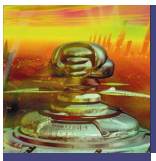


Logik und Computerbeweise
Schnupperuni 2007

Holger Bluhm,
Prof. Dr. Martin Kreuzer,
Stefan Kühling

02.08.2007

Inhaltsverzeichnis

1 (Aussagen–)Logik **1**

Logik, was ist das eigentlich? 1

Grundlagen 3

Aussagenlogische Übersetzungen 7

2 (Computer–)Algebra **9**

Algebraisches Vorgeplänkel 10

Von der Logik zur (Computer–)Algebra 13

3 CoCoA **15**

4 Drei Beispiele **17**

5 Aufgaben **27**

6 Lösungen **33**

1 (Aussagen–)Logik

Logik, was ist das eigentlich?

Schlägt man den Begriff im Lexikon nach, so bekommt man folgende Antworten:

> „***Logik***, *Lehre vom folgerichtigen (logischen) Denken.*“
>
> Witte Schülerlexikon, 18. Auflage 1957, Freiburg.

> „***Logik***, 1) *Fähigkeit, richtig zu denken;*
> 2) *Wissen vom Wesen und der Bildung der Begriffe und Urteile.*“
>
> Knaurs Lexikon a-z, 1969, München.

> „***Logik***, [griechisch ›Wort‹, ›Vernunft‹], *allgemein die Fähigkeit, richtig zu denken; im engeren Sinn die Kunst so zu argumentieren, daß sich aus gesicherten Voraussetzungen über einen Sachverhalt richtige, das heißt logisch schlüssige Folgerungen ziehen lassen.*
> *Durch logisches Denken lernt man klare, eindeutige Beziehungen zwischen einzelnen Aussagen herzustellen. Ohne den logischen Gebrauch der Sprache würde die menschliche Verständigung erschwert; auch Computer könnten ohne Logik nicht funktionieren.*“
>
> Der Jugend Brockhaus, 1985, Wiesbaden.

Diese Zitate vermitteln schon einen relativ guten Eindruck, was mit Logik gemeint ist. Dieses Bild wollen wir nun *mathematisieren*.

In der *formalen Logik* widmen wir uns dem Studium der formalen Beziehungen zwischen Denkinhalten. Der Prototyp einer mathematischen Beschreibung solcher Denkinhalte ist der der *Aussage*, für die wir die folgende Pseudodefinition verwenden.

Definition 1.1
Eine (logische) **Aussage** ist ein sprachliches Gebilde, das entweder **wahr** (kurz `w` oder 1) oder **falsch** (kurz `f` oder 0) ist.

Mit den hier vom Himmel fallenden Begriffen **wahr** und **falsch** werden die üblicherweise mit einer Aussage verbundenen Wahrheitswerte bezeichnet. In einem gewissen Sinn beschäftigt sich die formale Logik mit „Aussagen über Aussagen“.

Beispiel 1.2 Die folgenden sprachlichen Gebilde stellen Beispiele für Aussagen dar.

$$\begin{aligned} A &= \text{„Berlin ist die Hauptstadt von Deutschland.“} \\ B &= \text{„Der Wal ist ein Fisch.“} \\ C &= \text{„Für jede Zahl } x \in \mathbb{R} \text{ gilt } x^2 \geq 0.\text{“} \\ D &= \text{„Das Programm } \texttt{MyProg}(\ldots) \text{ terminiert.“} \end{aligned}$$

Hingegen stellen die folgenden sprachlichen Gebilde „Aussagen über Aussagen“ dar.

$$\begin{aligned} E &= \text{„Die Aussagen } A \text{ und } B \text{ sind beide wahr.“} \\ F &= \text{„Die Aussage } B \text{ gilt nicht.“} \quad = \quad \text{„Der Wal ist kein Fisch.“} \end{aligned}$$

Das sprachliche Gebilde „Morgen wird es regnen“ ist jedoch keine Aussage im Sinn von Definition 1.1, denn ihr Wahrheitswert hängt vom Standpunkt des Betrachters ab.

In der mathematischen Logik wird eine *Symbolisierung* der Aussagen vorgenommen. Anstelle einer Aussage betrachten wir also ein Aussagensymbol (z.B. A oder B). Diese Aussagensymbole können wir dann mit *Junktoren* (d.h. Verknüpfungen wie „und zugleich“ $\wedge$, „oder“ $\vee$ oder „nicht“ $\neg$) zu komplizierteren *logischen Formeln* zusammensetzen. Je nachdem, mit welchen Wahrheitswerten die Aussagensymbole belegt werden, erhalten solche logischen Formeln ebenfalls Wahrheitswerte. Die Regeln, nach denen Aussagensymbole oder allgemeiner so genannte *atomare Formeln* zu komplizierteren Formeln zusammengesetzt werden, nennt man die *Syntax* eines logischen Systems. Die Regeln, nach denen logische Formeln mit Wahrheitswerten versehen werden, nennt man die *Semantik* eines logischen Systems.

Schließlich bleibt noch eine Aufgabe: Wie kann man feststellen, ob eine logische Formel unter allen möglichen Belegungen der atomaren Formeln mit Wahrheitswerten stets den Wahrheitswert „wahr“ liefert? Oder ob sie stets den Wahrheitswert „falsch“ liefert? Dies ist die Aufgabe eines logischen *Kalküls*.

Definition 1.3
Ein **logisches System** besteht aus den folgenden Teilen.

a) Gewisse formale Ausdrücke werden als **atomare Formeln** bezeichnet. Die **Syntax** des logischen Systems legt fest, wie man die atomaren Formeln mit Hilfe gewisser **Junktoren** oder **Operatoren** zu komplizierteren Formeln zusammenfügen darf. Die sich ergebenden **logischen Formeln** sind dabei erst einmal nur nach gewissen Regeln erstellte Zeichenketten ohne „Inhalt“ oder „Bedeutung“.

b) Die **Semantik** des logischen Systems besteht aus einer Reihe von Regeln, die festlegen, wie die Formeln mit Wahrheitswerten versehen werden können. Dadurch erhalten die Formeln eine gewisse „Bedeutung“ oder „Interpretation“. Eine Belegung der atomaren Formeln mit Wahrheitswerten, für die eine Gesamtformel F den Wert „wahr“ ergibt, nennt man ein **Modell** für F. Besitzt F kein Modell, so heißt F eine **unerfüllbare Formel**. Liefert F bei jeder Belegung den Wert „wahr“, so heißt F eine **Tautologie** oder eine **allgemein gültige Formel**.

c) Optional gibt es für ein logisches System auch ein **logisches Kalkül** (oder einfach **Kalkül**). Ein Kalkül besteht aus einer Reihe von mechanisch anzuwendenden, starren Regeln für die Umformung von Formeln. Das Ziel der Anwendung eines logischen Kalküls ist es, die Unerfüllbarkeit einer vorgegebenen Formel nachzuweisen oder ein Modell für sie zu konstruieren. Kalküle eignen sich meist für die algorithmische Implementierung im Computer.

Das einfachste logische System ist die Aussagenlogik, die im nächsten (Unter–)Abschnitt ausführlich untersucht werden wird. Für die Aussagenlogik gibt es mehrere Kalküle. Bestandteil solcher Kalküle sind meist Regeln für Äquivalenzumformungen von Formeln. Dies bedeutet, dass man Formeln in andere Formeln überführt, die bei jeder **Belegung** (d.h. den elementaren Wahrheitswerten der einzelnen Aussagen) denselben Wahrheitswert liefern und deswegen für die Untersuchung der Unerfüllbarkeit bzw. Allgemeingültigkeit als zu der Ausgangsformel gleichwertig betrachtet werden können.
Auf dem ersten Blick mag es überraschen, dass man bei einem logaschen Kalkül i.A. nur die Unerfüllbarkeit einer Formel bzw. einer Formelmenge nachzuweisen sucht. Jedoch ist eine Formel F genau dann allgemein gültig, wenn ihre Negation $\neg F$ unerfüllbar ist. Ebenso ist eine Formel G genau dann eine Folgerung aus einer Menge von Formeln $\{F_1, \ldots, F_n\}$, wenn die Formel $F_1 \wedge \cdots \wedge F_n \wedge \neg G$ unerfüllbar ist. Alle drei Aufgaben sind also äquivalent.

Grundlagen

Jetzt wollen wir die Definition 1.3 mit Leben erfüllen, dafür brauchen wir erstmal eine genauere Definition der Syntax eines logischen Systems.

Definition 1.4 (Die Syntax der Aussagenlogik)

a) Eine **atomare Formel** ist von der Form A_i mit $i \in \mathbb{N}$, d.h. atomare Formeln sind nur die einfachen Aussagen.

b) Eine beliebige Formel entsteht induktiv aus atomaren Formeln, wobei die folgenden Schritte erlaubt sind:

b1) Jede atomare Formel ist eine Formel.

b2) Sind F, G zwei Formeln, so sind auch $(F \wedge G)$ sowie $(F \vee G)$ Formeln.

b3) Für jede Formel F ist auch $\neg F$ eine Formel.

Hierbei heißt $F \wedge G$ die **Konjunktion** von F und G,
$F \vee G$ die **Disjunktion** von F und G, und
$\neg F$ die **Negation** von F.

Seien z.B. A_1, A_2, A_3 elementare Aussagen, so sind $(\neg A_1 \vee (A_2 \wedge A_3))$ und $((A_1 \wedge A_2) \vee A_3)$ (aussagenlogische) Formeln, wohingegen $A_1 \vee A_2 \wedge A_3$ keine Formel ist, da die Klammerung fehlt (die Junktoren $\wedge$ und $\vee$ binden gleich stark).

Zur Vereinfachung der Konstruktion von Formeln führen wir die folgenden Abkürzungen ein.

Notationen 1.5

a) Für Aussagen verwenden wir statt $A_0, A_1, A_2, \ldots$ auch A, B, C etc.

Seien nun die Formeln $F_1, F_2, F_3, \ldots$ gegeben.

b) Für $(\neg F_1 \vee F_2)$ schreiben wir auch $(F_1 \Rightarrow F_2)$. Wir nennen $F_1 \Rightarrow F_2$ eine **Folgerung**.

c) Für $(F_1 \wedge F_2) \vee (\neg F_1 \wedge \neg F_2)$ schreiben wir auch $(F_1 \Leftrightarrow F_2)$. Wir nennen $F_1 \Leftrightarrow F_2$ eine **Äquivalenz**.

Nachdem wir jetzt ein paar Regeln haben, wie wir kompliziertere Formeln sinnvoll aus anderen Formeln bauen können, brauchen wir noch Vorschriften, die uns sagen, wie wir den Wahrheitswert einer solchen komplizierteren Formel aus den Wahrheitswerten der Einzelformeln bestimmen können. Dies regelt die Semantik.

Definition 1.6 (Die Semantik der Aussagenlogik)

a) Die Elemente der Menge $\{\texttt{wahr}, \texttt{falsch}\}$ heißen die **Wahrheitswerte**. Wir schreiben auch 1 statt `wahr` und 0 statt `falsch`.

b) Sei M eine Menge von atomaren Formeln. Eine **Belegung** von M ist eine Abbildung $\alpha : M \to \{0, 1\}$.

c) Sei $\widehat{M}$ die Menge aller Formeln, die mit Hilfe der atomaren Formeln in M gebildet werden können, und sei $\alpha : M \to \{0, 1\}$ eine Belegung. Dann erweitern wir α zu einer Abbildung $\widehat{\alpha} : \widehat{M} \to \{0, 1\}$ gemäß den folgenden Vorschriften.

c1) Für atomare Formeln $A \in M$ gilt $\widehat{\alpha}(A) = \alpha(A)$.

c2) Für Formeln $F, G \in \widehat{M}$ gilt

$$\widehat{\alpha}((F \wedge G)) = \begin{cases} 1 & \text{falls } \widehat{\alpha}(F) = 1 \textbf{ und } \widehat{\alpha}(G) = 1, \\ 0 & \text{sonst.} \end{cases}$$

c3) Für Formeln $F, G \in \widehat{M}$ gilt

$$\widehat{\alpha}((F \vee G)) = \begin{cases} 1 & \text{falls } \widehat{\alpha}(F) = 1 \textbf{ oder } \widehat{\alpha}(G) = 1 \text{ (oder beides)}, \\ 0 & \text{sonst.} \end{cases}$$

c4) Für $F \in \widehat{M}$ gilt für **nicht** F

$$\widehat{\alpha}(\neg F) = \begin{cases} 1 & \text{falls } \widehat{\alpha}(F) = 0, \\ 0 & \text{sonst.} \end{cases}$$

Im Folgenden schreiben wir der Einfachheit halber α statt $\widehat{\alpha}$. Ist eine Belegung der in einer Formel vorkommenden Aussagensymbole gegeben, so ist der Wahrheitswert der Formel gemäß dieser Definition leicht zu ermitteln.

Wenn die Formeln nicht zu kompliziert (groß) sind, dann lässt sich der Wahrheitswert einer Formel mit Hilfe der Wahrheitstafelmethode bestimmen, dabei geht man gemäß den Definitionen 1.4 und 1.6 und ggf. mit Hilfe der Notation 1.5 auf die Wahrheitswerte der Elementarereignisse zurück.

Bemerkung 1.7 (Wahrheitstafeln)

Seien F, G zwei Formeln und $\alpha : M \to \{0, 1\}$ eine Belegung der in F und G vorkommendnen atomaren Formeln.

a) Der sprachliche Gebrauch von „**und**“ im Sinne von „sowohl als auch“ wird mit $\wedge$ bezeichnet, der Gebrauch von „**oder**“ im nicht exklusiven Sinne wird mit $\vee$ symbolisiert und für „**nicht**“ schreiben wir $\neg$. Diese drei Operation werden durch die folgenden Wahrheitstafel beschrieben:

$\alpha(A)$	$\alpha(B)$	$\alpha(A \wedge B)$
1	1	1
1	0	0
0	1	0
0	0	0

$\alpha(A)$	$\alpha(B)$	$\alpha(A \vee B)$
1	1	1
1	0	1
0	1	1
0	0	0

$\alpha(A)$	$\alpha(\neg A)$
1	0
0	1

b) Die in Notation 1.5 beschriebenen Verküpfungnen $\Rightarrow$ und $\Leftrightarrow$ werden mit

$\alpha(A)$	$\alpha(B)$	$\alpha(A \Rightarrow B)$
1	1	1
1	0	0
0	1	1
0	0	1

$\alpha(A)$	$\alpha(B)$	$\alpha(A \Leftrightarrow B)$
1	1	1
1	0	0
0	1	0
0	0	1

beschrieben. Man beachte hierbei, dass man bei $\Rightarrow$ aus etwas falschem ($\alpha(A) = 0$) alles folgern kann.

Definition 1.8

Sei F eine aussagenlogische Formel und sei $\alpha : M \to \{0,1\}$ eine Belegung.

a) Sind alle in F vorkommenden atomaren Formeln in M enthalten, so heißt α zu F **passend**.

b) Ist α zu F passend und gilt $\alpha(F) = 1$, so schreiben wir $\alpha \models F$. Wir sagen, dass F unter der Belegung α gilt und nennen α ein **Modell** für F.

c) Ist $\mathcal{F}$ eine Menge aussagenlogischer Formeln, so heißt α ein **Modell** für $\mathcal{F}$, wenn für alle $F \in \mathcal{F}$ gilt: $\alpha \models F$. In diesem Fall schreiben wir $\alpha \models \mathcal{F}$.

d) Eine Menge $\mathcal{F}$ von Formeln heißt **erfüllbar**, falls $\mathcal{F}$ mindestens ein Modell besitzt. Ansonsten heißt $\mathcal{F}$ **unerfüllbar**.

e) Eine Formel F heißt **allgemein gültig** oder eine **Tautologie**, wenn jede zu F passende Belegung ein Modell für F ist.

Satz 1.9

Eine Formel F ist genau dann eine Tautologie, wenn $\neg F$ unerfüllbar ist.

Beweis

Genau dann ist F eine Tautologie, wenn für alle zu F passenden Belegungen $\alpha : M \to \{0,1\}$ gilt $\alpha \models F$, also genau dann, wenn für alle zu F passenden Belegungen α nicht gilt $\alpha \models \neg F$. Dies bedeutet gerade, dass $\neg F$ unerfüllbar ist. □

Definition 1.10

Zwei Formeln F und G heißen (semantisch) **äquivalent**, wenn für alle zu F und G passenden Belegungen $\alpha : M \to \{0,1\}$ die Gleichung $\alpha(F) = \alpha(G)$ gilt. In diesem Fall schreiben wir $F \equiv G$.

Satz 1.11 (ohne Beweis) **(Die fundamentalen Äquivalenzen der Aussagenlogik)**

Für aussagenlogische Formeln F, G, H gelten die folgenden Äquivalenzen:

a) $(F \wedge F) \equiv F$ *sowie* $(F \vee F) \equiv F$
(**Idempotenz**)

b) $(F \wedge G) \equiv (G \wedge F)$ *sowie* $(F \vee G) \equiv (G \vee F)$
(**Kommutativität**)

c) $((F \wedge G) \wedge H) \equiv (F \wedge (G \wedge H))$ *sowie* $((F \vee G) \vee H) \equiv (F \vee (G \vee H))$
(**Assoziativität**)

d) $(F \wedge (F \vee G)) \equiv F$ *sowie* $(F \vee (F \wedge G)) \equiv F$
(**Absorption**)

e) $(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H))$ *sowie* $(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$
(**Distributivität**)

f) $\neg\neg F \equiv F$
(**Doppelnegation**)

g) $\neg(F \wedge G) \equiv (\neg F \vee \neg G)$ *sowie* $\neg(F \vee G) \equiv (\neg F \wedge \neg G)$
(**de Morgansche Regeln**)

h) *Ist F eine Tautologie, so gilt* $(F \vee G) \equiv F$ *sowie* $(F \wedge G) \equiv G$.
(**Tautologieregeln**)

i) *Ist F unerfüllbar, so gilt* $(F \vee G) \equiv G$ *sowie* $(F \wedge G) \equiv F$.
(**Unerfüllbarkeitsregeln**)

In Anbetracht der Assoziativität können wir im Weiteren überflüssige Klammerpaare in aussagenlogischen Formeln weglassen.

Folgerung 1.12 (Unerfüllbarkeitsproblem)

Wenn man zeigen möchte, dass eine Formel G immer aus einer Formelmenge $\{F_1, \ldots, F_n\}$ folgt, also dass $(F_1 \wedge \cdots \wedge F_n) \Rightarrow G$ eine Tautologie ist, so zeigt man die Unerfüllbarkeit von

$$\begin{aligned}
\neg((F_1 \wedge \cdots \wedge F_n) \Rightarrow G) &\overset{1.5.b)}{\equiv} \neg(\neg(F_1 \wedge \cdots \wedge F_n) \vee G) \\
&\overset{\substack{1.11.g)\\ 1.11.f)}}{\equiv} (F_1 \wedge \cdots \wedge F_n) \wedge \neg G \\
&\overset{1.11.c)}{\equiv} F_1 \wedge \cdots \wedge F_n \wedge \neg G.
\end{aligned}$$

Wir zeigen also die Unerfüllbarkeit der Voraussetzungen zusammen mit der negierten Behauptung.

Bemerkung 1.13 (exklusives oder)

Die Formel $\neg(F \Leftrightarrow G)$ bzw. $(\neg F \Leftrightarrow G)$ oder $(F \Leftrightarrow \neg G)$ ist gleichbedeutend mit dem „exklusiven oder“ zwischen F und G, d.h. entweder es gilt F oder es gilt G, aber nicht beides:

$$\begin{aligned}
(F \vee G) \wedge \neg(F \wedge G) &\overset{1.11.f)}{\equiv} \neg\neg((F \vee G) \wedge \neg(F \wedge G)) \\
&\overset{1.11.g)}{\equiv} \neg(\neg(F \vee G) \vee \neg\neg(F \wedge G)) \\
&\overset{\substack{1.11.g)\\ 1.11.f)}}{\equiv} \neg((\neg F \wedge \neg G) \vee (F \wedge G)) \\
&\overset{1.11.b)}{\equiv} \neg((F \wedge G) \vee (\neg F \wedge \neg G)) \\
&\overset{1.5.c)}{\equiv} \neg(F \Leftrightarrow G).
\end{aligned}$$

Also ist das „exklusive oder“ das Gegenteil der Äquivalenz:

$\alpha(F)$	$\alpha(G)$	$\alpha(F \Leftrightarrow G)$	$\alpha(\neg(F \Leftrightarrow G))$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	1	0

Andere gängige Symbole für das „exklusive oder“ sind auch

$\otimes$, `XOR` und $\dot{\vee}$.

Aussagenlogische Übersetzungen

Wenn man ein sprachliches Gebilde (z.B. einen Aufgabentext) in logische Formeln übersetzen möchte, geht man immer nach dem gleichen Rezept vor.

1) **Festlegung der Abkürzungen**: Jeder Elementaraussage wird eine Abkürzung zugeordnet. Wie z.B. $A =$ „Anton kommt zur Geburtstagsfeier“.

2) **Übersetzung der Aussagen**: Mit Hilfe der Elementaraussagen werden dann die Aussagen zu Formeln übersetzt. Hierbei gibt es folgende Übersetzungsregeln.

   - **„A gilt (dann), wenn B gilt“** oder „wenn B gilt, dann gilt auch/folgt A“:
   $$B \Rightarrow A.$$
   - **„A gilt genau dann, wenn B gilt“**:
   $$A \Leftrightarrow B.$$
   - **„A gilt nur (dann), wenn B gilt“**, d.h. ich weiß, dass A gilt, also muss auch B (als Voraussetzung) eingetreten sein:
   $$A \Rightarrow B.$$

   Gelten mehrere Aussagen zusammen, so werden sie mit „und“ $\wedge$ zusammengesetzt.

3) **$\Rightarrow$, $\Leftrightarrow$ und „entweder oder“** werden mittels ihrer Definitionen übersetzt und ersetzt:
   „Folgerung“
   $$A \Rightarrow B \overset{1.5.b)}{\equiv} \neg A \vee B$$
   „Äquivalenz“
   $$\begin{aligned} A \Leftrightarrow B &\equiv (A \Rightarrow B) \wedge (B \Rightarrow A) \\ &\overset{1.5.b)}{\equiv} (\neg A \vee B) \wedge (\neg B \vee A) \\ &\overset{1.5.c)}{\equiv} (A \wedge B) \vee (\neg A \wedge \neg B) \end{aligned}$$
   „entweder oder“
   $$\neg (A \Leftrightarrow B) \overset{1.13}{\equiv} (A \vee B) \wedge \neg (A \wedge B).$$

4) **Das Unerfüllbarkeitsproblem** wird wie in Folgerung 1.12 beschrieben formuliert.

5) **Die fundamentale Äquivalenzen** (Satz 1.11) werden benutzt um die Formel in einheitliche Gestalt zu bringen, d.h. zu vereinfachen.

6) **Auswertung/Kalkül**.

Jetzt fehlt nur noch ein Kalkül zum Auswerten der Formeln (Kapitel 3), hierzu benutzen wir die Computeralgebra. Dafür sind auch wieder ein paar Vorbereitungen (Kapitel 2) zu treffen.

Beispiel 1.14 (Philosophisches)
Platon hatte Recht mit seiner Einschätzung des Sokrates genau dann, wenn Sokrates kein großer Philosoph war. Wenn Sokrates ein großer Philosoph war, dann hatte Aristoteles Recht mit seiner Einschätzung des Platon. Aristoteles hatte nur dann Recht mit seiner Einschätzung des Platon, falls Platon Recht hatte mit seiner Einschätzung des Sokrates.

1) Festlegung der Abkürzungen:

$$\begin{aligned} S &= \text{„Sokrates war ein großer Philosoph.“} \\ A &= \text{„Aristoteles hatte Recht mit seiner Einschätzung des Platon.“} \\ P &= \text{„Platon hatte Recht mit seiner Einschätzung des Sokrates.“} \end{aligned}$$

2), 3) Übersetzung der Aussagen:

- „Platon hatte Recht mit seiner Einschätzung des Sokrates genau dann, wenn Sokrates kein großer Philosoph war.“
$$F_1 := (P \Leftrightarrow \neg S)$$
- „Wenn Sokrates ein großer Philosoph war, dann hatte Aristoteles Recht mit seiner Einschätzung des Platon.“
$$F_2 := (S \Rightarrow A) \equiv (\neg S \vee A)$$
- „Aristoteles hatte nur dann Recht mit seiner Einschätzung des Platon, falls Platon Recht hatte mit seiner Einschätzung des Sokrates.“
$$F_3 := (A \Rightarrow P) \equiv (\neg A \vee P)$$
- Alle Aussagen zusammen werden beschrieben durch die Formel
$$F := F_1 \wedge F_2 \wedge F_3.$$

6) Somit ergibt sich für die Formel

$$F := (P \Leftrightarrow \neg S) \wedge (\neg S \vee A) \wedge (\neg A \vee P)$$

folgende Wahrheitstabelle.

$\alpha(P)$	$\alpha(S)$	$\alpha(A)$	$\alpha(P \Leftrightarrow \neg S)$	$\alpha(\neg S \vee A)$	$\alpha(\neg A \vee P)$	$\alpha(F)$
1	1	1	0	1	1	0
1	1	0	0	0	1	0
1	0	1	1	1	1	1
1	0	0	1	1	1	1
0	1	1	1	1	0	0
0	1	0	1	0	1	0
0	0	1	0	1	0	0
0	0	0	0	1	1	0

Also sind die Belegungen $\alpha(P) = \alpha(A) = 1$, $\alpha(S) = 0$ und $\alpha(P) = 1$, $\alpha(S) = \alpha(A) = 0$ Modelle für F.

2 (Computer–)Algebra

Das Wort Computer–Algebra ist aus den Worten Algbra und Computer zusammengesetzt. In dieser speziellen Richtung der Algebra geht es um Berechnungen, die sich besonders gut mit dem Computer durchführen lassen. Es bleibt also noch zu klären, was die Algebra eigentlich für eine Art der Mathematik ist.

> „***Algebra*** (w.)*, ursprünglich Lehre von den Gleichungen, jetzt allgemein die Buchstabenrechnung*“
>
> Witte Schülerlexikon, 18. Auflage 1957, Freiburg.

> „***Algebra*** [arab.]*, Lehre von den Gleichungen, verwendet Buchstabenrechnung. —* ***Algebraische Funktion****, eine mathematische Funktion, die nach d. Regeln der Algebra zusammengesetzt ist.*“
>
> Knaurs Lexikon a-z, 1969, München.

> „***Algebra****, Teilgebiet der Mathematik, das sich mit Gleichungen und Ungleichungen beschäftigt. Das Rechnen mit Gleichungen ist sehr alt. Die ältesten Aufgaben über quadratische Gleichungen, die man kennt, finden sich auf Keilschrifttafeln der Babylonier* (2000 v.Chr.)*. Von der Beschäftigung der Ägypter mit Gleichungen zeugt das ›Rechenbuch des Ahmes‹, eine Papyrosrolle von 20 m Länge und 30 cm Breite, das um etwa 1700 v.Chr. entstand.*
> *Bei den Griechen beschäftigten sich vor allem Heron von Alexandria, Diophant und Euklid mit der Gleichungslehre. So löste Euklid* (um 325 v.Chr.) *die quadratische Gleichung auf rein geometrische Weise durch Flächenverwandlung. Heron* (60 n.Chr.) *und Diophant* (um 250 n.Chr.) *gaben rechnerische Lösungen der quadratischen Gleichung an. Neben Gleichungen verwendeten griechische Mathematiker, so z. B. Euklid, Diophant und Archimedes* (um 250 v.Chr.)*, auch schon Ungleichungen.*
> *Das Erbe der Griechen übernahmen die Inder und Araber. Die Inder, die mit negativen Zahlen rechnen konnten, stellten das paarweise Auftreten der Lösungen quadratischer Gleichungen fest.*
> *In der Frühzeit der Mathematik wurden alle Rechnungen und Formeln in Worten ausgedrückt. Erst allmählich führte man Abkürzungen für häufig gebrauchte Ausdrücke ein. So bezeichnete Diophant unbekannte Zahlen mit dem Zeichen ζ* (griechisches Schluß-s)*.*
> *Erst Leonardo von Pisa* (um 1200) *verwendete in größerem Ausmaß Buchstaben als Platzhalter. Die ausschließliche und folgerichtige Benutzung von Buchstaben ist dem Franzosen François Viète* (* 1540, † 1576) *zu verdanken. Im 16. Jahrh. gelang die Lösung der Gleichungen 3. und 4. Grades mit Hilfe der cardanoschen Formeln, nach dem italienischen Mathematiker Geronimo Cardano* (* 1501, † 1576)*.*
> *Den grundlegenden Satz der Algebra, auch* ***Fundamentalsatz der Algebra*** *genannt fand 1799 Carl Friedrich Gauß. Der Satz besagt, daß jede Gleichung n–ten Grades genau n Lösungen hat, daß also z. B. eine Gleichung 3. Grades genau 3 Lösungen besitzt.*“
>
> Der Jugend Brockhaus, 1985, Wiesbaden.

Wenn man sich den Vortrag mal anschaut, dann tauchen dort die Begriffe „Körper“ als Rechenraum, „Ideal“ und „Ring“ beim Aufruf von CoCoA auf. Diese Begriffe haben in der Mathematik andere Bedeutungen als im alltäglichen Leben. Diese müssen erst ein Mal Stück für Stück bereit gestellt werden.

Algebraisches Vorgeplänkel

In einer Menge können Elemente in einem gewissen Zusammenhang stehen. So lässt sich für ganze Zahlen x, y z.B. entscheiden, ob x kleiner als y oder x ein Teiler von y ist. In der Mathematik heißen solche Zusammenhänge auch Relationen und sind wie folgt definiert.

Definition 2.1
Seien M, M_1, M_2 Mengen.

a) Eine Teilmenge R von $M_1 \times M_2$ heißt **Relation** zwischen M_1 und M_2. Im Fall $M_1 = M_2$ sprechen wir von einer Relation auf M_1.
Ist $(x, y) \in R$, so sagen wir x und y stehen in Relation und schreiben $x \sim_R y$ oder kurz $x \sim y$.

b) Eine Relation $\sim$ auf M heißt **Äquivalenzrelation**, wenn für beliebige $x, y, z \in M$ gilt:
(A_1) Reflexivität:
$$x \sim x$$
(A_2) Symmetrie:
$$x \sim y \;\Rightarrow\; y \sim x$$
(A_3) Transitivität:
$$x \sim y \text{ und } y \sim z \;\Rightarrow\; x \sim z.$$

c) Ist $\sim$ eine Äquivalenzrelation auf M und $x \in M$, so heißt die Menge
$$\overline{x} := \{y \in M \mid x \sim y\}$$
die **Äquivalenzklasse** von x (bezüglich der Relation $\sim$).

Beispiel 2.2

a) Die Allrelation $M \times M$ und die identische Relation I_M ($x \sim y :\Leftrightarrow x = y$) sind Äquivalenzrelationen.

b) Die Teilmenge $\{(x, y) \in \mathbb{Z}^2 \mid x \text{ teilt } y\}$ von $\mathbb{Z}^2$ ist eine reflexive, transitive Relation. Sie ist aber nicht symmetrisch, denn 2 teilt 4, aber 4 ist kein Teiler von 2.

c) Sei $n \in \mathbb{N}$ fest gewählt. Dann wird durch
$$x \sim y \;:\Leftrightarrow\; n \text{ ist Teiler von } x - y$$
eine Äquivalenzrelation auf $\mathbb{Z}$ definiert. Dabei stehen zwei ganze Zahlen also genau dann in Relation, wenn sie bei Division mit n den gleichen Rest lassen. Bei dieser Relation ist die Schreibweise $x \equiv y \bmod n$ („x ist kongruent zu y modulo n“) gebräuchlich.
Bzgl. dieser Relation gibt es genau n Äquivalenzklassen. Die Menge dieser Äquivalenzklassen wird mit $\mathbb{Z}/_{n\mathbb{Z}}$ bezeichnet.
Für $n = 2$ teilt man so die ganzen Zahlen in die geraden ($\overline{0}$) und ungeraden ($\overline{1}$) Zahlen ein.

Die Menge $\mathbb{Z}/_{n\mathbb{Z}}$ ist im Folgenden von besonderer Bedeutung. Sie liefert uns für $n = 2$ den Zahlenraum, den wir für unsere späteren Berechnungen benötigen. Wichtig ist, dass es sich dabei nicht nur um eine Menge mit n Elementen handelt, sondern dass diese Menge eine gewisse Struktur besitzt, so dass wir mit den Elementen rechnen können.

In der realen Welt, in der man sich hauptsächlich mit den Mengen $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ beschäftigt, rechnen wir mit Zahlen, d. h. wir können z. B. addieren und multiplizieren. Anders ausgedrückt lassen sich Zahlen verknüpfen und diese Verknüpfungen genügen gewissen Regeln. Die einfachste Struktur, die wir auf eine solche Weise erhalten, ist eine Gruppe, die wie folgt definiert ist.

Definition 2.3

Sei G eine nichtleere Menge und $\circ$ eine Verknüpfung auf G. Dann heißt $(G, \circ)$ bzw. G eine **Gruppe**, falls gilt:

(G_1)**:** $\circ$ ist assoziativ auf M, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ für alle $x, y, z \in G$;

(G_2)**:** es existiert ein neutrales Element e in G, d.h. für alle $x \in G$ gilt $x \circ e = x = e \circ x$;

(G_3)**:** für alle $x \in G$ existiert ein inverses Element $x^{-1} \in G$ mit $x \circ x^{-1} = e = x^{-1} \circ x$.

Eine Gruppe G heißt **abelsch** oder **kommutativ**, wenn zusätzlich gilt

(G_4): $\circ$ ist kommutativ auf M, d.h. $x \circ y = y \circ x$ für alle $x, y \in G$.

Beispiel 2.4

a) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind Gruppen.

b) $(\mathbb{N}_0, +)$ und $(\mathbb{N}, \cdot)$ sind keine Gruppen.

c) Auf der Menge der Äquivalenzklassen $\mathbb{Z}/_{n\mathbb{Z}}$ bzgl. der Relation aus Beispiel 2.2.a) lässt sich wie folgt eine Addition definieren. Für ganze Zahlen x, y sei $\overline{x} + \overline{y} := \overline{x + y}$. Zusammen mit dieser Verknpfung bildet $\mathbb{Z}/_{n\mathbb{Z}}$ eine abelsche Gruppe.

Im Allgemeinen können auf einer Menge mehrere Verknüpfungen definiert sein, z.B. eine Addition und eine Multiplikation. Dazu erweiteren wir den Begriff der Gruppe und erhalten einen sogenannten Ring.

Definition 2.5

Ein **Ring** ist eine nichtleere Menge R mit zwei Verknüpfungen $+$ und $\cdot$ (Addition und Multiplikation), so dass

(R_1): $(R, +)$ eine abelsche Gruppe ist
(ihr neutrales Element bezeichnen wir als **Nullemelent** 0);

(R_2): $\cdot$ assoziativ auf R ist;

(R_3): die **Distributivgesetze** gelten:

$$x\,(y + z) = xy + xz, \qquad (x + y)\,z = xz + yz \qquad \text{für alle } x, y, z \in R.$$

Ein Ring R heißt **kommutativ**, falls die Multiplikation in R kommutativ ist.

Das neutale Element von R bzgl. $\cdot$, falls es überhaupt existiert, heißt **Einselement** — wir bezeichnen es mit 1 — und R heißt dann Ring mit 1 (mit Einselement oder Eins).

Beispiel 2.6

a) $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ sind zusammen mit der üblichen Addition und Multiplikation Ringe.

b) Die Menge $\mathbb{Q}[x]$ aller Polynome in einer Variablen über $\mathbb{Q}$ bildet einen Ring.

c) Auf $\mathbb{Z}/_{n\mathbb{Z}}$ ist durch $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ eine Multiplikation definiert. Mit dieser wird $\mathbb{Z}/_{n\mathbb{Z}}$ zu einem kommutativen Ring mit 1.

Im späteren Verlauf, insbesondere bei den Berechnungen mit CoCoA, kommt der Begriff des Ideals vor. Ein Ideal ist einfach eine Teilmenge eines Ringes, die gewissen Eigenschaften genügt.

Definition 2.7

Sei R ein kommutativer Ring und I eine Teilmenge von R. Dann heißt I ein **Ideal** in R, falls gilt:

a) $(I, +)$ ist abelsche Gruppe,

b) für alle $x \in I$ und $y \in R$ gilt $xy \in I$.

Beispiel 2.8

a) R und $\{0\}$ sind stets Ideale in R.

b) $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ ist ein Ideal in $\mathbb{Z}$ für jedes $n \in \mathbb{Z}$.

Wir haben gesehen, dass die Mengen $\mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ Ringe sind. Jedoch unterscheiden sich die letzten beiden Mengen wesentlich von der ersten. Denn in $\mathbb{Q}$ und $\mathbb{R}$ besitzt jedes von Null verschiedene Element ein multiplikatives Inverses. Es handelt sich also um besondere Ringe, sogenannte Körper.

Definition 2.9

Ein kommutativer Ring $(R, +, \cdot)$ mit 1 heißt **Körper**, falls jedes Element von $R \setminus \{0\}$ ein multiplikatives Inverses besitzt, d.h. wenn für alle $x \in R \setminus \{0\}$ ein $y \in R$ existiert mit $xy = 1$.

Beispiel 2.10

a) $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.

b) Ist $p \in \mathbb{N}$ eine Primzahl, so ist $\mathbb{Z}/_{p\mathbb{Z}}$ ein Körper. Auch die Umkehrung ist korrekt.

Also ist $\mathbb{Z}/_{2\mathbb{Z}}$ ein Körper mit zwei Elementen. Er wird auch mit $\mathbb{F}_2$ bezeichnet. Mit diesem Körper werden wir im Folgenden arbeiten, denn wir werden mit den Elementen $\overline{0}$ und $\overline{1}$ gerade die Wahrheitswerte `falsch` und `wahr` identifizieren.
Zuletzt wollen wir noch auf einige spezielle Rechenregeln hinweisen:

$$1 \cdot 1 = 1 \qquad 1 \cdot 0 = 0 \qquad 1 + 0 = 1 \qquad 1 + 1 = 0$$

oder allgemeiner

$$-x = x \qquad x^2 = x$$

für alle $x \in \mathbb{F}_2$.

Von der Logik zur (Computer–)Algebra

Wir wollen nun mit Hilfe der Computer–Algebra aussagenlogische Formeln auf ihre Erfüllbarkeit hin testen. Die Computer–Algebra erlaubt es uns, komplizierte Berechnungen mit Polynomen und Idealen bestehend aus Polynomen durchzuführen. Wir müssen nun lediglich die Formeln in algebraische Ausdrücke übersetzen. Die Idee dabei ist, eine Formel mit einem Ideal aus Polynomen zu identifizieren. Da wir dabei im Zahlenraum $\mathbb{F}_2$ rechnen werden, kommen als Nullstellen von Polynomen nur 0 und 1 in Frage. Mit CoCoA können wir nun die gemeinsamen Nullstellen aller Polynome bestimmen und erhalten so ein Modell für unsere Formel.
Genauer gehen wir wie folgt vor. Jede atomare Aussage A_i identifizieren wir mit dem Polynom $x_i - 1$. Damit übersetzen wir die Tatsache, dass $\alpha(A) = 1$ ein Modell liefert, in die Tatsache, dass 1 Nullstelle von $x_i - 1$ ist. Junktionen von atomaren Formeln werden durch Idealoperation dargestellt. Die folgende Übersicht zeigt die Vorgehensweise:

Logik	**Nullstellensuche**
Aussagensymbole	Variablen
A, B, C oder $A_1, \ldots, A_n$	x, y, z oder $x_1, \ldots, x_n$
Erfüllbarkeit von	Nullstelle von
A bzw. B	$(x-1) =: F$ bzw. $(y-1) =: G$
$\neg A$	$F + 1 = x$
$A \vee B$	$F \cdot G = (x-1)(y-1)$
$A \wedge B \equiv \neg(\neg A \vee \neg B)$	$(F+1)(G+1)+1 = (xy+1)$

Beispiel 2.11
Nehmen wir z.B. die unerfüllbare Formel $A \wedge \neg A$, die Aussagen A und $\neg A$ haben dann die Übersetzungen

$$(x-1) \quad \text{und} \quad ((x-1)+1) = x.$$

Damit hat dann die Formel $A \wedge \neg A$ die Übersetzung

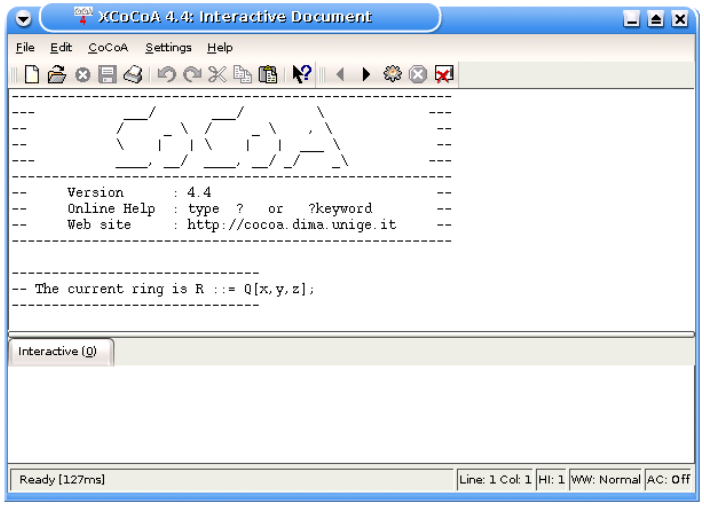
$$\begin{aligned} ((x-1)+1) \cdot (x+1) + 1 &= x \cdot (x+1) + 1 \\ &= x^2 + x + 1 \\ &= x^2 - x + 1. \end{aligned}$$

Dieses Polynom hat weder 0 noch 1 zur Nullstelle, also ist die zugehörige Formel nicht erfüllbar.

3 CoCoA

Natürlich ist diese Übersetzung mit anschließender Vereinfachung und Nullstellentest per Hand langsamer als die Wahrheitstafelmethode.

Jedoch haben wir für die Vereinfachungen und Nullstellensuche das Computeralgebra–System CoCoA zur Verfügung.



CoCoA–Befehle werden immer groß geschrieben und mit einem Semikolon beendet.

So legt dann `Use Z/(2)[x,y,z];` fest, dass wir in $\mathbb{F}_2$ rechnen und die Variablen x, y, z zur Verfügung haben. Ebenso verursacht z.B. `Use Z/(2)[x[1..6]];` die Festlegung von 6 Variablen $x_1, \ldots, x_6$ über $\mathbb{F}_2$.

Als Erstes setzen wir immer

```
K:=Ideal(x^2-x,y^2-y,z^2-z);
```

oder

```
K:=Ideal(x[1]^2-x[1],...,x[6]^2-x[6]);
```

Dieses *Körperideal* brauchen wir später.

Für das Aussagensymbol A verwenden wir das Polynom $x - 1$ und dieses geben wir dann als `I1:=Ideal(x-1);` in CoCoA ein.

Natürlich können so auch bereits übersetzte, größere Formeln/Polynome eingegeben/verwendet werden.

Mit A,B, eingegeben als `I1`,`I2`, können wir auch

$A \wedge B$ mit `J1:=I1+I2;`
$A \vee B$ mit `J2:=Intersection(I1,I2);`
$\neg A$ mit `J3:=K:I1;`

eingeben.

Mit `ReduceGBasis(J);` wird dann das Ideal `J` ausgewertet.

Als Ausgabe erhalten wir dann (hier nur für eine Variable x)

$[1] \;\widehat{=}\;$ die Formel ist unerfüllbar
$[x] \;\widehat{=}\;$ die Formel gilt für $x = 0$, also für $\alpha(A) = 0$
$[x+1] \;\widehat{=}\;$ die Formel gilt für $x = 1$, also für $\alpha(A) = 1$
$[x\hat{}2 + x]^* \;\widehat{=}\;$ die Formel gilt immer (Tautologie)

Beispiel 3.1

Wir wollen die Formel

$$\begin{aligned} F &:= (P \Leftrightarrow \neg S) \wedge (\neg S \vee A) \wedge (\neg A \vee P) \\ &\equiv (\neg P \vee \neg S) \wedge (P \vee S) \wedge (\neg S \vee A) \wedge (\neg A \vee P) \end{aligned}$$

auf Erfüllbarkeit testen.

Wir verwenden die Variablen x für P, y für S und z für A:

```
Use Z/(2)[x,y,z];
K:=Ideal(x^2-x,y^2-y,z^2-z);
```

Um das Eingegebene besser mit der Formel vergleichen zu können, verwenden wir
`P:=Ideal(x-1);` für P,
`S:=Ideal(y-1);` für S,
`A:=Ideal(z-1);` für A.

$$F = (\neg P \vee \neg S) \wedge (P \vee S) \wedge (\neg S \vee A) \wedge (\neg A \vee P)$$

```
F := Intersection(K:P,K:S)
     + Intersection(P,S)
     + Intersection(K:S,A)
     + Intersection(K:A,P);
```

Wertet man F mit `ReducedGBasis(F);` aus, so erhält man

```
[y, z^2 + z, x + 1]
```

und sortiert

```
[x + 1, y, z^2 + z],
```

was unserem bekannten Ergebnis von Seite 8 entspricht:

$$\alpha(P) = 1,\ \alpha(S) = 0 \text{ und } \alpha(A) \text{ ist beliebig.}$$

* $x^2 + x = (x+1) \cdot x = (x-1) \cdot x$ in $\mathbb{F}_2$

4 Drei Beispiele

Aufgabe 4.1 (Beurteilungen)

In einer Firma gibt es drei Abteilungen A, B, C, die für die Durchführung eines Projekts in Frage kommen. Sie begutachten sich gegenseitig wie folgt:

- Abteilung A schreibt: „Die Abteilungen B und C schaffen das Projekt nicht.“
- Abteilung B schreibt: „Abteilung A kann das Projekt durchführen, Abteilung C aber nicht.“
- Abteilung C schreibt: „Abteilung A kann das Projekt durchführen, nicht aber Abteilung B.“

Der Chef weiß, dass eine zu dem Projekt fähige Abteilung die anderen Abteilungen korrekt einschätzen kann und dass es mindestens eine fähige Abteilung gibt.

a) Stellen Sie eine aussagenlogische Formel auf, deren Erfüllbarkeit damit äquivalent ist, dass der Chef eine geeignete Abteilung finden kann.

b) Lösen Sie das Problem des Chefs.

Lösung 4.1

a)

- Festlegung der Abkürzungen:

$$\begin{aligned} A &= \text{„Abteilung } A \text{ kann das Projekt durchführen“,} \\ B &= \text{„Abteilung } B \text{ kann das Projekt durchführen“,} \\ C &= \text{„Abteilung } C \text{ kann das Projekt durchführen“.} \end{aligned}$$

- Übersetzung der Aussagen/Informationen:
  - „Abteilung A schreibt: ‚Die Abteilungen B und C schaffen das Projekt nicht.‘ “:
$$F_1 := A \Rightarrow (\neg B \wedge \neg C)\,.$$
  - „Abteilung B schreibt: ‚Abteilung A kann das Projekt durchführen, Abteilung C aber nicht.‘ “:
$$F_2 := B \Rightarrow (A \wedge \neg C)\,.$$
  - „Abteilung C schreibt: ‚Abteilung A kann das Projekt durchführen, nicht aber Abteilung B.‘ “:
$$F_3 := C \Rightarrow (A \wedge \neg B)\,.$$
- Zusätzlich:
  - „Es gibt mindestens eine geignete Abteilung“:
$$F_4 := (A \vee B \vee C)\,.$$
- Also:

$$\begin{aligned} F &:= F_1 \wedge F_2 \wedge F_3 \wedge F_4 \\ &\equiv (A \Rightarrow (\neg B \wedge \neg C)) \wedge (B \Rightarrow (A \wedge \neg C)) \wedge (C \Rightarrow (A \wedge \neg B)) \wedge (A \vee B \vee C) \\ &\equiv (\neg A \vee (\neg B \wedge \neg C)) \wedge (\neg B \vee (A \wedge \neg C)) \wedge (\neg C \vee (A \wedge \neg B)) \wedge (A \vee B \vee C)\,. \end{aligned}$$

b) Wenn F erfüllbar ist, kann der Chef eine fähige Abteiliung finden:

$\alpha(A)$	$\alpha(B)$	$\alpha(C)$	$\alpha(\neg A \vee (\neg B \wedge \neg C))$	$\alpha(\neg B \vee (A \wedge \neg C))$	$\alpha(\neg C \vee (A \wedge \neg B))$	$\alpha(A \vee B \vee C)$	$\alpha(F)$
0	0	0	1	1	1	0	0
0	0	1	1	1	0	1	0
0	1	0	1	0	1	1	0
0	1	1	1	0	0	1	0
1	0	0	1	1	1	1	1
1	0	1	0	1	1	1	0
1	1	0	0	1	1	1	0
1	1	1	0	0	0	1	0

Nur Abteilung A kann das Projekt durchführen.

CoCoA

Die Formel F ist bereits in übersetzungsfreundlicher Gestalt:

$$F \;=\; (\neg A \vee (\neg B \wedge \neg C)) \wedge (\neg B \vee (A \wedge \neg C)) \wedge (\neg C \vee (A \wedge \neg B)) \wedge (A \vee B \vee C)\,.$$

- Festlegung des Grundringes:
  ```
  Use Z/(2)[x,y,z];
  ```
- Ideale:
  ```
  K:=Ideal(x^2-x,y^2-y,z^2-z);
  A:=Ideal(x-1);
  B:=Ideal(y-1);
  C:=Ideal(z-1);
  ```
- Übersetzungen der Teilformeln:
  - $F_1 = (\neg A \vee (\neg B \wedge \neg C))$
    ```
    J1:=Intersection(K:A,(K:B+K:C));
    ```
  - $F_2 = (\neg B \vee (A \wedge \neg C))$
    ```
    J2:=Intersection(K:B,(A+K:C));
    ```
  - $F_3 = (\neg C \vee (A \wedge \neg B))$
    ```
    J3:=Intersection(K:C,(A+K:B));
    ```
  - $F_4 = (A \vee B \vee C)$
    ```
    J4:=Intersection(A,Intersection(B,C));
    ```
    oder (einfacher)
    ```
    J4:=Intersection(A,B,C);
    ```
- Gesamtformel:
  ```
  J:=J1+J2+J3+J4;
  ```
- Auswertung:
  ```
  ReducedGBasis(J);
  ```
  liefert
  `[z, y, x + 1]` bzw. `[x + 1, y, z]`.
- Ergebnis:
  Dies gibt die Nullstellen $x = 1, y = z = 0$, also ist die einzig mögliche Belegung $\alpha(A) = 1$ und $\alpha(B) = \alpha(C) = 0$, d.h. nur Abteilung A kann das Projekt bis zum Ende der Woche durchführen.

Aufgabe 4.2 (Der Bulle von Transsylvanien: Lucy in the sky with diamonds)

Inspektor Craig hat wieder einmal schwierige Fälle zu lösen. Sein augenblickliches Revier ist Transsylvanien, ein Land, das gleichermaßen von Vampiren wie Menschen bewohnt wird. Hinzu kommt, dass ein beträchtlicher Teil der Bevölkerung von einer grausamen Geisteskrankheit heimgesucht wird, die ihre Opfer so sehr verwirrt, dass diese immer das Gegenteil dessen sagen, was sie eigentlich meinen. Erschwerend für seine Ermittlungen wirkt sich auch die Tatsache aus, dass Vampire im Gegensatz zu Menschen auch noch lügen (ein geisteskranker Vampir sagt also wieder die Wahrheit).

In seinem ersten Fall handelt es sich um zwei Schwestern namens Lucy und Minna. Inspektor Craig muss herausfinden, wer von ihnen ein Vampir ist. Er weiß, dass eine der beiden Schwestern ein Vampir ist und die andere ein Mensch. Über den Geisteszustand der Betreffenden ist nichts bekannt. Hier ist das Transkript der Untersuchung:

Insp. Craig (zu Lucy): „Erzählen Sie mir etwas, das Sie beide betrifft."

Lucy: „Wir sind beide verrückt."

Insp. Craig (zu Minna): „Stimmt das?"

Minna: „Natürlich nicht."

Hieraus konnte Inspektor Craig zu jedermanns Zufriedenheit nachweisen, welche der Schwestern ein Vampir war. Sie auch?

Lösung 4.2

Wir benutzen die folgenden Abbkürzungen:

$$\begin{aligned} L_W &= \text{„Lucy sagt die Wahrheit"},\\ L_M &= \text{„Lucy ist ein Mensch"},\\ L_g &= \text{„Lucy ist geistig gesund"},\\ M_W &= \text{„Minna sagt die Wahrheit"},\\ M_M &= \text{„Minna ist ein Mensch"},\\ M_g &= \text{„Minna ist geistig gesund"}. \end{aligned}$$

Der übersetzte Aufgabentext ergibt die folgende Formel:

$$F = \underbrace{(L_W \Leftrightarrow (L_M \Leftrightarrow L_g))}_{=:F_1} \wedge \underbrace{(M_W \Leftrightarrow (M_M \Leftrightarrow M_g))}_{=:F_2} \wedge \underbrace{(L_M \Leftrightarrow \neg M_M)}_{=:F_3} \wedge \underbrace{(L_W \Leftrightarrow (\neg L_g \wedge \neg M_g))}_{=:F_4} \wedge \underbrace{(M_W \Leftrightarrow \neg L_W)}_{=:F_5}.$$

Gesucht ist ein Modell für F.

Um eine Wahrheitstafel mit $2^6 = 64$ $\Big((2 \text{ Wahrheitswerte})^{6 \text{ Möglichkeiten}}\Big)$ Zeilen zu vermeiden formen wir die Formel F um: Wir benutzen F_3 und F_5, um M_M durch $\neg L_M$ und M_W durch $\neg L_W$ in F_2 zu ersetzen. Da ein Modell gesucht ist, d.h. eine Belegung von $L_W, L_M, L_g, M_W, M_M, M_g$, so dass $\alpha(F) = 1$ ist, müssen auch $\alpha(F_3) = 1 = \alpha(F_5)$ sein. Also ist der Wahrheitswert von L_M gleich dem von $\neg M_M$ und der Wahrheitswert von M_W gleich dem von $\neg L_W$. Wir erhalten somit

$$F' = \underbrace{(L_W \Leftrightarrow (L_M \Leftrightarrow L_g))}_{=:F_1} \wedge \underbrace{(\neg L_W \Leftrightarrow (\neg L_M \Leftrightarrow M_g))}_{=:F_2'} \wedge \underbrace{(L_W \Leftrightarrow (\neg L_g \wedge \neg M_g))}_{=:F_4}$$

und eine Wahrheitstabelle mit nur noch $2^4 = 16$ Zeilen:

$\alpha(L_W)$	$\alpha(L_M)$	$\alpha(L_g)$	$\alpha(M_g)$	$\alpha(L_M \Leftrightarrow L_g)$	$\alpha(F_1)$	$\alpha(\neg L_M \Leftrightarrow M_g)$	$\alpha(F_2')$	$\alpha(\neg L_g \wedge \neg M_g)$	$\alpha(F_4)$	$\alpha(F')$
0	0	0	0	1	0	0	0	1	0	0
0	0	0	1	1	0	1	1	0	1	0
0	0	1	0	0	1	0	0	0	1	0
0	0	1	1	0	1	1	1	0	1	1
0	1	0	0	0	1	1	1	1	0	0
0	1	0	1	0	1	0	0	0	1	0
0	1	1	0	1	0	1	1	0	1	0
0	1	1	1	1	0	0	0	0	1	0
1	0	0	0	1	1	0	1	1	1	1
1	0	0	1	1	1	1	0	0	0	0
1	0	1	0	0	0	0	1	0	0	0
1	0	1	1	0	0	1	0	0	0	0
1	1	0	0	0	0	1	0	1	1	0
1	1	0	1	0	0	0	1	0	0	0
1	1	1	0	1	1	1	0	0	0	0
1	1	1	1	1	1	0	1	0	0	0

Es gibt also zwei Möglichkeiten:

1) $\alpha(L_W) = \alpha(L_M) = 0$, $\alpha(L_g) = \alpha(M_g) = 1$. Mit F_3 folgt: $\alpha(M_M) = 1$ und mit F_5 folgt $\alpha(M_W) = 1$. Also: Lucy ist ein geistig gesunder, lügender Vampir, Minna ist ein gesunder, die Wahrheit sagender Mensch.

2) $\alpha(L_W) = 1$, $\alpha(L_M) = \alpha(L_g) = \alpha(M_g) = 0$. Mit F_3 und F_5 folgen: $\alpha(M_M) = 1$ und $\alpha(M_W) = 0$. Also: Lucy ist ein verwirrter, die Wahrheit sagender Vampir, Minna ist ein verwirrter, lügender Mensch.

In jedem Fall ist Lucy der Vampir und Minna der Mensch.

CoCoA

Zuerst muss die Formel F' mit Hilfe der Definition der Äquivalenz (Notation 1.5.c)) umgeschrieben werden:

$$\begin{aligned} F' &= (L_W \Leftrightarrow (L_M \Leftrightarrow L_g)) \wedge (\neg L_W \Leftrightarrow (\neg L_M \Leftrightarrow M_g)) \wedge (L_W \Leftrightarrow (\neg L_g \wedge \neg M_g)) \\ &\equiv \big[\big(L_W \Leftrightarrow \underbrace{(L_M \Leftrightarrow L_g)}_{G_1}\big)\big] \wedge \big[\big(\neg L_W \Leftrightarrow \underbrace{(\neg L_M \Leftrightarrow M_g)}_{G_2}\big)\big] \wedge [(L_W \Leftrightarrow (\neg L_g \wedge \neg M_g))] \\ &\overset{1.5.c)}{\equiv} [(L_W \wedge G_1) \vee (\neg L_W \wedge \neg G_1)] \wedge [(\neg L_W \wedge G_2) \vee (L_W \wedge \neg G_2)] \\ &\qquad \wedge [(L_W \wedge (\neg L_g \wedge \neg M_g)) \vee (\neg L_W \wedge \neg (\neg L_g \wedge \neg M_g))]\,. \end{aligned}$$

mit

$$\begin{aligned} G_1 &:= (L_M \Leftrightarrow L_g) \\ &\overset{1.5.c)}{\equiv} [(L_M \wedge L_g) \vee (\neg L_M \wedge \neg L_g)] \\ G_2 &:= (\neg L_M \Leftrightarrow M_g) \\ &\overset{1.5.c)}{\underset{1.11.f)}{\equiv}} [(\neg L_M \wedge M_g) \vee (L_M \wedge \neg M_g)] \end{aligned}$$

- Festlegung des Grundringes:
  ```
  Use Z/(2)[x[1..6]];
  ```
- Ideale:
  ```
  K:=Ideal(x[1]^2-x[1],x[2]^2-x[2],x[3]^2-x[3],x[4]^2-x[4]);
  LW:=Ideal(x[1]-1);
  LM:=Ideal(x[2]-1);
  LG:=Ideal(x[3]-1);
  MG:=Ideal(x[4]-1);
  ```
- Übersetzungen der Teilformeln:
  - $G_1 = [(L_M \wedge L_g) \vee (\neg L_M \wedge \neg L_g)]$
    ```
    I1:=Intersection((LM+LG),(K:LM+K:LG));
    ```
  - $G_2 = [(\neg L_M \wedge M_g) \vee (L_M \wedge \neg M_g)]$
    ```
    I2:=Intersection((K:LM+MG),(LM+MG));
    ```
  - $F_1 = [(L_W \wedge G_1) \vee (\neg L_W \wedge \neg G_1)]$
    ```
    J1:=Intersection((LW+I1),(K:LW+K:I1));
    ```
  - $F_2' = [(\neg L_W \wedge G_2) \vee (L_W \wedge \neg G_2)]$
    ```
    J2:=Intersection((K:LW+I2),(LW+K:I2));
    ```
  - $F_4' = [(L_W \wedge (\neg L_g \wedge \neg M_g)) \vee (\neg L_W \wedge \neg (\neg L_g \wedge \neg M_g))]$
    ```
    J4:=Intersection((LW+K:LG+K:MG),(K:LW+K:(K:LG+K:MG)));
    ```

- Gesamtformel:

```
J:=J1+J2+J4;
```

- Auswertung:

```
ReducedGBasis(J);
```

liefert

```
[x[4]^2 + x[4], x[3] + x[4], x[2], x[1] + x[4] + 1].
```

Dies sind zwei Lösungen in einer.

  - `x[4]^2 + x[4]` bedeutet, dass $\texttt{x[4]}^2 + \texttt{x[4]} = 0$ sein muss, also, dass beide Zustände von `x[4]` vorkommen.
  - `x[3] + x[4]` heißt, dass in der Lösung `x[3]` und `x[4]` äquivalent sind, dies entspricht der Gleichung $\texttt{x[3]} + \texttt{x[4]} = 0$ und, da wir in $\mathbb{F}_2$ rechnen, $\texttt{x[3]} = \texttt{x[4]}$.
  - `x[2]` heißt, dass auf jeden Fall $\texttt{x[2]} = 0$ gelten muss, d.h. Lucy ist kein Mensch, also ist sie ein Vampir und nach der Vorüberlegung bedeutet dies, dass Minna der Mensch ist.
  - `x[1] + x[4] + 1` heißt, dass `x[1]` und `x[4]` sich gegenteilig verhalten, d.h. wenn $\texttt{x[1]} = 1$ gilt, dann ist $\texttt{x[4]} = 0$ und umgekehrt.

- Ergebnis:
  Da auf jeden Fall $\alpha(L_M) = 0$ gilt, ist Lucy der Vampir und Minna der Mensch.

Aufgabe 4.3 (Die Geburtstagsfeier)
Emil möchte seinen Geburtstag feiern. Leider sind seine Freunde Anne, Bernd, Christine und Dirk recht schwierig. Und zwar ist es so, dass Anne nur kommt, wenn auch Bernd kommt. Bernd kommt nur, wenn Christine kommt. Wenn wiederum Christine kommt, kommt auch Dirk. Wenn allerdings Bernd und Dirk kommen, kommt Christine nicht. Dirk kommt nur, wenn Anne oder Bernd kommen.

a) Stellen Sie eine aussagenlogische Formel auf, die die obige Situation beschreibt.

b) Zeigen Sie, dass keiner dieser vier Freunde zu Emils Geburtstagsfeier kommt.

Lösung 4.3

a)
- Abkürzungen:

$$\begin{aligned} A &= \text{„Anne kommt zu Emils Geburtstag“},\\ B &= \text{„Bernd kommt zu Emils Geburtstag“},\\ C &= \text{„Christine kommt zu Emils Geburtstag“},\\ D &= \text{„Dirk kommt zu Emils Geburtstag“}. \end{aligned}$$

- Übersetzung der Aussagen:
  - „Anne kommt nur, wenn Bernd kommt“:
  $$F_1 := (A \Rightarrow B) \equiv (\neg A \vee B)\,.$$
  - „Bernd kommt nur, wenn Christine kommt“:
  $$F_2 := (B \Rightarrow C) \equiv (\neg B \vee C)\,.$$
  - „Wenn Christine kommt, kommt auch Dirk“:
  $$F_3 := (C \Rightarrow D) \equiv (\neg C \vee D)\,.$$
  - „Wenn Bernd und Dirk kommen, kommt Christine nicht“:
  $$F_4 := ((B \wedge D) \Rightarrow \neg C) \equiv (\neg (B \wedge D) \vee \neg C) \equiv (\neg B \vee \neg D \vee \neg C)\,.$$
  - „Dirk kommt nur, wenn Anne oder Bernd kommen“:
  $$F_5 := (D \Rightarrow (A \vee B)) \equiv (\neg D \vee A \vee B)\,.$$

  Die gesamte Aussage wird durch die Konjunktion der Teilformeln beschrieben:

$$\begin{aligned} F &:= F_1 \wedge F_2 \wedge F_3 \wedge F_4 \wedge F_5\\ &\equiv (\neg A \vee B) \wedge (\neg B \vee C) \wedge (\neg C \vee D) \wedge (\neg B \vee \neg D \vee \neg C) \wedge (\neg D \vee A \vee B)\,. \end{aligned}$$

b)
- Wir wollen zeigen, dass keiner von Emils Freunden zu seiner Geburtstagsfeier kommt, also dass $F \Rightarrow G$ mit $G := (\neg A \wedge \neg B \wedge \neg C \wedge \neg D)$ eine Tautologie ist. Nach Folgerung 1.12 nehmen wir das Gegenteil an („Einer seiner Freunde kommt zu Emils Party“) $\neg G \equiv (A \vee B \vee C \vee D)$ und führen dies zu einem Widerspruch:

$$\begin{aligned} F' &:= F \wedge \neg G\\ &\equiv (\neg A \vee B) \wedge (\neg B \vee C) \wedge (\neg C \vee D) \wedge\\ &\qquad (\neg B \vee \neg D \vee \neg C) \wedge (\neg D \vee A \vee B) \wedge (A \vee B \vee C \vee D)\,. \end{aligned}$$

CoCoA

Die Formel F ist bereits in Übersetzungsfreundlicher Gestalt:

$$\begin{aligned} F' \;=\; & (\neg A \vee B) \wedge (\neg B \vee C) \wedge (\neg C \vee D) \wedge \\ & (\neg B \vee \neg D \vee \neg C) \wedge (\neg D \vee A \vee B) \wedge (A \vee B \vee C \vee D)\,. \end{aligned}$$

- Festlegung des Grundringes:

```
Use Z/(2)[x[1..4]];
```

- Ideale:

```
K:=Ideal(x[1]^2-x[1],x[2]^2-x[2],x[3]^2-x[3],x[4]^2-x[4]);
A:=Ideal(x[1]-1);
B:=Ideal(x[2]-1);
C:=Ideal(x[3]-1);
D:=Ideal(x[4]-1);
```

- Übersetzungen der Teilformeln:
  - $F_1 = (\neg A \vee B)$

```
J1:=Intersection(K:A,B);
```

  - $F_2 = (\neg B \vee C)$

```
J2:=Intersection(K:B,C);
```

  - $F_3 = (\neg C \vee D)$

```
J3:=Intersection(K:C,D);
```

  - $F_4 = (\neg B \vee \neg D \vee \neg C)$

```
J4:=Intersection(K:B,K:D,K:C);
```

  - $F_5 = (\neg D \vee A \vee B)$

```
J5:=Intersection(K:D,A,B);
```

  - $F_6 = (A \vee B \vee C \vee D)$

```
J6:=Intersection(A,B,C,D);
```

- Gesamtformel:

```
J:=J1+J2+J3+J4+J5+J6;
```

- Auswertung:

```
ReducedGBasis(J);
```

  liefert

```
[1].
```

- Ergebnis:
  Also ist die Formel unerfüllbar, d.h. $F \Rightarrow G$ ist eine Tautologie, somit kommt keiner von Emils Freunden zu seiner Geburtstagsfeier.

5 Aufgaben

Aufgabe 5.1 (Von der Schwierigkeit, Frauen zu verstehen)

Anne sagt: „Bettina sagt die Wahrheit.“

Bettina sagt: „Claudia lügt.“

Claudia sagt: „Anne und Bettina sagen beide die Wahrheit oder lügen beide.“

Wer lügt denn nun und wer sagt die Wahrheit?

Aufgabe 5.2 (Die Firma I)

In einer Firma werden zur Zeit die drei Projekte A, B und C bearbeitet. Um herauszufinden, welche Projekte bis zum Ende der Woche abgeschlossen werden, befragt der Chef der Firma die jeweiligen Projektleiter und erhält folgende Angaben:

1) Es können nicht alle Projekte fertiggestellt werden.
2) Um Projekt B fertigstellen zu können, muss Projekt A fertiggestellt sein.
3) Es wird auf jeden Fall Projekt B oder Projekt C fertiggestellt.
4) Projekt C kann nur fertiggestellt werden, wenn Projekt B fertiggestellt ist.

a) Stellen Sie eine aussagenlogische Formel auf, die die Bedingungen für die Fertigstellung der Projekte beschreibt.

b) Bestimmen Sie diejenigen Projekte, die bis zum Ende der Woche fertiggestellt werden.

Aufgabe 5.3 (Herakles heroische Heldentaten, Orakelsprüche)

Schon kurz nach der Geburt der Zwillingsbrüder Herakles und Eurystheus entstand ein Streit, wer von den beiden der rechtmäßige Herrscher sei. Dazu wurden die drei bekanntesten Orakel befragt.

Das Ammonion gab bekannt, dass die Orakelsprüche aus Klaros grundsätzlich falsch seien. Ebenso ließ das Orakel aus Klaros verlauten, dass die Orakelsprüche aus Delphi samt und sonders unzutreffend seien. Das Orakel aus Delphi jedoch behauptete, sowohl die Sprüche des Ammonions als auch die des Orakels in Klaros seien unwahr.

Wem sollten die armen Griechen nun glauben?

Aufgabe 5.4 (Der Tick mit dem Trick des vertrackten Naschens)

Donald war erbost: „Wer von euch hat von der Torte genascht?“ Seine Neffen blickten betreten auf das Backwerk, dessen kunstvolle Dekoration von kleinen Entenfingern (wie auch immer die aussehen) übel zugerichtet war. Einerseits wollten sie nicht petzen oder sich selbst beschuldigen, andererseits wollten sie ihren Onkel auch nicht belügen.

Nach einigen Anläufen quälte Tick aus sich heraus: „Trick oder ich waren es.“

Dann druckste Trick: „Entweder war es Track oder ich.“

Track gab an: „Entweder hat Tick (nicht) oder ich nicht genascht.“

Zum Erstaunen der drei wusste Donald sofort, wer genascht hatte. Nämlich?

Aufgabe 5.5 (Die Firma II)

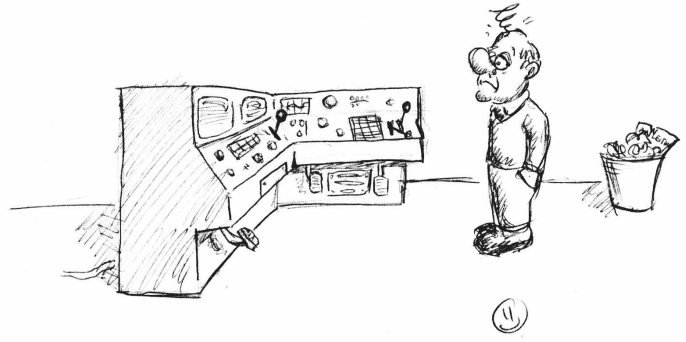
Ein neuer Mitarbeiter der Produktionsabteilung soll eine Maschine bedienen, deren Funktionsweise er jedoch nicht kennt. Zu seinem Unglück ist auch die Bedienungsanleitung nicht mehr vollständig vorhanden. Aus ihr erfährt er lediglich, dass er unbedingt den roten Knopf betätigen muss. Um auch die restlichen notwendigen Einstellungen der Maschine zu erfahren, befragt er schließlich seine Kollegen und erhält folgende Antworten:

1) Genau dann, wenn der rote Knopf gedrückt wird, muss auch der gelbe Knopf gedrückt werden.
2) Wenn der rote Knopf gedrückt und der grüne Hebel gezogen wird, dann muss auch das blaue Pedal getreten werden.
3) Wenn der gelbe Knopf gedrückt wird, muss auch der grüne Hebel gezogen werden.

Da er aus diesen Anweisungen nicht schlau wird, wendet er sich an seinen Meister, welcher sagt: „Ganz klar, du musst auf jeden Fall das blaue Pedal treten.“

a) Übersetzen Sie alle Anweisungen in aussagenlogische Formeln und geben Sie eine Formel an, deren Unerfüllbarkeit die Folgerung des Meisters bestätigt.

b) Benutzen Sie CoCoA um das Unerfüllbarkeitsproblem zu lösen.



Aufgabe 5.6 (Sofies Welt)

Nachdem Sofie schon einiges gelernt hat, reflektiert sie noch einmal über die alten Griechen. Nur dann, wenn Sokrates ein großer Philosoph war, war auch sein Schüler Platon ein großer Philosoph. Wenn Sokrates ein großer Philosoph war und den Mächtigen von Athen gefährlich erschien, dann musste er den Schierlingsbecher (Becher mit Gift) trinken. Sokrates erschien den Mächtigen Athens genau dann gefährlich, wenn auch Platon ein großer Philosoph war.

Stellen Sie eine aussagenlogische Formel auf, die zeigt, dass aus den obigen Überlegungen folgt, dass Sokrates den Giftbecher bekam, wenn er den Mächtigen von Athen gefährlich erschien. Zeigen Sie, dass dies zwangsläufig aus den Tatsachen folgt.

Index

A

abelsch . . . 11
Absorption . . . 5
Äquivalenz . . . 3
  semantisch . . . 5
Äquivalenz–
  Klasse . . . 10
  Relation . . . 10
Algebra . . . 9
allgemein gültige Formel . . . 2
Assoziativität . . . 5
atomare Formel . . . 2, 3
Aussage . . . 1

B

Belegung . . . 2, 3
  passende . . . 5

D

de Morgansche Regeln . . . 5
Disjunktion . . . 3
Distributivität . . . 5
Distributivitätsgesetz . . . 11
Doppelnegation . . . 5

E

Einselement . . . 11
exklusives oder . . . 6

F

falsch . . . 1
Folgerung . . . 3
Formel
  äquivalent . . . 5
  allgemein gültig . . . 2
  atomare . . . 2, 3
  logische . . . 2
  Tautologie . . . 2
  unerfüllbar . . . 2

G

Gruppe . . . 11
  abelsch . . . 11
  kommutativ . . . 11

I

Ideal
  Ring . . . 12
Idempotenz . . . 5

J

Junktor . . . 2

K

Kalkül . . . 2
Körper . . . 12
kommutativ
  Gruppe . . . 11
  Ring . . . 11
Kommutativität . . . 5
Konjunktion . . . 3

L

Logik . . . 1
logische Formel . . . 2
logisches System . . . 2

M

Modell . . . 2, 5

N

Negation . . . 3
nicht . . . 4
Nullelement . . . 11

O

oder . . . 4
  exklusives . . . 6
Operator . . . 2

R

Regeln
  de Morgan . . . 5
Relation . . . 10
  Äquivalenz– . . . 10
Ring . . . 11
  Distributivitätsgesetz . . . 11
  Einselement . . . 11
  Ideal . . . 12
  kommutativ . . . 11
  Nullelement . . . 11

S

Semantik . . . 2, 3
sematisch äquivalent . . . 5
Syntax . . . 2, 3
System
  logisches . . . 2

T

Tautologie . . . 2, 5
Tautologieregel . . . 5

U

und . . . 4
unerfüllbare Formel . . . 2
Unerfüllbarkeitsregeln . . . 5

W

wahr . . . 1
Wahrheitswert . . . 3

Literatur

[JBr] Der Jugend Brockhaus, Wiesbaden 1985.

[Fi] Gerd Fischer: *Lineare Algebra — eine Einführung für Studienanfänger*. 12. Auflage, Vieweg Studium, Braunschweig/Wiesbaden 2000.

[HNRS] Dirk Hennig, Alexandra Nolte, Gerhard Rosenberger, Martin Scheer: *Lineare Algebra und algebraische Strukturen für Informatiker*. Shaker, Aachen 2002.

[Kn] Knaurs Lexikon a-z, München 1969.

[KrKü] Martin Kreuzer, Stefan Kühling: *Logik für Informatiker*. Pearson Studium, München 2006.

[Wi] Witte Schülerlexikon, 18. Auflage, Freiburg 1957.

6 Lösungen

Lösung 6.1 (Von der Schwierigkeit, Frauen zu verstehen)

Intuitiv

- Angenommen, Anne sagt die Wahrheit. Dann sagt Bettina die Wahrheit und somit lügt Claudia. D.h. Claudias „wahre“ Aussage lautet: (Anne oder Bettina lügt) und (Bettina oder Anne sagt die Wahrheit). Dies ist ein Widerspruch zur Annahme, aus der folgt, dass Anne und Bettina die Wahrheit sagen.

- Also sagt Anne nicht die Wahrheit. Dann lügt Bettina. Somit sagt Claudia die Wahrheit. Da Claudia u.a. behauptet hat „Beide lügen“ ist alles in Ordnung: Claudia sagt die Wahrheit, Anne und Bettina lügen.

Mit Wahrheitstafeln

- Die Aussagen A, B, C seien folgendermaßen definiert:

$$\begin{aligned} A &= \text{„Anne sagt die Wahrheit“,} \\ B &= \text{„Bettina sagt die Wahrheit“,} \\ C &= \text{„Claudia sagt die Wahrheit“.} \end{aligned}$$

- Damit übersetzten sich die Aussagen zu folgender Formel:

$$F := (A \Leftrightarrow B) \wedge (B \Leftrightarrow \neg C) \wedge (C \Leftrightarrow (A \Leftrightarrow B))\,.$$

- Wir suchen jetzt mit einer Wahrheitstafel ein Modell für F:

$\alpha(A)$	$\alpha(B)$	$\alpha(C)$	$\alpha(A \Leftrightarrow B)$	$\alpha(B \Leftrightarrow \neg C)$	$\alpha(C \Leftrightarrow (A \Leftrightarrow B))$	$\alpha(F)$
0	0	0	1	0	0	0
0	0	1	1	1	1	1
0	1	0	0	1	1	0
0	1	1	0	0	0	0
1	0	0	0	0	1	0
1	0	1	0	1	0	0
1	1	0	1	1	0	0
1	1	1	1	0	1	0

  Es muss also $\alpha(A) = \alpha(B) = 0$ und $\alpha(C) = 1$ sein. Somit lügen Anne und Bettina, während Claudia die Wahrheit sagt.

CoCoA

Zuerst muss die Formel F mit Hilfe der Definition der Äquivalenz umgeschrieben werden:

$$\begin{aligned} F &= [A \Leftrightarrow B] \wedge [B \Leftrightarrow \neg C] \wedge [C \Leftrightarrow (A \Leftrightarrow B)] \\ &\overset{1.5.c)}{\equiv} [(A \wedge B) \vee (\neg A \wedge \neg B)] \wedge [(B \wedge \neg C) \vee (\neg B \wedge \neg\neg C)] \\ &\quad \wedge \big[\big(C \wedge \underbrace{((A \wedge B) \vee (\neg A \wedge \neg B))}_{\equiv (A \Leftrightarrow B)}\big) \vee \big(\neg C \wedge \neg \underbrace{((A \wedge B) \vee (\neg A \wedge \neg B))}_{\equiv (A \Leftrightarrow B)}\big)\big]. \\ &\overset{\substack{1.11.f) \\ 1.5.c)}}{\equiv} [(A \wedge B) \vee (\neg A \wedge \neg B)] \wedge [(B \wedge \neg C) \vee (\neg B \wedge C)] \\ &\quad \wedge [(C \wedge (A \Leftrightarrow B)) \vee (\neg C \wedge \neg (A \Leftrightarrow B))]\,. \end{aligned}$$

- Festlegung des Grundringes:

```
Use Z/(2)[x,y,z];
```

- Ideale:

```
K:=Ideal(x^2-x,y^2-y,z^2-z);
A:=Ideal(x-1);
B:=Ideal(y-1);
C:=Ideal(z-1);
```

- Übersetzungen der Teilformeln:
  - $F_1 = [A \Leftrightarrow B]$

```
J1:=Intersection((A+B),(K:A+K:B));
```

  - $F_2 = [B \Leftrightarrow \neg C]$

```
J2:=Intersection((B+K:C),(K:B+C));
```

  - $F_3 = [C \Leftrightarrow (A \Leftrightarrow B)]$

```
J3:=Intersection((C+J1),(K:C+K:J1));
```

- Gesamtformel:

```
J:=J1+J2+J3;
```

- Auswertung:

```
ReducedGBasis(J);
```

  liefert

`[z + 1, y, x]` bzw. `[x, y, z + 1]`.

- Ergebnis:

  Die einzig mögliche Belegung, so dass $\alpha(F) = 1$ gilt, ist $\alpha(A) = 0$, $\alpha(B) = 0$ und $\alpha(C) = 1$, d.h. Claudia sagt die Wahrheit und Anne und Bettina lügen.

Lösung 6.2 (Die Firma I)

- Festlegung der Abkürzungen:

$$\begin{aligned} A &= \text{„Projekt } A \text{ wird bis Ende der Woche fertig“,} \\ B &= \text{„Projekt } B \text{ wird bis Ende der Woche fertig“,} \\ C &= \text{„Projekt } C \text{ wird bis Ende der Woche fertig“.} \end{aligned}$$

- Übersetzung der Aussagen:
  - „Es können nicht alle Projekte fertiggestellt werden“:

$$F_1 := \neg(A \wedge B \wedge C).$$

  - „Um Projekt B fertigstellen zu können, muss Projekt A fertiggestellt sein“:

$$F_2 := (B \Rightarrow A).$$

  - „Es wird auf jeden Fall Projekt B oder Projekt C fertiggestellt“:

$$F_3 := (B \vee C).$$

  - „Projekt C kann nur fertiggestellt werden, wenn Projekt B fertiggestellt ist“:

$$F_4 := (C \Rightarrow B).$$

- Gesamtformel:

$$\begin{aligned} F &:= F_1 \wedge F_2 \wedge F_3 \wedge F_4 \\ &\equiv \neg(A \wedge B \wedge C) \wedge (B \Rightarrow A) \wedge (B \vee C) \wedge (C \Rightarrow B) \\ &\overset{\substack{1.5.b)\\ 1.11.g)}}{\equiv} (\neg A \vee \neg B \vee \neg C) \wedge (\neg B \vee A) \wedge (B \vee C) \wedge (\neg C \vee B) \end{aligned}$$

- Wahrheitstafel:

$\alpha(A)$	$\alpha(B)$	$\alpha(C)$	$\alpha(\neg A \vee \neg B \vee \neg C)$	$\alpha(\neg B \vee A)$	$\alpha(B \vee C)$	$\alpha(\neg C \vee B)$	$\alpha(F)$
1	1	1	0	1	1	1	0
1	1	0	1	1	1	1	1
1	0	1	1	1	1	0	0
1	0	0	1	1	0	1	0
0	1	1	1	0	1	1	0
0	1	0	1	0	1	1	0
0	0	1	1	1	1	0	0
0	0	0	1	1	0	1	0

- Antwort: Die einzig mögliche Belegung ist

$$\alpha(A) = \alpha(B) = 1 \text{ und } \alpha(C) = 0,$$

  also werden die Projekte A und B bis zum Ende der Woche fertig.

CoCoA

$$F \equiv \neg(A \wedge B \wedge C) \wedge (\neg B \vee A) \wedge (B \vee C) \wedge (\neg C \vee B).$$

- Festlegung des Grundringes:

```
Use Z/(2)[x,y,z];
```

- Ideale:

```
K:=Ideal(x^2-x,y^2-y,z^2-z);
A:=Ideal(x-1);
B:=Ideal(y-1);
C:=Ideal(z-1);
```

- Übersetzungen der Teilformeln:
  - $F_1 = \neg(A \wedge B \wedge C)$

```
J1:=K:(A+B+C);
```

  - $F_2 = (\neg B \vee A)$

```
J2:=Intersection(K:B,A);
```

  - $F_3 = (B \vee C)$

```
J3:=Intersection(B,C);
```

  - $F_4 = (\neg C \vee B)$

```
J4:=Intersection(K:C,B);
```

- Gesamtformel:

```
J:=J1+J2+J3+J4;
```

- Auswertung:

```
ReducedGBasis(J);
```

  liefert

```
[y + 1, x + 1, z]  bzw.  [x + 1, y + 1, z].
```

- Ergebnis:
  Die einzig mögliche Belegung, so dass $\alpha(F) = 1$ gilt, ist $\alpha(A) = \alpha(B) = 1$ und $\alpha(C) = 0$.

Lösung 6.3 (Herakles heroische Heldentaten, Orakelsprüche)

Umganssprachliche Lösung

Es gibt zwei Möglichkeiten, entweder das Orakel von Ammonion spricht die Wahrheit oder es irrt sich.

1. Möglichkeit: Das Orakel von Ammonion irrt sich nicht, d.h. das Orakel von Klaros liegt falsch. Also lautet die korrigierte Aussage, dass die Orakelsprüche aus Delphi war sind. Daraus ergibt sich, dass die Sprüche des Ammonion und aus Klaros falsch sind. Die erste Folgerung widerspricht der Annahme, dass sich das Orakel von Ammonion nicht irrt.

2. Möglichkeit: Das Orakel von Ammonion irrt sich, d.h. die Aussage ist falsch. Also irrt sich das Orakel von Klaros nicht. Daraus ergibt sich, dass der Orakelspruch von Delphi falsch ist. Somit sagen die Orakel von Ammonion oder das von Klaros die Wahrheit. Das Erste widerspricht zwar der Grundannahme, aber dass das Orakel von Klaros die Wahrheit spricht ist kein Widerspruch.

Insgesamt führt die 2. Möglichkeit zu keinem Widerspruch, falls das Ammonion irrt, der Spruch aus Klaros wahr ist und Delphi falsch liegt. Also sollte man auf das Orakel von Klaros hören.

Lösung mit Wahrheitstabelle

- Festlegung der Abkürzungen:

$$\begin{aligned} A &= \text{„Ammonion liegt richtig.“} \\ D &= \text{„Delphi liegt richtig.“} \\ K &= \text{„Klaros liegt richtig.“} \end{aligned}$$

- Übersetzung der Aussagen:
  - „Das Ammonion gab bekannt, dass die Orakelsprüche aus Klaros grundsätzlich falsch seien“:
$$F_1 := A \Leftrightarrow \neg K.$$
  - „Ebenso ließ das Orakel aus Klaros verlauten, dass die Orakelsprüche aus Delphi samt und sonders unzutreffend seien“:
$$F_2 := K \Leftrightarrow \neg D.$$
  - „Das Orakel aus Delphi jedoch behauptete, sowohl die Sprüche des Ammonions als auch die des Orakels in Klaros seien unwahr“:
$$F_3 := D \Leftrightarrow (\neg A \wedge \neg K)\,.$$
  - Alle drei Aussagen zusammen:
$$F := F_1 \wedge F_2 \wedge F_3.$$

- Wahrheitstabelle:

$\alpha(A)$	$\alpha(D)$	$\alpha(K)$	$\alpha(F_1) = \alpha(A \Leftrightarrow \neg K)$	$\alpha(F_2) = \alpha(K \Leftrightarrow \neg D)$	$\alpha(\neg A \wedge \neg K)$	$\alpha(F_3) = \alpha(D \Leftrightarrow (\neg A \wedge \neg K))$	$\alpha(F)$
0	0	0	0	0	1	0	0
0	0	1	1	1	0	1	1
0	1	0	0	1	1	1	0
0	1	1	1	0	0	0	0
1	0	0	1	0	0	1	0
1	0	1	0	1	0	1	0
1	1	0	1	1	0	0	0
1	1	1	0	0	0	0	0

- Antwort: Das Orakel von Klaros spricht die Wahrheit.

CoCoA

Zuerst muss die Formel F mit Hilfe der Definition der Äquivalenz (Notation 1.5.c)) umgeschrieben werden:

$$\begin{aligned} F &= (A \Leftrightarrow \neg K) \wedge (K \Leftrightarrow \neg D) \wedge (D \Leftrightarrow (\neg A \wedge \neg K)) \\ &\underset{1.11.f)}{\overset{1.5.c)}{\equiv}} [(A \wedge \neg K) \vee (\neg A \wedge K)] \wedge [(K \wedge \neg D) \vee (\neg K \wedge D)] \\ &\qquad \wedge [(D \wedge (\neg A \wedge \neg K)) \vee (\neg D \wedge \neg (\neg A \wedge \neg K))]\,. \end{aligned}$$

- Festlegung des Grundringes:
```
Use Z/(2)[x,y,z];
```

- Ideale:
```
N:=Ideal(x^2-x,y^2-y,z^2-z);
A:=Ideal(x-1);
D:=Ideal(y-1);
K:=Ideal(z-1);
```

- Übersetzungen der Teilformeln:
  - $F_1 = (A \wedge \neg K) \vee (\neg A \wedge K)$
```
J1:=Intersection((A+N:K),(N:A+K));
```
  - $F_2 = (K \wedge \neg D) \vee (\neg K \wedge D)$
```
J2:=Intersection((K+N:D),(N:K+D));
```
  - $F_3 = (D \wedge (\neg A \wedge \neg K)) \vee (\neg D \wedge \neg (\neg A \wedge \neg K))$
```
J3:=Intersection((D+N:A+N:K),(N:D+N:(N:A+N:K)));
```

- Gesamtformel:
```
J:=J1+J2+J3;
```

- Auswertung:
```
ReducedGBasis(J);
```
liefert
`[z + 1, y, x]` bzw. `[x, y, z + 1]`.

- Ergebnis:
Die einzig mögliche Belegung, so dass $\alpha(F) = 1$ gilt, ist, dass die Orakel von Ammonium und Delphi lügen ($\alpha(A) = \alpha(D) = 0$) und das Orakel von Klaros die Wahrheit sagt ($\alpha(K) = 1$).

Lösung 6.4 (Der Tick mit dem Trick des vertrackten Naschens)
Die Aussagensymbole A, B, C mögen für die folgenden Aussagen stehen:

$$\begin{aligned} A &= \text{Tick hat genascht,} \\ B &= \text{Trick hat genascht,} \\ C &= \text{Track hat genascht.} \end{aligned}$$

Dann übersetzen wir die Aussagen der drei Neffen folgendermaßen in aussagenlogische Formeln:

- „Trick oder ich [Tick] waren es“:
$$F_1 = A \vee B.$$
- „Entweder war es Track oder ich [Trick]“:
$$F_2 = \neg (C \Leftrightarrow B)$$
- „Entweder hat Tick nicht oder ich [Track] nicht genascht“:
$$F_3 = \neg (\neg A \Leftrightarrow \neg C) \equiv \neg A \Leftrightarrow C.$$

Wir gehen alle $2^3 = 8$ Möglichkleiten durch:

$\alpha(A)$	$\alpha(B)$	$\alpha(C)$	$\alpha(F_1) = \alpha(A \vee B)$	$\alpha(F_2) = \alpha(\neg(B \Leftrightarrow C))$	$\alpha(F_3) = \alpha(\neg A \Leftrightarrow C)$	$\alpha(F_1 \wedge F_2 \wedge F_3)$
0	0	0	0	0	0	0
0	0	1	0	1	1	0
0	1	0	1	1	0	0
0	1	1	1	0	1	0
1	0	0	1	0	1	0
1	0	1	1	1	0	0
1	1	0	1	1	1	1
1	1	1	1	0	0	0

Also hatten Tick und Trick genascht.

CoCoA

Zuerst muss die Formel F mit Hilfe der Definition der Äquivalenz umgeschrieben werden:

$$\begin{aligned} F &:= F_1 \wedge F_2 \wedge F_3 \\ &\equiv (A \vee B) \wedge \neg (C \Leftrightarrow B) \wedge \neg (\neg A \Leftrightarrow \neg C) \\ &\overset{\substack{1.5.c) \\ 1.11.f)}}{\equiv} [A \vee B] \wedge \neg [(C \wedge B) \vee (\neg C \wedge \neg B)] \wedge \neg [(\neg A \wedge \neg C) \vee (A \wedge C)]. \end{aligned}$$

- Festlegung des Grundringes:
```
Use Z/(2)[x,y,z];
```
- Ideale:
```
K:=Ideal(x^2-x,y^2-y,z^2-z);
A:=Ideal(x-1);
B:=Ideal(y-1);
C:=Ideal(z-1);
```
- Übersetzungen der Teilformeln:
  - $F_1 = [A \vee B]$
```
J1:=Intersection(A,B);
```
  - $F_2 = \neg [(C \wedge B) \vee (\neg C \wedge \neg B)]$
```
J2:=K:Intersection((C+B),(K:C+K:B));
```
  - $F_3 = \neg [(\neg A \wedge \neg C) \vee (A \wedge C)]$
```
J3:=K:Intersection((K:A+K:C),(A+C));
```
- Gesamtformel:
```
J:=J1+J2+J3;
```
- Auswertung:
```
ReducedGBasis(J);
```
liefert
`[z, x + 1, y + 1]` bzw. `[x + 1, y + 1, z]`.
- Ergebnis:
Die einzig mögliche Belegung, so dass $\alpha(F) = 1$ gilt, ist $\alpha(A) = \alpha(B) = 1$ und $\alpha(C) = 0$, d.h. Tick und Trick haben genascht.

Lösung 6.5 (Die Firma II)

- Festlegung der Abkürzungen:

$$\begin{aligned} R &= \text{„Der rote Knopf wird gedrückt“,} \\ G &= \text{„Der gelbe Knopf wird gedrückt“,} \\ H &= \text{„Der grüne Hebel wird gezogen“,} \\ P &= \text{„Das blaue Pedal wird getreten“.} \end{aligned}$$

- Übersetzung der Aussagen:
  - „Der rote Knopf muss unbedingt gedrückt werden“:
$$F_0 := R.$$
  - „Genau dann, wenn der rote Knopf gedrückt wird, muss auch der gelbe Knopf gedrückt werden“:
$$F_1 := (R \Leftrightarrow G).$$
  - „Wenn der rote Knopf gedrückt und der grüne Hebel gezogen wird, dann muss auch das blaue Pedal getreten werden“:
$$F_2 := ((R \wedge H) \Rightarrow P).$$
  - „Wenn der gelbe Knopf gedrückt wird, muss auch der grüne Hebel gezogen werden“:
$$F_3 := (G \Rightarrow H).$$
  - Behauptung: „Das blaue Pedal wird getreten“:
$$F_4 := P.$$

- Unerfüllbarkeitsproblem:
  Zu zeigen ist, dass aus $F_0, \ldots, F_3$ die Formel F_4 immer folgt, also dass
$$(F_0 \wedge F_1 \wedge F_2 \wedge F_3) \Rightarrow F_4$$
  eine Tautologie ist. Wir zeigen nach Folgerung 1.12 die Unerfüllbarkeit von
$$\begin{aligned} F &:= \neg[(F_0 \wedge F_1 \wedge F_2 \wedge F_3) \Rightarrow F_4] \\ &\overset{1.12}{\equiv} F_0 \wedge F_1 \wedge F_2 \wedge F_3 \wedge \neg F_4 \\ &\equiv R \wedge (R \Leftrightarrow G) \wedge ((R \wedge H) \Rightarrow P) \wedge (G \Rightarrow H) \wedge \neg P \end{aligned}$$

- Vereinfachung der Formel:
  Da nach F_1 die Aussagen R und G äquivalent sind, ersetzen wir in der gesamten Formel die Aussage G durch R.
$$\begin{aligned} F &\equiv R \wedge ((R \wedge H) \Rightarrow P) \wedge (R \Rightarrow H) \wedge \neg P \\ &\overset{1.5.c)}{\underset{1.11.g)}{\equiv}} R \wedge (\neg R \vee \neg H \vee P) \wedge (\neg R \vee H) \wedge \neg P. \end{aligned}$$

Man sieht jetzt schon an der Formel, dass $\alpha(R) = 1$ gelten muss, damit die Formel erfüllbar ist, dies nutzen wir nun aus, d.h. nach einigen Umformungen können wir nach Satz 1.11 die $\neg R$ eliminieren:

$$\begin{aligned} F &\overset{1.11.a),e)}{\equiv} [(R \wedge \neg R) \vee (R \wedge (\neg H \vee P))] \wedge [(R \wedge \neg R) \vee (R \wedge H)] \wedge \neg P \\ &\overset{1.11.i),a)}{\equiv} R \wedge (\neg H \vee P) \wedge H \wedge \neg P. \end{aligned}$$

Mit H eliminieren wir jetzt das $\neg H$ aus $(\neg H \vee P)$:

$$\begin{aligned} F &\overset{1.11.e)}{\equiv} R \wedge [(\neg H \wedge H) \vee (P \wedge H)] \wedge \neg P \\ &\overset{1.11.i)}{\equiv} R \wedge P \wedge H \wedge \neg P. \end{aligned}$$

- Da zur Erfüllbarkeit der Formel P und $\neg P$ zusammen gelten müssten, ist F unerfüllbar, also stimmt die Behauptung, d.h. das blaue Pedal muss getreten werden.

CoCoA

Zuerst muss die Formel F mit Hilfe der Definition der Folgerung und der der Äquivalenz umgeformt werden:

$$\begin{aligned} F &= R \wedge (R \Leftrightarrow G) \wedge ((R \wedge H) \Rightarrow P) \wedge (G \Rightarrow H) \wedge \neg P \\ &\overset{1.5.b),\,c)}{\equiv} R \wedge [(R \wedge G) \vee (\neg R \wedge \neg G)] \wedge [\neg (R \wedge H) \vee P] \wedge [\neg G \vee H] \wedge \neg P. \end{aligned}$$

- Festlegung des Grundringes:

```
Use Z/(2)[x[1..4]];
```

- Ideale:

```
K:=Ideal(x[1]^2-x[1],x[2]^2-x[2],x[3]^2-x[3],x[4]^2-x[4]);
G:=Ideal(x[1]-1);
H:=Ideal(x[2]-1);
R:=Ideal(x[3]-1);
P:=Ideal(x[4]-1);
```

- Übersetzungen der Teilformeln:
  - $F_0 = R$

```
J0:=R;
```

  - $F_1 = [(R \wedge G) \vee (\neg R \wedge \neg G)]$

```
J1:=Intersection((R+G),(K:R+K:G));
```

  - $F_2 = [\neg (R \wedge H) \vee P]$

```
J2:=Intersection(K:(R+H),P);
```

  - $F_3 = [\neg G \vee H]$

```
J3:=Intersection(K:G,H);
```

  - $F_4 = \neg P$

```
J4:=K:P;
```

- Gesamtformel:

```
J:=J0+J1+J2+J3+J4;
```

- Auswertung:

```
ReducedGBasis(J);
```

  liefert

```
[1].
```

- Ergebnis:
  Also ist $\neg ((F_0 \wedge F_1 \wedge F_2 \wedge F_3) \Rightarrow F_4)$ unerfüllbar, d.h. $(F_0 \wedge F_1 \wedge F_2 \wedge F_3) \Rightarrow F_4$ ist eine Tautologie, somit folgt zwangsläufig aus den Voraussetzungen und Bedingungen (F_1 bis F_4), dass das blaue Pedal (F_5) getreten werden muss.

Lösung 6.6 (Sofies Welt)

- Festlegung der Abkürzungen:

$$\begin{aligned} S &= \text{„Sokrates war ein großer Philosoph“}, \\ P &= \text{„Platon war ein großer Philosoph“}, \\ M &= \text{„Sokrates erschien den Mächtigen Athens gefährlich“}, \\ G &= \text{„Sokrates muss den Schierlingsbecher trinken“}. \end{aligned}$$

- Übersetzung der Aussagen:
  - „Nur dann, wenn Sokrates ein großer Philosoph war, war auch [...] Platon ein großer Philosoph“:
    $$F_1 := (P \Rightarrow S) \equiv (\neg P \vee S).$$
  - „Wenn Sokrates ein großer Philosoph war und den Mächtigen von Athen gefährlich erschien, dann musste er den Schierlingsbecher (Becher mit Gift) trinken“:
    $$F_2 := ((S \wedge M) \Rightarrow G) \equiv (\neg (S \wedge M) \vee G).$$
  - „Sokrates erschien den Mächtigen Athens genau dann gefährlich, wenn auch Platon ein großer Philosoph war“:
    $$F_3 := (M \Leftrightarrow P).$$
  - Behauptung: „Sokrates bekam den Giftbecher, wenn er den Mächtigen von Athen gefährlich erschien“:
    $$H := (M \Rightarrow G) \equiv (\neg M \vee G).$$
- Unerfüllbarkeitsproblem:
  Zu zeigen ist, dass $(F_1 \wedge F_2 \wedge F_3) \Rightarrow H$ eine Tautologie ist, also zeigen wir die Unerfüllbarkeit von

$$\begin{aligned} F := \neg ((F_1 \wedge F_2 \wedge F_3) \Rightarrow H) &\equiv \neg (\neg (F_1 \wedge F_2 \wedge F_3) \vee H) \\ &\equiv F_1 \wedge F_2 \wedge F_3 \wedge \neg H \\ &\equiv (\neg P \vee S) \wedge (\neg (S \wedge M) \vee G) \wedge (M \Leftrightarrow P) \wedge \neg (\neg M \vee G). \end{aligned}$$

- Vereinfachung der Formel:
  Da nach F_3 die Aussagen M und P äquivalent sind, ersetzen wir überall P durch M. Anwenden der de Morganschen Regeln liefert dann

$$F \equiv (\neg M \vee S) \wedge (\neg S \vee \neg M \vee G) \wedge M \wedge \neg G.$$

  Da zur Erfüllbarkeit der Formel $\alpha(M) = 1$ gelten muss, löschen wir das $\neg M$ in den $\vee$–Verknüpfungen (Satz 1.11.e), i)):

$$F \equiv S \wedge (\neg S \vee G) \wedge M \wedge \neg G.$$

  Das gleiche machen wir jetzt mit $\neg S$:

$$F \equiv S \wedge G \wedge M \wedge \neg G.$$

- Da zur Erfüllbarkeit der Formel G und $\neg G$ zusammen gelten müssten, ist F unerfüllbar, also stimmt die Behauptung, d.h. Sokrates bekam den Schierlingsbecher.

CoCoA

Die Formel F muss nur noch mit Hilfe der Definition der Äquivalenz umgeformt werden:

$$\begin{aligned} F &= (\neg P \vee S) \wedge (\neg (S \wedge M) \vee G) \wedge (M \Leftrightarrow P) \wedge \neg (\neg M \vee G) \\ &\overset{1.5.c)}{\equiv} (\neg P \vee S) \wedge (\neg (S \wedge M) \vee G) \wedge [(M \wedge P) \vee (\neg M \wedge \neg P)] \wedge \neg (\neg M \vee G)\,. \end{aligned}$$

- Festlegung des Grundringes:
  `Use Z/(2)[w,x,y,z];`
- Ideale:
  ```
  K:=Ideal(w^2-w,x^2-x,y^2-y,z^2-z);
  G:=Ideal(w-1);
  M:=Ideal(x-1);
  P:=Ideal(y-1);
  S:=Ideal(z-1);
  ```
- Übersetzungen der Teilformeln:
  - $F_1 = (\neg P \vee S)$
    `J1:=Intersection(K:P,S);`
  - $F_2 = (\neg (S \wedge M) \vee G)$
    `J2:=Intersection(K:(S+M),G);`
  - $F_3 = [(M \wedge P) \vee (\neg M \wedge \neg P)]$
    `J3:=Intersection((M+P),(K:M+K:P));`
  - $F_4 = \neg (\neg M \vee G)$
    `J4:=K:Intersection(K:M,G);`
- Gesamtformel:
  `J:=J1+J2+J3+J4;`
- Auswertung:
  `ReducedGBasis(J);`
  liefert
  `[1].`
- Ergebnis:
  Die Formel ist unerfüllbar, somit ist die negierte Formel eine Tautologie, d.h. aus den Bedingungen (F_1 bis F_3) folgt zwangsläufig, dass Sokrates den Giftbecher bekam, wenn er den Mächtigen Athens gefährlich erschien (F_4).