Modellierung

Prof. Dr. Sibylle Schwarz
HTWK Leipzig, Fakultät IM
Gustav-Freytag-Str. 42a, 04277 Leipzig
Zimmer ZU 411 (Zuse-Bau)
https://informatik.htwk-leipzig.de/schwarz
sibylle.schwarz@htwk-leipzig.de

Wintersemester 2026/27

Informatik

Informatik Lehre von der symbolischen Darstellung und Verarbeitung von Information durch Algorithmen

Teilgebiete der Informatik:

theoretisch
- Sprachen zur Formulierung von Information und Algorithmen,
- Möglichkeiten und Grenzen der Berechenbarkeit durch Algorithmen,
- Grundlagen für technische und praktische (und angewandte) Informatik

technisch
- maschinelle Darstellung von Information
- Mittel zur Ausführung von Algorithmen

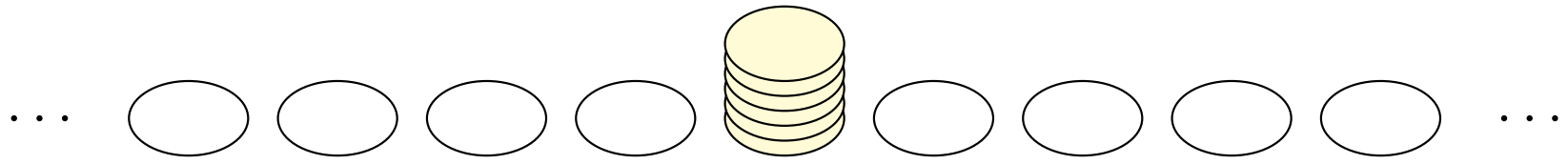
(Rechnerarchitektur, Hardware-Entwurf, Netzwerk, ...)

praktisch Entwurf und Implementierung von Algorithmen (Betriebssysteme, Compilerbau, SE, ...)

angewandt Anwendung von Algorithmen (Text- und Bildverarbeitung, Datenbanken, KI, Medizin-, Bio-, Wirtschafts-, Medien-Informatik, ...)

Beispiel Münzenspiel

Spielfeld:
(unendlich viele) Stapel von Münzen nebeneinander



1. Zu Beginn liegen 5 Münzen auf einem Stapel, alle anderen Stapel sind leer.
2. In jedem Zug werden zwei Münzen von einem Stapel (auf dem wenigstens zwei Münzen liegen) genommen und eine davon auf den rechten, die andere auf den linken Nachbarstapel gelegt.
3. Das Spiel ist zuende, wenn kein Zug mehr möglich ist.

Münzenspiel: Fragen

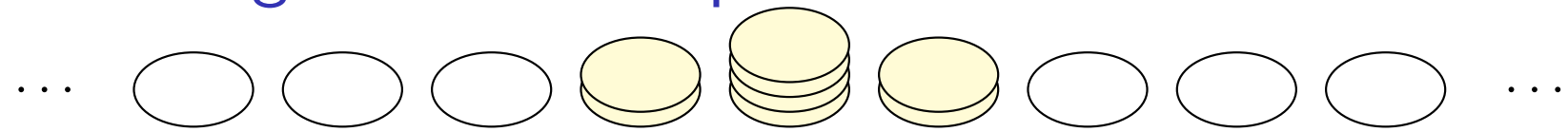
- In welchen Spielzuständen sind keine Züge möglich?
- Welche Zustände sind aus dem Startzustand erreichbar?
- Wieviele Züge können (mindestens / höchstens) gespielt werden, bis kein Zug mehr möglich ist?

Münzenspiel für zwei Personen mit den zusätzlichen Regeln:

4. Beide Spieler ziehen abwechselnd.
5. Wer am Zug ist, wenn kein Zug mehr möglich ist, verliert. (Der andere gewinnt.)

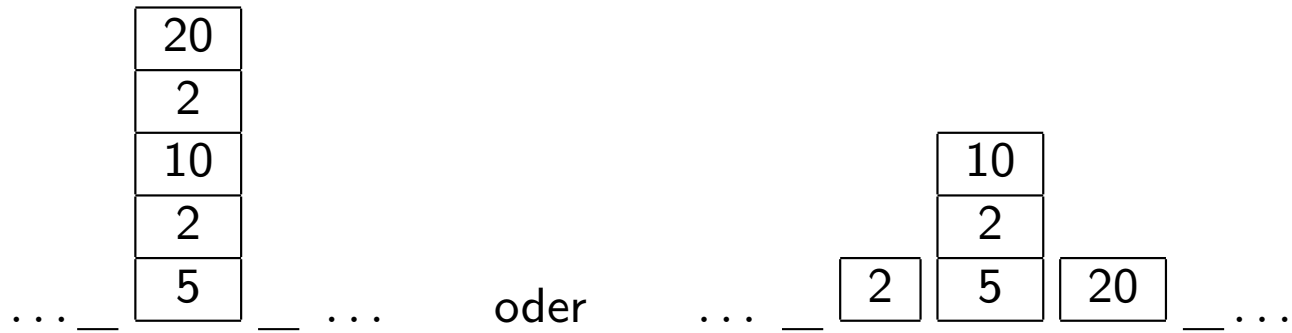
- Kann der Spieler, der den ersten Zug macht, gewinnen?
- Wie kann der Spieler, der den ersten Zug macht, gewinnen?
- Gewinnt immer der Spieler, der den ersten Zug macht?
- (Wie) Hängt das von der Anzahl der Münzen zu Beginn ab?

Modellierung des Münzenspiels: Zustände



Zustand (Konfiguration): Momentaufnahme des Spielfeldes
vor oder nach einem (vollständigen) Spielzug
formale (maschinenlesbare) Modellierung eines Spielzustandes, z.B. durch

- Folge von Stapeln (Folgen) von Münzen verschiedener Werte, z.B.



- Folge natürlicher Zahlen (Anzahlen der Münzen je Stapel),
  z.B. $[\ldots, 0, 5, 0, \ldots]$ oder $[\ldots, 0, 1, 3, 1, 0, \ldots]$
- endliche Folge natürlicher Zahlen (nur relevanter Bereich),
  z.B. $[5]$ oder $[1, 3, 1]$ oder $[0, 5, 0]$ oder $[0, 1, 3, 1, 0]$

Abstraktion von Art und Anzahl der Objekte
ermöglicht einfache Übertragung auf ähnliche Aufgaben

Modellierung des Münzenspiels: Ablauf

Modellierung aller möglichen Übergänge zwischen Zuständen
z.B. als

- formale Darstellung der Spielregeln als (beidseitig unendliche) Folge mit den Positionen $\mathbb{Z} = [\ldots, -2, -1, 0, 1, 2, \ldots]$

  Startzustand : $[\ldots, 0, 5, 0 \ldots]$

  Spielzug: Ersetzung einer Teilfolge des Zustandes der Form $[x, y+2, z]$ durch $[x+1, y, z+1]$
  Regel: $[x, y+2, z] \rightarrow [x+1, y, z+1]$

  Spielende , wenn jedes Element der Folge < 2
  (kein Zug mehr möglich)
- formale (graphische) Darstellung aller möglichen Spielabläufe

Modellierung des Verlaufes eines Spieles z.B. als

- Weg im Spielgraphen
- (gültige) Folge von Positionen in $\mathbb{Z}$,
  an der die (hier einzige) Regel angewendet wurde

Modelle

Modelle sind Abstraktionen (Vereinfachungen)
realer Dinge, Eigenschaften, Beziehungen, Vorgänge

- Auswahl der (für den Anwendungsbereich, zur Problemlösung) wichtigen Informationen
- Vernachlässigung unwichtiger Details

Beispiele:

- Spielzustände im Münzspiel:

  wichtig: lineare Anordnung der Positionen (Spielfeld), Zuordnung von (Münz-)Anzahlen zu Positionen,
  unwichtig: Art und Werte der Münzen, Abstände der Stapel, ...
- Liniennetzplan

  wichtig: Stationen, Verbindungen zwischen Stationen, Art der Verbindung (z.B. Liniennummer)
  unwichtig: genaue Linienführung, aktuelle Verspätungen, Baustellen,...
- Grundriss, Stundenplan, Ablaufplan, Kostenplan
- Holzmodelle von Gebäuden, Modellfahrzeuge (`https://smart-driving.htwk-leipzig.de/`)

Art der Modelle abhängig von Problembereich und geplanter Verwendung

Prozess beim Lösen von Aufgaben (Problemen)

Analyse der (informalen) Aufgabe, Identifikation von

- Aufgabenbereich (Kontext)
- Frage (Typ, mögliche Werte, Eigenschaften der Eingabedaten)
- gewünschte Lösung (Ausgabe: Typ, Eigenschaften, Zusammenhang mit Eingabe)

Modellierung (Abstraktion und formale Darstellung) von

- Aufgabenbereich (Kontext)
- Anforderungen an Eingaben
- Anforderungen an Lösungen

Modellierung von Daten
und deren Eigenschaften und Beziehungen zueinander

Entwurf einer Lösungsstrategie für die modellierte Aufgabe
(mit vorhandenen oder neuen Methoden)
Modellierung von Abläufen und deren Eigenschaften

Umsetzung der Lösungsstrategie im Modellbereich

Ausführung der Lösungsstrategie im Modellbereich

Übertragung der Lösung vom Modellbereich in die Realität

Formalisierung: Syntax und Semantik

algorithmische (maschinelle) Verarbeitung von Information
erfordert geeignete Darstellung der Information

- Formalismus (Kalkül):
  formale Sprache, Maschinen-(und Menschen-)lesbar
- eindeutige Zuordnung einer Bedeutung zu den Elementen des Formalismus

Semantik (Bedeutung)
Was wird dargestellt?

Syntax (Darstellungsform)
Wie wird es dargestellt?
(meist viele verschiedene Möglichkeiten)

Beispiel: Münzspiel

Formale Methoden

Abstraktion von unwichtigen Details
(Entwicklung und Verwendung von Modellen)

Präzisierung der relevanten Aussagen
(eindeutige Semantik)

Systematisches Lösen (auch maschinell) von formal dargestellten Problemen möglich

Struktureigenschaften formaler Beschreibungen Schlussweisen unabhängig von Bedeutung der Aussagen

Aus der Modulbeschreibung

Modul C114 Modellierung (8 ECTS-Punkte)

Arbeitsaufwand: **Präsenzzeit** 6 SWS = 4 SWS V + 2 SWS S
Selbststudienzeit 156 h

Lernziele: Die Studierenden können mathematische und logische Grundkonzepte zur Modellierung praktischer Aufgabenstellungen anwenden.
Sie können Anforderungen an Software und Systeme formal beschreiben und wissen, dass deren Korrektheit mit formalen Methoden nachweisbar ist.

Inhalt der Lehrveranstaltung Modellierung

Einführung in formale Beschreibungsverfahren in der Informatik
Modellierung von

Aussagen durch aussagenlogische Formeln

Daten durch

- Mengen
- Wörter (Folgen) und Sprachen
- Terme

Zusammenhängen (Beziehungen) durch

- Relationen
- Graphen
- Strukturen
- Abstrakte Datentypen

Abläufen durch Zustandübergangssysteme

Eigenschaften, Anforderungen (für Daten und Systeme) durch
Formeln der Prädikatenlogik (der ersten Stufe)
(Ausblick in nichtklassische Logiken)

Lernziele (und Nebenwirkungen)

- Fähigkeit zur Abstraktion
- Verständnis der grundlegenden Modellierungs-Formalismen der Informatik:
  Logik, Mengen, Relationen, Graphen, Terme, Strukturen, Datentypen
- anwendungsbereite Kenntnisse zur Modellbildung
- Zusammenhänge zu anderen Gebieten der Informatik und zur Mathematik

Literatur

Folien zur Vorlesung, jeweils nach der Vorlesung veröffentlicht

`https://informatik.htwk-leipzig.de/schwarz/lehre/ws26/modellierung`

empfohlene Bücher:

- zur Modellierung:
  - Uwe Kastens, Hans Kleine Büning: Modellierung - Grundlagen und formale Methoden, Hanser 2008
- zur Logik
  - Michael Huth, Mark Ryan: Logic in Computer Science, Cambridge University Press 2010
  - Uwe Schöning: Logik für Informatiker, Spektrum, 1995
  - Martin Kreuzer, Stefan Kühling: Logik für Informatiker, Pearson Studium, 2006

Organisation der Lehrveranstaltung

Folien, Übungsserien, Termine, Änderungen, ... unter `https://informatik.htwk-leipzig.de/schwarz/lehre/ws26/modellierung`

Präsenzstudium 6 SWS

Lehrveranstaltungen für jeden Studenten:

Vorlesung jeden Donnerstag und Freitag (4SWS)

Seminar (5 Gruppen) Montag bis Mittwoch (2SWS)

Gäste, Wiederholer (vor JG 26): mit MIB-Gruppen

- Besprechung der Übungsserien (Vorrechnen)
- Fragen zum aktuellen Vorlesungsinhalt

Selbststudium: (incl. PV) 156 h $\approx$ 10 h/Woche

Vor- und Nachbereitung der Vorlesungen anhand Folien und angegebener Literatur

Übungsaufgaben zu jeder Vorlesung (wöchentlich einzusenden)

klar, überschaubar, Feedback

schriftliche Übungsserien (vor Donnerstag)

praktische Aufgaben im Autotool (vor Montag)

Literaturstudium ergänzend, Beitrag zur Lösung der Aufgaben

Selbstudium

Vor- und Nachbereitung jeder Lehrveranstaltung (Vorlesung, Seminar, Praktikum, ...)

Unterlagen zu den Lehrveranstaltungen (Folien, eigene Notizen) durcharbeiten
(enthalten auch zum Lösen der Übungsaufgaben notwendige Definitionen, Herleitungen, Beispiele, . . .)

Übungsaufgaben regelmäßig und rechtzeitig lösen,
(Aufgaben vom Typ der) Übungsaufgaben gehören zum Inhalt des Moduls und werden geprüft

Fachliteratur benutzen (z.B. Bücher, E-Books in Bibliothek), enthalten Erklärungen, zusätzliche Übungsaufgaben
(Internet-Quellen sind oft unzuverlässig)

Lerngruppen bilden und gemeinsam lernen und Aufgaben lösen

Nachfragen bei Dozenten (E-Mail, Sprechzeit, nach der Lehrveranstaltung,. . .), Mitstudenten, älteren Studenten, Fachschaft, . . .

Schriftliche Übungsaufgaben (Übungsserien)

- gestellt jeweils am Donnerstag
  (Aufgaben zu den Vorlesungen am Donnerstag und Freitag)
- Lösungen bis zum folgenden Mittwoch ausschließlich online über OPAL einzusenden (wie in der Einführungswoche erklärt)
  genau eine pdf-Datei je Aufgabe, Dateiname `serieX-aufgY-Z.pdf` für Lösung zu Aufgabe Y von Übungsserie X vom den Studierenden mit Familiennamen Z,
- Lösung in Gruppen aus ≤ 3 Studierenden zulässig (und empfohlen), Namen aller Mitglieder der Gruppe oben auf der Lösung vermerken, jedes Gruppenmitglied sendet die (gemeinsame) Lösung zu Opal Dateiname `serieX-aufgY-Z1-Z2-Z3.pdf`
- Bewertung bis zum folgenden Sonntag
  (0: falsch, 1: überwiegend richtig, 2: korrekt)
- Besprechung in der darauffolgenden Übung
  Vorträge (Vorrechnen) zu den Aufgabenlösungen

Übungsserien auch unter `https://informatik.htwk-leipzig.de/schwarz/lehre/ws26/modellierung`

Nicht im Opal-Kurs eingesendete Lösungen werden nicht gewertet.

Seminar (Übungen)

Lernziele bei der Bearbeitung der Übungsaufgaben:

- Nachbereitung der letzten Vorlesung anhand der Vorlesungsfolien und Literatur (z.B. der angegebenen)
- Vorbereitung der nächsten Vorlesung
- Vorbereitung der Seminarvorträge zu jeder Aufgabe

Seminar (Übungen):

- Besprechung der Lösungen der schriftlichen Übungsaufgaben, Vorrechnen zur Prüfungszulassung
- Fragen zum aktuellen Vorlesungsstoff und zu den neuen schriftlichen und praktischen Übungsaufgaben
- in jede Übung mitbringen: (alles sofort les- und auffindbar) alle bisherigen Vorlesungsfolien und eigene Notizen dazu, Übungsserien und eigene Lösungen

Praktische Hausaufgaben – Autotool

`https://autotool.imn.htwk-leipzig.de/new`

(Einführung am vergangenen Donnerstag)

einmal zu Beginn:

- Anmeldung über Shibboleth (HRZ-Login)
- Click „Einschreibung“,
  eigene Übungsgruppe auswählen

jedes Mal:

- Anmeldung über Shibboleth (HRZ-Login)
- Aufgabe ansehen (Click „Bearbeiten“)
- Aufgabe lösen (meist mit Stift, Papier, Folien, Literatur),
  Lösung in Textfeld eintragen,
  Click „Textfeld absenden“
- Autotool-Antwort lesen und verstehen !

Prüfung

Zulassungsvoraussetzungen (Prüfungsvorleistungen):
regelmäßige erfolgreiche Lösung der Übungsaufgaben,
also alle folgenden drei Bedingungen:

- rechtzeitige Einsendung von richtigen Lösungen
  (mit wenigstens 1 Punkt bewertet) zu wenigstens 70% aller gestellten schriftlichen Übungsaufgaben (OPAL)
- Präsentation: mindestens drei Vorträge in den Seminaren
  (richtiges „Vorrechnen“ der Lösungen)
  je einmal bis Ende November, Dezember und Januar
- 50% aller Punkte für praktische Pflichtaufgaben (Autotool)

Prüfung: Klausur 120 min

Aufgabentypen aus den Übungsserien

einziges zugelassenes Hilfsmittel:
ein beidseitig handbeschriebenes A4-Blatt

Aussagenlogik

Aussagen

Aussage = Behauptung

Beispiele:

- Es regnet.
- Die Straße ist nass.
- 9 ist eine Primzahl.
- $\sqrt{2} \in \mathbb{Q}$
- $3 < 5$
- $x < 5$ (hängt von x ab, keine Aussage)
- Ist $x < 5$? (keine Aussage)
- Sei $x < 5$. (keine Aussage)
- Morgen regnet es.
- Es ist nicht alles Gold, was glänzt.

Wahrheitswerte

Prinzipien der klassischen Logik:

Zweiwertigkeit: Jede Aussage ist wahr oder falsch.

ausgeschlossener Widerspruch:

Keine Aussage ist sowohl wahr als auch falsch.

Wahrheitswerte 1 (wahr) oder 0 (falsch)

Jede Aussage p hat genau einen Wahrheitswert $\mathrm{W}(p) \in \{0, 1\}$.

Beispiele:

- $\mathrm{W}(\text{Es regnet.}) = ?$
- $\mathrm{W}(\text{Die Straße ist nass.}) = ?$
- $\mathrm{W}(\text{9 ist eine Primzahl.}) = 0$
- $\mathrm{W}(\sqrt{2} \in \mathbb{Q}) = 0$
- $\mathrm{W}(3 < 5) = 1$
- $\mathrm{W}(\text{Morgen regnet es.}) = ?$
- $\mathrm{W}(\text{Es ist nicht alles Gold, was glänzt.}) = 1$

Zusammengesetzte Aussagen – Junktoren

Junktor (mit zugeordneter Stelligkeit):
Symbol (Syntax) für Verknüpfung von Aussagen
z.B. „und“ (zweistellig), „nicht“ (einstellig)

Gottlob Frege (1848–1925):

Die Bedeutung des Ganzen ist eine Funktion der Bedeutung seiner Teile.

Der Wahrheitswert einer zusammengesetzten Aussage lässt sich aus den Wahrheitswerten ihrer Teilaussagen berechnen.

Semantik (Bedeutung) eines n-stelligen Junktors $*$:
$[\![*]\!] : \{0,1\}^n \longrightarrow \{0,1\}$
(n-stellige Funktion auf der Menge $\{0,1\}$)

Wahrheitswertkonstanten (nullstellige Junktoren):

$\mathbb{t}$ mit $[\![\mathbb{t}]\!] = 1$

$\mathbb{f}$ mit $[\![\mathbb{f}]\!] = 0$

Konjunktion $\wedge$

Es regnet und 9 ist eine Primzahl.

- W(9 ist eine Primzahl.)$= 0$
- W(Es regnet.)$=?$
- W(Es regnet und 9 ist eine Primzahl.)$=0$

$p \wedge q$ ist genau dann wahr,
wenn beide Aussagen p und q wahr sind.

W(p)	W(q)	W($p \wedge q$)
0	0	0
0	1	0
1	0	0
1	1	1

$$\mathrm{W}(p \wedge q) = \min(\mathrm{W}(p), \mathrm{W}(q))$$

$[\![\wedge]\!] = \min$ ist kommutativ, assoziativ

$$\bigwedge_{i=1}^{n} p_i = p_1 \wedge p_2 \wedge \cdots \wedge p_n$$

Disjunktion $\vee$ (inklusiv)

Es regnet oder $3 < 5$.

- $\mathrm{W}(3 < 5) = 1$
- W(Es regnet)=?
- W(Es regnet oder $3 < 5$.)=1

$p \vee q$ ist genau dann wahr,
wenn wenigstens eine der Aussagen p und q wahr ist.

$\mathrm{W}(p)$	$\mathrm{W}(q)$	$\mathrm{W}(p \vee q)$
0	0	0
0	1	1
1	0	1
1	1	1

$$\mathrm{W}(p \vee q) = \max(\mathrm{W}(p), \mathrm{W}(q))$$

$[\![\vee]\!] = \max$ ist kommutativ, assoziativ

$$\bigvee_{i=1}^{n} p_i = p_1 \vee p_2 \vee \cdots \vee p_n$$

Negation $\neg$

$\neg(\sqrt{2} \in \mathbb{Q})$ (oft auch $\sqrt{2} \notin \mathbb{Q}$)

- $W(\sqrt{2} \in \mathbb{Q}) = 0$
- $W(\neg(\sqrt{2} \in \mathbb{Q})) = 1$

$\neg p$ ist genau dann wahr, wenn p falsch ist.

$W(p)$	$W(\neg p)$
0	1
1	0

$$W(\neg p) = 1 - W(p)$$

Implikation $\rightarrow$

Wenn es regnet, dann ist die Straße nass.

- W(Es regnet.)=?
- W(Die Straße ist nass.)=?
- W(Wenn es regnet, dann ist die Straße nass.)=1

$p \rightarrow q$ ist genau dann wahr,
wenn die Aussage p falsch oder die Aussage q wahr ist.

W(p)	W(q)	W($p \rightarrow q$)
0	0	1
0	1	1
1	0	0
1	1	1

$$\mathrm{W}(p \rightarrow q) = \begin{cases} 1 & \text{falls } \mathrm{W}(p) \leq \mathrm{W}(q) \\ 0 & \text{sonst} \end{cases}$$

Äquivalenz $\leftrightarrow$

$3 < 5$ gilt genau dann, wenn $0 < 5 - 3$ gilt.

- $W(3 < 5) = 1$
- $W(0 < 5 - 3) = 1$
- W(3 < 5 gilt genau dann, wenn $0 < 5 - 3$ gilt.)=1

$p \leftrightarrow q$ ist genau dann wahr, wenn
entweder beide Aussagen p und q gelten
oder beide nicht gelten.

$W(p)$	$W(q)$	$W(p \leftrightarrow q)$
0	0	1
0	1	0
1	0	0
1	1	1

$$W(p \leftrightarrow q) = \begin{cases} 1 & \text{falls } W(p) = W(q) \\ 0 & \text{sonst} \end{cases}$$

Was bisher geschah

- Inhalt und Organisation der Lehrveranstaltung
- Modellierung:
  - Diagramm: Realität – (formales) Modell
    (Aufgabe, Kontext, Lösung)
  - Einordnung in Prozess zur (maschinellen) Lösung von Aufgaben
  - Syntax und Semantik formaler Darstellungen
- Beispiel Münzenspiel: Modellierung von
  - Daten: Spielzustände
  - Abläufen:
    - Spielzug (Zustandsübergang)
    - graphische Darstellung gesamter Spiele
  - Eigenschaften: Endzustände (ohne Zugmöglichkeit)
- (klassische) Aussagenlogik

WH: Aussagenlogik

- Aussage = Behauptung
- Aussagenvariablen p (Syntax)
- klassische Logik: Wahrheitswerte $W(p) \in \{0, 1\}$ (Semantik)
- Kombination von Formeln durch Junktoren (Syntax)
- Wahrheitswert einer zusammengesetzten Formel wird aus Wahrheitswerten der Teilformeln berechnet. (Semantik)

		Syntax	Semantik
	Stelligkeit	Symbol	Wahrheitswertfunktion
wahr	0	$\mathbb{t}$	1
falsch	0	$\mathbb{f}$	0
Konjunktion	2	$\wedge$	min
Disjunktion	2	$\vee$	max
Negation	1	$\neg$	$x \mapsto 1 - x$
Implikation	2	$\rightarrow$	$\leq$
Äquivalenz	2	$\leftrightarrow$	$=$

Modellierung in Aussagenlogik (Beispiele)

- Wenn Leo ein Bier bestellt, bestellt auch Mark eins.
  Aussagen:
  - Leo bestellt Bier.
  - Mark bestellt Bier.

  Aussagenvariablen:
  - lb - Leo bestellt Bier.
  - mb - Mark bestellt Bier.

  Formel: $lb \rightarrow mb$
- Leo und Mark bestellen nie zugleich Bier.
  Formel: $\neg(lb \wedge mb)$
- Mark bestellt höchstens dann Bier, wenn Leo Bier bestellt.
  Formel: $\neg lb \rightarrow \neg mb$
- Wenn es morgens vor 7 oder abends nach 7 ist, ist es dunkel.
  Aussagenvariablen:
  - m - Es ist morgens vor 7.
  - a - Es ist abends nach 7.
  - d - Es ist dunkel.

  Formel: $(m \vee a) \rightarrow d$
- Morgens vor 7 und abends nach 7 ist es dunkel.
  Formel: $(m \rightarrow d) \wedge (a \rightarrow d)$

Aussagenlogische Formeln (Syntax)

Junktoren z.B. $\mathbb{t}, \mathbb{f}$ (nullstellig), $\neg$ (einstellig),
$\wedge, \vee, \rightarrow, \leftrightarrow$ (zweistellig)

Aussagenvariablen (Atome), z.B. $p, q, r, s, \ldots$ oder $p_1, p_2, \ldots$

Definition (induktiv)

Die Menge AL(P) aller aussagenlogischen Formeln mit Aussagenvariablen aus der Menge P ist definiert durch:

IA: Alle Aussagenvariablen $p \in P$ sind Formeln. ($P \subseteq \mathrm{AL}(P)$).

IS:
- $\mathbb{t}$ und $\mathbb{f}$ sind Formeln.
- Ist φ eine Formel, dann ist auch $\neg\varphi$ eine Formel.
- Sind φ und ψ Formeln, dann sind auch $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$ und $\varphi \leftrightarrow \psi$ Formeln.

IS': (Verallgemeinerung aller Unterpunkte zu IS)
Sind j ein n-stelliger Junktor und $\varphi_1, \ldots, \varphi_n$ Formeln, dann ist auch $j(\varphi_1, \ldots, \varphi_n)$ eine Formel.
(Aus $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{AL}(P)$ folgt $j(\varphi_1, \ldots, \varphi_n) \in \mathrm{AL}(P)$.)

Aussagenlogische Formeln (Beispiele)

Junktoren der klassischen Aussagenlogik: $\{\mathbb{t}, \mathbb{f}, \neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$

kürzere Notation:
ohne äußere Klammern und Klammern um $\neg\varphi$

Beispiele:

$\mathbb{t} \wedge (\neg\mathbb{t})$	Formel ohne Aussagenvariablen	$(\in \mathsf{AL}(\emptyset))$
$\neg\neg\neg p$	Formel mit Aussagenvariable p	$(\in \mathsf{AL}(\{p\}))$
$\wedge(p \vee q)$	keine Formel (syntaktisch unkorrekt)	$(\notin \mathsf{AL}(P))$
$\neg(p \rightarrow q)$	Formel mit Aussagenvariablen p, q	$(\in \mathsf{AL}(\{p, q\}))$
$\rightarrow q$	keine Formel (syntaktisch unkorrekt)	$(\notin \mathsf{AL}(P))$

Baumstruktur (analog arithmetischen Termen)

Beispiel:

$$\varphi = ((p \wedge \neg q) \rightarrow (\neg r \vee (p \leftrightarrow q))) \qquad \in \mathsf{AL}(\{p, q, r\})$$

Menge aller Aussagenvariablen einer Formel

Definition (induktiv):
Für jede aussagenlogische Formel $\varphi \in \mathrm{AL}(P)$ ist die Menge $\mathrm{var}(\varphi)$ aller in φ vorkommenden Aussagenvariablen definiert durch:

IA: falls $\varphi = p$ (Atom), dann $\mathrm{var}(\varphi) = \{p\}$

IS:
- nullstellige Junktoren ($\mathbb{t}, \mathbb{f}$):
  für $\varphi = \mathbb{t}$ oder $\varphi = \mathbb{f}$ gilt $\mathrm{var}(\varphi) = \emptyset$
- einstellige Junktoren ($\neg$):
  für $\varphi = \neg\varphi_1$ gilt $\mathrm{var}(\varphi) = \mathrm{var}(\varphi_1)$
- zweistellige Junktoren ($* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$):
  für $\varphi = \varphi_1 * \varphi_2$ gilt $\mathrm{var}(\varphi) = \mathrm{var}(\varphi_1) \cup \mathrm{var}(\varphi_2)$

Beispiel:
Für $\varphi = p \rightarrow ((q \leftrightarrow \mathbb{t}) \vee (r \rightarrow q))$ gilt $\mathrm{var}(\varphi) = \{p, q, r\}$

Anzahl der Variablenvorkommen in einer Formel

Definition (induktiv):
Für jede aussagenlogische Formel $\varphi \in \mathrm{AL}(P)$ ist die Anzahl von Variablenvorkommen varcount(φ) definiert durch:

IA: falls $\varphi = p$ (Atom), dann $\mathrm{varcount}(\varphi) = 1$

IS:
- nullstellige Junktoren ($\mathbb{t}, \mathbb{f}$):
  $\mathrm{varcount}(\mathbb{t}) = \mathrm{varcount}(\mathbb{f}) = 0$
- einstellige Junktoren ($\neg$):
  $\mathrm{varcount}(\neg\varphi) = \mathrm{varcount}(\varphi)$
- zweistellige Junktoren ($* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$):
  $\mathrm{varcount}(\varphi * \psi) = \mathrm{varcount}(\varphi) + \mathrm{varcount}(\psi)$

Beispiel:
$\varphi = p \rightarrow ((q \leftrightarrow \mathbb{t}) \vee (r \rightarrow q))$ gilt $\mathrm{varcount}(\varphi) = 4$

varcount(φ) ist die Anzahl aller mit Variablen markierten Blätter im Formelbaum von φ

Allgemein gilt $\mathrm{varcount}(\varphi) \geq |\mathrm{var}(\varphi)|$

Menge aller Teilformeln einer Formel

Definition (induktiv):
Für jede aussagenlogische Formel $\varphi \in \mathrm{AL}(P)$ ist die Menge $\mathrm{TF}(\varphi)$ aller in φ vorkommenden Teilformeln definiert durch:

IA: falls $\varphi = p$ (Atom), dann $\mathrm{TF}(\varphi) = \{p\}$

IS:
- nullstellige Junktoren ($\mathbb{t}, \mathbb{f}$):
  für $\varphi = \mathbb{t}$ oder $\varphi = \mathbb{f}$ gilt $\mathrm{TF}(\varphi) = \{\varphi\}$
- einstellige Junktoren ($\neg$):
  für $\varphi = \neg\varphi_1$ gilt $\mathrm{TF}(\varphi) = \{\varphi\} \cup \mathrm{TF}(\varphi_1)$
- zweistellige Junktoren ($* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$):
  für $\varphi = \varphi_1 * \varphi_2$ gilt $* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$
  $\mathrm{TF}(\varphi) = \{\varphi\} \cup \mathrm{TF}(\varphi_1) \cup \mathrm{TF}(\varphi_2)$

Beispiel:
Für $\varphi = p \rightarrow ((q \leftrightarrow \mathbb{t}) \vee (r \rightarrow q))$ gilt

$$\mathrm{TF}(\varphi) = \left\{ \begin{array}{l} p \rightarrow ((q \leftrightarrow \mathbb{t}) \vee (r \rightarrow q)), p, (q \leftrightarrow \mathbb{t}) \vee (r \rightarrow q), \\ q \leftrightarrow \mathbb{t}, r \rightarrow q, q, \mathbb{t}, r \end{array} \right\}$$

Prinzip der strukturellen Induktion

Beobachtung:
Bestimmung von Variablenmenge, Größe, Menge der Teilformeln einer aussagenlogischen Formel geschah nach demselben Schema:

Definition einer Funktion $f : \mathrm{AL}(P) \to X$ durch

Induktion über die Struktur der Formel

Für jede aussagenlogische Formel $\varphi \in \mathrm{AL}(P)$ ist der Funktionswert $f(\varphi)$ definiert durch:

- IA: Definition des Funktionswertes $f(\varphi)$ für Atome $\varphi = p$ (Blätter im Formelbaum)
- IS: Definition des Funktionswertes $f(\varphi)$ für zusammengesetzte Formeln φ durch die Funktionswerte der Teilformeln von φ

Aussagenlogische Interpretationen (Semantik)

(Belegungen der Aussagenvariablen mit Wahrheitswerten)

Interpretation (Belegung) für Formeln $\varphi \in \mathrm{AL}(P)$:
ordnet jeder Aussagenvariable in P einen Wahrheitswert zu,
ist eine Funktion $W : P \longrightarrow \{0, 1\}$
(eine Zeile in der WW-Tabelle für φ)

Beispiel: $P = \{p, q\}$ und W_{10} mit $W_{10}(p) = 1$ und $W_{10}(q) = 0$

Wahrheitswerte für Formeln

Belegung $W : P \to \{0,1\}$ fortgesetzt zu Funktion $W : \mathrm{AL}(P) \to \{0,1\}$

Der Wert $W(\varphi)$ der Formel φ in der Interpretation W wird induktiv mit den Wahrheitswertfunktionen der Junktoren
aus den Werten der Teilformeln von φ bestimmt:

IA: falls $\varphi = p$ (Atom), dann $W(\varphi) = W(p)$

IS:
- nullstellige Junktoren $\mathbb{t}, \mathbb{f}$: $W(\mathbb{t}) = 1$, $W(\mathbb{f}) = 0$
- einstelliger Junktor $\neg$:
  für $\varphi = \neg\psi$ gilt $W(\neg\psi) = [\![\neg]\!]\, W(\psi) = 1 - W(\psi)$
- zweistellige Junktoren $* \in \{\vee, \wedge, \to, \leftrightarrow\}$:

$$
\begin{array}{lcll}
W(\psi_1 \wedge \psi_2) & = & W(\psi_1)[\![\wedge]\!]\, W(\psi_2) & = \min\left(W(\psi_1), W(\psi_2)\right) \\
W(\psi_1 \vee \psi_2) & = & W(\psi_1)[\![\vee]\!]\, W(\psi_2) & = \max\left(W(\psi_1), W(\psi_2)\right) \\
W(\psi_1 \to \psi_2) & = & W(\psi_1)[\![\to]\!]\, W(\psi_2) & = \begin{cases} 1 & \text{falls } W(\psi_1) \leq W(\psi_2) \\ 0 & \text{sonst} \end{cases} \\
W(\psi_1 \leftrightarrow \psi_2) & = & W(\psi_1)[\![\leftrightarrow]\!]\, W(\psi_2) & = \begin{cases} 1 & \text{falls } W(\psi_1) = W(\psi_2) \\ 0 & \text{sonst} \end{cases}
\end{array}
$$

Beispiel: $\varphi = ((p \wedge \neg q) \to (\neg r \vee (p \leftrightarrow q)))$

$W_{010}(p) = 0,\ W_{010}(q) = 1,\ W_{010}(r) = 0,\ W_{010}(\varphi) = \ldots$

Wahrheitswerttabellen

Darstellung der Werte einer Formel $\varphi \in \mathrm{AL}(P)$ in allen möglichen Interpretationen $W \in \mathbb{W}(P)$ in einer Tabelle

Jede Zeile repräsentiert eine Interpretationen $W : \mathrm{var}(\varphi) :\to \{0,1\}$

$W(p_1)$	$W(p_2)$	$\cdots$	$W(p_{n-1})$	$W(p_n)$	$W(\varphi)$
0	0	$\cdots$	0	0	
0	0	$\cdots$	0	1	
		$\vdots$			
1	1	$\cdots$	1	1	

Beispiel:$((p \wedge \neg q) \to (\neg r \vee (p \leftrightarrow q)))$

Wahrheitswerttabellen von Formeln φ mit n Aussagenvariablen sind Wertetabellen n-stelliger Boolescher Funktionen $f_\varphi : \{0,1\}^n \longrightarrow \{0,1\}$.

Die Semantik jeder aussagenlogischen Formel φ mit n Aussagenvariablen ist eine n-stellige Boolesche Funktion.

Modelle aussagenlogischer Formeln

Die Belegung $W : P \to \{0, 1\}$ der Aussagenvariablen in P erfüllt die Formel $\varphi \in \mathrm{AL}(P)$ (ist ein Modell von φ) genau dann, wenn $W(\varphi) = 1$.

Beispiel:
Modelle (erfüllende Belegungen) der Formel

$$\varphi = p \vee (q \wedge \neg p) \in \mathrm{AL}(\{p, q\})$$

- Belegung $W_{10} : \{p, q\} \to \{0, 1\}$ mit $W_{10}(p) = 1$ und $W_{10}(q) = 0$ ist ein Modell für φ, weil $W_{10}(\varphi) = 1$.
- Belegung $W_{00} : \{p, q\} \to \{0, 1\}$ ist kein Modell für φ, weil $W_{00}(\varphi) = 0$.
- W_{01} mit $W_{01}(p) = 0$ und $W_{01}(q) = 1$ ist ein Modell für φ,
- W_{11} mit $W_{11}(p) = 1$ und $W_{11}(q) = 1$ ist ein Modell für φ.

Modellmengen aussagenlogischer Formeln

Modellmenge (Menge aller Modelle) der Formel $\varphi \in \mathrm{AL}(P)$:

$$\mathrm{Mod}(\varphi) = \{W : P \to \{0,1\} \mid W(\varphi) = 1\}$$

(Diese Darstellung ist oft kürzer als die WW-Tabelle)

Beispiele:

- $\mathrm{Mod}(p \vee (q \wedge \neg p)) = \{W_{10}, W_{01}, W_{11}\}$,
- $\mathrm{Mod}(p \to p) = \{W_0, W_1\} = \{W : \{p\} \to \{0,1\}\}$ (alle möglichen Belegungen für p),
- $\mathrm{Mod}(p \wedge \neg p) = \emptyset$

Was bisher geschah: klassische Aussagenlogik

Syntax Symbole und Struktur

- Menge P von Aussagenvariablen $(p, q, r, \ldots)$
- Junktoren (je mit Stelligkeit):
  $\mathbb{t}(0), \mathbb{f}(0), \neg(1), \vee(2), \wedge(2), \rightarrow(2), \leftrightarrow(2)$
- aussagenlogische Formeln $\mathrm{AL}(P)$ (induktive Def.):
  - IA Atome (Aussagenvariablen) $\in P$
  - IS zusammengesetzte Formeln $(\varphi, \psi, \eta, \ldots)$:
    Verknüpfung von Formeln durch Junktoren

Prinzip der strukturellen Induktion über Baumstruktur von Formeln

Semantik (Bedeutung der Syntaxelemente)

- einer Aussagenvariablen: Wahrheitswert $\in \{0, 1\}$
- aller Aussagenvariablen einer Menge P:
  Belegung (Interpretation) $W : P \rightarrow \{0, 1\}$
- eines n-stelligen Junktors $*$:
  Wahrheitswertfunktion $[\![*]\!] : \{0, 1\}^n \rightarrow \{0, 1\}$
- einer Formel unter einer Belegung W:
  Funktion $W : \mathrm{AL}(P) \rightarrow \{0, 1\}$
- Modell (erfüllende Belegung) für $\varphi \in \mathrm{AL}(P)$:
  Belegung $W : P \rightarrow \{0, 1\}$ mit $W(\varphi) = 1$
- Modellmenge $\mathrm{Mod}(\varphi)$ der Formel $\varphi \in \mathrm{AL}(P)$:
  Menge aller Modelle von φ

WH: Modelle aussagenlogischer Formeln

Die Belegung $W : P \to \{0, 1\}$ der Aussagenvariablen in P erfüllt die Formel $\varphi \in \mathrm{AL}(P)$ (ist ein Modell von φ) genau dann, wenn $W(\varphi) = 1$.

Modellmenge (Menge aller Modelle) der Formel $\varphi \in \mathrm{AL}(P)$:

$$\mathrm{Mod}(\varphi) = \{W : P \to \{0, 1\} \mid W(\varphi) = 1\}$$

(Diese Darstellung ist oft kürzer als die WW-Tabelle)

Beispiele:

- $\mathrm{Mod}(p \vee (q \wedge \neg p)) = \{W_{10}, W_{01}, W_{11}\}$,
- $\mathrm{Mod}(p \to p) = \{W_0, W_1\} = \{W : \{p\} \to \{0, 1\}\}$ (alle möglichen Belegungen für p),
- $\mathrm{Mod}(p \wedge \neg p) = \emptyset$

Modellierungsbeispiel Party

umgangssprachliche Beschreibung der Situation (Kontext):

Anna geht zur Party, wenn Max oder Paul hingehen. (1)

Max geht zur Party, wenn Paul nicht hingeht. (2)

Anna geht nirgends ohne ihren Hund hin. (3)

formale Beschreibung der Situation:

- elementare Aussagen (Atome):

  a Anna geht zur Party.

  m Max geht zur Party.

  p Paul geht zur Party.

  h Annas Hund geht zur Party.

  $P = \{a, h, m, p\}$ (Menge der Aussagenvariablen)

- zusammengesetzte Aussage (aussagenlogische Formel):

$$\varphi = \underbrace{((m \vee p) \to a)}_{(1)} \wedge \underbrace{(\neg p \to m)}_{(2)} \wedge \underbrace{\neg(a \wedge \neg h)}_{(3)} \in \mathrm{AL}(P)$$

Modellmenge $\mathrm{Mod}(\varphi) = \ldots$

Menge aller Situationen, in denen alle Aussagen wahr sind

Welche dieser Situationen ist Hunde-frei? $\mathrm{Mod}(\varphi \wedge \neg h) = \ldots$

Erfüllbarkeit und Allgemeingültigkeit von Formeln

Definition: Eine Formel $\varphi \in \mathrm{AL}(P)$ heißt

erfüllbar , wenn $\mathrm{Mod}(\varphi) \neq \emptyset$,
also (wenigstens) eine Belegung $W : P \to \{0,1\}$ mit $W(\varphi) = 1$ existiert
Beispiel: $\neg p \to p$

unerfüllbar (Widerspruch), wenn $\mathrm{Mod}(\varphi) = \emptyset$,
also keine Belegung $W : P \to \{0,1\}$ mit $W(\varphi) = 1$ existiert.
(wenn also für jede Belegung W gilt $W(\varphi) = 0$),
Beispiel: $p \wedge \neg p$

allgemeingültig (Tautologie), wenn $\mathrm{Mod}(\varphi) = \{W : P \to \{0,1\}\}$,
also für jede Belegung $W : P \to \{0,1\}$ gilt $W(\varphi) = 1$
(wenn also keine Belegung W mit $W(\varphi) = 0$ existiert).
Beispiel: $p \to p$

Fakt

Eine Formel $\varphi \in \mathrm{AL}(P)$ ist genau dann allgemeingültig, wenn die Formel $\neg\varphi$ unerfüllbar ist.

Beweis: ...

Formelmengen

Formelmenge $\Phi \subseteq \mathrm{AL}(P)$

(Menge von Bedingungen)

Beispiele:

- $\{p, p \to q\} \subseteq \mathrm{AL}(P)$
- $\{p, p \to q, \neg q\} \subseteq \mathrm{AL}(P)$
- $\{p \to q\} \subseteq \mathrm{AL}(P)$
- $\emptyset \subseteq \mathrm{AL}(P)$

Semantik von Formelmengen

Eine Belegung $W : P \to \{0, 1\}$ erfüllt eine Menge $\Phi \subseteq \mathrm{AL}(P)$ von Formeln genau dann, wenn W jede Formel $\varphi \in \Phi$ erfüllt.

Beispiele:

- einziges Modell für $\{p, p \to q\}$: W_{11}
- $\{p, p \to q, \neg q\}$ hat kein Modell,
- Modelle für $\{p \to q\}$: W_{00}, W_{01}, W_{11}
- Jede Belegung ist ein Modell für die Formelmenge $\emptyset$.

Modellmengen von Formelmengen

Menge aller Modelle einer Menge $\Phi \subseteq \mathrm{AL}(P)$ von Formeln:

$$\mathrm{Mod}(\Phi) = \{W : P \to \{0,1\} \mid \text{ für jedes } \psi \in \Phi \text{ gilt } W \in \mathrm{Mod}(\psi)\}$$

kürzere Formulierung derselben Definition: $\mathrm{Mod}(\Phi) = \bigcap_{\psi \in \Phi} \mathrm{Mod}(\psi)$

Beispiele:

- $\mathrm{Mod}(\{p, p \to q\}) = \mathrm{Mod}(\{p\}) \cap \mathrm{Mod}(\{p \to q\})$
  $= \{W_{10}, W_{11}\} \cap \{W_{00}, W_{01}, W_{11}\} = \{W_{11}\}$,
- $\mathrm{Mod}(\{p, p \to q, \neg q\}) = \emptyset$,
- $\mathrm{Mod}(\{p \to q\}) = \{W_{00}, W_{01}, W_{11}\}$
- $\mathrm{Mod}(\emptyset) = \{W : P \to \{0,1\}\}$ (Menge aller Belegungen)

Fakt

Eine Belegung $W : P \to \{0,1\}$ erfüllt eine endliche Formelmenge $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ genau dann, wenn sie die Formel $\varphi_1 \wedge \cdots \wedge \varphi_n$ erfüllt.

kürzere Formulierung derselben Aussage: $\mathrm{Mod}(\Phi) = \mathrm{Mod}\left(\bigwedge_{\psi \in \Phi} \psi\right)$

Modellierung durch aussagenlogische Formelmengen

Aussagen:

1. Es wird nicht mehr viel Eis gekauft, wenn es kalt ist.
2. Der Eisverkäufer ist traurig, wenn nicht viel Eis gekauft wird.
3. Es ist kalt.

Darstellung als Formelmenge $\Phi \subseteq \mathrm{AL}(\{k, t, v\})$:

$$\Phi = \{k \to \neg v, \neg v \to t, k\}$$

$\mathrm{Mod}(\Phi) = \{W_{110}\}$

neue zusätzliche Aussage:

4. Der Eisverkäufer ist nicht traurig.

Erweiterung der Formelmenge Φ zu

$$\Phi' = \Phi \cup \{\neg t\} = \{k \to \neg v, \neg v \to t, k, \neg t\}$$

$\mathrm{Mod}(\Phi') = \emptyset$ (Formelmenge Φ' unerfüllbar)

Semantische Äquivalenz aussagenlogischer Formeln

Definition

Zwei Formeln $\varphi, \psi \in \mathrm{AL}(P)$ heißen genau dann
(semantisch) äquivalent ($\varphi \equiv \psi$), wenn $\mathrm{Mod}(\varphi) = \mathrm{Mod}(\psi)$.

alternative Formulierung:
$\varphi \equiv \psi$ gdw. für jede Belegung $W : P \to \{0, 1\}$ gilt $W(\varphi) = W(\psi)$.

Äquivalente Formeln haben dieselbe Semantik (Wahrheitswertfunktion).

Beispiele: $p \to q \equiv \neg p \vee q$, $p \vee q \equiv \neg p \to q$

allgemein: Für alle Formeln $\varphi, \psi \in \mathrm{AL}(P)$ gilt

$$\begin{aligned} \varphi \to \psi &\equiv \neg\varphi \vee \psi \\ \varphi \vee \psi &\equiv \neg\varphi \to \psi \\ \varphi \wedge \psi &\equiv \neg(\varphi \to \neg\psi) \\ \varphi \leftrightarrow \psi &\equiv (\varphi \to \psi) \wedge (\psi \to \varphi) \end{aligned}$$

Achtung: Das Symbol $\equiv$ ist kein Junktor (Syntax), sondern ein Symbol für eine Beziehung zwischen Formeln (Semantik).

Aber: Für alle Formeln $\varphi, \psi \in \mathrm{AL}(P)$ lässt sich beweisen:
$\varphi \equiv \psi$ gilt genau dann, wenn die Formel $\varphi \leftrightarrow \psi$ allgemeingültig ist.

Wichtige Äquivalenzen

Für alle aussagenlogischen Formeln $\varphi, \psi, \eta \in \mathsf{AL}(P)$ gilt:

- $\varphi \vee \varphi \equiv \varphi, \quad \varphi \wedge \varphi \equiv \varphi, \quad \varphi \vee \mathbb{f} \equiv \varphi, \quad \varphi \wedge \mathbb{t} \equiv \varphi$
- $\varphi \vee \psi \equiv \psi \vee \varphi, \quad \varphi \wedge \psi \equiv \psi \wedge \varphi$
  (Kommutativität von $\wedge$ und $\vee$)
- $\varphi \vee (\psi \vee \eta) \equiv (\varphi \vee \psi) \vee \eta$
  $\varphi \wedge (\psi \wedge \eta) \equiv (\varphi \wedge \psi) \wedge \eta$
  (Assoziativität von $\wedge$ und $\vee$)
- $\varphi \wedge (\psi \vee \eta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \eta)$
  $\varphi \vee (\psi \wedge \eta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \eta)$
  (Distributivgesetze)
- $\neg\neg\varphi \equiv \varphi$ (Doppelnegation)
- $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi, \quad \neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$
  (DeMorgansche Regeln)
- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi), \quad \varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$
  (Dualität von $\wedge$ und $\vee$)
- $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$ (Kontraposition)
- $(\varphi \wedge \psi) \vee (\neg\varphi \wedge \psi) \equiv \psi$ (Fallunterscheidung)

Was bisher geschah: klassische Aussagenlogik

Syntax Symbole und Struktur, Junktoren: $\mathbb{t}, \mathbb{f}$, $\neg$, $\vee, \wedge, \rightarrow, \leftrightarrow$

Prinzip der strukturellen Induktion über Baumstruktur von Formeln, arithmetischen Ausdrücken usw.

- induktive Definition von (unendlichen) Mengen
- induktive Definition von Funktionen auf induktiv definierten Mengen

Semantik (Bedeutung der Syntaxelemente)

- eines Junktors: Wahrheitswertfunktion
- einer Aussagenvariablen: Wahrheitswert
- einer Formel aus AL(P) unter einer Belegung $W : P \rightarrow \{0, 1\}$: Funktion $W : \mathrm{AL}(P) \rightarrow \{0, 1\}$
- einer Formel aus AL(P) unter allen möglichen Belegungen: Boolesche Funktion
- Modelle (erfüllende Belegungen) von Formeln
- Modellmengen aussagenlogischer Formeln
- Erfüllbarkeit, Allgemeingültigkeit von Formeln
- semantische Äquivalenz von Formeln

WH: Semantische Äquivalenz aussagenlogischer Formeln

Definition

Zwei Formeln $\varphi, \psi \in \mathrm{AL}(P)$ heißen genau dann
(semantisch) äquivalent ($\varphi \equiv \psi$), wenn $\mathrm{Mod}(\varphi) = \mathrm{Mod}(\psi)$.

alternative Formulierung:
$\varphi \equiv \psi$ gdw. für jede Belegung $W : P \to \{0, 1\}$ gilt $W(\varphi) = W(\psi)$.

Äquivalente Formeln haben dieselbe Semantik (Wahrheitswertfunktion).

Beispiele: $p \to q \equiv \neg p \vee q$, $p \vee q \equiv \neg p \to q$

allgemein: Für alle Formeln $\varphi, \psi \in \mathrm{AL}(P)$ gilt

$$\begin{aligned} \varphi \to \psi &\equiv \neg\varphi \vee \psi \\ \varphi \vee \psi &\equiv \neg\varphi \to \psi \\ \varphi \wedge \psi &\equiv \neg(\varphi \to \neg\psi) \\ \varphi \leftrightarrow \psi &\equiv (\varphi \to \psi) \wedge (\psi \to \varphi) \end{aligned}$$

Achtung: Das Symbol $\equiv$ ist kein Junktor (Syntax), sondern ein Symbol für eine Beziehung zwischen Formeln (Semantik).

Aber: Für alle Formeln $\varphi, \psi \in \mathrm{AL}(P)$ lässt sich beweisen:
$\varphi \equiv \psi$ gilt genau dann, wenn die Formel $\varphi \leftrightarrow \psi$ allgemeingültig ist.

WH: Wichtige Äquivalenzen

Für alle aussagenlogischen Formeln $\varphi, \psi, \eta \in \mathsf{AL}(P)$ gilt:

- $\varphi \vee \varphi \equiv \varphi, \quad \varphi \wedge \varphi \equiv \varphi, \quad \varphi \vee \mathbb{f} \equiv \varphi, \quad \varphi \wedge \mathbb{t} \equiv \varphi$
- $\varphi \vee \psi \equiv \psi \vee \varphi, \quad \varphi \wedge \psi \equiv \psi \wedge \varphi$
  (Kommutativität von $\wedge$ und $\vee$)
- $\varphi \vee (\psi \vee \eta) \equiv (\varphi \vee \psi) \vee \eta$
  $\varphi \wedge (\psi \wedge \eta) \equiv (\varphi \wedge \psi) \wedge \eta$
  (Assoziativität von $\wedge$ und $\vee$)
- $\varphi \wedge (\psi \vee \eta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \eta)$
  $\varphi \vee (\psi \wedge \eta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \eta)$
  (Distributivgesetze)
- $\neg\neg\varphi \equiv \varphi$ (Doppelnegation)
- $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi, \quad \neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$
  (DeMorgansche Regeln)
- $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi), \quad \varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$
  (Dualität von $\wedge$ und $\vee$)
- $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$ (Kontraposition)
- $(\varphi \wedge \psi) \vee (\neg\varphi \wedge \psi) \equiv \psi$ (Fallunterscheidung)

WH: Nachweis von Aussagen über alle Formeln

Aussagen der Form: Für alle Formeln $\varphi, \psi \in \mathsf{AL}(P)$ gilt ...
lassen sich nicht mit Wahrheitswerttabellen nachweisen.

Beispiel:
Für alle Formeln $\varphi, \psi \in \mathsf{AL}(P)$ gilt $\varphi \to \psi \equiv \neg\varphi \vee \psi$
Nach Definition von $\equiv$ ist zu zeigen: $\mathsf{Mod}(\varphi \to \psi) = \mathsf{Mod}(\neg\varphi \vee \psi)$

$$
\begin{aligned}
\mathsf{Mod}(\varphi \to \psi) &\overset{\text{Def. Mod}}{=} \{W : P \to \{0,1\} \mid W(\varphi \to \psi) = 1\} \\
&\overset{\text{Def. } [\![\to]\!]}{=} \{W : P \to \{0,1\} \mid W(\varphi) \leq W(\psi)\} \\
&\overset{\text{Def. } \leq}{=} \{W : P \to \{0,1\} \mid W(\varphi) = 0 \text{ oder } W(\psi) = 1\} \\
&\overset{\text{Def. } [\![\neg]\!]}{=} \{W : P \to \{0,1\} \mid W(\neg\varphi) = 1 \text{ oder } W(\psi) = 1\} \\
&\overset{\text{Def. max}}{=} \{W : P \to \{0,1\} \mid \max(W(\neg\varphi), W(\psi)) = 1\} \\
&\overset{\text{Def. } [\![\vee]\!]}{=} \{W : P \to \{0,1\} \mid W(\neg\varphi \vee \psi)) = 1\} \\
&\overset{\text{Def. Mod}}{=} \mathsf{Mod}(\neg\varphi \vee \psi)
\end{aligned}
$$

WH: Strukturelle Induktion

Induktive Definition von Mengen

Beispiel: Menge $\mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\})$ aller aussagenlogischen Formeln, die nur die Aussagenvariablen p, q und die Junktoren $\neg$ und $\rightarrow$ enthalten

- IA: Grundbausteine, im Bsp.: elementare Formeln (Atome) p, q
- IS: Regeln zur Konstruktion zusammengesetzter Elemente
  im Bsp.: Zusammensetzen von Formeln durch Junktoren
  Für alle Formeln φ_1 und φ_2 aus der Menge $\mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\})$
  sind auch $\neg\varphi_1$ und $\varphi_1 \rightarrow \varphi_2$ in der Menge $\mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\})$.

Beispiel: $\neg p \rightarrow (\neg q \rightarrow p) \in \mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\})$, $\neg p \vee q \notin \mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\})$

ermöglicht induktive Definition von Funktionen auf induktiv definierten Mengen (Beispiel: Funktion $f : \mathrm{AL}_{\{\neg,\rightarrow\}}(\{p,q\}) \rightarrow \mathbb{Z}$):

- IA: Funktionswert für Grundbausteine, z.B. $f(p) = 2$, $f(q) = 3$
- IS: Vorschrift zur Berechnung des Funktionswertes des zusammengesetzten Elementes aus Funktionswerten der Teilstrukturen
  z.B. $f(\neg\varphi_1) = 2f(\varphi_1)$, $f(\varphi_1 \rightarrow \varphi_2) = f(\varphi_1) + 3f(\varphi_2)$

Beispiel: $f(\neg p \rightarrow (\neg q \rightarrow p)) = 40$

Beweise durch strukturelle Induktion

Induktiver Nachweis von Eigenschaften (E) jedes Elementes induktiv definierter Mengen

Beispiel: Für jede Formel $\varphi \in \mathrm{AL}_{\{\neg,\rightarrow\}}(\{p\})$ gilt $f(\varphi) > \mathrm{varcount}(\varphi)$ (E)

IA: Nachweis der Eigenschaft (E) für Grundbausteine,
im Bsp.: $f(p) \overset{\text{(Def. } f\text{)}}{=} 2 > 1 \overset{\text{(Def. varcount)}}{=} \mathrm{varcount}(p)$

IS: Nachweis der Eigenschaft (E) für zusammengesetzte Elemente aus den Nachweisen der Eigenschaft für die Teilstrukturen

IH (Induktionshypothese): Eigenschaft (E) für Teilstrukturen
im Bsp.: $f(\varphi_1) > \mathrm{varcount}(\varphi_1)$ und $f(\varphi_2) > \mathrm{varcount}(\varphi_2)$

IB (Induktionsbehauptung): Eigenschaft (E) für die (aus diesen Teilstrukturen) zusammengesetzten Elemente, im Bsp.:
$f(\neg\varphi_1) > \mathrm{varcount}(\neg\varphi_1)$, $f(\varphi_1 \rightarrow \varphi_2) > \mathrm{varcount}(\varphi_1 \rightarrow \varphi_2)$

B (Induktionsbeweis): Nachweis, dass IB aus IH folgt, Bsp.:

$$f(\neg\varphi_1) = 2f(\varphi_1) \overset{\text{(IH)}}{>} 2\mathrm{varcount}(\varphi_1) \geq \mathrm{varcount}(\varphi_1) = \mathrm{varcount}(\neg\varphi_1)$$

$$\begin{aligned} f(\varphi_1 \rightarrow \varphi_2) = f(\varphi_1) + 3f(\varphi_2) &\overset{\text{(IH)}}{>} \mathrm{varcount}(\varphi_1) + 3\mathrm{varcount}(\varphi_2) \\ &\geq \mathrm{varcount}(\varphi_1) + \mathrm{varcount}(\varphi_2) = \mathrm{varcount}(\varphi_1 \rightarrow \varphi_2) \end{aligned}$$

Junktorbasen (vollständige Operatorensysteme)

Zu einer Menge J von Junktoren ist die Menge $\mathrm{AL}_J(P)$ definiert durch

IA: Für jede Aussagenvariable $p \in P$ gilt $p \in \mathrm{AL}_J(P)$

IS:
- für jeden 0-stelligen Junktor $* \in J$ gilt $* \in \mathrm{AL}_J(P)$
- für jeden 1-stelligen Junktor $* \in J$ und alle Formeln $\varphi \in \mathrm{AL}_J(P)$ gilt $*\varphi \in \mathrm{AL}_J(P)$
- für jeden 2-stelligen Junktor $* \in J$ und alle Formeln $\varphi, \psi \in \mathrm{AL}_J(P)$ gilt $\varphi * \psi \in \mathrm{AL}_J(P)$

Definition: Eine Menge J von Junktoren heißt genau dann Junktorbasis (vollständiges Operatorensystem), wenn zu jeder Formel $\varphi \in \mathrm{AL}(P)$ eine Formel $\psi \in \mathrm{AL}_J(P)$ mit $\varphi \equiv \psi$ existiert.

Beispiele:

- Die Mengen $\{\neg, \vee, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \wedge\}$ sind Junktorbasen.
- Die Mengen $\{\neg, \rightarrow\}$, $\{\mathbb{f}, \rightarrow\}$ sind Junktorbasen. (ÜA)
- Die Mengen $\{\vee, \wedge\}$ und $\{\vee, \wedge, \rightarrow\}$ sind keine Junktorbasen. (ÜA)

Beweis durch strukturelle Induktion – Beispiel

Fakt: Die Menge $\{\neg, \vee, \wedge\}$ ist eine Junktorbasis.

alternative Formulierung:
Zu jeder Formel $\varphi \in \mathrm{AL}(P)$ existiert eine Formel ψ mit den Eigenschaften

E1 $\psi \in \mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$ und

E2 $\varphi \equiv \psi$ (d.h. $\mathrm{Mod}(\varphi) = \mathrm{Mod}(\psi)$)

Beweis: induktiv über die Struktur von $\varphi \in \mathrm{AL}(P)$
(Konstruktion einer Formel ψ mit den Eigenschaften E1 und E2):
Induktionsanfang: $\varphi = p \in P$
Zu jedem $\varphi = p \in P$ erfüllt $\psi = p$ (Ansatz) beide Eigenschaften

E1 $\psi \in \mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$, nach IA in der Def. von $\mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$ und

E2 $\varphi \equiv \psi$, wegen $\mathrm{Mod}(\varphi) = \mathrm{Mod}(p) = \mathrm{Mod}(\psi)$

Beweis durch strukturelle Induktion – IH und IB

Induktionsschritt: φ ist eine zusammengesetzte Formel

IH : Zu $\varphi_1, \varphi_2 \in \mathsf{AL}(P)$ existieren Formeln ψ_1, ψ_2 mit

- E1 $\psi_1, \psi_2 \in \mathsf{AL}_{\{\neg,\vee,\wedge\}}(P)$ und
- E2 $\varphi_1 \equiv \psi_1$ und $\varphi_2 \equiv \psi_2$

IB : für jede mögliche Struktur (Junktor in der Wurzel) von φ

- IB$\neg$: zu $\varphi = \neg\varphi_1$ existiert eine Formel ψ mit
  - E1 $\psi \in \mathsf{AL}_{\{\neg,\vee,\wedge\}}(P)$ und
  - E2 $\varphi \equiv \psi$
- IB$\vee$: zu $\varphi = \varphi_1 \vee \varphi_2$ existiert eine Formel ψ mit E1 und E2
- IB$\wedge$: zu $\varphi = \varphi_1 \wedge \varphi_2$ existiert eine Formel ψ mit E1 und E2
- IB$\rightarrow$: zu $\varphi = \varphi_1 \rightarrow \varphi_2$ existiert eine Formel ψ mit E1 und E2
- IB$\leftrightarrow$: zu $\varphi = \varphi_1 \leftrightarrow \varphi_2$ existiert eine Formel ψ mit E1 und E2
- IB$\mathbb{t}$: zu $\varphi = \mathbb{t}$ existiert eine Formel ψ mit E1 und E2
- IB$\mathbb{f}$: zu $\varphi = \mathbb{f}$ existiert eine Formel ψ mit E1 und E2

Beweis durch strukturelle Induktion – (einfache) Beweise

Induktionsschritt: Beweise

(Schritt B für jede mögliche Struktur der Formel $\varphi \in \mathrm{AL}(P)$)

B$\neg$: z.z.: aus IH folgt IB$\neg$, Ansatz: $\psi = \neg\psi_1$

Beweis: Für $\psi = \neg\psi_1$ gelten

E1 $\psi \in \mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$ gilt wegen $\psi_1 \in \mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$ (nach IH) und IS (für $\neg$) in der Definition von $\mathrm{AL}_{\{\neg,\vee,\wedge\}}(P)$

E2 $\varphi \equiv \psi$ (wird gezeigt durch $\mathrm{Mod}(\psi) = \mathrm{Mod}(\varphi)$)

$$
\begin{aligned}
\mathrm{Mod}(\psi) &\overset{\text{Def. } \psi}{=} \mathrm{Mod}(\neg\psi_1) \\
&\overset{\text{Def. Mod}}{=} \{W : P \to \{0,1\} \mid W(\neg\psi_1) = 1\} \\
&\overset{\text{Def. } [\![\neg]\!]}{=} \{W : P \to \{0,1\} \mid W(\psi_1) = 0\} \\
&\overset{\text{IH: } \psi_1 \equiv \varphi_1}{=} \{W : P \to \{0,1\} \mid W(\varphi_1) = 0\} \\
&\overset{\text{Def. } [\![\neg]\!]}{=} \{W : P \to \{0,1\} \mid W(\neg\varphi_1) = 1\} \\
&\overset{\text{Def. Mod}}{=} \mathrm{Mod}(\neg\varphi_1) \overset{\text{Struktur von } \varphi}{=} \mathrm{Mod}(\varphi)
\end{aligned}
$$

B$\vee$: z.z.: aus IH folgt IB$\vee$, Ansatz: $\psi = \psi_1 \vee \psi_2$

Beweis: Für $\psi = \psi_1 \vee \psi_2$ gelten E1 wegen ..., E2 wegen ...

B$\wedge$: z.z.: aus IH folgt IB$\wedge$, Ansatz: $\psi = \psi_1 \wedge \psi_2$, Beweis : ...

Beweis durch strukturelle Induktion – Beweise

B$\to$: z.z.: aus IH folgt IB$\to$, Ansatz: $\psi = \neg\psi_1 \vee \psi_2$

Beweis: Für $\psi = \neg\psi_1 \vee \psi_2$ gelten

E1 $\psi \in \mathsf{AL}_{\{\neg,\vee,\wedge\}}(P)$ wegen ...

E2 $\varphi \equiv \psi$ (gezeigt durch $\mathsf{Mod}(\psi) = \mathsf{Mod}(\varphi)$)

$$
\begin{aligned}
\mathsf{Mod}(\psi) &\overset{\text{Def. } \psi}{=} \mathsf{Mod}(\neg\psi_1 \vee \psi_2) \\
&\overset{\text{Def. Mod}}{=} \{W : P \to \{0,1\} \mid W(\neg\psi_1 \vee \psi_2) = 1\} \\
&\overset{\text{Def. } [\![\vee]\!]}{=} \{W : P \to \{0,1\} \mid \max(W(\neg\psi_1), W(\psi_2)) = 1\} \\
&\overset{\text{Def. max}}{=} \{W : P \to \{0,1\} \mid W(\neg\psi_1) = 1 \text{ oder } W(\psi_2) = 1\} \\
&\overset{\text{Def. } [\![\neg]\!]}{=} \{W : P \to \{0,1\} \mid W(\psi_1) = 0 \text{ oder } W(\psi_2) = 1\} \\
&\overset{\text{IH}}{=} \{W : P \to \{0,1\} \mid W(\varphi_1) = 0 \text{ oder } W(\varphi_2) = 1\} \\
&\overset{\text{Def. } \leq}{=} \{W : P \to \{0,1\} \mid W(\varphi_1) \leq W(\varphi_2)\} \\
&\overset{\text{Def. } [\![\to]\!]}{=} \{W : P \to \{0,1\} \mid W(\varphi_1 \to \varphi_2) = 1\} \\
&\overset{\text{Def. Mod}}{=} \mathsf{Mod}(\varphi_1 \to \varphi_2) \overset{\text{Struktur von } \varphi}{=} \mathsf{Mod}(\varphi)
\end{aligned}
$$

analog: B$\leftrightarrow$, B$\mathbb{t}$ (Ansatz: $p \vee \neg p$ für ein beliebiges $p \in P$), B$\mathbb{f}$

Umformen von Formeln

Nebenwirkung des (induktiven) Beweises zur Junktorbasis-Eigenschaft:

Fakt:
Jede aussagenlogische Formel kann schrittweise durch Ersetzung äquivalenter Teilformeln in semantisch äquivalente Formeln umgeformt werden.
(Änderung der Syntax bei unveränderter Semantik)

Beispiel:

$$\begin{aligned} \neg(p \to q) &\overset{(\varphi\to\psi\equiv\neg\varphi\vee\psi)}{\equiv} \neg(\neg p \vee q) \\ &\overset{(\text{deMorgan})}{\equiv} \neg\neg p \wedge \neg q \\ &\overset{(\neg\neg\varphi\equiv\varphi)}{\equiv} p \wedge \neg q \end{aligned}$$

Was bisher geschah

Modellierung von Aussagen in (klassischer) Aussagenlogik

Syntax:

- Atome : Aussagenvariablen
- Junktoren $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$
- induktive Definitionen von Formelmengen: $\mathrm{AL}(P), \mathrm{AL}_J(P)$
- Baumstruktur von Formeln
- Beweise durch strukturelle Induktion
- Junktorbasen
- äquivalente Umformungen

Semantik:

- Belegungen der Aussagenvariablen
- Wahrheitswerte von Formeln unter Belegungen
- Modelle von Formeln und Formelmengen
- Modellmenge und WW-Tabelle von Formeln und Formelmengen
- erfüllbare, allgemeingültige Formeln
- semantische Äquivalenz von Formeln

Normalformen aussagenlogischer Formeln

spezielle aussagenlogische Formeln:

- **Atom** Aussagenvariable
- **Literal** Atom oder negiertes Atom
- **Klausel** Disjunktion von Literalen

Normalformen:

- **NNF** Formeln, in denen das Negationssymbol $\neg$ höchstens auf Atome angewendet wird, heißen in Negations-Normalform.
  Beispiel: $\neg p \vee ((\neg q \vee p) \wedge q)$, $\neg p$, p
- **CNF** Formeln der Form $\bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_i} l_{i,j} \right)$ mit Literalen $l_{i,j}$ heißen in konjunktiver Normalform. (Konjunktion von Klauseln)
  Beispiel: $(\neg p \vee \neg q) \wedge (p \vee q) \wedge \neg q$, $p \vee q$, $p \wedge \neg q$, $\neg p$
- **DNF** Formeln der Form $\bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_i} l_{i,j} \right)$ mit Literalen $l_{i,j}$ heißen in disjunktiver Normalform.
  Beispiel: $\neg p \vee (\neg q \wedge p) \vee (p \wedge q)$, $p \vee q$, $p \wedge \neg q$, $\neg p$

Satz über Normalformen

Satz

Zu jeder Formel $\varphi \in \mathsf{AL}(P)$ *existieren*

- *eine äquivalente Formel* $\psi \in \mathsf{AL}(P)$ *in NNF,*
- *eine äquivalente Formel* $\psi' \in \mathsf{AL}(P)$ *in CNF und*
- *eine äquivalente Formel* $\psi'' \in \mathsf{AL}(P)$ *in DNF.*

Transformation beliebiger Formeln in Normalformen:

1. $\{\vee, \wedge, \neg\}$ ist eine Junktorbasis, d.h.
   Formeln mit Junktoren $\rightarrow, \leftrightarrow, \mathbb{t}, \mathbb{f}$ lassen sich in äquivalente Formeln mit ausschließlich den Junktoren $\vee, \wedge, \neg$ umformen
2. Konstruktion einer NNF durch (ggf. mehrmalige) Anwendung der deMorganschen Regeln
3. Konstruktion der CNF und DNF durch (ggf. mehrmalige) Anwendung der Distributivgesetze auf die NNF

Normalformen – Beispiel

$$
\begin{aligned}
(a \to b) \to c &\overset{(\varphi\to\psi\equiv\neg\varphi\vee\psi)}{\equiv} (\neg a \vee b) \to c \\
&\overset{(\varphi\to\psi\equiv\neg\varphi\vee\psi)}{\equiv} \neg(\neg a \vee b) \vee c \\
&\overset{\text{(deMorgan)}}{\equiv} (\neg\neg a \wedge \neg b) \vee c \\
&\overset{(\neg\neg\varphi\equiv\varphi)}{\equiv} (a \wedge \neg b) \vee c && \text{(NNF, DNF)} \\
&\overset{\text{(Distributivität)}}{\equiv} (a \vee c) \wedge (\neg b \vee c) && \text{(NNF, CNF)}
\end{aligned}
$$

Modellierungsbeispiel Taxi

umgangssprachliche Angaben zur Situation:
Wenn der Zug zu spät kommt und kein Taxi am Bahnhof steht, ist Tom nicht pünktlich. Der Zug kam zu spät und Tom ist pünktlich.

Frage: Stand ein Taxi am Bahnhof?

formale Beschreibung:

- elementare Aussagen (Atome): $P = \{p, t, z\}$
  p – Tom ist pünktlich, t – Taxi steht da, z – Zug hat Verspätung
- Beschreibung der Situation (Kontext) als Formelmenge:

$$\Phi = \{(z \wedge \neg t) \rightarrow \neg p, z \wedge p\}$$

- Modellierung der Frage als Behauptung : t
  (positive Antwort auf die Frage)

Alle möglichen Situationen, in denen alle Angaben erfüllt sind:
$\mathrm{Mod}(\Phi) = \ldots$
Antwort auf die Frage: ja,
weil für jede Belegung $W \in \mathrm{Mod}(\Phi)$ gilt $W(t) = 1$,
also $\mathrm{Mod}(\Phi) \subseteq \mathrm{Mod}(t)$

Semantisches Folgern

Definition

Für jede Formelmenge $\Phi \subseteq \mathrm{AL}(P)$ (Kontext)
und jede Formel $\psi \in \mathrm{AL}(P)$ (Behauptung) heißt
ψ genau dann semantische Folgerung aus Φ wenn $\mathrm{Mod}(\Phi) \subseteq \mathrm{Mod}(\psi)$.

Notation: $\Phi \models \psi$ (ψ folgt semantisch aus Φ)

Beispiele:

- $\{p, p \to q\} \models q$ gilt, weil
  $\mathrm{Mod}(\{p, p \to q\}) = \{W_{11}\} \subseteq \{W_{01}, W_{11}\} = \mathrm{Mod}(q)$,
- $\{p, \neg(q \wedge p)\} \models \neg q$, weil ...
- $p \models q \to p$, weil ...
- $q \to p \not\models p$, weil ...
- $\emptyset \models p \vee \neg p$, weil ...
- $\emptyset \not\models p$, weil ...

Notation für Spezialfälle

für $\Phi = \{\varphi\}$	:	φ	$\models$	ψ	(statt	$\{\varphi\}$	$\models$	ψ)
für $\Phi = \emptyset$	:		$\models$	ψ	(statt	$\emptyset$	$\models$	ψ)

Modellierungsbeispiel: Winterkleidung

- Wenn es kalt ist, trägt Paul immer eine Mütze, einen Schal oder Handschuhe.
- Ohne Handschuhe oder Schal trägt er keine Mütze.
- Mütze und Handschuhe trägt er nie zusammen.
- Handschuhe und Schal trägt er immer zugleich.

Modellierung als (aussagenlogische) Formelmenge

$$\Phi = \{m \vee s \vee h, \neg(h \vee s) \rightarrow \neg m, \neg(m \wedge h), h \leftrightarrow s\}$$

Welche der folgenden Aussagen sind semantische Folgerungen daraus:

- Bei Kälte trägt er immer einen Schal. $\psi_1 = s$
- Bei Kälte trägt er immer Handschuhe oder Mütze. $\psi_2 = h \vee m$
- Er trägt nie Handschuhe. $\psi_3 = \neg h$

Sätze über das Folgern

Satz

Für jede endliche Formelmenge $\Phi = \{\varphi_1, \ldots, \varphi_n\} \subseteq \mathsf{AL}(P)$ *gilt*

$$\Phi \models \psi \quad \textit{genau dann, wenn} \quad \bigwedge_{i=1}^{n} \varphi_i \models \psi$$

Beweis: verwendet Fakt auf Folie 46

Satz

Für jede Formelmenge $\Phi \subseteq \mathsf{AL}(P)$ *und jede Formel* $\psi \in \mathsf{AL}(P)$ *gilt*
$\Phi \models \psi$ *genau dann, wenn* $\Phi \cup \{\neg\psi\}$ *unerfüllbar ist.*

Beweis

Satz

Für jede Formel $\psi \in \mathsf{AL}(P)$ *gilt* $\models \psi$ *genau dann, wenn* ψ *allgemeingültig.*

Satz

Für je zwei beliebige Formeln $\varphi, \psi \in \mathsf{AL}(P)$ *gilt* $\varphi \equiv \psi$ *genau dann, wenn*

1. $\varphi \models \psi$ *und* $\psi \models \varphi$ *gilt,*
2. *die Formel* $\varphi \leftrightarrow \psi$ *allgemeingültig ist.*

Typische praktische Folgerungsprobleme

- kombinatorische Probleme, z.B. Planungsprobleme (Registerzuweisung, Zeitplanung), Graphfärbung
- Verifikation digitaler Schaltungen:

  gegeben: Schaltung:
  (Ausgabe-Verhalten als boolesche Funktion, Formel φ)
  Spezifikation (logische Formel ψ)
  Frage: Erfüllt die Schaltung die Spezifikation? (Gilt $\varphi \models \psi$?)

  Gegenbeispiel bei negativer Antwort:
  Belegung $W : P \to \{0, 1\}$ mit $W(\varphi \wedge \neg\psi) = 1$
- Verifikation von Software:

  gegeben: Programm (Ausgabe-Verhalten als Formelmenge Φ)
  Spezifikation (logische Formel ψ)
  Frage: Erfüllt das Programm die Spezifikation? (Gilt $\Phi \models \psi$?)

  Gegenbeispiel bei negativer Antwort:
  Belegung $W : P \to \{0, 1\}$ mit $W \in \mathrm{Mod}(\Phi \cup \{\neg\psi\})$

Erfüllbarkeitsproblem für AL (SAT)

Aufgabe SAT:

gegeben: beliebige Formel $\varphi \in \mathrm{AL}(P)$
Frage: Ist φ erfüllbar (satisfiable) ? (Gilt $\mathrm{Mod}(\varphi) \neq \emptyset$?)

Instanz, z.B.

$$\varphi = ((z \wedge \neg t) \rightarrow \neg p) \wedge (z \wedge p) \wedge \neg t$$

einige mögliche Lösungsverfahren:

semantisch : Berechnung der Modellmenge (WW-Tabelle)

syntaktisch :

- äquivalente Umformungen ($\varphi \equiv \mathbb{f}$)
- aussagenlogische Resolution von $\mathbb{f}$ aus φ

DNF-SAT

Aufgabe DNF-SAT: gegeben: DNF $\varphi = \bigvee_{i=1}^{m} \bigwedge_{j=1}^{k_i} l_{i,j} \in \mathrm{AL}(P)$
Frage: Ist φ erfüllbar?

Instanz, z.B. $(p \wedge \neg q \wedge \neg p) \vee (q \wedge p \wedge \neg q) \vee (\neg p \wedge \neg q)$
Lösungsidee:

- φ ist genau dann erfüllbar, wenn (wenigstens) eine der m Konjunktionen $\bigwedge_{j=1}^{k_i} l_{i,j}$ erfüllbar ist.
- Konjunktion $\bigwedge_{j=1}^{k_i} l_{i,j}$ ist genau dann unerfüllbar, wenn für eine Aussagenvariable $x \in \mathrm{var}(\varphi)$ gilt: $\{x, \neg x\} \subseteq \{l_{i,j} \mid j \in \{1, \ldots, k_i\}\}$ (Widerspruch).

Lösungsverfahren:

- für jede Konjunktion der DNF Widerspruchsfreiheit überprüfen,
  Falls eine widerspruchsfreie Konjunktion gefunden:
  DNF erfüllbar, sonst DNF unerfüllbar
- Überprüfung der Widerspruchsfreiheit einer Konjunktion:
  für jedes Literal überprüfen, ob Negation in derselben Konjunktion,
  falls gefunden: diese Konjunktion unerfüllbar

DNF-SAT ist einfach (schnell) zu lösen.

CNF-SAT

Aufgabe CNF-SAT:

gegeben: CNF $\varphi = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{k_i} l_{i,j} \in \mathrm{AL}(P)$
Frage: Ist φ erfüllbar?

Instanz z.B. $(p \vee \neg q \vee r) \wedge (q \vee p \vee \neg r) \wedge (\neg p \vee \neg q)$
Lösungsansätze:

- Test aller möglichen Belegungen, hoher Aufwand
  (für große Anzahl an Aussagenvariablen unpraktikabel)
- Umformung in eine zu φ äquivalente DNF ψ
  Test von ψ auf Erfüllbarkeit
  (für große Anzahl an Aussagenvariablen unpraktikabel)
- Konstruktion einer Formel ψ mit
  1. ψ erfüllbar gdw. φ erfüllbar und
  2. Erfüllbarkeit für ψ einfach zu testen

CNF-SAT ist die dem menschlichen Formulieren von Bedingungen naheliegendste Form, aber schwierig zu lösen. (hoher Zeitaufwand)

2-CNF und 2SAT

2-CNF: Formel der Form

$$\varphi = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{k_i} l_{i,j} \quad \text{mit} \quad \forall i \in \{1, \ldots, m\} : k_i \leq 2$$

Beispiele:

- $(p \vee q) \wedge (\neg p \vee r) \wedge \neg q$ ist 2-CNF,
- $(p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$ ist 2-CNF,
- $q \vee \neg p \vee r$ ist CNF (und DNF), aber keine 2-CNF

Aufgabe 2SAT:

gegeben: 2-CNF φ
Frage: Ist φ erfüllbar?

2SAT ist einfach (schnell) zu lösen. (hier ohne Beweis)
Aber:
Nicht zu jeder Formel $\varphi \in \mathrm{AL}(P)$ existiert eine äquivalente 2-CNF.

3-CNF und 3SAT

3-CNF: Formel der Form

$$\varphi = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{k_i} l_{i,j} \quad \text{mit} \quad \forall i \in \{1, \ldots, m\} : k_i \leq 3$$

Instanz z.B. $(p \vee \neg q \vee r) \wedge (q \vee p \vee \neg r) \wedge (\neg p \vee \neg q)$

Aufgabe 3SAT:

gegeben: 3-CNF φ
Frage: Ist φ erfüllbar?

bekannt (hier ohne Beweis):
Zu jeder Formel $\varphi \in \mathrm{AL}(P)$ lässt sich eine erfüllbarkeitsäquivalente 3-CNF konstruieren.

bekannt (Beweis im Master-Studium):
3SAT ist schwierig zu lösen. (zeitaufwendig, NP-vollständig)

SAT-Solver

SAT-Solver: Werkzeug zum Lösen von (CNF-)SAT-Instanzen

SAT-Solver

- benutzen heuristische Verfahren,
- finden für praktische Probleme oft schnell eine Lösung,
- meist Ausgabe eines Modells (wenn wenigstens eins existiert)

aktive Forschung auf diesem Gebiet:

jährlich Wettbewerbe (`www.satcompetition.org/`)

typische Anwendung von SAT-Solvern:

1. Modellierung des ursprünglichen Problems P als CNF φ in DIMACS-Format (oft maschinell),
2. Lösung mit SAT-Solver
3. Übersetzung erfüllender Belegung für φ in Lösung für P

Modellierungsbeispiel: Zuordnung Person – Land

In einem Eisenbahnabteil sitzen die Herren Lehmann und Müller.
Einer ist Sachse und einer Thüringer.
Welche Zuordnungen sind möglich?
Modellierung in Aussagenlogik:
Aussagenvariablen: $P = \{LS, LT, MS, MT\}$

LS	Herr Lehmann ist Sachse.
LT	Herr Lehmann ist Thüringer.
MS	Herr Müller ist Sachse.
MT	Herr Müller ist Thüringer.

Jeder der beiden Personen kommt aus genau einem Land, also

1. Jede Person kommt aus wenigstens einem Land.
   $LS \vee LT, MS \vee MT$
2. Aus jedem Land kommt wenigstens eine Person.
   $LS \vee MS, LT \vee MT$
3. Jede Person kommt aus höchstens einem Land.
   $LS \rightarrow \neg LT, LT \rightarrow \neg LS, MS \rightarrow \neg MT, MT \rightarrow \neg MS$
   oder (äquivalent) $\neg LS \vee \neg LT, \neg MS \vee \neg MT$
4. Aus jedem Land kommt höchstens eine Person. (analog)

Lösung mit SAT-Solver

Eingabe im DIMACS-Format für CNF (ASCII):

- erste Zeile enthält Typ (`cnf`), Anzahl der Aussagenvariablen und Disjunktionen (z.B. `p cnf 4 8`)
- Aussagenvariablen $\{1, \ldots, n\}$
- jede Disjunktion (Klausel) eine Zeile, `0` markiert Ende der Klausel – statt $\neg$, Literale durch Leerzeichen getrennt,

Darstellung der Zuordnungs-Aufgabe als CNF in DIMACS-Format

```
p cnf 4 8
c 1:LS, 2:LT, 3:MS, 4:MT
1 2 0
3 4 0
...
```

Lösung mit SAT-Solver, z.B. minisat, Ausgabe: eine erfüllende Belegung

```
SATISFIABLE
1 -2 -3 4 0
```

Interpretation der SAT-Solver-Ausgabe als (ein) Modell:
LS (1) und MT (4) sind wahr, also Lehmann Sachse, Müller Thüringer.
für weitere Modelle zusätzliche Klauseln, die bekanntes Modell verhindern
im Beispiel: Zeile `-1 2 3 -4 0` hinzufügen

Einsatz von SAT-Solvern

typische Anwendungen für SAT-Solver z.B.

- Zuordnungen (mit vielen beteiligten Individuen), z.B. Ressourcen-Planung
  - Aufgabenverteilung
  - Planen, z.B. Stundenplan
  - Job-Scheduling (Betriebssystem)
- Constraint-Lösen, kombinatorische Suchprobleme, z.B. Graph-Färbungen (Register-Zuordnung, Sudoku)
- Folgerungsprobleme, z.B.
  - Schaltkreisentwurf und -verifikation
  - Konfiguration von Hard- und Software
  - Model-Checking (Verifikation von Software und Systemen)

Modellierungsbeispiel: n-Damen-Aufgabe

Frage: Lassen sich n Damen so auf einem $n \times n$-Schachbrett anordnen, dass keine Dame eine andere bedroht?

Lösung: zulässige Anordnung, falls möglich

Bedingungen für zulässige Anordnungen:

- n Damen auf dem Feld, also in jeder Zeile (wenigstens) eine
- keine Zeilenbedrohung
- keine Spaltenbedrohung
- keine diagonale Bedrohung

für ganz kleine Spielfelder:

- $n = 1$: Zulässige Anordnung
  einer Dame auf einem 1×1-Schachbrett möglich.
- $n = 0$: Zulässige Anordnung
  keiner Dame auf einem 0×0-Schachbrett möglich.

Repräsentation der 2-Damen-Aufgabe

4 Felder – Aussagenvariablen $\{x_1, \ldots, x_4\}$

1	2
3	4

Bedingungen:

1. in jeder Zeile (wenigstens) eine Dame
   $x_1 \vee x_2$, $x_3 \vee x_4$
2. keine Zeilenbedrohung (in jeder Zeile höchstens eine Dame)
   $x_1 \rightarrow \neg x_2$ $(\equiv \neg x_1 \vee \neg x_2)$
   $x_3 \rightarrow \neg x_4$ $(\equiv \neg x_3 \vee \neg x_4)$
3. keine Spaltenbedrohung (in jeder Spalte höchstens eine Dame)
   $x_1 \rightarrow \neg x_3$ $(\equiv \neg x_1 \vee \neg x_3)$
   $x_2 \rightarrow \neg x_4$ $(\equiv \neg x_2 \vee \neg x_4)$
4. keine diagonale Bedrohung
   $x_1 \rightarrow \neg x_4, x_2 \rightarrow \neg x_3,$

Man vergleiche 1. bis 3. mit dem Beispiel Zuordnungen

Repräsentation der 3-Damen-Aufgabe

1	2	3
4	5	6
7	8	9

9 Felder – Aussagenvariablen $\{x_1, \ldots, x_9\}$

Bedingungen:

1. in jeder Zeile (wenigstens) eine Dame

   $x_1 \vee x_2 \vee x_3$, $x_4 \vee x_5 \vee x_6$, $x_7 \vee x_8 \vee x_9$

2. keine Zeilenbedrohung (in jeder Zeile höchstens eine Dame)

   $x_1 \rightarrow \neg x_2 (\equiv \neg x_1 \vee \neg x_2)$, $x_1 \rightarrow \neg x_3$, $x_2 \rightarrow \neg x_3$

   $x_4 \rightarrow \neg x_5$, $x_4 \rightarrow \neg x_6$, $x_5 \rightarrow \neg x_6$

   $x_7 \rightarrow \neg x_8$, $x_7 \rightarrow \neg x_9$, $x_8 \rightarrow \neg x_9$

3. keine Spaltenbedrohung (in jeder Spalte höchstens eine Dame)

   $x_1 \rightarrow \neg x_4$, $x_1 \rightarrow \neg x_7$, $x_4 \rightarrow \neg x_7$

   $x_2 \rightarrow \neg x_5$, $x_2 \rightarrow \neg x_8$, $x_5 \rightarrow \neg x_8$

   $x_3 \rightarrow \neg x_6$, $x_3 \rightarrow \neg x_9$, $x_6 \rightarrow \neg x_9$

4. keine diagonale Bedrohung

   $x_1 \rightarrow \neg x_5$, $x_1 \rightarrow \neg x_9$, $x_5 \rightarrow \neg x_9$

   $x_2 \rightarrow \neg x_6$, $x_4 \rightarrow \neg x_8$

   $x_3 \rightarrow \neg x_5$, $x_3 \rightarrow \neg x_7$, $x_5 \rightarrow \neg x_7$

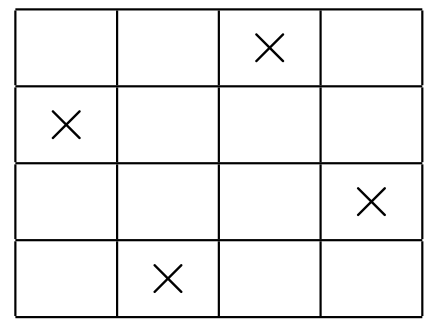
   $x_2 \rightarrow \neg x_4$, $x_6 \rightarrow \neg x_8$

4 Damen

16 Felder – Aussagenvariablen $\{x_1, \ldots, x_{16}\}$

eine mögliche Lösung (Modell, erfüllende Belegung):

$$\left(\begin{array}{cccccccc}
 & \neg 1 & \wedge & \neg 2 & \wedge & 3 & \wedge & \neg 4 \\
\wedge & 5 & \wedge & \neg 6 & \wedge & \neg 7 & \wedge & \neg 8 \\
\wedge & \neg 9 & \wedge & \neg 10 & \wedge & \neg 11 & \wedge & 12 \\
\wedge & \neg 13 & \wedge & 14 & \wedge & \neg 15 & \wedge & \neg 16
\end{array}\right)$$



Was bisher geschah

Modellierung von Aussagen in (klassischer) Aussagenlogik

Syntax:

- induktive Definitionen von Formelmengen: $\mathrm{AL}(P), \mathrm{AL}_J(P)$
- Baumstruktur von Formeln
- Beweise durch strukturelle Induktion
- Junktorbasen
- Normalformen: NNF, CNF, DNF

Semantik:

- Wahrheitswerte von Formeln unter Belegungen
- Modelle von Formeln und Formelmengen
- Modellmengen von Formeln und Formelmengen
- erfüllbare, allgemeingültige Formeln
- semantische Äquivalenz von Formeln
- semantisches Folgern von Formeln aus Formelmengen
- Transformation von Folgerungs- in Erfüllbarkeitsprobleme
- Erfüllbarkeitsprobleme DNF-SAT, CNF-SAT, 2SAT, 3SAT
- maschinelles Lösen von Aufgaben durch SAT-Solver

WH: Modellierungsbeispiel Winterkleidung

- Wenn es kalt ist, trägt Paul immer eine Mütze, einen Schal oder Handschuhe.
- Ohne Handschuhe oder Schal trägt er keine Mütze.
- Mütze und Handschuhe trägt er nie zusammen.
- Handschuhe und Schal trägt er immer zugleich.

Modellierung als (aussagenlogische) Formelmenge

$$\Phi = \{m \vee s \vee h, \neg(h \vee s) \rightarrow \neg m, \neg(m \wedge h), h \leftrightarrow s\}$$

Welche der folgenden Aussagen sind semantische Folgerungen daraus:

- Bei Kälte trägt er immer einen Schal. $\psi_1 = s$
- Bei Kälte trägt er immer Handschuhe oder Mütze. $\psi_2 = h \vee m$
- Er trägt nie Handschuhe. $\psi_3 = \neg h$

schon bekannt: Lösung durch

- Modellmengen $\text{Mod}(\Phi) \subseteq \text{Mod}(\psi)$

bei Problemen mit vielen Variablen aufwendig

gut wäre: syntaktisches Verfahren

Syntaktisches Ableiten – Ziel

gegeben: Formelmenge $\Phi \subseteq \mathsf{AL}(P)$
und Formel $\psi \in \mathsf{AL}(P)$
Frage : Gilt $\Phi \models \psi$?

Ziel:
Verfahren zur Beantwortung dieser Frage durch syntaktische Operationen (ohne Verwendung der Semantik, Modellmengen)

$\vdash$ passt zu $\models$ gdw.
für jede Formelmenge $\Phi \subseteq \mathsf{AL}(P)$ und jede Formel $\psi \in \mathsf{AL}(P)$ gilt

$$\Phi \vdash \psi \quad \text{gdw.} \quad \Phi \models \psi$$

Korrektheit: Aus $\Phi \vdash \psi$ folgt $\Phi \models \psi$

Vollständigkeit: Aus $\Phi \models \psi$ folgt $\Phi \vdash \psi$

Logische Kalküle

Verfahren zur schrittweisen syntaktischen Ableitung
von sematischen Folgerungen (Formeln)
aus einer Menge von Formeln (Hypothesen)

Definition von

Axiomen (Schemata für) Formeln

Schlussregeln zur syntaktischen Ableitung von Folgerungen aus Formelmengen (Axiomen, Hypothesen, Annahmen)
oft mehrere Voraussetzungen und eine Folgerung

Ableitungen (und Beweisen) durch geeignete Kombinationen von Schlussregeln (Baumstruktur)

Kalküle - Definition

Kalkül $K = (A, R)$ mit Mengen von

Axiome A, d.h. (Schemata für) Formeln, deren Gültigkeit vorausgesetzt wird,

Schlussregeln R zur syntaktischen Ableitung von Folgerungen (weitere gültige Formeln) aus Formelmengen (Axiomen und Hypothesen)

häufige Darstellung von Schlussregeln als Verzweigung (nach oben):

$$\frac{\varphi_1 \qquad \cdots \qquad \varphi_n}{\psi}$$

- Voraussetzungen (oben): $\varphi_1, \ldots, \varphi_n$
- Folgerung (unten): ψ

Beweis im Kalkül = Baum mit

- Blätter: Axiome
- innere Knoten: (instanziierte) Schlussregeln

Beispiel Taxi

Wenn der Zug zu spät kommt und kein Taxi am Bahnhof steht, ist Tom nicht pünktlich. Der Zug kam zu spät und Tom ist pünktlich.
Frage: Stand ein Taxi am Bahnhof? (Gilt $\Phi_T \models t$?)
Ableitungsbaum für $\{v \to (\neg t \to \neg p), v, p\} \vdash t$:

$$\dfrac{\dfrac{\dfrac{v \qquad v \to (\neg t \to \neg p)}{\neg t \to \neg p}\,(\text{MP}) \qquad \dfrac{p}{\neg\neg p}\,(\neg\neg\text{I})}{\neg\neg t}\,(\text{MT})}{t}\,(\neg\neg\text{E})$$

sequentielle Darstellung der Ableitung (des Beweises):

1. v (Annahme)
2. $v \to (\neg t \to \neg p)$ (Annahme)
3. $\neg t \to \neg p$ (MP) mit 1 und 2
4. p (Annahme)
5. $\neg\neg p$ ($\neg\neg$I) mit 4
6. $\neg\neg t$ (MT) mit 3 und 5
7. t ($\neg\neg$E) mit 6

Aussagenlogische Resolution – Idee

Folgerungsproblem: gegeben: Formelmenge Φ
und Formel ψ
Frage: Gilt $\Phi \models \psi$?

Idee:
schrittweise Erweiterung der Formelmenge Φ durch Hinzufügen von semantischen Folgerungen ψ aus Φ (also Formeln ψ mit $\Phi \models \psi$).

Dabei bleibt die Modellmenge unverändert,
d.h. $\mathsf{Mod}(\Phi \cup \{\psi\}) = \mathsf{Mod}(\Phi)$. (Warum?)

Spezialfall $\psi = \mathbb{f}$:
$\Phi \models \mathbb{f}$ gilt genau dann, wenn Φ unerfüllbar ist (einen Widerspruch enthält).

Aussagenlogischer Resolutionskalkül

Resolutionsregel für $\psi, \eta \in \mathsf{AL}(P)$ und Aussagenvariable $p \in P$:

$$\frac{\psi \vee p \qquad \neg p \vee \eta}{\psi \vee \eta}\ (\mathsf{R})$$

alternative Darstellung:

$$\frac{\neg\psi \to p \qquad p \to \eta}{\neg\psi \to \eta}\ (\mathsf{R})$$

gegeben: Formelmenge Φ
Formel ψ
Frage : Gilt $\Phi \models \psi$?

Idee: Schrittweise Erweiterung der Formelmenge Φ um semantische Folgerungen der Form $\psi \vee \eta$, falls $\{p \vee \psi, \neg p \vee \eta\} \subseteq \Phi$ (Anwendung der Resolutionsregel)

Spezialfall: Φ enthält nur Klauseln

Mengendarstellung von Formeln in CNF

$$\text{CNF} \quad \varphi = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{i,j}$$

WH: Disjunktionen $\bigvee_{j=1}^{m_i} l_{i,j}$ heißen Klauseln

Spezialfall: leere Klausel mit $m_i = 0$

$$\bigvee_{i=1}^{0} l_i = \bigvee_{i \in \emptyset} l_i \equiv \mathbb{f}$$

Repräsentation der CNF φ als Menge von Klauseln:

$$\varphi = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} l_{i,j} \quad \mapsto \quad \left\{ \bigvee_{j=1}^{m_i} l_{i,j} \mid i \in \{1, \ldots, n\} \right\}$$

Beispiele für CNF als Klauselmengen

Notation:

- Jede Klausel enthält jedes Literal nur einmal.
  (keine Einschränkung, weil $\forall \varphi \in \mathsf{AL}(P) : \varphi \vee \varphi \equiv \varphi$)
- Literale in jeder Klausel in alphabetischer Reihenfolge
  (keine Einschränkung weil $\vee$ kommutativ).
- Mengen enthalten jede Klausel nur einmal.
  (keine Einschränkung, weil $\forall \varphi \in \mathsf{AL}(P) : \varphi \wedge \varphi \equiv \varphi$)

$$
\begin{aligned}
a \vee b \vee \neg c \vee a &\mapsto \{a \vee b \vee \neg c\} \\
a \wedge b \wedge \neg c \wedge a &\mapsto \{a, b, \neg c\} \\
(a \vee \neg b \vee a) \wedge (b \vee a) \wedge (\neg c \vee a) &\mapsto \{a \vee \neg b, a \vee b, a \vee \neg c\} \\
(a \vee \neg b) \wedge (\neg c \vee a) \wedge (a \vee b) \wedge (b \vee a) &\mapsto \{a \vee \neg b, a \vee b, a \vee \neg c\}
\end{aligned}
$$

Resolutionsprinzip

Regel allgemein:

$$\frac{\psi \vee l \qquad \eta \vee \neg l}{\psi \vee \eta}\,(\mathrm{R})$$

Regel für Klauseln:

$$\frac{l_1 \vee \cdots \vee l_n \vee l \qquad l'_1 \vee \cdots \vee l'_m \vee \neg l}{l'_1 \vee \cdots \vee l'_m}\,(\mathrm{R})$$

Resolvente $R = l_1 \vee \cdots \vee l_n \vee l'_1 \vee \cdots \vee l'_m$

Beispiele:

- Klauseln $K_1 = a \vee \neg b \vee c$ und $K_2 = \neg c \vee d \vee \neg e$ haben eine Resolvente $R = a \vee \neg b \vee d \vee \neg e$
- Klauseln $K_1 = a \vee \neg b$ und $K_2 = \neg a \vee b \vee \neg c$ haben zwei Resolventen $R_1 = \neg b \vee b \vee \neg c$, $R_2 = \neg a \vee a \vee \neg c$

Satz (Resolutionslemma)

Für jede CNF (Klauselmenge) Φ und die Resolvente R zweier Klauseln aus Φ gilt

$$\mathrm{Mod}(\Phi) = \mathrm{Mod}(\Phi \cup \{R\})$$

Ableitungen durch Resolution

Resolutionsableitung aus einer Klauselmenge Φ (CNF):
endliche Folge $C_1, \ldots C_n$ von Klauseln, wobei für jede Klausel C_i gilt:

- $C_i \in \Phi$ oder
- C_i ist eine Resolvente von Klauseln C_j, C_k mit $j < i$ und $k < i$.

Resolutionsableitung der Klausel ψ aus Klauselmenge Φ:
Resolutionsableitung $C_1, \ldots C_n$ in Φ mit $C_n = \psi$

Beispiel: Resolutionsableitung von d aus

$$\Phi = \{\underbrace{a \vee b \vee c}_{C_1}, \underbrace{\neg b \vee d}_{C_2}, \underbrace{\neg a \vee d}_{C_3}, \underbrace{\neg c \vee d}_{C_4}\}$$

$$R(C_1, C_4) = \underbrace{a \vee b \vee d}_{C_5}, \quad R(C_3, C_5) = \underbrace{b \vee d}_{C_6}, \quad R(C_2, C_6) = d$$

Baumdarstellung

Resolutionsableitungen nach $\mathbb{f}$

Problem:
Es existiert keine Resolutionsableitung von $\neg a \vee \neg b \vee d$ aus

$$\Phi = \{a \vee b \vee c, \neg b \vee d, \neg a \vee d, \neg c \vee d\}$$

aber es gilt $\Phi \models \neg a \vee \neg b \vee d$.

Lösung:

- Es gilt $\Phi \models \psi$ gdw. $\Phi \cup \{\neg\psi\}$ unerfüllbar.
- Unerfüllbarkeitsbeweis für $\Phi \cup \{\neg\psi\}$ durch Resolutionsableitung von $\mathbb{f}$ aus $\Phi \cup \{\neg\psi\}$ (Klauselform)

Beispiel: Resolutionsableitung von $\mathbb{f}$ aus

$$\Phi \cup \{\neg\psi\} = \{a \vee b \vee c, \neg b \vee d, \neg a \vee d, \neg c \vee d, a, b, \neg d\}$$

Beschränkte Ausdrucksstärke der Aussagenlogik

- Aussagen immer zweiwertig
  (nur wahr oder falsch, keine Zwischenwerte),
  z.B.: Die Rose ist rot. Das Bier ist kalt. Der Student ist fleißig.

  (Erweiterung zu mehrwertigen Logiken, fuzzy logic)
- Aussagen immer absolut
  (keine Abhängigkeit vom Kontext, z.B. Ort, Zeitpunkt),
  z.B.: Es regnet. $x > 3$

  (Erweiterung zur Modal- und Temporallogiken)
- Aussagen über alle Elemente „großer“ Mengen aufwendig
  (Erstellung, Platzbedarf), z.B. Zuordnungen
- keine Aussagen über Elemente einer unendlichen Mengen oder
  Mengen unbestimmter Mächtigkeit möglich, z.B.
  - Jede durch 4 teilbare Zahl ist gerade.
  - Es gibt eine gerade Primzahl.
  - Es ist nicht alles Gold was glänzt.

  (Erweiterung zur Prädikatenlogik)

notwendige Vorbereitung:

Modellierung von Individuenbereichen, Eigenschaften und Beziehungen

Modellierungsbeispiel

1. Max ist ein Fisch.
2. Alle Fische schwimmen.
3. Also schwimmt Max.

Individuenbereich (Objekte): Lebewesen

Individuen (Konstanten): Max

Eigenschaften: istFisch, schwimmt

prädikatenlogische Formeln:

1. istFisch(Max)
2. $\forall x$ (istFisch(x) $\rightarrow$ schwimmt(x))
3. schwimmt(Max)

Modellierung in Prädikatenlogik

Grundannahme:
Die zu modellierende Welt besteht aus Individuen, die
Eigenschaften haben und
zueinander in Beziehungen (Relationen, Funktionen) stehen.

Aussagen beschreiben Eigenschaften von Individuen
und Beziehungen zwischen Individuen.

Formalisierung solcher Aussagen durch prädikatenlogische Formeln.

Prädikatenlogische Aussagen – Beispiele Verwandschaft

- Personen sind genau dann Geschwister, wenn sie dieselbe Mutter oder denselben Vater haben.
- A ist genau dann Nachfahre von B, wenn
  B Vater oder Mutter von A ist oder
  ein Elternteil von A Nachfahre von B ist.
- Nachfahren derselben Person sind miteinander verwandt.

Individuenbereich: Menge von Personen

Beziehungen: Nachfahre, verwandt, Geschwister, $=$

Funktionen: Mutter, Vater

Prädikatenlogische Aussagen – Beispiele Zahlen

- Primzahlen sind genau diejenigen natürlichen Zahlen, die genau zwei verschiedene Teiler haben.
- Gerade Zahlen sind genau diejenigen natürlichen Zahlen, die durch 2 teilbar sind.
- Es existieren gerade Primzahlen.
- Nachfolger ungerader Primzahlen sind nicht prim.
- Das Quadrat jeder geraden Zahl ist gerade.

Individuenbereich: Menge $\mathbb{N}$ aller natürlichen Zahlen

Eigenschaften: prim, gerade

Beziehungen: teilt, $=$

Funktionen: Nachfolger, Quadrat

Was bisher geschah

Modellierung von Aussagen
zur Beschreibung von Situationen, Anforderungen
(klassische) Aussagenlogik

- Syntax: Atome sind Aussagenvariablen, Junktoren
  $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$
  induktive Definition: Baumstruktur der Formeln
  strukturelle Induktion
- Semantik: Belegungen, WW-Tabellen, Modellmengen
- erfüllbare, allgemeingültige Formeln, Äquivalenz von Formeln
- semantisches Folgern
- syntaktisches Schließen (Resolutionskalkül)

Erfüllbarkeits-Aufgaben

- Modellierungsbeispiele, Anwendungen
- SAT-Solver
- Transformation von Allgemeingültigkeits- und Folgerungsfragen in Erfüllbarkeitsfragen

Modellierung von Individuenbereichen durch Mengen

Naiver Mengenbegriff von Georg Cantor (1845-1918):
Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Dinge unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.

Mengen werden dargestellt:

extensional durch Angabe aller Elemente
(nur für endliche Mengen möglich)
Beispiel: $\{0, 1, 2, 3\}$, $\{\{a\}, 5, \{a, b\}\}$

intensional durch Angabe der gemeinsamen Eigenschaft aller Elemente (oft durch prädikatenlogische Formeln)
Beispiele:
$\{x \mid (x \in \mathbb{N}) \wedge (x < 4)\} = \{x \in \mathbb{N} \mid x < 4\}$
$\{x \mid x \in \mathbb{N} \wedge \exists y((y \in \mathbb{N}) \wedge (x = 2y + 1))\}$

Modellierungsbeispiel Skatkarten (extensional)

Modellierung:

- Jede Karte hat Farbe und Wert (wichtig)
- deutsches oder französisches Blatt? (egal)
- Ordnung zwischen Karten derselben Farbe (wichtig)
  z.B. $7 < 8 < 9 < 10 < B < D < K < A$ bei Null-Spiel
- Bedienregeln
- Trumpfregeln

Formale Darstellung der Karten:
Jede Karte ist eindeutig repräsentiert durch Paar von

Farbe aus der Menge $F = \{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$ und

Wert
- Zahl aus der Menge $Z = \{7, 8, 9, 10\}$ oder
- Bild aus der Menge $B = \{B, D, K, A\}$

Modellierungsbeispiel gerade Zahlen (intensional)

Gerade Zahlen sind genau die durch 2 teilbaren ganzen Zahlen.

Individuen: $\mathbb{Z}$ (Menge aller ganzen Zahlen)

Eigenschaften: gerade

Beziehungen: Teilbarkeit ganzer Zahlen $(a|b)$

präziser mit Definition der Teilbarkeit:

$x \in \mathbb{Z}$ ist genau dann gerade, wenn $2|x$

$x \in \mathbb{Z}$ ist genau dann gerade, wenn ein $y \in \mathbb{Z}$ mit $2y = x$ existiert.

Bedingung für „x ist eine gerade Zahl“ als prädikatenlogische Formel:

$$(x \in \mathbb{Z}) \wedge \exists y((y \in \mathbb{Z}) \wedge (2y = x))$$

Menge aller geraden Zahlen:

$$\begin{aligned} & \{x \mid (x \in \mathbb{Z}) \wedge \exists y((y \in \mathbb{Z}) \wedge (2y = x))\} \\ = \; & \{x \in \mathbb{Z} \mid \exists y((y \in \mathbb{Z}) \wedge (2y = x))\} \\ = \; & \{2y \mid y \in \mathbb{Z}\} = 2\mathbb{Z} \end{aligned}$$

Was sind analog $3\mathbb{Z}$, $1\mathbb{Z}$, $0\mathbb{Z}$, $2\mathbb{N}$, $3\mathbb{N}$, $1\mathbb{N}$, $0\mathbb{N}$, $2\mathbb{N}+1$, $3\mathbb{N}+1$, $3\mathbb{N}+2$?

Endliche Mengen

Menge A heißt endlich gdw. eine Zahl $n \in \mathbb{N}$ existiert, so dass A genau n Elemente enthält.
Die leere Menge $\emptyset$ ist die (eindeutig bestimmte) Menge, die kein Element enthält.
Beispiele:

- $\{x \mid (x \in \mathbb{N}) \wedge (x \leq 10)\}$ endlich
- $\{x \mid (x \in 2\mathbb{N}) \wedge (x < 100)\}$ endlich
- $\{x \mid (x \in 2\mathbb{N}) \wedge (x > 100)\}$ nicht endlich
- $\{x \mid (x \in 2\mathbb{N}) \wedge (x < 100)\}$ nicht endlich
- $\{x \mid (x \in 2\mathbb{Z}) \wedge (x \in 2\mathbb{N}+1)\} = \emptyset$ endlich
- $\{x \mid x$ ist Primzahl $\}$ nicht endlich (Widerspruchsbeweis)

$|A|$ heißt Mächtigkeit (Kardinalität) von A.
Beispiele:

- $|\{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}| = 4$
- $|\{\text{rot, grün, blau}\}| = 3$
- $|\{x \mid x \in \mathbb{N} \wedge x \leq 10\}| = 11$
- $|\{a, b, \{a, b\}, \{a, a, b\}, b\}| = 3$
- $|\emptyset| = 0$

Beziehungen zwischen Mengen

$\in$ Element-Relation
Notation $x \in M$ für: x ist Element der Menge M
Negation kurz $\notin$: $a \notin M$ gdw. $\neg(a \in M)$
Beispiele: $a \in \{a, b, 2\}$, $\{a\} \notin \{a, b, 2\}$

$\subseteq$ Teilmengen-Relation
$A \subseteq B$ gdw. $\forall x\,(x \in A \rightarrow x \in B)$
Beispiele: $\{a, b\} \subseteq \{2, a, b, \{2\}\}$, $\{a\} \subseteq \{a\}$,
$\{a\} \not\subseteq \{\{a\}\}$, aber $\{a\} \in \{\{a\}\}$

$=$ Mengengleichheit
$A = B$ gdw. $\forall x\,(x \in A \leftrightarrow x \in B)$
Beispiele: $\{a, b, 2\} = \{2, a, b, 2\}$, $\{a, b, 2\} \neq \{a, \{b\}, 2\}$

$\subset$ echte Teilmenge
$A \subset B$ gdw. $(A \subseteq B) \wedge \neg(A = B)$
Beispiele: $\{2, a\} \subset \{a, b, 2\}$,
$\{2, a\} \not\subset \{2, a\}$, $\{2, a, b\} \not\subset \{2, a\}$

Was bisher geschah

Modellierung von Aussagen
in klassischer Aussagen-Logik

Modellierung von Daten durch Mengen

- Darstellung:

  extensional durch Angabe aller Elemente
  (nur für endliche Mengen möglich)

  intensional durch Angabe der charakterisierenden
  Eigenschaft aller Elemente der Menge
  (als prädikatenlogische Formel)

- leere Menge $\emptyset$
- Mengenbeziehungen $\in, \subseteq, =, \subset$
- Mächtigkeit (Kardinalität) endlicher Mengen

Operationen auf Mengen

Vereinigung $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$
$(x \in (A \cup B)) \leftrightarrow ((x \in A) \vee (x \in B))$
Beispiel: $\{a, c, d\} \cup \{b, c\} = \{a, b, c, d\}$

Schnitt $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$
$(x \in (A \cap B)) \leftrightarrow ((x \in A) \wedge (x \in B))$
Beispiel: $\{a, c, d\} \cap \{b, c\} = \{c\}$

Differenz $A \setminus B = \{x \mid (x \in A) \wedge \neg(x \in B)\}$
$(x \in (A \setminus B)) \leftrightarrow ((x \in A) \wedge \neg(x \in B))$
Beispiel: $\{a, c, d\} \setminus \{b, c\} = \{a, d\}$

symmetrische Differenz $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
Beispiel: $\{a, c, d\} \Delta \{b, c\} = \{a, b, d\}$
Nachweis $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

bei gegebenem Universum U mit $A \subseteq U$:

Komplement $\overline{A} = U \setminus A = \{x \in U \mid \neg(x \in A)\}$
$(x \in \overline{A}) \leftrightarrow \neg(x \in A)$
Beispiel: Für $U = \{a, b, c, d\}$ gilt $\overline{\{a, c\}} = \{b, d\}$

Wichtige Beziehungen zwischen Mengenoperationen

(analog Regeln für $\neg, \vee, \wedge$ in der Aussagenlogik)
Für alle Mengen A, B, C gilt

- $A \cup A = A$, $A \cap A = A$
- $A \cup \emptyset = A$, $A \cap \emptyset = \emptyset$,
- $A \cup B = B \cup A$ und $A \cap B = B \cap A$
  (Kommutativität von $\cap$ und $\cup$)
- $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
  (Assoziativität von $\cap$ und $\cup$)
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (ÜA)
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  (Distributivgesetze)
- $\overline{\overline{A}} = A$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$ und $\overline{A \cap B} = \overline{A} \cup \overline{B}$
  (DeMorgansche Regeln)
- $\overline{\overline{A} \cap \overline{B}} = A \cup B$ und $\overline{\overline{A} \cup \overline{B}} = A \cap B$
  (Dualität von $\cap$ und $\cup$)

Disjunkte Mengen

Mengen A und B mit $A \cap B = \emptyset$ heißen disjunkt.
Beispiele:

- $\{a, b\}$ und $\{c, d\}$ sind disjunkt, weil $\{a, b\} \cap \{c, d\} = \emptyset$
- $\{a, b\}$ und $\{b, c\}$ sind nicht disjunkt, weil $\{a, b\} \cap \{b, c\} = \{b\} \neq \emptyset$
- Jede Menge M ist disjunkt zu $\emptyset$, weil $M \cap \emptyset = \emptyset$
- $2\mathbb{Z}$ und $2\mathbb{Z} + 1$ sind disjunkt
- $2\mathbb{Z}$ und $3\mathbb{Z}$ sind nicht disjunkt, weil $0 \in 2\mathbb{Z} \cap 3\mathbb{Z}$, also $2\mathbb{Z} \cap 3\mathbb{Z} \neq \emptyset$

Mengen $A_1, \ldots, A_n$ heißen genau dann paarweise disjunkt,
wenn $\forall i \in \{1, \ldots, n\}\ \forall j \in \{1, \ldots, n\} \setminus \{i\} : A_i \cap A_j = \emptyset$
Beispiele:

- $A_1 = \{a, d\}, A_2 = \{c\}, A_3 = \{b, e\}$ sind paarweise disjunkt, weil $A_1 \cap A_2 = \{a, d\} \cap \{c\} = \emptyset$, $A_1 \cap A_3 = \{a, d\} \cap \{b, e\} = \emptyset$ und $A_2 \cap A_3 = \{c\} \cap \{b, e\} = \emptyset$
- $A_1 = \{a, d\}, A_2 = \{c\}, A_3 = \{b, d\}$ sind nicht paarweise disjunkt, weil $A_1 \cap A_3 = \{a, d\} \cap \{b, d\} = \{d\} \neq \emptyset$

Zerlegungen (Partitionen) von Mengen

Eine Familie $\{A_i \mid i \in I\}$ paarweise disjunkter nichtleerer Mengen A_i mit

$$\bigcup_{i \in I} A_i = B$$

heißt Zerlegung (Partition) der Menge B.
Beispiele:

- $\{\underbrace{\{a, b\}}_{A_1}, \underbrace{\{c\}}_{A_2}\}$ ist eine Zerlegung der Menge $\{a, b, c\}$,
  weil $A_1 \cap A_2 = \{a, b\} \cap \{c\} = \emptyset$ und
  $A_1 \cup A_2 = \{a, b\} \cup \{c\} = \{a, b, c\}$
- $\{\underbrace{\{a\}}_{A_1}, \underbrace{\{b\}}_{A_2}, \underbrace{\{c\}}_{A_3}\}$ ist eine Zerlegung der Menge $\{a, b, c\}$
- $\{\underbrace{\{a, b\}}_{A_1}, \underbrace{\emptyset}_{A_2}, \underbrace{\{c\}}_{A_3}\}$ ist keine Zerlegung der Menge $\{a, b, c\}$
- $\{\underbrace{\{a\}}_{A_1}, \underbrace{\{c\}}_{A_2}\}$ ist keine Zerlegung der Menge $\{a, b, c\}$,
  aber eine Zerlegung der Menge $\{a, c\}$
- $\{2\mathbb{N}, 2\mathbb{N} + 1\}$ ist eine Zerlegung der Menge $\mathbb{N}$, $\{2\mathbb{N}, 3\mathbb{N}, 4\mathbb{N}\}$ nicht

Potenzmenge

Die Potenzmenge 2^A einer Menge A ist die Menge aller Teilmengen von A

$$2^A = \{B \mid B \subseteq A\}$$

Beispiele:

- Für $A = \{0\}$ gilt $2^A = 2^{\{0\}} = \{\emptyset, \{0\}\}$,
- Für $A = \{\heartsuit\}$ gilt $2^A = 2^{\{\heartsuit\}} = \{\emptyset, \{\heartsuit\}\}$,
- $2^{\{a,b,c\}} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$,
- Für $A = \{0\}$ gilt $2^{\left(2^A\right)} = 2^{\left(2^{\{0\}}\right)} = \{\emptyset, \{\emptyset\}, \{\{0\}\}, \{\emptyset, \{0\}\}\}$,
- Amtssprachen in der Schweiz:
  $S = \{\text{Deutsch, Französisch, Italienisch, Rätoromanisch}\}$
  mögliche Amtssprachkenntnisse der Bewohner: 2^S

Mächtigkeit der Potenzmengen endlicher Mengen:

$$\text{Für jede endliche Menge } A \text{ gilt } \left|2^A\right| = 2^{|A|}$$

Beweis durch Induktion über $|A|$

Modellierungsbeispiele mit Potenzmengen

- Menge aller Möglichkeiten, die Bauteile A, B, C, D einzusetzen (nicht notwendig alle, jedes höchstens einmal)
  $=$ Menge aller Teilmengen der Menge $\{A, B, C, D\}$
  $= 2^{\{A,B,C,D\}}$

  Anzahl aller Möglichkeiten:
  $|2^{\{A,B,C,D\}}| = 2^{|\{A,B,C,D\}|} = 2^4 = 16$
- Menge aller in einem Skatblatt aus 7 Karten möglichen Farbkombinationen
  $=$ Menge aller nichtleeren Teilmengen von $\{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$
  $= 2^{\{\diamondsuit,\heartsuit,\spadesuit,\clubsuit\}} \setminus \{\emptyset\}$
  $(2^4 - 1 = 15$ Möglichkeiten$)$

Aussonderungsprinzip

Zu jeder Menge A und jeder Eigenschaft P existiert eine Menge

$$B = \{x \mid (x \in A) \wedge \ (x \text{ hat die Eigenschaft } P)\} = \{x \in A \mid P(x)\}$$

Beispiele:

- $A =$ Menge aller Fahrräder und ($P(x)$ gdw. x rosa)
  $B =$ Menge aller rosa Fahrräder
- $A =$ Menge aller Skatkarten und
  $P(x)$ gdw. x bedient $(\spadesuit, A)$ (in Null-Spiel)
  $B = \{(\spadesuit, W) \mid W \in \{7, 8, 9, 10, B, D, K\}\}$
- $A = \{x \mid (x \in \mathbb{N}) \wedge (x \leq 100)\} = \{0, \ldots, 100\}$ und
  ($P(x)$ gdw. x gerade)
  $B = \{x \mid (x \in \mathbb{N}) \wedge (x \leq 100) \wedge (2|x)\}$
- $A = 2\mathbb{N}$ und ($P(x)$ gdw. $x \leq 100$)
- $A = \mathbb{N}$ und ($P(x)$ gdw. $2|x$ und $x \leq 100$)

Russells Paradox

(Problem der naiven Mengenlehre)
Annahme:
Es existiert eine Menge A, die alle Mengen (als Elemente) enthält.
Nach Aussonderungsprinzip mit Eigenschaft $P(x)$ gdw. $\neg(x \in x)$
existiert dann auch die Menge

$$B = \{x \mid (x \in A) \wedge P(x)\} = \{x \mid (x \in A) \wedge \neg(x \in x)\}$$

Frage: Gilt $B \in B$?
Weil B eine Menge und jede Menge Element von A ist, gilt $B \in A$. $(\star)$
Für jede Menge x gilt $(x \in x)$ oder $\neg(x \in x)$, also zwei Fälle für $x = B$:

1. $\underline{(B \in B)}$: nach Def. von B also $B \in A$ und $\underline{\neg(B \in B)}$ (Widerspruch)
2. $\underline{\neg(B \in B)}$: nach Def. von B also $\neg((B \in A) \wedge \neg(B \in B))$, wegen $\neg((B \in A) \wedge \neg(B \in B)) \equiv \neg(B \in A) \vee (B \in B)$, also zwei Fälle:
   - 2.1 $\neg(B \in A)$: Widerspruch zu $(B \in A)$ in $(\star)$
   - 2.2 $\underline{(B \in B)}$: Widerspruch

Annahme führt in in allen Fällen zum Widerspruch, ist damit widerlegt.
Eine solche Menge A, die jede Menge (und damit insbesondere auch B) als Element enthält, kann nicht existieren.

alternative Formulierungen: Barbier, Kreter

Mögliche Lösungen

- axiomatischer Aufbau der Mengenlehre
  Fundierungsaxiom:
  Keine Menge kann sich selbst als Element enthalten.
- Klassentheorie (Mengen, Klassen, echte Klassen)
  Klasse aller Mengen ist echte Klasse
- Typentheorie (Hierarchie)
  alle Elemente einer Menge M haben niedrigeren Typ als M
  (in der Informatik übliche Lösung)

(Kartesisches) Produkt von Mengen

$$A \times B = \{(x, y) \mid (x \in A) \wedge (y \in B)\}$$

Beispiele:

- $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$
- $\{1, \ldots, m\} \times \{1, \ldots, n\}$
  $= \{(i, j) \mid i \in \{1, \ldots, m\} \wedge j \in \{1, \ldots, n\}\}$
  häufig als Indexmenge in Matrizen, digitalen Bildern,...
- Namen = Vornamen $\times$ Familiennamen
- Telefonbuch = (Namen $\times$ Vornamen) $\times$ Nummer
- Zeit = (Stunde $\times$ Minute) $\times$ Sekunde
  $= (\{0, \ldots, 23\} \times \{0, \ldots, 59\}) \times \{0, \ldots, 59\}$

Beispiele

- $(1,2) \in (\{0,1\} \times \{1,2\})$, aber $(1,2) \notin (\{1,2\} \times \{0,1\})$
  $(\{0,1\} \times \{1,2\}) \cap (\{1,2\} \times \{0,1\}) = \{(1,1)\}$
- Cafeteria-Essen aus
  $\{\text{Bratwurst, Wiener, Knacker}\} \times \{\text{Kartoffelsalat, Nudelsalat}\}$
  $3 \cdot 2 = 6$ Möglichkeiten
- $12 \cdot 15$ mögliche (gemischte) Tanzpaare aus
  je einem von 12 Männern und je einer von 15 Frauen
- $\{a\} \times \mathbb{N} = \{(a,0),(a,1),(a,2),\ldots\} = \{a_0, a_1, a_2, \ldots\}$

Eigenschaften des Produktes von Mengen

- $\times$ ist nicht kommutativ
  z.B. $\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
  $\neq \{1, 2\} \times \{a, b\} = \{(1, a), (2, a), (1, b), (2, b)\}$
- $\times$ ist „fast“ assoziativ,
  $(A \times B) \times C$ und $A \times (B \times C)$ mit $A \times B \times C$ identifizierbar
  z.B. $(\{a\} \times \{1, 2\}) \times \{\alpha, \beta\} = \{(a, 1), (a, 2)\} \times \{\alpha, \beta\}$
  $= \{((a, 1), \alpha), ((a, 2), \alpha), ((a, 1), \beta), ((a, 2), \beta)\}$
  und $\{a\} \times (\{1, 2\} \times \{\alpha, \beta\}) = \{a\} \times \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta)\}$
  $= \{(a, (1, \alpha)), (a, (2, \alpha)), (a, (1, \beta)), (a, (2, \beta))\}$
  lassen sich beide eineindeutig zuordnen zu
  $\{(a, 1, \alpha), (a, 2, \alpha), (a, 1, \beta), (a, 2, \beta)\} \subseteq A \times B \times C$
- Für jede Menge A gilt $A \times \emptyset = \emptyset$.
- Für alle Mengen A, B, C gilt:
  Aus $A \subseteq B$ folgt $A \times C \subseteq B \times C$
- Distributivgesetze: Für alle Mengen A, B, C gilt
  $(A \cup B) \times C = (A \times C) \cup (B \times C)$ und
  $(A \cap B) \times C = (A \times C) \cap (B \times C)$ (ÜA)
- Für alle endlichen Mengen A und B gilt $|A \times B| = |A| \cdot |B|$

Modellierungsbeispiel Skatkarten

Formale Darstellung der Karten:

Jede Karte ist eindeutig repräsentiert durch

Farbe aus der Menge $F = \{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$ und

Wert
- Zahl aus der Menge $Z = \{7, 8, 9, 10\}$ oder
- Bild aus der Menge $B = \{B, D, K, A\}$

Menge aller Werte $W = Z \cup B$

Menge aller Karten:

$$K = \{(x, y) \mid x \in F \wedge y \in W\} = F \times (Z \cup B)$$

Verteilung der Karten nach dem Geben:

- Skat: $S = \{k_{s,1}, k_{s,2}\} \subseteq K$ mit $|S| = 2$
- für jedes $i \in \{1, 2, 3\}$ Blatt des Spielers i:
  $B_i = \{k_{i,1}, \ldots, k_{i,10}\} \subseteq K$ mit $|B_i| = 10$

wobei

1. $B_1 \cap B_2 = \emptyset$, $B_1 \cap B_3 = \emptyset$, $B_2 \cap B_3 = \emptyset$,
   $S \cap B_1 = \emptyset$, $S \cap B_2 = \emptyset$, $S \cap B_3 = \emptyset$ und
2. $K = S \cup B_1 \cup B_2 \cup B_3$

Also ist $\{S, B_1, B_2, B_3\}$ eine disjunkte Zerlegung von K.

Vereinigung disjunkter Mengen

Vereinigung $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$
Beispiel: Kunden $K = \{a, b, d\}$, Lieferanten $L = \{b, c, d\}$,
Vereinigung $G = K \cup L = \{a, b, c, d\}$ (Geschäftspartner)
enthält keine Information darüber, ob b Kunde oder Lieferant ist

Idee: Mengen vor Vereinigung durch Hinzufügen einer Kennzeichen-Komponente „disjunkt machen“
(Verwaltung von Paaren aus Kennzeichen und Element)
Disjunkte Vereinigung der Mengen $\{A_i\}_{i \in I}$ mit Indexmenge I:

$$\dot{\bigcup}_{i \in I} A_i = \bigcup_{i \in I} A'_i \quad \text{mit} \quad A'_i = \{i\} \times A_i = \{(i, x) \mid x \in A_i\}$$

Mächtigkeit der disjunkten Vereinigung der Mengen $\{A_i\}_{i \in I}$:

$$\left|\dot{\bigcup}_{i \in I} A_i\right| = \left|\bigcup_{i \in I} A'_i\right| = \sum_{i \in I} |A_i|$$

Beispiel Geschäftspartner

- Menge aller Kunden: $A_K = \{a, b, d\}$
- Menge aller Lieferanten: $A_L = \{b, c, d\}$,
- Kennzeichnung (Indexmenge) $I = \{K, L\}$
- gekennzeichnete Geschäftspartner:
  Kunden: $A'_K = \{K\} \times A_K = \{(K, a), (K, b), (K, d)\}$,
  Lieferanten: $A'_L = \{L\} \times A_L = \{(L, b), (L, c), (L, d)\}$
- Menge aller gekennzeichneten Geschäftspartner:
  $A'_K \cup A'_L = \{(K, a), (K, b), (L, b), (L, c), (K, d), (L, d)\}$

Anzahl der (gekennzeichneten) Geschäftspartner

$$|A_K \dot\cup A_L| = |A'_K \cup A'_L| = |A_k| + |A_L| = 6$$

Was bisher geschah

Modellierung von Aussagen in klassischer Aussagen-Logik

Modellierung von Daten durch Mengen

- extensionale und intensionale Darstellung
- Mächtigkeiten von (endlichen) Mengen $|M|$
- Beziehungen zwischen Mengen $\subseteq, =, \subset$
- leere Menge $\emptyset$
- Potenzmenge 2^M
- Mengen-Operationen $\cup, \cap, \overline{\ }, \setminus, \Delta,$
- Zerlegungen
- disjunkte Vereinigung
- (kartesisches) Produkt $\times$

Modellierungsbeispiele

Kartesisches Produkt mehrerer Mengen

$$\bigtimes_{i=1}^{n} A_i = A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \mid \forall i \in \{1, \ldots, n\} : x_i \in A_i\}$$

Für endlich viele endliche Mengen A_i gilt

$$\left| \bigtimes_{i=1}^{n} A_i \right| = \prod_{i=1}^{n} |A_i|$$

Beispiele:

- 5-Gänge-Menü: Auswahl aus
  3 Vorspeisen, 2 Suppen, 5 Hauptgerichten, 3 Desserts, 2 Käse
  $3 \cdot 2 \cdot 5 \cdot 3 \cdot 2 = 180$ mögliche Kombinationen
- $|\{0, 1\}|^n = 2^n$ Binärwörter mit n Stellen
- 10^3 höchstens dreistellige Dezimalzahlen
- 6^5 verschiedene Ergebnisse beim fünfmal aufeinanderfolgenden Würfeln mit einem Würfel
- 6^5 verschiedene Ergebnisse beim Würfeln mit fünf verschiedenfarbigen Würfeln

Iterierte Produkte einer Menge

$$
\begin{aligned}
A^n &= \bigtimes_{i=1}^{n} A \\
A^0 &= \{\varepsilon\} && \text{mit leerem Wort } \varepsilon \\
A^* &= \bigcup_{n\in\mathbb{N}} A^n && \left(= A^0 \cup A^1 \cup \cdots = \{\varepsilon\} \cup A^1 \cup \cdots\right) \\
A^+ &= \bigcup_{n\in\mathbb{N}\setminus\{0\}} A^n = A^* \setminus \{\varepsilon\}
\end{aligned}
$$

(Notation: statt ε mitunter auch (), [])

Elemente aus A^n, A^+, A^* heißen (endliche)

- Folgen (Vektoren) $(a_1, a_2, \ldots, a_n)$,
- Listen $[a_1, a_2, \ldots, a_n]$, $[a_1, a_2, \ldots]$ oder
- Wörter (Strings) $a_1 a_2 \ldots a_n$

Iteriertes Produkt – Beispiele

- $\{0,1\}^*$ Menge aller Binärwörter (beliebiger Länge)
  z.B. $10, 10010, 010, \varepsilon$
- Menge aller Binärwörter der Länge 3
  $\{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- $\{0,1,2\}^*$ Menge aller Ternärwörter (beliebiger Länge)
  z.B. $20, 1202010, \varepsilon$
- Menge aller Ternärwörter der Länge 2
  $\{0,1,2\}^2 = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$
- $\{0\} \cup (\{1,2,3,4,5,6,7,8,9\} \times \{0,1,2,3,4,5,6,7,8,9\}^*)$
  Menge aller natürlichen Zahlen in Dezimaldarstellung (ohne führende Nullen)
- $\{a,b\}^*$ alle Wörter (beliebiger Länge), die nur Buchstaben aus der Menge $\{a,b\}$ enthalten , z.B. $aba, ababa, aaaa, bbbaaa, \varepsilon$
- $\{\{a,b\}^*\}^*$ alle Folgen (Listen) solcher Wörter
  z.B. $[a, aa, aaa]$, $[ba]$, ε, $[\varepsilon, \varepsilon, \varepsilon]$

Folgen

Folgen (Listen, Wörter) werden definiert:

extensional durch Angabe der Elemente und ihrer Reihenfolge
Beispiele: 3210, $[1, 4, 9, 16, 25]$, *abababababa*

intensional durch Angabe einer Eigenschaft, die für jeden Index i das i-te Element eindeutig bestimmt.
Beispiele: $(4 - i)_{1 \leq i \leq 4}$, $(i^2)_{i \in \{1,\ldots,5\}}$,

$$(w_i)_{0 \leq i \leq 10} \text{ mit } w_i = \begin{cases} a & \text{falls } i \in 2\mathbb{Z} \\ b & \text{sonst} \end{cases}$$

$$(v_i)_{i \in \mathbb{N}} \text{ mit } v_i = \begin{cases} a & \text{falls } i \in 2\mathbb{Z} \\ b & \text{sonst} \end{cases}$$

$$(i^2)_{i \in \mathbb{N}} = [0, 1, 4, 9, \ldots], \; (3)_{k \in \mathbb{N}} = [3, 3, 3, 3, \ldots]$$

Länge der Folge $(a_n)_{n \in I}$:
Anzahl der Elemente ($=$ Mächtigkeit der Indexmenge $I \subseteq \mathbb{N}$)

Modellierung durch Mengen und Folgen

- Menge aller Skatkarten in einem Spiel:
  $S = \{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\} \times (\{7, 8, 9, 10\} \cup \{B, D, K, A\})$
- Folge aller Unter (B) nach Wert aufsteigend geordnet
  $[(\clubsuit, B), (\spadesuit, B), (\heartsuit, B), (\diamondsuit, B)] \in S^4$
- Folge aller Karten der Farbe $\spadesuit$ nach Wert (Nullspiel) aufsteigend geordnet
  $[(\spadesuit, 7), (\spadesuit, 8), (\spadesuit, 9), (\spadesuit, 10), (\spadesuit, B), (\spadesuit, D), (\spadesuit, K), (\spadesuit, A)] \in S^8$
- Menge aller Möglichkeiten der (zwei) Karten im Skat:
  $\{\{h, k\} \mid h \in S \wedge k \in S \wedge h \neq k\} = \{M \subseteq S \mid 2 = |M|\} \subseteq 2^S$
  (Warum nicht $\subseteq S^2$?)
- Blatt = Menge aller Karten auf der Hand (zu Beginn des Spieles)
  $B \in 2^S$ mit $|B| = 10$ (10 verschiedene Karten)
- Kartenfächer (zu Beginn des Spieles): Folge $(k_1, \ldots, k_{10}) \in S^{10}$ mit $|\{k_1, \ldots, k_{10}\}| = 10$ (alle Karten verschieden), z.B.
  $[(\spadesuit, B), (\heartsuit, B), (\diamondsuit, A), (\diamondsuit, 9), (\clubsuit, A), (\clubsuit, K), (\clubsuit, 9), (\heartsuit, 10), (\heartsuit, 8), (\heartsuit, 7)]$
- Stich: Folge von drei nacheinander gelegten Karten (geordnetes Tripel) $(k_1, k_2, k_3) \in S^3$ mit $|\{k_1, \ldots, k_3\}| = 3$
- Spiel: Folge der (während des Spiels gefallenen) Stiche $\in \left(S^3\right)^{10}$

Zusammenhänge Folgen – Mengen

zu gegebener Folge $(a_n)_{n \in I}$:

- Menge $\{a_n \mid n \in I\}$ der Elemente der Folge $(a_n)_{n \in I}$ (eindeutig)
  - Folge $[1, 4, 9, 16]$, Menge der Elemente $\{1, 4, 9, 16\}$
  - Folge $[a, a, a, \ldots]$, Menge der Elemente $\{a\}$

  (Gegebene Folge nicht eindeutig rekonstruierbar)
- Menge aller Anfangsstücke der Folge (eindeutig)
  Beispiel: $(2^n)_{n \in \mathbb{N}}$, Menge $\{\varepsilon, [1], [1, 2], [1, 2, 4], \ldots\}$
  (Folge lässt sich eindeutig rekonstruieren.)

zu gegebener Menge A:

- Folgen $(a_n)_{n \in I}$ sind durch Mengen definiert (A^*, A^ω)
- beliebige Anordnung der Elemente einer Menge zu Folgen (i.A. nicht eindeutig, mehrere Möglichkeiten), z.B.
  - $M = \{a, b, c, d\}$, Folgen $[a, b, c, d], [b, d, b, c, d, a]$
  - $M = \mathbb{N}$, Folgen $[0, 1, 2, \ldots]$, $[0, 2, 4, 6, 8, 1, 3, 5, 7, 9, 10, 12 \ldots]$
  - $M = \mathbb{Z}$, Folgen $[0, 1, -1, 2, -2, 3, -3, \ldots]$
    $[0, 1, 2, 3, -3, -2, -1, 4, 5, \ldots]$

Alphabet, Wort, (formale) Sprache

Alphabet (endliche) Menge A von Symbolen

Wort endliche Folge von Symbolen $w = w_1 \cdots w_n$ mit $\forall i \in \{1, \ldots, n\} : w_i \in A$

Länge eines Wortes $|w|$ = Anzahl der Symbole in w

Anzahl der Vorkommen eines Symboles in einem Wort $|w|_a$ = Anzahl der a in w (für $a \in A$)

Sprache Menge von Wörtern $L \subseteq A^*$

Wörter – Beispiele

abbaavatar

ist ein Wort (Zeichenkette) mit Symbolen aus der Menge $\{a, b, r, t, v\}$,
tar und *bratbart* auch, *trallala* und $ab + ba$ nicht

2026

ist ein Wort mit Symbolen aus der Menge $\{0, 6, 2\}$,
026 und 0620060 auch, -60 nicht

$$(x + y) \cdot (z - x)$$

ist ein Wort mit Symbolen aus der Menge $\{x, y, z, (,), +, -, \cdot\}$,
$()xz(xy + -$ auch, $x + 3 \cdot z$ nicht

$$(\neg p \wedge p) \rightarrow q$$

ist ein Wort mit Symbolen aus der Menge $\{p, q, \wedge, \neg, \rightarrow, (,)\}$,
$q \rightarrow (p \rightarrow q)$ und $\wedge)(\neg p \wedge$ auch, $p \leftrightarrow q$ nicht

otto holt obst .

ist ein Wort mit Symbolen aus der Menge $\{otto, obst, holt, .\}$,
. otto . . otto auch, *los otto* nicht

Verkettung von Wörtern (Folgen)

Verkettung $\circ$ von Wörtern: $\circ : A^* \times A^* \to A^*$
Für alle Wörter $u, v \in A^*$ ist $u \circ v = w$ mit

$$\forall i \in \{1, \ldots, |u| + |v|\} : w_i = \begin{cases} u_i & \text{falls } i \leq |u| \\ v_{i-|u|} & \text{falls } i > |u| \end{cases}$$

(Für $u = u_1 \cdots u_{|u|}, v = v_1 \cdots v_{|v|} \in A^*$ ist $u \circ v = u_1 \cdots u_{|u|} v_1 \cdots v_{|v|}$)

Beispiel: $anne \circ marie = annemarie$

Eigenschaften der Operation $\circ$:

- $\circ$ ist assoziativ, d.h.

$$\forall u \in A^* \ \forall v \in A^* \ \forall w \in A^* \ ((u \circ v) \circ w = u \circ (v \circ w))$$

- $\forall w \in A^* \ (\varepsilon \circ w = w \circ \varepsilon = w)$
  (Das leere Wort ε ist neutrales Element für $\circ$)
- $\circ$ ist nicht kommutativ.
  Gegenbeispiel: $u = marie, v = anne$
  $u \circ v = marieanne \neq annemarie = v \circ u$

Umkehrung (gespiegeltes Wort)

Umkehrung w^R von w definiert durch

$$\forall i \in \{1, \ldots, |w|\} : w_i^R = w_{|w|-i+1}$$

(Für $w = w_1 \cdots w_{|w|}$ ist $w^R = w_{|w|} \cdots w_1$)

Beispiele: $(marie)^R = eiram$, $(2026)^R = 6202$, $(101)^R = 101$

$$\left(to \circ \left(\left(m \circ (ate)^R \right)^R \circ n \right)^R \right)^R = \ldots$$

Fakt

Für jedes Wort $w \in A^*$ gilt $\left(w^R\right)^R = w$.

Palindrome

Palindrom: Wort w mit $w = w^R$
B: *anna*, *neben*, ε, jedes Wort der Länge 1

Die Menge aller Palindrome über dem Alphabet A ist

$$\begin{aligned} L_{\text{pal}} &= \{w \in A^* \mid w = w^R\} \\ &= \underbrace{\{w \circ w^R \mid w \in A^*\}}_{L_{\text{pal0}}} \cup \underbrace{\{w \circ a \circ w^R \mid w \in A^* \wedge a \in A\}}_{L_{\text{pal1}}} \end{aligned}$$

Beispiele für Wörter aus L_{pal}:

- $\mathit{otto} = \mathit{ot} \circ \mathit{to} = \mathit{ot} \circ (\mathit{ot})^R$ für $w = \mathit{ot} \in A^* = \{a, \ldots, z\}^*$
- $\mathit{reliefpfeiler} = \mathit{relief} \circ p \circ \mathit{feiler} = \mathit{relief} \circ p \circ (\mathit{relief})^R$
  für $w = \mathit{relief} \in A^* = \{a, \ldots, z\}^*$
- $1 = \varepsilon \circ 1 \circ \varepsilon = \varepsilon \circ 1 \circ \varepsilon^R$ für $A = \{0, 1\}$
- $\varepsilon = \varepsilon \circ \varepsilon = \varepsilon \circ \varepsilon^R$

Was bisher geschah

Modellierung von Aussagen durch Logiken

Modellierung von Daten durch

Mengen

- extensionale und intensionale Darstellung
- Mächtigkeiten endlicher Mengen, $\emptyset$
- Beziehungen zwischen Mengen $\subseteq, =, \subset$
- Mengen-Operationen $\cup, \cap, \overline{\ }, \setminus, \Delta, \times, {}^{n}, {}^{*}, 2^{M}$

Folgen (Vektoren, Listen, Wörtern) über einer Menge A

- extensionale und intensionale Darstellung
- Länge von Folgen, leeres Wort ε (leere Folge)
- unendliche Folgen,
  endliche Folgen fester Länge (Tupel, Vektoren),
  endliche Folgen variabler Länge (Wörter, Listen)
- Operationen auf Wörtern: Verkettung $\circ$, ^{R}
- Palindrome

Präfix-Beziehung zwischen Wörtern (Folgen)

Präfix (Anfangswort) $\sqsubseteq$

$$\forall u \in A^* \; \forall v \in A^* \; ((u \sqsubseteq v) \quad \leftrightarrow \quad (\exists w \in A^* \; (u \circ w = v)))$$

(Für zwei beliebige Wörter $u \in A^*, v \in A^*$ gilt $u \sqsubseteq v$ genau dann, wenn ein Wort $w \in A^*$ existiert, so dass $u \circ w = v$ gilt.)

Beispiele:

- $an \sqsubseteq anna$ (mit $w = na$)
- $tom \sqsubseteq tomate$ (mit $w = ate$)
- $oma \not\sqsubseteq tomate$
- $tat \not\sqsubseteq tomate$
- für jedes Wort $u \in A^*$ gilt $\varepsilon \sqsubseteq u$ (mit $w = u$)
- für jedes Wort $u \in A^*$ gilt $u \sqsubseteq u$ (mit $w = \varepsilon$)

(analog zur Teiler-Beziehung zwischen natürlichen Zahlen)

Postfix-Beziehung auf Wörtern (Folgen)

Postfix (Suffix):

$$\forall u \in A^* \; \forall v \in A^* \; (\; \text{Postfix}(u, v) \leftrightarrow (\exists w \in A^* \; (w \circ u = v)))$$

Für zwei Wörter $u = u_1 \cdots u_m \in A^*, v = v_1 \cdots v_n \in A^*$ heißt u genau dann Postfix (Suffix) von v, wenn ein Wort $w \in A^*$ existiert, so dass $w \circ u = v$ gilt.

Beispiele:

- *enten* ist Postfix von *studenten* (mit $w = stud$)
- ε ist Postfix von *studenten* (mit $w = studenten$)
- *ente* ist kein Postfix von *studenten*
- *den* ist kein Postfix von *studenten*

Infix-Beziehung auf Wörtern (Folgen)

Infix (Teilwort, Faktor):

$$\forall u \in A^* \, \forall v \in A^* \; \big(\mathrm{Infix}(u, v) \leftrightarrow \big(\exists w \in A^* \exists w' \in A^* \; (w \circ u \circ w' = v)\big)\big)$$

Für zwei Wörter $u = u_1 \cdots u_m \in A^*$, $v = v_1 \cdots v_n \in A^*$ heißt u genau dann Infix von v, wenn zwei Wörter $w, w' \in A^*$ existieren, so dass $w \circ u \circ w' = v$ gilt.

Beispiele:

- *oma* ist Infix von *tomate* (mit $w = t$, $w' = te$)
- *tom* ist Infix von *tomate* (mit $w = \varepsilon$, $w' = ate$)
- *den* ist Infix von *studenten* (mit $w = stu$, $w' = ten$)
- *ente* ist Infix von *studenten* (mit $w = stud$, $w' = n$)
- *ente* ist kein Infix von *student*
- *enten* ist Infix von *studenten* (mit $w = stud$, $w' = \varepsilon$)

Weitere Beziehungen zwischen Wörtern

bei gegebener Reihenfolge $<$ auf dem Alphabet A:

lexikographische Ordnung auf A^*:

$\forall u, v \in A^* : u \leq_{\text{lex}} v$ gdw.

L1: $u \sqsubseteq v$ oder

L2: $\exists w \in A^* \; \exists x, y \in A : x < y \wedge wx \sqsubseteq u \wedge wy \sqsubseteq v$

quasi-lexikographische (Längen-lexikographische) Ordnung auf A^*:

$\forall u, v \in A^* : u \leq_{\text{qlex}} v$ gdw.

Q1: $|u| < |v|$ oder

Q2: $|u| = |v| \wedge u \leq_{\text{lex}} v$

Beispiele: für $A = \{b, o, y\}$ mit $b < o < y$

- $bob \leq_{\text{lex}} bobby$ wegen $bob \sqsubseteq bobby$ (L1)
- $bob \leq_{\text{qlex}} bobby$ wegen $|bob| < |bobby|$ (Q1)
- $bobby \leq_{\text{lex}} bobo$ mit $w = bob, x = b, y = o$ (L2)
- $bobo \leq_{\text{qlex}} bobby$ wegen $|bobo| < |bobby|$ (Q1)
- $bob \leq_{\text{qlex}} boy$ wegen $|bob| = |boy|$ und $bob \leq_{\text{lex}} boy$ (Q2)

(Formale) Sprachen

Alphabet endliche Menge A von Symbolen

Wort über A: $w \in A^*$ (Folge von Symbolen aus A)

Sprache über A: $L \subseteq A^*$ (Menge von Wörtern über A)

Voraussetzung für maschinelle Verarbeitung:
endliche Darstellung von (evtl. unendlichen) Sprachen

verschiedene Darstellungen in den LV zur theoretischen Informatik
z.B. Automaten und formale Sprachen im 4. Semester (INB)

Beispiele für Sprachen

- Menge aller englischen Wörter $L_1 \subset \{a, \ldots, z\}^*$
- Menge aller deutschen Wörter $L_2 \subset \{a, \ldots, z, \text{ß}, \text{ä}, \text{ö}, \text{ü}\}^*$
- Menge aller möglichen RNA $L_3 \subseteq \{A, U, G, C\}^*$
- Menge aller natürlichen Zahlen in Dezimaldarstellung $L_4 = \{0, \ldots, 9\}^*$ (evtl. mit führenden Nullen)
- Menge aller natürlichen Zahlen in Binärdarstellung (Bitfolgen beliebiger Länge) $L_5 = \{0, 1\}^*$
- Menge aller aussagenlogischen Formeln in AL$(\{p, q, r\})$ $L_6 \subset \{p, q, r, \mathbb{t}, \mathbb{f}, \neg, \vee, \wedge, \rightarrow, \leftrightarrow, (,)\}^*$,
- Menge aller arithmetischen Ausdrücke über $\mathbb{Z}$ (ohne Variablen) $L_7 \subset \{0, \ldots, 9, +, \cdot, -, /, (,)\}^*$,
- Menge aller deutschen Sätze $L_8 \subset (L_2 \cup \{., , , !, ?, (,), -\})^*$

Sprachen als Mengen

Sprachen $L \subseteq A^*$ sind Mengen von Wörtern (endlichen Folgen)
Mengenbeziehungen auf Sprachen:

$$L \subseteq L' \quad \text{gdw.} \quad \forall w \in A^* \; ((w \in L) \rightarrow (w \in L'))$$
$$L = L' \quad \text{gdw.} \quad \forall w \in A^* \; ((w \in L) \leftrightarrow (w \in L'))$$

Mengenoperationen auf Sprachen:

$$\begin{aligned} L \cup L' &= \{w \mid w \in L \vee w \in L'\} \\ L \cap L' &= \{w \mid w \in L \wedge w \in L'\} \\ L \setminus L' &= \{w \mid w \in L \wedge w \notin L'\} \end{aligned}$$

Komplement einer Sprache $L \subseteq A^*$: $\overline{L} = A^* \setminus L$
Beispiel:

$$\begin{aligned} L &= \{w \mid w \in \{0,1\}^* \wedge \exists n \in \mathbb{N}(|w| = 2n)\} \\ \overline{L} &= \{w \mid w \in \{0,1\}^* \wedge \exists n \in \mathbb{N}(|w| = 2n+1)\} \end{aligned}$$

Operationen auf Sprachen

Verkettung $\circ$ von Sprachen:

$$L_1 \circ L_2 = \{u \circ v \mid (u \in L_1) \wedge (v \in L_2)\}$$

Beispiel:

$$\begin{aligned} L_1 &= \{111, 1, 10\} \quad L_2 = \{00, 0\} \\ L_1 \circ L_2 &= \{111, 1, 10\} \circ \{00, 0\} \\ &= \{1110, 11100, 10, 100, 1000\} \end{aligned}$$

Spiegelung $L^R = \{w^R \mid w \in L\}$

Beispiel: $L = \{a, ab, aba, abab\}$
$L^R = \{a, ba, aba, baba\}$

Iterierte Verkettung

- für Sprachen $L \subseteq A^*$

$$L^0 = \{\varepsilon\} \qquad \forall n \in \mathbb{N}: \qquad L^{n+1} = L \circ L^n = \underbrace{L \circ \cdots \circ L}_{n+1-\text{mal}}$$

$$L^* = \bigcup_{n \in \mathbb{N}} L^n \qquad\qquad L^+ = \bigcup_{n \in \mathbb{N} \setminus \{0\}} L^n$$

- für Wörter (endliche Folgen) $u \in A^*$:

$$\begin{aligned} u^n &= \underbrace{u \circ \cdots \circ u}_{n-\text{mal}} \in A^*, \\ u^* &= \{u\}^* = \{u^n \mid n \in \mathbb{N}\} \subseteq A^* \\ u^+ &= \{u\}^+ = \{u^n \mid n \in \mathbb{N} \setminus \{0\}\} \subseteq A^* \end{aligned}$$

Beispiele:

$$\begin{aligned} (101)^3 &= 101101101 \quad \text{und} \quad 101^3 = 10111 \\ a^* &= \{a^i \mid i \in \mathbb{N}\} = \{\varepsilon, a, aa, aaa, \ldots\} \\ (ab)^* &= \{(ab)^i \mid i \in \mathbb{N}\} = \{\varepsilon, ab, abab, ababab, \ldots\} \\ \varepsilon^* &= \{\varepsilon\} = \varepsilon^+ \end{aligned}$$

Mehr Beispiele für Sprachen

- $\{aa, b\}^*$

$$\begin{aligned} &= \{u_1 \circ \cdots \circ u_n \mid n \in \mathbb{N} \wedge \forall i \in \{1, \ldots, n\}\ (u_i \in \{aa, b\})\} \\ &= \{\varepsilon, b, aa, bb, aab, baa, bbb, aaaa, aabb, baab, bbaa, bbbb, \ldots\} \end{aligned}$$

  $ab \notin \{aa, b\}^*$, $ba \notin \{aa, b\}^*$, $aba \notin \{aa, b\}^*$
- $\emptyset \circ \{aba, bb\} = \emptyset$
- $\{\varepsilon\} \circ \{aba, bb\} = \{aba, bb\}$
- $\{bb\}^* = \{w \in \{b\}^* \mid\ |w| \in 2\mathbb{N}\} = \{\varepsilon, bb, bbbb, \ldots\}$
- $(\{1\} \circ \{0\}^*)^* = \{w \in \{0, 1\}^* \mid w_1 = 1\} \cup \{\varepsilon\}$

Reguläre Ausdrücke – Syntax

Die Menge RegExp(A) aller regulären Ausdrücke über einem Alphabet A ist (induktiv) definiert durch:

IA: $\emptyset \in \mathrm{RegExp}(A)$,
$\varepsilon \in \mathrm{RegExp}(A)$ und
für jedes Symbol $a \in A$ gilt $a \in \mathrm{RegExp}(A)$

IS: für alle $E \in \mathrm{RegExp}(A)$ und $F \in \mathrm{RegExp}(A)$ gilt
$(E + F), EF, (E)^* \in \mathrm{RegExp}(A)$.

(Baumdarstellung)

Beispiele:

- $(\emptyset + 1) \in \mathrm{RegExp}(\{0, 1\})$,
- $(\varepsilon + ((ab)^* a)^*) \in \mathrm{RegExp}(\{a, b\})$,
- $(\spadesuit\heartsuit^*\emptyset + \diamondsuit)^* \in \mathrm{RegExp}(\{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\})$,
- für beliebiges Alphabet A gilt $\varepsilon \in \mathrm{RegExp}(A)$,
$(\varepsilon + \emptyset) \in \mathrm{RegExp}(A)$,
- $0+(1+2+3+4+5+6+7+8+9)(0+1+2+3+4+5+6+7+8+9)^*$
$\in \mathrm{RegExp}(\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\})$

Reguläre Ausdrücke – Semantik

Jeder reguläre Ausdruck $E \in \mathrm{RegExp}(A)$ repräsentiert die wie folgt definierte Sprache $L(E) \subseteq A^*$:

IA:
- $L(\emptyset) = \emptyset$
- $L(\varepsilon) = \{\varepsilon\}$
- $\forall a \in A : L(a) = \{a\}$

IS: $\forall E, F \in \mathrm{RegExp}(A)$:
- $L(E + F) = L(E) \cup L(F)$
- $L(EF) = L(E) \circ L(F)$
- $L(E^*) = L(E)^*$

Eine Sprache $L \subseteq A^*$ heißt genau dann regulär, wenn ein regulärer Ausdruck $E \in \mathrm{RegExp}(A)$ existiert, so dass $L = L(E)$.
Beispiele: Für $A = \{a, b\}$ gilt

$$
\begin{aligned}
L(ab^*) &= \{a, ab, abb, abbb, abbbb, \ldots\} = \{ab^i \mid i \in \mathbb{N}\} \\
L((ab)^*) &= \{\varepsilon, ab, abab, ababab, \ldots\} = \{(ab)^i \mid i \in \mathbb{N}\} \\
L((a+b)^*) &= \{a, b\}^* \\
L(a^*b^*) &= \{u \circ v \mid u \in a^* \wedge v \in b^*\} = \{a^i b^j \mid i \in \mathbb{N} \wedge j \in \mathbb{N}\} \\
L((a^*b^*)^*) &= \{a, b\}^*
\end{aligned}
$$

Beispiele

- Für $E = 0 + (1 + 2 + \cdots + 9)(0 + 1 + \cdots + 9)^*$ ist
  $L(E)$ = Menge aller Dezimaldarstellungen natürlicher Zahlen
- für $A = \{A, B, \ldots, Z, a, b, \ldots, z\}$ ist $L(A^*(oma + otto)A^*) =$
  Menge aller Wörter mit Infix *oma* oder *otto* (oder beiden)
  z.B. $tomate \in L(A^*(oma + otto)A^*)$, $lotto \in L(A^*(oma + otto)A^*)$,
  $ottomane \in L(A^*(oma + otto)A^*)$
- Menge aller möglichen HTWK-Email-Adressen
  $\subset L((A + \cdots + Z + a + \cdots + z + 0 + \cdots + 9 + . + -)^*$@htwk-leipzig.de)

Reguläre Ausdrücke ermöglichen eine
endliche Darstellung unendlicher Sprachen.

Aber: Nicht jede (unendliche) Sprache ist regulär. (Warum?)

(mehr dazu in den LV zur theoretischen Informatik,
z.B. Automaten und Formale Sprachen im 4. Semester)

Beispiele regulärer Sprachen

- $L_1 = \emptyset$ ist eine reguläre Sprache, weil
  $\emptyset \in \text{RegExp}(A)$ und $L(\emptyset) = \emptyset = L_1$
- $L_2 = \{a, bab\}$ ist eine reguläre Sprache, weil
  $a + bab \in \text{RegExp}(A)$ und $L(a + bab) = L_2$
- $L_3 = \{w \in \{a, b, c\}^* \mid abba \sqsubseteq w\}$ ist regulär, weil
  $abba(a + b + c)^* \in \text{RegExp}(\{a, b, c\})$ und
  $L(abba(a + b + c)^*) = L_3$
- $L_4 = \{w \in \{a, b, c\}^* \mid aa$ oder bbb sind Infix von $w\}$
  ist eine reguläre Sprache, weil
  $(a + b + c)^*(aa + bbb)(a + b + c)^* \in \text{RegExp}(\{a, b, c\})$
  und $L((a + b + c)^*(aa + bbb)(a + b + c)^*) = L_4$
- $\{w \in \{a, b\}^* \mid |w| \in 2\mathbb{N}\} = L(((a + b)(a + b))^*)$