Deduktion in der Aussagenlogik

(Erläuterungen zu Kapitel 17 des FGI-1-Foliensatzes)

Frank Heitmann*

1 Motivation

Wenn man sich erstmal darauf eingelassen hat, dass man mit Formeln etwas sinnvolles machen kann und dass es dann insb. von Interesse ist ihren Wahrheitswert bzw. ihren Wahrheitswerteverlauf zu wissen, stellt sich sogleich die Frage, wie man diesen bestimmen kann und wie man dies möglichst effizient (d.h. meist möglichst schnell) machen kann.[1]

Man möchte also gegeben eine Formel F z.B. wissen, ob eine Belegung $\mathcal{A}$ mit $\mathcal{A}(F) = 1$ existiert (also ob F erfüllbar ist), oder ob F von *jeder* Belegung zu 1 ausgewertet wird (dann ist F eine Tautologie) bzw. von keiner (dann ist F eine Kontradiktion). Ebenso möchte man vielleicht gegeben zwei Formeln F und G wissen, ob $F \models G$ gilt, d.h. ob G aus F folgt, eine Frage die sich darauf zurückführen lässt, ob $F \Rightarrow G$ eine Tautologie ist. Eine ähnliche Frage ist die, ob $M \models G$ für eine Formelmenge M gilt. All diese Fragen sind in verschiedenen Kontexten von Interesse (siehe Fussnote oben) und all diese Fragen lassen sich durch Aufstellen von Wahrheitstafeln (und ggf. ihrer Interpretation) lösen.

*heitmann@informatik.uni-hamburg.de

[1] Wer noch ein bisschen Motivation braucht, warum man denn nun Formeln in der Informatik braucht, denke z.B. an die Modellierung und Verifikation von Systemen. Man kann sich bespielsweise vorstellen, dass man mehrere Eigenschaften eines Systems durch Formeln modelliert, z.B. mit A die Eigenschaft, dass das System einen Abbruch-Knopf hat und mit $A \Rightarrow B$ die Eigenschaft, dass *wenn* der Abbruch-Knopf gedrückt wird, dass *dann* das System sofort den Ablauf unterbricht. Man kann nun $\{A, A \Rightarrow B\} \models B$ zeigen, dass also das System zum Stoppen gebracht werden kann, wenn A und $A \Rightarrow B$ gegeben ist. (Hier wird zwar der Folgerbarkeitsbegriff zur Illustration benutzt, aber dieser kann, da $F \models G$ genau dann gilt, wenn $F \Rightarrow G$ eine Tautologie ist, auf den Tautologiebegriff zurückgeführt werden.) Dies Beispiel hat - neben seinem offensichtlichen "Toy-Example"-Charakter - den Nachteil, dass es etwas ungenau wirkt. Man will ja mit $A \Rightarrow B$ eher einen temporalen Aspekt ausdrücken. Will man dies (die Verifikation von Systemen) tatsächlich ausführen, so braucht man andere Logiken. Doch obiges Beispiel mag einen Eindruck davon geben, was man mit Formeln und Logiken in diesem Kontext so machen kann und tatsächlich enthalten andere Logiken meist die Aussagenlogik als Teillogik. Die Aussagenlogik kann also sowohl als nötige Grundlage dieser anderen, spannenderen Logiken angesehen werden, als auch als Spielweise, um Begriffe erst einmal einzuüben, bevor man sie für kompliziertere Logiken verallgemeinert.

Weitere Anwendungsfelder neben der Modellierung, Spezifikation und Verifikation von Systemen, sind z.B. Datenbanken und künstliche Intelligenz. Zudem schärft die Beschäftigung mit Logik die Fähigkeit logisch zu denken, was einem, auch wenn es zuerst vielleicht nicht so erscheinen mag, beim Entwurf von Systemen aller Art oft eine gute Hilfe ist.

Ableitungen bieten nun ein weiteres Werkzeug, um Aussagen über die semantischen Eigenschaften einer Formel oder einer Formelmenge machen zu können. Ableitungen bedienen sich dabei ausschließlich *syntaktischer* Muster. Rein aufgrund der Syntax von Formeln (also deren "Aussehen") werden letztendlich Schlussfolgerungen bezüglich der semantischen Eigenschaften getätigt. Warum aber braucht man dieses neue - und für die, die es schon mal gesehen haben: zugegebenermassen recht kompliziert erscheinende - Werkzeug, wenn man doch alles so schön mit Wahrheitstafeln lösen kann?

Ein Problem mit Wahrheitstafeln (bzw. mit dem Versuch alles mit Wahrheitstafeln zu lösen) ist die Komplexität des Verfahrens. Wenn man n Aussagensymbole in einer Formel hat, so hat die zugehörige Wahrheitstafel bereits 2^n Zeilen![2] Bei 10 Aussagesymbolen hat man also bereits über 1000, bei 20 schon über eine Million und bei 50 schon eine Billiarde Zeilen.[3] Wenn nun aber z.B. das Muster $F \vee \neg F$ in vorliegt, so kann man *ohne jede Kenntnis* des Aussehens von F, sagen, dass hier eine Tautolgie vorliegt. F wird nämlich (unabhängig von seinem Aussehen, bzw. seines Aufbaus, F könnte z.B. $A \vee B$ sein oder $A \Rightarrow (B \wedge C)$, eben ganz allgemein irgendeine Formel) von einer Belegung entweder zu 0 oder 1 ausgewertet. $\neg F$ dann jeweils zum Gegenteil und damit wird immer F oder $\neg F$ zu 1 ausgewertet und die Disjunktion ist damit stets wahr. Treten in F nun bspw. 10 Aussagesymbole auf, so hätten wir bereits eine Wahrheitstafel mit $2^{10} = 1024$ Zeilen. Statt diese zu erstellen und zu prüfen, dass in jeder Zeile $F \vee \neg F$ zu 1 ausgewertet wird, ist es schneller und einfacher aus dem vorliegenden syntaktischen Muster zu schließen, dass eine Tautologie vorliegt.

Trotzdem wäre es im Prinzip stets möglich eine Wahrheitstafel zu erzeugen, auch wenn dies recht aufwendig werden kann. Ein weiterer (und wichtigerer) Vorteil der Ableitungsmethode ist aber, dass in anderen Logiken als der Aussagenlogik die Wahrheitstafelmethode *gar nicht mehr durchführbar ist*, weil die Wahrheitstafel nämlich unendlich gross und damit nicht mehr erstellt werden kann! In diesen Logiken ist es aber meist möglich Ableitungen zu definieren und damit ein Werkzeug in der Hand zu haben, um z.B. Tautologien nachzuweisen und allgemein, ohne eine Wahrheitstafel und nur mit syntaktischen Mitteln, Rückschlüsse auf die semantischen Eigenschaften einer Formel zu ziehen. Um dies an einer einfacheren Logik einzuüben (und auch da die Aussagenlogik wie schon gesagt als Teil der meisten anderen Logiken auftritt), lohnt es sich, Ableitungen schon für die Aussagenlogik zu definieren.[4]

---

[2] Hat eine Formel n Aussagesymbole, so kann jedes von ihnen zu 0 oder 1 ausgewertet werden, d.h. für jedes gibt es zwei Möglichkeiten. Kombinatorisch ergibt sich dann, dass man insgesamt 2^n Möglichkeiten hat die Aussagesymbole mit Wahrheitswerten zu belegen. Eine andere Sichtweise ist, dass in der ersten Zeile der Wahrheitstafel alle Aussagesymbole zu 0, in der letzten alle zu 1 ausgewertet werden. Man "zählt" also sozusagen binär von $00\ldots0$ bis $11\ldots1$, was genau 2^n Zahlen sind.

[3] Und eine Formel(-menge) mit 50 verschiedenen Aussagesymbolen ist nicht so selten, wie man vielleicht zuerste denken mag. Man denke hier wieder an das Beispiel der Systemmodellierung. 50 Eigenschaften in einem System modellieren zu wollen ist gar nicht so abwegig.

[4] Wem das jetzt immer noch nicht als Motivation reicht, dem kann ich nur sagen, "Sorry, aber irgendwer hat sich mal ausgedacht, dass man das FGI-1-Modul bestanden haben muss,

2 Grundlagen

Unser Ziel ist es rein aus den syntaktischen Eigenschaften von Formeln auf andere Formeln und letztendlich auf semantische Eigenschaften zu schliessen. Im vorherigen Abschnitt hatten wir schon die Formel $F \vee \neg F$ als Beispiel, die unabhängig davon, was F genau ist, eine Tautologie ist. Kennen wir noch weitere Muster? $F \wedge \neg F$ wäre vielleicht ein weiteres. Dieses ist unabhängig von F eine Kontradiktion. Spannender - und nützlicher - wird das Ganze, wenn wir aus Formeln andere Formeln *ableiten*. Damit meinen wir, dass wir aus Mustern, die wir in *gegebenen* Formeln finden, eine *neue* Formel herleiten können. Um dies zu verstehen, ist es nützlich sich klar zu machen, dass eine gegebene Formel oder eine schon abgeleitete Formel als *wahr* angesehen wird. Man muss hier etwas aufpassen, da man mit Wahrheit ja im Prinzip auf semantischer Ebene argumentiert, dennoch läuft das, was später *getan* wird, auf rein syntaktischer Ebene ab. Ein Beispiel soll dies verdeutlichen. Haben wir z.B. die Formel $F \Rightarrow G$ und die Formel F gegeben, so heißt dies, dass wir diese Formeln als wahr annehmen dürfen.[5] Dann können wir aber schlussfolgern, dass auch G wahr sein muss! Zur Begründung schaue man sich die Wahrheitstafel an. Die Belegung, die F und $F \Rightarrow G$ wahr macht, macht auch G wahr. Es gibt gar keine andere Möglichkeit für G, als wahr zu sein. Ohne Kenntnis der inneren Struktur von F und G konnten wir also allein aus dem Muster $F \Rightarrow G$, F (*beide* Formeln gehören zum Muster!) darauf schließen, dass G wahr sein muss. Was wir hier gemacht haben, ist nichts anderes als den *Modus Ponens*

$$\frac{F,\ F \Rightarrow G}{G}$$

anzuwenden, eine der *Inferenzregeln*, die wir im nachfolgenden noch kennenlernen werden. Daran, dass wir F und $F \Rightarrow G$, die sogenannten *Prämissen* (G wird als *Konklusion* bezeichnet), zur Erläuterung als wahr angenommen haben, sollte man sich erstmal nicht stören. Wir kommen später darauf zurück. Zunächst merken wir uns einfach, dass Formeln, die gegeben sind, bzw. in der Ableitung auftreten, "wahr" sind. Wir werden diese (semantische) Wahrheit lediglich für Erläuterungen nutzen, um den Sinn (und die Sinnhaftigkeit) des Verfahrens zu erklären. Sie wird nicht im Verfahren (während der Ableitung) genutzt, das Ableiten selbst bleibt also ein rein syntaktisches Verfahren!

Wenn man nun also zwei beliebig komplizierte Formeln, wie z.B.

$$((A \Rightarrow B) \vee (C \wedge \neg A)) \Rightarrow (C \wedge (A \vee \neg(B \Rightarrow C))), (A \Rightarrow B) \vee (C \wedge \neg A)$$

gegeben hat (und weiss, dass diese wahr sind), so kann man versuchen obiges Muster, also F und $F \Rightarrow G$ in ihnen wiederzufinden. Hier ist es tatsächlich

wenn man den Abschluss machen will!" - Also: Augen zu und durch! Ist auch alles nicht so schlimm.... wirklich!

[5] Man nehme dies erstmal so hin. Wenn F eine Kontradiktion ist, dann geht das ja eigentlich gar nicht, wir gehen jetzt aber erstmal davon aus, dass uns irgendjemand zwei Formeln $F \Rightarrow G$ und F gibt, uns über deren internen Aufbau nichts sagt (F und G können, wie im vorherigen Abschnitt bei $F \vee \neg F$ erläutert, wieder ganz beliebige, komplexe Formeln sein), aber uns versichert, dass sie wahr sind.

vorhanden:

$$\underbrace{\overbrace{((A \Rightarrow B) \vee (C \wedge \neg A))}^{F} \Rightarrow \overbrace{(C \wedge (A \vee \neg(B \Rightarrow C)))}^{G}}_{F \Rightarrow G}, \underbrace{(A \Rightarrow B) \vee (C \wedge \neg A)}_{F}$$

und man kann G ableiten. (Man beachte, dass eine Wahrheitstafel hier ganz schön Arbeit gewesen wäre - wenn auch mehr wegen der Vielzahl an Teilformeln als wegen der Anzahl der Aussagensymbole.)

In den nachfolgenden Unterabschnitten wollen wir formale Begrifflichkeiten einführen, die wir benötigen werden, um anschließend (in Abschnitt 3) den Begriff der Ableitung formal zu fassen.

2.1 Substitutionen

Wir wollen uns zunächst daran machen die "Mustererkennung" zu formalisieren. Im vorherigen Abschnitt haben wir an einem Beispiel gezeigt, wie das Muster F, $F \Rightarrow G$ in zwei Formeln gefunden werden kann. Es stellt sich sogleich die Frage, ob und falls ja wie man dies verallgemeinern kann? Wir haben zwar z.B. gesagt, dass $((A \Rightarrow B) \vee (C \wedge \neg A))$ dem F in der Prämisse der Inferenzregel entspricht, aber wenn wir dies versuchen so herum zu definieren, dann wird es schwierig dies mathematisch auszudrücken.[6] Einfacher ist es zu sagen, dass man *in der Prämisse* F und G durch Formeln ersetzt und dass *dadurch* Formeln entstehen müssen, die man bereits hat. Dies erreicht man durch sogenannte Substitutionen. Dies sind Abbildungen, die Aussagensymbole auf Formeln abbilden und dann auf komplexere Formeln erweitert werden, indem man im Prinzip lediglich sagt, dass sie nur auf die Aussagensymbole wirken und Junktoren und Klammern ignorieren. Definiert man sich z.B. eine Substitution sub mittels $sub(A) = D \vee E$ und $sub(B) = D \wedge \neg E$ so wird aus $A \Rightarrow B$ durch Anwendung der Substitution $sub(A \Rightarrow B) = (D \vee E) \Rightarrow (D \wedge \neg E)$, es wird also überall in der Formel A durch $sub(A)$ und B durch $sub(B)$ ersetzt. Mitels einer induktiven Definition kann man dies exakt definieren, der Sinn sollte aber auch so klar geworden sein und wir wollen es dabei belassen.

Zurück zu unserem Beispiel kann man also eine Substituion mittels

$$\begin{aligned} sub(F) &= ((A \Rightarrow B) \vee (C \wedge \neg A)) \\ sub(G) &= (C \wedge (A \vee \neg(B \Rightarrow C))) \end{aligned}$$

definieren und hat so eine Substituion derart, dass diese Substituion angewendet auf die Prämissen der Inferenzregel (also auf F und $F \Rightarrow G$) zu zwei Formeln führt, die gegeben (bzw. später: "bereits abgeleitet") sind. Darum können wir dann die Formel ableiten, die wir erhalten, wenn wir *diese* Substituion auf die Konklusion anwenden.[7] Wir kommen hierauf in Abschnitt 3 noch einmal näher zu sprechen.

[6] Wer möchte kann dies versuchen. Man müsste irgendwie Teilformeln so auf F und G abbilden, dass man die Prämisse erzeugt. Für einzelne Beispiele, kann man das natürlich definieren, aber wie definiert man das so, dass es allgemein gilt?

[7] Eine andere Sichtweise wäre es die Inferenzregel ein weiteres Mal hinzuschreiben, aber

2.2 Exkurs: Zum Begriff der Wahrheit in Ableitungen

Weiter oben wurde mehrfach gesagt, dass wir bei den gegebenen Formeln einfach davon ausgehen, dass sie wahr sind. Es sollte aber an dem Beispiel mit dem Modus Ponens klar geworden sein, dass dies Wahrheit nirgends ausgenutzt wird, sondern lediglich zur Erklärung diente. Da man mit Ableitungen versucht auf die semantischen Eigenschaften von Formeln zu schließen, hatte man natürlich auch die Semantik im Hinterkopf, als man sich diese Methode ausgedacht hat. Dennoch bleiben Ableitungen ein rein syntaktisches Verfahren.

Das Ziel, dass man mit Ableitungen verfolgt ist es, aus einer gegebenen Formelmenge M eine Formel F abzuleiten, notieren tut man dies mittels $M \vdash F$. Man will nun, und darauf sind die Inferenzregeln ausgerichtet, erreichen, dass $M \vdash F$ genau dann gilt, wenn $M \models F$ gilt. Es macht daher Sinn bei den gegebenen Formeln in M davon auszugehen, dass sie wahr sind (und dann syntaktisch mit ihnen zu arbeiten), denn wenn man - nun nicht syntaktisch, sondern semantisch - $M \models F$ nachweisen will, so muss man zeigen, dass alle Belegungen, die alle Formeln in M wahr machen, auch F wahr machen. Hier interessiert man sich also auch nur für die Belegungen, die die Formeln in M wahr machen.[8]

Stellt man sich M als die Menge der Formeln vor, von denen man weiss, dass sie wahr sind, dann kann man nun F in diese Menge aufnehmen und ggf. mit ihrer Hilfe weitere Formeln ableiten. Dies ist genau das, was passiert, wenn man weiter ableitet und nun auch F in der Ableitung benutzt (nachdem man $M \vdash F$ gezeigt hat).

Die *korrekten* Inferenzregeln sind alle so gewählt, dass sie die Beziehung “$M \vdash F$ gdw. $M \models F$” nicht gefährden, d.h. sie sind so gewählt, dass sie auch semantisch Sinn machen; soll heissen: Sie stehen nicht im Widerspruch zur (semantischen) Folgerbarkeitsbeziehung. Dazu mehr im nächsten Abschnitt.

2.3 Korrekte Inferenzregeln

Inferenz- oder Ableitungsregeln haben die Form

$$\frac{F_1, \dots, F_n}{G}.$$

Wir haben also eine Ansammlung von n Formeln F_1 bis F_n in der Prämisse und eine Formel G als Konklusion. Zunächst kann man sich da nun beliebig

überall (in Prämisse und Konklusion) F und G durch $sub(F)$ bzw. $sub(G)$ zu ersetzen. Liegen dann die Formeln der (substituierten) Prämisse vor, dann darf die (substituierte) Konklusion abgeleitet werden.

[8] Das wir uns hier auf den Fall $M \vdash F$ bzw. $M \models F$ beschränken, also auf den Fall rein unter Berücksichtigung der Syntax Aussagen über die (semantische) Folgerbarkeitsbeziehung zu machen, ist keine Einschränkung, da man mit $M = \emptyset$ auch Aussagen darüber treffen kann, ob eine Tautologie vorliegt. F ist nämlich genau dann eine Tautologie, wenn $\emptyset \models F$ gilt. Daraus folgt, dass F auch dann eine Tautologie ist, wenn wir F aus der leeren Menge ableiten können. (Ähnlich kann man, um zu überprüfen ob F eine Kontradiktion ist, prüfen, ob $\neg F$ eine Tautologie ist.) Eine Formel aus der leeren Menge abzuleiten ist uns hier (in FGI-1) nur im Hilbertkalkül möglich, da wir ansonsten noch weitere Inferenzregeln benötigen würden.

viele Regeln vorstellen. Bedenkt man jedoch, dass wir aus einer Menge M nur Formeln F ableiten können wollen, die wir auch (semantisch) folgern können, dann müssen wir aufpassen.

Hat man nämlich z.B. die Regel $\frac{A \wedge B}{\neg A}$, so kann man aus der Formel $A \wedge B$ (bzw. jeder Menge die diese Formel enthält oder eine Formel nach diesem Muster) plötzlich $\neg A$ ableiten. Hier gilt aber die Folgerbarkeitsbeziehung nicht![9]

Wenn man aber nur Regeln zulässt bei denen die Konklusion aus der Prämisse *semantisch folgt*, so hat man keine Probleme (warum folgt gleich). Wir definieren daher, dass eine Inferenzregel wie oben korrekt ist genau dann, wenn $\{F_1, \dots, F_n\} \models G$ gilt. Warum genügt dies? Weil ganz allgemein aus $M \models G$, auch $sub(M) \models sub(G)$ folgt (für jede Substitution sub)[10], d.h. haben wir eine korrekte Inferenzregel und wenden diese an, dann gibt es ja eine Substitution sub derart, dass $sub(F_1), \dots, sub(F_n)$ schon gegeben sind (man denke an obiges Beispiel mit dem Modus Ponens). Wir dürfen dann $sub(G)$ ableiten. $sub(G)$ folgt nach obigen (mit $M = \{F_1, \dots, F_n\}$) dann aber auch aus $sub(F_1), \dots, sub(F_n)$.

Ist also eine Inferenzregel gegeben und soll diese auf Korrektheit geprüft werden, ist lediglich zu zeigen, dass die Konklusion aus der Prämisse folgt. Dies geht recht schnell mit Wahrheitstafeln. Will man zeigen, dass eine Inferenzregel nicht korrekt ist, reicht ein Gegenbeispiel, d.h. eine Belegung, die alle Formeln der Prämisse wahr, aber die Konklusion falsch macht.

3 Ableitungen und Kalküle

Nun haben wir alles, was wir benötigen, um Ableitungen sauber zu definieren. Tatsächlich wurde (fast) alles auch bereits erwähnt, so dass in diesem Abschnitt alles nur noch einmal zusammengetragen und an einem Beispiel erläutert wird.

Ableitungen finden streng genommen in einem Kalkül statt. Man kann zwar definieren, wie man mit einer Inferenzregel arbeitet, aber die Ableitung als ganzes findet in einem Kalkül statt. Der Kalkül gibt dabei u.a. an, welche Inferenzregeln in der Ableitung benutzt werden dürfen. Genauer ist ein Kalkül $\mathcal{C}$ ein Tripel $\mathcal{C} = (\mathcal{L}, Ax, \mathcal{R})$ bestehen aus der Sprache $\mathcal{L}$, einer Menge von Axiomen Ax und einer Menge von Inferenzregeln $\mathcal{R}$. Die Sprache gibt an, wie die Formeln aussehen, mit denen wir arbeiten. Hier ist die dies Menge der aussagenlogischen Formeln. Die Axiome sind Formeln (es gilt also $Ax \subseteq \mathcal{L}$), die als gültig gegeben sind (sie unterscheiden sich noch geringfügig von den Formeln, bei denen wir oben von "gegeben" gesprochen haben, wir kommen darauf gleich zurück). Die Inferenzregeln sind die (korrekten) Inferenzregeln, die in der Ableitung benutzt werden dürfen. Leitet man nun aus einer gegebenen Menge M von Formeln (M darf dabei auch leer sein) eine Formel F im Kalkül $\mathcal{C}$ ab, so notiert man dies als $M \vdash_{\mathcal{C}} F$. Bei einer Ableitung darf man drei Dinge tun:

- Man darf eine Formel aus M in die Ableitung aufnehmen.

[9] $\mathcal{A}(A) = \mathcal{A}(B) = 1$ macht die Prämisse $A \wedge B$ wahr, nicht aber $\neg A$.

[10] Siehe dazu den Beweis dafür, dass $\models sub(F)$ von $\models F$ impliziert wird. Die Aussage hier lässt sich ähnlich beweisen. Man darf das hier aber auch einfach erstmal glauben.

- Man darf ein Axiom $H \in Ax$ und eine (beliebige!) Substitution sub nehmen und die Formel $sub(H)$ in die Ableitung aufnehmen.
- Man darf eine Inferenzregel anwenden. Die dabei gewonnen (d.h. abgeleitete) Formel, darf man in die Ableitung aufnehmen.

Auf den dritten Punkt gehen wir gleich noch näher ein. Zunächst beachte man den Unterschied im ersten und zweiten Punkt. Die Formeln aus M darf man nur so wie sie gegeben sind in die Ableitung aufnehmen.[11] Auf die Axiome hingegen darf man eine Substitution anwenden und die dann gewonnene Formel in die Ableitung aufnehmen.[12]

Der dritte Punkt (Anwendung einer Inferenzregel) lässt sich wie folgt formalisieren: Sei $\frac{F_1,\ldots,F_n}{G}$ eine Inferenzregel. Wenn es eine Substituion sub gibt derart, dass $sub(F_1),\ldots,sub(F_n)$ schon in der Ableitung auftreten, dann darf $sub(G)$ in die Ableitung aufgenommen werden. Man notiert dies, indem man dort, wo man $sub(G)$ in die Ableitung aufnimmt, angibt mit welcher Inferenzregel dies geschah, welche Substituion benutzt wurde und wo die Formeln in der Ableitung sind, die $sub(F_1)$, $sub(F_2)$ usw. entsprechen. Im gleich folgenden Beispiel wird dieses Vorgehen verdeutlicht. Zunächst wollen wir nocheinmal ausführen, was gewonnen ist, wenn man $M \vdash_{\mathcal{C}} F$ gezeigt hat. Gegeben ist also eine Menge M von Formeln. Mit diesen Formeln hat man z.B. Systemeigenschaften modelliert. Diese Formeln werden semantisch als wahr angenommen. Ferner sind im Kalkül $\mathcal{C}$ vielleicht Axiome gegeben. Diese stellen tautologische Aussagen wie z.B. $A \Rightarrow A$ da und können ohne Bedenken benutzt werden.[13] Leitet man nun F aus M ab, so gilt (sofern alle Inferenzregeln korrekt sind und insb. auch der Kalkül korrekt ist, etwas worauf wir hier nicht näher eingehen wollen) auch $M \models F$ und wir wissen, dass F wahr ist, wenn die Formeln in M wahr sind. Drückt F eine gewünschte Eigenschaft des Systems aus (z.B. die Möglichkeit den Ablauf zu stoppen), so können wir nun sagen, dass diese gegeben ist.

Kommen wir nun zu einem kleineren Beispiel, dass das Ableiten illustrieren soll.[14]

Wir verzichten vorerst auf Axiome und nehmen in unseren Kalkül die Regeln DS, MP und DE auf, d.h. die Regeln $\frac{\neg B,\, A\vee B}{A}$, $\frac{\neg A,\, A\vee B}{B}$ für DS (zwei Regeln!), die Regel $\frac{A,\, A\Rightarrow B}{B}$ für MP und die Regeln $\frac{A}{A\vee B}$, $\frac{B}{A\vee B}$ für DE. Die Sprache ist die der Aussagenlogik. Wir wollen nun folgendes (in diesem Kalkül) beweisen:

$$\{\neg(A \vee D), B \Rightarrow C, (A \vee D) \vee B\} \vdash A \vee C,$$

[11]Wenn man mit diesen z.B. Systemeigenschaften modelliert, dann soll man an den Formeln nicht noch mit Substitutionen herumspielen dürfen.

[12]Begründung hierfür: Ein Axiom wird als “immer wahr” angesehen, also als tautologisch, ist F eine Tautologie, so auch $sub(F)$ und Dinge, die immer gelten, darf man aufnehmen, ohne dass man Gefahr läuft nun falsche Eigenschaften des Systems nachzuweisen.

[13]Im Prinzip kürzt man mit ihnen den Beweis nur ab, da Tautologien aus der leeren Menge beweisbar sind und man daher den Beweis für sie an beliebiger Stelle in die Ableitung einbauen könnte.

[14]Wer sich noch unsicher fühlt: Es lohnt sich hier einfach einen Stift in die Hand zu nehmen und dies auf einem Blatt Papier Schritt für Schritt mitzumachen. Keine Ahnung warum genau, aber durch die Tätigkeit mit dem Stift geht das besser in den Kopf und man versteht es viel leichter, als wenn man nur die gleich folgende Buchstabenwüste liest.

d.h. wir wollen die Formel $A \vee C$ aus der Formelmenge $\{\neg(A \vee D), B \Rightarrow C, (A \vee D) \vee B\}$ ableiten und dürfen dabei die obigen Inferenzregeln benutzen. Zunächst sieht man, dass die erste und die dritte Formel ähnlich aufgebaut sind wie die Prämissen der zweiten DS Regel, d.h. dieses Muster liegt hier vor. Nehmen wir $sub(A) = (A \vee D)$ und $sub(B) = B$, so erhalten wir mit $sub(\neg A) = \neg sub(A)$ und $sub(A \vee B) = sub(A) \vee sub(B)$, d.h. indem wir die Substituion auf die Prämissen der Infernzregel anwenden, zwei Formeln, die in M enthalten sind, wir können also $sub(B) = B$ (die Substitution angewendet auf die Konklusion der Inferenzregel) ableiten. Streng genommen müssen wir vorher die beiden Formeln aus der gegebenen Formelmenge in die Ableitung aufnehmen. In der unten folgenden schrittweisen Ausführung der Ableitung geschieht dies auch. Wenn wir nun B haben, dann schreit dieses und das $B \Rightarrow C$ förmlich nach der Anwendung des Modus Ponens. Dadurch gelangt man zu C (die nötige Substitution ist $sub(A) = B$ und $sub(B) = C$, dadurch erreicht man wieder, dass die Formeln, die man erhält, wenn man diese Substitution auf die Formeln der Prämisse der Inferenzregel anwendet, schon in der Ableitung auftreten). Zuletzt gelangt man durch Anwendung der zweiten DE Regel zu $A \vee C$. Im einzelnen sieht eine mögliche Ableitung wie folgt aus (mit M sei dabei die gegebene Formelmenge bezeichnet):

Nr	Formel	Begründung
(1)	$\neg(A \vee D)$	aus M
(2)	$(A \vee D) \vee B$	aus M
(3)	B	(1), (2), $DS2$, $sub(A) = (A \vee D), sub(B) = B$
(4)	$B \Rightarrow C$	aus M
(5)	C	(3), (4), MP, $sub(A) = B, sub(B) = C$
(6)	$A \vee C$	(4), (5), $DE2$, $sub(A) = A, sub(B) = C$

Dieses Beispiel ist noch recht übersichtlich, insb. kann man gut schon an der Formelmenge M sehen, was man tun kann. In anderen Fällen ist es meist nützlich “von unten” anzufangen (also sich vom Ziel aus zu fragen, wie man hier wohl hingelangen kann; meist ist eine Kombination von beidem nötig). Wir illustrieren dies an einem schwierigeren Beispiel. Hier wollen wir den Kalkül $\mathcal{C} = (\mathcal{L}_{AL}, \{H_8\}, \{KE, MP, MT\})$ benutzen. Die Sprache ist also die der Aussagenlogik, wir haben ein Axiom $H_8 = \neg\neg A \Rightarrow A$ und die drei Regeln Konjunktionseinführung $\frac{A,B}{A \wedge B}$, Modus Ponens $\frac{A,\, A \Rightarrow B}{B}$ und Modus Tollens $\frac{\neg B,\, A \Rightarrow B}{\neg A}$. Wir wollen in diesem Kalkül $B \wedge C$ aus $\{\neg\neg C, \neg B \Rightarrow \neg C\}$ ableiten. Wie hilft uns nun der Ansatz “von unten” vorzugehen? Wir haben $B \wedge C$ als Ziel. Betrachten wir die zur Verfügung stehenden Inferenzregeln, so ist die einzige Möglichkeit ein und ($\wedge$) einzuführen die Regel KE (bei diesem Vorgehen betrachtet man zunächst nur die Konklusionen der Inferenzregeln!), die letzte benutze Regel wird also KE sein. Um diese zu benutzen müssen wir aber vorher bereits B und C abgeleitet haben. Wenn wir ein C ableiten wollen, so kann dies höchstens durch den Modus Ponens passieren (die anderen beiden Regeln haben noch Junktoren in der Konklusion). Betrachtet man aber die Prämisse des Modus Ponens, so sieht man, dass dazu C auch auf der rechten Seite einer Implikation vorkommen müsste. Da in der gegebenen Formelmenge C nur in negierter Form auftritt, ist dies nicht möglich. Es sieht aus als wären wir in einer Sackgasse. Hier hilft uns nun aber das Axiom! Ersetzen wir in diesem A durch C erhalten wir $\neg\neg C \Rightarrow C$ (und schon tritt C doch auf der rechten Seite einer Implikation auf). Wir könnten nun mittels des Modus Ponens an das C herankommen (d.h. es ableiten), wenn wir $\neg\neg C$ hätten. Dies ist in der Formelmenge gegeben! So können wir C ableiten. An B heranzukommen geht mit einem ähnlichen Ansatz. Wir haben aber kein $\neg\neg B$, hätten wir dies, könnten wir wieder mit dem MP (und dem Axiom) B herleiten. Wir haben in M aber nur eine Formel in der $\neg B$ auftritt. Ein Blick auf die Inferenzregeln gibt aber Anlass zur Hoffnung: Mit MT können wir eine Negation einführen. Ersetzt man in MT B durch $\neg C$ und A durch $\neg B$, so erhalten wir in der Prämisse die beiden Formeln der gegebenen Menge und können $\neg\neg B$ ableiten. Mit dem eben gesagten sind wir dann fertig. Im einzelnen:

Nr	Formel	Begründung
(1)	$\neg\neg C$	aus M
(2)	$\neg B \Rightarrow \neg C$	aus M
(3)	$\neg\neg B$	(1), (2), MT mit $sub(B) = \neg C$, $sub(A) = \neg B$
(4)	$\neg\neg B \Rightarrow B$	H_8 mit $sub(A) = B$
(5)	B	(3), (4), MP mit $sub(A) = \neg\neg B$, $sub(B) = B$
(6)	$\neg\neg C \Rightarrow C$	H_8 mit $sub(A) = C$
(7)	C	(1), (6), MP mit $sub(A) = \neg\neg C$, $sub(B) = C$
(8)	$B \wedge C$	(5), (7), KE mit $sub(A) = B$, $sub(B) = C$