Logik und Beweisen

Skript

Uwe Petermann
Department of Computer Science
University of Applied Sciences Leipzig
G.-Freytag-Str. 42, Leipzig
uwe@imn.htwk-leipzig.de

6. Februar 2006

1 Einleitung

In vielen Situationen wird das Wort Logik gebraucht. Man spricht von Geschäftslogiken, von der Logik eines Programms, davon, daß ein Argument nicht logisch erscheint, oder daß eine gewünschte Tatsache „logischerweise“ aus den gemachten Annahmen folgt.
Tatsächlich ist die Logik für den Informatiker ein sehr wirksames Werkzeug, wenn es darum geht, das Verhalten von Programmen und Systemen zu beschreiben. Man kann die Rolle der Logik mit der Rolle klassischer mathematischer Disziplinen vergleichen, die es anderen Ingenieurwissenschaften ermöglichen, exakt das Verhalten der in der jeweiligen Disziplin konstruierten Artefakte vorherzusagen.
Leider gibt es einen kleinen Unterschied zuungunsten der Informatiker. Während das für die Nichtinformatikdisziplinen notwendige mathematische Wissen reichhaltig in der Lehre angeboten wird, findet sich für die Logik, zumindest sobald die Aussagenlogik verlassen wird, wenig Platz. Die Aussagenlogik ist aber absolut unzureichend für das Beschreiben und Verstehen des Verhaltens von Programmen. Da die Eigenschaften von Datenstrukturen beschrieben werden müssen, wofür sich algebraische Strukturen anbieten, benötigt man die Prädikatenlogik. Da die zum Einsatz kommenden Strukturen meist durch rekursive Bildungsvorschriften beschrieben werden, muß Induktion als Folgerungsmechanismus benutzt werden. Schließlich verlangt das Beschreiben des Programmverhaltens selbst zumindest algorithmische (oder dynamische) Logik [10, 11, 4, 3, 7]. Denn diese Logiken betrachten nicht nur die Datenstrukturen, sondern beschreiben auch die Bedeutung der Konstrukte von Programmiersprachen.
Vor allem aber muß die Logik so dargeboten werden, daß sie neben der nötigen Ausdrucksstärke ihrer Regeln eine praktikable Notation bietet. Außerdem ist für exaktes Folgern, als Analogon zum exakten Rechnen, eine Computerunterstützung unabdingbar.
Im vorliegenden Skript wird versucht, den Sequenzenkalkül so darzustellen, daß er für Informatiker praktikabel wird. Der Logiker Gerhard Gentzen [2] entwickelte diesen Kalkül, weil die vorher im Stil von David Hilbert [6] entwickelten Kalküle nur sehr wenig das natürliche, logische Folgern widerspiegelten. Genau gesagt entwickelte Gentzen zwei Kalküle. Zunächst den Kalkül des natürlichen Schließens. Dieser modelliert das Folgern eines Menschen tatsächlich auf „natürliche“ Weise. Allerdings ist dieser Kalkül weniger geeignet, auch die Suche nach einer Argumentation zu beschreiben. In der Praxis ist aber der Nachweis der Korrektheit eines Programms oder eine lückenlose Schlußkette, die etwa in der Kriminalistik einen Täter überführt, stets das Ergebnis einer mehr oder weniger langen Suche. Mit einem zweiten, dem sogenannten Sequenzenkalkül, ist es Gentzen gelungen, beide Aspekte, die Präsentation der fertigen Argumentation und die Suche nach ihr, gleich gut widerzuspiegeln.
Ein Sequenzenkalkül ist auch die Grundlage für ein erfolgreiches System zur Spezifikation und Verifikation von Programmen, KIV, der Karlsruhe Interactive Verifier [5, 8, 9]. Es steht für die Lehre als freie Software zur Verfügung und kann nach einer gewissen Einarbeitung auf erschwinglicher Technik betrieben werden.
Im vorliegenden Skript werden zunächst die Bedeutung der aussagenlogischen Verknüpfungszeichen wiederholt sowie Grundbegiffe der Mengenlehre und der Prädikatenlogik aufgefrischt. Danach werden Regeln für die Konstruktion von Nachweisen für die Gültigkeit logischer Ausdrücke aufgestellt und an Beispielen illustriert. In einem geplanten zweiten Teil sollen algebraische Strukturen besprochen werden, darunter solche, die in der Informatik eine sehr wichtige Rolle spielen. Schließlich werden Methoden des Korrekheitsnachweises für Programme besprochen.
Anliegen dieses Skripts ist eine zugängliche Darstellung, mit dem Ziel exaktes logisches Folgern in praktischen Beschäftigung mit Programmen zu unterstützen. Für die theoretische Fundierung der dargestellten prädikatenlogischen Beweismethoden und weitere Einzelheiten wird auf [1] und [12] verwiesen.

2 Zur Aussagenlogik

In der Aussagenlogik wird der Wahrheitswert von Aussagen betrachtet. Dies sind logische Formeln in denen Individuenvariablen nicht vorkommen oder deren Belegung mit Werten nicht betrachtet wird.

Beispiel 2.1 In der Formel $p \wedge q \vee r$ kommen nur die Aussagenvariablen p, q und r vor. Ihnen werden Wahrheitswerte zugeordnet. Die innere Struktur dieser als elementar aufgefaßten Aussagen wird nicht betrachtet.

Beispiel 2.2 In der Formel $(\forall\, x.a(x,y)) \wedge b(y) \vee \exists\, z.c(x,y,z)$ kommen zwar Prädikatssymbole a, b und c und Individuenvariablen x, y und$z$ vor. Jedoch untersucht die Aussagenlogik nicht, wie den Teilformeln $\forall\, x.a(x,y)$, $b(y)$ und $\exists\, z.c(x,y,z)$ Wahrheitswerte in Abhängigkeit von deren Struktur und von der Bedeutung der Prädikatssymbole zuzuordnen sind.

In der einfachsten Form der Aussagenlogik werden zwei Wahrheitswerte „wahr“ und „falsch“ betrachtet. Diese werden oft durch 1 bzw. 0 dargestellt.
Die Bedeutung der aussagenlogischen Verknüpfungszeichen $\neg$, $\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ wird durch folgende Tabellen dargestellt.

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

p	$\neg p$
0	1
1	0

Abbildung 1: Bedeutung der aussagenlogischen Junktoren

Anhand der Tabelle in Abbildung 1 wird ersichtlich, wie die Wahrheitswerte für aussagenlogischen Ausdrücke in Abhängigkeit von den Wahrheitswerten ihrer Teilausdrücke berechnet werden können. Durch Aufstellung von Wahrheitswerttabellen kann die Gültigkeit jedes aussagenlogischen Ausdrucks untersucht werden. Allerdings wächst deren Größe exponentiell in der Anzahl der vorkommenden Aussagenvariablen.
In vielen Fällen wird man kürzere Nachweise für die Gültigkeit angeben können, indem man die Regeln aus der Tabelle in Abbildung 2 in Abschnitt 5.2 benutzt. Diese Regeln werden auch später für die Behandlung der aussagenlogischen Junktoren in prädikatenlogischen Ausdrücken benutzt. Zur Konstruktion der Beweise wird auf die Ausführungen in Abschnitt 5.2 verwiesen.

3 Elemente der Mengenlehre

Notation: Die Aussage „a ist Element der Menge A“ notieren wir als $a \in A$.

Extensionalitätsprinzip: Zwei Mengen A und B sind genau dann gleich, wenn

$$\text{für alle } x \text{ gilt: } x \in A \leftrightarrow x \in B$$

Beispiel 3.1

(1) Die Mengen $\{-2, -1, 0, 1\}$ und $\{-2, 1\}$ sind nicht gleich.

Die erstgenannte Menge enthält ein Element, zum Beispiel das Element 0, welches in der zweitgenannten Menge nicht vorkommt.

(2) Die Mengen $\{a, b, c, a\}$ und $\{b, a, c\}$ sind gleich.

Die Mehrfachnennung des Elements a in der ersten Menge und die veränderte Reihenfolge der Aufzählung der Elemente sind dabei ohne Belang.

Definition von Mengen durch logische Ausdrücke: Die Menge derjenigen Elemente einer Menge B, die einen logischen Ausdruck Φ erfüllen, wird mit

$$\{x \in B \mid \Phi(x)\}$$

bezeichnet.

Die Schreibweise kann zu $\{x \mid \Phi(x)\}$ verkürzt werden, wenn aus dem Kontext klar ist, daß nur von Teilmengen einer gemeinsamen Obermenge gesprochen wird.

Beispiel 3.2

(1) Die Mengen $A = \left\{x \in R \mid x^2 + x - 2 = 0\right\}$
und $B = \left\{y \in R \mid y^2 + y - 2 > 0\right\}$ sind nicht gleich.

(2) Die Mengen $A = \left\{x \in Z \mid x^2 + x - 2 = 0\right\}$
und $B = \left\{y \in R \mid y^2 + y - 2 = 0\right\}$ sind gleich.

Leere Menge: Es gibt eine Menge, sie wird mit $\emptyset$ notiert, welche kein Element enthält. Sie kann durch $\{x \mid x \neq x\}$ beschrieben werden.

Teilmengenrelation: Die Relation $\subseteq$ (Inklusion) wird wie folgt definiert: Für Mengen A und B gilt $A \subseteq B$ genau dann, wenn

$$\text{für alle } x \text{ gilt: } x \in A \rightarrow x \in B$$

Die Relation $\subset$ (strikte Inklusion) wird wie folgt definiert: Für Mengen A und B gilt $A \subset B$ gilt genau dann, wenn

$$\begin{gathered}\text{für alle } x \text{ gilt: } x \in A \rightarrow x \in B \\ \text{und es ein } x \text{ gibt mit: } x \notin A \wedge x \in B\end{gathered}$$

geordnetes Paar: Wenn A und B Mengen sind, dann existiert für deren Elemente x und y die Menge $\{\{x\}, \{x, y\}\}$. Sie wird mit (x, y) notiert und *geordnetes Paar* genannt.

Geordnete Paare (x, y) und (u, v) sind genau dann gleich, wenn $x = u$ und $y = v$ gelten.

Operationen mit Mengen: Wenn A und B Mengen sind, dann heißen die Mengen

$\{x \mid x \in A \wedge x \in B\}$ *Durchschnitt*, Notation $A \cap B$,
$\{x \mid x \in A \vee x \in B\}$ *Vereinigung*, Notation $A \cup B$,
$\{x \mid x \in A \wedge x \notin B\}$ *Differenz*, Notation $A \setminus B$,
$\{x \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$ *symmetrische Differenz*,
$\{B \mid B \subseteq A\}$ *Potenzmenge*, Notation $\mathcal{P}(A)$,
$\{(x, y) \mid x \in A \wedge y \in B\}$ *Kartesisches Produkt*, Notation $A \times B$,

der Mengen A und B.

4 Elemente der Prädikatenlogik

Bereits im vorigen Abschnitt wurden prädikatenlogische Ausdrücke verwendet, z.B.: $x \in A \wedge\ x \in B$ oder $A \subset B$. Diese Ausdrücke beschreiben Relationen zwischen Mengen bzw. zwischen Elementen und Mengen. Die Zeichen $\in$ und $\subset$ werden als *Relationssymbole* bezeichnet. Relationssymbole werden durch Relationen interpretiert.
Im Unterschied zu den Ausdrücken werden $A \cap B$ oder $A \times B$ als *Terme* bezeichnet. Die Zeichen $\times$ und $\cap$ sind *Funktionssymbole*. Ihre Interpretation ist jeweils eine Funktion. Im vorliegenden Beispiel ordnet die Funktion ihren Argumenten, beliebigen Mengen A und B eine neue Menge als Wert zu. Terme können als Bestandteil von prädikatenlogischen Ausdrücken auftreten, z.B. in

$$A \cap B \subseteq A$$

oder

$$(x \in A \wedge\ y \in B) \rightarrow (x, y) \in A \times B$$

.
Relations- und Funktionssymbole müssen nicht notwendig zwei Argumente haben. Beispielsweise ist das Symbol $\mathcal{P}$, welches für die Konstruktion der Potenzmenge benutzt wird, ein *einstelliges* Funktionssymbol. Das Symbol $\emptyset$ hat gar kein Argument, es wird als *nullstelliges* Funktionssymbol oder als *Konstante* bezeichnet.
Ausdrücke wie $A \cap B \subseteq A$ oder $A \subset B$ werden auch als *atomar* bezeichnet, da sie im Gegensatz zu $(x \in A \wedge\ y \in B) \rightarrow (x, y) \in A \times B$ keine logischen Verknüpfungszeichen enthalten.
In der Prädikatenlogik treten neben den aussagenlogischen Verknüpfungszeichen $\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ noch die *Quantoren* $\forall$, der *universelle Quantor*, und $\exists$, der *Existenzquantor*, auf.

Beispiel 4.1

$$\forall\ A.(A \cap B \subseteq A)$$

$$\exists\ B.(A \cup B \subseteq A)$$

$$\forall\ A.\exists\ B.(A \cup B \subseteq A)$$

$$\exists\ A.\forall\ B.(A \cup B \subseteq A)$$

In diesem Unterabschnitt wurden bisher nur Ausdrücke mit den Relations- und Operationssymbolen $\in, \subseteq, \subset, \cap, \cup, \ldots$ behandelt. Dabei haben wir ihnen eine feste Bedeutung oder Interpretation zugeordnet, nämlich die aus der Mengenlehre geläufige. Man spricht deshalb auch von interpretierten Symbolen. Wir werden auch Ausdrücke ohne vorgegebene Interpretation der darin vorkommenden Prädikats-, Funktions- und Konstantensymbole betrachten. Dann werden die Relations- und Operationssymbole oftmals allgemeiner als $p, q, r, f, g, \ldots$ geschrieben. Die vorstehenden vier Formeln nehmen bei Verwendung dieser Symbole die folgende Form an.

Beispiel 4.2

$$\forall\ A.p(g(A, B), A)$$

$$\exists\ B.p(g(A, B), A)$$

$$\forall\ A.\exists\ B.p(g(A, B), A)$$

$$\exists\ A.\forall\ B.p(g(A, B), A)$$

Es werden nun die Begriffe der Erfülltheit und der Gültigkeit von Ausdrücken präzisiert.

Definition 4.1
Es sei r ein n-stelliges Relationssymbol und $t_1, \ldots, t_n$ seien Terme. Der atomare Ausdruck $r(t_1, \ldots, t_n)$ ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen des Relationssymbols r durch eine Relation R über M und der Funktionssymbole in den Termen $t_1, \ldots, t_n$ durch Funktionen über M sowie der freien Variablen in den Termen $t_1, \ldots, t_n$ durch Elemente der Menge M erfüllt*, wenn für die Werte $\xi_1, \ldots, \xi_n$, die sich bei Auswertung der Terme $t_1, \ldots, t_n$ unter der betrachteten Belegung ergeben, $(\xi_1, \ldots, \xi_n) \in R$ gilt. □

Beispiel 4.3
$B \subseteq A \cup B$ ist bei mengentheoretischer Interpretation der Symbole $\subseteq$ und $\cup$ bei beliebiger Belegung von A und B mit Mengen erfüllt.
$B \subseteq A \cap B$ ist bei mengentheoretischer Interpretation der Symbole $\subseteq$ und $\cap$ bei Belegung von A und B mit ein und derselben Menge erfüllt.

Definition 4.2
Ein nichtatomarer Ausdruck A, der nur unter Anwendung der aussagenlogischen Verknüpfungszeichen $\neg$, $\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ aus den atomaren Ausdrücken $A_1, \ldots, A_n$ gebildet wurde, ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen der Relationssymbole durch Relationen über M und der Funktionssymbole durch Funktionen über M sowie der freien Variablen in A durch Elemente der Menge M erfüllt*, wenn sich dies aus den Wahrheitswerttabellen für die aussagenlogischen Verknüpfungszeichen $\neg$, b$\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ und der Erfülltheit der Ausdrücke $A_1, \ldots, A_n$ bei der gleichen Interpretation ergibt. □

Beispiel 4.4
$(A \subseteq B) \rightarrow (A \cup B \subseteq B)$ ist bei mengentheoretischer Interpretation der Symbole $\subseteq$ und $\cup$ bei beliebiger Belegung von A und B erfüllt. Denn eine beliebige Belegung von A und B mit Mengen, bei der $A \subseteq B$ erfüllt ist, erfüllt auch $A \cup B \subseteq B$.
$\neg\ (B \subset A \cap B)$ ist bei mengentheoretischer Interpretation der Symbole $\subset$ und $\cap$ bei Belegung von A mit einer echten Teilmenge der Menge, mit der B belegt ist, erfüllt.

Definition 4.3
Ein Ausdruck $\forall\ x.\Phi$ ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen der Relationssymbole durch Relationen über M und der Funktionssymbole durch Funktionen über M sowie der freien Variablen in $\forall\ x.\Phi$ durch Elemente der Menge M erfüllt*, wenn Φ für alle Belegungen der Variablen x mit Werten aus M erfüllt ist. □

Beispiel 4.5
$\forall\ A.(A \cup B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole und bei Belegung von B mit der leeren Menge erfüllt.

Definition 4.4
Ein Ausdruck $\exists\ x.\Phi$ ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen der Relationssymbole durch Relationen und der Funktionssymbole durch Funktionen über M sowie der freien Variablen in $\exists\ x.\Phi$ durch Elemente der Menge M erfüllt*, wenn es eine Belegung der Variablen x mit einem Wert aus M gibt, für die Φ erfüllt ist. □

Beispiel 4.6
$\exists\ A.(A \cap B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole und bei Belegung von B mit der leeren Menge erfüllt.
$\forall\ A.(A \cup B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole und bei Belegung von B mit einer nichtleeren Menge nicht erfüllt.

Definition 4.5
Ein Ausdruck Φ ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen der Relationssymbole durch Relationen und der Funktionssymbole durch Funktionen über M erfüllbar*, wenn es eine Belegung der freien Variablen in Φ durch Elemente der Menge M gibt, so daß Φ erfüllt ist. □

Beispiel 4.7
$\forall\ A.(A \cup B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole erfüllbar. Es genügt dazu, B mit der leeren Menge zu belegen.

Definition 4.6
Ein Ausdruck Φ ist genau dann *bei einer vorgegebenen Menge M sowie Interpretationen der Relationssymbole durch Relationen und der Funktionssymbole durch Funktionen über M gültig*, wenn für alle Belegungen der freien Variablen in Φ durch Elemente der Menge M der Ausdruck Φ erfüllt ist. □

Beispiel 4.8
$\forall\ A.(A \cup B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole nicht gültig.
$\exists\ A.(A \cup B \subseteq A)$ ist bei mengentheoretischer Interpretation der Symbole gültig.

Definition 4.7
Ein Ausdruck Φ ist genau dann *erfüllbar*, wenn es eine Menge M sowie Interpretationen der Relationssymbole durch Relationen und der Funktionssymbole durch Funktionen über M und eine Belegung der freien Variablen in Φ durch Elemente der Menge M gibt, so daß Φ erfüllt ist. □

Beispiel 4.9
$\forall\ A.p(g(A,B),A)$ ist erfüllbar.

Definition 4.8
Ein Ausdruck Φ ist genau dann *allgemeingültig*, wenn für alle Mengen M sowie Interpretationen der Relationssymbole durch Relationen und der Funktionssymbole durch Funktionen über M und alle Belegungen der freien Variablen in Φ durch Elemente der Menge M der Ausdruck Φ erfüllt ist. □

Beispiel 4.10
$\forall\ A.p(g(A,B),A)$ ist nicht allgemeingültig.
$\exists\ X.\forall\ Y.p(X,Y) \rightarrow \forall$ a. $\exists$ b. q(b,a) ist allgemeingültig.

5 Zum Beweisen in der Prädikatenlogik

5.1 Zum Kalkülbegriff

Im Abschnitt 4 wurde die Bedeutung prädikatenlogischer Konstrukte erklärt. In diesem Abschnitt werden Regeln angegeben, mit denen korrekte Beweise für die Gültigkeit prädikatenlogischer Formeln konstruiert werden können. Eine solche Regelmenge wird als *Kalkül* bezeichnet. Der hier vorgestellte Kalkül geht auf Gentzen [2] zurück. Jeder Beweis, der nach diesen Regeln konstruiert wurde, ist logisch korrekt. Diese Eigenschaft eines Kalküls wird als *Korrektheit* bezeichnet. Für jede gültige Formel der Prädikatenlogik existiert ein nach diesen Regeln konstruierter Beweis. Diese Eigenschaft eines Kalküls wird als *Vollständigkeit* bezeichnet. Für weitere Einzelheiten wird auf [1] und [12] verwiesen.

5.2 Natürlichen Schließen und Sequenzenkalkül in der Prädikatenlogik

Nachfolgend wird eine praktikable Formalisierung des Beweisbegriffs angegeben. Diese beruht darauf, Vorschriften für die Behandlung von Formeln im Verlaufe eines Beweises anzugeben. Diese hängen vom Hauptverknüpfungszeichen der Formel und von ihrer Rolle als zulässige Annahme oder Beweisverpflichtung ab.
Die Vorschriften werden anhand der Definition der Bedeutung der logischen Ausdrücke in Abschnitt 4 begründet. Jeder Vorschrift wird ein Name zugeordnet. Eine tabellarische Zusammenfassung der Regeln ist in den Abbildungen 2 und 3 angegeben.

(1) Ein *Beweis* ist eine formale Darstellung einer Argumentation. Diese führt in mehreren Schritte von Beweissituation zu Beweissituation. Jede dieser Situationen ist durch eine Menge von zulässigen Annahmen und von offenen Beweisverpflichtungen charakterisiert.

(2) *Zulässige Annahmen* sind entweder von Anfang an gegeben oder ergeben sich durch Anwendung der nachfolgend beschriebenen Regeln während der Argumentation. Bei den zulässigen Annahmen, die schon zu Beginn der Argumentation gegeben sind, handelt es sich um gültige mathematische Sätze oder in Spezifikationen von Datenstrukturen zugesicherte Eigenschaften über die in der nachzuweisenden logischen Formel vorkommenden interpretierten Symbole.

    Das Vorhandensein dieser Formeln in der Menge der Annahmen widerspiegelt, daß nur bestimmte Interpretationen der beteiligten Symbole bei Feststellung der Gültigkeit betrachtet werden.

(3) Eine Argumentation kann *verzweigen*. Dies kommt in folgenden Situationen vor.

    (a) Es wird eine Konjunktion als Beweisverpflichtung behandelt. Dann ist für jedes Glied der Konjunktion ein Einzelnachweis zu führen, wobei die zulässigen Annahmen übernommen werden.

        Dies entspricht der Bedeutung der Konjunktion, die besagt, daß eine Konjunktion bei einer Interpretation genau dann erfüllt ist, wenn jedes ihrer Glieder bei dieser Interpretation erfüllt ist.

        Diese Situation wird durch die Regel $\wedge$ -I widergespiegelt.

    (b) Es soll eine Beweisverpflichtung unter Verwendung einer Disjunktion als zulässiger Annahme nachgewiesen werden. Dann ist für die Beweisverpflichtung unter Übernahme von jeweils einem Glied der Disjunktion in die Menge der zulässigen Annahmen ein Einzelnachweis zu führen.

        Dies entspricht der Bedeutung der Disjunktion, die besagt, daß eine Disjunktion bei einer Interpretation nur dann erfüllt ist, wenn eines ihrer Glieder bei dieser Interpretation erfüllt ist. Dabei ist allerdings nicht gewiß, welches der Glieder erfüllt ist.

        Diese Situation wird durch die Regel $\vee$ -E widergespiegelt.

(4) Anfangs kommt genau der nachzuweisende logische Ausdruck als Beweisverpflichtung vor.

(5) In Laufe einer Argumentation können jedoch auch Situationen mit *mehreren, dann alternativ zu verstehenden, Beweisverpflichtungen* auftreten. Diese entstehen dann, wenn eine Disjunktion als Beweisverpflichtung zu behandeln ist. Dann werden statt dieser alle Disjunktionsglieder als Beweisverpflichtungen gehalten. Es genügt dann, eine dieser Einzelbeweisverpflichtungen einzulösen.

Dies entspricht der Bedeutung der Disjunktion, die besagt, daß eine Disjunktion bei einer Interpretation bereits dann erfüllt ist, wenn eines ihrer Glieder bei dieser Interpretation erfüllt ist.

Diese Situation wird durch die Regel $\vee$ -I widergespiegelt.

(6) In Laufe einer Argumentation sind Situationen mit *mehreren zulässigen Annahmen* möglich. Diese entstehen dann, wenn eine Konjunktion als zulässige Annahme genutzt wird. Dann werden statt dieser alle Konjunktionsglieder als zulässige Annahmen gehalten.

Dies entspricht der Bedeutung der Konjunktion, die besagt, daß eine Konjunktion bei einer Interpretation nur dann erfüllt ist, wenn jedes ihrer Glieder bei dieser Interpretation erfüllt ist.

Diese Situation wird durch die Regel $\wedge$ -E widergespiegelt.

(7) Ein Zweig einer Argumentation ist abgeschlossen, wenn eine der Beweisverpflichtungen als zulässige Annahme vorkommt.

(8) Ein Zweig einer Argumentation ist auch abgeschlossen, wenn eine der zulässigen Annahmen die Negation einer anderen ist.

Diese entspricht der Vorstellung der klassischen Logik, daß eine Aussage und ihre Negation nicht gleichzeitig wahr sein können. Aus einem solchen Widerspruch kann eine beliebige Formel gefolgert werden.

Diese Situation wird durch die Regel $\neg$ -E widergespiegelt.

(9) Eine Negation $\neg$ F als Beweisverpflichtung wird behandelt, indem die Formel F den Annahmen hinzugefügt und daraus ein Widerspruch hergeleitet wird.

Diese entspricht der Vorstellung der klassischen Logik, daß eine Aussage und ihre Negation nicht gleichzeitig wahr sein können. Aus einem solchen Widerspruch kann eine beliebige Formel gefolgert werden.

Diese Situation wird durch die Regel $\neg$ -I widergespiegelt.

(10) Eine Implikation als Beweisverpflichtung wird behandelt, indem ihre Voraussetzung den Annahmen hinzugefügt und aus dieser verstärkten Annahmenmenge die Folgerung der Disjunktion gezeigt wird.

Damit wird der laut Wahrheitswerttabelle in Abbildung 1 kritische Fall ausgeschlossen, daß die Annahme einer Implikation erfüllt jedoch deren Schlußfolgerung nicht erfüllt ist.

Diese Situation wird durch die Regel $\rightarrow$ -I widergespiegelt.

(11) Sind eine Implikation A $\rightarrow$ B und Formel A zulässige Annahmen, dann darf Formel B zu den zulässigen Annahmen hinzugefügt werden.

Diese Schlußweise ist durch die Wahrheitswerttabelle in Abbildung 1 gerechtfertigt.

Diese Situation wird durch die Regel $\rightarrow$ -E widergespiegelt.

(12) Eine universell quantifizierte Formel $\forall$ x. F(x) als Beweisverpflichtung wird behandelt, indem die Formel F(a) unter den unveränderten Annahmen gezeigt wird. Wichtig ist hierbei, daß die Variable a im bisherigen Beweis noch nicht frei vorkommt.

Dies entspricht der Definition 4.3. Durch die Verwendung einer neuen Variablen ist gesichert, daß ein von der bisherigen Argumentation unabhängiges Element betrachtet wird, welches in der weiteren Überlegung auch nicht mehr geändert wird. In der mathematischen Argumentation verwenden wir dafür die Floskel: „Sei a beliebig aber von nun an fest."

Diese Situation wird durch die Regel ∀ -I widergespiegelt.

(13) Ist eine universell quantifizierte Formel ∀ x. F(x) zulässige Annahme, dann darf für einen beliebigen Term t die Formel F(t) zu den gültigen Annahmen hinzugefügt werden.

Diese Schlußweise ist durch Definition 4.3 gerechtfertigt. Denn wenn F(x) für alle x gilt, dann auch für den Wert des Terms t bei der gerade betrachteten Belegung.

Diese Situation wird durch die Regel ∀ -E widergespiegelt.

(14) Ist eine existentiell quantifizierte Formel ∃ x. F(x) Beweisverpflichtung, genügt es, für einen beliebigen Term t die Beweisverpflichtung F(t) zu einzulösen.

Diese Schlußweise ist durch Definition 4.4 gerechtfertigt. Denn wenn F(t) für einen Term t gilt, dann ist mit dem Wert dieses Terms auch ein Element bekannt dessen Existenz im Ausdruck ∃ x. F(x) verlangt wird.

Diese Situation wird durch die Regel ∃ -I widergespiegelt.

(15) Eine existentiell quantifizierte Formel ∃ x. F(x) als zulässige Annahme wird genutzt, indem die Formel F(a) zusätzlich zu den bereits vorhandenen Annahmen genutzt wird. Wichtig ist hierbei, daß die Variable a im bisherigen Beweis noch nicht frei vorkommt.

Dies entspricht der Definition 4.4. Es ist durch die Verwendung einer neuen Variablen gesichert, daß ein von der bisherigen Argumentation unabhängiges Element betrachtet wird, welches in der weiteren Überlegung auch nicht mehr geändert wird. In der mathematischen Argumentation verwenden wir dafür die Floskel: „Sei a beliebig aber von nun an fest."

Diese Situation wird durch die Regel ∃ -E widergespiegelt.

5.3 Abschluß von Beweiszweigen

Tritt einer der folgenden Beweissituationen auf, ist der betreffende Zweig der Beweises abgeschlossen. Ein Beweis ist abgeschlossen, wenn jeder seiner Zweige abgeschlossen ist.

(1) Aus der Annahme A kann die Beweisverpflichtung A hergeleitet werden.

(2) Eine Beweisverpflichtung A ∨ ¬ A ist gelöst.

(3) Aus einem Widerspruch A ∧ ¬ A kann eine beliebige Formel abgeleitet werden.

5.4 Zur Darstellung von Beweisen in der Prädikatenlogik

Bei der Darstellung von Beweisen ist durch geeignete Notation oder Wortwahl der Status von Ausdrücken als Annahme oder Beweisverpflichtung deutlich zu machen. In einer stärker formalisierten Darstellung kann dies durch die Verwendung des Ableitungssymbols ⊢ erreicht werden. Beispielsweise kann man Beweissituationen wie folgt durch sogenannte Sequenzen darstellen.

Folge zulässiger Annahmen ⊢ Folge von Beweisverpflichtungen

Ein Kalkül für das Behandeln solcher Beweissituationen wird als Sequenzenkalkül bezeichnet. Diese Notation wird auch in den in Abschnitt 6 angegebenen computergenerierten Beweisdarstellungen benutzt. In diesen Darstellungen kommen zu jeder Sequenz noch Verwaltungsinformationen hinzu. Sequenzen haben dann die folgende Form.

Formel	Vorkommen als Beweisverpflichtung	Vorkommen als Annahme
$\neg$ A	A wird angenommen. Unter dieser Annahme ist ein Widerspruch herzuleiten. Bezeichnung: $\neg$ -I Beispiel: 6.5,6.6 Alternativbezeichnung: prop simplification	Wird $\neg$ A angenommen und kann auch A angenommen werden, dann ist ein Widerspruch gezeigt. Bezeichnung: $\neg$ -E Beispiel: 6.5 Alternativbezeichnung: prop simplification; axiom
A $\wedge$ B	Um A $\wedge$ B nachzuweisen, sind A und B unabhängig voneinander nachzuweisen Bezeichnung: $\wedge$ -I Beispiel: 6.2 Alternativbezeichnung: case distinction right	Kann A $\wedge$ B angenommen werden, können sowohl A als auch B als Annahme genutzt werden. Bezeichnung: $\wedge$ -E Beispiele: 6.2,6.4,6.6 Alternativbezeichnung: prop simplification
A $\vee$ B	Zum Nachweis von A $\vee$ B genügt es, Teilausdruck A oder Teilausdruck B nachzuweisen Bezeichnung: $\vee$ -I Beispiel: 6.3 Alternativbezeichnung: prop simplification	Um aus A $\vee$ B eine Formel C nachzuweisen, ist C sowohl aus A (ohne B) als auch aus B (ohne A) nachzuweisen. Bezeichnung: $\vee$ -E Beispiel: 6.3 Alternativbezeichnung: case distinction left
A $\rightarrow$ B	Um A $\rightarrow$ B nachzuweisen, wird A angenommen, und es ist B unter der Annahme von A zu zeigen. Bezeichnung: $\rightarrow$ -I Beispiele: 6.1,6.3,6.4 Alternativbezeichnung: prop simplification	Kann A $\rightarrow$ B und kann auch A angenommen werden, dann ist B gezeigt. Bezeichnung: $\rightarrow$ -E Beispiel: 6.7 Alternativbezeichnung: case distinction left

Abbildung 2: Beweisregeln für aussagenlogische Junktoren

Schrittnummer Name der benutzten Schlußregel Nummer der betroffenen Formel
Folge zulässiger Annahmen $\vdash$ Folge von Beweisverpflichtungen

Hierbei ist mit Name der benutzten Schlußregel die in den Abbildungen 2 und 3 angegebene Alternativbezeichnung gemeint.
In Abschnitt 6 werden zu den computergenerierten Beweisdarstellungen auch überarbeitete Darstellungen angegeben, die näher an der natürlichsprachlichen Argumentation sind. Darin werden die einzelnen Beweisschritte wie folgt dargestellt:

Schrittnummer Name der benutzten Schlußregel
eventuelle nähere Erläuterung
betroffene Formel

Bei deren Übertragung in natürliche Sprache werden in jedem Beweisschritt nur die jeweils betroffenen Formeln der Beweissituation erwähnt. Dabei wird aber stets herausgestellt, ob es sich um eine Annahme oder eine Beweisverpflichtung handelt.

Formel	Vorkommen als Beweisverpflichtung	Vorkommen als Annahme
$\forall$ x. F(x)	Um $\forall$ x. F(x) nachzuweisen muß F(a) nachgewiesen werden. Dabei ist a eine Variable, die noch nicht im Beweis frei vorkommt, insbesondere nicht in F(x). Sprechweise: „Sei a beliebig aber von nun an fest.“ Bezeichnung: $\forall$ -I Beispiel: 6.1,6.2 Alternativbezeichnung: all right	Kann $\forall$ x. F(x) angenommen werden, dann kann für einen beliebigen Term t F(t) angenommen werden. Bezeichnung: $\forall$ -E Beispiel: 6.1,6.2 Alternativbezeichnung: all left
$\exists$ x. F(x)	Zum Nachweis von $\exists$ x. F(x) genügt es, für einen beliebigen Term t F(t) nachzuweisen. Bezeichnung: $\exists$ -I Beispiel: 6.1,6.3 Alternativbezeichnung: exists right	Um aus $\exists$ x. F(x) eine Formel C nachzuweisen, ist C aus F(a) nachzuweisen, wobei die Variable a noch nicht im Beweis frei vorkommt, insbesondere nicht in C. Sprechweise: „Sei a ein beliebiges aber von nun an festes Element mit F(a)“ Bezeichnung: $\exists$ -E Beispiel: 6.1,6.3 Alternativbezeichnung: exists left

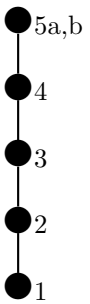
Abbildung 3: Beweisregeln für prädikatenlogische Junktoren

6 Beispielbeweise

Die in den vorhergehenden Abschnitten eingeführten Folgerungsregeln werden in den folgenden Abschnitten 6.1, ..., 6.7 an Beispielbeweisen illustriert. Bis auf den etwas längeren, aber unverzweigten, Beweis 6.7 wird für jeden der Beweise die Verzweigungsstruktur durch einen Baum angegeben. Dieser „wächst von unten nach oben“. Die Knotennummerierungen beziehen sich auf die einzelnen Beweissituationen.
Alle Beweise wurden mit einem Beweiser (KIV) durchgeführt. Um den hier gewünschten Grad der Detailiertheit zu erreichen, wurde die Automatik ausgeschaltet werden.
In den folgenden Abschnitten 6.1, ..., 6.7 wird jeweils ein rechnergestützt erzeugter Beweis dargestellt. Deren Druckversionen sind jeweils automatisch erzeugt. Jedem dieser automatisch gesetzten Beweise wurde eine handbearbeitete Version vorangestellt. Diese orientiert sich an der sprachlichen Argumentation, wie sie ein Mathematiker wählen würde. Um dabei die Vergleichbarkeit mit dem computergestützt erzeugten Original zu erreichen, waren gewisse Kompromisse im Ausdruck nötig.

6.1 (∃ a. ∀ x. pp(a, x)) → (∀ b. ∃ y. pp(y, b))

Beweisstruktur:



---

1) Regel: → -I
Nachzuweisen ist nachstehende Formal. Es wird vorstehende Regel benutzt.
(∃ a. ∀ x. pp(a, x)) → (∀ b. ∃ y. pp(y, b))

---

2) Wir nehmen an:
∃ a. ∀ x. pp(a, x)

2a) Regel: ∀ -I
Und zeigen unter der Annahme 2) und unter Anwendung vorstehender Regel:
∀ b. ∃ y. pp(y, b)

---

3) Regel: ∃ -E
Dazu betrachten wir ein beliebiges, aber von nun an festes b, und mit vorgenannter Regel zeigen wir:
∃ y. pp(y, b)

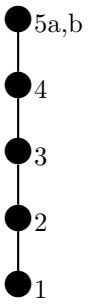
---

4) Regel: ∀ -E
Sei a ein beliebiges, aber von nun an festes Element, welches gemäß Annahme 2) existiert. Wir nutzen vorstehende Regel, denn wir können annehmen:
∀ x. pp(a, x)

5a) In Annahme 4) setzen wir b für x ein und erhalten die Annahme:
pp(a, b)

5b) Regel: ∃ -I
Damit kann a als das Element gewählt werden, dessen Existenz in 3) zu zeigen war.
Damit ist 3) nachgewiesen.
Damit ist 2a) nachgewiesen.
Damit ist 1) nachgewiesen.
q.e.d.

Originalbeweis zu 6.1:



$\vdash (\exists\ a.\ \forall\ x.\ pp(a, x)) \rightarrow (\forall\ b.\ \exists\ y.\ pp(y, b))$

- proofsteps: 5
- interactions: 5
- automation: 0.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: prop simplification 1
$\vdash (\exists\ a.\ \forall\ x.\ pp(a, x)) \rightarrow (\forall\ b.\ \exists\ y.\ pp(y, b))$

---

2) Interactive: all right 1
$\exists\ a.\ \forall\ x.\ pp(a, x) \vdash \forall\ b.\ \exists\ y.\ pp(y, b)$

---

3) Interactive: exists left 1
$\exists\ a.\ \forall\ x.\ pp(a, x) \vdash \exists\ y.\ pp(y, b)$

---

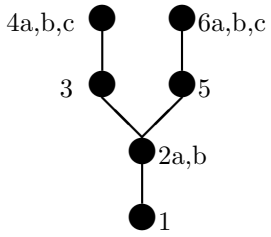
4) Interactive: all left 1 with b
$\forall\ x.\ pp(a, x) \vdash \exists\ y.\ pp(y, b)$

---

5) Interactive: exists right 1 with a
$pp(a, b) \vdash \exists\ y.\ pp(y, b)$

6.2 $(\forall\ \mathbf{x.}\ \mathbf{p(x)} \wedge \mathbf{q(x)}) \rightarrow (\forall\ \mathbf{x.}\ \mathbf{p(x)}) \wedge (\forall\ \mathbf{x.}\ \mathbf{q(x)})$

Beweisstruktur:



Beweis:

1) Regel: $\rightarrow$ -I
Nachzuweisen ist:
$(\forall$ x. p(x) $\wedge$ q(x)) $\rightarrow$ ($\forall$ x. p(x)) $\wedge$ ($\forall$ x. q(x))

2a) Um 1) mittels genannter Regel nachzuweisen, nehmen wir an:
$\forall$ x. p(x) $\wedge$ q(x)

2b) Regel: $\wedge$ -I
. . . und zeigen mittels vorstehender Regel:
($\forall$ x. p(x)) $\wedge$ ($\forall$ x. q(x))

3) Regel: $\forall$ -I
Um 2b) zu zeigen, müssen wir sowohl den folgenden Ausdruck als auch den Ausdruck 5) als gültig nachweisen. Dazu wird vorstehende Regel genutzt.
$\forall$ x. p(x)

4a) Regel: $\forall$ -E
Um 3) zu zeigen, betrachten wir ein beliebiges aber von nun an festes a und wenden vorstehende Regel auf 2b) an. zeigen:
p(a)

4b) Regel: $\wedge$ -E
Das in 4a) genannte a kann für x in 2a) eingesetzt werden. Auf die dadurch erhaltene Annahme kann vorstehende Regel angewendet werden.
p(a) $\wedge$ q(a)

4c) Aus 4b) folgt die Behauptung 4a). Damit ist dieser Zweig des Beweises abgeschlossen.

5) Regel: $\forall$ -I
anzuwenden auf von 2b) stammende Beweisverpflichtung:
$\forall$ x. q(x)

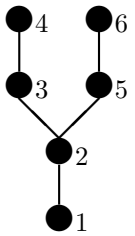
6a) Regel: $\forall$ -E
Um 5) zu zeigen, betrachten wir ein beliebiges aber von nun an festes b und zeigen mittels vorstehender, auf 2a) anzuwendender, Regel :
q(b)

6b) Regel: $\wedge$ -E
Das in 6a) genannte b kann für x in 2a) eingesetzt werden. Dadurch erhalten wir folgende Annahme, auf die vorstehende Regel angewendet wird:
p(b) $\wedge$ q(b)

6c) Aus 6b) folgt die Behauptung 6a). Damit ist dieser Zweig des Beweises abgeschlossen.

Mit 4c) und 6c) sind beide Zweige des Nachweises von 2b) abgeschlossen.
Damit ist der Nachweis von 1) abgeschlossen.
q.e.d.

Originalbeweis zu 6.2 :



$\vdash (\forall\ x.\ p(x) \wedge q(x)) \rightarrow (\forall\ x.\ p(x)) \wedge (\forall\ x.\ q(x))$

- proofsteps: 6
- interactions: 6
- automation: 0.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: prop simplification 1
$\vdash (\forall\ x.\ p(x) \wedge q(x)) \rightarrow (\forall\ x.\ p(x)) \wedge (\forall\ x.\ q(x))$

---

2) Interactive: case distinction right 1
$\forall\ x.\ p(x) \wedge q(x) \vdash (\forall\ x.\ p(x)) \wedge (\forall\ x.\ q(x))$

---

3) Interactive: all right 1
$\forall\ x.\ p(x) \wedge q(x) \vdash \forall\ x.\ p(x)$

---

4) Interactive: all left 1 with x
$\forall\ x.\ p(x) \wedge q(x) \vdash p(x)$

---

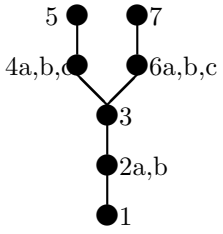
5) (from 2) Interactive: all right 1
$\forall\ x.\ p(x) \wedge q(x) \vdash \forall\ x.\ q(x)$

---

6) Interactive: all left 1 with x
$\forall\ x.\ p(x) \wedge q(x) \vdash q(x)$

6.3 $(\exists\ \mathbf{x.}\ \mathbf{p(x)} \vee \mathbf{q(x)}) \rightarrow (\exists\ \mathbf{x.}\ \mathbf{p(x)}) \vee (\exists\ \mathbf{x.}\ \mathbf{q(x)})$

Beweisstruktur:



Beweis:

---

1) Regel: $\rightarrow$ -I
Mittels vorstehender Regel ist nachzuweisen:
$(\exists$ x. p(x) $\vee$ q(x)) $\rightarrow$ ($\exists$ x. p(x)) $\vee$ ($\exists$ x. q(x))

2a) Regel: $\exists$ -E
Um 1) nachzuweisen, wird nachfolgende Formel angenommen und auf sie vorstehende Regel angewendet.
$\exists$ x. p(x) $\vee$ q(x)

2b) Es ist zu zeigen:
($\exists$ x. p(x)) $\vee$ ($\exists$ x. q(x))

---

3) Regel: $\vee$ -E
Sei a ein beliebiges aber von nun an festes Element, welches laut 2a) existiert. Folgende Annahme wird nach vorstehender Regel in den Fällen 4a) und 6a) per Fallunterscheidung genutzt wird:
p(a) $\vee$ q(a)

4a) Unter folgender Annahme
p(a)

4b) Regel: $\vee$ -I
ist mittels vorstehender Regel zu zeigen:
($\exists$ x. p(x)) $\vee$ ($\exists$ x. q(x))

4c) Regel: $\exists$ -I
Um 4b) zu zeigen, genügt es, unter Anwendung vorstehender Regel, zu zeigen:
$\exists$ x. p(x)

---

5) Um 4c) zu zeigen, genügt es, in 4c) das Element a für x einzusetzen.
Damit ist dieser Zweig des Beweises wegen Annahme 4a) abgeschlossen.

6a) Unter folgender Annahme
q(a)

6b) Regel: $\vee$ -I
ist mittels vorstehender Regel zu zeigen:
($\exists$ x. p(x)) $\vee$ ($\exists$ x. q(x))

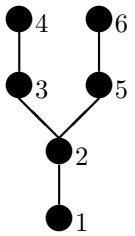
6c) Regel: $\exists$ -I
Um 6b) zu zeigen, genügt es, unter Anwendung vorstehender Regel, zu zeigen:
$\exists$ x. q(x)

---

7) Um 6c) zu zeigen, genügt es, in 6c) das Element a für x einzusetzen.
Damit ist dieser Zweig des Beweises wegen Annahme 6a) abgeschlossen.

Mit 4c) und 6c) sind beide Zweige des Nachweises von 2b) abgeschlossen.
Damit ist der Nachweis von 1) abgeschlossen.
q.e.d.

Originalbeweis zu 6.3 :



$\vdash (\exists\ x.\ p(x) \lor q(x)) \rightarrow (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

- proofsteps: 7
- interactions: 7
- automation: 0.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: prop simplification 1
$\vdash (\exists\ x.\ p(x) \lor q(x)) \rightarrow (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

---

2) Interactive: exists left 1
$\exists\ x.\ p(x) \lor q(x) \vdash (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

---

3) Interactive: case distinction left 1
$p(x) \lor q(x) \vdash (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

---

4) Interactive: prop simplification 1
$p(x) \vdash (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

---

5) Interactive: exists right 1 with x
$p(x) \vdash \exists\ x.\ p(x), \exists\ x.\ q(x)$

---

6) (from 3) Interactive: prop simplification 1
$q(x) \vdash (\exists\ x.\ p(x)) \lor (\exists\ x.\ q(x))$

---

7) Interactive: exists right 2 with x
$q(x) \vdash \exists\ x.\ p(x), \exists\ x.\ q(x)$

6.4 $(\forall$ x. p(x) $\rightarrow$ qq(x, ff(x))) $\wedge$ p(a) $\rightarrow$ qq(a, ff(a))

Beweisstruktur:

---

1) Regel: $\rightarrow$ -I
Nachzuweisen ist mittels vorstehender Regel:

(∀ x. p(x) → qq(x, ff(x))) ∧ p(a) → qq(a, ff(a))

2a) Regel: $\wedge$ -E
Um 1) nachzuweisen, wird folgende Formal angenommen und auf sie vorstehende Regel angewendet:

(∀ x. p(x) → qq(x, ff(x))) ∧ p(a)

2b) Es ist zu zeigen:

qq(a, ff(a))

2c) Regel: $\forall$ -E
Aus Annahme 2a) erhält man folgende Annahme, auf die vorgenannte Regel anwendbar ist:

∀ x. p(x) → qq(x, ff(x))

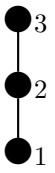
2d) und die Annahme :

p(a)

3a) In die Annahme 2c) kann das Element a für die Variable x eingesetzt werden. Man erhält die Annahme:
p(a) → qq(a, ff(a))

Regel: $\rightarrow$ -E
Aus Annahme 3a) und Annahme 2d) folgt die zu beweisende Formel 2b).
Damit ist der Nachweis von 1) abgeschlossen.
q.e.d.

Originalbeweis zu 6.4 :



$\vdash (\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge p(a) \rightarrow qq(a, ff(a))$

- proofsteps: 3
- interactions: 3
- automation: 0.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: prop simplification 1
$\vdash (\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge p(a) \rightarrow qq(a, ff(a))$

---

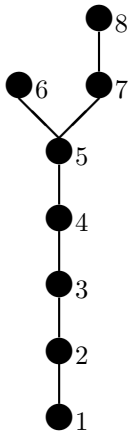
2) Interactive: prop simplification 1
$(\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge p(a) \vdash qq(a, ff(a))$

---

3) Interactive: all left 1 with a
$\forall\ x.\ p(x) \rightarrow qq(x, ff(x)), p(a) \vdash qq(a, ff(a))$

6.5 (∀ x. p(x) → qq(x, ff(x))) ∧ ¬ qq(a, ff(a)) → ¬ p(a)

Beweisstruktur:



⊢ (∀ x. p(x) → qq(x, ff(x))) ∧ ¬ qq(a, ff(a)) → ¬ p(a)

---

1) Regel → -I
Mittels vorstehender Regel ist nachzuweisen:
(∀ x. p(x) → qq(x, ff(x))) ∧ ¬ qq(a, ff(a)) → ¬ p(a)

2a) Regel: ¬ -I
Um 1) zu lösen, ist nachstehende Beweisverpflichtung zu lösen:
¬ p(a)
Unter Anwendung vorstehender Regel wird p(a) zu den Annahmen hinzugefügt und es ist ein Widerspruch herzuleiten.

2b) Um 2a) zu lösen kann folgende Annahme genutzt werden.
(∀ x. p(x) → qq(x, ff(x))) ∧ ¬ qq(a, ff(a))

---

3) Regel: ∧ -E
Um 2a) zu lösen, wird vorstehende Regel auf die Annahme 2b) angewendet:
(∀ x. p(x) → qq(x, ff(x))) ∧ ¬ qq(a, ff(a))

3a) Damit stehen die folgende und Annahme 4) zusätzlich zur Verfügung.
¬ qq(a, ff(a))

---

4) Regel: ∀ -E with a
Auf die nunmehr verfügbare nachstehende Annahme wird vorstehende Regel angewendet.
∀ x. p(x) → qq(x, ff(x))

---

5) Regel: → -E
Vorstehene Regel wird auf die nachstehende Annahme und auf die und in 2a) genannte angewendet.
p(a) → qq(a, ff(a))

---

6) Abschluß eines Beweiszweigs nach (1) Abschnitt 5.3: p(a) ⊢ p(a)

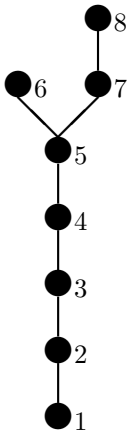
---

7) Regel: ¬ -E
Vorstehene Regel kann auf nachstehende Annahme und die in 3a) genannte angewendet werden.
qq(a, ff(a))

---

8) Abschluß eines Beweiszweigs nach (1) Abschnitt 5.3: qq(a, ff(a)) ⊢ qq(a, ff(a))
Damit ist wie in 2a) gefordert ein Widerspruch in den Annahmen gezeigt.
Damit ist 1) gezeigt.
q.e.d.

Originalbeweis zu 6.5:



$\vdash (\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge \neg\ qq(a, ff(a)) \rightarrow \neg\ p(a)$

- KIV-settings: options: “use basic multiset-rules” heuristics: “multiset axiom”
- proofsteps: 8
- interactions: 6
- automation: 25.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: Implication right 1
$\vdash (\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge \neg\ qq(a, ff(a)) \rightarrow \neg\ p(a)$

---

2) Interactive: Conjunction left 1
$(\forall\ x.\ p(x) \rightarrow qq(x, ff(x))) \wedge \neg\ qq(a, ff(a)) \vdash \neg\ p(a)$

---

3) Interactive: Negation left 2
$\forall\ x.\ p(x) \rightarrow qq(x, ff(x)), \neg\ qq(a, ff(a)) \vdash \neg\ p(a)$

---

4) Interactive: Negation right 2
$\forall\ x.\ p(x) \rightarrow qq(x, ff(x)) \vdash qq(a, ff(a)), \neg\ p(a)$

---

5) Interactive: all left 2 with a
$p(a), \forall\ x.\ p(x) \rightarrow qq(x, ff(x)) \vdash qq(a, ff(a))$

---

6) Interactive: Implication left 2
$p(a), p(a) \rightarrow qq(a, ff(a)) \vdash qq(a, ff(a))$

---

7) multiset axiom: axiom
$p(a) \vdash p(a), qq(a, ff(a))$

---

8) (from 6) multiset axiom: axiom
$qq(a, ff(a)), p(a) \vdash qq(a, ff(a))$

6.6 $\neg\ ((\forall\ \mathbf{x.\ p(x)}) \wedge (\exists\ \mathbf{a.}\ \neg\ \mathbf{p(a)}))$

Beweisstruktur:

---

1) Regel: ¬-I
Mittels vorstehender Regel ist nachzuweisen:
$\neg\ ((\forall$ x. p(x)) $\wedge$ ($\exists$ a. $\neg$ p(a)))

2a) Regel: $\wedge$ -E
Um 1) nachzuweisen, nimmt man nachstende Formel an und wendet vorstehende Regel auf sie an.

($\forall$ x. p(x)) $\wedge$ ($\exists$ a. $\neg$ p(a))

2b) und hat diese Annahme zum Widerspruch zu führen:
$\perp$

3a) Aus Annahme 2a) erhält man die folgende und Annahme 3b).
$\forall$ x. p(x)

3b) Regel: $\exists$ -E
Auf die folgende Annahme wird vorstehende Regel angewendet.
$\exists$ a. $\neg$ p(a)

3c) Es sei nun a ein beliebiges aber von nun an festes Element, welches nach Annahme 3b) existiert und für das nachfolgende Bedingung gilt.

$\neg$ p(a)

---

4) Regel: $\forall$ -E
Das Element a kann in Annahme 3a) für x eingesetzt werden. Man erhält die Annahme :

p(a)
Annahme 4) ist in Widerspruch zu Annahme 3c).
Damit ist 2b) gezeigt.
Damit ist 1) gezeigt.
q.e.d.

Originalbeweis zu 6.6 :

$\vdash \neg ((\forall \text{ x. p(x)}) \wedge (\exists \text{ a. } \neg \text{ p(a)}))$

- proofsteps: 4
- interactions: 4
- automation: 0.0 %
- used lemmas: -
- used simplifier rules:

---

1) Interactive: prop simplification 1
$\vdash \neg ((\forall \text{ x. p(x)}) \wedge (\exists \text{ a. } \neg \text{ p(a)}))$

---

2) Interactive: prop simplification 1
$(\forall \text{ x. p(x)}) \wedge (\exists \text{ a. } \neg \text{ p(a)}) \vdash$

---

3) Interactive: exists left 2
$\forall \text{ x. p(x)}, \exists \text{ a. } \neg \text{ p(a)} \vdash$

---

4) Interactive: all left 1 with a
$\forall \text{ x. p(x)}, \neg \text{ p(a)} \vdash$

6.7 $(\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z)) \rightarrow (\forall\ b.\ \exists\ v.\ gf(v,\ b))$

---

1) Regel: $\rightarrow$ -I
Mittels vorstehender Regel ist nachzuweisen:
$(\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z)) \rightarrow (\forall\ b.\ \exists\ v.\ gf(v,\ b))$

---

2) Regel: $\wedge$ -E
Um 1) zu lösen, ist vorstehende Regel auf folgende Annahme anzuwenden, um 3) zu lösen:
$(\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,z))$

2a) Wegen Annahme 2) sind sowohl :
$\forall\ u.\ \exists\ a.\ f(a,\ u)$

2b) als auch die folgende zulässige Annahmen:
$\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,z)$

---

3) Regel: $\forall$ -I
Unter Annahme 2) ist mittels vorstehender Regel nachstehende Beweisverpflichtung zu lösen. Dazu ist ein beliebiges aber von nun an festes b zu betrachten.
$\forall\ b.\ \exists\ v.\ gf(v,\ b)$

3a) Nachzuweisen:
$\exists\ v.\ gf(v,\ b)$

---

4) Regel: $\forall$ -E mit b
Das in 3) genannte b kann für u in Annahme 2a) eingesetzt werden.
$\forall\ u.\ \exists\ a.\ f(a,\ u)$

---

5) Regel: $\exists$ -E
Auf die aus 4) erhaltene Annahme ist vorstehende Regel anwendbar.
$\exists\ a.\ f(a,\ b)$

5a) Sei a ein beliebiges aber von nun an festes Element, für welches wegen 5) angenommen wird:
$f(a,\ b)$

---

6) Regel: $\forall$ -E mit a
Das in 5a) genannte a kann für u in Annahme 2a) eingesetzt werden[1].
$\forall\ u.\ \exists\ a.\ f(a,\ u)$

Regel: $\exists$ -E
7) Auf die aus 6) erhaltene Annahme ist vorstehende Regel anwendbar.
$\exists\ a_0.\ f(a_0,\ a)$

7a) Es sei a_0 ein beliebiges, von nun an festes Element, für welches wegen 7) angenommen wird:
$f(a_0,\ a)$

Regel: $\wedge$ -I
7b) Aus den Annahmen 5) und 7) folgt mit vorstehender Regel die Annahme:
$f(a_0,\ a) \wedge f(a,\ b)$

Regel: $\forall$ -E für x, y und z
8) Einsetzen von a_0, a, b für die Variablen x, y, z in Annahme 2b)
$\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,z)$

Regel: $\rightarrow$ -E
9) Vorstehende Regel wendet man wird auf Annahme 7b) und folgende aus 8) enstandene an:
$f(a_0,\ a) \wedge f(a,\ b) \rightarrow gf(a_0,\ b)$

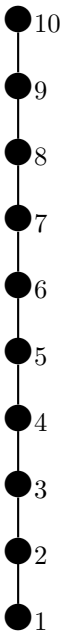
---

[1] Hinweis: Damit es nicht zur Konfusion der ungebundenen Variablen a aus Formel 5) mit der gebundenen Variablen a aus Formel 2a-1) kommt, wird letztere in a_0 umbenannt.

Regel: $\rightarrow$ -E
9a) Aus Annahmen 8a) und 9) folgt mit vorstehender Regel die Annahme:
$gf(a_0, b)$

Regel: $\exists$ -I
10) Laut 9a) ist mit a_0 ein Elements vorhanden, dessen Existenz nachzuweisen war, um unter Anwendung vorstehender Regel 3a) zeigen.
Damit ist 3) gezeigt.
Damit ist 1) gezeigt.
q.e.d.

Originalbeweis zu 6.7 :



$\vdash (\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z)) \rightarrow (\forall\ b.\ \exists\ v.\ gf(v,\ b))$

---

1) Interactive: prop simplification 1
$\vdash (\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z)) \rightarrow (\forall\ b.\ \exists\ v.\ gf(v,\ b))$

2) Interactive: prop simplification 1
$(\forall\ u.\ \exists\ a.\ f(a,\ u)) \wedge (\forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z)) \vdash \forall\ b.\ \exists\ v.\ gf(v,\ b)$

3) Interactive: all right 1
$\forall\ u.\ \exists\ a.\ f(a,\ u),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \forall\ b.\ \exists\ v.\ gf(v,\ b)$

4) Interactive: all left 1 with b
$\forall\ u.\ \exists\ a.\ f(a,\ u),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \exists\ v.\ gf(v,\ b)$

5) Interactive: exists left 1
$\exists\ a.\ f(a,\ b),\ \forall\ u.\ \exists\ a.\ f(a,\ u),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \exists\ v.\ gf(v,\ b)$

6) Interactive: all left 2 with a
$f(a,\ b),\ \forall\ u.\ \exists\ a.\ f(a,\ u),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \exists\ v.\ gf(v,\ b)$

7) Interactive: exists left 2
$f(a,\ b),\ \exists\ a_0.\ f(a_0,\ a),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \exists\ v.\ gf(v,\ b)$

8) Interactive: all left 3 with a_0, a, b
$f(a,\ b),\ f(a_0,\ a),\ \forall\ x,\ y,\ z.\ f(x,\ y) \wedge f(y,\ z) \rightarrow gf(x,\ z) \vdash \exists\ v.\ gf(v,\ b)$

9) Interactive: case distinction left 3
$f(a,\ b),\ f(a_0,\ a),\ f(a_0,\ a) \wedge f(a,\ b) \rightarrow gf(a_0,\ b) \vdash \exists\ v.\ gf(v,\ b)$

10) Interactive: exists right 1 with a_0
$gf(a_0,\ b),\ f(a,\ b),\ f(a_0,\ a) \vdash \exists\ v.\ gf(v,\ b)$

Inhaltsverzeichnis

Abbildungsverzeichnis

Literatur

[1] W. Bibel. *Deduktion*. R. Oldenbourg, Muenchen, 1992.

[2] G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210 and 405–431, 1935. Engl. transl. in [**?**].

[3] D. Harel. Proving the correctness of regular deterministic programs: a unifying survey using dynamic logic. *Theoretical Computer Science*, 12(1):61–81, Sept. 1980.

[4] D. Harel, D. Kozen, and R. Parikh. Process logic: expressiveness, decidability, completeness. *J. Computer and systems science*, 25(2):144–170, 1982.

[5] M. Heisel, W. Reif, and W. Stephan. Program Verification by Symbolic Execution and Induction. In K. Morik, editor, *11th German Workshop on Artifical Intelligence. Proceedings*, number 152 in Informatik Fachberichte. Springer, 1987.

[6] D. Hilbert and P. Bernays. *Grundlagen der Mathematik*. Springer, Berlin, 1934.

[7] U. Petermann. Algorithmische Logik. In L. Kreiser, S. Gottwald, and W. Stelzner, editors, *Nichtklassische Logik*. Akademie-Verlag, Berlin, 1987.

[8] W. Reif. The KIV System: Systematic Construction of Verified Software. In D. Kapur, editor, *11th Conference on Automated Deduction. Proceedings*, Lecture Notes in Computer Science. Albany, NY, USA, Springer, 1992.

[9] W. Reif. Risikofaktor Software. In K. P. Jantke and G. Grieser, editors, *4. Leipziger Informatiktage*. FIT Leipzig, HTWK Leipzig, 1996.

[10] A. Salwicki. Formalized algorithmic languages. *Bull. Acad. Pol. Sci., Ser. Sci. Math. Astr. Phys.*, 18(5), 1970.

[11] A. Salwicki. Algorithmic theories of data structures. In M. Nielsen and E. M. Schmidt, editors, *Automata, Languages and Programming, 9th Colloquium*, volume 140 of *Lecture Notes in Computer Science*, pages 458–472, Aarhus, Denmark, 12–16 July 1982. Springer-Verlag.

[12] D. Siefkes. *Formalisieren und Beweisen Logik fuer Informatiker*. Vieweg, Braunschweig, 1990.