Karlsruher Institut für Technologie

Institute of Information Security and Dependability
Dr. Mattias Ulbrich
https://formal.kastel.kit.edu/

Übungsblatt 4

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in:		Tutorium Nr.:	
Nach-,Vorname 1:		,	
Matr.nr. 1:			
Nach-,Vorname 2:		,	
Matr.nr. 2:			

Ausgabe: 21. November 2023, 14:30 Uhr

Abgabe: 1. Dezember 2023, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 4:	/ 20	Blätter 1 – 4, Stud. 1:	/ 80
		Blätter 1 – 4, Stud. 2:	/ 80

Aufgabe 1 - Wettervorhersagen (6.5 Punkte)

Gegeben seien die aussagenlogischen Variablen R, B, S und T mit der folgenden Bedeutung.

- R = „Es regnet."
- B = „Ein Regenbogen ist zu sehen."
- S = „Die Person hat einen Regenschirm dabei."
- T = „Die Person bleibt trocken."

a) Übersetzen Sie die folgenden natürlichsprachlichen Aussagen jeweils in Aussagenlogik.

   i) „Ein Regenbogen ist nur zu sehen, wenn es regnet." (0.5 Punkte)

   ii) „Wenn es regnet, die Person aber keinen Schirm dabei hat, dann wird die Person nass." (0.5 Punkte)

   iii) „Wenn die Person einen Schirm dabei hat, bleibt die Person trocken." (0.5 Punkte)

b) Sei Γ die Menge aller Aussagen aus Aufgabenteil (a). Beweisen Sie in natürlicher Sprache die Folgerung $\Gamma \models (T \land \neg S) \to \neg B$, indem Sie den folgenden Lückentext vervollständigen. (2 Punkte)

   Zu zeigen ist die folgende Aussage:

   "____
   ____"

   Angenommen, das sei nicht wahr. Dann gilt, dass ____________________ ____________________*, aber trotzdem* ______________________________.

   Mit Aussage __ *aus Aufgabenteil (a) folgt dann, dass* ________________.

   Daraus und aus der Tatsache, dass die Person keinen Schirm dabei hat, folgt mit Aussage __ *aus Aufgabenteil (a), dass* ______________________________.

   Daraus ergibt sich ein Widerspruch zur Annahme. Also muss die ursprüngliche Aussage richtig sein.

c) Nehmen Sie an, Sie wollen wissen, ob ein Regenbogen zu sehen ist, ohne aus dem Fenster schauen zu müssen. Ihr Mitbewohner ist gerade nach Hause gekommen und ist nicht nass geworden. Wenn Sie ihn nun fragen, ob er einen Regenschirm dabei hatte und er mit nein antwortet, wissen Sie, dass kein Regenbogen zu sehen ist (Falls er mit ja antwortet, müssen

Sie wohl doch den Rollladen hochziehen). Zeigen Sie, dass diese Argumentation gültig ist, indem Sie einen Beweisbaum für die folgende Formel angeben: (3 Punkte)

$$((T \land \neg S) \to \neg B) \to (T \to (\neg S \to \neg B))$$

Lösung 1

a) i) $B \to R$

ii) $(R \land \neg S) \to \neg T$

iii) $S \to T$

b) *Zu zeigen ist die folgende Aussage:*

*„**Wenn die Person trocken bleibt, aber keinen Schirm dabei hat, ist kein Regenbogen zu sehen.**"*

*Angenommen, das sei nicht wahr. Dann gilt, dass **die Person trocken bleibt und keinen Schirm hat**, aber trotzdem **ein Regenbogen zu sehen ist**.*

*Mit Aussage **(i)** aus Aufgabenteil (a) folgt dann, dass **es regnet**.*

*Daraus und aus der Tatsache, dass die Person keinen Schirm dabei hat, folgt mit Aussage **(ii)** aus Aufgabenteil (a), dass **die Person nicht trocken bleibt**.*

Daraus ergibt sich ein Widerspruch zur Annahme. Also muss die ursprüngliche Aussage richtig sein.

c) Der folgende Beweisbaum zeigt, dass diese Argumentation tatsächlich gültig ist:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{T \vdash T}\,(\text{Ax}) \quad \dfrac{}{\neg S \vdash \neg S}\,(\text{Ax})}{T, \neg S \vdash T \land \neg S}\,(\land I) \qquad \dfrac{}{(T \land \neg S) \to \neg B \vdash (T \land \neg S) \to \neg B}\,(\text{Ax})}{((T \land \neg S) \to \neg B), T, \neg S \vdash \neg B}\,(\to E)}{((T \land \neg S) \to \neg B), T \vdash \neg S \to \neg B}\,(\to I)}{((T \land \neg S) \to \neg B) \vdash (T \to (\neg S \to \neg B))}\,(\to I)}{((T \land \neg S) \to \neg B) \to (T \to (\neg S \to \neg B))}\,(\to I)$$

Korrekturhinweise 1

a) jeweils ganz oder gar nicht, dabei ist auch die Umkehrung der Implikation zulässig

b) je **0.5 Punkte** für Lücke 1, Lücken 2+3, Lücken 4+5, Lücken 6+7

c) je **-0.5 Punkte** für fehlende oder falsche Regelanwendungen, insbesondere auf Ax und die korrekte Zusammenführung der Bedingungen vor $\vdash$ achten

Aufgabe 2 - Distributivgesetze (2+2 Punkte)

In der Vorlesung haben wir die Distributivgesetze für Mengen kennengelernt, aber nicht bewiesen. Da sowohl Mengen- als auch Aussagenlogik boolesche Algebren sind, liegt die Vermutung nahe, dass es die Distributivgesetze

(i) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

(ii) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

auch in der Aussagenlogik gelten.

a) Zeigen Sie $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$. Nutzen Sie dazu eine Wahrheitstabelle mit den folgenden Spalten: (2 Punkte)

$$A \quad B \quad C \quad (A \wedge B) \quad (A \wedge C) \quad (B \vee C) \quad A \wedge (B \vee C) \quad (A \wedge B) \vee (A \wedge C)$$

b) **Bonuspunkte:** Zeigen Sie die Hin-Richtung von (ii), nämlich

$$A \vee (B \wedge C) \to (A \vee B) \wedge (A \vee C)$$

indem Sie einen geschlossenen Beweisbaum im Kalkül des natürlichen Schließens für die Formel aufstellen. Sie können dafür das Schema aus Abb. 1 am Ende des Übungsblattes benutzen, müssen ihm aber nicht folgen. Markieren Sie an jedem Schlussstrich, welche Regel Sie angewendet haben. (2 Punkte)

Lösung 2

a) Wie in der folgenden Tabelle zu sehen ist, nehmen die beiden Formeln für alle Interpretationen den gleichen Wahrheitswert an und sind somit äquivalent:

A	B	C	$A \wedge B$	$A \wedge C$	$B \vee C$	$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$
f	f	f	f	f	f	f	f
f	f	w	f	f	w	f	f
f	w	f	f	f	w	f	f
f	w	w	f	f	w	f	f
w	f	f	f	f	f	f	f
w	f	w	f	w	w	w	w
w	w	f	w	f	w	w	w
w	w	w	w	w	w	w	w

b) Wir verwenden das Schema aus Abb. 1. Für den Beweisbaum siehe Abb. 2.

Korrekturhinweise 2

a) pro Fehler **-0.5 Punkte** pro Fehler, Folgefehler werden gegeben

b) je **-0.5 Punkte** für fehlende oder falsche Regelanwendungen, insbesondere auf Ax und die korrekte Zusammenführung der Bedingungen vor $\vdash$ achten

Aufgabe 3 - Syntaktische Spielereien (6.5 Punkte)

Seien P, Q und R aussagenlogische Variablen.

a) Zeigen Sie $P \vee Q \equiv P \vee (\neg P \wedge Q)$, indem Sie die eine Formel schrittweise in die andere umformen. Verwenden Sie dazu die Distributivgesetze aus der vorherigen Aufgabe und die Tautologien am Ende von Abschnitt 5.3 im Skript, zusammen mit der folgenden Äquivalenz: $F \equiv \mathtt{WAHR} \wedge F$. (2 Punkte)

b) Betrachten Sie die folgende aussagenlogische Formel:

$$F = (P \vee Q) \wedge (R \vee P) \wedge (\neg Q \vee \neg R \vee P)$$

Geben Sie alle Modelle von F an. (1 Punkt)

c) Ist F erfüllbar? Ist F allgemeingültig? Begründen Sie Ihre Antwort jeweils. (2 Punkte)

d) Geben Sie eine zu F äquivalente Formel G an, die so kurz wie möglich ist, d. h. so wenig aussagenlogische Variablen und Konnektive wie möglich enthält. Begründen Sie, warum $F \equiv G$ und warum G kürzestmöglich ist. (1 Punkt)

e) Geben Sie eine aussagenlogische Formel F' an, sodass F' nicht allgemeingültig ist, $F \lor F'$ jedoch allgemeingültig ist. (0.5 Punkte)

Lösung 3

a)

		Hinweis
$\mathtt{P} \lor \mathtt{Q}$	$\equiv \mathtt{WAHR} \land (\mathtt{P} \lor \mathtt{Q})$	
	$\equiv (\mathtt{P} \rightarrow \mathtt{P}) \land (\mathtt{P} \lor \mathtt{Q})$	Definition von $\mathtt{WAHR}$
	$\equiv (\neg \mathtt{P} \lor \mathtt{P}) \land (\mathtt{P} \lor \mathtt{Q})$	Definition von $\rightarrow$
	$\equiv (\mathtt{P} \lor \neg \mathtt{P}) \land (\mathtt{P} \lor \mathtt{Q})$	Kommutativität von $\lor$
	$\equiv \mathtt{P} \lor (\neg \mathtt{P} \land \mathtt{Q})$	Distributivgesetz

b) Die Modelle von F sind genau die Interpretationen $I \in \mathbb{B}^{Var_{AL}}$, für die $I(\mathtt{P}) = \mathbf{w}$ gilt. Das wird z. B. aus der folgenden Wahrheitstabelle ersichtlich (nicht gefordert):

$\mathtt{P}$	$\mathtt{Q}$	$\mathtt{R}$	$\mathtt{P} \lor \mathtt{Q}$	$\mathtt{R} \lor \mathtt{P}$	$\neg \mathtt{Q} \lor \neg \mathtt{R} \lor \mathtt{P}$	$(\mathtt{P} \lor \mathtt{Q}) \land (\mathtt{R} \lor \mathtt{P}) \land (\neg \mathtt{Q} \lor \neg \mathtt{R} \lor \mathtt{P})$
f	**f**	**f**	**f**	**f**	**w**	**f**
f	**f**	**w**	**f**	**w**	**w**	**f**
f	**w**	**f**	**w**	**f**	**w**	**f**
f	**w**	**w**	**w**	**w**	**f**	**f**
w	**f**	**f**	**w**	**w**	**w**	**w**
w	**f**	**w**	**w**	**w**	**w**	**w**
w	**w**	**f**	**w**	**w**	**w**	**w**
w	**w**	**w**	**w**	**w**	**w**	**w**

c) F ist erfüllbar, denn es gibt Modelle von F, wie in der vorherigen Teilaufgabe gezeigt. F ist jedoch nicht allgemeingültig, denn für alle $I \in \mathbb{B}^{Var_{AL}}$ mit $I(\mathtt{P}) = \mathbf{f}$ gilt $val_I(F) = \mathbf{f}$.

d) $G = \mathtt{P}$

Es gilt $G \equiv F$, denn für $I \in \mathbb{B}^{Var_{AL}}$ ist $val_I(F) = \mathbf{w}$ genau dann, wenn $val_I(G) = \mathbf{w}$, nämlich wenn $I(\mathtt{P}) = \mathbf{w}$. Es kann keine kürzere aussagenlogische Formel als G geben, die zu F äquivalent ist, da bereits $G \in M_0 = Var_{AL}$.

e) $F' = \neg\mathtt{P}$

Korrekturhinweise 3

a) je **-0.5 Punkte** pro fehlerhaftem / fehlendem Schritt (auch auf die korrekte Definition von $\rightarrow$ aus dem Skript achten)

b) ganz oder gar nicht, Begründung wird nicht gefordert

c) je **1 Punkt** pro Antwort, diese sollten kompatibel zur Antwort in (c) sein (auch, wenn die falsch war)

d) je **0.5 Punkte** für Formel und Begründung, diese dürfen sehr kurz gehalten sein

e) ganz oder gar nicht

Aufgabe 4 - Die Akte Hoare (5 Punkte)

Im Hauptquartier der GBI herrscht absolutes Chaos. Durch Ihre Hilfe konnten die Agenten, die als Spione für den berüchtigten Dr. Meta agiert haben, identifiziert werden. Besser gesagt: der Agent. Der Großteil der Beweislast ruht allein auf dem Agenten mit Decknamen Hoare. Doch bevor er befragt werden kann, wird Hoare leblos in seinem Büro aufgefunden. Alles deutet auf einen Suizid hin.

Doch Ihre neue Vorgesetzte, GBI-Detektivin mit Decknamen Lovelace, ist skeptisch. Sie stand Agent Hoare nahe und kann nicht glauben, dass er wirklich spioniert haben soll. Sie beschließt, eigene Ermittlungen durchzuführen.

Der Konkurrent von Detektivin Lovelace innerhalb der GBI, Deckname Zuse, hat maßgeblich zur Überführung von Hoare beigetragen. Er war es, der Hoare als denjenigen überführt hat, der die Schichtpläne der GBI für den kommenden Monat an den vermeintlichen Superbösewicht gesendet hat. Die Überführung stützt sich auf die folgenden Behauptungen Zuses:

1) Sowohl Agent Bellman, Agent Ford als auch Agent Hoare waren an diesem Tag im Hauptquartier, jedoch niemand sonst.

2) Wenn Bellman schuldig ist, hatte er genau einen Komplizen.

3) Wenn Ford unschuldig ist, dann ist es auch Hoare.

4) Wenn es genau zwei Schuldige gibt, dann ist Bellman einer von ihnen.

5) Wenn Hoare unschuldig ist, ist auch Ford unschuldig.

Helfen Sie Detektivin Lovelace, den wahren Schuldigen zu überführen!

a) Übersetzen Sie die obigen Behauptungen 1)-5) in aussagenlogische Formeln G_1-G_5. Beschränken Sie sich dabei nur auf die Informationen, die relevant sind, um herauszufinden, welcher Agent schuldig ist. Verwenden Sie die aussagenlogischen Variablen $\mathtt{B}$, $\mathtt{F}$, $\mathtt{H}$ mit den Bedeutungen: (2.5 Punkte)
   - $\mathtt{B}$ = „Bellman ist schuldig.“
   - $\mathtt{F}$ = „Ford ist schuldig.“
   - $\mathtt{H}$ = „Hoare ist schuldig.“

b) Zuse hat bewiesen, dass $G_1 \land G_2 \land G_3 \land G_4 \land G_5 \to \mathtt{H}$ allgemeingültig ist. Er meint daher, dass Hoare schuldig sein müsse. Lovelace grübelt über diesen Beweis. Schließlich huscht ein triumphierenden Grinsen über ihr Gesicht. Welche Bedingung in Abhängigkeit von G_1,G_2,G_3,G_4,G_5,$\mathtt{H}$,$\mathtt{B}$,$\mathtt{F}$ muss zusätzlich noch gelten, um Hoares Schuld zu beweisen? Begründen Sie Ihre Antwort. Begründen Sie, warum diese Bedingung unerfüllbar ist. (2.5 Punkte)

Lösung 4

a) Mit den oben eingeführten aussagenlogischen Variablen formulieren wir:
   1) $G_1 = \mathtt{B} \lor \mathtt{F} \lor \mathtt{H}$
   2) $G_2 = \mathtt{B} \to ((\mathtt{F} \land \neg\mathtt{H}) \lor (\neg\mathtt{F} \land \mathtt{H}))$
   3) $G_3 = \neg\mathtt{F} \to \neg\mathtt{H}$
   4) $G_4 = ((\neg\mathtt{B} \land \mathtt{F} \land \mathtt{H}) \lor (\mathtt{B} \land \neg\mathtt{F} \land \mathtt{H}) \lor (\mathtt{B} \land \mathtt{F} \land \neg\mathtt{H})) \to \mathtt{B}$
   5) $G_5 = \neg\mathtt{H} \to \neg\mathtt{F}$

b) Sei $F = G_1 \land G_2 \land G_3 \land G_4 \land G_5$. Um Hoare als schuldig zu überführen, muss für alle Modelle $I \in \mathbb{B}^{Var_{AL}}$ von F gelten, dass $I(\mathtt{H}) = \mathbf{w}$, was Zuse ja bewiesen hat.

Außerdem muss aber unter einer Interpretation, die eine Lösung dieses Falls darstellt, F zu **w** auswerten.

Allerdings ist F unerfüllbar. Das zeigen wir, indem wir zeigen, dass es keine Interpretation $I \in \mathbb{B}^{Var_{AL}}$ gibt, sodass $val_I(G_i) = \mathbf{w}$ für alle $1 \leq i \leq 5$.

Angenommen, es gäbe eine solche Interpretation I. Dann gälte:

Da $val_I(G_1) = \mathbf{w}$, muss mindestens für eine Variable $\mathtt{A} \in \{\mathtt{B}, \mathtt{F}, \mathtt{H}\}$, gelten, dass $I(\mathtt{A}) = \mathbf{w}$.

Angenommen, es ist $I(\mathtt{B}) = \mathbf{w}$. Damit $val_I(G_2) = \mathbf{w}$, muss entweder $I(\mathtt{F}) = \mathbf{w}$ oder $I(\mathtt{H}) = \mathbf{w}$ sein. Im ersten Fall müsste $I(\mathtt{H}) = \mathbf{f}$ und damit, um $val_I(G_5) = \mathbf{w}$ sicherzustellen, auch $I(\mathtt{F}) = \mathbf{f}$ sein, ein Widerspruch. Analog ergibt sich im zweiten Fall ein Widerspruch mit $val_I(G_3) = \mathbf{w}$. Also muss $I(\mathtt{B}) = \mathbf{f}$ gelten.

Angenommen, $I(\mathtt{F}) = \mathbf{w}$. Dann muss, damit $val_I(G_3) = \mathbf{w}$, auch $I(\mathtt{H}) = \mathbf{w}$ sein. Dann wäre jedoch $val_I(G_4) = \mathbf{f}$, da zwar $val_I(\neg \mathtt{B} \wedge \mathtt{F} \wedge \mathtt{H}) = \mathbf{w}$, jedoch $val_I(B) = \mathbf{f}$. Analog ergibt sich ein Widerspruch unter der Annahme, dass $I(\mathtt{H}) = \mathbf{w}$.

Also muss $I(\mathtt{B}) = I(\mathtt{F}) = I(\mathtt{H}) = \mathbf{f}$ gelten, doch dies steht im Widerspruch zu unserer eingehenden Annahme.

Da F unerfüllbar ist, können wir, obwohl $F \to \mathtt{H}$ allgemeingültig ist, nicht auf $\mathtt{H}$ schließen.

Korrekturhinweise 4

a) je **0.5 Punkte** pro Formel, ganz oder gar nicht

b) **0.5 Punkte** für die Bedingung und **1 Punkt** für die Begründung, **1 Punkt** für den Unerfüllbarkeitsbeweis, dort Teilpunkte nach eigenem Ermessen

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \lor (B \land C) \vdash A \lor (B \land C)}\,(\mathsf{Ax}) \quad \dfrac{\vdots}{\;} \quad \dfrac{\vdots}{\;}}{\;} \qquad \dfrac{\dfrac{}{A \lor (B \land C) \vdash A \lor (B \land C)}\,(\mathsf{Ax}) \quad \dfrac{\vdots}{\;} \quad \dfrac{\vdots}{\;}}{\;}}{\;}}{A \lor (B \land C) \to (A \lor B) \land (A \lor C)}$$

Abbildung 1: Schema eines Beweises in natürlichem Schließen für Aufgabe 2 b.

$$\dfrac{\dfrac{*_1 \qquad *_2}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \vdash (\mathtt{A} \lor \mathtt{B}) \land (\mathtt{A} \lor \mathtt{C})}\,(\land I)}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \to (\mathtt{A} \lor \mathtt{B}) \land (\mathtt{A} \lor \mathtt{C})}\,(\to I)$$

wobei $*_1$ der folgende Beweisbaum:

$$\dfrac{\dfrac{}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \vdash \mathtt{A} \lor (\mathtt{B} \land \mathtt{C})}\,(\mathsf{Ax}) \qquad \dfrac{\dfrac{\dfrac{}{\mathtt{A} \vdash \mathtt{A}}\,(\mathsf{Ax})}{\mathtt{A} \vdash \mathtt{A} \lor \mathtt{B}}\,(\lor I_l)}{\mathtt{A} \to \mathtt{A} \lor \mathtt{B}}\,(\to I) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{B} \land \mathtt{C}}\,(\mathsf{Ax})}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{B}}\,(\land E_l)}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{A} \lor \mathtt{B}}\,(\lor I_r)}{\mathtt{B} \land \mathtt{C} \to \mathtt{A} \lor \mathtt{B}}\,(\to I)}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \vdash \mathtt{A} \lor \mathtt{B}}\,(\lor E)$$

und $*_2$ der folgende Beweisbaum:

$$\dfrac{\dfrac{}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \vdash \mathtt{A} \lor (\mathtt{B} \land \mathtt{C})}\,(\mathsf{Ax}) \qquad \dfrac{\dfrac{\dfrac{}{\mathtt{A} \vdash \mathtt{A}}\,(\mathsf{Ax})}{\mathtt{A} \vdash \mathtt{A} \lor \mathtt{C}}\,(\lor I_l)}{\mathtt{A} \to \mathtt{A} \lor \mathtt{C}}\,(\to I) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{B} \land \mathtt{C}}\,(\mathsf{Ax})}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{C}}\,(\land E_r)}{\mathtt{B} \land \mathtt{C} \vdash \mathtt{A} \lor \mathtt{C}}\,(\lor I_r)}{\mathtt{B} \land \mathtt{C} \to \mathtt{A} \lor \mathtt{C}}\,(\to I)}{\mathtt{A} \lor (\mathtt{B} \land \mathtt{C}) \vdash \mathtt{A} \lor \mathtt{C}}\,(\lor E)$$

Abbildung 2: Lösung für Aufgabe 2 b.

Bitte beachten Sie die folgenden Hinweise:

- Lösungen **müssen** handschriftlich erstellt werden
- Ihre Abgabe sollte die erste Seite dieser Datei als Deckblatt haben
- Ihre Abgabe muss **rechtzeitig** erfolgen

Außerdem, wenn Sie Ihre Ausarbeitung über die Abgabekästen im Keller des Informatik-Gebäudes abgeben:

- Ihre Abgabe muss in der oberen **linken** Ecke zusammengeheftet werden
- Tablet-Ausdrucke sind zulässig

Wenn Sie Ihre Ausarbeitung online über ILIAS abgeben, dann achten Sie darauf:

- Ihre Abgabe muss **genau eine** PDF-Datei sein
- Scans und lesbare Fotos sind zulässig
- Abgabe erfolgt unter „Tutorien“ im Ordner **Ihres** Tutoriums