Beweisnetze in linearer Logik

Christoph Reichenbach
<creichen@rbg.informatik.tu-darmstadt.de>

Darmstadt, 24. Juni 2002

Zusammenfassung

Beweisnetze sind bipartite Graphen, die große Ähnlichkeiten mit Beweisen im linearen Sequenzenkalkül aufweisen, dabei jedoch ohne ein Äquivalent zur exchange-Regel auskommen. Auch bei der Schnitt-Elimination ergibt sich, daß Beweisnetze eine abstraktere Beschreibung als Sequenzen- Beweise sind, also oft mit mehreren solchen korellieren.

1 Motivation

Bei der Beobachtung der Effekte von Schnitteliminationen im linearen Fall begegnen wir schnell Konfigurationen der Art

$$\dfrac{\dfrac{\vdash \Gamma, A}{\vdash \Gamma', A}(r) \qquad \dfrac{\vdash A^\perp, \Delta}{\vdash A^\perp, \Delta'}(s)}{\vdash \Gamma', \Delta'}(cut)$$

für bestimmte Regeln *(r)* und *(s)*. Wenn wir nun die Anwendung der *(cut)*-Regel nach oben verschieben wollen (wie wir dies bei der Schnittelimination gerne tun würden), stoßen wir auf die Frage, ob auf die dann verbleibenden $\vdash \Gamma, \Delta$ zuerst *(r)* oder zuerst *(s)* angewendet werden sollte; eine Frage, auf die es nach unserem Kenntnisstand keine eindeutige Antwort zu geben scheint.

Dies gibt Anlaß zur Suche nach einer abstrakteren Darstellung linearer Beweise, in der wir die aus beiden möglichen Entscheidungen resultierenden miteinander identifizieren würden. Eine solche wurde tatsächlich bereits in [Gir87] angegeben und soll hier vorgestellt werden, wobei wir uns zunächst dazu auf **MLL**, das multiplikative Fragment der linearen Logik, beschränken. Betrachten wir aber vorerst einmal eine etwas allgemeinere Konstruktion.

2 Beweisstrukturen

Definition 1 *Eine Beweisstruktur in* **MLL** *ist ein Tupel* $\Theta = (F, L)$ *mit* $F \subseteq \mathcal{F}_{LL} \times \mathbb{N}$ *(wobei* $\mathcal{F}_{LL}$ *die Menge aller Formeln der linearen Logik ist) und* $L \subseteq \{\otimes, \invamp, ax, cut\} \times 2^F \times 2^F$*, in dem*

(i) für jedes $l \in L$ *eine der folgenden Bedingungen erfüllt ist:*

- $l = (ax, \emptyset, \{(A, i_1), (A^\perp, i_2)\})$*, wobei* $i_1 \neq i_2$ *(Axiom-Link)*
- $l = (\otimes, \{(A, i_1), (B, i_2)\}, \{(A \otimes B, i_3)\})$*, wobei* i_1, i_2, i_3 *paarweise ungleich (Times-Link)*
- $l = (\invamp, \{(A, i_1), (B, i_2)\}, \{(A \invamp B, i_3)\})$*, wobei* i_1, i_2, i_3 *paarweise ungleich (Par-Link)*

- *$l = (cut, \{(A, i_1), (A^\perp, i_2)\}, \emptyset)$, wobei $i_1 \neq i_2$ (Cut-Link)*

(ii) Für alle $f \in F$ genau ein $(o, P_l, C_l) \in L$ existiert, so daß $f \in C_l$

(iii) Für alle $f \in F$ höchstens ein $(o, P_l, C_l) \in L$ existiert, so daß $f \in P_l$

(iv) $F \neq \emptyset$

In Tripeln $l = (o, \mathcal{P}, \mathcal{C}) \in L$ bezeichnen wir die Elemente von $\mathcal{P}$ als *Prämissen* von l, die Elemente von $\mathcal{C}$ als dessen *Konklusionen*. l selbst nennen wir *Link*. Die Elemente von F werden in diesem Text *Vorkommen von Formeln* tituliert werden[1], oder, wenn Verwechslung ausgeschlossen ist, zur Vereinfachung nur "Formeln", und schreiben für (A, i) nur A. Bei Verwendung dieser Vereinfachungen meinen wir für Vorkommen von Formeln $A = (A_r, i)$ und $B = (B_r, j)$ dann mit $A^\perp$, $A \parr B$ und $A \otimes B$ entsprechend $(A_r^\perp, k)$, $(A_r \parr B_r, k)$ bzw. $(A_r \otimes B_r, k)$ für ein passendes k. Formelvorkommen, die nicht als Prämisse eines Links auftreten, bezeichnen wir als *terminale Vorkommen von Formeln*, die Links, deren Konklusionen sie sind, als *terminale Links*.

Bemerkung: Das Verständnis dieser Strukturen als (gerichtete) bipartite Graphen ergibt sich durch eine Knotenmenge, die in die Partition $\{F, L\}$ zerfällt und eine geeignete Definition der (gerichteten) Kanten, z.B. von Links zu ihren Konklusionen und von Prämissen zu ihren Links.

Definition 2 *Eine Beweisstruktur $\Theta' = (F', L')$ ist Teilstruktur einer Beweisstruktur $\Theta = (F, L)$ gdw $F' \subseteq F$ und $L' \subseteq L$; dies schreiben wir $\Theta' \subseteq \Theta$.*

2.1 Desequentialisierung

Definition 3 *Die Desequentialisierung eines Beweises im* **MLL**-*Sequenzenkalkül ist eine Beweisstruktur, induktiv (über die Struktur des Beweises) definiert wie folgt:*

- $\dfrac{}{\vdash A, A^\perp}$ *(identity): Wir führen A und $A^\perp$ mit frischen Indizes als (Vorkommen von) Formeln ein, sowie einen Axiom-Link $(ax, \emptyset, \{A, A^\perp\})$.*

- $\dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}$ *(par): Die die Formeln A und B einführende Beweisstruktur erweitern wir durch die neue Formel $A \parr B$ für einen frisches Index und fügen einen Par-Link $(\parr, \{A, B\}, \{A \parr B\})$ hinzu.*

- $\dfrac{\vdash \Gamma, A \quad \vdash B, \Delta}{\vdash \Gamma, A \otimes B, \Delta}$ *(times): Hier werden zwei Beweisstrukturen $\Theta_1 = (F_1, L_1)$, $\Theta_2 = (F_2, L_2)$ mit $A \in F_1$ und $B \in F_2$ miteinander verbunden. Um eine Invalidierung der Struktur zu vermeiden, fordern wir o.B.d.A. (durch Umbenennung der Indices erreichbar), daß $F_1 \cap F_2 = \emptyset$. Die resultierende Struktur definieren wir wie folgt:*

  $$\Theta_{1+2} = (F_1 \cup F_2 \cup \{A \otimes B\}, F_1 \cup F_2 \cup \{(\otimes, \{A, B\}, \{A \otimes B\})\})$$

  für einen neuen Index.

- $\dfrac{\vdash \Gamma, A \quad \vdash A^\perp, \Delta}{}$ *(cut): Analog zur (times)-Regel, wobei jedoch keine neue Formel eingefügt wird und der neue Link von der Gestalt $(cut, \{A, A^\perp\}, \emptyset)$ ist.*

[1] *occurences of formulas* ist die Bezeichnung, die Girard verwendet, aber die Übersetzung davon ist genauso umständlich zu sprechen.

Definition 4 *Ein Beweisnetz Θ ist eine Beweisstruktur, für die ein Beweis im* **MLL***-Sequenzenkalkül existiert, dessen Desequentialisierung es ist. Analog bezeichnen wir das Finden eines solchen sequentiellen Beweises zu einem Beweisnetz als Sequentialisierung.*

Mit Beweisnetzen haben wir nun die von uns gesuchte Struktur. Da die Desequentialisierung auf **MLL** vollständig definiert ist, sind Beweisnetze eine allgemeine Repräsentierung für Beweise in **MLL**; es verbleibt zu zeigen, daß sie allgemeiner sind als Beweise im **MLL**-Sequenzenkalkül.

Satz 1 *Es existieren Beweise π_1, π_2 im Sequenzenkalkül von* **MLL***, deren Desequentialisierungen identisch sind. Analog zu [Gir87] schreiben wir in diesem Fall $\pi_1 \rightsquigarrow \pi_2$.*

Beweis: Durch Finden eines Beispiels:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp} \quad \dfrac{}{\vdash B, B^\perp}}{\vdash A \otimes B, A^\perp, B^\perp}\otimes}{\vdash A \otimes B, A^\perp \parr B^\perp}\parr \quad \dfrac{}{\vdash C, C^\perp}}{\vdash (A \otimes B) \otimes C, A^\perp \parr B^\perp, C^\perp}\otimes \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash A, A^\perp} \quad \dfrac{}{\vdash B, B^\perp}}{\vdash A \otimes B, A^\perp, B^\perp}\otimes \quad \dfrac{}{\vdash C, C^\perp}}{\vdash (A \otimes B) \otimes C, A^\perp, B^\perp, C^\perp}\otimes}{\vdash (A \otimes B) \otimes C, A^\perp \parr B^\perp, C^\perp}\parr$$

Diesen beiden (nicht identischen) Beweisen ist durch den in Definition 3 angegebenen Desequentialisierungsalgorithmus das gleiche Beweisnetz zugeordnet.

$\square$

2.2 Ein kleiner Exkurs in die Graphentheorie

Für die nächste Sektion benötigen wir, um bestimmte Eigenschaften von aus Beweisnetzen erstellten Graphen zu zeigen, zwei kleine Hilfssätze aus der Graphentheorie, die zwar wohlbekannt sind, zu Zwecken der Vollständigkeit jedoch hier wiedergegeben werden sollen.

Definition 5 *Ein ungerichteter Graph ist ein Tupel $G = (V, E)$, für das gilt, daß $E \subseteq V \times V$ symmetrisch ist.*

Definition 6 *Ein Pfad in einem ungerichteten Graphen $G = (V, E)$ ist ein $n+1$-Tupel $\rho\colon \{0..n\} \to V$, für das gilt, daß $\forall i \in \{0..(n-1)\}.(\rho(i), \rho(i+1)) \in E$. Wir setzen $\lambda_\rho = n$ und sagen, daß der Pfad ρ von $\rho(0)$ nach $\rho(\lambda_\rho)$ führt. Der zu diesem inverse Pfad ρ^{-1} ist definiert als $\rho^{-1}(x) = \rho(\lambda_\rho - x)$ und existiert in einem ungerichteten Graphen trivialerweise genau dann, wenn ρ existiert.*

Definition 7 *Ein Pfad ρ in einem Graphen $G = (V, E)$ berührt einen Knoten $k \in V$ gdw $\exists i \in \{0..\lambda_\rho\}.\rho(i) = k$ gilt.*

Definition 8 *Ein Zyklus auf einem Graphen G ist ein Pfad ζ in G, für den gilt, daß $\zeta(x) = \zeta(y) \to x = y \vee (\{x, y\} = \{0, \lambda_\zeta\})$.*

Definition 9 *Ein Graph ist azyklisch oder zyklenfrei genau dann, wenn keine Zyklen auf ihm existieren.*

Definition 10 *Ein Graph $G = (V, E)$ ist verbunden gdw für alle $p_1, p_2 \in V$ ein Pfad ρ in G existiert, so daß $\rho(0) = p_1$ und $\rho(\lambda_\rho) = p_2$.*

Definition 11 *Die Konkatenation zweier Pfade* $\rho_1\colon \{0..n\} \to V$*,* $\rho_2\colon \{0..m\} \to V$ *über einem Graphen* $G = (V, E)$*, bezeichnet als*

$$(\boldsymbol{.})\colon (\{0..n\} \to V) \times (\{0..m\} \to V) \to (\{0..(m+n)\} \to V)$$

ist für den Fall $\rho_1(n) = \rho_2(0)$ *definiert als*

$$\rho_1 \boldsymbol{.} \rho_2(x) = \begin{cases} \rho_1(x) & falls \;\; x < n \\ \rho_2(x-n) & falls \;\; n \leq x \leq (n+m) \end{cases}$$

Definition 12 *Ein Pfad* ρ' *ist Teilpfad von* ρ*, wenn Pfade* ρ_a*,* ρ_b *existieren, so daß* $\rho = \rho_a \boldsymbol{.} \rho' \boldsymbol{.} \rho_b$*.*

Lemma 1 *Seien* $G_1 = (V_1, E_1)$ *und* $G_2 = (V_2, E_2)$ *azyklische, verbundene und ungerichtete Graphen, und* $V_1 \cap V_2 = \emptyset$*. Dann ist für beliebige* $\nu_1 \in V_1$*,* $\nu_2 \in V_2$ *die Verbindung der beiden Graphen durch die Kante* (ν_1, ν_2)*, der Graph*

$$G_{1+2} = (V_{1+2} = V_1 \cup V_2, E_{1+2} = E_1 \cup E_2 \cup \{(\nu_1, \nu_2), (\nu_2, \nu_1)\})$$

ebenfalls zyklenfrei und verbunden.

Beweis:

(i) Verbundenheit: Da G_1 und G_2 jeweils verbunden sind, können nicht verbundene Knotenpunkte p_1, p_2 nur so liegen, daß einer der beiden in V_1 und der ander in V_2 liegt. o.B.d.A. sei $p_1 \in V_1$ und $p_2 \in V_2$. Da $\nu_1 \in V_1$ und $\nu_2 \in V_2$ existieren Pfade ρ_1 mit $\rho_1 = (p_1, .., \nu_1)$ und $\rho_2 = (\nu_2, .., p_2)$. Da (ν_1, ν_2) trivialerweise ein Pfad ist, verbindet nun der Pfad $(\rho_1 \boldsymbol{.} (\nu_1, \nu_2)) \boldsymbol{.} \rho_2$ die Punkte p_1, p_2. $\lightning$

(ii) Zyklenfreiheit: Sei ζ ein Zyklus in G_{1+2}. Wenn für alle $i \in \{0..\lambda_\zeta\}$ gilt, daß $\zeta(i) \in V_j$ mit $j \in \{1, 2\}$, dann ist ζ auch eingeschränkt auf G_j ein Zyklus, was der Annahme widerspricht. Also existieren $k, l \in \{0..\lambda_\zeta\}$ mit $\zeta(k) \in V_1$ und $\zeta(l) \in V_2$. Sei o.B.d.A. $k = 0$. Dann können wir ζ aufteilen in $\zeta = \rho_1 \boldsymbol{.} \rho_2$ mit $\rho_1 = (\zeta(0), .., \zeta(l))$ und $\rho_2 = (\zeta(l), .., \zeta(\lambda_\zeta))$.

Nun gilt gemäß Definition von G_{1+2} jedoch für alle $p_1 \in V_1, p_2 \in V_2$ mit $(p_1, p_2) \in E_{1+2}$, daß $(p_1, p_2) = (\nu_1, \nu_2)$ oder $(p_1, p_2) = (\nu_2, \nu_1)$ (sonst wären V_1 und V_2 nicht disjunkt gewesen). Damit müßen i_1, i_2 mit $\rho_1(i_1) = \rho_2(i_2) = \nu_1$ existieren, insbesondere aber auch ein Zyklus $(\zeta(0), .., \nu_1, ..\zeta(\lambda_\zeta)$, der nur in G_1 liegt. $\lightning$

□

Korollar 1 *Sei* $G = (V, E)$ *ein azyklischer und verbundener Graph. Dann ist* $G' = (V \cup p, E \cup \{(p, v), (v, p)\})$ *für ein* $v \in V$ *ebenfalls ein azyklischer und verbundener Graph, da* G' *die Verbindung von* G *und einem trivial azyklischen und verbundenen ungerichteten Graphen* $G_p = (\{p\}, \emptyset)$ *über die Kante* (p, v) *ist.*

2.3 Das Korrektheistskriterium von Danos und Regnier

Definition 13 *Für eine Beweisstruktur* $\Theta = (F, L)$ *mit* $L_{\wp} = \{(\wp, P, C) \in L\}$ *ist ein Switching* s *definiert als eine Funktion*

$$s\colon L_{\wp} \to V$$

für die gilt, daß für alle $l \in L_{\wp}$ *mit* $l = (\wp, P, C)$ $s(l) \in P$*.*

Ein Switching dient also dazu, für Par-Links eine der Prämissen auszuwählen; für ein Beweisnetz mit n verschiedenen Par-Links existieren offensichtlich 2^n verschiedene Switchings.

Definition 14 *Der aus einem Beweisnetz $\Theta = (F, L)$ durch ein Switching s induzierte Graph ist ein ungerichteter Graph $G_s = (F, E_s)$, so daß Kanten $\{(\varphi_1, \varphi_2), (\varphi_2, \varphi_1)\} \subseteq E_s$ sind, genau dann wenn ein Link $l = (o, P, C) \in L$ existiert, für den einer der folgenden Fälle eintritt:*

(i) $o = ax$ *und* $\varphi_1, \varphi_2 \in C$

(ii) $o = cut$ *und* $\varphi_1, \varphi_2 \in P$

(iii) $o = \otimes$ *und* $\varphi_1 \in P$ *sowie* $\varphi_2 \in C$

(iv) $o = ⅋$ *und* $\varphi_1 \in C$ *sowie* $s(l) = \varphi_2$

Lemma 2 *Wenn $\Theta' \subseteq \Theta$ für zwei Beweisstrukturen Θ, Θ', dann gilt für die durch Switchings s über Θ induzierten Graphen $G_s = (F, E_s)$ (aus Θ) und $G'_s = (F', E'_s)$ (aus Θ'), daß $F' \subseteq F$ und $E'_s \subseteq E_s$, also daß G'_s Teilgraphen von G_s sind.*

Beweis: $F' \subseteq F$ gilt gemäß Definition; da die Induzierung von Graphen bei konstantem s offensichtlich monoton über der sie induzierenden Link-Menge ist, gilt $E'_s \subseteq E_s$.

Satz 2 *(Danos, Regnier in [DR89]): Eine Beweisstruktur ist ein Beweisnetz genau dann, wenn alle aus ihm durch Switchings induzierte Graphen azyklisch und verbunden sind. Dies bezeichnen wir als das Danos-Regnier-Korrektheitskriterium.*

Beweis: "$\Rightarrow$": Sei $\Theta = (F, L)$ das betreffende Beweisnetz. Dann existiert gemäß Definition 4 ein Beweis π, dessen Desequentialisierung Θ ist. Wir beweisen die Korrektheit der Aussage für ein festes, aber beliebiges Switching s über Θ durch Induktion über die Struktur von π, wobei wir die gleichen Fälle behandeln wie in Definition 3.

- **[IV]** $\dfrac{}{\vdash A, A^\perp}$ (identity): Sei $(ax, \emptyset, \{A, A^\perp\}) \in L$ der entsprechende Link in L. Dann beinhaltet der induzierte Graph G' offensichtlich genau eine Kante, die die beiden einzigen Knoten verbindet und ist trivialerweise azyklisch und verbunden.
- $\dfrac{\vdash \Gamma, A, B}{\vdash \Gamma, A ⅋ B}$ (par): Sei $\Theta = (F, L)$ ein Beweisnetz mit den terminalen Formeln Γ, A, B (wobei A, B einzelne Formeln sind und Γ eine Multimenge von Formeln ist). Gemäss Induktionsannahme ist der induzierte Graph G_s azyklisch und verbunden. Wir bilden nun $\Theta' = (F', L')$ durch Hinzufügen der notwendigen Formel und des Links, mit dem durch s aus ihm induzierten Graphen $G'_s = (V', E')$. Sei nun $l = (⅋, \{A, B\}, \{A ⅋ B\}) \in L'$ der Link, der die Differenz zwischen L und L' bildet; damit ist G_s der Graph G'_s erweitert um l und die Kante $(l, s(l))$, die l mit G'_s verbindet, dann ist G'_s offensichtlich wieder azyklisch und verbunden.
- $\dfrac{\vdash \Gamma, A \quad \vdash B, \Delta}{\vdash \Gamma, A \otimes B, \Delta}$ (times): $\Theta_1 = (F_1, L_1)$, $\Theta_2 = (F_2, L_2)$ seien wie in der Konstruktionsvorschrift gegeben. Bezeichnen wir $G_{1,s}$ und $G_{2,s}$ als die induzierten Graphen, für sie gilt die Induktionsannahme. $G_{s,i+1}$ konstruieren wir nun durch Verbindung der beiden durch den neuen Knoten $l = A \otimes B$ und für $\nu_x \in F_{\Theta_x}, x \in \{1, 2\}$ jeweils Kanten (ν_x, l); mit beiden Kanten verbinden wir azyklische und verbundene Graphen miteinander.

- $\dfrac{\vdash \Gamma, A \quad \vdash A^{\perp}, \Delta}{}$ (cut): Gemäß Induktionsannahme sind die Beweisstrukturen Θ_1 und Θ_2, die wir verbinden wollen, Beweisnetze; da wir im Falle eines Links nur eine Kante einführen, verbinden wir wieder nur zwei azyklisch verbundene Graphen.

Um die Rückrichtung zu zeigen, benötigen wir nun jedoch noch ein paar Werkzeuge:

2.3.1 Imperien

Definition 15 *In einer das Danos-Regnier-Korrektheitskriterum erfüllenden Beweisstruktur $\Theta = (F, L)$ ist das Reich oder Imperium einer Prämisse A eines Links $(\otimes, \{A, B\}, A \otimes B)$, geschrieben eA , definiert als die Menge aller Formeln C, für die eine der folgenden Bedingungen gilt:*

(i) $C = A$

(ii) $\exists\ l \in L.l = (⅋, \{C, D\}, \{H\})$ *für ein* $H \in eA$

(iii) $\exists\ l \in L.l = (⅋, \{H_1, H_2\}, \{C\})$ *für* $H_1, H_2 \in eA$

(iv) $\exists\ l \in L.l = (\otimes, \{C, D\}, \{H\})$ *für ein* $H \in eA$

(v) $\exists\ l \in L.l = (\otimes, \{H_1, H_2\}, \{C\})$ *für* $H_1 \in eA$, *es sei denn,* $H_1 = A$

(vi) $\exists\ l \in L.l = (cut, \{C, H\}, \emptyset)$ *für ein* $H \in eA$, *es sei denn,* $H = A$

Definition 16 *Die Grenze eines Reiches eA sind alle Links $l = (c, \mathcal{P}, \mathcal{C})$, für die die Formel $\exists B, C \in (\mathcal{P} \cup \mathcal{C}).B \in eB \wedge C \notin eC$ gilt.*

Gemäss der Definition von Reichen beinhalten diese Links immer den Times-Link, dessen Prämisse die betrachtete Formel war, und ansonsten nur Par-Links.

Lemma 3 *Sei $\phi \in eA$ Element eines Reiches. Dann gilt für alle Switchings s, daß in dem von ihnen induzierten Graphen ein Pfad ρ von A nach ϕ existiert und alle von ρ berührten Punkte Elemente von eA sind, sofern ρ minimal ist.*

Beweis des Lemmas: Über strukturelle Induktion (bei Wahl eines festen, aber beliebigen Switchings s). Dabei berücksichtigen wir für Par-Links $l = (⅋, \{C, D\}, \{C⅋D\})$ und Wegstrecken $(C⅋D, C)$, daß im Falle der Wahl von $s(l) = D$ für das besagte Switching ein in eA liegender Pfad ρ von $C⅋D$ nach C führen muß; würde er eA verlassen, so gäbe es dafür nur zwei Möglichkeiten:

(i) Sei $B \neq A$ Prämisse des gleichen Links wie A, dann wäre ein Pfad über B möglich. In diesem Fall könnten wir mit einem Switching

$$s'(m) = \begin{cases} C & \iff m = l \\ s(m) & sonst \end{cases}$$

jedoch im durch s' induzierten Graphen einen Zyklus über B und C bilden. ↯

(ii) Es existiert eine Kante $(E, E⅋F)$ in ρ, wobei $E \in eA$, $E⅋F \notin eA$. Erneut konstruieren wir ein Switching

$$s'(m) = \begin{cases} F & \iff s(m) = E \\ s(m) & sonst \end{cases}$$

Da jedoch C auch im Fall des durch s' induzierten Graphen mit A verbunden sein muß (ohne B zu berühren, analog zum vorherigen Punkt), können wir über die Anzahl der F von eA trennenden Par-Links induzieren und dadurch mittels einer Konstruktion von Zyklen den Widerspruch zeigen. ↯

$\square$

Lemma 4 *In einer das Danos-Regnier-Korrektheitskriterium erfüllenden Beweisstruktur* $\Theta = (F, L)$ *gilt für die Prämissen* A, B *eines terminalen Times- oder Cut-Links* $(c, \{A, B\}, \mathcal{C})$, *mit* $c \in \{\otimes, cut\}$, *daß* $eA \cap eB = \emptyset$.

Beweis des Lemmas: Sei $C \in eA \cap eB$. Dann gilt für alle Switchings, daß in den durch sie induzierten Graphen ein Pfad von A nach C existiert, der nicht B berührt, und analog ein solcher für B, der nicht A berührt; somit existiert in den induzierten Graphen ein Zyklus über A und B. ↯

$\square$

Dieses Ergebnis versichert uns, daß wir im Falle einer Komplettabdeckung aller Formeln durch die Vereinigung der Reiche der Prämissen eines terminalen Cut- oder Times-Links eine Aufspaltung in zwei Teilstrukturen (plus, für Times-Links, deren Konklusion) erreichen. Um zu zeigen, daß wir auch einen Link finden können, der diese Aufteilung erzwingt, benötigen wir allerdings noch zwei Definitionen und ein Lemma:

Definition 17 *Ein principial switching für das Imperium* eA *aus einem Link* $(c, \{A, B\}, \mathcal{C})$ *ist ein Switching* s_{eA}, *für das gilt, daß alle Formeln* C, *für die ein Pfad von* A *nach* C *existiert, entweder in* eA *liegen oder* B *oder ein Element aus* $\mathcal{C}$ *berühren.*

Ein solches Switching existiert für alle Imperien; es wird gebildet, in dem in allen Grenzformeln $l = (⅋, \{B, C\}, \{B ⅋ C\})$ mit $B \in eA$ und $C \notin eA$ $s_{eA}(l) = C$ gewählt wird. Par-Links, deren Prämissen beide in eA liegen, sind gemäß Lemma 3 nicht beeinträchtigt.

Definition 18 A *ist eine geerbte Prämisse eines Links* l *gdw eine der folgenden Bedingungen gilt:*

(i) A *ist Prämisse von* l

(ii) Es existiert ein Link l', *dessen Konklusion Prämisse von* l *und für den* A *eine geerbte Prämisse ist.*

Lemma 5 *In einer das Danos-Regnier-Kriterium erfüllenden Beweisstruktur* $\Theta = (F, L)$, *deren terminale Links nur Times- und Cut-Links sind, läßt sich zu jedem terminalen Link* $l = (c, \{A, B\}, \mathcal{C})$, *für den* $F \setminus (eA \cup eB) = \mathcal{C}$ *nicht gilt, ein terminaler Link* $l' = (c', \{C, D\}, \mathcal{C}')$ *finden, für den gilt, daß* $eA \cup eB \subset e\phi$, *wobei* $\phi \in \{C, D\}$.

Beweis des Lemmas Wir zeigen, daß $\{A, B\} \subseteq eC$ für ein o.B.d.A. gewähltes C aus den Prämissen von l', somit gilt die Folgerung gemäß Konstruktionsvorschrift für Imperien.

Sei $l_b = (⅋, \{F, G\}, \{F ⅋ G\})$ ein Link aus der Grenze von eA (l_b muß existieren, solange $eA \cup eB$ nicht maximal ist). Dann ist $F ⅋ G$ geerbte Prämisse eines terminalen Cut- oder Times-Links, den wir als l' wählen. F und G sind damit in eC für eine Prämisse C von l'. Wir wählen nun ein principial switching s_{eC} von eC, in dem o.B.d.A. gelte, daß $s_{eC}(l_b) = F$, wobei $F \in eA$ gilt, und betrachten den induzierten Graphen. In diesem muß gelten, daß ein Pfad von F nach A existiert– da aber auch trivialerweise ein Pfad von C nach $F ⅋ G$ existiert, gilt $A, B \in eC$, also $eA, eB \subset eC$.

$\square$

Lemma 6 *Für eine beliebige, das Danos-Regnier-Kriterum erfüllende Beweisstruktur $\Theta = (F, L)$, deren terminale Links frei von $⅋$-Links sind und die nicht nur eine triviale, aus Axiom-Links bestehende Struktur ist, existiert ein Link $(\otimes, \{A, B\}, \mathcal{C})$ oder $(cut, \{A, B\}, \mathcal{C})$, für den gilt, daß durch Entfernen des Links (und ggf. der Konklusion des Links) das Beweisnetz in zwei das genannte Kriterum erfüllende Beweisstrukturen zerfällt.*

Beweis des Lemmas Da wir Nichttrivialität und Par-Link-Freiheit fordern, muß im Netz zumindest ein terminaler Cut- oder Times-Link existieren. Unter den möglichen terminalen Links wählen wir einen und nennen in l. Um sicherzustellen, daß nach Entfernung des Links die aus der resultierenden Struktur induzierten Graphen noch verbunden sind, fordern wir, daß $F \setminus (eA \cup eB) = \mathcal{C}$.
Falls l diese Eigenschaften nicht erfüllt, muß gemäss Definition der Reiche gelten, daß mindestens eines von ihnen eine Grenze hat, die nicht nur aus l besteht, sondern auch noch aus (mindstens) einem Par-Link l'. Dieser darf jedoch nicht terminal sein, gemäß Voraussetzung. Wir können dann jedoch einen terminalen Link $l_t = (c, \{C, D\}, \mathcal{C})$ mit $c \in (\otimes, cut)$ finden, für den gilt, daß $(eA \cup eB) \subset eC$ (gemäss Lemma 5); durch diesen streng monotonen und beschränkten Prozess erhalten wir schliesslich eine Komplettabdeckung, sofern das Danos-Regnier-Kriterium erfüllt ist.

$\square$

Fortsetzung des Beweises zu Satz 2: "$\Leftarrow$": Wir induzieren nun über die Anzahl der Links in Beweisnetzen. Dieser Beweis liefert uns ein *Sequentialisierungsverfahren*, um aus einem Beweisnetz einen Beweis im Sequenzenkalkül von **MLL** zu destillieren.

(i) **[IV]** Sei nur ein Link gegeben, dann muß dies ein Axiom-Link der Form $(ax, \emptyset, \{(A, i), (A^{\perp}, j)\})$ sein, da alle anderen Links eine nichtleere Prämissenmenge haben und die Formeln dieser Menge Konklusionen eines anderen Links sein müssten. Wir schreiben im Falle einer Identity-Regel $\overline{\vdash A, A^{\perp}}$.

(ii) Sei mehr als ein Link gegeben. Dann muß einer der terminalen Links ein Par-Link, Times-Link oder Cut-Link sein, da ansonsten alle induzierten Graphen nicht verbunden wären. In diesen Fällen wählen wir jeweils einen dieser Links l und eventuell (im Falle eines Par- bzw. Times-Links) die terminale Formel ϕ, die seine Konklusion ist, aus, und zeigen, daß das bzw. die Beweisnetze, die wir durch Entfernung von l (und ggf. ϕ) erhalten, ebenfalls korrekte Beweisnetze sind und wir einen Beweisschritt im Sequenzenkalkül notieren können, der uns bei einer Desequentialisierung den entfernten Link wieder rekonstruiert.

- Par-Link $(⅋, \{A, B\}, \{A ⅋ B\})$: Gemäß Induktionsannahme sind A und B terminale Vorkommen von Formeln eines korrekten Beweisnetzes Θ'. Die Formeln der verbleibenden terminalen Formelvorkommen fassen wir in einer Multimenge Γ zusammen, nun können wir notieren:

$$\dfrac{\begin{array}{c}\Theta' \\ \vdots \\ \vdash \Gamma, A, B\end{array}}{\vdash \Gamma, A ⅋ B}\ (par)$$

- Times-Link ($\otimes\{A,B\},\{A,\parr B\}$): In diesem Fall scheint es naheliegend, das Beweisnetz in zwei Netze aufzuspalten, die dann eine geringere Anzahl von Links hätten:

$$\dfrac{\dfrac{\Theta_1}{\vdots}\quad\dfrac{\Theta_2}{\vdots}}{}\qquad \dfrac{\vdash\Gamma, A \quad \vdash B, \Delta}{\vdash\Gamma, A\otimes B, \Delta}\;(times)$$

  Allerdings existieren Beweisnetze mit terminalen Times-Links, deren Entfernung das Netz nicht in zwei Netze spaltet; gemäß Lemma 6 gilt jedoch, daß wir immer einen Times- oder Cut-Link finden können, an dem wir das Netz spalten können, sofern nicht ein (vorher offensichtlich noch entfernbarer) Par-Link als terminaler Link im Netz auftritt.

- Cut-Link ($cut\{(A,i),(A^{\perp},j)\},\emptyset\}$): Analog zum Times-Link; wir notieren hierbei natürlich entsprechend

$$\begin{array}{cc} \Theta_1 & \Theta_2 \\ \vdots & \vdots \end{array}$$
$$\dfrac{\vdash\Gamma, A \quad \vdash A^{\perp}, \Delta}{\vdash\Gamma, \Delta}\;(cut)$$

□

3 Boxen

In [Gir87] führt Girard eine einfache Methode ein, um, in Emulation des Sequenzenkalküls, beliebige andere Regeln in Beweisnetze einbinden zu können. Für unser Modell von Beweisnetzen scheint die folgende Definition passend:

Definition 19 *Eine Box ist zwei Mengen von Vorkommen von Formeln* $\mathcal{B} = (\phi_1, i_1), .., (\phi_n, i_n)$ *und* $\mathcal{P} = (\varphi_1, j_1), .., (\varphi_m, j_m)$*, wobei* $i_1, .., i_n, j_1, ..j_m$ *paarweise ungleich sind, zusammen mit einem Link* $\mathcal{A} = (box, \mathcal{P}, \mathcal{B})$*, für die gilt, daß* $\vdash\phi_1, ..., \phi_n$ *im linearen Sequenzenkalkül herleitbar ist (insbesondere ist auch* $\mathcal{P} = \emptyset$ *erlaubt).*

Die vorhergehenden Definitionen müssen dazu entsprechend angepasst werden; Boxen werden dabei im Wesentlichen wie Axiom-Links behandelt.

Boxen können nach Prof. Girards Vorstellung Beweisnetze, und somit auch andere Boxen, beinhalten[2]; nach aussen hin verhalten sie sich jedoch atomar. Dies erlaubt nun zwar, die komplette lineare Logik in Beweisnetzen darzustellen, aber ein reeller Vorteil entsteht dadurch nicht [3].

Literatur

[DR89] Danos, Vincent und Laurent Regnier: *The Structures of Multiplicatives.* Archive for Mathematical Logic, 28:181–203, 1989.

[2] Dies ist in unserer Definition durch $\mathcal{P}$ explizitiert

[3] In [Gir96] erläutert er dies näher: "Traditional sequent calculus is therefore a system of proofnets in which the only links are boxes, and all the improvement made in 9 years consists in progressively restricting the use of boxes[...]".

[Gir87] Girard, Jean-Yves: *Linear logic.* Theoretical Computer Science, 50:1–102, 1987.

[Gir96] Girard, Jean-Yves: *Proof-nets: The parallel syntax for proof-theory.* Logic and Algebra, 1996.