The Journal of Symbolic Logic
Volume 76, Number 1, March 2011

ON THE NON-CONFLUENCE OF CUT-ELIMINATION

MATTHIAS BAAZ AND STEFAN HETZL

Abstract. We study cut-elimination in first-order classical logic. We construct a sequence of polynomial-length proofs having a non-elementary number of different cut-free normal forms. These normal forms are different in a strong sense: they not only represent different Herbrand-disjunctions but also differ in their propositional structure.

This result illustrates that the constructive content of a proof in classical logic is not uniquely determined but rather depends on the chosen method for extracting it.

§1. Introduction. Cut-elimination, originally introduced by Gentzen in [3] together with the sequent calculus, is one of the most fundamental proof transformations. Its first—and intended—application was to serve as a tool for consistency proofs, the prime example being Gentzen's analysis of Peano Arithmetic [4]. Later the view emerged that methods for carrying out consistency proofs can be applied fruitfully to concrete mathematical proofs. What is obtained thereby is a more direct, elementary proof of a theorem which in turn may serve to extract concrete bounds, witnesses or similar constructive information. This applies to cut-elimination as well as to other tools for consistency proofs as Hilbert's epsilon calculus [9] and Gödel's Dialectica interpretation [8]. A wealth of such proof analyses, most often based on variants of the Dialectica interpretation, can be found in the literature, see e.g., [10]. An example of the application of cut-elimination is Girard's demonstration that from the topological Fuerstenberg-Weiss proof of van der Waerden's theorem, the original combinatorial proof can be obtained [6, annex 4.A].

Gentzen's original proof [3] of the cut-elimination theorem applies a set of proof reductions according to a particular strategy which is chosen with regard to a general termination proof. From the point of view of analysing concrete mathematical proofs such a restriction is no longer reasonable. At each stage of a cut-elimination process one has the choice between different cuts to reduce and—for a single cut—there are different ways of reducing it. In how far does this formal non-determinism lead to mathematical differences in the resulting elementary proofs? This question is of foundational importance as it concerns the relationship between a proof and its constructive content. Moreover, it also has significant practical implications, for what is usually sought in unwinding a proof is not just any constructive version of it but one that has certain desirable intentional features, like representing a small upper bound, an efficient program, etc.

Received December 11, 2009.

1943-5886/11/7601-0016/$3.80

In this paper we will demonstrate that at times there can be a large number of strongly different cut-free proofs corresponding to a single proof with cuts via the standard set of proof reductions. To that aim we exhibit a sequence (χ_n) of proofs s.t. the number of inferences in χ_n can be bounded by a polynomial in n, however the number of different cut-free normal forms cannot be bounded by an elementary function in n. This sequence, being specifically constructed for the purpose of illustrating this phenomenon, is quite obviously an extreme example. Nevertheless, the structure of the proofs is realistic and we can expect this effect to appear—in a weakened form—in mathematical proofs too. In particular, the proofs do not contain weakening which rules out certain trivially non-confluent configurations. Furthermore, it must be emphasised that the resulting normal forms are different in a strong sense: they not only represent pairwise different Herbrand-disjunctions but the Herbrand-disjunctions of two normal forms also differ in their propositional structure.

§2. Sequent calculus.

DEFINITION 1 (**LK**-proof). A *sequent* is a pair of multisets of formulas. An **LK**-*proof* χ is a tree built up as follows: axiom sequents are of the form

$$A \to A$$

for a formula A. The rules are

$$\frac{\Gamma \to \Delta, A \quad \Pi \to \Lambda, B}{\Gamma, \Pi \to \Delta, \Lambda, A \wedge B}\ \wedge_{\mathrm{r}} \qquad \frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ \wedge_{\mathrm{l}_1} \qquad \frac{B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta}\ \wedge_{\mathrm{l}_2}$$

$$\frac{A, \Gamma \to \Delta \quad B, \Pi \to \Lambda}{A \vee B, \Gamma, \Pi \to \Delta, \Lambda}\ \vee_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B}\ \vee_{\mathrm{r}_1} \qquad \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \vee B}\ \vee_{\mathrm{r}_2}$$

$$\frac{\Gamma \to \Delta, A \quad B, \Pi \to \Lambda}{A \supset B, \Gamma, \Pi \to \Delta, \Lambda}\ \supset_{\mathrm{l}} \qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, A \supset B}\ \supset_{\mathrm{r}_1} \qquad \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}\ \supset_{\mathrm{r}_2}$$

$$\frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}\ \neg_{\mathrm{l}} \qquad \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A}\ \neg_{\mathrm{r}}$$

$$\frac{A\{x \leftarrow t\}, \Gamma \to \Delta}{(\forall x)A, \Gamma \to \Delta}\ \forall_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A\{x \leftarrow \alpha\}}{\Gamma \to \Delta, (\forall x)A}\ \forall_{\mathrm{r}}$$

$$\frac{\Gamma \to \Delta, A\{x \leftarrow t\}}{\Gamma \to \Delta, (\exists x)A}\ \exists_{\mathrm{r}} \qquad \frac{A\{x \leftarrow \alpha\}, \Gamma \to \Delta}{(\exists x)A, \Gamma \to \Delta}\ \exists_{\mathrm{l}}$$

For the variable α and the term t the following must hold:

1. t must not contain a variable that occurs bound in A,
2. α is called an *eigenvariable* and must not occur in $\Gamma \cup \Delta \cup \{A\}$.

$$\frac{\Gamma \to \Delta}{A, \Gamma \to \Delta}\ \mathrm{w}_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A}\ \mathrm{w}_{\mathrm{r}} \qquad \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta}\ \mathrm{c}_{\mathrm{l}} \qquad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}\ \mathrm{c}_{\mathrm{r}}$$

$$\frac{\Gamma \to \Delta, A \quad A, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

An instance of a rule in a proof will be called *inference*. A proof is called *regular* if the strong quantifier inferences (i.e., $\forall_r$ and $\exists_l$) have pairwise different eigenvariables. Throughout this paper we use the standard-set of proof rewrite steps for cut-elimination, a complete description of which can be found in Appendix A. If a proof π can be reduced by a sequence of steps to a proof π', this is denoted as $\pi \to^c \pi'$.

§3. Non-confluence in cut-elimination. In discussing confluence properties of cut-elimination in classical logic, the proof form

$$\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta}}{\Gamma \to \Delta, A}\,\mathrm{w_r} \qquad \dfrac{\dfrac{(\chi_2)}{\Pi \to \Lambda}}{A, \Pi \to \Lambda}\,\mathrm{w_l}}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{cut}$$

has received considerable attention [7, 17, 18]. While this is a sequent calculus proof that can be reduced to both χ_1 and χ_2, as an *input* it remains an unconvincing example as it is not realistic as formalisation of a mathematical proof: there clearly is no point in introducing the formula A which is neither proved nor used. Therefore, the first step in our analysis is to restrict the set of input proofs in a way that rules out the above configuration. Indeed, we will consider only such proofs that do not contain any weakenings.

3.1. Proofs without weakening.

DEFINITION 2. We define several proof reductions: Let χ be a proof, ρ be a weakening in χ which is not the lowest inference of χ and ρ' be the inference below ρ.

1. If the main occurrence of ρ is in the context of ρ', then exchange ρ and ρ', e.g., for ρ' being $\wedge_{l_1}$ define

$$\dfrac{\dfrac{\dfrac{(\xi)}{A, \Gamma \to \Delta}}{A, \Gamma \to \Delta, C}\,\mathrm{w_r}}{A \wedge B, \Gamma \to \Delta, C}\,\wedge_{l_1} \quad \to \quad \dfrac{\dfrac{\dfrac{(\xi)}{A, \Gamma \to \Delta}}{A \wedge B, \Gamma \to \Delta}\,\wedge_{l_1}}{A \wedge B, \Gamma \to \Delta, C}\,\mathrm{w_r}$$

   In order to keep strong termination, the above reduction is only allowed if ρ' is not a weakening itself.
2. Otherwise the main occurrence of ρ is auxiliary occurrence of ρ'.
   (a) If ρ' is a contraction, then delete both ρ and ρ', i.e.

$$\dfrac{\dfrac{\dfrac{(\xi)}{\Gamma \to \Delta, A}}{\Gamma \to \Delta, A, A}\,\mathrm{w_r}}{\Gamma \to \Delta, A}\,\mathrm{c_r} \quad \to \quad \dfrac{(\xi)}{\Gamma \to \Delta, A}$$

   (b) If ρ' is a unary logical inference, then delete ρ', e.g., for ρ' being $\vee : r1$ define

$$\dfrac{\dfrac{\dfrac{(\xi)}{\Gamma \to \Delta}}{\Gamma \to \Delta, A}\,\mathrm{w_r}}{\Gamma \to \Delta, A \vee B}\,\vee_{r_1} \quad \to \quad \dfrac{\dfrac{(\xi)}{\Gamma \to \Delta}}{\Gamma \to \Delta, A \vee B}\,\mathrm{w_r}$$

(c) If ρ' is a binary inference, then delete ρ' and the subproof which does not contain ρ, e.g., for ρ' being $\wedge_r$ and ρ being in the left subproof above ρ' define

$$\dfrac{\dfrac{\dfrac{(\xi_1)}{\Gamma \to \Delta}}{\Gamma \to \Delta, C}\ w_r \quad \dfrac{(\xi_2)}{\Pi \to \Lambda, D}}{\Gamma, \Pi \to \Delta, \Lambda, C \wedge D}\ \wedge_r \quad \to \quad \dfrac{\dfrac{(\xi_1)}{\Gamma \to \Delta}}{\Gamma, \Pi \to \Delta, \Lambda, C \wedge D}\ w^*$$

Analogous reductions apply for ρ being w_l and/or ρ' being of another rule type. We define $\to^v$ as the compatible, reflexive and transitive closure of the union of the reductions 1 and 2a and $\to^w$ as that of all the reductions above. We write $|\chi|$ for the *number of inferences* in the proof χ.

PROPOSITION 1. For each proof χ of a sequent s there exists a weakening-free proof χ' of a sequent $s' \subseteq s$ with $|\chi'| \leq |\chi|$.

PROOF. Observe that $\to^w$ is strongly terminating and that a $\to^w$-normal form of χ has the shape

$$\dfrac{\dfrac{(\chi')}{\Gamma \to \Delta}}{\Pi, \Gamma \to \Delta, \Lambda}\ w^*$$

where $\Pi, \Gamma \to \Delta, \Lambda$ is the end-sequent of χ. As $\xi \to^w \xi'$ implies $|\xi'| \leq |\xi|$ the claim follows. ⊣

3.2. Proof variants. In order to describe cut-elimination sequences in a concise way later on, we need some more machinery concerning the appearances of redundant contractions and weakenings in proofs.

DEFINITION 3. Let χ be a proof of a sequent $\Gamma \to \Delta$, then a proof χ' is called *variant* of χ if

$$\chi' \to^v \dfrac{\dfrac{(\chi)}{\Gamma \to \Delta}}{\Pi, \Gamma \to \Delta, \Lambda}\ w^*$$

for some (possibly empty) multisets of formulas Π and Λ.

Note that the relation of being a variant is reflexive and transitive. As a notational abbreviation we write $\widetilde{\chi}$ to denote a variant of χ. We also write $\chi \to^c \widetilde{\xi}$ for: there exists a variant ξ' of ξ s.t. $\chi \to^c \xi'$ and $\widetilde{\chi} \to^c \widetilde{\xi}$ for: for any variant χ' of χ there exists a variant ξ' of ξ s.t. $\chi' \to^c \xi'$. An essential fact about the relation of a proof χ to any of its variants $\widetilde{\chi}$ is that the witnesses of quantifiers in the end-sequent are identical.

We now go on to state some basic results about the behaviour of variants under cut-elimination. As the proofs of the following lemmas do not provide important logical insights but are of a purely technical nature, we only sketch them here. The key property is that of $\to^v$ and $\to^c$ being commuting reductions as stated in the following

LEMMA 1. If $\chi_1 \to^c \chi_2$ then $\widetilde{\chi_1} \to^c \widetilde{\chi_2}$.

PROOF. By induction on the length of the given reduction sequence $\chi_1 \to^{\mathrm{c}} \chi_2$. Each reduction step in this sequence is translated to a corresponding reduction step in $\widetilde{\chi_1} \to^{\mathrm{c}} \widetilde{\chi_2}$ plus permutations of the superfluous weakenings and contractions over the reduced cut. ⊣

LEMMA 2. If $\pi[\chi] \to^{\mathrm{c}} \psi$, then $\pi[\widetilde{\chi}] \to^{\mathrm{c}} \widetilde{\psi}$.

PROOF. Let $\Gamma \to \Delta$ be the end-sequent of π, $\Pi \to \Lambda$ that of χ and $\Sigma, \Pi \to \Lambda, \Theta$ that of $\widetilde{\chi}$. Then the end-sequent of $\pi[\widetilde{\chi}]$ is $\Sigma, \Gamma \to \Delta, \Theta$ and

$$\pi[\widetilde{\chi}] \to^{\mathrm{v}} \pi\left[\begin{array}{c}(\chi)\\ \dfrac{\Pi \to \Lambda}{\Sigma, \Pi \to \Lambda, \Theta}\ \mathrm{w}^*\end{array}\right] \to^{\mathrm{v}} \begin{array}{c}(\pi[\chi])\\ \dfrac{\Gamma \to \Delta}{\Sigma, \Gamma \to \Delta, \Theta}\ \mathrm{w}^*\end{array}$$

so $\pi[\widetilde{\chi}]$ is a variant of $\pi[\chi]$ and the result follows from Lemma 1. ⊣

LEMMA 3. If $\chi_1 \to^{\mathrm{c}} \widetilde{\chi_2}$ and $\chi_2 \to^{\mathrm{c}} \widetilde{\chi_3}$ then $\chi_1 \to^{\mathrm{c}} \widetilde{\chi_3}$.

PROOF. By Lemma 1. ⊣

LEMMA 4. Let χ be a proof of $\Gamma \to \Delta$, let χ' be a variant of χ with end-sequent $\Gamma, \Gamma' \to \Delta, \Delta', F$ and let ξ be a proof of $F, \Pi \to \Lambda$. Then there is a variant χ'' of χ s.t.

$$\frac{\begin{array}{cc}(\chi') & (\xi)\\ \Gamma, \Gamma' \to \Delta, \Delta', F & F, \Pi \to \Lambda\end{array}}{\Gamma, \Gamma', \Pi \to \Delta, \Delta', \Lambda}\ \mathrm{cut} \quad \to^{\mathrm{c}} \quad \begin{array}{c}(\chi'')\\ \Gamma, \Gamma', \Pi \to \Delta, \Delta', \Lambda\end{array}$$

PROOF. First observe that F in χ' is only introduced by weakening. Then use a cut-elimination strategy that moves ξ into χ', duplicating it at contractions of F and eventually deleting all copies at the final weakenings. ⊣

3.3. Non-deterministic projection. Having laid the groundwork of proof variants in the previous section, we now set about defining basic building blocks for proofs exhibiting non-confluent behaviour. To that aim, we define—for X and Y being arbitrary formulas—the *projections*

$$\pi_1(X, Y) := \frac{X \to X}{X \wedge Y \to X}\ \wedge_{\mathrm{l}_1} \qquad \text{and} \qquad \pi_2(X, Y) := \frac{Y \to Y}{X \wedge Y \to Y}\ \wedge_{\mathrm{l}_2}\ .$$

Usually, X and Y will be understood from the context and we will just write π_1 and π_2. The reader is referred to Appendix B for an index of formal proofs that are used outside of a local context, like π_1 and π_2 defined above will be.

Our first technical result worth expounding in some detail concerns the reachability of both of the above projections from a single proof. To simplify the notation we will—given two proofs χ_1 and χ_2—write $\mathrm{cut}(\chi_1, \chi_2)$ to denote the proof obtained by combining χ_1 and χ_2 by a cut if the cut formula is obvious from the context.

PROPOSITION 2. Let X, Y be formulas. Then there is a weakening-free proof $\pi(X, Y)$ of $X \wedge Y \to X, Y$ such that both $\pi \to^{\mathrm{c}} \widetilde{\pi_1}$ and $\pi \to^{\mathrm{c}} \widetilde{\pi_2}$.

PROOF. Define $B := (X \wedge Y) \supset (X \wedge Y)$ and $\pi' :=$

$$\dfrac{\dfrac{\dfrac{\dfrac{B \to B}{\to B, \neg B}\ \neg_{\mathrm{r}}}{\to B \vee \neg B, B}\ \vee_{\mathrm{r}_2} \quad \dfrac{B \to B}{B \to B \vee \neg B}\ \vee_{\mathrm{r}_1}}{\to B \vee \neg B, B \vee \neg B}\ \mathrm{cut}}{\to B \vee \neg B}\ \mathrm{c}_{\mathrm{r}}$$

and $\pi'' :=$

$$\dfrac{\dfrac{(p_1) \qquad\qquad (p_2)}{B \vee \neg B, X \wedge Y \to X, X \wedge Y \quad X \wedge Y, B \vee \neg B, X \wedge Y \to Y}\ \text{cut}}{\dfrac{[B \vee \neg B]^2, [X \wedge Y]^2 \to X, Y}{B \vee \neg B, X \wedge Y \to X, Y}\ \text{c}^*}$$

and $p_1 :=$

$$\dfrac{\dfrac{\dfrac{(\pi_1)}{X \wedge Y \to X \wedge Y \quad X \wedge Y \to X}\ \supset_\text{l} \qquad \dfrac{\dfrac{X \wedge Y \to X \wedge Y}{\to X \wedge Y, B}\ \supset_{\text{r}_1}}{\neg B \to X \wedge Y}\ \neg_\text{l}}{B \vee \neg B, X \wedge Y \to X \wedge Y, X}\ \vee_\text{l}$$

and $p_2 :=$

$$\dfrac{\dfrac{\dfrac{(\pi_2)}{X \wedge Y \to X \wedge Y \quad X \wedge Y \to Y}\ \supset_\text{l} \qquad \dfrac{\dfrac{X \wedge Y \to X \wedge Y}{X \wedge Y \to B}\ \supset_{\text{r}_2}}{\neg B, X \wedge Y \to}\ \neg_\text{l}}{B \vee \neg B, X \wedge Y, X \wedge Y \to Y}\ \vee_\text{l}$$

and $\pi := \text{cut}(\pi', \pi'')$. Reducing the contraction-right of $B \vee \neg B$ at the end of π' and permuting the two copies of π'' into the left and right part respectively of π', we obtain $\pi \to^\text{c} \chi_2 =$

$$\dfrac{\dfrac{(\chi_3) \qquad\qquad (\chi_4)}{X \wedge Y \to X, Y, B \quad B, X \wedge Y \to X, Y}\ \text{cut}}{\dfrac{[X \wedge Y]^2 \to [X]^2, [Y]^2}{X \wedge Y \to X, Y}\ \text{c}^*}$$

where $\chi_3 =$

$$\dfrac{\dfrac{\dfrac{B \to B}{\to B, \neg B}\ \neg_\text{r}}{\to B, B \vee \neg B}\ \vee_{\text{r}_2} \qquad \dfrac{(\pi'')}{B \vee \neg B, X \wedge Y \to X, Y}}{X \wedge Y \to X, Y, B}\ \text{cut}$$

and $\chi_4 =$

$$\dfrac{\dfrac{B \to B}{B \to B \vee \neg B}\ \vee_{\text{r}_1} \qquad \dfrac{(\pi'')}{B \vee \neg B, X \wedge Y \to X, Y}}{B, X \wedge Y \to X, Y}\ \text{cut}$$

Eliminating the cut on $B \vee \neg B$ in χ_4 completely leads to $\chi_4 \to^\text{c} \chi_5 =$

$$\dfrac{\dfrac{\dfrac{(\pi_1)}{X \wedge Y \to X \wedge Y \quad X \wedge Y \to X}\ \supset_\text{l}}{B, X \wedge Y \to X}\ \text{w}_\text{r} \qquad \dfrac{\dfrac{(\pi_2)}{X \wedge Y \to X \wedge Y \quad X \wedge Y \to Y}\ \supset_\text{l}}{B, X \wedge Y \to Y}\ \text{w}_\text{l}}{B, X \wedge Y \to X, X \wedge Y \qquad X \wedge Y, B, X \wedge Y \to Y}\ \text{cut}$$

$$\dfrac{[B]^2, [X \wedge Y]^2 \to X, Y}{B, X \wedge Y \to X, Y}\ \text{c}^*$$

By choosing to reduce the left or the right weakening in χ_5, we obtain $\chi_5 \to^\text{c} \widetilde{\xi_1}$ and $\chi_5 \to^\text{c} \widetilde{\xi_2}$ where

$$\xi_1 = \dfrac{\dfrac{(\pi_1)}{X \wedge Y \to X \wedge Y \quad X \wedge Y \to X}\ \supset_\text{l}}{B, X \wedge Y \to X} \qquad \text{and}$$

$$\xi_2 = \dfrac{\dfrac{}{X \wedge Y \to X \wedge Y}\ (\pi_2) \quad X \wedge Y \to Y}{B, X \wedge Y \to Y}\ \supset_{\mathrm{l}}$$

Furthermore, χ_3 can—by first eliminating the cut on $B \vee \neg B$, then the one on $X \wedge Y$—be reduced to a variant of

$$\xi_3 = \dfrac{\dfrac{\dfrac{X \wedge Y \to X \wedge Y}{\to X \wedge Y, B}\ \supset_{\mathrm{r}_1}}{\to B, B}\ \supset_{\mathrm{r}_2}}{\to B}\ \mathrm{c}_{\mathrm{r}}$$

Now observe that for both $i = 1, 2$, $\mathrm{cut}(\xi_3, \xi_i) \to^{\mathrm{c}} \widetilde{\pi_i}$ which implies $\mathrm{cut}(\chi_3, \chi_4) \to^{\mathrm{c}} \widetilde{\pi_i}$ and therefore $\pi \to^{\mathrm{c}} \widetilde{\pi_i}$. ⊣

The reader not interested in the input proofs being weakening-free might replace the above proof π by a shorter one (containing weakening) with the same cut-elimination behaviour. Building on a proof π having the property stated in the above proposition, the rest of this section is devoted to providing a flexible construction for combining pre-existing proofs in a way which allows reduction to any of them. Specifically we will prove the following

PROPOSITION 3. Let $\chi_1, \ldots, \chi_n$ be weakening-free proofs where χ_i proves $\Gamma_i, \Pi \to F$ and let $\Gamma = \Gamma_1, \ldots, \Gamma_n$. Then there exists a weakening-free proof $\pi(\chi_1, \ldots, \chi_n)$ of $\Gamma, \Pi \to F$ s.t.

$$\pi(\chi_1, \ldots, \chi_n) \to^{\mathrm{c}} \widetilde{\chi_k} \qquad \forall k \in \{1, \ldots, n\}.$$

In order to prove the above statement we first need an additional auxiliary construction. From now on, let $\bigwedge$ denote finite left-associative conjunction.

DEFINITION 4. Let $F_1, \ldots, F_n$ be formulas and for $k \in \{1, \ldots, n\}$ let π^n_k denote the proof

$$\dfrac{\dfrac{F_k \to F_k}{\bigwedge_{i=1}^{k} F_i \to F_k}\ \wedge^{?}_{\mathrm{l}_2}}{\bigwedge_{i=1}^{n} F_i \to F_k}\ \wedge^{*}_{\mathrm{l}_1}$$

where ? denotes 0 or 1 application and $*$ denotes ≥ 0 applications of a rule.

LEMMA 5. Let $F_1, \ldots, F_n$ be formulas. Then there is a weakening-free proof $\pi^n(F_1, \ldots, F_n)$ of $\bigwedge_{i=1}^{n} F_i \to F_1, \ldots, F_n$ s.t. for every $k \in \{1, \ldots, n\}$ there is a reduction $\pi^n(F_1, \ldots, F_n) \to^{\mathrm{c}} \widetilde{\pi^n_k}$.

PROOF. For $n = 1$ define $\pi^1(F_1)$ as $F_1 \to F_1$, the claim follows trivially. For $n > 1$ define $\pi^n(F_1, \ldots, F_n)$ as

$$\dfrac{\begin{array}{cc}(\pi(\bigwedge_{i=1}^{n-1} F_i, F_n)) & (\pi^{n-1}(F_1, \ldots, F_{n-1})) \\ \bigwedge_{i=1}^{n} F_i \to \bigwedge_{i=1}^{n-1} F_i, F_n & \bigwedge_{i=1}^{n-1} F_i \to F_1, \ldots, F_{n-1}\end{array}}{\bigwedge_{i=1}^{n} F_i \to F_1, \ldots, F_n}\ \mathrm{cut}$$

If $k < n$, then by Proposition 2: $\pi(\bigwedge_{i=1}^{n-1} F_i, F_n) \to^{\mathrm{c}} \widetilde{\pi_1}$, by induction hypothesis $\pi^{n-1}(F_1, \ldots, F_{n-1}) \to^{\mathrm{c}} \widetilde{\pi_k^{n-1}}$ and by Lemma 2:

$$\dfrac{\dfrac{(\widetilde{\pi_1})}{\bigwedge_{i=1}^{n} F_i \to \bigwedge_{i=1}^{n-1} F_i, F_n} \quad \dfrac{(\widetilde{\pi_k^{n-1}})}{\bigwedge_{i=1}^{n-1} F_i \to F_1, \ldots, F_{n-1}}}{\bigwedge_{i=1}^{n} F_i \to F_1, \ldots, F_n}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{(\widetilde{\pi_k^n})}{\bigwedge_{i=1}^{n} F_i \to F_1, \ldots, F_n}$$

If $k = n$ then by Proposition 2: $\pi(\bigwedge_{i=1}^{n-1} F_i, F_n) \to^{\mathrm{c}} \widetilde{\pi_2}$ and by Lemma 4:

$$\pi^n(F_1, \ldots, F_n) \to^{\mathrm{c}} \widetilde{\pi_n^n}. \qquad \dashv$$

Proof of Proposition 3. Define $\xi_1 := \chi_1$ and for $1 \le j \le n$:

$$\xi_j := \dfrac{\dfrac{\dfrac{(\xi_{j-1})}{\Gamma_1, \ldots, \Gamma_{j-1}, \Pi \to \bigwedge_{i=1}^{j-1} F} \quad \dfrac{(\chi_j)}{\Gamma_j, \Pi \to F}}{\Gamma_1, \ldots, \Gamma_j, \Pi, \Pi \to \bigwedge_{i=1}^{j} F}\ \mathrm{c}_{\mathrm{l}}^*}{\Gamma_1, \ldots, \Gamma_j, \Pi \to \bigwedge_{i=1}^{j} F}\ \wedge_{\mathrm{r}}$$

Define $\pi(\chi_1, \ldots, \chi_n)$ as

$$\dfrac{\dfrac{(\xi_n)}{\Gamma, \Pi \to \bigwedge_{i=1}^{n} F} \quad \dfrac{\pi^n(F, \ldots, F)}{\bigwedge_{i=1}^{n} F \to F, \ldots, F}}{\dfrac{\Gamma, \Pi \to F, \ldots, F}{\Gamma, \Pi \to F}\ \mathrm{c}_{\mathrm{r}}^*}\ \mathrm{cut}$$

By Lemma 5: $\pi^n(F, \ldots, F) \to^{\mathrm{c}} \widetilde{\pi_k^n}$. We will first show by induction on n that $\mathrm{cut}(\xi_n, \pi_k^n) \to^{\mathrm{c}} \widetilde{\chi_k}$. If $n = 1$ then π_k^n is just an axiom and the claim is trivial. Let $n > 1$: If $k = n$ then

$$\dfrac{\dfrac{(\xi_n)}{\Gamma, \Pi \to \bigwedge_{i=1}^{n} F} \quad \dfrac{F \to F}{\bigwedge_{i=1}^{n} F \to F}\ \wedge_{\mathrm{l}_2}}{\Gamma, \Pi \to F}\ \mathrm{cut} \quad \to^{\mathrm{c}} \quad \dfrac{\dfrac{\dfrac{(\chi_n)}{\Gamma_n, \Pi \to F} \quad F \to F}{\Gamma_n, \Pi \to F}\ \mathrm{cut}}{\Gamma, \Pi, \Pi \to F}\ \mathrm{w}^*}{\Gamma, \Pi \to F}\ \mathrm{c}^* \quad \to^{\mathrm{c}} \widetilde{\chi_n}.$$

If $k < n$ then

$$\dfrac{\dfrac{(\xi_n)}{\Gamma, \Pi \to \bigwedge_{i=1}^{n} F} \quad \dfrac{\dfrac{(\pi_k^{n-1})}{\bigwedge_{i=1}^{n-1} F \to F}}{\bigwedge_{i=1}^{n} F \to F}\ \wedge_{\mathrm{l}_1}}{\Gamma, \Pi \to F}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{\dfrac{\dfrac{(\xi_{n-1}) \qquad (\pi_k^{n-1})}{\Gamma_1, \ldots, \Gamma_{n-1}, \Pi \to \bigwedge_{i=1}^{n-1} F \quad \bigwedge_{i=1}^{n-1} F \to F}\ \text{cut}}{\Gamma_1, \ldots, \Gamma_{n-1}, \Pi \to F}\ \text{w}^*}{\dfrac{\Gamma, \Pi, \Pi \to F}{\Gamma, \Pi \to F}\ \text{c}^*}$$

which by induction hypothesis reduces to $\widetilde{\chi_k}$.

Then by Lemma 2: $\text{cut}(\xi_n, \widetilde{\pi_k^n}) \to^{\text{c}} \widetilde{\chi_k}$ and therefore $\pi(\chi_1, \ldots, \chi_n) \to^{\text{c}} \widetilde{\chi_k}$. ⊣

The above building blocks equip us with basic infrastructure concerning the construction of non-confluent (and weakening-free) proofs. To carry this non-confluence to the non-elementary asymptotic behaviour sketched in the introduction, we will rely on a proof sequence that demonstrates the non-elementary lower bound on the increase of proof length.

§4. The complexity of cut-elimination. It is a well-known result, originally due to Statman [16] and Orevkov [12], that cut-elimination in first-order logic leads to a non-elementary increase of the length of a proof. Usually, such a result is proved by exhibiting a sequence of short proofs with cuts and showing that each sequence of cut-free proofs of the proved formulas must grow non-elementarily. In this section we will in addition show that the sequence of short proofs reduces to a certain sequence of cut-free proofs which will be useful later.

We use the language of Pudlák's sequence from [15] but consent ourselves with a simpler proofs having polynomial length, but exponential size. We consider a language for arithmetic containing besides equality the symbols $0, s(\cdot)$ and $+$ as well as the unary function symbol $2^{\cdot}$. In addition, our language contains a unary predicate symbol $I(\cdot)$ whose intended interpretation is "an initial segment of the natural numbers". We use the following set of axioms $\mathscr{A}$ (some of which are assigned abbreviations):

$$\begin{aligned}
&\forall x\, x = x,\\
&\forall x \forall y\, (x = y \supset y = x),\\
&\forall x \forall y \forall z\, (x = y \supset y = z \supset x = z),\\
C_I \equiv\ &\forall x \forall y\, (x = y \supset I(x) \supset I(y)),\\
&\forall x \forall y\, (x = y \supset s(x) = s(y)),\\
&\forall x_1 \forall x_2 \forall y_1 \forall y_2\, (x_1 = y_1 \supset x_2 = y_2 \supset x_1 + x_2 = y_1 + y_2),\\
&\forall x \forall y\, (x = y \supset 2^x = 2^y),\\
&\forall x\, x + 0 = x,\\
&\forall x \forall y\, x + s(y) = s(x + y),\\
&\forall x \forall y \forall z\, x + (y + z) = (x + y) + z,\\
&2^0 = s(0),\\
&\forall x\, 2^{s(x)} = 2^x + 2^x,
\end{aligned}$$

$$Z_I \equiv I(0),$$
$$S_I \equiv \forall x\,(I(x) \supset I(s(x))).$$

We define the "tower of twos"-terms $\mathrm{tt}_0 := 2^0$ and $\mathrm{tt}_{n+1} := 2^{\mathrm{tt}_n}$. We write letters $u, v, \ldots$ for terms in the signature $0, s, +, 2^{\cdot}$, furthermore $m, n, \ldots$ for natural numbers and $|u|$ for the value of a variable-free term u in the standard model. The proofs will have the end-sequent $\mathscr{A} \to I(\mathrm{tt}_n)$. Let $C_0(u) \equiv I(u)$ and $C_{n+1}(u) \equiv \forall z(C_n(z) \supset C_n(z + 2^u))$ which will serve as cut-formulas.

For notational convenience, we use a calculus **LK'** in the description of the non-elementary reduction which differs from **LK** only in that it replaces the rules $\supset_{\mathrm{r}_1}$ and $\supset_{\mathrm{r}_2}$ by the rule

$$\frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B}\ \supset_{\mathrm{r}}$$

The obvious translation from **LK'** replaces the above rule by $\supset_{\mathrm{r}_2}, \supset_{\mathrm{r}_1}, \mathrm{c}_{\mathrm{r}}$ and turns weakening-free proofs into weakening-free proofs.

LEMMA 6. Let π' and ψ' be **LK'**-proofs with translations π, ψ in **LK**. If $\pi' \to^{\mathrm{c}} \psi'$ in **LK'**, then $\pi \to^{\mathrm{c}} \widetilde{\psi}$ in **LK**.

PROOF. In the light of Lemma 3, it suffices to check this for a single reduction step. If $\pi' \to^{\mathrm{c}} \psi'$ is an implication-elimination, let $\pi \to^{\mathrm{c}} \pi_1$ be the corresponding **LK**-step and observe $\pi_1 \to^{\mathrm{v}} \psi$ and thus π_1 is a variant of ψ. If $\pi' \to^{\mathrm{c}} \psi'$ permutes an $\supset_{\mathrm{r}}$-inference over a cut, $\pi \to^{\mathrm{c}} \psi$ can be achieved by the corresponding three reduction steps. For any other reduction $\pi \to^{\mathrm{c}} \psi$ is obtained directly by the corresponding reduction step. ⊣

To save space and increase readability, we use certain abbreviations for writing down proofs: we usually omit $\mathscr{A}$ in the antecedent of a sequent. The availability of a sufficient number of copies of elements of $\mathscr{A}$ is assumed throughout. If it is obvious from the context how to finish a formal proof (possibly using formulas from $\mathscr{A}$) we indicate this by vertical dots. We use the following abbreviation for equality inference: If u_1 and u_2 are terms s.t. $u_1 = u_2$ can be proven from $\mathscr{A} \setminus \{Z_I, S_I\}$, then we use $\overline{C_n(u_1) \to C_n(u_2)}$ to abbreviate a proof of the form

$$\dfrac{\dfrac{\dfrac{}{\begin{array}{c}(\varepsilon)\\ I(u[u_1]) \to I(u[u_2])\end{array}}}{\vdots}}{\dfrac{C_{n-1}(\alpha) \to C_{n-1}(\alpha) \quad C_{n-1}(\alpha + 2^{u_1}) \to C_{n-1}(\alpha + 2^{u_2})}{C_n(u_1), C_{n-1}(\alpha) \to C_{n-1}(\alpha + 2^{u_2})}\ \forall_{\mathrm{r}}, \supset_{\mathrm{r}}}\ \forall_{\mathrm{l}}, \supset_{\mathrm{l}}$$

where ε is cut-free. Note that

$$\dfrac{\overline{C_n(u_1) \to C_n(u_2)} \quad \overline{C_n(u_2) \to C_n(u_3)}}{C_n(u_1) \to C_n(u_3)}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad \overline{C_n(u_1) \to C_n(u_3)}$$

and therefore, if $\bar{\chi}$ is a proof where all axioms are of this bar-form, also

$$\dfrac{\begin{array}{c}(\bar{\chi})\\ \Gamma \to \Delta, C_n(u_1)\end{array} \quad \overline{C_n(u_1) \to C_n(u_2)}}{\Gamma \to \Delta, C_n(u_2)}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad \begin{array}{c}(\bar{\chi})\\ \Gamma \to \Delta, C_n(u_2).\end{array}$$

Thus the same cut-elimination relation can be applied to the bar-notation directly. In addition, we write $\langle\ \rangle$ instead of $(\ )$ to indicate that we use a more convenient notation for terms over the natural numbers, so e.g., $C_n(2^u+(2^u+2^u))$ is abbreviated as $C_n\langle 3\cdot 2^u\rangle$ even though our formal language contains neither 3 nor $\cdot$. Finally, we abbreviate $\overline{C_n\langle u\rangle \to C_n\langle u\rangle}$ as $\overline{C_n\langle u\rangle}$.

DEFINITION 5. Let $n,k\geq 0$, let u,v be terms and define $\gamma(n,k,u,v) :=$

$$\dfrac{\dfrac{\overline{C_n\langle v+(k-1)\cdot 2^u\rangle}\qquad \overline{C_n\langle v+k\cdot 2^u\rangle}}{C_{n+1}\langle u\rangle, C_n\langle v+(k-1)\cdot 2^u\rangle \to C_n\langle v+k\cdot 2^u\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}}{\vdots}$$

$$\dfrac{\overline{C_n\langle v+0\cdot 2^u\rangle}\qquad [C_{n+1}\langle u\rangle]^{k-1}, C_n\langle v+1\cdot 2^u\rangle \to C_n\langle v+k\cdot 2^u\rangle}{[C_{n+1}\langle u\rangle]^k, C_n\langle v\rangle \to C_n\langle v+k\cdot 2^u\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}$$

Let $n\geq 1$, $k>0$, u be a term and define

$$\xi(n,k,u) := \dfrac{\dfrac{(\gamma(n-1,2^k,u,\alpha))}{[C_n\langle u\rangle]^{2^k}, C_{n-1}\langle\alpha\rangle \to C_{n-1}\langle\alpha+2^k\cdot 2^u\rangle}\ \forall_{\mathrm{r}},\supset_{\mathrm{r}}}{[C_n\langle u\rangle]^{2^k}\to C_n\langle u+k\rangle}\ \mathrm{c}^*_{\mathrm{l}}$$

and for $k=0$ let $\xi(n,0,u) := \overline{C_n\langle u\rangle \to C_n\langle u\rangle}$.

Let $n\geq 2$, u be a variable-free term and define

$$\chi(n,u) := \dfrac{(\xi(n-1,2^{|u|},\alpha))}{C_{n-1}\langle\alpha\rangle \to C_{n-1}\langle\alpha+2^u\rangle}\ \forall_{\mathrm{r}},\supset_{\mathrm{r}}$$

and for $n=0,1$ define $\chi(0,0) := \overline{Z_I\to C_0\langle 0\rangle}$ and

$$\chi(1,0) := \dfrac{\dfrac{\overline{I\langle\alpha\rangle\to I\langle\alpha\rangle}\quad \overline{I\langle\alpha+1\rangle\to I\langle\alpha+1\rangle}}{I\langle\alpha\rangle, S_I\to I\langle\alpha+1\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}}{S_I\to C_1\langle 0\rangle}\ \forall_{\mathrm{r}},\supset_{\mathrm{r}}$$

Let $n\geq 0$, u be a term and define

$$\delta(n,u) := \dfrac{\begin{array}{c}(\chi(n,0))\\ \to C_n\langle 0\rangle\end{array}\quad \overline{C_n\langle 2^u\rangle\to C_n\langle 2^u\rangle}}{C_{n+1}\langle u\rangle\to C_n\langle 2^u\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}$$

Finally, for $n\geq 0$ define

$$\psi_n := \dfrac{\dfrac{\begin{array}{c}(\chi(n,0))\\ \to C_n\langle 0\rangle\end{array}\quad \begin{array}{c}(\delta(n-1,0))\\ C_n\langle 0\rangle\to C_{n-1}\langle \mathrm{tt}_1\rangle\end{array}}{\to C_{n-1}\langle \mathrm{tt}_1\rangle}\ \mathrm{cut}}{\vdots}$$

$$\dfrac{\to C_1\langle \mathrm{tt}_{n-1}\rangle\qquad \begin{array}{c}(\delta(0,\mathrm{tt}_{n-1}))\\ C_1\langle \mathrm{tt}_{n-1}\rangle\to C_0\langle \mathrm{tt}_n\rangle\end{array}}{\to C_0\langle \mathrm{tt}_n\rangle}\ \mathrm{cut}$$

The following two propositions, due to Statman [16] and Orevkov [12], establish the non-elementary lower bound on cut-elimination.

PROPOSITION 4. The length $|\psi_n|$ of ψ_n can be bound by a polynomial in n and for all $n \geq 0$: ψ_n proves $\mathscr{A} \to I(\mathrm{tt}_n)$.

PROPOSITION 5. Let u be a variable-free term, then each cut-free proof of $\mathscr{A} \to I(u)$ contains at least $|u|$ instances of S_I.

The above two results together establish the non-elementary increase in proof-length during cut-elimination. We now continue to explicitly describe a reduction of the ψ_n thereby exhibiting a sequence of normal forms. The reduction of the ψ_n will proceed—like an avalanche—from top to bottom, increasing in size. The reduction can be described by two nested inductions, the inner one iterating duplication to produce exponentiation which is in turn iterated by the outer to produce the non-elementary growth. The crucial observation, and the outer induction step, is the following.

LEMMA 7. For $n \geq 2$ and any variable-free term u:

$$\mathrm{cut}(\chi(n+1,u), \delta(n,u)) \to^{\mathrm{c}} \chi(n, 2^u).$$

In order to prove the above lemma, we first have to treat the inner induction.

DEFINITION 6. Let $n \geq 1, k \geq 0, u$ be a variable-free term and define $\xi_{\mathrm{a}}(n,k,u) :=$

$$\dfrac{\dfrac{}{C_n\langle u\rangle \to C_n\langle u\rangle} \quad \begin{matrix}(\xi(n,k,u+2^0))\\ C_n\langle u+1\rangle \to C_n\langle u+k+1\rangle\end{matrix}}{C_n\langle u\rangle, C_{n+1}\langle 0\rangle \to C_n\langle u+k+1\rangle}\ \forall_{\mathrm{l}}, \supset_{\mathrm{l}}$$

LEMMA 8. For $n \geq 1, k \geq 0$ and any variable-free term u:

$$\mathrm{cut}(\chi(n+1,0), \xi_{\mathrm{a}}(n,k,u)) \to^{\mathrm{c}} \xi(n,k+1,u)$$

PROOF. Abbreviate

$$\dfrac{\begin{matrix}(\gamma(n-1,2,u,\alpha))\\ [C_n\langle u\rangle]^2, C_{n-1}\langle\alpha\rangle \to C_{n-1}\langle\alpha + 2^{u+1}\rangle\end{matrix}}{[C_n\langle u\rangle]^2 \to C_n\langle u+1\rangle}\ \forall_{\mathrm{r}}, \supset_{\mathrm{r}}$$

as ξ' and for $i = 0, \ldots, 2^k$ abbreviate $C_{n-1}\langle\alpha + i \cdot 2^{u+1}\rangle$ as F_i. We have

$$\mathrm{cut}(\chi(n+1,0), \xi_{\mathrm{a}}(n,k,u)) \to^{\mathrm{c}} \mathrm{cut}(\xi(n,1,u), \xi(n,k,u+2^0)) \to^{\mathrm{c}}$$

$$\dfrac{\dfrac{\dfrac{\begin{matrix}(\xi')\\ [C_n\langle u\rangle]^2 \to C_n\langle u+1\rangle\end{matrix} \quad \dfrac{\overline{F_{2^k-1}}}{C_n\langle u+1\rangle, F_{2^k-1} \to F_{2^k}}\ \forall_{\mathrm{l}}, \supset_{\mathrm{l}} \quad \overline{F_{2^k}}}{[C_n\langle u\rangle]^2, F_{2^k-1} \to F_{2^k}}\ \mathrm{cut}}{\vdots}}{\dfrac{\dfrac{\begin{matrix}(\xi')\\ [C_n\langle u\rangle]^2 \to C_n\langle u+1\rangle\end{matrix} \quad \dfrac{\overline{F_0} \quad [C_n\langle u\rangle]^{2^{k+1}-2}, F_1 \to F_{2^k}}{[C_n\langle u\rangle]^{2^{k+1}-2}, C_n\langle u+1\rangle, F_0 \to F_{2^k}}\ \forall_{\mathrm{l}}, \supset_{\mathrm{l}}}{[C_n\langle u\rangle]^{2^{k+1}}, F_0 \to F_{2^k}}\ \mathrm{cut}}{[C_n\langle u\rangle]^{2^{k+1}} \to C_n\langle u+k+1\rangle}\ \forall_{\mathrm{r}}, \supset_{\mathrm{r}}}{C_n\langle u\rangle \to C_n\langle u+k+1\rangle}\ \mathrm{c}^*_{\mathrm{l}}$$

which—by induction on 2^k—reduces to $\xi(n,k+1,u)$. ⊣

PROOF OF LEMMA 7. $\mathrm{cut}(\chi(n+1,u),\delta(n,u)) \to^{\mathrm{c}} \mathrm{cut}(\chi(n,0),\xi(n,2^{|u|},0)) \to^{\mathrm{c}}$

$$\dfrac{\dfrac{(\chi(n,0))\ \to C_n\langle 0\rangle \qquad \dfrac{\overline{C_{n-1}\langle\alpha+2^{2^u}-1\rangle} \qquad \overline{C_{n-1}\langle\alpha+2^{2^u}\rangle}}{C_n\langle 0\rangle, C_{n-1}\langle\alpha+2^{2^u}-1\rangle \to C_{n-1}\langle\alpha+2^{2^u}\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}}{C_{n-1}\langle\alpha+2^{2^u}-1\rangle \to C_{n-1}\langle\alpha+2^{2^u}\rangle}\ \mathrm{cut}}{\vdots}$$

$$\dfrac{\dfrac{(\chi(n,0))\ \to C_n\langle 0\rangle \qquad \dfrac{\overline{C_{n-1}\langle\alpha\rangle} \qquad C_{n-1}\langle\alpha+1\rangle \to C_{n-1}\langle\alpha+2^{2^u}\rangle}{C_n\langle 0\rangle, C_{n-1}\langle\alpha\rangle \to C_{n-1}\langle\alpha+2^{2^u}\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}}{C_{n-1}\langle\alpha\rangle \to C_{n-1}\langle\alpha+2^{2^u}\rangle}\ \mathrm{cut}}{\to C_n\langle 2^u\rangle}\ \forall_{\mathrm{r}},\supset_{\mathrm{r}}$$

which—by induction on 2^{2^u} using Lemma 8 in each step—reduces to $\chi(n,2^u)$. ⊣

Up to this point, the axioms Z_I and S_I have not entered the picture. They correspond to $C_0(0)$ and $C_1(0)$ and are inserted into the proof in the last two steps.

DEFINITION 7. Let $k \geq 0$, u be a term and define $\gamma'(k,u) :=$

$$\dfrac{\dfrac{\overline{I\langle u+k-1\rangle \to I\langle u+k-1\rangle} \qquad \overline{I\langle u+k\rangle \to I\langle u+k\rangle}}{I\langle u+k-1\rangle, S_I \to I\langle u+k\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}}{\vdots}$$

$$\dfrac{\overline{I\langle u\rangle \to I\langle u\rangle} \qquad I\langle u+1\rangle, [S_I]^{k-1} \to I\langle u+k\rangle}{I\langle u\rangle, [S_I]^k \to I\langle u+k\rangle}\ \forall_{\mathrm{l}},\supset_{\mathrm{l}}$$

and $\gamma^*(k) :=$

$$\dfrac{(\gamma'(k,0))\ Z_I, [S_I]^k \to I\langle k\rangle}{Z_I, S_I \to I\langle k\rangle}\ \mathrm{c}^*_{\mathrm{l}}$$

PROPOSITION 6. For $n \geq 2$: $\psi_n \to^{\mathrm{c}} \gamma^*(2_n)$.

PROOF. By repeated application of Lemma 7, $\psi_n \to^{\mathrm{c}}$

$$\dfrac{\dfrac{(\chi(2,\mathrm{tt}_{n-2}))\ \to C_2\langle \mathrm{tt}_{n-2}\rangle \qquad (\delta(1,\mathrm{tt}_{n-2}))\ S_I, C_2\langle \mathrm{tt}_{n-2}\rangle \to C_1\langle \mathrm{tt}_{n-1}\rangle}{S_I \to C_1\langle \mathrm{tt}_{n-1}\rangle}\ \mathrm{cut} \qquad (\delta(0,\mathrm{tt}_{n-1}))\ Z_I, C_1\langle \mathrm{tt}_{n-1}\rangle \to C_0\langle \mathrm{tt}_n\rangle}{Z_I, S_I \to C_0\langle \mathrm{tt}_n\rangle}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{\dfrac{\dfrac{(\gamma'(2_n,\alpha))\ [S_I]^{2_n}, I\langle\alpha\rangle \to I\langle\alpha+\mathrm{tt}_n\rangle}{S_I, I\langle\alpha\rangle \to I\langle\alpha+\mathrm{tt}_n\rangle}\ \mathrm{c}^*_{\mathrm{l}}}{S_I \to C_1\langle \mathrm{tt}_{n-1}\rangle}\ \forall_{\mathrm{r}},\supset_{\mathrm{r}} \qquad (\delta(0,\mathrm{tt}_{n-1}))\ Z_I, C_1\langle \mathrm{tt}_{n-1}\rangle \to C_0\langle \mathrm{tt}_n\rangle}{Z_I, S_I \to C_0\langle \mathrm{tt}_n\rangle}\ \mathrm{cut}$$

$$\to^{\mathrm{c}} \quad \gamma^*(2_n).$$ ⊣

§5. Strong non-confluence. We are now approaching the main result of this paper: the definition of a proof sequence posessing a non-elementary number of different normal forms under cut-elimination. The basic idea underlying the construction is to modify the sequence $(\psi_n)_{n\geq 0}$ to the following end: instead of showing that $I(\cdot)$ holds for large numbers, we will—given a first-order signature Σ—show that there exist terms over Σ that have a large depth. By making suitable use of the non-confluent building blocks described in Section 3, the existence of a large term will be shown in a way that permits reduction to *any* witness term of the required depth.

We augment our language by a unary function symbol $d(\cdot)$ that will be used to encode the depth of terms and we also add the relation symbol $\leq$ whose intended interpretation is the usual one on the natural numbers. To our axiom set $\mathscr{A}$ we add

$$\forall x \forall y\, (x = y \supset x \leq y),$$
$$\forall x \forall y\, (x \leq y \supset x \leq s(y)),$$
$$\forall x_1 \forall x_2 \forall y_1 \forall y_2\, (x_1 = y_1 \supset x_2 = y_2 \supset x_1 \leq x_2 \supset y_1 \leq y_2).$$

We assume given a finite first-order signature Σ which is disjoint from the signature considered so far and contains at least one constant symbol and at least one function symbol. For each constant symbol $c \in \Sigma$ we add

$$d(c) = 0$$

to $\mathscr{A}$ and for each function symbol $f \in \Sigma$ of arity r and for $j = 1, \ldots, r$ we add

$$T_f^j \equiv \forall n \forall x_1 \ldots \forall x_r (d(x_1) \leq n \supset \cdots \supset d(x_{j-1}) \leq n \supset d(x_j) = n$$
$$\supset d(x_{j+1}) \leq n \supset \cdots \supset d(x_r) \leq n \supset d(f(x_1, \ldots, x_r)) = s(n))$$

to $\mathscr{A}$. We define the formula abbreviations

$$L(n) \equiv \exists x\, d(x) \leq n, \quad E(n) \equiv \exists x\, d(x) = n, \text{ and } \quad F(n) \equiv L(n) \wedge E(n)$$

with the aim of considering the substitution instance $(\psi_n\{I \leftarrow F\})_{n\geq 0}$. The rationale for using F here and not E is that during reduction, the chosen formula will act like an induction hypothesis and the introduction of $\leq$ will allow us to also reduce to such witness terms that contain branches of different depths. A marginally simpler sequence, using only E, with the same property of posessing a non-elementary number of different normal forms can be constructed if one is willing to restrict the set of reachable witness terms to those having only branches of maximal depth.

Having fixed F, it is now time to re-examine our axiom set $\mathscr{A}$. It includes three axioms that contain I and—under the substitution $\{I \leftarrow F\}$—they will become

$$C_F \equiv \forall x \forall y\, (x = y \supset F(x) \supset F(y)),$$
$$Z_F \equiv F(0),$$
$$S_F \equiv \forall x\, (F(x) \supset F(s(x))).$$

These formulas can be proved from the rest of $\mathscr{A}$ and thus be removed from the end-sequents of our sequence by appending additional cuts to $\psi_n\{I \leftarrow F\}$. Indeed, the key to obtaining a strong non-confluence lies in *how* these formulas will be proved. In this regard, there clearly is not much to be expected from the first, the compatibility of equality w.r.t. F. The proofs of the second and the third however provide the induction basis and step respectively of the witness term construction.

Consequently, it will be a seed of non-confluence implanted into these two proofs that, by the large increase of proof length, will proliferate to yield a non-elementary number of different normal forms. In the following three sections we describe the proofs of the above three formulas.

5.1. Compatibility. Let

$$\tau_{C_L}(u,v) := \dfrac{\begin{array}{c}\vdots\\ u=v, d(\gamma)\leq u \to d(\gamma)\leq v\end{array}}{u=v, L(u)\to L(v)}\ \exists_{\mathrm{l}}, \exists_{\mathrm{r}}$$

and let $\tau_{C_E}(u,v)$ be the analogous proof of $u=v, E(u)\to E(v)$. Let

$$\tau'_C(u,v) := \dfrac{\begin{array}{cc}(\tau_{C_L}) & (\tau_{C_E})\\ u=v, L(u)\to L(v) & u=v, E(u)\to E(v)\end{array}}{u=v, F(u)\to F(v)}\ \mathrm{c}^*_{\mathrm{l}}, \wedge_{\mathrm{l}_1}, \wedge_{\mathrm{l}_2}, \wedge_{\mathrm{r}}$$

and

$$\tau_C := \dfrac{\dfrac{\begin{array}{c}(\tau'_C(\alpha,\beta))\\ \alpha=\beta, F(\alpha)\to F(\beta)\end{array}}{\to \alpha=\beta\supset(F(\alpha)\supset F(\beta))}\ \supset^*_{\mathrm{r}}}{\to \forall x\forall y(x=y\supset(F(x)\supset F(y)))}\ \forall^*_{\mathrm{r}}$$

5.2. Non-deterministic constant witnesses. For each constant symbol $c\in\Sigma$, define

$$\gamma^{\leq}_c := \dfrac{\to d(c)\leq 0}{\to L(0)}\ \exists_{\mathrm{r}} \quad \text{and} \quad \gamma^{=}_c := \dfrac{\to d(c)=0}{\to E(0)}\ \exists_{\mathrm{r}}$$

Let $c_1,\ldots,c_n$ be the constant symbols in Σ, define

$$\gamma^{\leq} := \pi(\gamma^{\leq}_{c_1},\ldots,\gamma^{\leq}_{c_n}), \quad \gamma^{=} := \pi(\gamma^{=}_{c_1},\ldots,\gamma^{=}_{c_n})$$

and

$$\tau_0 := \dfrac{\begin{array}{cc}(\gamma^{\leq}) & (\gamma^{=})\\ \to L(0) & \to E(0)\end{array}}{\to F(0)}\ \wedge_{\mathrm{r}}$$

The above proof allows the production of arbitrary constant witnesses because $\tau^{\leq} \to^{\mathrm{c}} \widetilde{\tau^{\leq}_{c_i}}$ and $\tau^{=} \to^{\mathrm{c}} \widetilde{\tau^{=}_{c_i}}$ for all $i\in\{1,\ldots,n\}$ by Proposition 3 and a proof has exactly the same witnesses as any of its variants.

5.3. Non-deterministic function witnesses. Finally, we have to prove $\forall x(F(x)\supset F(s(x)))$ from $\mathscr{A}$ in a way which permits reduction to any possible witness. Proving this formula amounts to proving both $E(s(u))$ and $L(s(u))$ from $F(u)$. For $E(s(u))$ we proceed as follows: for $r\in\mathbb{N}$ and $j\in\{1,\ldots,r\}$ define the set of formulas

$$\Gamma^r_j(u) := d(\alpha_1)\leq u,\ldots,d(\alpha_{j-1})\leq u, d(\alpha_j)=u, d(\alpha_{j+1})\leq u,\ldots,d(\alpha_r)\leq u$$

We will often abbreviate $\alpha_1, \ldots, \alpha_r$ as $\vec{\alpha}$ if r is clear from the context. Let f be a function symbol from Σ, r be the arity of f and define

$$\varphi^{=}_{f,j}(u) := \dfrac{\dfrac{\vdots}{\Gamma^r_j(u) \to d(f(\vec{\alpha})) = s(u)}\ \exists_{\mathrm{r}}}{\Gamma^r_j(u) \to E(s(u))}\ \mathrm{c}^*_{\mathrm{l}}, \wedge^*_{\mathrm{l}_1}, \wedge_{\mathrm{l}_2}, \exists^*_{\mathrm{l}}$$

This proof provides a witness for $E(s(u))$ that has f as top-level symbol and whose j-th branch is guaranteed to have sufficient depth. We then combine these proofs by defining

$$\varphi^{=}_{f}(u) := \pi(\varphi^{=}_{f,1}(u), \ldots, \varphi^{=}_{f,\mathrm{ar}(f)}(u))$$

and for $f_1, \ldots, f_n$ being all function symbols in Σ

$$\varphi^{=}(u) := \pi(\varphi^{=}_{f_1}(u), \ldots, \varphi^{=}_{f_n}(u)).$$

So by Proposition 3 and Lemma 3: $\varphi(u) \to^{\mathrm{c}} \widetilde{\varphi^{=}_{f,j}(u)}$ for all function symbols f in Σ and all $j \in \{1, \ldots, \mathrm{ar}(f)\}$.

To prove $L(s(u))$ from $\mathscr{A}$ we have two possibilities: we can choose a witness term of depth $|s(u)|$ as done in

$$\varphi^{\leq}_{f,j}(u) := \dfrac{\dfrac{\vdots}{\Gamma^r_j(u) \to d(f(\vec{\alpha})) \leq s(u)}\ \exists_{\mathrm{r}}}{\Gamma^r_j(u) \to L(s(u))}\ \mathrm{c}^*_{\mathrm{l}}, \wedge^*_{\mathrm{l}_1}, \wedge_{\mathrm{l}_2}, \exists^*_{\mathrm{l}}$$

Secondly, we can also choose a witness term of depth strictly less than $|s(u)|$ as in

$$\varphi^{<}(u) := \dfrac{\dfrac{\vdots}{d(\beta) \leq u \to d(\beta) \leq s(u)}\ \exists_{\mathrm{r}}}{d(\beta) \leq u \to L(s(u))}\ \wedge_{\mathrm{l}_1}, \exists_{\mathrm{l}}$$

We define

$$\varphi^{\leq}_{f}(u) := \pi(\varphi^{\leq}_{f,1}(u), \ldots, \varphi^{\leq}_{f,\mathrm{ar}(f)}(u))$$

and

$$\varphi^{\leq}(u) := \pi(\varphi^{<}, \varphi^{\leq}_{f_1}(u), \ldots, \varphi^{\leq}_{f_n}(u)).$$

Define

$$\tau_s := \dfrac{(\tau'_s(\alpha))}{\to (\forall x)(F(x) \supset F(s(x)))}\ \forall_{\mathrm{r}}, \supset_{\mathrm{r}}$$

where

$$\tau'_s(u) := \dfrac{(\varphi^{\leq}(u)) \quad (\varphi^{=}(u))}{F(u) \to F(s(u))}\ \mathrm{c}_{\mathrm{l}}, \wedge_{\mathrm{r}}$$

5.4. A strongly non-confluent sequence. The main result of this paper is the following theorem which will be proved in the current section.

THEOREM 1. Let Σ be a finite signature containing at least one constant symbol and at least one function symbol. Then there is a sequence $(\chi_n)_{n\geq 1}$ of weakening-free proofs s.t. χ_n proves $\mathscr{A} \to \exists x\, d(x) = \mathrm{tt}_n$, $|\chi_n|$ is polynomial in n and for any term t over Σ with $\mathrm{depth}(t) = 2_n$ there is a normal form $\xi(t)$ of χ_n where t is the only witness of $(\exists x)$.

Define χ_n as

$$\dfrac{\dfrac{(\tau_s)\ \to S_F \qquad \dfrac{(\tau_0)\ \to Z_F \qquad \dfrac{(\tau_C)\ \to C_F \quad (\psi_n^*\{I \leftarrow F\})\ C_F, Z_F, S_F \to F(\mathrm{tt}_n)}{Z_F, S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut} \qquad \dfrac{E(\mathrm{tt}_n) \to E(\mathrm{tt}_n)}{F(\mathrm{tt}_n) \to E(\mathrm{tt}_n)}\ \wedge_{l_2}}{\to F(\mathrm{tt}_n) \qquad\qquad\qquad\qquad F(\mathrm{tt}_n) \to E(\mathrm{tt}_n)}\ \mathrm{cut}}{\to E(\mathrm{tt}_n)}\ \mathrm{cut}$$

where ψ_n^* is the translation of ψ_n from **LK'** to **LK**. Observe that χ_n is of length polynomial in n as ψ_n is. The rest of this section is devoted to describing a cut-elimination strategy that produces a normal form with t as witness. Its first part will be general and only in the end will it depend on the given t.

DEFINITION 8. A proof ω of $F(u) \to F(v)$ is called *witness-preserving* if for any cut-free proof χ of $\Gamma \to F(u)$ there is a cut-free proof χ' s.t.

$$\dfrac{(\chi)\ \Gamma \to F(u) \quad (\omega)\ F(u) \to F(v)}{\Gamma \to F(v)}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad (\chi')\ \Gamma \to F(v)$$

and the witnesses of the existential quantifiers of $F(v)$ in χ' are those of $F(u)$ in χ.

LEMMA 9. Let ε be a proof of the form $\overline{I(u_1) \to I(u_2)}$, then

$$\dfrac{(\tau_C)\ \to C_F \quad (\varepsilon\{I \leftarrow F\})\ C_F, F(u_1) \to F(u_2)}{F(u_1) \to F(u_2)}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad (\omega)\ F(u_1) \to F(u_2)$$

s.t. ω is cut-free and witness-preserving.

PROOF. All axioms in $\varepsilon\{I \leftarrow F\}$ are of the form $F(v) \to F(v)$ or $v = w \to v = w$ and thus already $\mathrm{cut}(\tau_C, \varepsilon\{I \leftarrow F\})$ is witness-preserving. Eliminating the universal quantifier and the two implications from the cut turns inference patterns of the form

$$\dfrac{(\tau_C)\ \to C_F \qquad \dfrac{(\chi_3)\ \Gamma_3 \to \Delta_3, v_1 = v_2 \qquad \dfrac{(\chi_1)\ \Gamma_1 \to \Delta_1, F(v_1) \quad (\chi_2)\ F(v_2), \Gamma_2 \to \Delta_2}{F(v_1) \supset F(v_2), \Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2}\ \supset_l}{C_F, \Gamma \to \Delta}\ \forall_1^*, \supset_l}{\Gamma \to \Delta}\ \mathrm{cut}$$

into

$$\dfrac{\dfrac{\dfrac{(\chi_3)}{\Gamma_3 \to \Delta_3, v_1 = v_2} \quad \dfrac{\dfrac{(\chi_1)}{\Gamma_1 \to \Delta_1, F(v_1)} \quad \dfrac{(\tau'_C(v_1,v_2))}{v_1 = v_2, F(v_1) \to F(v_2)}\ \text{cut}}{v_1 = v_2, \Gamma_1 \to \Delta_1, F(v_2)} \quad \dfrac{(\chi_2)}{F(v_2), \Gamma_2 \to \Delta_2}\ \text{cut}}{v_1 = v_2, \Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2}\ \text{cut}}{\Gamma \to \Delta}$$

Now axioms as well as $\tau'_C(v_1, v_2)$ are witness-preserving and the composition (by a cut) of witness-preserving proofs is witness-preserving, thus the original axioms $F(v) \to F(v)$ of $\varepsilon\{I \leftarrow F\}$ are turned into witness-preserving proofs and therefore ω itself is witness-preserving. ⊣

DEFINITION 9. An *F-chain of length* 0 is a proof of the form

$$\dfrac{\dfrac{(\tau_0)}{\to F(0)} \quad \dfrac{(\omega)}{F(0) \to F(u)}\ \text{cut}}{\to F(u)}$$

where ω is witness-preserving. An *F-chain of length $l+1$* is a proof of the form

$$\dfrac{\dfrac{\dfrac{(\xi)}{\to F(u)} \quad \dfrac{(\tau'_s(u))}{F(u) \to F(s(u))}\ \text{cut}}{\to F(s(u))} \quad \dfrac{(\omega)}{F(s(u)) \to F(v)}\ \text{cut}}{\to F(v)}$$

where ξ is an F-chain of length l and ω is witness-preserving.

LEMMA 10. Let u be a variable-free term, let χ be an F-chain with end-sequent $\to F(u)$, let $e_=$ be the existential quantifier in $E(u)$ and $e_\leq$ that in $L(u)$, then

1. For any term t over Σ of depth $|u|$ there is a cut-free proof χ' s.t. $\chi \to^{\mathrm{c}} \chi'$ and t is the only witness of $e_=$.
2. For any term t over Σ of depth at most $|u|$ there is a cut-free proof χ' s.t. $\chi \to^{\mathrm{c}} \chi'$ and t is the only witness of $e_\leq$.

PROOF. By induction on $|u|$. If $|u| = 0$, then t is a constant symbol c and

$$\chi \quad \to^{\mathrm{c}} \quad \dfrac{\dfrac{(\widetilde{\gamma^{\leq}_c})}{\to L(0)} \quad \dfrac{(\widetilde{\gamma^{=}_c})}{\to E(0)}\ \wedge_{\mathrm{r}}}{\to F(0)} \quad \dfrac{(\omega)}{F(0) \to F(u)}\ \text{cut}}{\to F(u)}$$

As c is the only witness of the existential quantifier in $\gamma^{\leq}_c$ ($\gamma^{=}_c$) it is the only witness in $\widetilde{\gamma^{\leq}_c}$ ($\widetilde{\gamma^{=}_c}$) and the claim follows from ω being witness-preserving.

If $|u| = n+1$ and t has depth $n+1$, then $t = f(t_1, \ldots, t_r)$ and there is a $j \in \{1, \ldots, r\}$ s.t. t_j has depth n. Letting ξ be the F-chain of length n, observe that

$\mathrm{cut}(\xi, \tau'_s(u)) \to^{\mathrm{c}}$

$$\dfrac{\dfrac{(\xi)}{\to F(u)} \quad \dfrac{(\widetilde{\varphi^{\leq}_{f,j}})}{F(u) \to L(s(u))}\ \mathrm{cut}}{\to L(s(u))} \quad \dfrac{\dfrac{(\xi)}{\to F(u)} \quad \dfrac{(\widetilde{\varphi^{=}_{f,j}})}{F(u) \to E(s(u))}\ \mathrm{cut}}{\to E(s(u))}\ \wedge_{\mathrm{r}}}{\to F(s(u))}$$

Now observe that

$$\mathrm{cut}(\xi, \varphi^{=}_{f,j}(u)) \to^{\mathrm{c}} \dfrac{\dfrac{(\xi)}{\to F(u)} \quad \dfrac{\dfrac{\dfrac{\vdots}{\Gamma^r_j(u) \to d(\vec{f}(\vec{\alpha})) = s(u)}\ \exists_{\mathrm{r}}}{\Gamma^r_j(u) \to E(s(u))}}{[F(u)]^r \to E(s(u))}\ \wedge^*_{\mathrm{l}_1}, \wedge_{\mathrm{l}_2}, \exists^*_{\mathrm{l}}\ \mathrm{cut}}{[F(u)]^{r-1} \to E(s(u))} \quad \dfrac{\dfrac{(\xi)}{\to F(u)} \quad \dfrac{\vdots}{F(u) \to E(s(u))}}{\to E(s(u))}$$

which is the key step for creating a tree-structure from the original linear structure step-by-step. By induction hypothesis the j-th copy of ξ can be reduced to a cut-free proof having t_j as the only witness of its $=$-quantifier and all other copies of ξ are reduced to cut-free proofs having t_i $(i \neq j)$ as only witness of its respective $\leq$-quantifier. Eliminating the remaining cuts results in a cut-free proof $\xi^{=}$ of $\to E(s(u))$ having t as only witness of the $=$-quantifier. Analogously $\mathrm{cut}(\xi, \varphi^{\leq}_{f,j}(u))$ reduces to a cut-free proof $\xi^{\leq}$ of $\to L(s(u))$ having t as only witness of the $\leq$-quantifier. We therefore obtain

$$\chi \quad \to^{\mathrm{c}} \quad \dfrac{\dfrac{(\widetilde{\xi^{\leq}})}{\to L(s(u))} \quad \dfrac{(\widetilde{\xi^{=}})}{\to E(s(u))}\ \wedge_{\mathrm{r}}}{\to F(s(u))} \quad \dfrac{(\omega)}{F(s(u)) \to F(v)}\ \mathrm{cut}}{\to F(v)}$$

and claim 1 as well as claim 2 for the depth of t being $|u|$ follows as ω is witness-preserving.

For the case of t having depth at most n, observe that $\chi \to^{\mathrm{c}}$

$$\dfrac{\dfrac{\dfrac{(\xi')}{\to F(u)} \quad \dfrac{(\widetilde{\varphi^{<}(u)})}{F(u) \to L(s(u))}\ \mathrm{cut}}{\to L(s(u))} \quad \dfrac{(\xi^*)}{\to E(s(u))}\ \wedge_{\mathrm{r}}}{\to F(s(u))} \quad \dfrac{(\omega)}{F(s(u)) \to F(v)}\ \mathrm{cut}}{\to F(v)}$$

where ξ' is a cut-free proof having t as only witness of its $\leq$-quantifier which can be obtained by the induction hypothesis and ξ^* is an arbitrary cut-free proof. Furthermore $\mathrm{cut}(\xi', \varphi^{<}(u))$ reduces to a cut-free proof which contains t as only witness for its $\leq$-quantifier. The claim then follows from ω being witness-preserving. $\dashv$

PROOF OF THEOREM 1. By Proposition 6, $\psi_n\{I \leftarrow F\} \to^{\mathrm{c}} \gamma^*(2_n)\{I \leftarrow F\}$ is an **LK**'-reduction sequence so by Lemma 6 and the observation that $\gamma^*(2_n)$ is in the intersection of **LK** and **LK**', $\chi_n \to^{\mathrm{c}} \widetilde{\xi_n}$ where ξ_n is

$$\dfrac{\dfrac{(\tau_s)\ \to S_F \qquad \dfrac{(\tau_0)\ \to Z_F \qquad \dfrac{(\tau_C)\ \to C_F \qquad (\gamma_n^*(2_n)\{I \leftarrow F\})\ C_F, Z_F, S_F \to F(\mathrm{tt}_n)}{Z_F, S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{\to F(\mathrm{tt}_n)}\ \mathrm{cut}$$

plus the final cut deriving E from F. Furthermore, ξ_n reduces to

$$\dfrac{\dfrac{(\tau_s)\ \to S_F \qquad \dfrac{(\tau_0)\ \to Z_F \qquad \dfrac{\dfrac{(\omega_0)\ F(0) \to F\langle 0\rangle \qquad \dfrac{\dfrac{(\omega_{2_n-1})\ F\langle 2_n-1\rangle \to F\langle 2_n-1\rangle \qquad (\omega_{2_n})\ F\langle 2_n\rangle \to F(\mathrm{tt}_n)}{F\langle 2_n-1\rangle, S_F \to F(\mathrm{tt}_n)}\ \forall_1, \supset_1}{\vdots}}{F\langle 1\rangle, [S_F]^{2_n-1} \to F(\mathrm{tt}_n)}\ \forall_1, \supset_1}{Z_F, [S_F]^{2_n} \to F(\mathrm{tt}_n)}\ \mathrm{c}_1^*}{Z_F, S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{S_F \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{\to F(\mathrm{tt}_n)}\ \mathrm{cut}$$

where—by Lemma 9—the ω_i are witness-preserving. After elimination of the universal quantifier and the implication in S_F, we obtain

$$\dfrac{\dfrac{(\tau_0)\ \to F(0) \qquad \dfrac{\dfrac{(\omega_0)\ F(0) \to F\langle 0\rangle \qquad \dfrac{\dfrac{(\tau_s'\langle 2_n-1\rangle)\ F\langle 2_n-1\rangle \to F\langle 2_n\rangle \qquad (\omega_{2_n})\ F\langle 2_n\rangle \to F(\mathrm{tt}_n)}{F\langle 2_n-1\rangle \to F\langle 2_n\rangle}\ \mathrm{cut}}{\vdots}}{F\langle 0\rangle \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{F(0) \to F(\mathrm{tt}_n)}\ \mathrm{cut}}{\to F(\mathrm{tt}_n)}\ \mathrm{cut}$$

which can be turned into an F-chain of length 2_n by permutations of inferences over cuts. Now, by applying Lemma 10 we obtain an arbitrary witness term for the existential quantifier in $E(\mathrm{tt}_n)$. ⊣

§6. Herbrand-skeletons. The above Theorem 1 shows not only that there is a non-elementary number of different sequent calculus proofs which are normal forms of χ_n, but also that the induced Herbrand-disjunctions of these normal forms differ. We can further strengthen this result by showing that even the abstract logical structures of the induced Herbrand-disjunctions are different. To that aim, we introduce Herbrand-skeletons which relate to Herbrand-disjunctions as proof skeletons [13, 14, 11] relate to proofs. Herbrand-skeletons are also closely related to the mating method [1] for automated theorem proving.

Let s be a prenex sequent without strong quantifiers. A sequent s' is called *Herbrand-sequent* of s if s' consists of quantifier-free instances of formulas from s

and s' is a tautology. A sequent E is called *expansion* of s if every formula in E is a quantifier-free instance of a formula on the same side of s. An expansion E is called *generic* if all its substitutions are variable-renamings, injective and have pairwise disjoint ranges.

Let E be an expansion of s and let $\equiv$ be an equivalence relation on the atoms of E. The pair $(E, \equiv)$ is called *unifiable* if there is a substitution θ s.t. all pairs in $\equiv \theta$ are syntactic equalities. Every unifiable $(E, \equiv)$ has a most general unifier (mgu), see e.g., [2]. A unifiable pair $(E, \equiv)$ is called *closed* if $A_1\theta = A_2\theta$ implies $A_1 \equiv A_2$ for θ being an mgu and A_1, A_2 being any atoms in E. A unifiable pair $(E, \equiv)$ is called *tautological*, if $E\theta$ is a tautology, for θ being an mgu.

A pair $(E, \equiv)$ is called *Herbrand-skeleton* if E is generic and $(E, \equiv)$ is unifiable, closed and tautological. For two Herbrand-skeletons $(E_1, \equiv_1)$ and $(E_2, \equiv_2)$, write $(E_1, \equiv_1) \leq (E_2, \equiv_2)$ if $E_1 \subseteq E_2$ and $\equiv_1 \subseteq \equiv_2$. A Herbrand-skeleton $(E, \equiv)$ is called *minimal* if $(E', \equiv') \leq (E, \equiv)$ implies $(E', \equiv') = (E, \equiv)$ for all Herbrand-skeletons $(E', \equiv')$. A sequent s is said to *realize* a Herbrand-skeleton $(E, \equiv)$ if there is a substitution σ s.t. $E\sigma = s$ satisfying $A_1 \equiv A_2 \Rightarrow A_1\sigma = A_2\sigma$ for all atoms A_1, A_2 in E.

Two Herbrand-skeletons $(E_1, \equiv_1)$ and $(E_2, \equiv_2)$ of s are called *isomorphic* if there is a bijection φ of the formulas of E_1 to those of E_2 which pairs only instances of the same formula of s and satisfies: $A \equiv_1 B$ iff $\varphi(A) \equiv_2 \varphi(B)$ for all atoms A, B in E_1. Let s' be a Herbrand-sequent of s. Let E be a generic expansion of s s.t. there is a bijection φ of the formulas of s' to the formulas of E which pairs only instances of the same formula of s. Let $\equiv$ be the equivalence relation on the atoms of E which is induced by syntactic identity of atoms in s' along φ. Then the Herbrand-skeleton $(E, \equiv)$ is said to be *induced by* s'. A Herbrand-skeleton induced by a cut-free proof π is the one induced by the Herbrand-sequent of π. Modulo isomorphism, each Herbrand-sequent and thus each cut-free proof induces a unique Herbrand-skeleton.

The main lemma, whose proof will occupy the rest of this section is

LEMMA 11. Let u and t be variable-free terms and let $(E, \equiv)$ be a minimal Herbrand-skeleton of $\mathscr{A} \to d(t) = u$. Then there is a unique Herbrand-sequent realizing $(E, \equiv)$.

It is the key to proving the following

THEOREM 2. Let u be a variable-free term, let χ_1, χ_2 be cut-free proofs of $\mathscr{A} \to \exists x\, d(x) = u$ having t_1 and t_2 respectively as only witness terms. If $t_1 \neq t_2$, then the Herbrand-skeletons induced by χ_1 and χ_2 do not contain isomorphic minimal Herbrand-skeletons.

PROOF. As $\mathscr{A} \to$ is not valid, each minimal Herbrand-skeleton of χ_1 (χ_2) is also a minimal Herbrand-skeleton of $\mathscr{A} \to d(t_1) = u$ ($\mathscr{A} \to d(t_2) = u$) and must contain $d(t_1) = u$ ($d(t_2) = u$) on its right side. Let $(E_1, \equiv_1)$ and $(E_2, \equiv_2)$ be minimal Herbrand-skeletons of $\mathscr{A} \to d(t_1) = u$ and $\mathscr{A} \to d(t_2) = u$ respectively. Note that t_1 and t_2 are variable-free as $\mathscr{A} \to d(t_1) = u$ and $\mathscr{A} \to d(t_2) = u$ are provable. So by Lemma 11 there are unique Herbrand-sequents s_1 and s_2 realizing $(E_1, \equiv_1)$ and $(E_2, \equiv_2)$. Now if $(E_1, \equiv_1) \cong (E_2, \equiv_2)$, then $s_1 = s_2$ and therefore $t_1 = t_2$. ⊣

6.1. Pruned proofs. In this section, we reduce the problem of finding all realizations of a minimal Herbrand-skeleton of $\mathscr{A} \to d(t) = u$ to the more manageable problem of finding all unifiers of a certain class of pseudo-proofs.

A *pseudo-proof* is composed of axioms of the form $A \to B$ for atomic A, B and rules from **LK**. Let $(E, \equiv)$ be a Herbrand-skeleton with mgu σ, let π be a proof of $E\sigma$, then $\pi/_{(E,\equiv)}$ denotes the pseudo-proof with end-sequent E obtained from π by omitting the mgu.

A formula is called *implicational* if it is an atom or of the form $A \supset G$ for an atom A and an implicational formula G. A sequent $\Gamma \to A$ is called implicational if A is an atom and all formulas in Γ are implicational. A proof is called *pruned* if it contains only $\supset_l$- and atomic contraction-left-inferences.

LEMMA 12. Let s be an implicational tautological sequent. Then there is an $s' \subseteq s$ which has a pruned proof.

PROOF. We describe a sequence of cut-free proofs

$$\chi_0, \chi_0', \chi_0'', \chi_0''', \chi_1, \chi_1', \chi_1'', \chi_1''', \ldots, \chi_n, \chi_n', \chi_n''$$

s.t. χ_n'' is a pruned proof of a sequent $s' \subseteq s$. For χ_0 we take any cut-free proof of s. As s is implicational and all the proofs in the sequence are cut-free they only consist of $\supset_l$-inferences, weakenings and contractions. We let χ_i' be any $\to^w$-normal form of χ_i; χ_i'' is χ_i' without its final weakenings and thus consists of $\supset_l$-inferences and contractions only.

Claim. Let χ be a proof containing only $\supset_l$ and contraction. Then all sequents in χ have exactly one formula on the right side.

PROOF OF THE CLAIM. By induction on χ: The claim is clearly true for the axioms and is inherited by contractions on the left. The only other rule appearing in χ is $\supset_l$ and in

$$\frac{\Gamma_1 \to \Delta_1, A \quad B, \Gamma_2 \to \Delta_2}{A \supset B, \Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2}\ \supset_l$$

$|\Delta_1 \cup \Delta_2| > 1$ implies $|\Delta_1| > 0$ or $|\Delta_2| > 1$ both of which contradict the induction hypothesis. ⊣

So all χ_i'' consist of $\supset_l$-inferences and contractions on the left only. Let the weight of a contraction be the number of logical symbols in the contracted formula and the weight $w(\chi)$ of a proof χ be the sum over the weights of all its contractions. Let c be a contraction in χ_i'' s.t. there are direct ancestor paths (i.e., paths that do not contain active formulas of other contractions) to the main formulas of $\supset_l$-inferences i_1 and i_2. By inference permutations we obtain a proof χ_i''' with $w(\chi_i''') = w(\chi_i'')$ containing one of the following inference patterns:

$$\dfrac{\dfrac{\dfrac{}{}\,i_1}{}\,i_2}{c} \quad , \quad \dfrac{\dfrac{}{}\,i_1}{\dfrac{}{}\,i_2}{c} \quad \text{or} \quad \dfrac{\dfrac{}{}\,i_1 \quad \dfrac{}{}\,i_2}{\supset_l}{c}$$

or one of the above where i_1 and i_2 are exchanged. In any of these cases, and for any distribution of the auxiliary formulas to proof branches, one can obtain, by a

local proof rewriting, a proof χ_{i+1} with strictly smaller weight. For example,

$$\dfrac{\dfrac{\dfrac{\Gamma_1 \to A \quad \Pi, B \to C}{\Gamma_1, \Pi, A \supset B \to C}\, i_1 \quad \dfrac{\Gamma_2 \to A \quad \Sigma, B, D \to E}{\Gamma_2, \Sigma, A \supset B, D \to E}\, i_2}{\Gamma_1, \Gamma_2, \Pi, \Sigma, A \supset B, A \supset B, C \supset D \to E}\, \supset_l}{\Gamma_1, \Gamma_2, \Pi, \Sigma, A \supset B, C \supset D \to E}\, c_l$$

rewrites to

$$\dfrac{\dfrac{\Gamma_1 \to A \quad \dfrac{\dfrac{\Pi, B \to C \quad \Sigma, B, D \to E}{\Pi, \Sigma, B, B, C \supset D \to E}\, \supset_l}{\Pi, \Sigma, B, C \supset D \to E}\, c_l}{\Gamma_1, \Pi, \Sigma, A \supset B, C \supset D \to E}\, \supset_l}{\Gamma_1, \Gamma_2, \Pi, \Sigma, A \supset B, C \supset D \to E}\, w^*$$

As the weight is strictly decreasing we will eventually find a χ_n'' with weight 0 consisting of $\supset_l$- and c_l-inferences only which is a pruned proof. ⊣

LEMMA 13. Let $(E, \equiv)$ be a minimal Herbrand-skeleton with mgu θ. Then $E\theta$ has no strict subsequent which is a tautology.

PROOF. Suppose $s \subset E\theta$ is a tautology, then there is $E' \subset E$ s.t. $s = E'\theta$. Then $(E', \equiv\restriction E')$ is unifiable with some mgu σ and we have $A_1\sigma = A_2\sigma \Rightarrow A_1\theta = A_2\theta$ for all atoms $A_1, A_2 \in E'$. As $(E, \equiv)$ is unifiable and closed, $A_1 \equiv A_2$ iff $A_1\theta = A_2\theta$ for all atoms $A_1, A_2 \in E$. Let $\equiv'$ be the closure of $\equiv\restriction E'$ w.r.t. E', then $(E', \equiv')$ is unifiable with mgu σ and as $A_1 \equiv' A_2$ iff $A_1\sigma = A_2\sigma$ we have $\equiv' \subseteq \equiv$. So $(E', \equiv')$ is a Herbrand-skeleton strictly smaller than $(E, \equiv)$ which contradicts minimality. ⊣

A pseudo-proof π is called *unifiable* if there is a substitution σ s.t. $\pi\sigma$ is a proof. For a pseudo-proof π of E, write $\mathrm{ax}(\pi)$ for the equivalence relation induced by the axioms of π on the atoms of E. The crucial transformation of the problem is stated in the following

LEMMA 14. Let $(E, \equiv)$ be a minimal Herbrand-skeleton of $\mathscr{A} \to d(t) = u$. Then there is a unifiable pruned pseudo-proof π of E having the same mgus as $(E, \equiv)$.

PROOF. Let σ be any mgu of $(E, \equiv)$, then $E\sigma$ is a tautological implicational sequent which by Lemmas 13 and 12 has a pruned proof ψ. Then $\pi := \psi/_{(E,\equiv)}$ is a pruned pseudo-proof of E and as $\mathrm{ax}(\pi) \subseteq \equiv$, $(E, \mathrm{ax}(\pi))$ is unifiable. Let $\mathrm{ax}(\pi)^*$ be the closure of $\mathrm{ax}(\pi)$ w.r.t. E. Then $\mathrm{ax}(\pi)^* = \equiv$ because if $\mathrm{ax}(\pi)^* \subset \equiv$, $(E, \mathrm{ax}(\pi)^*)$ would be a Herbrand-skeleton strictly smaller than $(E, \equiv)$ contradicting minimality. Therefore π has the same mgus as $(E, \equiv)$. ⊣

We are now able to control the unification process by the following order.

DEFINITION 10. Let π be a pruned pseudo-proof of an implicational sequent E. For two axioms $A_1 \to A_2$ and $A_3 \to A_4$ in π, write $A_1 \to A_2 >_\pi^1 A_3 \to A_4$ if E contains a formula $\ldots A_2 \supset \cdots \supset A_3$ with the occurrence of A_2 in the axiom being ancestor of the occurrence of A_2 in the end-sequent and analogously for A_3. Write $>_\pi$ for the transitive closure of $>_\pi^1$.

LEMMA 15. Let π be a pruned pseudo-proof of an implicational sequent E. Then $>_\pi$ is acyclic.

PROOF. For atom occurrences A_1, A_2 in E write $A_1 \sim A_2$ if A_1 and A_2 are of opposite polarity but in the same formula and write $A_1 \operatorname{ax} A_2$ if π contains an axiom consisting of an ancestor of A_1 and one of A_2. Suppose $>_\pi$ is cyclic, then there are axioms $N_1 \to P_1 >_\pi^1 \cdots >_\pi^1 N_n \to P_n >_\pi^1 N_{n+1} \to P_{n+1} = N_1 \to P_1$ and hence formulas $\cdots P_i \supset \cdots \supset N_{i+1}$ in E for $i = 1, \ldots, n$ and therefore $\sim \cup \operatorname{ax}$ would be cyclic. We show that this is impossible by induction on π: If π is an axiom only, then $\sim \cup \operatorname{ax}$ is obviously acyclic. If the last inference of π is $\mathrm{c_l}$, then the same cycle would appear in the premise as each formula relevant for the cycle contains an implication and $\mathrm{c_l}$ is atomic. If the last inference is $\supset_\mathrm{l}$, then all ancestors of the N_i and P_i must appear in the same premise sequent, for otherwise there would be some i s.t. N_i and P_i appear in different premise sequents which is impossible by $N_i \operatorname{ax} P_i$ and therefore the same cycle appears in the premise sequent. ⊣

6.2. Unification. This section is devoted to the description of the unification process, the important invariants of which constitute the following notion of unification structure. An atom of the form $d(t) = u$, $u = d(t)$, $d(t) \leq u$, or $u \leq d(t)$ is called *d-atom*. The domain of a substitution is $\operatorname{dom}(\sigma) = \{x \mid x\sigma \neq x\}$, the variable-range is $\operatorname{vrge}(\sigma) = \bigcup_{x \in \operatorname{dom}(\sigma)} \operatorname{Var}(x\sigma)$.

DEFINITION 11. A *unification structure* is a triple (π, L, U) where π is a unifiable pruned pseudo-proof of an expansion E of $\mathscr{A} \to d(t) = u$, for t and u being variable-free terms, $\operatorname{ax}(\pi) = L \uplus U$, U is upwards-closed w.r.t. $<_\pi$, L is downwards-closed w.r.t. $<_\pi$ and the following conditions are fulfilled:

1. If $A_1 \to A_2 \in U$, then $A_1 = A_2$.
2. For all $t = s \to t = s \in U$ and all $t \leq s \to t \leq s \in U$: $\operatorname{Var}(t) = \operatorname{Var}(s)$ and if $t = s$, or $t \leq s$ respectively, is a d-atom, then $\operatorname{Var}(t) = \operatorname{Var}(s) = \emptyset$.
3. $\operatorname{Var}(E) = \operatorname{Var}(L)$.

LEMMA 16. Let (π, L, U) be a unification structure and $A_1 \to A_2$ be a $<_\pi$-maximal axiom in L. Then there is a mgu σ of $A_1 = A_2$ s.t.

$$(\pi\sigma, (L \setminus \{A_1 \to A_2\})\sigma, (U \cup \{A_1 \to A_2\})\sigma)$$

is a unification structure.

PROOF. Abbreviate $L' := (L \setminus \{A_1 \to A_2\})\sigma$, $U' := (U \cup \{A_1 \to A_2\})\sigma$. $A_1 = A_2$ is unifiable because π is, let σ be any mgu with $\operatorname{Var}(\sigma) \subseteq \operatorname{Var}(E)$. $\pi\sigma$ is a unifiable pruned pseudo-proof of the expansion $E\sigma$ of $\mathscr{A} \to d(t) = u$ where E is the end-sequent of π. $\operatorname{ax}(\pi\sigma) = L' \uplus U'$ with U' being upwards-closed and L' being downwards-closed as $A_1 \to A_2$ is maximal in L. Property 1 follows from 1 of (π, L, U) for all $B_1 \to B_2$ in $U\sigma$ and, as σ is a unifier of $A_1 = A_2$, also for $A_1\sigma \to A_2\sigma$.

Property 2 follows from 2 of (π, L, U) for all $t\sigma = s\sigma \to t\sigma = s\sigma$ and $t\sigma \leq s\sigma \to t\sigma \leq s\sigma$ in $U\sigma$, so it remains to prove it for $A_1\sigma \to A_2\sigma$. $A_1\sigma$, being a negative atom, is head atom of an implicational formula F in $E\sigma$; we make a case distinction on F: if F is a single atom, it is an instance of one of $x = x$, $x + 0 = x$, $x + s(y) = s(x + y)$, $x + (y + z) = (x + y) + z$, $2^0 = s(0)$, $2^{s(x)} = 2^x + 2^x$ or $d(c) = 0$ for a constant symbol c. In each of these cases, 2 can be verified immediately. If F is an instance of one of $x = y \supset y = x$, $x = y \supset s(x) = s(y)$, $x_1 = y_1 \supset x_2 = y_2 \supset x_1 + x_2 = y_1 + y_2$, $x = y \supset 2^x = 2^y$, $x = y \supset x \leq y$, $x \leq y \supset x \leq s(y)$,

$x = y \supset y = z \supset x = z$, $x_1 = y_1 \supset x_2 = y_2 \supset x_1 \leq x_2 \supset y_1 \leq y_2$ or T_f^j for a function symbol f note that due to $A_1\sigma \to A_2\sigma$ being a minimal element of U', all body atoms of F are in $U\sigma$ and 2 for $A_1\sigma \to A_2\sigma$ follows from 2 for these body atoms.

For showing 3 it is enough to prove $\mathrm{Var}(E\sigma) \subseteq \mathrm{Var}(L')$, the other direction follows immediately from $\pi\sigma$ being cut-free. Let $u \in \mathrm{Var}(E\sigma)$, then, by the choice of σ, $u \in \mathrm{Var}(E)$ and thus by 3 of (π, L, U) also $u \in \mathrm{Var}(L)$. As σ is a unifier, $\mathrm{dom}(\sigma) \cap \mathrm{vrge}(\sigma) = \emptyset$, thus $u \notin \mathrm{dom}(\sigma)$ and therefore $u \in \mathrm{Var}(L\sigma)$. It remains to show that $u \in \mathrm{Var}(A_1\sigma \to A_2\sigma)$ implies $u \in \mathrm{Var}(L\sigma)$ which, as $L' = L\sigma \setminus \{A_1\sigma \to A_2\sigma\}$, implies $\mathrm{Var}(L') = \mathrm{Var}(L\sigma)$ and hence 3. $A_2\sigma$, being a positive atom, is either $d(t) = u$, in which case it is variable-free, or a body atom in an implicational formula F in $E\sigma$, whose head atom is in $L\sigma$. We make a case distinction on F: if F is an instance of one of $x = y \supset y = x$, $x = y \supset s(x) = s(y)$, $x_1 = y_1 \supset x_2 = y_2 \supset x_1 + x_2 = y_1 + y_2$, $x = y \supset 2^x = 2^y$, $x = y \supset x \leq y$, $x \leq y \supset x \leq s(y)$ or T_f^j for a function symbol f, then u also appears in the head atom and thus $u \in \mathrm{Var}(L\sigma)$. Assume F is $x\theta = y\theta \supset y\theta = z\theta \supset x\theta = z\theta$; if $u \in \mathrm{Var}(x\theta)$ or $u \in \mathrm{Var}(z\theta)$, then $u \in \mathrm{Var}(L\sigma)$; if $u \in \mathrm{Var}(y\theta)$ and $A_2\sigma$ is $x\theta = y\theta$, then, as $A_2\sigma$ is in U', by 2 $u \in \mathrm{Var}(x\theta)$ and thus $u \in \mathrm{Var}(L\sigma)$; analogous for $A_2\sigma$ being $y\theta = z\theta$. Assume F is $x_1\theta = y_1\theta \supset x_2\theta = y_2\theta \supset x_1\theta \leq x_2\theta \supset y_1\theta \leq y_2\theta$; if $A_2\sigma$ is $x_1\theta = y_1\theta$, then, as $A_2\sigma$ is in U', by 2 $\mathrm{Var}(x_1\theta) = \mathrm{Var}(y_1\theta)$ and thus $u \in \mathrm{Var}(L\sigma)$; analogously for $A_2\sigma$ being $x_2\theta = y_2\theta$. If $A_2\sigma$ is $x_1\theta \leq x_2\theta$ then by 2 $\mathrm{Var}(x_1\theta) = \mathrm{Var}(x_2\theta)$; if one of $x_1\theta = y_1\theta$ and $x_2\theta = y_2\theta$ is in L', it is in $L\sigma$ and thus $u \in \mathrm{Var}(L\sigma)$; if one of them, wlog $x_1\theta = y_1\theta$ is in U', by applying 2 we have $\mathrm{Var}(x_1\theta) = \mathrm{Var}(y_1\theta)$ and hence $u \in \mathrm{Var}(L\sigma)$. ⊣

PROOF OF LEMMA 11. Let $(E, \equiv)$ be a minimal Herbrand-skeleton of $\mathscr{A} \to d(t) = u$ and let π be the pruned pseudo-proof of E obtained by Lemma 14. Letting L^* be the set of all axioms in π, observe that $(\pi, L^*, \emptyset)$ is a unification structure. As $<_\pi$ is acyclic (Lemma 15), a unification structure $(\pi\theta, L, U)$, for any θ and with $L \neq \emptyset$ has a $<_\pi$-maximal axiom in L. Therefore, by repeated application of Lemma 16 we eventually obtain a unification structure $(\pi\sigma, \emptyset, U^*)$ with σ being an mgu of π and by Lemma 14 also of $(E, \equiv)$. By property 3 of $(\pi\sigma, \emptyset, U^*)$, $E\sigma$ is variable-free and thus the only sequent realizing $(E, \equiv)$. ⊣

§7. Conclusion. We have shown how to construct a sequence of proofs with non-elementary many different normal forms. Our result is strengthened on the one hand by the proofs with cuts being free of weakening and on the other hand by the cut-free proofs being different in the strong sense of their Herbrand-disjunctions differing on both the term- and the propositional level.

Moreover, the proofs with cuts are completely symmetric w.r.t. their normal forms in the sense that they do not provide a reason for preferring one normal form over another. Indeed, the proved formula $\exists x\, d(x) = \mathrm{tt}_n$ blatantly admits any term of correct depth as witness and the term constructors τ^0 and τ^s do not emphasise any particular constant or function symbol since their main component is an equal combination of all of them. Therefore, any confluent restriction of cut-elimination rules out a non-elementary number of results each one as natural as the one it produces and therefore cannot be justified on mathematical grounds.

We expect this proof sequence to constitute a useful test case for other methods (than cut-elimination) for the extraction of constructive information from proofs. In particular, as future work we plan to analyse the result delivered by Gödel's Dialectica interpretation (as in [5]).

Acknowledgements. The authors would like to thank Daniel Weller and an anonymous referee for important remarks.

REFERENCES

[1] Peter B. Andrews, *Theorem proving via general matings*, ***Journal of the ACM***, vol. 28 (1981), no. 2, pp. 193–214.

[2] Franz Baader and Wayne Snyder, *Unification theory*, ***Handbook of automated reasoning*** (Alan Robinson and Andrei Voronkov, editors), Elsevier, 2001, pp. 445–533.

[3] Gerhard Gentzen, *Untersuchungen über das logische Schließen*, ***Mathematische Zeitschrift***, vol. 39 (1934–1935), pp. 176–210,405–431.

[4] ———, *Die Widerspruchsfreiheit der reinen Zahlentheorie*, ***Mathematische Annalen***, vol. 112 (1936), pp. 493–565.

[5] Philipp Gerhardy and Ulrich Kohlenbach, *Extracting Herbrand disjunctions by functional interpretation*, ***Archive for Mathematical Logic***, vol. 44 (2005), pp. 633–644.

[6] Jean-Yves Girard, ***Proof theory and logical complexity***, Elsevier, 1987.

[7] Jean-Yves Girard, Paul Taylor, and Yves Lafont, ***Proofs and types***, Cambridge University Press, 1989.

[8] Kurt Gödel, *Über eine noch nicht benützte Erweiterung des finiten Standpunktes*, ***Dialectica***, vol. 12 (1958), pp. 280–287.

[9] David Hilbert and Paul Bernays, ***Grundlagen der Mathematik II***, Springer, 1939.

[10] Ulrich Kohlenbach, ***Applied proof theory: Proof interpretations and their use in mathematics***, Springer, 2008.

[11] Jan Krajíček and Pavel Pudlák, *The number of proof lines and the size of proofs in first order logic*, ***Archive for Mathematical Logic***, vol. 27 (1988), pp. 69–84.

[12] V. P. Orevkov, *Lower bounds for increasing complexity of derivations after cut elimination*, ***Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta***, vol. 88 (1979), pp. 137–161.

[13] ———, *Reconstitution of the proof from its scheme* (*russian abstract*), ***8th Soviet Conference on Mathematical Logic***, 1984.

[14] ———, *Reconstruction of a proof by its analysis*, ***Doklady Akademii Nauk***, vol. 293 (1987), no. 3, pp. 313–316, (russian).

[15] Pavel Pudlák, *The lengths of proofs*, ***Handbook of proof theory*** (Sam Buss, editor), Elsevier, 1998, pp. 547–637.

[16] Richard Statman, *Lower bounds on Herbrand's theorem*, ***Proceedings of the American Mathematical Society***, vol. 75 (1979), pp. 104–107.

[17] Christian Urban, ***Classical logic and computation***, Ph.D. thesis, University of Cambridge, October 2000.

[18] Christian Urban and Gavin Bierman, *Strong normalization of cut-elimination in classical logic*, ***Fundamenta Informaticae***, vol. 45 (2000), pp. 123–155.

Appendix A. Cut-elimination. Cut-elimination is the following reduction relation $\to^{\mathrm{c}}$ on regular proofs. If the cut formula is introduced by negation inferences on both sides immediately above the cut, then

$$\dfrac{\dfrac{\overset{(\chi_1)}{A, \Gamma \to \Delta}}{\Gamma \to \Delta, \neg A}\,\neg_{\mathrm{r}} \quad \dfrac{\overset{(\chi_2)}{\Pi \to \Lambda, A}}{\neg A, \Pi \to \Lambda}\,\neg_{\mathrm{l}}}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{cut} \qquad \to^{\mathrm{c}} \qquad \dfrac{\overset{(\chi_2)}{\Pi \to \Lambda, A} \quad \overset{(\chi_1)}{A, \Gamma \to \Delta}}{\Gamma, \Pi \to \Delta, \Lambda}\,\mathrm{cut}$$

If the cut formula is introduced by inferences for conjunction on both sides immediately above the cut, then

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{(\chi_2)}{\Pi \to \Lambda, B}}{\Gamma, \Pi \to \Delta, \Lambda, A \wedge B}\ \wedge_{\mathrm{r}} \quad \dfrac{\dfrac{(\chi_3)}{A, \Theta \to \Sigma}}{A \wedge B, \Theta \to \Sigma}\ \wedge_{\mathrm{l}_1}}{\Gamma, \Pi, \Theta \to \Delta, \Lambda, \Sigma}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{(\chi_3)}{A, \Theta \to \Sigma}}{\Gamma, \Theta \to \Delta, \Sigma}\ \mathrm{cut}}{\Gamma, \Pi, \Theta \to \Delta, \Lambda, \Sigma}\ \mathrm{w}^*$$

and symmetrically for $\wedge_{\mathrm{l}_2}$. The other binary connectives, $\vee$ and $\supset$ are treated analogously. If the cut formula is introduced by $\forall_{\mathrm{r}}$ and $\forall_{\mathrm{l}}$ immediately above the cut, then

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A\{x \leftarrow \alpha\}}}{\Gamma \to \Delta, (\forall x)A}\ \forall_{\mathrm{r}} \quad \dfrac{\dfrac{(\chi_2)}{A\{x \leftarrow t\}, \Pi \to \Lambda}}{(\forall x)A, \Pi \to \Lambda}\ \forall_{\mathrm{l}}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{\dfrac{(\chi_1\{\alpha \leftarrow t\})}{\Gamma \to \Delta, A\{x \leftarrow t\}} \quad \dfrac{(\chi_2)}{A\{x \leftarrow t\}, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

The case of the existential quantifier is treated symmetrically. If the cut formula is introduced by an axiom immediately above the cut, then

$$\dfrac{A \to A \quad \dfrac{(\chi)}{A, \Gamma \to \Delta}}{A, \Gamma \to \Delta}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad \dfrac{(\chi)}{A, \Gamma \to \Delta}$$

and symmetrically for the axiom being on the right side above the cut. If the cut formula is introduced by weakening immediately above the cut, then

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta}}{\Gamma \to \Delta, A}\ \mathrm{w}_{\mathrm{r}} \quad \dfrac{(\chi_2)}{A, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut} \qquad \to^{\mathrm{c}} \qquad \dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{w}^*$$

and symmetrically for the weakening on the right side above the cut. If the cut formula is introduced by a contraction immediately above the cut, then

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A, A}}{\Gamma \to \Delta, A}\ \mathrm{c}_{\mathrm{r}} \quad \dfrac{(\chi_2)}{A, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda}\ \mathrm{cut}$$

$$\to^{\mathrm{c}}$$

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A, A} \quad \dfrac{(\chi_2)}{A, \Pi \to \Lambda}}{\Gamma, \Pi \to \Delta, \Lambda, A}\ \text{cut} \qquad \dfrac{(\chi_2')}{A, \Pi \to \Lambda}}{\dfrac{\Gamma, \Pi, \Pi \to \Delta, \Lambda, \Lambda}{\Gamma, \Pi \to \Delta, \Lambda}\ \text{c}^*}\ \text{cut}$$

where χ_2' is defined from χ_2 by renaming all eigenvariables in χ_2 by fresh ones in order to keep the regularity of the proof. The case of c_l is treated symmetrically. Furthermore, for any unary rule r

$$\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{\dfrac{(\chi_2)}{A, \Pi' \to \Lambda'}}{A, \Pi \to \Lambda}\ r}{\Gamma, \Pi \to \Delta, \Lambda}\ \text{cut} \qquad \to^{\text{c}} \qquad \dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{(\chi_2)}{A, \Pi' \to \Lambda'}}{\Gamma, \Pi' \to \Delta, \Lambda'}\ \text{cut}}{\Gamma, \Pi \to \Delta, \Lambda}\ r$$

which is a valid proof as regularity ensures that the eigenvariable condition cannot be violated. For any binary rule r

$$\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{\dfrac{(\chi_2)}{A, \Pi' \to \Lambda'} \quad \dfrac{(\chi_3)}{\Pi'' \to \Lambda''}}{A, \Pi \to \Lambda}\ r}{\Gamma, \Pi \to \Delta, \Lambda}\ \text{cut}$$

$$\to^{\text{c}}$$

$$\dfrac{\dfrac{\dfrac{(\chi_1)}{\Gamma \to \Delta, A} \quad \dfrac{(\chi_2)}{A, \Pi' \to \Lambda'}}{\Gamma, \Pi' \to \Delta, \Lambda'}\ \text{cut} \qquad \dfrac{(\chi_3)}{\Pi'' \to \Lambda''}}{\Gamma, \Pi \to \Delta, \Lambda}\ r$$

Analogous permutation rules apply for r being on the left side of the cut and/or the cut formula being in the other subproof of r.

Appendix B. Index of proofs. This appendix contains an index of formal proofs that we refer to outside of a local context and the page numbers of their respective definitions.

INSTITUTE OF DISCRETE MATHEMATICS AND GEOMETRY (E104)
VIENNA UNIVERSITY OF TECHNOLOGY
WIEDNER HAUPTSTRAßE 8-10, 1040 VIENNA, AUSTRIA
E-mail: baaz@logic.at

LABORATOIRE PREUVES, PROGRAMMES ET SYSTÈMES (PPS)
UNIVERSITÉ PARIS DIDEROT – PARIS 7
175 RUE DU CHEVALERET, 75013 PARIS, FRANCE
E-mail: stefan.hetzl@pps.jussieu.fr