Turning cycles into spirals

A. Carbone

Mathématiques/Informatique
Université de Paris XII
61 Avenue du Général de Gaulle
94010 Créteil, France

In [13] Parikh proved the first mathematical result about concrete consistency of contradictory theories. In [6] it is shown that the bounds of concrete consistency given by Parikh are optimal. This was proved by noticing that very large numbers can be actually constructed through very short proofs. A more refined analysis of these short proofs reveals the presence of cyclic paths in their logical graphs. Indeed in [6] it is shown that cycles need to exist for the proofs to be short. Here we present a new sequent calculus for classical logic which is close to Linear Logic in spirit, enjoys cut-elimination, is *acyclic* and its proofs are just *elementary* larger than proofs in LK. The proofs in the new calculus can be obtained by a *small perturbation* of proofs in LK and they represent a geometrical alternative for studying structural properties of LK-proofs. They satisfy the constructive disjunction property and most important, simpler geometrical properties of their logical graphs. The geometrical counterpart to a cycle in LK is represented in the new setting by a *spiral* which is passing through sets of formulas logically grouped together by the nesting of their quantifiers.

Key words: Cut elimination, Gentzen sequent calculus, cycles in proofs, structure of proofs, complexity of proofs.

1 Introduction

The structure of LK proofs presents intriguing combinatorial aspects which turn out to be very difficult to study [6,8]. It is well-known that as soon as one wants to intervene over the structure of a proof to simplify it, the complexity of the proof might increase enormously [16,12,14]. There is a link between the presence of cut formulas with *nested* quantifiers and the *non-elementary* expansion needed to prove a theorem without the help of such formulas. If one considers the graph defined by tracing the flow of occurrences of formulas (in the sense of [2]) for proofs allowing a non-elementary compression, one

finds that such graphs contain cycles [5] or almost cyclic structures[6]. These cycles codify in a *small* space (i.e. a proof with a small number of lines) all the information which is present in the proof once cuts on formulas with nested quantifiers are eliminated. See [5] for a precise discussion.

If one needs to preserve the complexity of the proof and the logical relations between the occurrences of the formulas in the proof, not much room is left for handling and simplifying the structure. Rules appearing in the proof might be moved up and down the proof structure but not much more than these operations can be actually performed and no substantial structural change can be obtained. The modifications preserve indeed the topological properties of the underlying graphs of proofs.

Yet we are interested to see whether there is a way to *perturb* slightly the graph structure to render it more transparent but at the same time keeping the complexity only *elementary* bounded. In fact, we would like to have a framework where to study the relation between the logical strength of a deduction argument and the complication of its associated proof structure. We will present here a setting where cyclic paths in proofs are eliminated and their coding effect recaptured by the interaction of *sets* of formulas in the proof. These sets of formulas will be defined through extended forms of $\forall$:*right* and $\exists$:*left* rules and their interaction will be induced by the nesting of quantifiers. Geometrically, this amounts to replacing cyclic paths by *spirals* which wind around in the proof and pass through the sets of formulas. Here the geometry of the graphs associated to LK changes because identifications of formulas usually present in short proofs of LK are not anymore required.

In the next section we introduce the notion of a logical graph of a proof. This concept is at the basis of the structural analysis of proofs in LK that we are considering here. In section 3 we introduce a new calculus (which we call ALK for 'Acyclic LK') whose logical graphs of its proofs have no cyclic paths and which is such that for any proof in LK it is possible to find a proof in ALK which is only elementary larger. We prove here the cut elimination theorem for ALK, the acyclicity property and we give precise bounds on the complexity of the transformation between the two systems. We hope that ALK will help to make progress in the understanding of phenomena linked to shortening of proofs.

2 The flow graphs of proofs

The notion of *logical flow graph* of a proof in LK has been introduced by Buss in [2] as a tool to trace the flow of occurrences of formulas in a proof. Properties of logical flow graphs are discussed in [3] where the notion is used

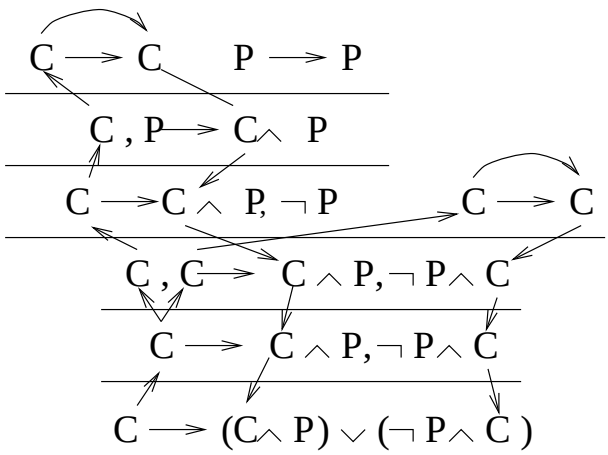

Fig. 1. Logical paths between formula occurrences in a proof

to analyse the structure of classical proofs.[1] For our purposes we use a variant of the notion of Buss, in which we restrict ourselves to *atomic* occurrences of formulas, as in [3].

We will not formally define the notion of a logical flow graph here and we address the reader to [2] and [3] instead. We will illustrate anyhow what it is through an example and an informal discussion of its properties. This will be sufficient to follow the arguments in this paper. Take the proof in Figure 1 and notice the occurrences of the atomic formula C be logically linked by the proof. Similar links exist for P. Buss considers also links between formulas which are logically more complicated, as $C \wedge P$ or $\neg P \wedge C$ for instance, but we will not need this.

The *logical flow graph* of a proof Π is the directed graph which we can read off the proof, whose nodes are labelled by the atomic occurrences of formulas in Π, and whose edges are the links induced by the rules of Π (as illustrated).

The logical flow graph carries a natural orientation, as discussed in [3]. This orientation reflects the underlying flow of information; roughly speaking, the orientation goes from *hypothesis* to *conclusions*. In the graph above, this idea is reflected in the fact that from negative occurrences of formulas in the end-sequent one reaches the positive ones following a sequence of edges (for instance, the occurrence of A on the left hand side of the sequent arrow is linked to the occurrence on the right hand side); negative occurrences in a sequent have edges going up in the proof and positive occurrences have edges going down.

Negative occurrences are linked to positive ones through axioms, and positive

[1] The idea of using the flow of occurrences to study the structure of proofs is fundamental in the work of Jean-Yves Girard [11] where graphs called *proof nets* are associated to Linear Logic proofs.

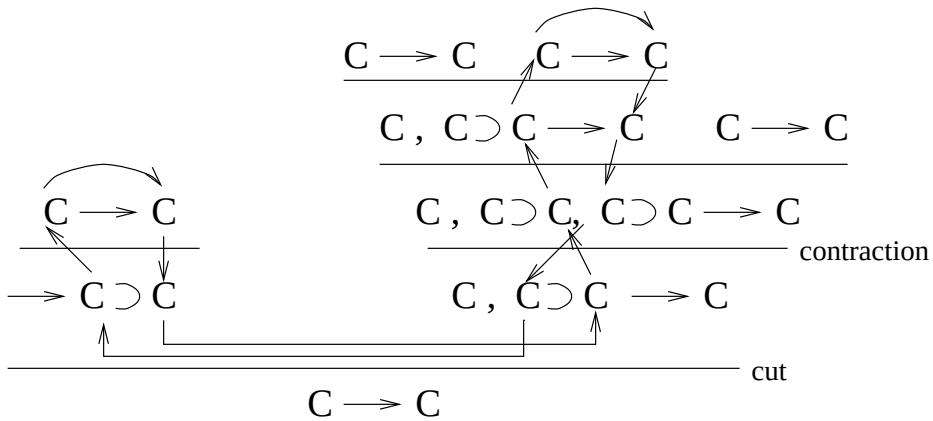

Fig. 2. A proof whose logical flow graph contains an oriented cycle

occurrences are linked to negative through cuts, as in Figure 2. In the picture we traced only some of the links between the occurrences of C to emphasize the presence of a *closed* sequence of edges in the logical graph.

We call any sequence of consecutive edges in the logical flow graph of a proof a *logical path* (two consecutive edges in this sequence should meet in a vertex which is a source for one and a sink for the other) or simply a *path*. Notice that paths are usually intended to be *oriented*. We call any logical path starting and ending with two (distinct) formulas occurring in the end-sequent of the proof a *bridge*. We call *direct path* a logical path passing through either positive or negative occurrences *only*. Notice that a direct path cannot cross an axiom or a cut, since this would force the path to pass through both positive and negative formula occurrences. Moreover, notice that the number of occurrences in a direct path is bounded by the height of Π.

We say that a formula is *directly linked* to another in a proof if there is a direct path between them. A specific occurrence of an atomic formula in a proof is called s-formula. A formula A is a *variant* of B, if A can be obtained from B by changing some (maybe none) of the terms in B. Two occurrences of formulas lying in a logical path are variants of each other (this is to say that they might not be occurrences of the *same* formula).

In [3] it is shown that cut-free proofs do not contain *cycles*, i.e. paths starting with an occurrence of a formula and going back to it. It is also proved that proofs containing cuts but no contractions are also acyclic. (Notice that the cyclic path illustrated in the example above passes through both a cut rule and a contraction rule.) From these properties it follows that the interaction between contractions *and* cuts is at the origin of the complication in proof structures. In Section 5 we will show how to transform a proof possibly containing cycles into a proof which is acyclic, by only an *elementary* expansion. This can be done by changing slightly the formal setting of LK to allow a control over the interaction between contractions and cuts (in Section 3 we

propose the system ALK). We will discriminate for this purpose certain cuts from others with respect to the well-known constructive disjunction property. It is important to keep in mind here that to ensure the elementary bound one *needs* to switch calculus. In fact in [5] it is shown that there exist provable statements whose *short* proofs *must* contain cycles. The elimination of these cycles (in LK) would force a non-elementary expansion of the proof.

3 The calculus ALK

We want to introduce here the calculus ALK (Acyclic LK) whose proofs have simpler structural properties than the proofs formulated in Gentzen's sequent calculus LK. The name has its origin in the fact that the logical graph of a proof in ALK is always *acyclic*. Given any proof in LK of a sequent one can effectively find a proof in ALK for the same sequent whose complexity is elementary in the complexity of the LK-proof (here the result holds both for number of lines and number of symbols). For the converse, the situation is much simpler. In fact, given any ALK-proof, one can find a LK-proof for the same sequent with essentially the same number of lines (and symbols).

The logical flow graph of a LK-proof which contains cycles will be transformed into a logical flow graph of a ALK-proof where cycles, roughly speaking, are replaced by *spirals*.

Being allowed for an analogy we would like to say that the effect of the transformation of Π into an ALK-proof can be seen as the effect of going from a space to its covering. This idea was indeed the origin for the formulation of ALK. In this view a proof in LK can be seen as a *projection* of a proof in ALK, where the *identification* of some of the formulas (corresponding to the identification of points of the spiral over the circle as illustrated in Figure 3) force the presence of cycles.

The importance for a calculus as ALK lies on the hope that it will tell us some more about the folding and unfolding of proofs. The combinatorics behind proofs is a very complicated mechanism (see [6,4,9]) and not at all understood. Short proofs can be thought as obtained from large ones by folding them properly, following some given order of identification of the subgraphs. Is there some general reason for which at times we might be obstructed in doing this folding? Short proofs seem special coincidences, whose existence is allowed by some elegant and 'miraculous' combinatorial phenomena. How can one find 'symmetries' in large proofs to provide short proofs from them? These are wide open questions. An analysis is found in [9].

In Section 4 we will show

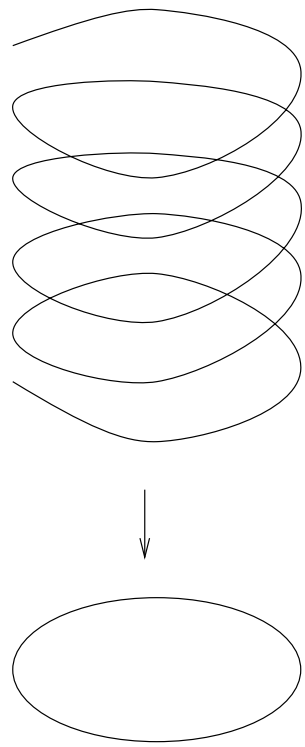

Fig. 3. A cycle as a projection of a spiral

Theorem 1 *Let $\Pi : ? \to \Delta$ be a proof in LK of n lines. There is a proof $\Pi' : ? \to \Delta$ in ALK of at most $2^{2^{\mathcal{O}(n)}}$ lines.*

The converse is also true, namely that given a proof in ALK of some sequent S there is a proof in LK for the same sequent with a number of lines which is *linear* in the number of lines of the ALK-proof. In Section 5 we will show

Theorem 2 *Let Π be a proof in ALK. The logical flow graph of Π is acyclic.*

3.1 Axioms and rules

The calculus ALK is formulated as LK except for the $\forall$:*right*, $\exists$:*left* rules and the cut rule. The latter imposes restrictions on the use of contractions in the proof. Before describing the calculus we should introduce some more terminology. Without loss of generality we do not consider the logical symbol $\supset$ since it is easily definable from the $\neg, \vee$ symbols.

Definition 3 *A contraction in Π with main formula C satisfies the* disjunction property *if for each positive disjunction (negative conjunction) in $A \vee B$ ($A \wedge B$) occurring as a subformula in C either A has only direct paths to some weak variants of A, or B has only direct paths to some weak variants of B, or both.*

Even though Definition 3 refers to both disjunctions and conjunctions we will call the property above *disjunction property* because of its obvious connection with the well-known constructive property.

The *axioms* of ALK will be sequents of the form

$$A, ? \rightarrow \Delta, A$$

where $?, \Delta$ are collections of *weak* formulas and A is atomic. (To assume atomicity is not a restriction and the assumption simplifies our exposition.)

The *logical rules* of ALK are the following:

$\neg : \mathit{left}$ $\quad \dfrac{? \rightarrow \Delta, A}{\neg A, ? \rightarrow \Delta}$ $\qquad \neg : \mathit{right}$ $\quad \dfrac{A, ? \rightarrow \Delta}{? \rightarrow \Delta, \neg A}$

$\wedge : \mathit{right}$ $\quad \dfrac{?_1 \rightarrow \Delta_1, A \quad ?_2 \rightarrow \Delta_2, B}{?_1, ?_2 \rightarrow \Delta_1, \Delta_2, A \wedge B}$

$\wedge : \mathit{left}$ $\quad \dfrac{A, ? \rightarrow \Delta}{A \wedge B, ? \rightarrow \Delta}$ $\qquad \dfrac{A, ? \rightarrow \Delta}{B \wedge A, ? \rightarrow \Delta}$

$\vee : \mathit{left}$ $\quad \dfrac{A, ?_1 \rightarrow \Delta_1 \quad B, ?_2 \rightarrow \Delta_2}{A \vee B, ?_1, ?_2 \rightarrow \Delta_1, \Delta_2}$

$\vee : \mathit{right}$ $\quad \dfrac{? \rightarrow \Delta, A}{? \rightarrow \Delta, A \vee B}$ $\qquad \dfrac{? \rightarrow \Delta, A}{? \rightarrow \Delta, B \vee A}$

$\exists : \mathit{left}_{ext}$ $\quad \dfrac{A(b), \ldots, A(b), ? \rightarrow \Delta}{(\exists x)A(x), \ldots, (\exists x)A(x), ? \rightarrow \Delta}$

$\exists : \mathit{right}$ $\quad \dfrac{? \rightarrow \Delta, A(t)}{? \rightarrow \Delta, (\exists x)A(x)}$

$\forall : \mathit{left}$ $\quad \dfrac{A(t), ? \rightarrow \Delta}{(\forall x)A(x), ? \rightarrow \Delta}$

$\forall : \mathit{right}_{ext}$ $\quad \dfrac{? \rightarrow \Delta, A(b), \ldots, A(b)}{? \rightarrow \Delta, (\forall x)A(x), \ldots, (\forall x)A(x)}$

The rules $\forall : right_{ext}$, $\exists : left_{ext}$ are extensions of the $\forall : right$ and $\exists : left$ rules of LK. Indeed, if the antecedent is constituted by only one formula then the rules coincide. We do not fix any bound on the number of auxiliary formulas in the antecedent (we think of having an infinite number of rules here). As usual, in the $\exists : left_{ext}$ and $\forall : right_{ext}$ 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. The formula B in $A \wedge B$ or $A \vee B$ in $\wedge$:*left* and $\vee$:*right* rules is called *weak* (as well as those formulas occurring in the collections $?, \Delta$ of the axioms).

The *structural rules* are

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

$$\textit{Cut} \qquad \frac{?_1 \to \Delta_1, A \quad A, ?_2 \to \Delta_2}{?_1, ?_2 \to \Delta_1, \Delta_2}$$

where we ask the auxiliary formulas of a cut rule to have direct logical paths passing *only* through contraction rules satisfying the disjunction property.

The condition on the applicability of the cut rule to a formula A in the proof is clearly *non local*, it depends indeed on the 'history' of A in the proof, on the way A has been built in the proof. This characteristic of ALK is a reminder of Linear Logic where the modalities $?, !$ help to keep track of 'past' information. (In a Linear Logic proof, the lack of modalities in a formula says that no contractions have been applied to the formula or its subformulas, i.e. the proof is linear [11].)

Notice that ALK allows contractions which do not satisfy the disjunction property but in this case, a contracted formula is required to end up in the end-sequent of the proof. It is easy to see that if contractions satisfying the disjunction property were the only contractions allowed, then ALK would not have been a calculus for classical logic. (There are classical sequents $A \to B$ for which we would only be able to prove $A, \ldots, A \to B, \ldots, B$ for some multiple repetition of A's and B's. In fact, any classical sequent could be *almost* provable except for this kind of multiplicity of occurrences.)

Theorem 4 *The calculus ALK enjoys cut-elimination.*

Sketch of proof The usual procedure of cut-elimination for LK can be applied to a proof in ALK with suitable changes concerning the $\forall : right_{ext}$ and

$\exists : \mathit{left}_{ext}$ rules. We will discuss only the case of the $\forall : \mathit{right}_{ext}$. The $\exists : \mathit{left}_{ext}$ case can be treated similarly. Suppose we have the following subproof

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ ?_1 \to \Delta_1, A(b)^1, \ldots, A(b)^r\end{array}}{?_1 \to \Delta_1, (\forall x)A(x)^1, \ldots, (\forall x)A(x)^r} \quad \dfrac{\begin{array}{c}\Pi_2\\ A(t), ?_2 \to \Delta_2\end{array}}{(\forall x)A(x), ?_2 \to \Delta_2}}{?_1, ?_2 \to \Delta_1, \Delta_2, (\forall x)A(x)^1, \ldots, (\forall x)A(x)^{r-1}}$$

If $(\forall x)A(x)^i$ for some $i = 0 \ldots r-1$ has a direct path to the endsequent, then we contract $(\forall x)A(x)^r$ with it and eliminate the cut. Otherwise all occurrences $(\forall x)A(x)^i$ end-up into some cut-formula. In this case, the cut over the occurrence $(\forall x)A(x)^r$ can be eliminated by replacing it with r cuts, one for each antecedent $A(b)^i$ of the $\forall : \mathit{right}_{ext}$ rule. This means that we will have r new cuts and r new copies of the subproof Π_2. Notice that we need to substitute the eigenvariable b with the term t, and introduce as weak formulas (using the version of Lemma 6 for LK proved in [3]) exactly $r-1$ occurrences of $(\forall x)A(x)$ also.

It is routine to check that an ALK-proof is transformed by the steps of reduction into another ALK-proof. For this we need to check that the new contractions and new weak formulas added in the proof do not introduce some *new* unwanted contraction, i.e. some contraction which does not satisfy the disjunction property and will end up into some cut-formula.

Since at each step of transformation the procedure does not touch contractions lying above the cut being examined, we are sure that these contractions will not become unwanted (we use here the fact that to check the disjunction property one only needs to look at paths going towards the axioms). Hence, let us look first at those contractions that have been introduced as *new*. They are applied to pairs of formulas coming from copies of the same subproof. If the formulas in the pair were to satisfy the disjunction property, then their contraction would also satisfy the property because the formulas have the same 'history' (again, we use here the fact that to check the disjunction property one only needs to look at paths going towards the axioms). If the property was not satisfied by the pair, it would continue not to be satisfied by the contracted formula. But in this latter case, we are sure that the contracted formula would have a path to the end-sequent, because by induction on the construction the formulas in the pair have to have a direct path to the end-sequent.

Notice now that the introduction of *new* weak formulas added in the proof during the procedure might induce some contraction occurring later in the proof (i.e. below the cut being examined) to be affected. Namely it might happen that some contraction which was not satisfying the disjunction property at

step i in the procedure, would start to enjoy it at step $i+1$ because of these changes. This does not cause any problem.

It is important to remark here that the procedure of cut-elimination we defined above for $\forall : right_{ext}$ (and similarly for $\exists : left_{ext}$) is introducing r cuts only when *all* the antecendents are directly linked to cut-formulas. This makes possible the application of these cuts. In fact, if some antecedent of the $\forall : right_{ext}$ rule was not ending-up into a cut-formula, then we could not be sure that a cut could be applied to such occurrence. This occurrence could possibly not satisfy the disjunction property. $\square$

The calculus ALK is reminder of *constructive* logics. In fact, we could have defined ALK in such a way that not only the *disjunction* property needs to be satisfied for a cut to be applied but also an analogue of the usual *existential* property. We could have asked, for instance, that for each contraction formula C in a proof Π and for each atomic $B(x)$ occurring as a subformula in C, any pair of variants $B(t_1)$, $B(t_2)$ in Π lying along two distinct direct paths from $B(x)$ are such that $t_1 = t_2\sigma$ or $t_2 = t_1\sigma$, for some substitution σ.

With this further restriction on the applicability of cuts, we would nevertheless be able to prove the cut-elimination theorem for ALK, an analogue of Theorem 1 (with the same elementary bounds) and the acyclicity property. The proofs would be essentially the same. We avoided treating explicitly this extra condition because the existential property does not seem to be a central matter for studying the complication of the logical flow graph of proofs. For instance, the acyclicity property turns out to have a propositional nature, being a consequence of the disjunction property. This reflects the fact that the logical flow graph of a proof is concerned with atomic occurrences only, independently of the way quantifiers are playing a role in the logic.

4 From proofs in LK to proofs in ALK

In this section we show that any proof in LK can be transformed into a proof in ALK with an elementary increase of the size of the proof. Theorem 1 is an immediate consequence of the more precise bound we compute. The symbol $N(\Pi)$ will denote the number of lines in the proof Π.

Theorem 5 *Let $\Pi : S$ be a proof in LK. Suppose that Π contains c contractions which do not satisfy the disjunction property and have direct paths to cut-formulas. Then there is a proof $\Pi' : S$ in ALK such that $N(\Pi') \leq 3 \cdot 2^{2^c} \cdot N(\Pi)$.*

Before giving the proof we need to show a few easy structural lemmas for proofs in ALK. Similar statements are provable for proofs in LK. Their proofs are essentially the same.

Lemma 6 (Addition of weak occurrences) *Let $\Pi : ? \to \Delta$ be a ALK-proof of k lines and Λ, Θ be multisets. An ALK-proof $\Pi' : ?, \Lambda \to \Delta, \Theta$ can be constructed such that $N(\Pi') = N(\Pi)$.*

PROOF. 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 immediate subproofs of Π whenever R is binary, or to the only one immediate subproof whenever R is unary; apply again the rule R to the result. Notice that we may have to rename variables to handle the cases $\exists$:$left_{ext}$ and $\forall$:$right_{ext}$ (but this can be done as described in [15]). Since the structure of Π' is essentially the same as the structure of Π (the only difference lies in the presence of weak occurrences Λ, Θ in Π') we have that $N(\Pi') = N(\Pi)$. $\square$

Lemma 7 (Elimination of weak occurrences) *Let $\Pi : S$ be an ALK-proof of n lines and A a weak occurrence of a formula in S (i.e. A comes from a weak occurrence lying in some axiom of Π). Let S' be the result of omitting A from S. Then an ALK-proof $\Pi' : S'$ can be constructed such that $N(\Pi') = N(\Pi)$.*

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). It follows that the tree-like structure of Π' is the same as the tree-like structure of Π and then $N(\Pi') = N(\Pi)$. $\square$

Lemma 8 *Let $\Pi : S$ be proof in ALK of k lines. Then there is a proof $\Pi' : S$ in ALK of at most k lines such that it never happens that an auxiliary formula of a binary rule is weak, or that the auxiliary formula of a unary logical rule is weak, or that an auxiliary formula of a contraction rule, $\exists$:$left_{ext}$ rule or $\forall$:$right_{ext}$ rule is weak. Furthermore, if Π is cut-free then Π' is cut-free.*

PROOF. This is proved by induction on the height of the proof Π. Suppose that the last rule of inference of Π is a binary rule where at least one of the auxiliary formulas is weak. Suppose a $\wedge$:*right* rule (similarly for $\vee$:*left* and cut rules) is applied to the subproofs $\Pi_1 : ?_1 \to \Delta_1, A$ and $\Pi_2 : ?_2 \to \Delta_2, B$, where A is a weak occurrence in Π_1. By eliminating A from Π_1 (using Lemma 7) and adding (using Lemma 6) to the resulting proof weak occurrences $?_2, \Delta_2, A \wedge B$

we obtain a proof with the same number of lines as Π_1 of the sequent $?_1, ?_2 \rightarrow \Delta_1, \Delta_2, A \wedge B$. Let Π' be such a proof.

Suppose now that the last rule of inference of Π is a unary logical rule applied to a weak auxiliary formula. Suppose that a $\wedge$:*left* rule (similarly for $\vee$:*right*) is applied to the subproof $\Pi_1 : A, ?_1 \rightarrow \Delta_1$, where A is a weak occurrence in Π_1. We first eliminate A from Π_1 (using Lemma 7) and then we add the weak formula $A \wedge B$ (using Lemma 6). The proof we obtain has the same number of lines as Π_1. Let it be Π'. The case of $\neg$:*right*, $\neg$:*left*, $\forall$:*left*, $\exists$:*right* rules is handled similarly.

If the last rule of inference is a contraction where one or both auxiliary formulas are weak, the treatment is similar. This is also the case for $\forall$:$right_{ext}$ and $\exists$:$left_{ext}$ rules. $\square$

Lemma 9 *Let $\Pi : S$ be an ALK-proof. Then there is an ALK-proof $\Pi' : S$ such that $N(\Pi') \leq N(\Pi)$ and $\#$ contractions$(\Pi') \leq 2 \cdot \#$ axioms(Π').*

PROOF. By Lemma 8 we may assume that every auxiliary formula for a contraction rule has some direct path to a distinguished occurrence in some axiom.

Given a formula A which appears in the proof, let $\mathcal{X}_A$ denote the set of distinguished occurrences in axioms which are linked to A by direct paths. Let $c(A)$ denote the number of times that a contraction rule was used in the history of A within the proof. (This includes contractions on subformulas in A.)

We claim now that $c(A) < |\mathcal{X}_A|$ (where $|\mathcal{X}_A|$ denotes the cardinality of the set $\mathcal{X}_A$). This is easy to check using induction. If an occurrence of a formula B is used as an auxiliary formula for a contraction rule, then $|\mathcal{X}_B| > 0$, because B cannot be weak. When two occurrences of B are contracted into each other, the corresponding $\mathcal{X}$'s are disjoint, and so the number of their elements add. One also adds 1 to the count of the number of contractions, but the strict inequality is preserved.

The total number of contractions used in the proof is the sum of $c(A)$ over all formulas A which either appear in the end-sequent or are used as cut-formulas. This is easy to see. One can also check that the sets $\mathcal{X}_A$ for these formulas are pairwise disjoint. Thus the number of contractions is strictly less than the number of distinguished occurrences in the axioms, and the proposition follows. $\square$

PROOF. (Theorem 5) In the sequel we call *non-trivial* any contraction which is directly linked to some cut-formula and does not satisfy the disjunc-

tion property. We want to show that Π can be transformed into a proof with no non-trivial contractions. The idea is to avoid non-trivial contractions by duplicating in a suitable way the proof. We will see that for each cut-formula C in Π, we will obtain a proof with many cuts on copies of the cut-formula C.

We build the proof Π' by induction on the height of subproofs of Π and we eliminate the non-trivial contractions from the top down. We will build by steps a new proof Π' (with no non-trivial contractions) which will have essentially the same logical content as Π, in the sense that its sequents will be sequents in Π but where each formula might have multiple occurrences (in the sense described below). Given a subproof $\Pi_0 : S_0$ of Π (where c_0 is the number of non-trivial contractions contained in Π_0) we find a proof $\Pi'_0 : S'_0$ which will be a subproof of Π' such that the following conditions are satisfied:

(i) the sequent S'_0 is defined as the sequent S_0 except for the number of occurrences of formulas in it (we refer to this number as the *multiplicity* of a formula) which might be greater in S'_0 than in S_0. Moreover, if an atomic subformula of a formula in S_0 has direct paths only to weak occurrences in Π_0, then each of its counterparts in S'_0 enjoys the same property, and
(ii) the multiplicity of a formula in the sequent S'_0 is bounded by 2^{c_0}. If a formula A in S'_0 has multiplicity larger than 1, then there is a direct path from the corresponding A in S_0 which goes towards the axioms in Π_0 and which crosses at least one non-trivial contraction along the way, and
(iii) if a formula A is contracted in Π'_0 and does not satisfy the disjunction property, then there is a direct path from the corresponding A in Π_0 which goes to S_0, and
(iv) the proof Π'_0 contains no non-trivial contractions, and
(v) $\#\ lines(\Pi'_0) \leq 2^{2^{c_0}} \cdot N(\Pi_0)$.

The disjunction property is nicely compatible with the inductive nature of our construction. More precisely, when we construct a proof Π'_0 we will use copies of proofs from lower stages in the construction. We might combine them using binary rules and *new* contractions might be introduced, but nothing else. By combining these constituent proofs we will not disturb the disjunction property of their contractions (this uses the fact that to verify the disjunction property of a contraction one need only look at what happens to paths going up towards the axioms). Then, to verify (iv) we will need only to verify that no *new* contraction will be non-trivial. These points will be clearer when we are in the actual construction, but it will be helpful to have this principle in mind, that only the new contractions really need to be checked.

Note that in the multiplicities of formulas everything is exactly the same, the arguments in the formulas in particular. At the end of the construction we will obtain a proof $\Pi' : S$ with no non trivial contractions and with end-sequent S with no extra multiplicities (remember that contractions applied to formu-

las directly linked to the endsequent do not need to satisfy the disjunction property).

To make the construction we proceed as follows. If Π_0 is an axiom then we take Π_0' to be Π_0. In general we assume that we are given a subproof Π_0 with at least one rule of inference and that we have already accomplished the construction for all proper subproofs of Π_0.

Suppose the last rule of inference in Π_0 is a contraction rule applied to $\Pi_1 : ? \to \Delta, C^1, C^2$. Apply the induction hypothesis to Π_1 and call this proof Π_1'. If R is non-trivial in Π then let Π_0' be Π_1'. Otherwise, Π_1' will contain a copy of C^1, C^2 with no multiplicity (this is easy to check with the definition of non-triviality; notice that the test of non-triviality has to be performed on the proof Π because of those contractions that have a direct path to the endsequent of Π and do not satisfy the disjunction property). We define Π_0' to be the proof obtained by applying the contraction rule R to C^1, C^2 in Π_1'.

Suppose the last rule of inference R of Π_0 is a unary rule, for instance let it be an $\vee$:*right* rule applied to a proof $\Pi_1 : ? \to \Delta, B$ containing c_1 non-trivial contractions. (Thus c_0 is the same as c_1 in this case.) Our induction hypothesis provides a proof Π_1' of the form $?^* \to \Delta^*, B^1, \ldots, B^r$, where $r \leq 2^{c_1}$. Apply r times the $\vee$:*right* rule to obtain a proof $\Pi_0' : ?^* \to \Delta^*, B \vee C^1, \ldots, B \vee C^r$. (Notice that we do not get non-trivial multiplicities for $B \vee C$ unless B has non-trivial multiplicity already. Also, we have added no new contractions, and the disjunctive property for the old contractions is undisturbed by our application of the rules.) It is easy to check that conditions (i)–(iv) are satisfied. For condition (v), since $r \leq 2^{c_1}$ and $\#\, lines(\Pi_1') \leq 2^{2^{c_1}} \cdot N(\Pi_1)$ we have

$$\begin{aligned}
\#\, lines(\Pi_0') &= \#\, lines(\Pi_1') + r \\
&\leq 2^{2^{c_1}} \cdot N(\Pi_1) + 2^{c_1} \\
&\leq 2^{2^{c_1}} \cdot (N(\Pi_1) + 1) \\
&= 2^{2^{c_1}} \cdot N(\Pi_0)
\end{aligned}$$

The $\wedge$:*left* rule is handled in exactly the same manner, and the negation rules as well as $\exists$:*right* and $\forall$:*left* rules are similar. We should only be a bit careful to handle $\forall$:*right* and $\exists$:*left* rules. Suppose the last rule of inference R of Π_0 is a $\forall$:*right* rule applied to a proof $\Pi_1 : ? \to \Delta, A(b)$ containing c_1 non-trivial contractions. (Again c_0 is the same as c_1 in this case.) Our induction hypothesis provides a proof Π_1' of the form $?^* \to \Delta^*, A(b)^1, \ldots, A(b)^r$, where $r \leq 2^{c_1}$. If $r = 1$ then we apply $\forall$:*right* to $?^* \to \Delta^*, A(b)$, otherwise we apply the $\forall$:$right_{ext}$ rule to the $A(b)$'s and obtain a sequent of the form $?^* \to \Delta^*, (\forall x)A(x)^1, \ldots, (\forall x)A(x)^r$. (Notice that we have added no new contractions, and the disjunction property for the old contractions is undis-

turbed.) It is easy now to check that conditions (i)–(iv) are satisfied.

Suppose the last rule of inference R of Π_0 is a binary rule, say a $\wedge$:*right* applied to $\Pi_1 : ?_1 \to \Delta_1, B$ and $\Pi_2 : ?_2 \to \Delta_2, C$, where c_1, c_2 are the number of non-trivial contractions in Π_1, Π_2 respectively, and $c_0 = c_1 + c_2$. By the induction hypothesis we have two proofs $\Pi_1' : ?_1^* \to \Delta_1^*, B^1, \ldots, B^k$ and $\Pi_2' : ?_2^* \to \Delta_2^*, C^1, \ldots, C^r$ that we can combine to build a proof $\Pi_0' : ?_1^*, ?_2^* \to \Delta_1^*, \Delta_2^*, B \wedge C^1, \ldots, B \wedge C^{k \cdot r}$. The construction is a bit delicate.

If $r = k = 1$ then Π_0' is defined by combining Π_1', Π_2' with a $\wedge$:*right* rule and

$$\begin{aligned}
\#\, lines(\Pi_0') &\leq \#\, lines(\Pi_1') + \#\, lines(\Pi_2') + 1 \\
&\leq 2^{2^{c_1}} \cdot N(\Pi_1) + 2^{2^{c_2}} N(\Pi_2) + 1 \\
&\leq 2^{2^{c_1+c_2}} \cdot (N(\Pi_1) + N(\Pi_2) + 1) \\
&= 2^{2^{c_1+c_2}} \cdot N(\Pi_0)
\end{aligned}$$

This satisfies the required properties, and so we suppose that $\max(r, k) > 1$. We will assume that $r > 1$, the other case being symmetric. To build Π_0' we first build a proof $\Pi^{B \wedge C^1} : ?_1^*, ?_2^* \to \Delta_1^*, \Delta_2^*, B^1 \wedge C^1, \ldots, B^1 \wedge C^r, B^2, \ldots, B^k$ from Π_2' and r copies of Π_1' followed by contractions on $?_1^*, \Delta_1^*, B^2, \ldots, B^k$. Note that we are adding new contractions for the first time in the construction. However it is easy to see that these contractions do not cause problems.

The main point is that the new contractions are being applied to formulas with identical histories. This is because the multiple copies of the formulas being contracted arise exactly from a duplication of subproofs; one only contracts copies of formulas which had exactly the same role in the corresponding duplicated subproofs. (That is, we contract the various copies of B^2 into one formula, but we never contract a copy of B^2 with a copy of B^3. This is very important.) The new contractions will satisfy the disjunction property if and only if their immediate ancestors already satisfied it. This is derived without too much trouble from this identical nature of the histories, and the fact that $\wedge$:*left* and $\vee$:*right* introduce a weak auxiliary formula. (The latter is used to prove the disjunction property of the contraction over connectives which were not part of an earlier contraction.)

This argument applies equally to the copies of the formulas $B_2, \ldots, B_k$ as to the formulas in $?_1^*$ and Δ_1^*. All that matters is the way that the formulas arose from duplicated subproofs. In particular the $\wedge$:*right* rule under consideration does not really play an active role in the testing of these new contractions.

Then we build a proof $\Pi^{B \wedge C^1, B \wedge C^2} : ?_1^*, ?_2^* \to \Delta_1^*, \Delta_2^*, B^1 \wedge C^1, \ldots, B^1 \wedge C^r, B^2 \wedge C^1, \ldots, B^2 \wedge C^r, B^3, \ldots, B^k$ from Π_2' and r copies of $\Pi^{B \wedge C^1}$ followed by new

contractions (as before). Recursively we build a proof $\Pi^{B\wedge C^1,\ldots,B\wedge C^k}$ and we call it Π'_0.

Let us compute the number of lines used in the proof. Let L_j denote the number of lines after j levels of the construction, i.e., $L_j = \#lines(\Pi^{B\wedge C^1,\ldots,B\wedge C^j})$, and $L_k = \#lines(\Pi'_0)$. Then we have that $L_{j+1} \leq r\cdot(L_j+1)+\#lines(\Pi'_2)$ for each $1 \leq j < k$, and $L_1 = r\cdot(\#lines(\Pi'_1)+1)+\#lines(\Pi'_2)$. When $j \geq 1$ one can check that $L_j \leq r^j\cdot\#lines(\Pi'_1)+(\sum_{i=0}^{j-1} r^i)\cdot(\#lines(\Pi'_2)+r)$ through an easy induction argument. This implies that

$$\#lines(\Pi'_0)(=L_k) \leq r^k\cdot\#lines(\Pi'_1)+\mu_k\cdot(\#lines(\Pi'_2)+r)$$

where $\mu_1 = 1$ and $\mu_k \leq r^k$ when $k > 1$. (This uses the assumption that $r > 1$.)

Combining this with our induction hypothesis we get

$$\#lines(\Pi'_0) \leq (2^{c_2})^{2^{c_1}}\cdot 2^{2^{c_1}}\cdot N(\Pi_1)+\mu_k\cdot(2^{2^{c_2}}\cdot N(\Pi_2)+2^{c_2})$$

where $\mu_1 = 1$ and $\mu_k \leq (2^{c_2})^{2^{c_1}}$ when $k > 1$. Let us check that

$$\#lines(\Pi'_0) \leq 2^{2^{c_1+c_2}}\cdot(N(\Pi_1)+N(\Pi_2)+1) = 2^{2^{c_1+c_2}}\cdot N(\Pi_0).$$

We have that $2^{(c_2+1)\cdot 2^{c_1}} \leq 2^{2^{c_1+c_2}}$ because $c_2+1 \leq 2^{c_2}$. It remains to check that $\mu_k\cdot 2^{2^{c_2}} \leq 2^{2^{c_1+c_2}}$. (This will take care of the last term too, since $2^{c_2} \leq 2^{2^{c_2}}$.)

This estimate is clear when $k = 1$. So suppose that $k > 1$, so that $c_1 > 0$ and $\mu_k\cdot 2^{2^{c_2}} = 2^{c_2\cdot 2^{c_1}+2^{c_2}}$. We need to check that $c_2\cdot 2^{c_1}+2^{c_2} \leq 2^{c_1+c_2}$. This follows easily from $c_2 \leq 2^{c_2-1}$ and the fact that $c_1 > 0$.

Thus we obtain the desired bound on $\#lines(\Pi_0)$ in this case. Notice that for this construction of Π_0 the formula $B\wedge C$ has multiplicity $k\cdot r \leq 2^{c_1+c_2}$, as required in (ii) above. There are no multiplicities unless at least one of B and C have already non-trivial multiplicity, in accordance with (i). Also the contractions that we introduced do not cause problems and this is easy to check by the same argument used before.

The other binary rule $\vee$:*left* is treated in exactly the same manner.

We are left with the case where Π_0 is obtained from a cut rule, applied to $\Pi_1 : ?_1 \to \Delta_1, C$ and $\Pi_2 : C, ?_2 \to \Delta_2$, say. We use our induction hypothesis to obtain proofs $\Pi'_1 : ?^*_1 \to \Delta^*_1, C^1, \ldots, C^k$ and $\Pi'_2 : C^1, \ldots, C^r, ?^*_2 \to \Delta^*_2$. This case is treated in practically the same manner as before. That is, we combine many copies of Π'_1 and Π'_2. We begin by taking Π'_2 and combining

it with r copies of Π'_1 using the cut rule r times and many contractions to get a proof of $?^*_1, ?^*_2 \to \Delta^*_1, \Delta^*_2, C^2, \ldots, C^k$. That is, we apply the cuts using always the occurrence C^1 of C in Π'_1 but systematically going through all the C's in Π'_2. We have made progress here because we have one fewer C on the right side and none on the left. We then combine Π'_2 with r copies of this new proof in a similar manner (with many contractions again) to get a proof of $?^*_1, ?^*_2 \to \Delta^*_1, \Delta^*_2, C^3, \ldots, C^k$. Continuing in this manner we get a proof of $?^*_1, ?^*_2 \to \Delta^*_1, \Delta^*_2$.

This is the proof Π'_0 that we want. We have exactly the same bounds for the number of lines as before, and we have not changed the multiplicities. The only other point is that all of the contractions that we introduce do not cause problems again by the same argument as before.

This completes the description of the inductive construction. It is clear now what we meant before, that to check that no non-trivial contractions are present in the proof we need only worry about the new contractions, the old contractions are not significantly affected by the additional operations.

To conclude the proof we need to apply Proposition 9 to Π'. (Here we use the fact that Lemma 8 applied to a proof containing no non-trivial contractions gives a proof which still contains no non-trivial contractions only. The procedure in Lemma 8 essentially introduces a larger number of weak occurrences, but does not add non-weak occurrences and this is compatible with the disjunction property.) We call the resulting proof Π' again. Notice that $N(\Pi') = \#\, lines(\Pi') + \#\, contractions(\Pi') \leq 3 \cdot \#\, lines(\Pi')$ by Lemma 9. $\Box$

PROOF. (Theorem 1) The number of contractions which do not satisfy the disjunction property and have direct paths to cut-formulas in Π is bounded by $N(\Pi)$. Apply Theorem 5 to Π (where $c \leq N(\Pi)$) and obtain the claim. $\Box$

Theorem 10 *Let $\Pi : S$ be a proof in ALK of n lines. Then there is a proof $\Pi' : S$ in LK of $\mathcal{O}(n)$ lines.*

PROOF. To convert an ALK-proof into an LK-proof is easy. We just need to apply contractions to the antecedents of $\exists$:$left_{ext}$ and $\forall$:$right_{ext}$ rules, apply $\exists$:*left* and $\forall$:*right* rules instead of the corresponding extended rules, and add new weak formulas to preserve the number of copies of quantified formulas in the consequent of $\exists$:$left_{ext}$ and $\forall$:$right_{ext}$ rules.

With this transformation the number of axioms remains the same but new contractions might have increased the complexity of the original proof. (Notice that Lemma 6 ensures that the new weak occurrences can be added with no increase of the number of lines). By Lemma 9 (to be precise we apply here

a version of the lemma for LK; the proof is the same as for ALK) we can find a LK-proof of S with a number of contractions which is bounded by the number of axioms. Hence we find a proof of S with $\mathcal{O}(n)$ lines. $\square$

5 Proofs in ALK are acyclic

The method described in Theorem 5 *simplifies* the logical flow graph of a proof in the sense of Theorem 2 which shows that the logical flow graph of a proof in ALK is acyclic.

PROOF. (Theorem 2) First we claim that for each cut-formula C and its dual C^* there is *at most* one s-formula D in C such that both D and D^* (i.e. the dual of D in C^*) have direct paths to distinguished occurrences in axioms in Π. To see this we look at the formula C and by steps, looking at its binary connectives, we will determine larger and larger subsets of s-formulas of C where there are no pairs of atomic s-formulas D, D^* both linked to distinguished occurrences.

Let us start by considering the maximal subformula C' of C whose main connective is binary. Notice that the set of s-formulas in C' is the same as the set of s-formulas in C (we essentially ignore negations and quantifiers here).

Suppose C' to be of the form $A \wedge B$ and let $A \wedge B$ appear positively in the sequent. This means that $A^* \wedge B^*$ in C^* has to have either all paths from B^* or from A^* going to weak occurrences by the triviality condition. Suppose all paths from B^* go to weak occurrences. They clearly satisfy our condition and we only need to go on and check that paths passing through A^* (or A if one prefers) behave as required. If $A \wedge B$ appears negatively in the sequent, we will have to look at paths passing through A (or B) as before. In case C' is of the form $A \vee B$ we proceed similarly.

We repeat the reasoning over the maximal subformula C' of A whose main connective is binary, and over and over again, over smaller subformulas until C' is atomic. The logical complexity of maximal formulas decreases after each iteration of the testing and the atomic case is reached after a finite number of steps. With each testing we ascertain that a larger set of s-formulas of C satisfies the condition. In fact, until the atomic case, no atomic s-formula in C together with its dual had both direct paths to distinguished occurrences. This proves the claim.

Now let us prove the proposition. Suppose that there was a cyclic path. (Because a cycle must be *oriented* this path cannot reach the end-sequent. If it

did, it would have to stop there.) Consider the smallest subproof of our proof which contains our cycle. Again the end-sequent of this smallest subproof cannot contain formulas from the cycle, but then one of the sequents which occurred just before must touch the cycle, by minimality. In fact the last rule used in this subproof must be a cut rule, and the cycle must go through the cut-formula. In all other cases we would have a formula in the cycle that would have nowhere else to go, by minimality and the definition of logical flow graph.

This occurrence of the cut rule combines two distinct subproofs, each of which contains a part of the cycle. This implies that the cycle must cross the cut at least twice, once going in each direction. That is, the cycle should have at least two edges which go across the cut, with opposite orientations. (Otherwise the cycle would have two ends which cannot be reconnected.) This situation is incompatible with the claim. One of the endpoints of one of these edges must have *all* direct paths going up to weak occurrences. The path would then have no place to cycle back to, and cannot follow such a path. Thus we conclude that there is no cycle and the proposition follows. □

Corollary 11 *If* $\Pi : S$ *is a* LK*-proof where all formulas directly linked to cuts satisfy the disjunction property, then there are no paths in* Π *which are cyclic.*

PROOF. We only need to observe that Π is an ALK-proof and therefore its logical flow graph is acyclic by Theorem 2. □

References

[1] G. Boolos. Don't eliminate cut. In *Journal of Philosophical Logic*, 13:373–378, 1984.

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

[3] A. Carbone. Interpolants, Cut Elimination and Flow Graphs for the Propositional Calculus. In *Annals of Pure and Applied Logic*, 83:249–299, 1997.

[4] A. Carbone. Some combinatorics behind proofs. Submitted for publication, 1995.

[5] A. Carbone. Cycling in proofs, feasibility and non speed-up for nonstandard arithmetic. I.H.E.S. preprint M/96/55, 1996 (Bures-sur-Yvette, France).

[6] A. Carbone. Proofs and Groups with distorted Length Function. Manuscript, 1996.

[7] A. Carbone and S. Semmes. Looking from the inside and from the outside. I.H.E.S. preprint M/96/44, 1996 (Bures-sur-Yvette, France).

[8] A. Carbone and S. Semmes. Making proofs without Modus Ponens: An introduction to the combinatorics and complexity of cut elimination. In *Bulletin of the American Mathematical Society*, 34:131–159, 1997.

[9] A. Carbone and S. Semmes. *Symmetry and algorithms: geometric structures and implicit description.* Book in preparation, 1997.

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

[11] J.Y. Girard. Linear Logic. In *Theoretical Computer Science*, 50:1–102, 1987.

[12] V. P. Orevkov. Lower Bounds for increasing complexity of derivations after cut elimination. In *Journal of Soviet Mathematics*, 20(4), 1982.

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

[14] R. Statman. Bounds for proof-search and speed-up in predicate calculus. In *Annals of Mathematical Logic*, 15:225–287. 1978.

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

[16] G.S. Tseitin. Complexity of a derivation in the propositional calculus. In *Zap. Nauchn. Sem. Leningrad Otd. Mat. Inst. Akad. Nauk SSSR*, 8:234–259. 1968.