pi^B$ and Δ_Π is $\Delta_\Pi^A \Delta_\Pi^B$;

   there exists a formula C_Π such that

   a. $L(C_\Pi) \subset^+ L(A) \cap L(B)$, and

b. $\Gamma^A_\Pi \rightarrow \Delta^A_\Pi, C_\Pi$ and $C_\Pi, \Gamma^B_\Pi \rightarrow \Delta^B_\Pi$ are provable sequents.

Notice that if Π is Π_* then Γ^A_Π is A, Δ^A_Π is $\emptyset$, Γ^B_Π is $\emptyset$, Δ^B_Π is B and $A \rightarrow C_{\Pi_*}$, $C_{\Pi_*} \rightarrow B$ turn out to be provable sequents.

Let us start first by considering subproofs Π of Π_*, of height 1 of the form $D, \Theta \rightarrow \Lambda, D$. There are four cases we should consider:

1. the l.h.s. (left hand side) distinguished occurrence of D has a direct logical path to A in Π_*, while the r.h.s. (right hand side) distinguished occurrence of D has a direct logical path to B; let C_Π to be D, the proof Π^A be $D, \Theta^A \rightarrow \Lambda^A, D$ and Π^B be $D, \Theta^B \rightarrow \Lambda^B, D$, where Θ^A, Λ^A and Θ^B, Λ^B are formulas of Θ, Λ with a direct logical path to A and to B respectively (this notation will be kept for the following). Notice that each formula in Θ, Λ has a logical path either to A or to B because there are no cuts in the proof.

2. the l.h.s. distinguished occurrence of D has a direct logical path to B, while the r.h.s. distinguished occurrence of D has a direct logical path to A; let C_Π be $\neg D$, the proof Π^A be
$$\frac{D, \Theta^A \rightarrow \Lambda^A, D}{\Theta^A \rightarrow \Lambda^A, D, \neg D}$$
and Π^B be
$$\frac{D, \Theta^B \rightarrow \Lambda^B, D}{\neg D, D, \Theta^B \rightarrow \Lambda^B}$$

3. both the l.h.s. and r.h.s. occurrences of D have a direct logical path to A; let C_Π be $\bot$ and define Π^A to be $D, \Theta^A \rightarrow \Lambda^A, D, \bot$ and Π^B to be $\bot, \Theta^B \rightarrow \Lambda^B$.

4. both the l.h.s. and r.h.s. occurrences of D have a direct logical path to B; let C_Π be $\top$, define Π^A to be $\Theta^A \to \Lambda^A, \top$ and Π^B to be $\top, D, \Theta^B \to \Lambda^B, D$.

For subproofs Π of height $k > 1$ we will examine the last rule of inference R.

Suppose R is a $\vee$:*left* rule of the form

$$\frac{\begin{array}{c}\Pi_1\\ D, \Theta_1 \to \Lambda_1\end{array} \quad \begin{array}{c}\Pi_2\\ E, \Theta_2 \to \Lambda_2\end{array}}{D \vee E, \Theta_{1,2} \to \Lambda_{1,2}}$$

By induction hypothesis there are two pairs of proofs Π_1^A, Π_2^A and Π_1^B, Π_2^B and two formulas C_{Π_1}, C_{Π_2} such that $L(C_{\Pi_1}), L(C_{\Pi_2}) \subset^+ L(A) \cap L(B)$. We will use this information to build $\Pi^A : \Gamma_\Pi^A \to \Delta_\Pi^A, C_\Pi$ and $\Pi^B : C_\Pi, \Gamma_\Pi^B \to \Delta_\Pi^B$, and the interpolant C_Π. There are two cases.

1. the main formula $D \vee E$ has a direct logical path to A. Let C_Π be $C_{\Pi_1} \vee C_{\Pi_2}$ and define Π^A to be

$$\frac{\dfrac{\dfrac{\begin{array}{c}\Pi_1^A\\ D, \Theta_1^A \to \Lambda_1^A, C_{\Pi_1}\end{array}}{D, \Theta_1^A \to \Lambda_1^A, C_{\Pi_1} \vee C_{\Pi_2}} \quad \dfrac{\begin{array}{c}\Pi_2^A\\ E, \Theta_2^A \to \Lambda_2^A, C_{\Pi_2}\end{array}}{E, \Theta_2^A \to \Lambda_2^A, C_{\Pi_1} \vee C_{\Pi_2}}}{D \vee E, \Theta_{1,2}^A \to \Lambda_{1,2}^A, C_{\Pi_1} \vee C_{\Pi_2}, C_{\Pi_1} \vee C_{\Pi_2}}}{D \vee E, \Theta_{1,2}^A \to \Lambda_{1,2}^A, C_{\Pi_1} \vee C_{\Pi_2}}$$

and Π^B to be

$$\frac{\begin{array}{c}\Pi_1^B\\ C_{\Pi_1}, \Theta_1^B \to \Lambda_1^B\end{array} \quad \begin{array}{c}\Pi_2^B\\ C_{\Pi_2}, \Theta_2^B \to \Lambda_2^B\end{array}}{C_{\Pi_1} \vee C_{\Pi_2}, \Theta_{1,2}^B \to \Lambda_{1,2}^B}$$

where Θ_Π^A is $\Theta_{1,2}^A$, Λ_Π^A is $\Lambda_{1,2}^A$, Θ_Π^B is $\Theta_{1,2}^B$, Λ_Π^B is $\Lambda_{1,2}^B$. Clearly, $L(C_{\Pi_1} \vee C_{\Pi_2}) \subset^+ L(A) \cap L(B)$.

2. the main formula $D \vee E$ has a direct logical path to B. Let C_Π be $C_{\Pi_1} \wedge C_{\Pi_2}$ and define Π^A to be

$$\frac{\begin{array}{cc} \Pi_1^A & \Pi_2^A \\ \Theta_1^A \rightarrow \Lambda_1^A, C_{\Pi_1} & \Theta_2^A \rightarrow \Lambda_2^A, C_{\Pi_2} \end{array}}{\Theta_{1,2}^A \rightarrow \Lambda_{1,2}^A, C_{\Pi_1} \wedge C_{\Pi_2}}$$

and Π^B to be

$$\frac{\dfrac{\dfrac{\begin{array}{c}\Pi_1^B \\ D, C_{\Pi_1} \Theta_1^B \rightarrow \Lambda_1^B\end{array}}{D, C_{\Pi_1} \wedge C_{\Pi_2}, \Theta_1^B \rightarrow \Lambda_1^B} \quad \dfrac{\begin{array}{c}\Pi_2^B \\ E, C_{\Pi_2}, \Theta_2^B \rightarrow \Lambda_2^B\end{array}}{E, C_{\Pi_1} \wedge C_{\Pi_2}, \Theta_2^B \rightarrow \Lambda_2^B}}{D \vee E, C_{\Pi_1} \wedge C_{\Pi_2}, C_{\Pi_1} \wedge C_{\Pi_2}, \Theta_{1,2}^B \rightarrow \Lambda_{1,2}^B}}{D \vee E, C_{\Pi_1} \wedge C_{\Pi_2}, \Theta_{1,2}^B \rightarrow \Lambda_{1,2}^B}$$

If R is a $\wedge$:*right* rule the way to build the formula C_* and the proofs associated to it is symmetric to the case we just discussed. Let now R be a $\vee$:*right* rule of the form

$$\frac{\begin{array}{c}\Pi_1 \\ \Theta \rightarrow \Lambda, D\end{array}}{\Theta \rightarrow \Lambda, D \vee E}$$

By induction hypothesis there are two proofs $\Pi_1^A : \Gamma_1^A \rightarrow \Delta_1^A, C_{\Pi_1}$ and $\Pi_1^B : C_{\Pi_1}, \Gamma_1^B \rightarrow \Delta_1^B$ and a formula C_{Π_1} such that $L(C_{\Pi_1}) \subset^+ L(A) \cap L(B)$. We will use this information to build Π^A, Π^B and the interpolant C_Π (we will refer to this notation also for R being $\exists$:*left*). There are two cases.

1. the main formula $D \vee E$ has a direct logical path to A. Let C_Π be C_{Π_1} and define Π^A to be

$$\frac{\begin{array}{c}\Pi_1^A \\ \Theta^A \rightarrow \Lambda^A, D, C_{\Pi_1}\end{array}}{\Theta^A \rightarrow \Lambda^A, D \vee E, C_{\Pi_1}}$$

and Π^B as Π_1^B.

2. the main formula $D \vee E$ has a direct logical path to B. Define C_Π to be C_{Π_1}, Π^A to be Π_1^A and Π^B as

$$\frac{\begin{array}{c}\Pi_1^B\\ C_{\Pi_1}, \Theta^B \rightarrow \Lambda^B, D\end{array}}{C_{\Pi_1}, \Theta^B \rightarrow \Lambda^B, D \vee E}$$

If R is a $\neg$:*right* or $\neg$:*left* applied to Π_1, then C_Π is defined as C_{Π_1} and the proofs Π^A, Π^B are built with the same ideas already used in the above cases.

Suppose R is a $\exists$:*left* of the form

$$\frac{\begin{array}{c}\Pi_1\\ D(b), \Theta \rightarrow \Lambda\end{array}}{(\exists x)D(x), \Theta \rightarrow \Lambda}$$

then we have to consider two cases.

1. the main formula $(\exists x)D(x)$ has a direct logical path to A. Let C be $(\exists x)C_1(x)$ (where x quantifies on the occurrences of the variable b in $C_1(b)$, if any) and define Π^A to be

$$\frac{\dfrac{\begin{array}{c}\Pi_1^A\\ D(b), \Theta^A \rightarrow \Lambda^A, C_1\end{array}}{D(b), \Theta^A \rightarrow \Lambda^A, (\exists x)C_1}}{(\exists x)D(x), \Theta^A \rightarrow \Lambda^A, (\exists x)C_1}$$

and Π^B as

$$\frac{\begin{array}{c}\Pi_1^B\\ C_1, \Theta^B \rightarrow \Lambda^B\end{array}}{(\exists x)C_1, \Theta^B \rightarrow \Lambda^B}$$

2. the main formula $(\exists x)D(x)$ has a direct logical path to B. Let C be $(\forall x)C_1$ and define Π^A to be

$$\frac{\begin{array}{c}\Pi_1^A\\ \Theta^A \rightarrow \Lambda^A, C_1\end{array}}{\Theta^A \rightarrow \Lambda^A, (\forall x)C_1}$$

and Π^B to be

$$\cfrac{\cfrac{\cfrac{\Pi_1^B}{D(b), C_1, \Theta^B \to \Lambda^B}}{D(b), (\forall x)C_1, \Theta^B \to \Lambda^B}}{(\exists x)D(x), (\forall x)C_1, \Theta^B \to \Lambda^B}$$

If R is either a $\exists$:*right* or a contraction rule applied to Π_1, then C is defined as C_1. The proofs Π^A, Π^B are built similarly to the cases discussed above.

Call C_*, Π_*^A, Π_*^B respectively, the formula C_{Π_*} and the proofs of $A \to C_{\Pi_*}, C_{\Pi_*} \to B$. To conclude the proof, we should map C_*, Π_*^A, Π_*^B into C, Π^A, Π^B expressed in the language L. If there is a predicate common to A and B, the formula C_* can be transformed into a formula C of L as follows. Let R be a k-ary predicate letter common to A and B and let R' be the formula $\forall y_1 \ldots \forall y_k R(y_1 \ldots y_k)$, where $y_1, \ldots, y_k$ are new bound variables. By replacing $\top$ by $\neg R' \vee R'$ and $\bot$ by its negation (i.e. $\neg(\neg R' \vee R')$), we can transform C_* into the desired interpolant C. The proofs $\Pi_*^A : A \to C_*$ and $\Pi_*^B : C_* \to B$ can be easily transformed into two proofs $\Pi^A : A \to C$ and $\Pi^B : C \to B$, where $\Theta \to \Lambda, \top$ and $\bot, \Theta \to \Lambda$ have been replaced by LK-proofs of $\Theta \to \Lambda, \neg R' \vee R'$ and $\neg(\neg R' \vee R'), \Theta \to \Lambda$ respectively.

If there is no predicate common to A and B, then notice that C_* is constituted by $\top$, $\bot$ and logical symbols only. By induction on the complexity of C_*, it can easily be shown (see Lemma 35 below) that either $\to C_*$ or $C_* \to$ is provable. Hence either $A \to$ or $\to B$ is provable.

This concludes the proof. □

Corollary 31 *Let* $\Pi : A \rightarrow B, C, \Pi^A, \Pi^B$ *be defined as in Theorem 29. Then, if a s-formula* D *in* A *has a path to a variant* D' *of* B *in* Π *then* D *occurs positively (negatively) in* A *iff* D' *occurs positively (negatively) in* B *iff there exists a variant of* D *and* D' *that occurs positively (negatively) in* C *and has a path to* D *and* D' *in* Π^A, Π^B*, respectively.*

Proof. This is a direct consequence of the way in which the interpolant has been built in the proof of Theorem 29. □

Notice that the original statement of the theorem can be strengthened considering any arbitrary sequent $\Gamma \rightarrow \Delta$. In fact this is our induction hypothesis.

Remark. Our proof is not essentially different from the ones proposed by Girard ([Gir87]) and Maehara (see [Tak75]). We believe though that the explicit use of flows in our construction gives a better understanding of the relations between the interpolant and the formulas in the sequent $A \rightarrow B$. In particular, the sets of formulas used in both the mentioned constructions turn out to be naturally justified by the use of flows. We will not point out any detail here. The interested reader can easily find such justifications by comparing the constructions.

4.1.2 On the complexity of the interpolants

Let the *size* of a formula A (denoted $|A|$) be inductively defined as follows: $|A|$ is 1 if A is atomic; $|A \land B| = |A \lor B| = |A| + |B| + 1$; $|\neg A| = |(\forall x)A| = |(\exists x)A| = |A| + 1$. There is a correspondence between the size of an interpolant for a tautology $A \rightarrow B$ and the complexity of a proof of it. For the first order predicate calculus with equality, it has been proved by Meyer ([Mey80]) that there is no general recursive bound on the length of the smallest interpolant. It is an open question whether or not the size of the interpolant in the propositional case can be bound by a polynomial function on the size of A and B[1]. The best known upper bound is exponential (see [Mun93]). We believe that properties of logical paths, correspondingly can point out in which sense certain tautologies are "easier" to prove than others and, why do they have simple interpolant (for a discussion concerning related topics see [Urq92]).

In this direction, we will show that if A (respectively B) has a "relatively simple construction" in Π, then the size of the interpolant for $A \rightarrow B$ is linearly bounded by the size of A. Note that the result is shown for the full predicate calculus and not only for the propositional case.

Our claim is precisely stated as follows

Theorem 32 *Let $\Pi : A \rightarrow B$ be a proof in LK (possibly with cuts); suppose there are no bridges from A back to A in Π (from B back to B, respectively). Then there is an interpolant C for $A \rightarrow B$ such that $|C| \leq (2k+5) \cdot |A|$ ($|C| \leq (2k+5) \cdot |B|$, respectvely), where k is*

[1] Let Σ be an alphabet and regard boolean expressions as words over Σ. Let Σ^* be the set of words over Σ and $TAUT \subset \Sigma^*$ be the set of tautologies. In [Mun84] it is shown that one of the following sentences is true:

1. $TAUT$ is accepted in deterministic polynomial time (viz. $NP = P$);
2. $TAUT$ is not accepted in non-deterministic polynomial time (viz. NP is not closed under complementation);
3. interpolation is polynomially intractable, i.e. for every function $\phi : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$, if ϕ is computable in deterministic polynomial time then for some tautology $B \rightarrow C$, $\phi(B, C)$ fails to be an interpolant for $B \rightarrow C$.

the arity of some predicate symbol in A, B. *Moreover,* $N(\Pi^A) \leq 4 \cdot |A|$ *and* $N(\Pi^B) \leq N(\Pi)$ *where* $\Pi^A : A \rightarrow C$ *and* $\Pi^B : C \rightarrow B$.

To show this we need some more definitions and considerations on logical flow graphs. As for the proof of theorem 29, we will extend the first order language L in which Π_* is formalized with the atomic formulas $\top$, $\bot$ and the system LK with the new axioms $\Theta \rightarrow \Lambda, \top$ and $\bot, \Theta \rightarrow \Lambda$. We call the new language and the new system L^+ and LK^+, respectively.

Definition 33 Let B be a formula in L. A *variation* B^* of B is a formula in L^+ obtained by substituting in B none, one or more of its s-formulas with $\top$ or $\bot$ as follows

1. if C is an s-formula that occurs *positively* in B then C is replaced by $\top$;
2. if C is an s-formula that occurs *negatively* in B then C is replaced by $\bot$.

Clearly, there are more than one variation associated to a given formula B.

Given a variation B^*, we denote ${}^*B$ the formula obtained from B^* replacing *all* occurrences of $\top, \bot$ with $\bot, \top$ respectively. For instance, if $\top \wedge B$ is the variation $(A \wedge B)^*$ then $\bot \wedge B$ will be also denoted ${}^*(A \wedge B)$.

Notice that a variation $(\neg B)^*$ of $\neg B$ can also be written as $\neg{}^*B$ and the formula ${}^*(\neg B)$ as $\neg B^*$, for some variation B^*.

Lemma 34 *Let* A *be a formula in* L. *For all variations* A^* *of* A *we have that the sequents* $A \rightarrow A^*$ *and* ${}^*A \rightarrow A$ *are* LK^+*-provable with a proof* Π *such that* $N(\Pi) \leq 4 \cdot |A|$.

Proof. By induction on the size of A

$|A| = 1$: If A^* is A then the claim is obviously satisfied since $A \rightarrow A$ is an axiom of LK; if A^* is $\top$ then $^*A$ is $\bot$ and the claim holds because $A^* \rightarrow \top$ and $\bot \rightarrow^* A$ are axioms;

$|A| > 1$: We will discuss in detail only the case in which A is of the form $\neg B$. The other cases can be handled similarly.

If A is of the form $\neg B$ and $(\neg B)^*$ is an arbitrary variation of it, we want to show that $\neg B \rightarrow (\neg B)^*$ and $^*(\neg B) \rightarrow \neg B$ are LK^+-provable sequents.

By induction we know that $B \rightarrow B^*$ and $^*B \rightarrow B$ are LK^+-provable sequents, for all variations B^* of B.

Then, for all pair of variations B^* it is easy to derive the sequent $\neg B \rightarrow \neg^* B$ from $^*B \rightarrow B$, and the sequent $\neg B^* \rightarrow \neg B$ from $B \rightarrow B^*$. Hence, the sequents $\neg B \rightarrow (\neg B)^*$ and $^*(\neg B) \rightarrow \neg B$ are LK^+-provable for all variations $(\neg B)^*$.

The bound on the number of lines of a proof of $A \rightarrow A^*$ or $^*A \rightarrow A$ is easy to obtain observing that to introduce a binary connective, we need 4 rule applications. □

Lemma 35 *Let A be a formula in L and A^* the variation of it made up of $\top, \bot$ and logical symbols only. Then the sequents $\rightarrow A^*$ and $^*A \rightarrow$ are LK^+-provable.*

Proof. By an easy induction on the complexity of A. □

Observe that in a sequent $A_1 \ldots A_k \rightarrow B_1 \ldots B_l$ all formulas A_i (for $i = 1 \ldots k$) appear negatively in the sequent. This justifies the statement of the following lemma (with respect to definition 33).

Lemma 36 *Let $\Pi : S$ be a LK^+-proof and let A be an s-formula in L (i.e. A is neither $\top$ or $\bot$) appearing negatively (resp. positively) in S. Then either there is a bridge between A and a variant of it in S or the sequent S' obtained by replacing A with $\top$ (resp. $\bot$) is valid.*

Proof. Let A be an s-formula occurring negatively in S and suppose there is no bridge to S starting from A. The case in which A occurs positively is handled similarly.

Transform $\Pi : S$ into $\Pi' : S'$ by replacing A and all its variants (linked to A by the logical flow graph) by $\top$. The logical flow graph of Π' is essentially the same as the logical flow graph of Π; the only difference concernes the sequence of edges associated to A (in Π), that in Π' is associated to $\top$ (because of the renaming).

We have to show that Π' *is* a proof. We discuss only few crucial cases; the others are treated similarly.

First, where Π has an axiom $C \to C$, Π' might contain $C' \to C''$, where C', C'' are obtained from C by replacing some variant of A by $\top$. Since the logical flow in Π links all the corresponding pairs of s-formulas in the two occurrences of C, we have that C'' must be C' (then we have $C' \to C'$ that is an axiom).

Second, where Π has a contraction, Π' might contain

$$\frac{\Gamma \to \Delta, C', C''}{\Gamma \to \Delta, C'''}$$

where C', C'', C''' are obtained from the formula C replacing some variant of A by $\top$. By definition of logical flow graph, each s-formula positively (negatively) occurring in C''' has incoming (outgoing) edges from (to) the corresponding s-formulas occurring in C' and C''. This implies that C', C'', C''' are actually the same formula and the inference in Π' is a valid inference.

Third, where Π has a $\vee$:*right* application, Π' might contain

$$\frac{\Gamma \rightarrow \Delta, B}{\Gamma \rightarrow \Delta, B \vee C'}$$

where C' is obtained from the formula C replacing some variant of A by $\top$. Clearly the inference is correct. □

Remark. The argument we use to prove Lemma 36 is very *similar* to the one used by Sam Buss to show Proposition 6 in [Bus91] (in fact, Proposition 6 could be stated with respect to LK^+ and our statement derived as a corollary from it; note that Proposition 6 is stated for LK plus the equality axioms).

Proof. (Theorem 32) Apply Lemma 36 repeatedly to all s-formulas in A that do not have a bridge to some variant in $A \rightarrow B$ in Π. In this way one obtains the proof $\Pi' : A^* \rightarrow B$. Notice that by hypothesis A does not have bridges to itself, so all s-formulas in A^* are either linked to some variant in B or their form is $\top, \bot$. This means that all predicates occurring in A^* are common to A and B. By Lemma 34 we also know that $A \rightarrow A^*$ is provable; and by definition of variation, the size of A^* is the same as the size of A. Now we need just to transform A^* into a formula C of the original language L. Let R be a k-ary predicate letter common to A and B and let R' be the formula $\forall y_1 \ldots \forall y_k R(y_1 \ldots y_k)$, where $y_1, \ldots, y_k$ are new bound variables. By replacing $\top$ by $\neg R' \vee R'$ and $\bot$ by its negation (i.e. $\neg(\neg R' \vee R')$), we can transform C_* into the formula C_*, i.e. the desired interpolant. Since $|A^*| = |A|$ then by the transformation we have that $|C| \leq (2k+5) \cdot |A|$, where k is the arity of some predicate in L.

This concludes the proof. □

4.1.3 Splitting a proof

The definition of good flow given in chapter 3 will be used in this section. We work here in the system LK that is contained in T_F. Following the steps in the proof of Lemma 21 one can show

Theorem 37 *There is an effective procedure that transforms every LK-proof $\Pi : S$ into a derivation $\Pi' : S$ with no cuts. Moreover if Π' has a good flow with base $H'(S)$ then Π has a good flow with base $H(S) = H'(S)$.*

This result is crucial to obtain the bounds on the complexity of the proofs in the following

Theorem 38 *If $\Pi : A \rightarrow B$ (possibly with cuts) is a proof in LK and there are no bridges from (to) A to (from) B then there exists either a proof $\Pi' : A \rightarrow$ or $\Pi' : \rightarrow B$ such that $N(\Pi') \leq N(\Pi)$.*

Notice that whenever the languages of A and B are disjoint, the claim says that we can always find either a proof of $A \rightarrow$ or a proof of $\rightarrow B$ with complexity bounded by the complexity of the original proof. This result cannot be obtained from the construction used to prove the Craig Interpolation Theorem because the proof Π may contain cuts.

To show the theorem we need the following proposition

Proposition 39 *Let* $\Pi : A \to B$ *be a cut-free proof in LK; assume there are no bridges from* A *to* B *in* Π *then there exists either a good flow* $\mathcal{F}^A$ *or a good flow* $\mathcal{F}^B$ *defined by all full paths originated in* A *or in* B*, respectively.*

Proof. Since there are no bridges from A to B, nor from B to A, we will show that each subproof of Π has associated to it either a flow for A or a flow for B. In particular, a flow $\mathcal{F}^A$ is built if $A \to$ is provable by stages on the subproofs of Π (respectively, $\mathcal{F}^B$ is built if $\to B$ is provable).

Let Π_* be a subproof of Π of height 1 of the form $D, \Theta \to \Lambda, D$. By hypothesis there are no bridges between A and B therefore both distinguished occurrences D should have a direct path either to A or to B. Suppose they have direct paths to A; then define $\mathcal{F}^A_*$ to contain all edges between s-formulas in the distinguished occurrences D and all active formulas in Θ, Λ with a direct path to A.

Let the subproof Π_* be of the form

$$\frac{\begin{array}{cc}\Pi_1 & \Pi_2 \\ D, \Theta_1 \to \Lambda_1 & E, \Theta_2 \to \Lambda_2\end{array}}{D \vee E, \Theta_{1,2} \to \Lambda_{1,2}}$$

where the formula $D \vee E$ has a direct path to A. If both Π_1 and Π_2 have flows $\mathcal{F}^A_1, \mathcal{F}^A_2$ associated to them then we define the flow associated to the subproof Π_* as their natural extension and call it $\mathcal{F}^A_*$. If both Π_1 and Π_2 have flows $\mathcal{F}^B_1, \mathcal{F}^B_2$ associated to them, then define the natural extension of $\mathcal{F}^B_1$ over Π_* and activate in the endsequent all s-formulas active in Θ_2, Λ_2. If Π_1 has a flow $\mathcal{F}^B_1$ and Π_2 has a flow $\mathcal{F}^A_2$, define the flow associated to the subproof as the natural extension of $\mathcal{F}_1^B$ and activate in the endsequent all s-formulas active in Θ_2, Λ_2. A similar definition is given in case Π_1 has a flow for A and Π_2 has a flow for B.

The flow associated to all other binary rules is defined in a similar way. In case of a unary rule, the flow will be defined as the natural extension of the flow of the subproof.

Notice that the flow associated to a proof is defined univocally (moreover, it always exists) and this implies that either A or B are provable, by Proposition 11. □

Proof. (Theorem 38) Let $\Pi : A \rightarrow B$ be a proof in LK. Apply the cut elimination procedure to it to find a cut-free proof Π'. Apply Lemma 39 to Π' and define a good flow associated to it, say $\mathcal{F}^A$. By Theorem 37 we can show that Π has a good flow as well (notice that the base for such flow coincides with the base induced by $\mathcal{F}^A$). Apply Proposition 11 and find a proof of $A \rightarrow$ with the desired bound on the complexity of the proof. □

4.2 The Intuitionistic Sequent Calculus LJ

We can formalize the intuitionistic calculus as a subsystem of LK, which we call LJ, following Gentzen. The system LJ is obtained from LK by imposing the restriction that in a sequent $\Gamma \rightarrow \Delta$, the cedent Δ consists of at most one formula. The inferences in LJ are those in LK where the succedent of each upper and lower sequent consists of at most one formula; thus there are no inferences in LJ corresponding to a right contraction. There is an exception: the intuitionistic $\vee$:*left* rule is formulated as

$$\frac{\Gamma_1, A \to C \quad \Gamma_2, B \to C}{\Gamma_1, \Gamma_2, A \vee B \to C}$$

We will show the Craig Interpolation Theorem for LJ following essentially the same ideas introduced for the proof given for LK.

Namely, for each subproof Π of Π_* with end-sequent $\Gamma_\Pi \to \Delta_\Pi$ (where Δ_Π is an empty collection or just a formula) we show that

1. there exist subcollections $\Gamma^A_\Pi, \Delta^A_\Pi$ and $\Gamma^B_\Pi, \Delta^B_\Pi$ of Γ_Π, Δ_Π such that

   a. each formula occurrence in $\Gamma^A_\Pi, \Delta^A_\Pi$ ($\Gamma^B_\Pi, \Delta^B_\Pi$, respectively) has a direct path to A (B, respectively), and

   b. Γ_Π is $\Gamma^A_\Pi \Gamma^B_\Pi$ and Δ_Π is $\Delta^A_\Pi \Delta^B_\Pi$;

   there exists a formula C_Π such that

   a. $L(C_\Pi) \subset^+ L(A) \cap L(B)$, and

   b. either $\Gamma^A_\Pi \to C_\Pi$ and $C_\Pi, \Gamma^B_\Pi \to \Delta^B_\Pi$, or $C_\Pi, \Gamma^A_\Pi \to \Delta^A_\Pi$ and $\Gamma^B_\Pi \to C_\Pi$ are provable sequents.

For LJ the treatment turns out to be a bit more delicate than for LK because of the restrictions on the form of the sequents. Our construction will not only be dependent on the direct paths linking the main formula in Π to $A \to B$ but also on the direct path linking the r.h.s. formula in the end-sequent of Π to $A \to B$.

Note that whenever the formula on the r.h.s. of the endsequent of a subproof Π of Π_* is linked to B, the interpolant C will appear in the r.h.s. of Π^A and l.h.s. of Π^B; whenever the formula on the r.h.s. of the endsequent of a subproof of Π_* is linked to A, the interpolant C will appear in the l.h.s. of Π^A and r.h.s. of Π^B. The $\neg$:*left* and $\neg$:*right* rules will induce a degree of freedom on the construction of the interpolant. Namely, whenever the cedent Δ is empty, then two different choices can be made: either the interpolant C can be in the r.h.s. cedent of Π^A or in the l.h.s. cedent of Π^A. This decision gives rise to two different ways to interpolate and seems to correspond to the notion of negative and positive interpolation introduced by Schutte.

4.2.1 Intuitionistic Interpolation Theorem

We will assume that, whenever there is no r.h.s. formula in an end-sequent of a given subproof Π of Π_*, the formula C_Π will appear in the r.h.s. cedent in Π^A and in the l.h.s. cedent in Π^B.

The formula C_Π and proofs Π^A, Π^B relative to subproofs of height 1 are built as follows. There are four cases we should consider:

1. the l.h.s. distinguished occurrence of D has a logical flow to A, while the r.h.s. distinguished occurrence of D has a logical flow to B; let C_Π to be D, the proof Π^A be $D, \Theta^A_\Pi \rightarrow D$ and Π^B be $D, \Theta^B_\Pi \rightarrow D$, where Θ^A and Θ^B are formulas of Θ_Π with a path to A and to B respectively (this notation will be kept for the following). Notice that each formula in Θ has a logical path either to A or to B because there are no cuts in the proof.

2. the l.h.s. distinguished occurrence of D has a logical path to B, while the r.h.s.

distinguished occurrence of D has a logical flow to A; let C_Π be D and the proof Π^A be $D, \Theta^A \rightarrow D$ and Π^B be $D, \Theta^B \rightarrow D$

3. both the l.h.s. and r.h.s. occurrences of D have a logical path to A; let C_Π be $\top$ and define Π^A to be $\top, D, \Theta^A \rightarrow D$ and Π^B be $\Theta^B \rightarrow \top$.

4. both the l.h.s. and r.h.s. occurrences of D have a logical path to B; let C_Π be $\top$ and define Π^A to be $\Theta^A \rightarrow \top$ and Π^B be $\top, D, \Theta^B \rightarrow D$.

For subproofs of height $k > 1$ we will examine the last rule of inference R.

Suppose R is a $\vee$:*left* rule of the form

$$\frac{\begin{array}{cc} \Pi_1 & \Pi_2 \\ D, \Theta_1 \rightarrow F & E, \Theta_2 \rightarrow F \end{array}}{D \vee E, \Theta_{1,2} \rightarrow F}$$

Then there are two cases. By induction there are two pairs of proofs Π_1^A, Π_2^A and Π_1^B, Π_2^B and two formulas C_{Π_1}, C_{Π_2} such that $L(C_{\Pi_1}), L(_{\Pi_2}) \subset^+ L(A) \cap L(B)$. We will use this information to build Π^A, Π^B and the formula C_Π such that

1. the main formula $D \vee E$ has a logical path to A and the formula F on the r.h.s. of the upper sequent of R has a path to A.

   Let C_Π be $C_{\Pi_1} \wedge C_{\Pi_2}$ and define Π^A to be

$$\frac{\dfrac{\dfrac{\Pi_1^A}{C_{\Pi_1}, D, \Theta_1^A \rightarrow F}}{C_{\Pi_1} \wedge C_{\Pi_2}, D, \Theta_1^A \rightarrow F} \quad \dfrac{\dfrac{\Pi_2^A}{C_{\Pi_2}, E, \Theta_2^A \rightarrow F}}{C_{\Pi_1} \wedge C_{\Pi_2}, E, \Theta_2^A \rightarrow F}}{\dfrac{C_{\Pi_1} \wedge C_{\Pi_2}, C_{\Pi_1} \wedge C_{\Pi_2}, D \vee E, \Theta_{1,2}^A \rightarrow F}{C_{\Pi_1} \wedge C_{\Pi_2}, D \vee E, \Theta_{1,2}^A \rightarrow F}}$$

and Π^B to be

$$\frac{\begin{matrix}\Pi_1^B \\ \Theta_1^B \to C_{\Pi_1}\end{matrix} \quad \begin{matrix}\Pi_2^B \\ \Theta_2^B \to C_{\Pi_2}\end{matrix}}{\Theta_{1,2}^B \to C_{\Pi_1} \wedge C_{\Pi_2}}$$

where Θ_Π^A is $\Theta_{1,2}^A$ and Λ_Π^A is F, Θ_Π^B is $\Theta_{1,2}^B$ and Λ_Π^B is $\emptyset$.

2. the main formula $D \vee E$ has a logical path to B and the formula F on the r.h.s. of the upper sequent of R has a path to A.

   Let C_Π be $C_{\Pi_1} \vee C_{\Pi_2}$ and define Π^A to be

$$\frac{\begin{matrix}\Pi_1^A \\ C_{\Pi_1}, \Theta_1^A \to F\end{matrix} \quad \begin{matrix}\Pi_2^A \\ C_{\Pi_2}, \Theta_2^A \to F\end{matrix}}{C_{\Pi_1} \vee C_{\Pi_2}, \Theta_{1,2}^A \to F}$$

   and Π^B to be

$$\frac{\dfrac{\begin{matrix}\Pi_1^B \\ D\Theta_1^B \to C_{\Pi_1}\end{matrix}}{D, \Theta_1^B \to C_{\Pi_1} \vee C_{\Pi_2}} \quad \dfrac{\begin{matrix}\Pi_2^B \\ E, \Theta_2^B \to C_{\Pi_2}\end{matrix}}{E, \Theta_2^B \to C_{\Pi_1} \vee C_{\Pi_2}}}{D \vee E, \Theta_{1,2}^B \to C_{\Pi_1} \vee C_{\Pi_2}}$$

The cases where F has a path to B and $D \vee E$ either a path to A or to B are symmetric to the ones we just discussed.

If R is a $\wedge$:*right* the formula will be $C_{\Pi_1} \wedge C_{\Pi_2}$ and the proofs Π^A and Π^B associated to it will be built similarly to the previous case. Let now R be a $\vee$:*right* rule of the form

$$\frac{\begin{matrix}\Pi_1 \\ \Theta \to D\end{matrix}}{\Theta \to D \vee E}$$

Then there are two cases. By induction there are two proofs Π_1^A and Π_1^B and an interpolant C_{Π_1}.

1. the main formula $D \vee E$ has a logical path to A.

   Let C_Π be C_{Π_1} and define Π^A to be

$$\frac{\begin{array}{c}\Pi_1^A\\ C_{\Pi_1}, \Theta^A \to D\end{array}}{C_{\Pi_1}, \Theta^A \to D \vee E}$$

   and Π^B as Π_1^B.

2. the main formula $D \vee E$ has a logical path to B. This case is symmetric to the previous one.

If R is a $\neg$:*right* of the form

$$\frac{\begin{array}{c}\Pi_1\\ D, \Theta_1 \to\end{array}}{\Theta_1 \to \neg D}$$

There are two cases we should consider.

1. the main formula $\neg D$ has a path to A. Then let C_Π be $\neg C_{\Pi_1}$, the proof Π^A be of the form

$$\frac{\dfrac{\begin{array}{c}\Pi_1^A\\ D, \Theta_1^A \to C_{\Pi_1}\end{array}}{\neg C_{\Pi_1}, D, \Theta_1^A \to}}{\neg C_{\Pi_1}, \Theta_1^A \to \neg D}$$

   and Π_1^B be

$$\frac{\begin{array}{c}\Pi_1^B\\ C_{\Pi_1}, \Theta_1^B \to\end{array}}{\Theta_1^B \to \neg C_{\Pi_1}}$$

2. the main formula $\neg D$ has a path to B. Then let C_Π be C_{Π_1}, the proof Π^A be $\Pi_1^A : \Theta_1^A \to C_{\Pi_1}$ and the proof Π^B be of the form

$$\frac{\begin{array}{c}\Pi_1^B\\ D, C_{\Pi_1}, \Theta_1^B \to\end{array}}{C_{\Pi_1}, \Theta_1^B \to \neg D}$$

The $\neg$:*left* case is symmetric to the $\neg$:*right*.

Suppose R is a $\exists$:*left* of the form

$$\frac{\begin{array}{c}\Pi_1\\ D(b), \Theta_1 \rightarrow E\end{array}}{(\exists x)D(x), \Theta_1 \rightarrow E}$$

We have to consider two cases. By induction there are two proofs Π_1^A and Π_1^B and an interpolant C_{Π_1}.

1. The main formula $(\exists x)D(x)$ has a logical path to A and E as well.

   Let C be $(\forall x)C_1$ and define Π^A to be

$$\frac{\dfrac{\begin{array}{c}\Pi_1^A\\ D(b), C_{\Pi_1}, \Theta^A \rightarrow E\end{array}}{D(b), (\forall x)C_{\Pi_1}\Theta^A \rightarrow E}}{(\exists x)D(x), (\forall x)C_{\Pi_1}, \Theta^A \rightarrow E}$$

   and Π^B as

$$\frac{\begin{array}{c}\Pi_1^B\\ \Theta^B \rightarrow C_{\Pi_1}\end{array}}{\Theta^B \rightarrow (\forall x)C_{\Pi_1}}$$

2. the main formula $(\exists x)D(x)$ has a logical path to B and E has a logical path to A.

   Let C_Π be $(\exists x)C_{\Pi_1}$ and define Π^A to be

$$\frac{\begin{array}{c}\Pi_1^A\\ C_{\Pi_1}, \Theta^A \rightarrow E\end{array}}{(\exists x)C_{\Pi_1}, \Theta^A \rightarrow E}$$

   and Π^B to be

$$\frac{\dfrac{\begin{array}{c}\Pi_1^B\\ D(b), \Theta^B \rightarrow C_{\Pi_1}\end{array}}{D(b), \Theta^B \rightarrow (\exists x)C_{\Pi_1}}}{(\exists x)D(x), \Theta^B \rightarrow (\exists x)C_{\Pi_1}}$$

The two cases where the E formula has a path to B are treated similarly.

If R is a $\exists$:*right* or a contraction rule applied to Π_1, then the interpolant C_Π is defined to be C_{Π_1}. The proofs Π^A, Π^B are built with the same ideas already used in the $\exists$:*left* case.

To conclude the proof, we should transform the formula C_* expressed in the language L^+ into a formula in L. This is done essentially as in the proof of Theorem 29 by substituting $\top$ with $\neg(R' \wedge \neg R')$. This concludes the proof.

Remark. Note that the results proved in subsections 4.1.2 and 4.1.3 hold for the system LJ as well.

4.3 The consistency of the sequent calculus

The consistency for LK can be derived directly from the corollary and the cut-elimination theorem. Nevertheless notice that the following property of logical paths holds for LK-proofs

Proposition 40 *Let Π be a LK-proof. Then there exists a bridge in Π.*

Proof. Let Π be a proof in LK and Π' be the result of the cut-elimination procedure applied to it. By induction on the height of Π' we easily see that there is a bridge for Π'. Going backwards in the cut-elimination procedure one can show that such bridge exists in Π as well (see Theorem 37). This proves the claim. □

Using the property, it is immediate to see that the empty sequent $\rightarrow$ cannot be derived in LK (if it was derivable, it should have a bridge but this is impossible since the sequent is empty), hence LK is consistent.

This proof is of interest because based on a property of flows that holds for arbitrary proofs, while the subformula property (on which the classical proofs are based) holds exclusively for cut-free proofs.

Bibliography

[Ber35] P. Bernays. Sur le platonisme dans les mathématiques. *L'Enseignement Mathématique*, 34:52–69, 1935.

[Bus91] S. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53:72–102, 1991.

[Dra85] A.G. Dragalin. Correctness of inconsistent theories with notion of feasibility. In *LNCS 208*, pages 58–79. Springer Verlag, 1985.

[Dum78a] M.E. Dummett. Wang's paradox. In *Truth and Other Enigmas*, pages 248–268. Harvard University Press, Cambridge, 1978. appeared also in *Synthese* 30:301–324, 1975.

[Dum78b] M.E. Dummett. Wittgenstein's philosophy of mathematics. In *Truth and Other Enigmas*, pages 166–185. Harvard University Press, Cambridge, 1978. appeared also in *The Philosophical Review*, Cornell University, 1959.

[EV61] A.S. Esenin-Volpin. Le programme ultra-intuitionniste des fondements des mathématiques. In *Infinitistic Methods, Proceedings of the Symposium on the*

Foundations of Mathematics, pages 201–223. PWN. Warsaw, 1961.

[EV70] A.S. Esenin-Volpin. The ultra-intuitionistic criticism and the antitraditional program for foundations of mathematics. In A. Kino, J. Myhill, and R.E. Vesley, editors, *Intuitionism and Proof Theory*, pages 3–45. North-Holland, 1970.

[Far84] W.M. Farmer. *Length of Proofs and Unification Theory*. PhD thesis, University of Wisconsin-Madison, 1984.

[Gan82] R.O. Gandy. Limitation to mathematical knowledge. In D. van Dalen, D. Lascar, and J. Smiley, editors, *Logic Colloquium 80*, pages 129–146. North-Holland Publishing Company, 1982.

[Gir87] J.Y. Girard. *Proof Theory and Logical Complexity*, volume 1 of *Studies in Proof Theory, Monographs*. Bibliopolis, 1987.

[Kle88] S.C. Kleene. *Introduction to Metamathematics*, volume 1 of *Bibliotheca Mathematica, Monographs on Pure and Applied Mathematics*. Groningen, Walters-Noordhoff, 1988.

[Kra87] J. Krajíček. Generalizations of proofs. In *Proceedings of the 5th Eastern Conference in Model Theory*. 1987. Wendisch-Rietz.

[Kra89] J. Krajíček. On the number of steps in proofs. *Annals of Pure and Applied Logic*, 41:153–178, 1989.

[Kre69] G. Kreisel. Axiomatizations of nonstandard analysis that are conservative extensions of formal systems for classical standard analysis. In W.A.J. Luxemburg, editor, *Application of Model Theory*, pages 93–106. Holt, Rinehart and Winston, New York, 1969.

[Kre71] G. Kreisel. A survey of proof theory ii. In J.E. Fenstad, editor, *Proceedings Second Scandinavian Logic Symposium*, pages 109–170. 1971.

[Man09] G. Mannoury. *Methodologisches und Philosophisches zur Elementar-Mathematik.* Visser, Haarlem, 1909.

[Mey80] A.R. Meyer. A note on the length of craig's interpolants. Technical report, Laboratory for Computer Science, M.I.T., October 1980.

[Mun84] D. Mundici. Np and craig's interpolation theorem. In G. Longo G. Lolli and A. Marcja, editors, *Logic Colloquium '82*. Elsevier Science Publishers - North Holland, 1984.

[Mun93] D. Mundici. A quadratic lower bound for the complexity of boolean interpolants. Technical report, Department of Computer Science, University of Milan, 1993.

[Nel86] E. Nelson. *Predicative Arithmetic.* Princeton University Press, Princeton, New Jersey, 1986.

[Ore84] V.P. Orevkov. Reconstruction of the proof from its scheme. In *Proceedings of the 7th Conference in Mathematical logic*, page 133. 1984. Russian abstract.

[Ore87] V.P. Orevkov. Reconstruction of the proof from its analysis. *Dokl. Akad. Nauk.*, 293 2:313–316, 1987.

[Par69] R. Parikh. A conservation result. In W.A.J. Luxemburg, editor, *Application of Model Theory*, pages 107–108. Holt, Rinehart and Winston, New York, 1969.

[Par71] R. Parikh. Existence and feasibility in arithmetic. *Journal of Symbolic Logic*, 36:494–508, 1971.

[Par73] Rohit Parikh. Some results on the length of proofs. *Transactions of the American Mathematical Society*, 177:29–36, 1973.

[Par83] R. Parikh. The problem of vague predicates. In R.S. Cohen and M.W. Wartofsky, editors, *Language, Logic and Method*, pages 241–261. 1983.

[Poi13] H. Poincaré. *The Foundations of Science*. Science Press, 1913.

[Pra71] D. Prawitz. Ideas and results in proof theory. In J.E. Fenstad, editor, *Proceedings Second Scandinavian Logic Symposium*, pages 235–307. 1971.

[Saz90] V.Yu. Sazonov. On feasible numbers. In *Proceedings of The Kleene's Conference on Mathematical Logic, Varna*, 1990.

[Sza77] M.E. Szabó. *Algebra of Proofs*. North-Holland, Amsterdam, 1977.

[Tak75] G. Takeuti. *Proof Theory*, volume 81 of *Studies in Logic and the Foundations of Mathematics*. North Holland, 1975.

[Tro90] A.S. Troelstra. Remarks on intuitionism and the philosophy of mathematics (revised version). In *Proceedings of the Congresso Internazionale "Nuovi Problemi della Logica e della Filosofia della Scienza"*, Viareggio 8-13 January, 1990.

[Urq92] A. Urquhart. Complexity of proofs in classical propositional logic. In Y.N. Moschovakis, editor, *Logic from Computer Science*, pages 597–608. Springer-Verlag, 1992.

[Vop79] P. Vopenka. *Mathematics in the Alternative Set Theory.* Teubner, Leipzig, 1979.

[Wit78] L. Wittgenstein. In R. Rhees G.H. von Wright and G.E.M. Anscombe, editors, *Remarks on the Foundations of Mathematics.* The MIT Press, Cambridge, 1978. Revised Version.

Index