BACHELORARBEIT

Die Unentscheidbarkeit der k-Beweisbarkeit

ausgeführt am

Institut für
Diskrete Mathematik und Geometrie
TU Wien

unter der Anleitung von

Stefan Hetzl

durch

Martin Gius
Matrikelnummer: 01611151
Spengergasse 11
1050 Wien

Wien, 20. Mai 2019

Inhaltsverzeichnis

1 Einleitung

Diese Bachelor-Arbeit ist eine detaillierte Ausführung des wissenschaftlichen Artikels 'The undecidability of k-provability' von Samuel R. Buss, der 1991 in der 53. Ausgabe der Zeitschrift Annals of Pure and Applied Logic erschien (vgl. [1]). Dabei geht es in erster Linie darum, Hilfsmittel einzuführen, die ermöglichen werden, zu beweisen, dass das Problem für gegebene Formel ϕ und Zahl k festzustellen, ob ein Beweis von ϕ in Gentzens Sequentialkalkül mit höchstens k Sequenten existiert, unentscheidbar ist. Oder genauer:

Hauptsatz (*Buss*) Sei LK Gentzens Sequentialkalkül mit einstelligem Funktionssybmol S und abzählbar vielen zweistelligen Relationssymbolen. Dann gibt es für jede semi-entscheidbare Menge X eine Formel $A(x)$ und ein $k \in \mathbb{N}$, sodass für alle $n \in \mathbb{N}$, $n \in X$ genau dann wenn $\rightarrow A(S^n 0)$ einen LK-Beweis mit weniger als k verschiedenen Sequenten hat.

In Abschnitt 2 werden wir dafür die Unentscheidbarkeit eines weiteren Problems, nämlich einer speziellen Version der Unifikation zweiter Stufe, mit Hilfe des Satzes von Matijacevič [5], zeigen. Die Motivation dafür ist, dass wir dann in Abschnitt 4 dieses Problem auf das eigentliche Problem der k-Beweisbarkeit reduzieren können, woraus die Unentscheidbarkeit folgt. Bei dieser Reduktion wird ein wesentliches Hilfsmittel der in Abschnitt 3 eingeführte logische Fluss-Graph eines Beweises sein, mit welchem man eine untere Schranke für die Anzahl der in einem Beweis benötigten Sequente angeben kann.

2 Unifikation zweiter Stufe mit partieller Substitution ist unentscheidbar

Im folgenden Abschnitt werden wir definieren, was ein Unifikationsproblem zweiter Stufe mit partieller Substitution ist, und sehen, dass dieses Problem unentscheidbar ist. In unserer Sprache befinden sich ein unäres Funktionssymbol S, ein zweistelliges Funktionssymbol $\circ$ und $a, b, c, \ldots$ Variablen der Prädikatenlogik erster Stufe, $\alpha, \beta, \gamma, \ldots$ Variablen zweiter Stufe, die über Terme der Prädikatenlogik erster Stufe reichen. Wir verwenden außerdem Metavariablen $r, s, t, \ldots$ für Terme erster Stufe und $\rho, \sigma, \tau, \ldots$ für Terme zweiter Stufe.

Definition 2.1. Es seien ρ und σ Metavariablen für Terme zweiter Stufe, t ein Term erster Stufe und a eine Variable erster Stufe. Dann ist die *Substitution zweiter Stufe von a durch ρ in t* definiert als die Menge aller Terme erster Stufe, die entstehen, wenn man an beliebigen Stellen in t an denen die Variable a steht, ρ für die Variable a substituiert oder nichts ändert. Wir schreiben $t(\rho//a)$ für diese Menge. Wir definieren außerdem, was es heißt, dass eine Unifikationsgleichung erfüllt ist:

$$t(\rho//a) = \sigma :\Leftrightarrow \exists \tau \in t(\rho//a) : \tau = \sigma.$$

Ist außerdem β eine Variable zweiter Stufe, die einen Term erster Stufe t repräsentiert, so schreiben wir auch $\beta(\rho//a)$ für die Menge $t(\rho//a)$.

Beispiel 2.2. Wir betrachten die Gleichung

$$\beta(Sa//a) = S\beta. \tag{2.1}$$

Man sieht leicht, dass Lösungen gegeben sind durch $\beta = S^k a$ für $k \geq 0$. Dies sind sogar die einzigen Lösungen der Gleichung. Um dies zu zeigen, gehen wir über den Termaufbau von einer Lösung β vor. Ist β eine Variable, so muss $\beta = a = S^0 a$ gelten. Sei β nun ein Term. Dann kann β nicht von der Form $t_1 \circ t_2$ sein, denn dann wäre die Gleichung offenbar nicht erfüllt. Also gilt $\beta = St$ und nach Induktionshypothese $t = S^k$. Wir erhalten also $\beta = S^{k+1}$.

Definition 2.3. Ein *Unifikationsproblem zweiter Stufe mit partieller Substitution* ist ein Gleichungssystem der folgenden Form:

$$\beta_{i_j}(\rho_j//a_{i_j}) = \sigma_j \qquad j = 1, \ldots, m; \quad i_j \in \{1, \ldots, k\};$$

Eine Lösung dieses Gleichungssystems ist eine Zuweisung von Termen erster Stufe zu den Variablen zweiter Stufe $\beta_1, \ldots, \beta_k$, sodass alle Gleichungen im Sinne von Definition 2.1 erfüllt sind.

Satz 2.4. *Das Unifikationsproblem zweiter Stufe mit partieller Substitution ist unentscheidbar.*

Beweis. Unsere Strategie wird es sein, die Lösbarkeit von diophantischen Gleichungen, das sind Polynomgleichungen mit ganzzahligen Koeffizienten, auf ein Unifikationsproblem zweiter Stufe mit partieller Substitution zurückzuführen. Ersteres Problem ist nämlich nach dem Satz von Matijacevič [5] unentscheidbar, womit auch unser Unfikationsproblem unentscheidbar sein muss. Um diese Reduktion durchzuführen, müssen wir Gleichungssysteme angeben, die uns eine Möglichkeit bieten, ganze Zahlen zu repräsentieren und die Korrektheit von Addition und Multiplikation zu garantieren. In Beispiel 2.2 haben wir bereits gesehen, wie man nicht negative Zahlen mittels Gleichung 2.1 darstellen kann. Um die Addition auszudrücken, benötigen wir Gleichungen, deren einzige Lösungen gegeben sind durch $\beta_1 = S^{k_1}a, \beta_2 = S^{k_2}a$ und $\beta_3 = S^{k_1+k_2}a$ für beliebige natürliche Zahlen k_1, k_2. Wir betrachten das folgende Gleichungssystem:

(1) $\beta_j(Sa||a) = S\beta_j, \qquad j = 1, 2, 3,$

(2) $\beta_1(\beta_2||a) = \beta_3,$

(3) $\beta_1(S\beta_2||a) = S\beta_3.$

Mittels Gleichung (1) erhalten wir wieder wie in Beispiel 2.2, dass $\beta_j = S^{k_j}a, j = 1, 2, 3$. Betrachten wir Gleichung (2), gibt es zwei Fälle: falls a in β_1 durch β_2 ersetzt wird, so gilt $k_1 + k_2 = k_3$. Wird die Substitution nicht durchgeführt, so gilt $k_1 = k_3$. Analog erhalten wir mittels Gleichung (3), dass $k_1 + k_2 = k_3$ oder $k_1 = k_3 + 1$. Also gilt insgesamt $k_1 + k_2 = k_3$. Die Korrektheit der Multiplikation zu erzwingen, ist etwas schwieriger. Wir werden uns überlegen, dass folgende Gleichungen das Gewünschte erfüllen.

(4) $\beta_j(Sa||a) = S\beta_j, \qquad j = 1, 2, 3,$

(5) $\beta_4(Sb||b) = S\beta_4,$

(6) $\beta'_j(Sa'||a') = S\beta'_j, \qquad j = 1, 2, 3,$

(7) $\beta'_4(Sb'||b') = S\beta'_4,$

(8) $\beta_j(a'||a) = \beta'_j, \qquad j = 1, 2, 3,$

(9) $\beta_4(b'||b) = \beta'_4,$

(10) $\beta_2(b||a) = \beta_4,$

(11) $\alpha(\beta_1//a, Sb//b, \beta'_1//a', Sb'//b', a \circ b \circ a' \circ b' \circ c//c) = \beta_3 \circ \beta_4 \circ \beta'_3 \circ \beta'_4 \circ \alpha,$

(12) $\alpha(\beta'_1//a, Sb'//b, a//a', b//b', a' \circ b' \circ c//c) = \beta'_3 \circ \beta'_4 \circ \alpha.$

Dabei sind die Substitutionen in den Gleichungen (11) und (12) als simultane Substitution zu verstehen. Darauf werden wir am Ende des Beweises nochmals zurückkommen. Abermals wie in Beispiel 2.2 erhalten wir, dass jede Lösung der Gleichungen (4) - (10)

$$\begin{aligned} &\beta_j = S^{k_j}a, \quad \beta'_j = S^{k_j}a' \qquad j = 1,2,3,\\ &\beta_4 = S^{k_2}b, \quad \beta'_4 = S^{k_2}b' \end{aligned}$$

erfüllen muss. Wir zeigen nun, dass (bis auf einen Trivialfall) die einzige Lösung der letzten beiden Gleichungen gegeben ist durch

$$\begin{aligned} \alpha := \; & S^{(k_2-1)k_1}a \circ S^{k_2-1}b \circ S^{(k_2-1)k_1}a' \circ S^{k_2-1}b' \circ \; \ldots \; \circ \\ & S^{2k_1}a \circ S^2 b \circ S^{2k_1}a' \circ S^2 b' \circ S^{k_1}a \circ Sb \circ S^{k_1}a' \circ Sb' \circ a \circ b \circ a' \circ b' \circ c, \end{aligned}$$

mit $k_1 \cdot k_2 = k_3$. Um zu sehen, dass α wirklich eine Lösung ist, reicht das Einsetzen in die Gleichungen, Durchführen aller Substitutionen wobei am Ende zu beachten ist, dass $k_1 \cdot k_2 = k_3$. Es bleibt zu zeigen, dass keine andere Lösung existiert. Sei also α^* eine weitere Lösung. Es könnte sein, dass $\alpha^* = c$. Damit die Gleichungen erfüllt sind, muss $k_3 = k_2 = 0$ gelten, dann ist α^* zwar nicht von obiger Form, aber $k_1 \cdot k_2 = k_3$ ist erfüllt, was eigentlich das ist, worauf es uns ankommt. Sei nun $\alpha^* \neq c$. Wir beobachten, dass α^* eine eindeutige Darstellung als $\rho_1 \circ \rho_2 \circ \cdots \circ \rho_t$ hat. Betrachten wir zusätzlich die Form der Substitutionen in Gleichung (11), so kommen wir zum Schluss, dass α^* von der Form

$$S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2$$

sein muss. Weiters ist $m_1 = k_3$, falls man die Substitution nicht durchführt oder $m_1 = k_3 - k_1$. Mit der selben Argumentation muss $n_1 = k_2$ oder $n_1 = k_2 - 1$. Analog für m'_1 und n'_1. Außerdem muss α_2 die Gleichung

$$\alpha_2(\beta_1//a, Sb//b, \beta'_1//a', Sb'//b', a \circ b \circ a' \circ b' \circ c//c) = S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a \circ S^{n'_1}b \circ \alpha_2$$

erfüllen. Nun folgt mittels Induktion über den Termaufbau von α^*, dass α^* die Form

$$S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a \circ S^{n'_1}b \circ \; \ldots \; \circ S^{m_t}a \circ S^{n_t}b \circ S^{m'_t}a \circ S^{n'_t}b$$

hat, wobei ähnlich wie zuvor für $i = 1, \ldots, t$

$$\begin{aligned} m_{i+1} &= m_i \quad \text{oder} \quad m_{i+1} = m_i - k_1,\\ m'_{i+1} &= m'_i \quad \text{oder} \quad m'_{i+1} = m'_i - k_1,\\ n_{i+1} &= n_i \quad \text{oder} \quad n_{i+1} = n_i - 1,\\ n'_{i+1} &= n'_i \quad \text{oder} \quad n'_{i+1} = n'_i - 1. \end{aligned}$$

Außerdem gilt $m_t = n_t = m'_t = n'_t$. Nun muss α^* Gleichung (12) auch erfüllen. Die rechte Seite der Gleichung ist von der Form

$$S^{k_3}a' \circ S^{k_2}b' \circ S^{m_1}a \circ S^{n_1}b \circ S^{m'_1}a' \circ S^{n'_1}b' \circ \alpha_2.$$

Daher muss, sodass α^* die Gleichung erfüllt, jeweils das erste a, b, a' bzw. b' durch $S^{k_1}a', Sb', a$ bzw. b substituiert werden (es gibt nämlich keine anderen Möglichkeiten, um aus einem Term mit a bzw. b am Ende einen Term mit a' bzw. b' am Ende zu gewinnen, oder umgekehrt). Wir erhalten somit

$$k_3 = m_1 + k_1,\ k_2 = n_1 + 1,\ m_1 = m'_1 \ \text{ und } \ n_1 = n'_1.$$

Außerdem erfüllt α_2 die Gleichung

$$\alpha_2(\beta'_1//a, Sb'//b, a//a', b//b', a' \circ b' \circ c//c) = S^{m'_1} \circ S^{n'_1} \circ \alpha_2.$$

Auch für α_2 können wir wie oben vorgehen und schließen

$$m'_1 = m_2 + k_1,\ n'_1 = n_2 + 1,\ m_2 = m'_2 \ \text{ und } \ n_2 = n'_2.$$

Dieses Vorgehen können wir nun wiederholen und erhalten mittels Induktion:

$$m_i = m'_i = m_{i+1} + k_1,\ n_2 = n'_i = n_{i+1} + 1 \qquad i = 1, \ldots, t-1.$$

Es folgt nun unmittelbar, dass

$$k_3 = m_i + ik_1 \ \text{ und } \ k_2 = n_i + 1 \qquad i = 1, \ldots, t.$$

Setzen wir nun $i = t$ so gilt $k_3 = m_t + tk_1 = tk_1$ und $k_2 = n_t + t = t$, also insgesamt $k_3 = k_1 \cdot k_2$. Wir haben also gezeigt, dass Gleichungen (4) - (12) Multiplikation korrekt ausdrücken. Wie bereits erwähnt, müssen wir uns aber noch einige Gedanken zur simultanen Substitution in den letzten beiden Gleichungen machen, die wir in Definition 2.1 nicht zugelassen haben. Wir können Gleichung (11) durch fünf Gleichungen ersetzen:

$$\begin{aligned} \alpha(\beta_1//a) &= \gamma_1 & \qquad \gamma_3(Sb'//b') &= \gamma_4 \\ \gamma_1(Sb//b) &= \gamma_2 & \qquad \gamma_4(a \circ b \circ a' \circ b' \circ c//c) &= \beta_3 \circ \beta_4 \circ \beta'_3 \circ \beta'_4 \circ \alpha \\ \gamma_2(\beta'_1//a') &= \gamma_3 \end{aligned}$$

Dies ist äquivalent, da in den Termen, mit denen substituiert wird, nur jene Variablen vorkommen, die substituiert werden. Bei Gleichung (12) ist dies nicht der Fall, es gibt trotzdem einen Ausweg mit den folgenden äquivalenten Gleichungen:

$$\alpha(a''//a', b''//b'), \qquad \alpha'(\beta'_1//a, Sb'//b, a//a'', b//b'', a' \circ b' \circ c//c) = \beta'_3 \circ \beta'_4 \circ \alpha.$$

Diese können nun wie zuvor mit sieben weiteren Gleichungen ausgedrückt werden.
Wir sehen also insgesamt, dass es eine effektive Methode gibt, diophantische Gleichungen mittels einem Unifikationsproblem mit partieller Substitution zu formulieren. Wie am Anfang erwähnt, folgt der Satz nun aus dem Satz von Matijacevič, siehe [5]. ■

Bemerkung 2.5. Aus dem Beweis geht sogar eine stärkere Version von Satz 2.4 vor: Für jede semi-entscheidbare Menge X gibt es eine Menge von partiellen Unifikationsgleichungen Ω, sodass für alle n, $n \in X$ genau dann wenn $\Omega \cup \{\beta_1 = S^n 0\}$ eine Lösung hat.

Um den Beweis des Hauptsatzes zu erleichtern, formulieren wir noch eine verstärkte Version von Satz 2.4. Wir können uns nämlich auf partielle Substitutionsgleichungen der Form $\beta(s//a) = \sigma$ beschränken, die die *spezielle Restriktion* erfüllen: s ist keine Variable zweiter Stufe und auch nicht die Variable a. Es ist nicht offensichtlich, dass der Satz in dieser Formulierung folgt, denn Gleichungen (2), (11) und (12) erfüllen die spezielle Restriktion nicht. Wir können allerdings (2) durch die Gleichung $\beta_1(SS\beta_2//a) = SS\beta_3$ ersetzen und die Addition wird noch immer korrekt definiert. In (12) und (13) ersetzen wir β_1 bzw. β_1' durch $S\beta_1$ und $S\beta_1'$. Dies definiert die Eigenschaft $(k_1 + 1)k_2 = k_3$. Die Multiplikation kann somit über $xy = z \leftrightarrow (x + 1)y = z + y$ definiert werden. Es folgt:

Satz 2.6. *Für jede semi-entscheidbare Menge X gibt es eine Menge Ω von partiellen Unifikationsgleichungen, die die spezielle Restriktion erfüllen, sodass für alle n, $n \in X$ genau dann wenn $\Omega \cup \{\beta_1 = S^n 0\}$ eine Lösung hat.*

3 Der logische Fluss-Graph im Sequentialkalkül

1 Definitionen und Bezeichnungen

Zu Beginn dieses Abschnitts werden wir eine kurze Einführung in Gentzens Sequentialkalkül geben und dann darauf aufbauende Begriffe definieren, die es uns erleichtern werden, den Hauptsatz zu beweisen. Unsere Sprache besteht aus Konstanten-, Relations- und Funktionssymbolen sowie logischen Symbolen und Variablen. Dabei unterscheiden wir zwischen freien Variablen $(a, b, c, \dots)$ und gebundenen Variablen $(x, y, z, \dots)$. Die logischen Symbole sind $\wedge, \vee, \neg, \supset, \exists$ und $\forall$. *Terme* werden mit freien Variablen, Konstantensymbolen und Funktionssymbolen gebildet. *Semiterme* dürfen auch gebundene Variablen enthalten. *Atomformeln* entstehen aus Termen und Relationssymbolen und *Formeln* aus Atomformeln und logischen Symbolen, wobei nur gebundene Variablen quantifiziert werden dürfen und nur freie Variablen frei vorkommen dürfen. *Semiformeln* sind Formeln in denen auch gebundene Variablen frei vorkommen können. Für genauere Definitionen verweise ich auf [2]. Ein *Sequent* ist von der Form

$$A_1, \dots, A_n \to B_1, \dots B_m,$$

wobei $A_1, \ldots, A_n, B_1, \ldots, B_m$ Formeln sind und $n, m \in \mathbb{N}$. Die beabsichtigte Bedeutung eines Sequents ist dabei $(A_1 \wedge \cdots \wedge A_n) \supset (B_1 \vee \cdots \vee B_m)$. Wir bezeichnen die Liste der Formeln links vom Pfeil als *Antecedent* und rechts als *Succedent*. Unsere Konvention wird es sein, Listen von Formeln im Antecedent mit Γ und Π und Listen von Formeln im Succedent mit Δ und Λ zu bezeichnen. *Axiome* sind Sequente der Form $A \to A$ und *Gleichheitsaxiome* sind Sequente der Form

$$\to t_1 = t_1, \quad t_1 = t_2 \to t_2 = t_1,$$

$$s_1 = t_1, \ldots, s_k = t_k, P(s_1, \ldots, s_k) \to P(t_1, \ldots, t_k),$$
$$s_1 = t_1, \ldots, s_k = t_k, f(s_1, \ldots, s_k) \to f(t_1, \ldots, t_k).$$

Dabei ist A eine Formel, $t_1, s_1, \ldots, t_k, s_k$ Terme, P ein k-stelliges Prädikatensymbol und f ein k-stelliges Funktionssymbol. Die folgenden Relationen zwischen Sequenten nennen wir *logische Inferenzen*:

$$\neg : \ell \, \frac{\Gamma \to \Delta, A}{\neg A, \Gamma \to \Delta}, \quad \neg : r \, \frac{A, \Gamma \to \Delta}{\Gamma \to \Delta, \neg A},$$

$$\wedge : r \, \frac{\Gamma \to \Delta, A \qquad \Gamma \to \Delta, B}{\Gamma \to \Delta, A \wedge B}, \quad \wedge : \ell \, \frac{A, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta} \quad \frac{B, \Gamma \to \Delta}{A \wedge B, \Gamma \to \Delta},$$

$$\vee : \ell \, \frac{A, \Gamma \to \Delta \qquad B, \Gamma \to \Delta}{A \vee B, \Gamma \to \Delta}, \quad \vee : r \, \frac{\Gamma \to \Delta, A}{\Gamma \to \Delta, A \vee B} \quad \frac{\Gamma \to \Delta, B}{\Gamma \to \Delta, A \vee B},$$

$$\supset : \ell \, \frac{\Gamma \to \Delta, A \qquad B, \Gamma \to \Delta}{A \supset B, \Gamma \to \Delta}, \quad \supset : r \, \frac{A, \Gamma \to \Delta, B}{\Gamma \to \Delta, A \supset B},$$

$$\exists : \ell \, \frac{A(b), \Gamma \to \Delta}{(\exists x) A(x), \Gamma \to \Delta}, \quad \exists : r \, \frac{\Gamma \to \Delta, A(t)}{\Gamma \to \Delta, (\exists x) A(x)},$$

$$\forall : \ell \, \frac{A(t), \Gamma \to \Delta}{(\forall x) A(x), \Gamma \to \Delta}, \quad \forall : r \, \frac{\Gamma \to \Delta, A(b)}{\Gamma \to \Delta, (\forall x) A(x)}.$$

Bei den Quantorenregeln $\exists : \ell$ und $\forall : r$ ist zu beachten, dass die freie Variable b nicht im unteren Sequent vorkommt. Als nächstes definieren wir die *strukturellen Inferenzen*:

$$\text{Schnitt} \, \frac{\Gamma \to \Delta, A \qquad A, \Pi \to \Lambda}{\Gamma, \Pi \to \Delta, \Lambda},$$

$$\text{Abschwächung } \frac{\Gamma \to \Delta}{A, \Gamma \to \Delta} \quad \frac{\Gamma \to \Delta}{\Gamma \to \Delta, A},$$

$$\text{Vertauschung } \frac{\Gamma, A, B, \Pi \to \Delta}{\Gamma, B, A, \Pi \to \Delta} \quad \frac{\Gamma \to \Delta, A, B, \Lambda}{\Gamma \to \Delta, B, A, \Lambda},$$

$$\text{Kontraktion } \frac{A, A, \Gamma \to \Delta}{A, \Gamma \to \Delta} \quad \frac{\Gamma \to \Delta, A, A}{\Gamma \to \Delta, A}.$$

Nun noch einige Bezeichnungen: die *Hauptformel* einer Inferenz ist jene Formel im unteren Sequent, auf die die Inferenz gewirkt hat. Die *Hilfsformeln* einer Inferenz sind die Formeln im oberen Sequent, die von der Inferenz verwendet werden. Die *Nebenformeln* einer Inferenz sind jene Formeln, die in den Listen $\Gamma, \Pi, \Delta, \Lambda$ stehen. Jetzt können wir definieren, was ein Beweis ist:

Definition 3.1. Ein *Beweis* eines Sequents S_n ist eine Liste von Sequenten $S_1, \ldots, S_n$, sodass jedes Sequent S_i ein Axiom, Gleichheitsaxiom oder unteres Sequent einer Inferenz mit oberem Sequent S_j und $j < i$ ist. Die *Länge* eines Beweises P ist die Anzahl der Sequente, symbolisch $|P|$. Außerdem nennen wir einen Beweis *baum-ähnlich*, falls jedes Vorkommnis eines Sequents (außer dem Endsequent) genau einmal als oberes Sequent einer Inferenz verwendet wird. Ist A eine Formel, so ist ein Beweis von A ein Beweis des Sequents $\to A$.

Das gerade definierte Beweissystem bezeichnen wir mit LK_e. Lässt man in der Sprache das Gleichheitssymbol weg und in den Beweisen die Gleichheitsaxiome, so erhält man das System LK. Außerdem bezeichnen wir mit den Symbolen $\top$ und $\bot$ Formeln, sodass $\to \top$ und $\bot \to$ gültige Sequente sind. Dabei sind die Symbole $\top$ und $\bot$ keine Symbole unserer Sprache.

Definition 3.2. Sei P ein Beweis und A eine Subformel einer Formel in P. Dann bezeichnen wir ein Vorkommnis von A in P als eine *s-Formel*.

Definition 3.3. Sei P ein Beweis. Der *logische Fluss-Graph von* P, notiert als G_P, ist definiert über seine Knoten- und Kantenmengen: Die Knotenmenge ist die Menge aller s-Formeln in P und die Kanten sind nach folgenden Regeln definiert:

1. In einem Axiom $A \to A$ gibt es eine Kante von der linken s-Formel A zur rechten s-Formel A. In einem Gleichheitsaxiom

$$s_1 = t_s, \ldots, s_k = t_k, R(s_1, \ldots, s_k) \to R(t_1, \ldots, t_k),$$

$$s_1 = t_s, \ldots, s_k = t_k, f(s_1, \ldots, s_k) \to f(t_1, \ldots, t_k),$$

definieren wir eine Kante von $R(\mathbf{s})$ nach $R(\mathbf{t})$ bzw. von $f(\mathbf{s})$ nach $f(\mathbf{t})$,

2.a) Ist A eine Nebenformel im Antecedent eines oberen Sequents, so gibt es eine Kante von der A entsprechenden s-Formel im unteren Sequent zu A,

2.b) Ist A eine Nebenformel im Succedent eines oberen Sequents, so gibt es eine Kante von A zur A entsprechenden s-Formel im unteren Sequent,

3.a) Ist A eine Hilfsformel im Antecedent eines oberen Sequents, so gibt es eine Kante von der A entsprechenden s-Formel in der Hauptformel des unteren Sequents zu A,

3.b) Ist A eine Hilfsformel im Succedent eines oberen Sequents, so gibt es eine Kante von A zur A entsprechenden s-Formel in der Hauptformel des unteren Sequents,

4. Bei einem Schnitt gibt es eine Kante von der Hilfsformel im Succedent des linken Sequents zur Hilfsformel im Antecedent des rechten Sequents,

5. Falls es eine Kante von einer s-Formel A_1 zu einer s-Formel A_2 gibt und B_1 eine Subformel von A_1 ist, so gibt es eine Kante von B_1 zur B_1 entsprechenden Subformel B_2 von A_2, falls B_1 positiv in A_1 vorkommt. Sonst gibt es eine Kante von B_2 nach B_1.

Definition 3.4. Sind A und B s-Formeln in einem Beweis P, so ist A eine *Variante* von B, falls man B aus A durch Änderung von (semi-)Termen in A erhalten kann.

Definition 3.5. Sei A eine s-Formel in einem Beweis P. A kommt *positiv* in P vor, genau dann wenn A positiv als Unterformel einer Formel im Succedent oder negativ als Unterformel einer Formel im Antecedent eines Sequents in P vorkommt. Andernfalls kommt A *negativ* in P vor.

Bemerkung 3.6. Sind A und B s-Formeln in einem Beweis P und ist in G_P eine Kante von A nach B oder B nach A, so sind A und B offenbar Varianten von einander.

Definition 3.7. Sei P ein Beweis. Ein *vorwärts-Pfad* von einer s-Formel A zu einer s-Formel B ist ein nicht-trivialer Pfad im logischen Fluss-Graphen G_P von A nach B. Ein *rückwärts-Pfad* von einer s-Formel A zu einer s-Formel B ist ein nicht-trivialer Pfad im logischen Fluss-Graphen G_P von B nach A. Wir nennen eine s-Formel B *vorwärts-erreichbar* von einer s-Formel A, falls ein vorwärts-Pfad von A nach B existiert oder $A = B$.

Beispiel 3.8. In der folgenden Abbildung steht links ein gewöhnlicher Beweis im Sequentialkalkül und rechts ist der logische Fluss-Graph für die Formeln A und B eingezeichnet (aus Gründen der Übersichtlichkeit wurden Kanten für andere s-Formeln nicht eingezeichnet).

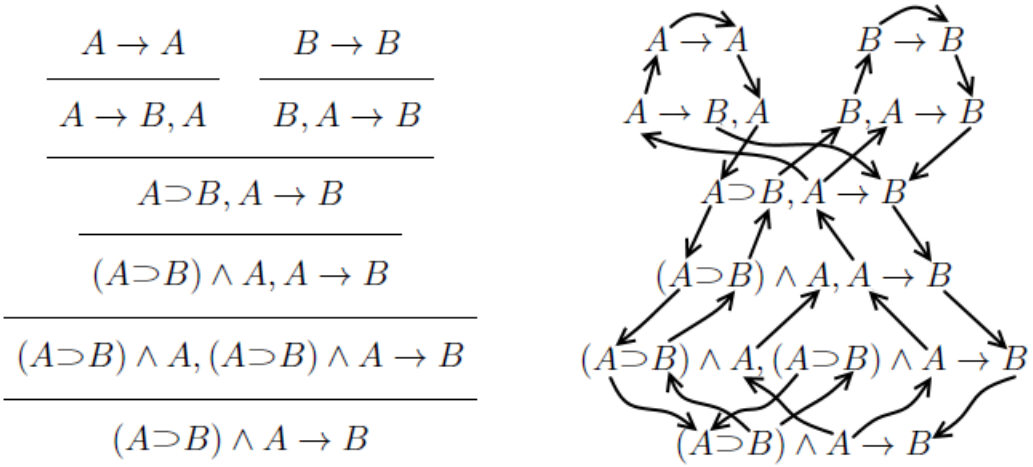

Abbildung 3.1: Ein Beweis und sein logischer Fluss-Graph

2 Hilfreiche Ergebnisse über den logischen Fluss-Graphen

Der logische Fluss-Graph eines Beweises ist ein Hilfsmittel, um die logischen Auswirkungen einer Formel im Beweis zu verfolgen. Zuerst werden wir ein paar Ergebnisse sehen, um die Struktur des logischen Fluss-Graphen besser verstehen zu können. Darauf werden wir sehen, dass man unter gewissen Voraussetzungen mit Hilfe des logischen Fluss-Graphen eine untere Schranke an die Anzahl der Sequente in einem Beweis geben kann. Dies wird später wesentlich in dem Beweis des Hauptsatzes eingehen. Für allgemeine Ergebnisse über das Sequentialkalkül verweise ich auf [3].

Proposition 3.9. *Sei P ein Beweis von $\Gamma \to \Delta$. Dann existiert ein baum-ähnlicher Beweis P' von $\Gamma \to \Delta$ und jeder Pfad in $G_{P'}$ lässt sich mit einem Pfad in G_P identifizieren.*

Beweis. Wir gehen induktiv über die Anzahl der Sequente in P, die mehrfach verwendet werden, vor. Im Induktionsanfang gibt es keine solchen Sequente, also ist P selbst baum-ähnlich. Im Induktionsschritt sei S das erste Sequent in P, das mehrfach verwendet wird. Dann gibt es einen Unterbeweis P_S von S in P. Wir transformieren P nun zu einem Beweis P^*, indem wir vor jeder Stelle, an der S in P in einer Inferenz gebraucht wird, den Beweis P_S schreiben. Außerdem können wir die neu entstandenen Pfade in G_{P^*} alle mit den Pfaden in G_{P_S} identifizieren. Damit existiert nun nach Induktionshypothese ein baum-ähnlicher Beweis P' von $\Gamma \to \Delta$ und alle Pfade in $G_{P'}$ lassen sich mit einem Pfad in G_P identifizieren. ■

Proposition 3.10. *Sei P ein Beweis. Dann gilt für jede Kante $E = (A, B)$ in G_P:*

a) falls E nach unten gerichtet ist, so sind A und B positive s-Formeln,

b) falls E nach oben gerichtet ist, so sind A und B negative s-Formeln,

c) falls E lateral ist, so ist A eine positive und B eine negative s-Formel oder umgekehrt.

Beweis. Sei $E = (A, B)$ eine Kante in G_P. Wir unterscheiden vier Fälle:

1.Fall: E ist durch Regel 2a) oder 2b) in Definition 3.3 entstanden. Ist E nach unten gerichtet, so sind A und B Formeln im Succedent eines Sequents und somit positiv. Ist E nach oben gerichtet, so sind A und B Formeln im Antecedent eines Sequents und somit negativ.

2.Fall: E ist durch Regel 3a) oder 3b) in Definition 3.3 entstanden. Ist E nach unten gerichtet, so ist A Formel im Succedent eines Sequents und somit positiv. Bei allen Inferenzen, bis auf die Negationen, bleibt die Formel B auch im Succedent und ist somit positiv, bei $\neg : r$ wechselt die Formel B ins Antecedent, wird aber negativ und somit insgesamt positiv. Falls E nach oben gerichtet ist, verläuft die Argumentation ähnlich.

3.Fall: E ist durch Regel 4) oder 5) in Definition 3.3 entstanden und es existiert eine Kante $E' = (A', B')$, wobei A' und B' die Oberformeln von A bzw. B bezeichnen. Ist also E nach unten gerichtet, so auch E'. Damit kommen A und B positiv in A' bzw. B' vor. Betrachtet man außerdem die Regeln, nach denen wir Kanten im logischen Fluss-Graphen bilden, so muss A' im Succedent eines Sequents stehen, damit eine nach unten gerichtete Kante entsteht. B' steht entweder im Succedent eines Sequents oder es steht $\neg B'$ im Antecedent eines Sequents. In jedem Fall sind sowohl A als auch B positiv in P. Ist E nach oben gerichtet, so auch E'. Mit ähnlicher Argumentation wie oben sieht man, dass A' und B' im Antecedent zweier Seqeuente liegen oder A' im Antecedent und $\neg B'$ im Succedent zweier Sequente. In jedem Fall erhält man, dass sowohl A als auch B negativ in P vorkommen.
Der Fall, in dem E lateral ist, kann nur bei Axiomen oder bei der Schnittregel eintreten. In beiden Fällen ist eine der s-Formeln im Succedent eines Sequents und eine im Antecedent eines Sequents. Da A und B Varianten sind, haben sie die gleiche Polarität in der Formel A' bzw. B' und damit verschiedene Polarität im Beweis P.

4.Fall: E ist durch Regel 4) oder 5) in Definition 3.3 entstanden und es existiert eine Kante $E' = (B', A')$, wobei A' und B' die Oberformeln von A bzw. B bezeichnen. Man kann wieder nach ähnlichem Schema wie in Fall 3. vorgehen, nur dass A und B nun negativ in A' bzw. B' vorkommen. ■

Proposition 3.11. *Sei P ein Beweis und A eine s-Formel in P.*

a) Falls A positiv in P auftritt, so ist jede Eingangskante von A in G_P entweder nach unten gerichtet oder lateral, dabei haben alle diese Kanten dieselbe Richtung. Falls sie nach unten gerichtet sind, so gibt es 0, 1 oder 2 Kanten. Außerdem gilt, falls P baum-ähnlich ist, dass der Ausgangsgrad von A gleich eins ist (oder null, falls A in einem Endsequent oder einem Sequent ist, das nicht im Beweis verwendet wird).

b) Falls A negativ in P auftritt, dann gibt es entweder eine laterale oder höchstens zwei nach oben gerichtete, von A ausgehende Kanten in G_P. Falls P baum-ähnlich ist, ist der Eingangsgrad von A gleich eins (oder null, falls A in einem Endsequent oder einem Sequent ist, das nicht im Beweis verwendet wird).

Beweis. ad a): Würde eine nach oben gerichtete Kante auf A zeigen, wäre dies ein Widerspruch zu Proposition 3.10. Sei nun E eine laterale Eingangskante von A und A' die Oberformel von A. Da A positiv in P vorkommt, kommt A entweder positiv in A' im Succedent oder negativ in A' im Antecedent eines Sequents vor. In beiden Fällen kann E nicht durch eine Schnittregel entstanden sein, da dort die Kante von A ausgehen müsste. Also steht A in einem Axiom. Daher kann es keine nach unten gerichteten Eingangskanten von A geben, da Axiome die "obersten" Sequente in Beweisen sind. Die Aussage über die Anzahl der nach unten gerichteten Eingangskanten ist klar, wenn man den logischen Fluss in allen Inferenzen betrachtet, beispielsweise gibt es keine nach unten gerichteten Eingangskanten genau dann, wenn A eine Unterformel einer Formel ist, die durch eine Abschwächung entstanden ist. Falls P baum-ähnlich ist und A nicht im Endsequent oder einem Sequent, das nicht im Beweis verwendet wird, vorkommt, erhält man mit ähnlichem Argument, dass der Ausgangsgrad von A eins sein muss. (In einem nicht baum-ähnlichen Beweis kann es passieren, dass ein Sequent bei mehreren Inferenzen verwendet wird, was den Ausgangsgrad erhöhen würde). ad b): Ähnlich zum Beweis von a). ■

Lemma 3.12. *Sind C^* und C' Formeln, so gilt:*

(a) Falls man C^* durch Ersetzen von positiv vorkommenden Unterformeln durch $\top$ aus C' erhalten kann, so ist das Sequent $C' \to C^*$ gültig.

(b) Falls man C^* durch Ersetzen von negativ vorkommenden Unterformeln durch $\top$ aus C' erhalten kann, so ist das Sequent $C^* \to C'$ gültig.

Beweis. Wir gehen mittels Induktion über den Formelaufbau vor. Sind C^* und C' Atomformeln, so gilt im Fall (a) entweder $C^* = C'$ oder $C^* = \top$. In jedem Fall ist das Sequent $C' \to C^*$ gültig. Der Fall (b) kann nicht eintreten, da Atomformeln keine negativ vorkommenden Unterformeln haben.
Gilt nun (a) und $C^* = \neg C_1^*$ bzw. $C' = \neg C_1'$, so kann man C_1^* aus C_1' durch Ändern von

negativ vorkommenden Unterformeln erhalten. Mit der Induktionshypothese angewendet auf (b) ist also das Sequent $C_1^* \to C_1'$ gültig. Damit können wir aus diesem Sequent mit zwei Negationen das Sequent $\neg C_1' \to \neg C_1^*$ beweisen. Symmetrisch geht man für (b) vor.
Gilt (a) und sind $C^* = C_1^* \supset C_2^*$ und $C' = C_1' \supset C_2'$, dann kann man C_1^* aus C_1' bzw. C_2^* aus C_2' durch Ändern von negativ bzw. positiv vorkommenden Unterformeln erhalten. Mit der Induktionshypothese erhalten wir also, dass die Sequente $C_1^* \to C_1'$ und $C_2' \to C_2^*$ gültig sind. Aus diesen Sequenten können wir nun das gewünschte Sequent folgendermaßen beweisen:

$$\dfrac{\dfrac{C_1^* \to C_1' \qquad C_2' \to C_2^*}{C_1' \supset C_2', C_1^* \to C_2^*}}{C_1' \supset C_2' \to C_1^* \supset C_2^*} \ .$$

Für (b) kann man wieder symmetrisch vorgehen. Die Vorgehensweise für Konjunktion und Disjunktion ist dieselbe und wird hier nicht ausgeführt. ■

Die Aussage der folgenden Propositionen ist, vereinfacht formuliert, dass, wenn eine s-Formel A im Endsequent eines Beweises eine wesentliche Rolle im Beweis spielt, dann gibt es einen Pfad von dieser Formel zurück ins Endsequent.

Proposition 3.13. *Sei P ein Beweis von $\Gamma \to \Delta$ und sei A eine atomare s-Formel ohne Gleichheitssymbol, die in $\Gamma \to \Delta$ negativ vorkommt. Dann gilt mindestens eine der folgenden Aussagen:*

(a) Es gibt einen vorwärts-Pfad in G_P von A zu einer anderen s-Formel B in $\Gamma \to \Delta$.

(b) Das Sequent $\Gamma^* \to \Delta^*$, das man durch Ersetzung von A durch $\top$ erhält, ist beweisbar.

Beweis. Wir betrachten den Fall, in dem A negativ im Endsequent vorkommt. Den anderen Fall kann man symmetrisch behandeln. Angenommen, es gibt keinen vorwärts-Pfad in G_P von A zurück ins Endsequent. Nach Proposition 3.9 gibt es einen baum-ähnlichen Beweis P_1 von $\Gamma \to \Delta$, sodass man die Pfade in G_{P_1} mit denen in G_P identifizieren kann. Damit gibt es auch keinen vorwärts-Pfad in G_{P_1} von A zurück ins Endsequent. Wir transformieren nun P_1 zu P_2 in dem wir alle von A vorwärts-erreichbaren s-Formeln in G_{P_1} durch $\top$ ersetzen. Es ist nicht offensichtlich, dass diese Transformation einen korrekten Beweis von $\Gamma^* \to \Delta^*$ liefert. Da die Transformation offenbar die Baum-Ähnlichkeit erhält, gibt es nur wenige Fälle, in denen die Korrektheit von P_2 scheitern könnte; nämlich genau bei Axiomen oder bei Kontraktionen. Bei allen anderen Inferenzen ist der Eingangs-und Ausgangsgrad aller s-Formeln im oberen und unteren Sequent höchstens eins (dies ist bei nicht baum-ähnlichen Beweisen im Allgemeinen nicht der Fall). Da

außerdem das Gleichheitssymbol in A nicht vorkommt, gibt es bei den Axiomen auch zwei Fälle, die wir uns überlegen werden. Falls A eine Unterformel einer Formel B ist und in P_1 das Axiom $B \to B$ verwendet wird, so ist auch $B^* \to B^*$ ein Axiom in P_2. Da A atomar ist, hat A die Form $Q(s_1, \dots, s_k)$ für ein Prädikatensymbol Q. Nun gibt es noch den Fall, dass ein Leibniz-Axiom in P_1 durch

$$r_1 = t_1, \dots, r_k = t_k, \top \to \top$$

ersetzt wurde. Dies ist zwar kein Axiom mehr, es ist aber ein gültiges Sequent, da ja sogar $\to \top$ gültig ist. Wir kommen nun zu den Kontraktionen. Beispielsweise könnte P_2 nun eine "Inferenz" der Form

$$\frac{\Pi \to \Lambda, C', C''}{\Pi \to \Lambda, C^*}$$

wobei C', C'' und C^* durch Ersetzen von Unterformeln der Form $Q(\dots)$ einer Formel C durch $\top$. Falls nun $Q(\dots)$ negativ in C vorkommt und in einer der drei Formeln durch $\top$ ersetzt wird, so wird die s-Formel in allen dreien durch $\top$ ersetzt. Dies gilt, da wegen der Baum-Ähnlichkeit die einzigen Kanten, die auf negativ vorkommende Unterformeln von C' und C'' zeigen, von den entsprechenden Unterformeln in C^* kommen.
Kommt $Q(\dots)$ positiv in C vor und wird in C' oder C'' durch $\top$ ersetzt, dann auch in C^*. Also kann man C^* sowohl von C' als auch von C'' erhalten, indem man positiv vorkommende Subformeln durch $\top$ ersetzt, damit muss nach Lemma 3.12 aber bereits $C' \supset C^*$ und $C'' \supset C^*$ gelten. Insgesamt kann man dann obige Inferenz durch zwei Schnitte und einer Kontraktion ersetzen.
Für die zweite Kontraktionsinferenz sowie für die impliziten Kontraktionen der Nebenformeln in $\vee : r$ und $\wedge : \ell$ argumentiert man analog. Wir haben also gezeigt, dass P_2 ein Beweis ist, womit also das Endsequent $\Gamma^* \to \Delta^*$ gültig ist. ■

Bemerkung 3.14. Im obigen Beweis war wesentlich für unsere Konstruktion, dass wir angenommen haben, dass der Fall (a) nicht gilt, wie das folgende Gegenbeispiel zeigt. Betrachten wir den Beweis:

$$\frac{A \to A}{A \to A \wedge B}\ .$$

Dieser würde durch unsere obige Transformation zu

$$\frac{\top \to \top}{\top \to \top \wedge B}\ ,$$

dessen Endsequent kein gültiges Sequent ist, falls B nicht gültig ist.

Proposition 3.15. *Sei P ein Beweis und $A \vee B$ eine negativ vorkommende s-Formel im Endsequent $\Gamma \to \Delta$. Dann gilt mindestens eine der folgenden Aussagen:*

(a) *Es gibt einen vorwärts-Pfad von $A \vee B$ zu einer anderen s-Formel in $\Gamma \to \Delta$.*

(b) *Es gibt eine $\vee : \ell$ Inferenz mit Hauptformel $A^* \vee B^*$, die von $A \vee B$ vorwärts-erreichbar ist.*

(c) *Das Sequent $\Gamma^* \to \Delta^*$, das durch Ersetzung von $A \vee B$ durch $\top$ entsteht, ist gültig.*

Beweis. Angenommen (a) und (b) gelten nicht. Wir gehen nun ähnlich wie in Proposition 3.13 vor. Nach 3.9 können wir P in einen baum-ähnlichen Beweis P_1 transformieren, der noch immer die Eigenschaften (a) und (b) nicht erfüllt. Nun erhalten wir P_2, indem wir jede von $A \vee B$ vorwärts-erreichbare s-Formel mit $\top$ ersetzen. Da P_2 baum-ähnlich ist, ist die einzige Möglichkeit, in der P_2 fehlschlagen könnte, ein korrekter Beweis zu sein, bei Kontraktionen (impliziten und expliziten). Hier geht außerdem ein, dass P_1 (b) nicht erfüllt, da dies in P_2 eine falsche Inferenz produzieren würde. Man kann analog vorgehen wie im Beweis von Proposition 3.13. Damit ist P_2 ein korrekter Beweis von $\Gamma^* \to \Delta^*$. ■

Proposition 3.16. *Sei P ein Beweis und A eine negativ vorkommende s-Formel im Endsequent $\Gamma \to \Delta$. Dann gilt mindestens eine der folgenden Aussagen:*

(a) *Es gibt einen vorwärts-Pfad von A zu einer anderen s-Formel in $\Gamma \to \Delta$.*

(b) *Es gibt eine von A vorwärts-erreichbare Formel, die Hauptformel einer Inferenz ist.*

(c) *Das Sequent $\Gamma^* \to \Delta^*$, das durch Ersetzung von A durch $\top$ entsteht, ist gültig.*

Proposition 3.17. *Sei P ein Beweis und $A \wedge B$ eine negativ vorkommende s-Formel im Endsequent $\Gamma \to \Delta$. Dann gilt mindestens eine der folgenden Aussagen:*

(a) *Es gibt einen vorwärts-Pfad von $A \wedge B$ zu einer anderen s-Formel in $\Gamma \to \Delta$.*

(b) *Es gibt mindestens zwei von $A \wedge B$ vorwärts-erreichbare Formeln, die Hauptformeln von $\wedge : \ell$ Inferenzen sind.*

(c) *Das Sequent $\Gamma^* \to \Delta^*$, das durch Ersetzung von $A \wedge B$ durch A entsteht, ist gültig.*

(d) *Das Sequent $\Gamma^* \to \Delta^*$, das durch Ersetzung von $A \wedge B$ durch B entsteht, ist gültig.*

Beweis. Angenommen (a) und (b) gelten nicht, und die einzige (falls überhaupt existente) $\wedge : \ell$ Inferenz mit von $A \wedge B$ vorwärts-erreichbaren Hauptformel ist von der Form

$$\frac{A^*, \Pi \to \Lambda}{A^* \wedge B^*, \Pi \to \Lambda} .$$

Der Fall, in dem B^* im oberen Sequent steht, kann symmetrisch behandelt werden. Nach Proposition 3.9 existiert ein baum-ähnlicher Beweis P_1, in dem (a) nicht gilt. Außerdem muss jede $\wedge : \ell$ Inferenz in P_1 von obiger Form sein, da in der Transformation nur Unterbeweise dupliziert wurden. Nun erhalten wir P_2, indem wir jede von $A \wedge B$ vorwärts-erreichbare s-Formel $A' \wedge B'$ durch A' ersetzen. Wir überlegen uns jetzt, dass alle "Inferenzen" in P_2 korrekt sind. Die Korrektheit könnte bei $\wedge$-Inferenzen oder Kontraktionen fehlschlagen. Bei allen anderen Inferenzen werden Subformeln oder Nebenformeln wegen der Baum-Ähnlichkeit immer sowohl im oberen als auch im unteren Sequent ersetzt, womit die Korrektheit erhalten bleibt. Wir haben uns bereits überlegt, dass alle $\wedge : \ell$ Inferenzen in P_1 von derselben Form wie in P sind, also wird daraus in P_2

$$\frac{A^*, \Pi \to \Lambda}{A^*, \Pi \to \Lambda} \,,$$

was offenbar korrekt ist. Eine $\wedge : r$ Inferenz mit von $A \wedge B$ vorwärts-erreichbarer Hauptformel wird in P_2 zu

$$\frac{\Pi \to \Lambda, A^* \qquad \Pi \to \Lambda, B^*}{\Pi \to \Lambda, A^*} \,.$$

Dies ist auch eine korrekte Inferenz. Wir kommen nun zu den Kontraktionen, es reicht, sich einen Fall zu überlegen, da man für die anderen analog vorgehen kann. Wir betrachten also Kontraktion einer Formel C in P_1, diese wird in P_2 zu

$$\frac{\Pi \to \Lambda, C', C''}{\Pi \to \Lambda, C^*} \,.$$

Dabei entstehen C', C'' und C^* durch Ersetzung einiger Unterformeln der Form $A' \wedge B'$ in C durch A'.

1.Fall: $A' \wedge B'$ kommt negativ in C vor. Nach Proposition 3.11 laufen die Kanten in G_{P_1} also vom Vorkommiss von $A' \wedge B'$ im unteren Sequent zum Vorkommnis im oberen. Weil dies, da P_1 baum-ähnlich ist, die einzigen Eingangskanten sind, werden in C^* genau jene Unterformeln ersetzt, die auch in C' und C'' ersetzt wurden. Das heißt $C' = C'' = C^*$, also ist obige Inferenz eine "gewöhnliche" Kontraktion.

2.Fall: $A' \wedge B'$ kommt positiv in C vor. Nach Proposition 3.11 laufen die Kanten in G_{P_1} also vom Vorkommiss von $A' \wedge B'$ im oberen Sequent zum Vorkommnis im unteren. Das heißt, falls in einer der Formeln C' oder C'' eine Ersetzung durchgeführt wird, dann auch in C^*. Man kann nun ähnlich wie in Lemma 3.12 schließen, dass dann sogar schon $C' \supset C^*$ und $C'' \supset C^*$ gültig sind. Damit können wir obige Inferenz durch zwei Schnitte und eine Kontraktion ersetzen. Für die impliziten Kontraktionen in $\vee : \ell$ bzw. $\wedge : r$ Inferenzen geht man analog vor. ■

Bemerkung 3.18. Die Propositionen 3.13 - 3.17 haben duale Versionen. Diese können erhalten werden, indem man in den Formulierungen 'negativ', 'vorwärts-Pfad', '$\top$', '$\vee$', '$\wedge$' '$\vee : \ell$' bzw. '$\wedge : \ell$' mit 'positiv', 'rückwärts-Pfad', '$\bot$', '$\wedge$','$\vee$', '$\wedge : r$' bzw. '$\vee : r$' ersetzt. Die Beweise kann man ähnlich führen.

Proposition 3.19. *Sei P ein Beweis mit Endsequent $\Gamma \to \Delta$ und $A \vee B$ ist eine im Endsequent negativ vorkommende s-Formel, wobei A und B atomare Formeln ohne Gleichheitssymbol sind. Dann gilt mindestens eine der folgenden Aussagen:*

(a) Es gibt einen vorwärts-Pfad von $A \vee B$ zurück ins Endsequent.

(b) Es gibt vorwärts-Pfade π_A und π_B von A bzw. B zurück ins Endsequent, sodass π_A und π_B bis zu einer $\vee : \ell$ Inferenz parallel laufen und dann auseinander gehen.

(c) Das Sequent $\Gamma^* \to \Delta^*$, das durch Ersetzung von $A \vee B$ durch $\top$ entsteht, ist gültig.

Beweis. Wir gehen ähnlich vor wie in den letzten Beweisen. Nach Proposition 3.9 können wir ohne Beschränkung der Allgemeinheit annehmen, dass P baum-ähnlich ist. Es reicht zu zeigen, dass P eine Inferenz der Form

$$\frac{A^*, \Pi \to \Lambda \qquad B^*, \Pi \to \Lambda}{A^* \vee B^*, \Pi \to \Lambda}$$

enthält, wobei $A^* \vee B^*$ vorwärts-erreichbar von $A \vee B$ ist und Pfade von A^* bzw. B^* ins Endsequent $\Gamma \to \Delta$ existieren. Angenommen, so eine Inferenz existiert nicht. Wir transformieren nun P in P_1, indem wir alle von $A \vee B$ im Endsequent vorwärts-erreichbaren s-Formeln durch $\top$ ersetzen und, falls es eine $\vee : \ell$ Inferenz mit von $A \vee B$ vorwärts-erreichbarer Hauptformel $A^* \vee B^*$ gibt, so ersetzen wir auch alle von A^* bzw. B^* vorwärts-erreichbaren s-Formeln durch $\top$. Wir zeigen nun wie gewohnt, dass dies (unter der Voraussetzung, dass (a) nicht gilt) P_1 in einen korrekten Beweis von $\Gamma^* \to \Delta^*$ transformiert, in dem wir die Korrektheit aller 'Inferenzen' in P_1 zeigen. Dies verläuft analog zu Propositionen 3.13 und 3.15. ■

4 Der Beweis des Hauptsatzes

In diesem Abschnitt werden wir den Hauptsatz beweisen, indem wir das Unifikationsproblem zweiter Stufe mit partieller Substitution (im Folgenden nur noch als "Unifikationsproblem" bezeichnet) aus Abschnitt 2 auf das k-Beweisbarkeitsproblem reduzieren. Wir werden also für ein gegebenes Unifikationsproblem eine Formel Φ und eine Zahl N

finden, sodass das Unifikationsproblem genau dann lösbar ist, wenn die Formel einen LK-Beweis in höchstens N Zeilen hat. Sei also

$$\beta_{i_j}(\rho_j // a_{i_j}) = \sigma_j, \quad j = 1, \ldots, m \quad i_j \in \{1, \ldots, k\}$$

ein Unifikationsproblem, das die spezielle Restriktion erfüllt (vgl. Satz 2.6). Wir werden β_j nicht nur als Variablen zweiter Stufe verwenden, sondern auch als gebundene Variablen im Sequentialkalkül. Sei nun $U_j,\ j = 1, \ldots, m$, die Semiformel

$$P_j(\sigma_j, \rho_j) \vee P_j(\beta_{i_j}, a_{i_j}) \vee P_j(z_j^1, b_j^1) \vee P_j(z_j^2, b_j^2) \vee P_j(z_j^3, b_j^3) \vee P_j(z_j^4, b_j^4),$$

mit einem zweistelligen Relationssymbol P_j, neuen gebundenen Variablen $z_j^1, \ldots, z_j^4$ und neuen freien Variablen $b_j^1, \ldots, b_j^4$. Wir definieren nun Φ als die Formel

$$\Big(\forall z_1^1 \forall z_1^2 \cdots \forall z_m^3 \forall z_m^4 \forall \beta_1 \cdots \forall \beta_k \bigwedge_{j=1}^{m} U_j\Big) \supset \Big(\bigwedge_{j=1}^{m} \exists y \exists x P_j(x, y)\Big).$$

Offenbar ist Φ eine gültige Formel, wir interessieren uns aber für die Länge des kürzesten Beweises von Φ. Dafür geben wir vorerst einen nicht optimalen Beweis von Φ an und werden dann sehen, dass wir ihn unter der Voraussetzung der Lösbarkeit des Unfikationsproblems verkürzen können. Es seien $t_1, \ldots, t_k, r_1^1, \ldots, r_m^4$ Terme, dann bezeichnen wir mit $U_j(\mathbf{t},\ \mathbf{r})$ die Semiformel, die entsteht, wenn in U_j die β_i's mit den t_i's und die z_i^l's mit den r_i^l's substituieren. Dann erhalten wir einen Beweis von Φ mit $k + 4m$ $\forall : \ell$ Inferenzen und einer $\supset : r$ Inferenz ausgehend vom Sequent

$$\bigwedge_{j=1}^{m} U_j(\mathbf{t},\ \mathbf{r}) \to \bigwedge_{j=1}^{m} \exists y \exists x P_j(x, y).$$

Dieses Sequent kann man von den m Sequenten

$$U_j(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_j(x, y) \quad j = 1, \ldots, m$$

mit $m - 1$ $\wedge : r$ und $2(m - 1)$ $\wedge : \ell$ Inferenzen herleiten, indem man $m - 1$ mal nach folgendem Muster vorgeht:

$$\dfrac{\dfrac{U_{m-1}(\mathbf{t},\mathbf{r}) \to \exists y \exists x P_{m-1}(x, y)}{U_{m-1}(\mathbf{t},\mathbf{r}) \wedge U_m(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_{m-1}(x, y)} \quad \dfrac{U_m(\mathbf{t},\mathbf{r}) \to \exists y \exists x P_m(x, y)}{U_{m-1}(\mathbf{t},\mathbf{r}) \wedge U_m(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_m(x, y)}}{U_{m-1}(\mathbf{t},\mathbf{r}) \wedge U_m(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_{m-1}(x, y) \wedge \exists y \exists x P_m(x, y)}\ .$$

Nun hat $U_j(\mathbf{t},\mathbf{r})$ die Form

$$P_j(\sigma_j^*, \rho_j^*) \vee P_j(t_{i_j}, a_{i_j}) \vee P_j(r_j^1, b_j^1) \vee P_j(r_j^2, b_j^2) \vee P_j(r_j^3, b_j^3) \vee P_j(r_j^4, b_j^4),$$

wobei σ_j^* und ρ_j^* die Terme sind, die man erhält, wenn man in σ_j bzw. ρ_j die β_i's durch t_i's ersetzt. Wir können also $U_j(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_j(x,y)$ mit fünf $\vee : \ell$ Inferenzen von Sequenten der Form $P_j(v,w) \to \exists y \exists x P_j(x,y)$ beweisen. Diese haben einen einfachen Beweis mit einem Axiom und zwei $\exists : r$ Inferenzen. Zählen wir also die Sequente, brauchen wir genau $6 \cdot 3 + 5 = 23$ um $U_j(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_j(x,y)$ zu beweisen (wegen der speziellen Restriktion sind alle Sequente verschieden). Insgesamt haben wir folglich Φ in

$$(k + 4m + 1) + (3m - 3) + 23m = k + 30m - 2$$

Sequenten bewiesen. Dies ist allerdings nicht der effizienteste Beweis, falls das Unifikationsproblem lösbar ist.
Wir wählen nun die Terme $\mathbf{t}$, sodass wir, wenn wir $\beta_i = t_i$ setzen eine Lösung für

$$\beta_{i_j}(\rho_j // a_{i_j}) = \sigma_j$$

erhalten. Daher muss es eine Menge S von Vorkommnissen von a_{i_j} in t_{i_j} geben, sodass man durch Substitution von jedem a_{i_j} in S durch ρ_j^*, σ_j^* erhält. Sei also $v(w)$ definiert als das Resultat der Substitution aller $a_{i_j} \in S$ durch w in t_{i_j}. Außerdem wählen wir die r_j^i als $v(b_j^i)$ für $i = 1,2,3,4$. Wir können nun eine kürzere Herleitung des Sequents $U_j(\mathbf{t}, r) \to \exists y \exists x P_j(x,y)$ angeben. Zuerst leiten wir mit 6 $\exists : r$ Inferenzen und 6 Axiomen die Sequente

$$\begin{aligned}
&P_j(\sigma_j^*, \rho_j^*) \to \exists y P_j(v(y), y),\\
&P_j(t_{i_j}, a_{i_j}) \to \exists y P_j(v(y), y),\\
&P_j(r_j^i, b_j^i) \to \exists y P_j(v(y), y), \quad i = 1,2,3,4,
\end{aligned}$$

her. Dies funktioniert, da $v(\rho_j^*) = \sigma_j^*$, $v(a_{i_j}) = t_{i_j}$ und $v(b_j^i) = r_j^i$. Nun erhalten wir mit fünf $\vee : \ell$ Inferenzen $U_j(\ \mathbf{t},\ \mathbf{r}) \to \exists y P_j(v(y), y)$. Letztlich betrachten wir folgenden Beweis:

$$\dfrac{U_j(\mathbf{t},\ \mathbf{r}) \to \exists y P_j(v(y), y) \qquad \dfrac{\dfrac{\dfrac{\dfrac{P_j(v(a),a) \to P_j(v(a),a)}{P_j(v(a),a) \to \exists x P_j(x,a)}}{P_j(v(a),a) \to \exists y \exists x P_j(x,y)}}{\exists y P_j(v(y),y) \to \exists y \exists x P_j(x,y)}}{U_j(\mathbf{t},\ \mathbf{r}) \to \exists y \exists x P_j(x,y)}\ \text{Schnitt} \quad .$$

Dabei ist a eine freie Variable, die nicht in t_{i_j} vorkommt. Zu beachten ist, dass wir für diese Herleitung einen Schnitt benötigt haben, denn nach [6] und [4] ist das Problem der k-Beweisbarkeit für das schnitt-freie Sequentialkalkül entscheidbar. Insgesamt haben wir also nur 22 Sequente für die Herleitung von $U_j(\mathbf{t}\ ,\mathbf{r}) \to \exists y \exists x P_j(x,y)$ gebraucht. Wir haben gezeigt: Hat das Unifikationsproblem zweiter Stufe eine Lösung, so kann die Formel Φ mit

$$(k + 4m + 1) + (3m - 3) + 22m = k + 29m - 2$$

Sequenten bewiesen werden, m Sequente weniger als vorher. Wir definieren nun also $N := k + 29m - 2$. Es bleibt nun die andere Richtung zu zeigen: hat ein Beweis von Φ höchstens N Sequente, so ist das Unifikationsproblem lösbar.

Sei also P ein Beweis von Φ. Wir nennen einen Term t einer Variable β_i in P zugewiesen, falls in P eine Inferenz der Form

$$\frac{A(t), \Gamma \to \Lambda}{(\forall \beta_i) A(\beta_i), \Gamma \to \Delta}$$

existiert, sodass es einen vorwärts-Pfad von der s-Formel $\forall \beta_i \cdots \forall \beta_k \bigwedge_j U_j$ im Endsequent zu der Formel $(\forall \beta_i) A(\beta_i)$ in der obigen Inferenz gibt. So eine Inferenz nennen wir *term-zuweisende Inferenz*. Zu beachten ist, dass mehr als ein Term einer Variable β_i in P zugewiesen werden kann. Wir werden sehen, dass uns genau die term-zuweisenden Inferenzen, unter bestimmten Voraussetzungen eine Lösung des Unifikationsproblems liefern.

Nun geben wir eine untere Schranke an die Anzahl der Sequente an, die in P vorkommen müssen. Dafür werden uns Propositionen 3.15 - 3.17 behilflich sein. Die Formel Φ kommt in $\to \Phi$ natürlich positiv vor, es gibt außerdem keinen Pfad von Φ zurück ins Endsequent und natürlich ist das Sequent $\to \bot$ ungültig. Damit folgt aus der dualen Version von Proposition 3.16, dass es eine von Φ vorwärts-erreichbare Inferenz in P gibt, diese muss offenbar eine $\supset : r$ Inferenz sein. Ähnlich kann man bei den Unterformeln von Φ, die einen bis $k + 4m$ All-Quantoren enthalten vorgehen, und schließt, dass P mindestens $k + 4m$ $\forall : \ell$ Inferenzen enthält. Betrachten wir die Unterformeln von Φ, die auf der rechten Seite der Implikation ein bis $m - 1$ Konjunktionen enthalten, so können in der dualen Version von Proposition 3.15 Fälle (a) und (c) nicht eintreten, da einerseits auf der linken Seite der Implikation keine Varianten der Formeln stehen und andererseits das Sequent nicht gültig wäre, wenn die rechte Seite der Implikation durch $\bot$ ersetzt wird. Also kommen in P mindestens $m - 1$ $\wedge : r$ Inferenzen vor. Mit ähnlichen Argumenten bekommen wir durch Propositionen 3.17 und 3.15, dass P mindestens $2m - 2$ $\wedge : \ell$ und $5m$ $\vee : \ell$ Inferenzen enthält. Insgesamt haben wir in P also schon mindestens $k + 12m - 2$ Sequente, die notwendigerweise verschieden sind, da sie verschiedenen Inferenzen entstammen.

Es verbleibt die Anzahl der Sequente in P zu zählen, die gebraucht werden, um $U_j \to \exists y \exists x P_j(x, y)$ herzuleiten (obwohl dieses Sequent im Allgemeinen in P gar nicht vorkommen muss). Die Idee ist dafür $m+1$ disjunkte Mengen von Sequenten $S_1, \ldots, S_m$ und XS zu definieren, sodass in keiner Menge bereits gezählt Sequente enthalten sind. XS repräsentiert eine Menge von 'überschüssigen' Sequenten. Wir werden zeigen:

Behauptung. *Die Mengen $S_1, \ldots, S_m$ und XS können so definiert werden, dass die Kardinalität jedes S_j mindestens 17 ist und dass, wenn alle S_j genau von der Kardinalität*

17 sind und wenn $XS = \emptyset$, es dann Terme $t_1, \dots, t_k$ gibt, die $\beta_1, \dots, \beta_k$ zugewiesen sind, sodass

$$t_{i_j}(\rho_j^* // a_{i_j}) = \sigma_j^*, \quad j = 1, \dots m.$$

Dabei sind ρ_j^* bzw. σ_j^* die Terme, die man erhält, wenn man in ρ_j bzw. σ_j jedes β_i für t_i substituiert.

Konnten wir dies nämlich beweisen, so folgt der Hauptsatz: da die S_j mindestens Kardinalität 17 haben und disjunkt sind, haben wir in P also mindestens $k+29m-2 = N$ Sequente gezählt. Sind in einem S_j mehr als 17 Sequente oder ist XS nicht leer, ist P also schon ein zu langer Beweis und wir müssen keine Lösung des Unifikationsproblems angeben. Sind das jedoch alle Sequente, so ist jedem β_i nur ein Term zugewiesen, da die S_j keine Termzuweisungen enthalten und wir nur eine für jedes i gezählt haben. Also folgt aus der Behauptung, dass die Terme, die den β_i zugewiesen werden, eine Lösung des Unifikationsproblems sind. Insgesamt haben wir also gezeigt: $\to \Phi$ hat einen Beweis in höchstens N Zeilen, genau dann wenn das Unifikationsproblem einen Lösung hat. Der Hauptsatz folgt somit aus Satz 2.6.

Es bleibt die Behauptung zu zeigen. Dafür benötigt es allerdings noch ein wenig Vorarbeit. Die Idee zum Beweis der Behauptung ist es nämlich, die Mengen S_j über gewisse Pfade in P zu definieren. Wir betrachten also vorerst die sechs Atomformeln auf der linken Seite der Implikation in Φ. Definieren wir für $i = 1, 2, 3, 4$

$$v_1 := \sigma_j, \quad w_1 := \rho_j, \quad v_2 = \beta_{i_j}, \quad w_2 := a_{i_j}, \quad v_{2+i} := z_j^i, \quad w_{2+i} := b_j^i,$$

so sind diese Atomformeln von der Form $P_j(v_i, w_i)$ für $i = 1, \dots, 6$. Dabei wurde in der Definition ein zweiter Subskript unterschlagen, um die Notation übersichtlicher zu halten. Nach Proposition 3.19 existiert für $i = 1, \dots, 6$ jeweils mindestens ein Pfad π_i von der s-Formel $P_j(v_i, w_i)$ zu der s-Formel $P_j(x, y)$ auf der rechten Seite der Implikation. Von diesen Pfaden wählen wir nun jeweils nur solche, sodass die folgenden Bedingungen erfüllt sind:

(R1) $\pi_1, \dots, \pi_6$ laufen von Anfang an so lange als möglich parallel, bis sie an $\vee : \ell$ Inferenzen auseinander gehen.

(R2) Ist $P_j(\tau_i, \tau_i') \vee \dots \vee P_j(\tau_6, \tau_6')$ eine s-Formel, durch die die Pfade $\pi_i, \dots, \pi_6$, $i < 6$ parallel laufen, dann sind die Semiterme $\tau_i', \dots, \tau_6'$ paarweise verschieden.

(R3) Die Pfade $\pi_1, \dots, \pi_6$ sind die kürzesten Pfade, sodass (R1) und (R2) erfüllt sind.

Wir müssen zeigen, dass solche Pfade überhaupt existieren. Es reicht dabei, die Existenz von Pfaden zu zeigen, die (R1) und (R2) erfüllen, da man (R3) dann erhält, indem man die Pfade solange kürzt, bis (R1) oder (R2) nicht mehr erfüllt sind. Folgende Proposition liefert uns das gewünschte Ergebnis:

Proposition 4.1. *Sei $j \in \{1, \dots, m\}$ beliebig aber fest und sei P ein Beweis von Φ. Dann gibt es Pfade $\pi_1, \dots, \pi_6$ in G_P von $P_j(v_i, w_i)$ nach $P_j(x, y)$, die (R1) und (R2) erfüllen.*

Beweis. Nach Proposition 3.9 können wir ohne Beschränkung der Allgemeinheit annehmen, dass P baum-ähnlich ist. Angenommen es gäbe solche sechs Pfade nicht. Wir werden sehen, dass es dann einen LK_e Beweis P^* von der Formel Φ^* gibt, die man erhält, wenn man in Φ U_j entweder mit $\top$ oder mit

$$\bigwedge_{1 \leq n < s \leq 6} w_n \neq w_s$$

ersetzt. Wir erinnern uns, dass $w_2, \dots, w_6$ verschiedene freie Variablen sind und dass $w_1 = \rho_j$ wegen der speziellen Restriktion verschieden von diesen Variablen ist. Also ist obige Formel äquivalent zu $\top$. Betrachtet man allerdings die Formel $\exists y \exists x P_j(x, y)$, so ist diese nicht allgemeingültig, steht aber auf der rechten Seite der Implikation, da U_j aber als einzige Formel in der linken Seite Information über $P_j(\cdots)$ enthalten hat und durch eine gültige Formel ersetzt wurde, kann Φ^* nicht gültig sein. Somit haben wir einen Widerspruch erzeugt, wenn wir in der Lage sind P^* zu konstruieren. Dafür führen wir nun einige neue Vokabeln ein, um den Beweis übersichtlicher zu gestalten. Wir betrachten für $i = 1, \dots, 6$ die sechs Unterformeln

$$A_i := \bigvee_{n=i}^{6} P_j(v_n, w_n)$$

von U_j, die im Endsequent von P vorkommen. Sei B eine von A_i vorwärts-erreichbare s-Formel, das heißt $B = \bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)$.

- Falls es $s \neq n$ gibt, mit $\tau'_s = \tau'_n$, nennen wir B R2-*schlecht*. Wir nennen außerdem einen Pfad R2-*schlecht*, falls eine Formel auf dem Pfad R2-schlecht ist.

- Falls es einen Pfad von A_i nach B gibt, der nicht R2-schlecht ist, nennen wir B R2-*gut* (d.h. R2-gut ist nicht das Gegenteil von R2-schlecht).

- Falls B R2-schlecht ist und es eine Kante von einer R2-guten Formel zu B gibt, so nennen wir B R2-*grenzwärtig*.

- Wir nennen eine s-Formel der Form $P_j(\cdots)$ *realisierbar*, falls es einen vorwärts-Pfad von der s-Formel zur $P_j(x, y)$ im Endsequent gibt.

Wir bilden nun P^* aus P, indem wir folgende Transformationen durchführen:

(1) Ist B eine maximale s-Formel, die vorwärts-erreichbar von einem A_i ist und ist eines der Disjunkte in B nicht realisierbar, dann ersetze B durch $\top$.

(2) Alle restlichen nicht realisierbaren s-Formeln $P_j(\cdots)$ werden mit $\top$ ersetzt.

(3) Ist B eine maximale s-Formel in P und hat die Form $\bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)$ mit $i \leq 5$ und wurde nicht durch (1) oder (2) ersetzt, so ersetzen wir B durch

$$B_{schlecht} := \Big(\bigvee_{n=i}^{6} P_j(\tau_n, \tau'_n)\Big) \wedge \Big(\bigwedge_{1\leq n<s\leq 6} \tau'_n \neq \tau'_s\Big),$$

falls B nicht R2-gut ist und mit

$$B_{gut} := \bigwedge_{1\leq n<s\leq 6} \tau'_n \neq \tau'_s$$

falls B R2-gut ist.

Beachte, dass $U_j = A_1$ R2-gut ist, und somit im Endsequent wirklich entweder mit $\top$ oder $\bigwedge_{1\leq n<s\leq 6} w_n \neq w_s$ ersetzt wird. Man kann nun ähnlich wie in den Propositionen des vorigen Abschnitts vorgehen, um zu zeigen, dass P^* ein korrekter Beweis ist, indem man die Korrektheit aller 'Inferenzen' in P^* überprüft. Dies übersteigt das Ausmaß dieser Arbeit und wir verweisen auf [1]. ■

Beweis der Behauptung.
Die Vorgehensweise wird nun so sein, dass wir für festes j jeweils drei (oder mehr) verschiedene Sequente mit den Pfaden $\pi_1, \ldots, \pi_6$ assoziieren und in S_j geben. Also $|S_j| > 17$ womit wir nicht zeigen müssen, dass das Unifikationsproblem eine Lösung hat. Dies wird uns aber nicht immer gelingen, es gibt auch den Fall, dass wir jeden Pfad mit jeweils zwei Sequenten assoziieren und dann noch fünf Sequente mit allen Pfaden gemeinsam. Dann hätte S_j also eine Kardinalität von genau 17 und wir müssen zeigen, dass entweder Sequente existieren, die wir in XS geben können, oder das Unfikationsproblem eine Lösung besitzt. Letzterer Fall ist somit offenbar der wichtigste und wird von uns am genausten betrachtet werden.

Sei also $j \in \{1, \ldots, m\}$ beliebig, aber fest und $i, n \in \{1, \ldots, 6\}$ mit $i \neq s$. Da die Pfade π_i und π_n beide in der s-Formel $P_j(x, y)$ im Endsequent enden, muss eine s-Formel ψ existieren, die die erste s-Formel auf π_i ist, die auch auf π_n liegt. Da π_i und π_n die kürzesten Pfade mit Eigenschaften (R1) und (R2) sind, ist ψ außerdem die erste s-Formel auf π_n, die auch auf π_i liegt (sonst könnte man kürzere Pfade mit den Eigenschaften angeben). Außerdem können wir ohne Beschränkung der Allgemeinheit annehmen, dass die zwei Pfade von ψ ins Endsequent übereinstimmen (sonst könnten wir einen der Pfade kürzen). Da ψ eine Variante von $P_j(x, y)$ ist, gibt es Semiterme τ_1, τ_2 sodass $\psi = P_j(\tau_1, \tau_2)$. Wir machen nun eine Fallunterscheidung über den Aufbau der Oberformel von ψ. Wie oben bereits erwähnt, behandeln wir den wichtigsten Fall zu erst.

1.Fall: ψ ist eine Unterformel einer Formel der Form $(\exists y)P_j(\tau, y)$. Dann muss jeder der zwei Pfade mindestens eine $\exists : r$ Inferenz und ein Axiom der Form $P_j(\cdots) \to P_j(\cdots)$ enthalten. Falls π_i und π_n nach oben gerichtet sind, sobald sie ψ erreichen, muss es Schnitt-Inferenzen geben, die die Richtung der Pfade, nachdem die Pfade nach unten durch die $\exists : r$ Inferenzen gelaufen sind, nach oben kehren. Dann haben wir unsere gewünschten drei Sequente gefunden und sind fertig. Seien π_i und π_n also nach unten gerichtet, sobald sie ψ erreichen. Damit es nun möglich ist, dass im Endsequent die Formel $(\exists y)(\exists x)P_j(x, y)$ zustande kommt, muss auf dem Pfad von ψ ins Endsequent zuerst der Existenzquantor 'entfernt' werden, um die richtigen Existenzquantoren mit zwei $\exists : r$ Inferenzen zu erhalten. Für das Entfernen vom Existenzquantor braucht es einen Schnitt, um den Pfad nach oben zu wenden, eine $\exists : \ell$ Inferenz, um den Quantor zu entfernen und ein Axiom, um den Pfad nach unten zu kehren. Insgesamt haben wir also mit jedem Pfad 2 Sequente assoziiert und fünf Sequente, die sich die Pfade teilen müssen. Wir werden nun sehen, dass, um eine so kleine Anzahl an Sequenten zu erhalten, eine Art von Unifikation stattfindet oder wir Sequente in XS geben können.
Wir erinnern uns, dass der Pfad π_i bei der s-Formel $P_j(v_i, w_i)$ beginnt, wobei v_i und w_i Semiterme sind. Folgen wir dem Pfad nach oben, so werden $\beta_1, \ldots, \beta_k$ Terme $t_1, \ldots, t_k$ durch $\forall : \ell$ Inferenzen zugewiesen. Außerdem werden auch den z^i's Terme zugewiesen. Kommen nun inmitten der term-zuweisungs Inferenzen andere Quantoreinführungen vor, so ist das nur möglich, wenn der Pfad durch ein Axiom nach unten gerichtet wurde und dann wieder durch einen Schnitt nach oben gerichtet. Dieses Axiom und diese Schnitt-Inferenz können wir in XS geben und sind fertig. Sind die term-zuweisungs Inferenzen also ununterbrochen von anderen Quantorinferenzen, so transformieren sie den Term v_i in einen Term v_i^*, der keine gebundenen Variablen enthält. Ähnlich erhält man aus dem Term v_n einen Term v_n^*, der keine gebundenen Variablen enthält. Außerdem erhält man für i oder n gleich eins, dass der Term $w_1 = \rho_j$ in einen Term ρ_j^* transformiert wird, in dem jedes Vorkommen von β_{i_k} durch t_{i_k} ersetzt wird. Da wir uns in LK und nicht in LK_e befinden, ist die einzige Möglichkeit, dass jeweils eine Existenzquantifikation ausreicht, um $P_j(v_i^*, w_i)$ bzw. $P_j(v_n^*, w_n)$ in $(\exists y)P_j(\tau, y)$ zu überführen, dass

$$\tau(w_i/y) = v_i^* \quad \text{und} \quad \tau(w_n/y) = w_n^* \tag{4.1}$$

Daher gilt

$$v_i^*(w_n//w_i) = \tau(w_i//y)(w_n//w_i) = \tau(w_n//y) = v_n^*.$$

Setzt man nun in obiger Gleichung $i = 2$ und $n = 1$ so erhält man

$$t_{i_j}(\rho_j^*//a_{i_j}) = \sigma_j^*,$$

womit die Behauptung in diesem Fall, unter der Annahme, dass wir auch bei den restlichen Pfaden keine zusätzlichen Sequente finden, gezeigt ist. Zu beachten ist,

dass wir in der obigen Gleichung nur eine partielle Substitution erhalten, da im Allgemeinen $w_1 = \rho_j^*$ die freien Variablen w_i für $i = 2, \ldots, 6$ enthalten könnte.

2.Fall: Bei anderen Fällen mit $\psi = P_j(\tau, y)$ für eine gebundene Variable y kann man ähnlich vorgehen.

3.Fall: ψ ist eine Unterformel einer Formel der Form $(\exists y)(\exists x)P_j(x, y)$. Ähnlich wie vorher sieht man, dass dann auf jedem Pfad mindestens zwei $\exists : r$ und ein Axiom liegen müssen, also insgesamt mindesten drei Sequente pro Pfad. Bei weiteren anderen Fällen, in denen ψ in der Reichweite zweier Quantoren liegt, kann man analog vorgehen.

4.Fall: ψ ist eine Unterformel einer Formel der Form $P_j(\tau, t)$, wobei τ ein Semiterm und t ein Term ist. Wegen der speziellen Restriktion gilt $w_i \neq w_n$. Deshalb muss entweder w_i oder w_n auf einem der Pfade zu t geändert worden sein. Wir werden sehen, dass dies mindestens vier Sequente benötigt. Wegen Eigenschaft (R1) laufen π_i und π_n so lange als möglich parallel (und nach oben gerichtet), bis sie an einer $\vee : \ell$ Inferenz auseinander laufen. Durch Eigenschaft (R2) stehen an dieser Inferenz s-Formeln $P_j(v_i', w_i')$ und $P_j(v_n', w_n')$ mit $w_i' \neq w_n'$. Also muss entweder w_i' oder w_n' in t transformiert werden. Da P ein LK Beweis ist, ist die einzige Möglichkeit in P Terme zu ändern, durch Quantorinferenzen. Der Pfad muss also durch ein Axiom nach unten gerichtet werden, dann wird w_i oder w_n mit einer $\exists : r$ oder $\forall : \ell$ Inferenz quantifiziert. Mit einem Schnitt wird der Pfad wieder nach oben gerichtet und durch eine weitere Quantorinferenz wird der Quantor wieder entfernt. Wir konnten also vier Sequente mit einem der Pfade assoziieren.

Die obige Analyse muss man nun auch noch unter Betrachtung von $3, 4, 5$ oder 6 Pfaden durchführen. Dies kann unter Umständen sehr mühsam sein, weswegen wir nur das Ergebnis der fertigen Analyse angeben werden. Es stellt sich heraus, dass entweder:

(a) Es gibt mindestens drei Sequente, die wir mit jeweils einem Pfad assoziieren können, oder, falls Fall 4. eintritt, gibt es jeweils vier Sequente, die wir mit fünf der Pfade assoziieren können, in jedem Fall also $|S_j| \geq 18$.

(b) Es gibt zwei Sequente, die wir mit jeweils einem Pfad assoziieren können, und fünf Sequente, die wir mit allen Pfaden assoziieren. Daher also $|S_j| = 17$, und ist XS leer, so kann man eine Lösung des Unifikationsproblems durch die termzuweisenden Inferenzen im Beweis P erhalten.

Die Behauptung ist nun allerdings noch nicht vollständig gezeigt: es könnte noch sein, dass die Mengen $S_1, \ldots, S_m$ nicht disjunkt sind. Es könnte nämlich passieren, dass die ersten $\exists : r$ und $\exists : \ell$ Inferenzen in Fall 1. oder die zwei Existenzeinführungen in Fall 3.

in mehr als einem S_j vorkommen. Dies tritt Beispielsweise ein, falls die s-Formel ψ von vorher in einer Formel der Form

$$(\exists z)(P_j(\tau, z) \vee P_{j'}(\tau', z)),$$

mit $j \neq j'$ vorkommt. Um dieses Problem zu beheben, muss man die Sequente zählen, die gebraucht werden, um die Disjunktion herzuleiten, und diese dann anstelle der üblichen Sequente in $S_{j'}$ geben. Analog geht man auch bei einer Konjunktion oder Implikation anstelle der Disjunktion vor. Es könnten nun auch mehr als ein logisches Konnektiv in der Formel vorkommen, dies wird aber immer sehr ineffizient sein und den Beweis verlängern. Für eine ausführlichere Argumentation verweise ich wieder auf [1]. Dies beendet den Beweis der Behauptung und wie wir uns bereits überlegt haben, auch den Beweis des Hauptsatzes. ■

Mit obigem Beweis erhalten wir außerdem den Hauptsatz für LK_e:

Hauptsatz. *Sei LK_e Gentzens Sequentialkalkül mit Gleichheitssymbol, einem einstelligen Funktionssymbol S, einem zweistelligen Funktionssymbol und abzählbar vielen zweistelligen Relationssymbolen. Dann gibt es für jede semi-entscheidbare Menge X eine Formel $A(x)$ und eine Zahl $k \in \mathbb{N}$ so, dass für alle n, $n \in X$ genau dann wenn $\to A(S^n 0)$ hat einen LK_e-Beweis mit höchstens k verschiedenen Sequenten.*

Beweis. Wir müssen nur die Formel Φ etwas modifizieren, sodass die Gleichheitsaxiome in einem effizienten Beweis nicht verwendet werden können. Dafür ersetzen wir in Φ jede Unterformel der Form $P_j(\cdots)$ durch

$$(\cdots((P_j(\cdots) \wedge \top) \wedge \top) \wedge \cdots \wedge \top)$$

mit N Konjunktionen, wobei N dieselbe Zahl wie im letzten Beweis ist. Da die Gleichheitsaxiome nur auf Atomformeln anwendbar sind, würde es mindestens $N \wedge : \ell$ Inferenzen brauchen, um überhaupt ein Gleichheitsaxiom auf ein $P_j(\cdots)$ anzuwenden. Wir können also analog wie im letzten Beweis vorgehen. ■

Literaturverzeichnis

[1] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic 53*, pages 75–102, 1991.

[2] Heinz-Dieter Ebbinghaus, Jörg Flum, Wolfgang Thomas, Jörg Flum, and Wolfgang Thomas. *Einführung in die mathematische Logik* -. Springer-Verlag, Berlin Heidelberg New York, 6. aufl. edition, 2018.

[3] Gaisi Takeuti. *Proof theory.* Dover, 2013.

[4] J. Krajiček und P. Pudlák. The number of proof lines and the size of proofs in first-order logic. *Arch. Math. Logic 27*, pages 69–84, 1988.

[5] Matiyasevich Yu. V. Enumerable sets are diophantine. *Soviet Mathematics 11*, page 354–357, 1970.

[6] V.P.Orevkov. Reconstruction of a proof from its scheme. *Soviet Math Dokl. 35*, pages 326–329, 1987.