

FGI-1 – Formale Grundlagen der Informatik I

Logik, Automaten und Formale Sprachen

Musterlösung 10: Ableitungen

Präsenzteil am 16.-19. Juni – Abgabe am 23.-26. Juni 2015

Präsenzaufgabe 10.1: Sei M eine Formelmenge und F eine Formel. Zeigen Sie, dass F genau dann aus M folgt, wenn $M \cup \{\neg F\}$ unerfüllbar ist (also $M \models F$ gdw. $M \cup \{\neg F\}$ unerfüllbar).

Lösung: Gelte $M \models F$ und sei \mathcal{A} eine Belegung, die alle Formeln in M wahr macht (tut \mathcal{A} dies nicht, so kann sie $M \cup \{\neg F\}$ bereits nicht mehr erfüllen). Wegen $M \models F$ gilt dann auch $\mathcal{A}(F) = 1$ und damit $\mathcal{A}(\neg F) = 0$. Damit wird $M \cup \{\neg F\}$ von \mathcal{A} nicht erfüllt und mit obiger Anmerkung ist $M \cup \{\neg F\}$ damit unerfüllbar.

Sei nun umgekehrt $M \cup \{\neg F\}$ unerfüllbar. Wir wollen $M \models F$ zeigen. Sei \mathcal{A} eine Belegung, die alle Formeln in M wahr macht. Da $M \cup \{\neg F\}$ unerfüllbar ist, muss dann $\mathcal{A}(\neg F) = 0$ gelten (sonst würde \mathcal{A} alle Formeln in $M \cup \{\neg F\}$ erfüllen) und folglich gilt $\mathcal{A}(F) = 1$. Damit ist dann $M \models F$ gezeigt.

Präsenzaufgabe 10.2:

1. Gegeben sei die Substitution sub mit $sub(A) = B \Rightarrow C$, $sub(B) = D \vee E$ und $sub(C) = sub(D) = D$. Bestimmen sie $sub(F)$ für $F = (A \Leftrightarrow C) \vee B$.
2. Seien $F = (A \Rightarrow B) \vee (\neg C \wedge A)$ und $G = ((A \vee C) \Rightarrow (D \vee A)) \vee (\neg \neg D \wedge B)$. Geben Sie eine Substitution sub an mit $sub(F) = G$ oder begründen Sie, warum dies nicht möglich ist.
3. Seien $F = (A \vee C) \Rightarrow (B \wedge E)$ und $G = (((D \vee C) \vee (E \Rightarrow B)) \Rightarrow (A \wedge B))$. Geben Sie eine Substitution sub an mit $sub(F) = G$ oder begründen Sie, warum dies nicht möglich ist.

Lösung:

1. Mit der angegebenen Substitution ist $sub(F) = ((B \Rightarrow C) \Leftrightarrow D) \vee (D \vee E)$.
2. Dies geht nicht. Man müsste A durch $(A \vee C)$ und durch B ersetzen, was nicht beides geht.
3. Mit $sub(A) = D \vee C$, $sub(B) = A$, $sub(C) = E \Rightarrow B$ und $sub(E) = B$ gilt $sub(F) = G$.

Präsenzaufgabe 10.3:

1. Zeigen oder Widerlegen Sie, dass die folgenden Inferenzregeln korrekt sind:

$$\frac{\neg B, A \vee B}{A} \quad \frac{\perp}{A} \quad \frac{A \vee \neg B, A \Rightarrow B}{A}$$

2. Sei $\mathcal{C} = (\mathcal{L}_{AL}, Ax, \mathcal{R})$ ein Kalkül der Aussagenlogik mit $Ax = \{A \Rightarrow (B \Rightarrow A)\}$ und $R = \{\frac{F, F \Rightarrow G}{G}, \frac{F \wedge G}{G}\}$. Sei ferner $M = \{A \wedge B, (C \Rightarrow (A \wedge B)) \Rightarrow (B \wedge A)\}$.

Zeigen Sie $M \vdash_{\mathcal{C}} A$ durch Angabe einer Ableitung.

Lösung:

1. Wir arbeiten teilweise mit Wahrheitstafeln und teilweise ohne.

- Dies ist der Modus Tollens. Die Regel ist korrekt:

A	B	$\neg B$	$A \vee B$
0	0	1	0
0	1	0	1
1	0	1	1
1	1	0	1

Die Prämissen sind in der dritten Zeile wahr (und nur da). Dort ist auch A wahr. Daher gilt die Folgerbarkeitsbeziehung $\{\neg B, A \vee B\} \models A$ und die Regel ist korrekt.

- Das Symbol \perp haben wir im Kapitel über die Hornformeln eingeführt. Für jede Belegung \mathcal{A} gilt $\mathcal{A}(\perp) = 0$. Damit gilt $\perp \models A$ sofort, da es keine Belegung gibt, die die linke Seite wahr macht. Damit ist die Regel korrekt. (Sie sagt im Prinzip, dass man aus einem Widerspruch etwas Beliebiges ableiten darf.)
 - Diese Regel ist nicht korrekt. Beispielsweise ist \mathcal{A} mit $\mathcal{A}(A) = \mathcal{A}(B) = 0$ eine Belegung, die $A \vee \neg B$ und $A \Rightarrow B$ wahr macht, nicht aber A . Damit gilt die Folgerbarkeitsbeziehung nicht, die für die Korrektheit der Regel gelten müsste.
2. Leider kommen wir nicht direkt von $A \wedge B$ an das A heran, weil wir nur die Regel $\frac{F \wedge G}{G}$ haben. Wir machen das deshalb umständlicher:

- | | | |
|-----|--|---|
| (1) | $M \vdash (A \wedge B) \Rightarrow (C \Rightarrow (A \wedge B))$ | mit $sub(A) = A \wedge B$ und $sub(B) = C$ im Axiom |
| (2) | $\vdash A \wedge B$ | aus M |
| (3) | $\vdash C \Rightarrow (A \wedge B)$ | mit (1),(2), MP und
$sub(F) = A \wedge B, sub(G) = C \Rightarrow (A \wedge B)$ |
| (4) | $\vdash (C \Rightarrow (A \wedge B)) \Rightarrow (B \wedge A)$ | aus M |
| (5) | $\vdash B \wedge A$ | mit (3),(4), MP und
$sub(F) = (C \Rightarrow (A \wedge B)), sub(G) = (B \wedge A)$ |
| (6) | $\vdash A$ | mit (5), KL2 und $sub(F) = B, sub(G) = A$ |

Übungsaufgabe 10.4: Beweisen Sie, dass eine Inferenzregel $R = \frac{F_1, \dots, F_n}{G}$ genau dann korrekt ist, wenn $\{F_1, \dots, F_n\} \models G$ gilt. (Nutzen Sie dazu, die Definition der Korrektheit einer Inferenzregel auf Folie 31.)

VON
2

Lösung: Wir zeigen zunächst, dass $\{F_1, \dots, F_n\} \models G$ aus der Korrektheit einer Inferenzregel $R = \frac{F_1, \dots, F_n}{G}$ folgt. Diese Richtung ist relativ einfach. Nach der Definition der Korrektheit einer Inferenzregel gilt für alle Mengen M und Formeln H : Wenn $M \vdash_R H$, dann $M \models H$. Wir setzen $M := \{F_1, \dots, F_n\}$. Nun gilt mit der Substitution sub mit $sub(A) = A$ für alle Aussagensymbole $sub(\{F_1, \dots, F_n\}) = \{F_1, \dots, F_n\} \subseteq \{F_1, \dots, F_n\} = M$, d.h. R kann auf M angewendet werden und $sub(G)$ ist ableitbar. Nun ist aber $sub(G) = G$ und wir haben also $\{F_1, \dots, F_n\} \vdash_R G$ woraus aufgrund der Korrektheit der Inferenzregel $\{F_1, \dots, F_n\} \models G$ folgt.

Die Rückrichtung ist komplizierter. Gelte also $\{F_1, \dots, F_n\} \models G$. Wir wollen zeigen, dass die Inferenzregel $R = \frac{F_1, \dots, F_n}{G}$ korrekt ist. Sei dazu M eine Formelmenge und H eine Formel mit $M \vdash_R H$. Wir wollen $M \models H$ zeigen, dass also jede Belegung, die alle Formeln aus M erfüllt auch H erfüllt.

Zunächst wissen wir wegen $M \vdash_R H$, dass H mit R direkt aus M ableitbar ist. Dazu muss $sub(\{F_1, \dots, F_n\}) \subseteq M$ gelten und $sub(G) = H$ sein (nach Definition der Anwendung einer Inferenzregel). Wir zeigen nun zwei Dinge:

1. Es gilt $sub(\{F_1, \dots, F_n\}) \models sub(G)$. Dies folgt aus $\{F_1, \dots, F_n\} \models G$, denn damit gilt für jede Substitution sub auch $sub(\{F_1, \dots, F_n\}) \models sub(G)$. (Letzteres kann man direkt (ähnlich wie beim Satz, dass $\models sub(F)$ aus $\models F$ folgt) zeigen oder indem man benutzt, dass $N = \{I_1, \dots, I_k\} \models I$ genau dann gilt, wenn $I_1 \wedge \dots \wedge I_k \models I$ gilt, was wiederum genau dann gilt, wenn $\models (I_1 \wedge \dots \wedge I_k) \Rightarrow I$ gilt. Dann folgt die Aussage direkt aus dem Satz, dass $\models sub(F)$ aus $\models F$ folgt.)
2. Gilt $N \models I$, so gilt auch $N' \models I$ für jede Menge $N' \supseteq N$. Dies folgt daraus, dass jede Belegung, die alle Formeln in N' erfüllt auch alle Formeln in N erfüllt.

Mit 1. gilt also $sub(\{F_1, \dots, F_n\}) \models sub(G)$ und wegen 2. können wir mit $M \supseteq sub(\{F_1, \dots, F_n\})$ auch $M \models sub(G) = H$ folgern, was zu zeigen war. (Anmerkung: Mit 1. und 2. oben zeigen wir eigentlich, dass wenn wir eine Substitution sub haben derart, dass wir $sub(\{F_1, \dots, F_n\})$ in einer Formelmenge X finden, dass wir aus dieser Formelmenge dann $sub(G)$ folgern können. Wir brauchen die Voraussetzung $M \vdash_R H$ also im Grunde genommen nur, damit wir wissen, dass M diese Eigenschaft tatsächlich hat!)

Übungsaufgabe 10.5:

VON
3

1. Seien $F = ((A \Leftrightarrow B) \wedge B \wedge \neg C)$ und $G = ((B \vee \neg C) \Leftrightarrow \neg C) \wedge \neg C \wedge \neg(B \vee \neg C)$. Geben Sie eine Substitution sub an mit $sub(F) = G$ oder begründen Sie, warum dies nicht möglich ist.
2. Zeigen Sie, dass für jede Formel F und jede Substitution sub gilt: Wenn F eine Tautologie ist, dann ist auch $sub(F)$ eine Tautologie. Vervollständigen Sie dazu den Beweis aus der Vorlesung. Führen Sie insb. die dort nicht ausgeführte strukturelle Induktion.

Lösung:

1. $sub(F) = G$ wird von sub mit $sub(A) = B \vee \neg C$, $sub(B) = \neg C$ und $sub(C) = B \vee \neg C$ erfüllt.
2. Wir wollen zeigen, dass wenn $\models F$ gilt, dass dann auch $\models sub(F)$ für jede Substitution sub gilt. Zum Beweis verfahren wir zunächst wie in der Vorlesung.

Seien A_1, \dots, A_n die in F vorkommenden Aussagensymbole und sei \mathcal{A} eine Belegung. Wir definieren eine neue Belegung \mathcal{A}' durch

$$\mathcal{A}'(A_i) := \mathcal{A}(sub(A_i)).$$

Dies ist möglich, da die A_i kontingent sind.

Wir zeigen nun, dass $\mathcal{A}'(F) = \mathcal{A}(sub(F))$ für jede Formel F und jede Substitution sub gilt, wenn die Belegung \mathcal{A}' wie oben definiert wird. Der Beweis gelingt mittels struktureller Induktion über den Aufbau von F .

Induktionsanfang. Für Aussagensymbole ist die Behauptung klar, da sie dann sofort aufgrund der Definition von \mathcal{A}' gilt: Sei $F = A$ ein Aussagesymbol, dann ist nach Definition $\mathcal{A}'(A) = \mathcal{A}(sub(A))$ und damit wie gewünscht $\mathcal{A}'(F) = \mathcal{A}(sub(F))$.

Induktionsannahme. Gelte die Behauptung für zwei Formeln F_1 und F_2 .

Induktionsschritt. Fall $F = \neg F_1$. Aufgrund der Induktionsannahme wissen wir zunächst $\mathcal{A}'(F_1) = \mathcal{A}(sub(F_1))$. Damit ist nach der Semantischen Definition von \neg und der Eigenschaft einer Substitutionsfunktion dann $\mathcal{A}'(F) = \mathcal{A}'(\neg F_1) = 1 - \mathcal{A}'(F_1) = 1 - \mathcal{A}(sub(F_1)) = \mathcal{A}(\neg sub(F_1)) = \mathcal{A}(sub(\neg F_1)) = \mathcal{A}(sub(F))$.

Fall $F = F_1 \vee F_2$. Es ist $\mathcal{A}'(F) = 1$ genau dann, wenn $\mathcal{A}'(F_1) = 1$ oder $\mathcal{A}'(F_2) = 1$ nach der semantischen Definition von \vee . Dies gilt aber nach Induktionsvoraussetzung genau dann, wenn $\mathcal{A}(sub(F_1)) = 1$ oder $\mathcal{A}(sub(F_2)) = 1$ ist, was wiederum nach Definition der Semantik von \vee genau dann gilt, wenn $\mathcal{A}(sub(F_1) \vee sub(F_2)) = 1$ gilt, was zuletzt wegen der Eigenschaften einer Substitutionsfunktion genau dann gilt, wenn $\mathcal{A}(sub(F_1 \vee F_2)) = 1$ also genau dann, wenn $\mathcal{A}(sub(F)) = 1$ gilt.

Die Fälle für \wedge , \Rightarrow und \Leftrightarrow verlaufen analog. Man braucht lediglich wie im Falls von \vee die semantische Definition des Junktors, die Induktionsannahme und dann erneut die semantische Definition des Junktors sowie die Eigenschaften von sub ausnutzen, um in allen drei Fällen zu $\mathcal{A}'(F) = \mathcal{A}(sub(F))$ zu kommen.

Nach dem Prinzip der strukturellen Induktion ist die Behauptung damit für alle aussagenlogischen Formeln gezeigt.

Da nun $\mathcal{A}'(F) = \mathcal{A}(sub(F))$ (für die Art und Weise wie \mathcal{A}' definiert wurde) nachgewiesen ist, folgt aus $\models F$ sofort $\mathcal{A}'(F) = 1$ und damit $\mathcal{A}(sub(F)) = \mathcal{A}'(F) = 1$ und damit ist $sub(F)$ ebenfalls eine Tautologie.

Übungsaufgabe 10.6:

von
7

1. Zeigen oder Widerlegen Sie, dass die folgenden Inferenzregeln korrekt sind:

$$\frac{A \Rightarrow B, B \Rightarrow A}{\neg B \vee A} \qquad \frac{(A \vee B) \Rightarrow C, \neg C \wedge \neg B}{A \vee B}$$

2. Sei $\mathcal{C} = (\mathcal{L}_{AL}, Ax, \mathcal{R})$ ein Kalkül der Aussagenlogik mit $Ax = \{A \Rightarrow (B \Rightarrow A)\}$ und $R = \{\frac{\neg G, F \Rightarrow G}{\neg F}, \frac{\neg G, F \vee G}{F}\}$. Sei ferner $M = \{A \vee C, \neg(E \Rightarrow C)\}$.

Zeigen Sie $M \vdash_{\mathcal{C}} A$ durch Angabe einer Ableitung.

Lösung:

1. Wir verfahren wie in der Präsenzaufgabe.

- Wir wollen $\{A \Rightarrow B, B \Rightarrow A\} \models \neg B \vee A$ zeigen. Sei \mathcal{A} eine Belegung, die $A \Rightarrow B$ und $B \Rightarrow A$ wahr macht. Dann ist entweder $\mathcal{A}(A) = \mathcal{A}(B) = 0$ oder $\mathcal{A}(A) = \mathcal{A}(B) = 1$. In beiden Fällen ist aber $\mathcal{A}(\neg B \vee A) = 1$ und damit gilt die Folgerbarkeitsbeziehung und die Regel ist korrekt.
- Hier gilt $\{(A \vee B) \Rightarrow C, \neg C \wedge \neg B\} \models A \vee B$ nicht. Beispielsweise ist \mathcal{A} mit $\mathcal{A}(A) = \mathcal{A}(B) = \mathcal{A}(C) = 0$ eine Belegung, die $(A \vee B) \Rightarrow C$ und $\neg C \wedge \neg B$ wahr macht, aber $A \vee B$ nicht.

2.

- | | | |
|-----|--|---|
| (1) | $M \vdash C \Rightarrow (E \Rightarrow C)$ | mit $sub(A) = C, sub(B) = E$ im Axiom |
| (2) | $\vdash \neg(E \Rightarrow C)$ | aus M |
| (3) | $\vdash \neg C$ | mit (1),(2), MT und
$sub(F) = C, sub(G) = E \Rightarrow C$ |
| (4) | $\vdash A \vee C$ | aus M |
| (5) | $\vdash A$ | mit (3),(4), DS1 und $sub(F) = A, sub(G) = C$ |

Informationen und Unterlagen zur Veranstaltung unter:

<http://www.informatik.uni-hamburg.de/TGI/lehre/v1/SS15/FGI1>