Grundlagen der Informatik

1. Semester, 1996

1.3. Beweise automatisieren

1.3.1. Aussagenlogische Formeln normieren, Beweise automatisieren

1.3.2. Prädikatenlogische Formeln normieren

1.3.3. Beweise normieren

Entscheidungsverfahren (1)

Beispiel:

Vor Ihnen stehen fünf Häuser verschiedener Farbe. Die Bewohner sind verschiedener Nationalität, halten verschiedene Tiere, bevorzugen verschiedene Getränke und haben verschiedene Rauchgewohnheiten:

- Dem Engländer gehört das rote Haus.
- Dem Spanier gehört der Hund.
- Im grünen Haus trinkt man Kaffee.
- Der Ukrainer trinkt Tee.
- Das grüne Haus steht unmittelbar rechts neben dem weißen Haus.
- Der Zigarettenraucher hält Schnecken.
- Der Zigarrenraucher wohnt im gelben Haus.
- Der Bewohner des mittleren Hauses trinkt Milch.
- Der Norweger bewohnt das erste Haus links.
- Der Pfeifenraucher lebt in dem Haus neben dem Mann mit dem Fuchs.
- Der Zigarrenraucher bewohnt das Haus neben dem Mann mit dem Pferd.
- Der Stumpenraucher trinkt Limonade.
- Der Japaner raucht Zigarillos.
- Der Norweger wohnt neben dem blauen Haus.

Wer trinkt Wasser? Wem gehört das Zebra?

Problem: finde eine Belegung, die die Formeln wahr macht, oder gebe "unerfüllbar" aus, falls es keine erfüllende Belegung gibt.

Lösungen:
- Ausprobieren
- Entscheidungsverfahren für die Erfüllbarkeit

Entscheidungsverfahren (2)

Definition 1.23

- Ein Entscheidungsverfahren für Erfüllbarkeit ist ein Algorithmus, der bei Eingabe einer endlichen Formelmenge X mit "ja" terminiert, falls X erfüllbar ist, und sonst mit "nein", und im Fall der Erfüllbarkeit eine Belegung ausgibt, unter der X wahr ist.
- Entscheidungsverfahren für Allgemeingültigkeit und für logische Folgerung sind entsprechend.
- Eine Eigenschaft, für die es ein Entscheidungsverfahren gibt, heißt entscheidbar. (z.B. Erfüllbarkeit)

Satz 1.15

Erfüllbarkeit, Allgemeingültigkeit und logische Folgerung sind für endliche Formelmengen entscheidbar: Die Methode der Wahrheitstafeln liefert Entscheidungsverfahren für Erfüllbarkeit, Allgemeingültigkeit und logische Folgerung.

Normalformen (1)

Beispiel:

- konjunktive Normalform: $(P \vee \neg R \vee S) \wedge (Q \vee R \vee S) \wedge (\neg P \vee Q \vee \neg S)$
- disjunktive Normalform: $(P \wedge \neg R \wedge S) \vee (Q \wedge R \wedge S) \vee (\neg P \wedge Q \wedge \neg S)$

Definition 1.24

- Ein Literal ist ein Atom oder seine Negation, d.h. von der Form P oder ¬P;
- ein Literal heißt positiv oder negativ, je nachdem ob es negiert ist oder nicht;
- eine Formel ist in konjunktiver Normalform, wenn sie entweder W oder F oder eine Konjunktion von Disjunktionen von Literalen ist, d.h. die Form hat:

  $(A_{1,1} \vee \ldots \vee A_{1,m_1}) \wedge (A_{2,1} \vee \ldots \vee A_{2,m_2}) \wedge \ldots \wedge (A_{n,1} \vee \ldots \vee A_{n,m_n})$

  wobei $n, m_1, \ldots, m_n \quad 1$ und die $A_{i,j}$ positive oder negative Literale sind und in keiner Disjunktion ein Atom mehrfach vorkommt.
- dual dazu ist die disjunktive Normalform, d.h. sie hat die Form:

  $(A_{1,1} \wedge \ldots \wedge A_{1,m_1}) \vee (A_{2,1} \wedge \ldots \wedge A_{2,m_2}) \vee \ldots \vee (A_{n,1} \wedge \ldots \wedge A_{n,m_n})$

Normalformen (2)

Satz 1.16

Jede Formel kann in eine äquivalente Formel in konjunktiver Normalform überführt werden, indem die folgenden Umformungsregeln sukzessive auf Teilformeln angewendt werden:

$(A \leftrightarrow B) \rightsquigarrow (A \rightarrow B) \wedge (B \rightarrow A)$	Bikonditionale und Konditionale entfernen
$(A \rightarrow B) \rightsquigarrow \neg A \vee B$	
$\neg\neg A \rightsquigarrow A$	doppelte Negation entfernen und
$\neg (A \wedge B) \rightsquigarrow \neg A \vee \neg B$, $\neg (A \vee B) \rightsquigarrow \neg A \wedge \neg B$	Negation nach innen und
$\neg W \rightsquigarrow F$, $\neg F \rightsquigarrow W$, $A \wedge W \rightsquigarrow A$,	Wahrheitswerte entfernen
$A \wedge F \rightsquigarrow F$, $A \vee W \rightsquigarrow W$, $A \vee F \rightsquigarrow A$	
$A \vee (B \wedge C) \rightsquigarrow (A \vee B) \wedge (A \vee C)$	Disjunktionen nach innen bringen und
$A \vee A \rightsquigarrow A$, $A \wedge A \rightsquigarrow A$	doppelte Disjunktion u. Konjunktion und
$A \vee \neg A \rightsquigarrow W$, $A \wedge \neg A \rightsquigarrow F$	Trivialitäten und Widersprüche entfernen

Normalformen (3)

Aufgabe: Formen Sie die Formel nach dem Verfahren aus Satz 1.16 in konjunktive Normalform um:

$(Q \wedge (Q \vee R \rightarrow S) \wedge (\neg P \vee Q \rightarrow R) \wedge (\neg(S \wedge P)))$

Entscheidungsverf. mit Normalformen

Satz 1.17

Eine Formel in konjunktiver Normalform ist allgemeingültig genau dann wenn sie die Form W hat.

neues Entscheidungsverfahren für die Allgemeingültigkeit einer Formel A

- bringe A nach Satz 1.16 in konjunktive Normalform
- Ist A nicht allgemeingültig, so liefert der Beweis des Satzes eine Belegung, unter der A falsch ist.

das Entscheidungsverfahren läßt sich auch für die Erfüllbarkeit und logische Folgerung verwenden

Problem: Berechnung der konjunktiven Normalform kann sehr aufwendig sein.

Entscheidungsverf. mit Normalformen

Aufgabe:

Bilden Sie aus den Aussagen des Inspektor-Craig-Beispiels eine konjunktive Normalform und zeigen Sie daß B schuldig ist.

Klauseln, Gentzen- & Hornformeln (1)

Definition 1.25

Eine Klausel ist eine endliche Menge von Literalen; sie repräsentiert eine Disjunktion:

$\{L_1,\ldots,L_n\}$ steht für $L_1 \vee \ldots \vee L_n$; wir benutzen beide Schreibweisen gleichwertig

Die leere Klausel {} steht für die leere Disjunktion, die immer falsch ist.

- nach Satz 1.16 ist jede Formel äquivalent zu einer endlichen Menge von Klauseln;
- in der Klausellogik arbeitet man deshalb mit endlichen Mengen von Klausel statt mit Formeln;
- allgemeingültige Formeln werden nicht durch W, sondern durch $A \vee P \vee \neg P$ und widersprüchliche durch die leere Klausel dargestellt;

Klauseln, Gentzen- & Hornformeln (2)

- Klauseln sind für die Darstellung von Formeln im Rechner gut geeignet

  z.B. ¬In(Affe),¬In(Kiste),¬In(Banane),¬Schieben(Affe,Kiste,Banane), Nah(Banane,Boden), Unter(Kiste,Banane)

- für uns sind Folgerungen (Konditionale) besser zu verstehen als Alternativen (Klausel)

  In(Affe) $\wedge$ In(Kiste) $\wedge$ In(Banane) $\wedge$ Schieben(Affe,Kiste,Banane) $\rightarrow$ Nah(Banane,Boden) $\vee$ Unter(Kiste,Banane)

- Klauseln sind nach Kaptiel 1.2.1 **äquivalent** zu Folgerungen:

  - {¬P1,…,¬Pn,Q1,…Qm} entspricht ¬P1 $\vee$…$\vee$ ¬Pn $\vee$ Q1 $\vee$…$\vee$ Qm

  - ist äquivalent zu: ¬ (P1 $\wedge$ … $\wedge$ Pn) $\vee$ Q1 $\vee$…$\vee$ Qm

  - ist äquivalent zu: P1 $\wedge$ … $\wedge$ Pn $\rightarrow$ Q1 $\vee$…$\vee$ Qm

Klauseln, Gentzen- & Hornformeln (3)

Definition 1.26

- eine Gentzenformel ist von der Form

  $P1 \wedge \ldots \wedge Pn \rightarrow Q1 \vee \ldots \vee Qm$ wobei n, m 0 und die Pi und Qj Atome. Die Atome in $P1 \wedge \ldots \wedge Pn$ und $Q1 \vee \ldots \vee Qm$ sind jeweils verschieden;
- eine leere Konjunktion schreiben wir als W, eine leere Disjunktion als F, d.h.

$W \rightarrow Q1 \vee \ldots \vee Qm$	oder $Q1 \vee \ldots \vee Qm$	positive Formel
$P1 \wedge \ldots \wedge Pn \rightarrow F$	oder $P1 \wedge \ldots \wedge Pn$	negative Formel
$W \rightarrow F$	oder F	Widerspruch

- eine Hornformel ist eine Gentzenformel mit höchstens einem Atom auf der rechten Seite des Konditionals:

  $P1 \wedge \ldots \wedge Pn \rightarrow Q$ wobei n 0 und die Pi und Q Atome.

  Speziell

$W \rightarrow Q$	oder Q	Faktum
$P1 \wedge \ldots \wedge Pn \rightarrow F$	oder $P1 \wedge \ldots \wedge Pn$	negative Formel
$W \rightarrow F$	oder F	Widerspruch

- eine Gentzenformel, für die Pi=Qj für ein Atom gilt, heißt tautologisch

Klauseln, Gentzen- & Hornformeln (4)

Aufgabe: Formen Sie die folgenden Formeln in (Mengen von) Gentzenformeln um

- $P \wedge \neg Q \rightarrow R \vee \neg S$

- $P \vee \neg Q \rightarrow R$

- $(P \rightarrow Q) \vee (R \rightarrow S)$

- $P \rightarrow Q \wedge R$

- $\neg (P \rightarrow Q)$

Grundlagen der Informatik

1. Semester, 1996

1.3. Beweise automatisieren

1.3.1. Aussagenlogische Formeln normieren, Beweise automatisieren

1.3.2. Prädikatenlogische Formeln normieren

1.3.3. Beweise normieren

1.3.4. Theorembeweiser

Normalformen

- jede prädikatenlogische Formel kann in konjunktive, disjunktive oder Gentzen-Normalform gebracht werden

- zwei Formeln A und B heißen stark äquivalent, wenn $A \leftrightarrow B$ allgemeingültig ist

  Beispiel:

  - $(P(w) \rightarrow P(z)) \leftrightarrow \neg P(w) \vee P(z)$ ist allgemeingültig, d.h. $P(w) \rightarrow P(z)$ und $\neg P(w) \vee P(z)$ sind stark äquivalent
  - $P(x)$ und $P(y)$ sind äquivalent, aber $P(x) \leftrightarrow P(y)$ nicht allgemeingültig

- Ersetzen wir in der Formel A die Teilformel B durch eine stark äquivalente Formel C, so ist die entsprechende Formel D stark äquivalent zur Ausgagnsformel A

  Beispiel:

  - Gegeben seien $(P(w) \rightarrow P(z)) \vee P(y)$ und $(P(w) \rightarrow P(z)) \leftrightarrow \neg P(w) \vee P(z)$. Damit ist $\neg P(w) \vee P(z) \vee P(y)$ stark äquivalent zu $(P(w) \rightarrow P(z)) \vee P(y)$.
  - Da $P(z) \leftrightarrow P(y)$ nicht allgemeingültig, ist $\neg P(w) \vee P(y) \vee P(y)$ nicht stark äquivalent zu $\neg P(w) \vee P(z) \vee P(y)$.

Umbennen und Einsetzen (1)

Definition 1.27

Variablen in einer Form umbennen heißt, Variable für Variablen so einzusetzen, daß verschiedene Variablen verschieden bleiben. Eine solche Substitution heißt Umbenennung.

Beispiel: Umbenennung von R(x,y,x) kann zu R(u,v,u), R(x,v,x), R(v,x,v),… führen, aber nicht zu R(x,x,x), R(u,v,v)

- Formeln, die durch Umbennung auseinander entstehen sind äquivalent
- Formeln sind gleich bis auf Umbenennung
- durch Umbenennung kann erreicht werden, daß zwei Formeln oder Formelmengen keine gleichen Variablen haben

Umbennen und Einsetzen (2)

Satz 1.18

Entsteht die Formel B aus Formel A durch Einsetzen, so folgt B aus A.

Aufgabe: Sind die folgenden Formeln widersprüchlich?

$P(x) \rightarrow Q(x)$, $Q(y) \rightarrow R(x,y)$, $\neg R(x,y)$, $Q(y) \vee R(x,y) \rightarrow P(z)$, $P(x) \vee Q(x)$,

$\neg (P(y) \wedge Q(y))$, $P(x) \rightarrow Q(x)$, $Q(z) \rightarrow P(z)$

Pränexe Normalform (1)

Ziel: alle Quantoren sollen in einer Formel vorne stehen

Definition 1.28

Eine Formel ist in pränexer Normalform, wenn kein Quantor im Bereich einer aussagenlog. Verknüpfung steht, d.h. wenn sie von der Form Q1x1… Qnxn A ist, wobei Q1…Qn All- oder Existenzquantoren sind, n>=0, und A quantorenfrei ist.

Beispiel: $\exists x \, \forall y \, (Q(x) \vee R(y))$

Pränexe Normalform (2)

Satz 1.19

Mit folgenden Umformungstregeln, sukzessive auf Teilformeln angewendet, können wir jede Formel in eine stark äquivalente Teilformel überführen:

$\forall x\ A \rightsquigarrow \forall y\ A\{x/y\}$, $\exists x\ A \rightsquigarrow \exists y\ A\{x/y\}$	Quantoren umbenennen
$\forall x\ A \wedge \forall x\ B \rightsquigarrow \forall x(A \wedge B)$, $\exists x\ A \vee \exists x\ B \rightsquigarrow \exists x\ (A \vee B)$	Quantoren zusammenfassen
$Qx\ A \wedge B \rightsquigarrow Qx\ (A \wedge B)$, $Qx\ A \vee B \rightsquigarrow Qx\ (A \vee B)$	falls x nicht frei in B und
$B \wedge Qx\ A \rightsquigarrow Qx\ (B \wedge A)$, $B \vee Qx\ A \rightsquigarrow Qx\ (B \vee A)$	Q ein Quantor
	Konjunktionen und Disjunktionen nach innen
$\neg\forall x\ A \rightsquigarrow \exists x\neg\ A$, $\neg\ \exists xA \rightsquigarrow \forall x\neg\ A$	Negationen nach innen

Dazu kommen die Regeln, mit denen wir zunächst $\leftrightarrow$ und $\rightarrow$ eliminieren

Pränexe Normalform (3)

Aufgabe:

Geben Sie zu folgenden Formeln möglichst kurze pränexe Normalformen an:

$\neg\ \exists x\ P(a,f(x)) \wedge (\forall x\ Q(g(f(x),b)) \vee \exists x\ \forall y\ Q(g(x,y)))$

$\exists x\ \forall y\ (Q(x) \vee R(y)) \leftrightarrow \forall y\ \exists x\ (Q(x) \vee R(y))$

Skolemisierung (1)

- Problem: mache Formeln quantorenfrei

  Beispiele: - $\forall x\ P(x)$ ist äquivalent zu $P(x)$

  - $\exists x\ P(x)$ ist nicht äquivalent zu $P(x)$ oder $P(t)$ für einen beliebigen Term

- Lösung: Einführung von Skolemfunktionen

- Prinzip:
  - ist $\exists x\ A$ eine Formel mit einer freien Variable y, so setzen wir in A für x den Term g(y) ein und erhalten B; wobei das Funktionssymbol g in A nicht vorkommen darf und die richtige Sorte haben muß
  - gilt $\exists x\ A$ in einer Struktur, so können wir g darin so definieren, daß B wahr wird: wir müssen nur für jedes g(y) eins der existierenden x auswählen
  - gilt $\exists x\ A$ nicht, so können wir für mindestens ein y kein x finden, das A wahr macht, also ist B falsch, egal wie wir g definieren
  - also sind $\exists x\ A$ und B erfüllbarkeitsgleich, d.h. sie sind beide erfüllbar oder beide unerfüllbar
  - enthält $\exists x\ A$ mehrere freie Variablen, so hat g sie alle als Argumente
  - eine solche Funktion g wird Skolemfunktion genannt

Skolemisierung (2)

Satz 1.20

Mit folgendem Verfahren können wir jede Formel in eine erfüllbarkeitsgleiche quantorenfreie Formel überführen

- bringe die Formel in pränexe Normalform
- lasse der Reihe nach (von außen nach innen) die Allquantoren weg
- führe für jeden Existenzquantor eine Skolemfunktion ein

Beispiel:

$\forall p \forall q (p°q \rightarrow \exists r$ zwischen(p,q,r))

aus der Euklidischen Geometrie wird umgeformt zu:

$p°q \rightarrow$ zwischen(p,q,**dazwischen**(p,q))

wobei 'dazwischen' eine neue Funktion ist, die zu zwei Punkten einen dazwischen auswählt

Grundlagen der Informatik

1. Semester, 1996

1.3. Beweise automatisieren

1.3.1. Aussagenlogische Formeln normieren, Beweise automatisieren

1.3.2. Prädikatenlogische Formeln normieren

1.3.3. Beweise normieren

1.3.4. Theorembeweiser

Ableiten: Beispiele (1)

Beispiel: Ballwurflogelei:

- Aus $Wa(a) \rightarrow \neg Wa(e) \wedge \neg Wa(f) \wedge \neg Wa(g)$ und $W(a)$ folgt $\neg Wa(e)$ und $\neg Wa(f)$ und $\neg Wa(g)$.
- Aus $\neg Wa(g)$ und $Wa(g) \leftrightarrow \neg Wa(e)$ folgt $Wa(e)$.
- Aus $Wa(a) \vee Wa(e) \vee Wa(f) \vee Wa(g)$ und $\neg Wa(a)$ und $\neg Wa(e)$ und $\neg Wa(f)$ folgt $Wa(g)$.

Ableitungsregeln:

- $P, P \rightarrow \neg Q \wedge \neg R \wedge \neg S \models \neg Q, \neg R, \neg S$
- $\neg S, S \leftrightarrow \neg Q \models Q$
- $P \vee Q \vee R \vee S, \neg P, \neg Q, \neg R \models S$

Ziel: finde allgemeinere Ableitungsregeln

Ableiten: Beispiele (2)

Die Formeln lassen sich mit folgenden 7 Regeln ableiten:

(0) $\frac{A\ ,\ \neg A}{F}$ Widerspruch

(1) $\frac{A\ ,\ A \rightarrow B}{B}$ Modus ponens

(2) $\frac{A \vee B}{\neg A \rightarrow B}$ Umformen

(3) $\frac{A \wedge B}{A}$

(4) $\frac{A \wedge B}{B}$

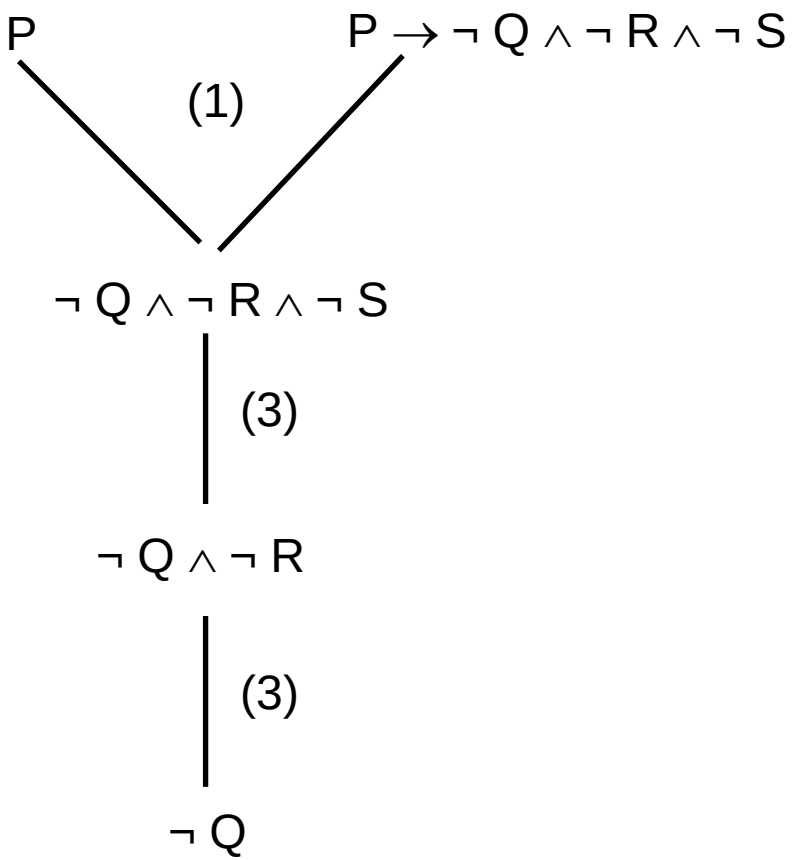
Abschwächen einer Konjunktion

(5) $\frac{A \leftrightarrow B}{A \rightarrow B}$

(6) $\frac{A \leftrightarrow \neg B}{\neg A \rightarrow B}$

Abschwächen eines Bikonditionals

Ableiten: Beispiele (3)



Ableitungsregeln (1)

Definition 1.29

Eine n-stellige Ableitungregel, n 0, hat die Form

$$\frac{A1,\ldots,An}{B}$$

wobei A1,…,An und B Formeln sind.

- eine Regel wird angewendet, indem wir für A1,…,An und B konkrete Formeln einsetzen, z.B. Wa(e), Tä(a), …
- das sukzessive Anwenden von Regeln nennen wir Ableiten
- eine einzelne Regelanwendung wird Ableitungsschritt genannt
- die Anfangsformeln werden Voraussetzungen der Ableitung genannt

Ableitungsregeln (2)

Aufgabe:

Stellen Sie für die Formeln

$\text{Wa(a)}, \text{Wa(a)} \rightarrow \neg\,\text{Wa(e)} \wedge \neg\,\text{Wa(f)} \wedge \neg\,\text{Wa(g)}\ ,\ \text{Wa(g)} \leftrightarrow \neg\,\text{Wa(e)}$

den Ableitungsbaum auf.

Korrektheit von Ableitungsregeln

Definition 1.30

- eine Ableitungsregel

$$\frac{A1,\ldots,An}{B}$$

heißt korrekt, wenn B aus A1,…,An folgt.

- eine Menge von Regeln (auch Regelsystem genannt) heißt korrekt, wenn jede ihrer Regeln korrekt ist.

Beispiel: $\frac{A\ ,\ A \rightarrow B}{B}$ (modus ponens) ist korrekt

Schnittregel (1)

die Schnittregel, angewendet auf Klauseln A, B und Atome P ist die einzige, die man für Klausellogik braucht

Definition 1.31

- Die Schnittregel (für Gentzenformeln)

$$\frac{A \to B \vee P \ , \ P \wedge C \to D}{A \wedge C \to B \vee D}$$

schneiden wir aus zwei Gentzenformeln das Atom P heraus und verschmelzen die Formeln zu einer neuen Gentzenformel; die Konjunktionen A,C und die Disjunktionen B, D dürfen dabei fehlen.

- ein Spezielfall ist die Einerschnittregel:

$$\frac{B \vee L \ , \neg L}{B}$$

- mit der positiven (negativen) Einerschnittregel wird ein Atom aus der Formel entfernt

$$\frac{W \to P \ , \ P \wedge C \to D}{C \to D} \quad \text{(positive E.)} \qquad \frac{A \to B \vee P \ , \ P \to F}{A \to B} \quad \text{(negative E.)}$$

Schnittregel (2)

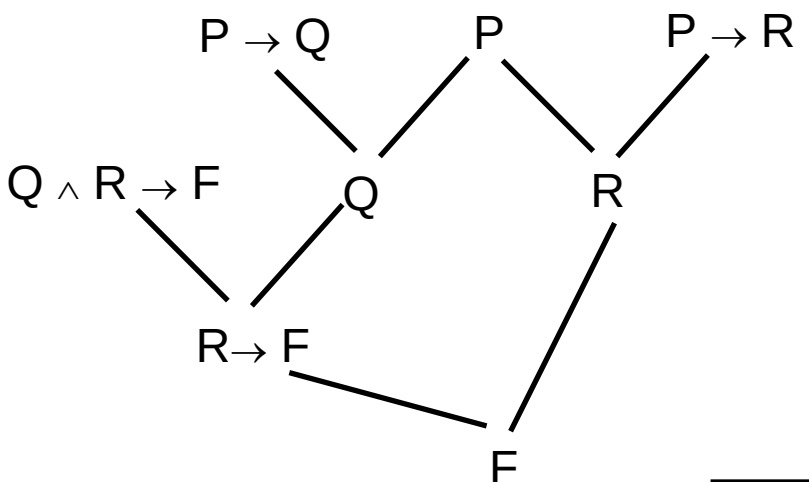
die Schnittregel ist ideal fürs Formalisieren von Widerspruchsbeweisen:

Um die Formel A zu beweisen,

- nehmen wir ¬A an,
- bringen ¬A in Gentzenform
- schneiden mit und zwischen den Voraussetzungen
- falls der Widerspruch, d.h. F auftritt, stop, ansonsten weiterschneiden

Beispiel: Beweise ¬P aus $P \to Q$, $P \to R$ und $\neg(Q \wedge R)$.

1. Schritt: nehme P zu den Voraussetzungen dazu
2. Schnitt: wende Schnittregel an bis Widerspruch



Ableitungsregeln f.d. offene Prädikatenlogik (1)

Definition 1.32

- Mit der Einsetzungs- oder Substitutionsregel können wir in einer Formel für Variablen Terme (keine Datenterme) einsetzen

$$\frac{A}{A\{x1/t1,\ldots,xn/tn\}}$$

wobei A eine Formel, x1,…xn Variablen und t1,…,tn Terme passender Sorten sind

- durch Einsetzen werden verschiedene Formeln unifiziert (vereinheitlicht)
- nach dem Einsetzen (Umbenennen) kann die Schnittregel angewendet werden

Ableitungsregeln f.d. offene Prädikatenlogik (2)

Beispiel: Affe-Banane-Beispiel

aus A1 $\text{Arme}(x) \wedge \text{Nah}(x,y) \rightarrow \text{Reichen}(x,y)$

und A5 $\text{Arme}(\text{Affe})$

kann man

auf A18 $\text{Nah}(\text{Affe},y) \rightarrow \text{Reichen}(\text{Affe},y)$

Aufgabe:

Bringen Sie die Schlüsse im Affe-Banane-Problem aus Kapitel 1.1 in die Form einer Ableitung mit Schnitt- und Einsetzungsregel.

Schwächste Vorbedingung

1. Semester, 1996

Aufgaben

Gesucht ist die schwächste Vorbedingung V zu folgenden Programmen

(1) *var x, y: integer;*

*x := 3 * x + 1;*

if x >= 12 then y:= x else y := -x;

*y := x * y;*

Nachbedingung N: y > 0

(2) *var s, t: integer;*

*s := 5 * t + 3;*

if s > t then t:= s - 8;

Nachbedingung N: -20 <= t <= 20