Schreibweisen:

$\forall x \ldots$	bedeutet	"für alle $x \ldots$"
$\exists x \ldots$	bedeutet	"es existiert ein x mit $\ldots$"
$G \Rightarrow H$	bedeutet	"wenn G, dann H"
		"aus G folgt H"
$G \Leftrightarrow H$	bedeutet	$G \Rightarrow H$ und $H \Rightarrow G$.

Satz 1.1

Sei R eine Äquivalenzrelation auf einer Menge A. Dann bilden die Äquivalenzklassen von R eine Partition von A.

Beweis:

Sei

$$\Pi = \{ [a] \mid a \in A \}.$$

Ziel: Beweis, dass Π eine Partition von A ist.

Hierzu müssen wir zeigen, dass

i) jede Äquivalenzklasse in Π nichtleer,
ii) die Äquivalenzklassen in Π paarweise disjunkt und
iii) A gleich der Vereinigung der Äquivalenzklassen in Π

sind.

Reflexivität von $R \Rightarrow a \in [a] \quad \forall a \in A$.
$\Rightarrow$ i)

Annahme:
Es existieren zwei verschiedene Äquivalenzklassen $[a]$ und $[b]$ mit $[a] \cap [b] \neq \emptyset$

Dann existiert ein $c \in A$ mit $c \in [a] \cap [b]$.

$\Rightarrow$

$(a,c) \in R$ und $(c,b) \in R$.

Transitivität von R $\Rightarrow$ $(a,b) \in R$

Symmetrie von R $\Rightarrow$ $(b,a) \in R$.

Betrachte $d \in [a]$ beliebig. Dann gilt

$(d,a) \in R$

Transitivität von R $\Rightarrow$ $(d,b) \in R$

$\Rightarrow$

$d \in [b]$

Also gilt $[a] \subseteq [b]$.

Ebenso zeigt man $[b] \subseteq [a]$.

Also gilt $[a] = [b]$, was ein Widerspruch zur Annahme $[a] \neq [b]$ ist.

$\Rightarrow$ ii)

Wegen $\bigcup \Pi = \bigcup_{a \in A} [a]$ und $a \in [a]$ $\forall a \in A$ gilt iii) offensichtlich.

∎

Gegeben eine Äquivalenzrelation R auf einer Menge A können wir die zu R korrespondierende Partition Π von A konstruieren.

Umgekehrt können wir die zu einer gegebenen Partition Π einer Menge A korrespondierende Äquivalenzrelation R wie folgt definieren:

$$R := \{ (a,b) \mid a,b \in A \text{ und } a,b \text{ sind in derselben Menge der Partition } \Pi \}.$$

Beachte, dass in der Definition von R die Elemente a und b nicht verschieden sein müssen.

Eine Relation, die reflexiv, antisymmetrisch und transitiv ist, heißt <u>partielle Ordnung</u>.

<u>Beispiel 1.15:</u>

<u>Vereinbarung</u>: Jede Person ist Vorfahr von sich selbst.

Dann ist folgende Relation R eine partielle Ordnung:

$$R := \{ (a,b) \mid a,b \text{ Personen und } a \text{ ist ein Vorfahr von } b \}$$

◊

Eine partielle Ordnung $R \subseteq A \times A$ heißt <u>totale Ordnung</u>, falls $\forall\, a,b \in A,\ a \neq b$

entweder $(a,b) \in R$ oder $(b,a) \in R$.

Beispiel 1.15 (Fortführung)

Obige Relation R ist nicht total, da Geschwister nicht miteinander in Relation stehen.

$\leq$ definiert eine totale Ordnung auf Zahlen. ◆

Eine Kette in einer binären Relation R ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $(a_i, a_{i+1}) \in R$ für $1 \leq i < n$. Wir sagen dann, dass $(a_1, a_2, \ldots, a_n)$ eine Kette von a_1 nach a_n ist. Die Kette $(a_1, a_2, \ldots, a_n)$ ist ein einfacher Kreis, falls $a_i \neq a_j$ für $1 \leq i < j \leq n$ und $(a_n, a_1) \in R$. Ein einfacher Kreis $(a_1, a_2, \ldots, a_n)$ ist trivial, falls $n = 1$. Andernfalls ist ein einfacher Kreis nichttrivial.

Satz 1.2

Eine Relation R ist genau dann eine partielle Ordnung, wenn reflexiv und transitiv ist und keine nichttriviale Kreise besitzt.

Beweis:

„$\Rightarrow$"

Annahme: R ist eine partielle Ordnung.

Definition von partielle Ordnung $\Rightarrow$

R ist reflexiv und transitiv.

Zu zeigen: R besitzt keine nichttriviale Kreise.

Annahme:

R hat nichttrivialen Kreis $(a_1, a_2, \dots, a_n)$, $n \geq 2$.

$\Rightarrow$

$(a_n, a_1) \in R$

Transitivität von R $\Rightarrow$ $(a_1, a_n) \in R$.

Dies ist ein Widerspruch zur Antisymmetrie der partiellen Ordnung

$\Rightarrow$

R besitzt keine nichttriviale Kreise.

„$\Leftarrow$"

Annahme:

R ist reflexiv, transitiv und besitzt keine nichttriviale Kreise.

Zu zeigen: R ist antisymmetrisch.

Annahme: R ist nicht antisymmetrisch

$\Rightarrow$

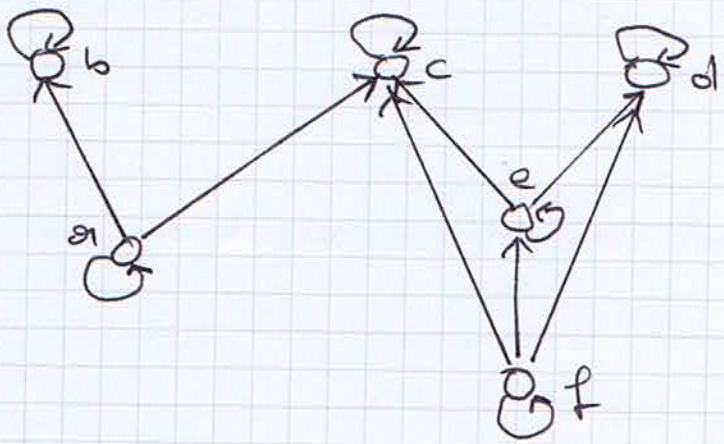
$\exists\, a, b$ mit $a \neq b$ und $(a,b), (b,a) \in R$

Dann ist (a,b) ein nichttrivialer Kreis, was gemäß Annahme nicht sein kann.

$\Rightarrow$ R ist antisymmetrisch.

Sei $R \subseteq A \times A$ eine partielle Ordnung. Ein Element $a \in A$ heißt **minimales Element bezüglich R**, falls $(b, a) \in R \Rightarrow b = a$. Falls die partielle Ordnung fest ist, dann heißt a auch **minimales Element von A**.

Beispiel 1.20



a und f sind die minimale Elemente.

Bemerkung

- Jede endliche partielle Ordnung besitzt mindestens ein minimales Element. (überzeugen Sie sich).
- Eine unendliche partielle Ordnung kann ein minimales Element besitzen oder nicht. (überzeugen Sie sich).

Beispiel 1.21

Sei S eine beliebige Kollektion von Mengen. Die Relation R_S sei wie folgt definiert:

$$R_S := \{ (A,B) \mid A,B \in S \text{ und } A \subseteq B \}.$$

R_S definiert eine partielle Ordnung auf S.

- Betrachte

$$S := \left\{ \{ x \mid x \in \mathbb{R} \text{ und } 0 \leq x \leq \tfrac{1}{n} \} \mid n \in \mathbb{N} \right\}$$

Dann besitzt R_S kein minimales Element.

- Betrachte

$$S := \{ \{a\}, \{b\}, \{a,b\} \}.$$

Dann besitzt R_S zwei minimale Elemente.

◆

Infixnotation:

Manchmal schreiben wir $a R b$ anstatt $(a,b) \in R$.

Für Gleichheit verwenden wir immer die Infix-notation. Wir schreiben

$$a = b \text{ anstatt } (a,b) \in =.$$

1.5 Abschlusseigenschaften

Die Summe zweier natürlichen Zahlen ist stets wieder eine natürliche Zahl. Daher sagen wir, dass die Menge $\mathbb{N}$ der natürlichen Zahlen unter der Operation Addition abgeschlossen ist. Die Differenz zweier natürlichen Zahlen kann eine negative Zahl ergeben. Da negative Zahlen keine natürliche Zahlen sind, ist somit $\mathbb{N}$ nicht unter der Operation Subtraktion abgeschlossen.

Frage:
Welche Zahlen müssen wir zu $\mathbb{N}$ hinzunehmen um eine unter Subtraktion abgeschlossene Menge, die $\mathbb{N}$ enthält, zu erhalten?

Wenn wir zu $\mathbb{N}$ die Null und die negative Zahlen hinzunehmen, dann erhalten wir die Menge $\mathbb{Z}$ der ganzen Zahlen. Diese ist unter der Subtraktion abgeschlossen. Wenn wir aus $\mathbb{Z}$ die Null oder eine negative Zahl entfernen, dann ist die resultierende Menge nicht mehr unter der Subtraktion abgeschlossen. Somit ist $\mathbb{Z}$ die kleinste Menge, die $\mathbb{N}$ enthält und unter Subtraktion abgeschlossen ist.

Weiterhin ist die Menge $\mathbb{Z}$ genau diejenige Menge von Zahlen, die man aus $\mathbb{N}$ mittels wiederholten Subtraktionen erhalten kann.

Daher heißt $\mathbb{Z}$ auch der Abschluss von $\mathbb{N}$ unter Subtraktion.

Ziel:
Entwicklung von allgemeinen Eigenschaften von Abschlüssen.

Hierm definieren wir zunächst allgemein, wann eine Menge abgeschlossen ist. Seien D eine Menge, $n \geq 0$ und $R \subseteq D^{n+1}$ eine $(n+1)$-stellige Relation auf D. Eine Teilmenge B von D heißt abgeschlossen unter R, falls

$$b_1, b_2, \ldots, b_n \in B \text{ und } (b_1, b_2, \ldots, b_{n+1}) \in R$$
$$\Rightarrow \quad b_{n+1} \in B.$$

Jede Eigenschaft der Form "B ist abgeschlossen unter den Relationen $R_1, R_2, \ldots, R_m$" heißt Abschlusseigenschaft von B.

Beispiel 1.22

Seien $D = 2^{\mathbb{N}}$, $n = 2$ und $R \subseteq D^3$ definiert durch

$$(S, T, U) \in R \iff U = S \cap T.$$

B ist abgeschlossen unter R bedeutet dann, dass der Durchschnitt zweier beliebigen Mengen in B wieder in B liegt.

Folgende Teilmenge $\mathcal{B}$ von D ist abgeschlossen unter R:

$$\mathcal{B} := \{\{x \in \mathbb{N} \mid a \leq x \leq b\} \mid a, b \in \mathbb{N}\}.$$

Beachte, dass $a > b$

$$\{x \in \mathbb{N} \mid a \leq x \leq b\} = \emptyset$$

impliziert.

Beispiel 1.23

Da Relationen selbst Mengen sind, können wir sagen, dass eine Relation unter einer oder mehreren anderen Relationen abgeschlossen ist.

Seien D eine Menge und $Q \subseteq (D \times D)^3$ eine dreistellige Relation auf D^2 definiert durch

$$Q := \{((a,b),(b,c),(a,c)) \mid a, b, c \in D\}.$$

Dann ist eine Relation $R \subseteq D \times D$ genau dann transitiv, wenn R unter Q abgeschlossen ist. Somit kann die Transitivität einer Relation als eine Abschlusseigenschaft aufgefasst werden.

Auch die Reflexivität von R kann als eine Abschlusseigenschaft aufgefasst werden. Hierzu definieren wir folgende einstellige Relation auf D^2:

$Q' := \{((a,a)) \mid a \in D\}$.

$R \subseteq D \times D$ ist genau dann reflexiv, wenn R unter Q' abgeschlossen ist.

◆

Beispiel 1.24

Seien D eine Menge, $n \geq 0$ und $f: D^n \to D$ eine Funktion. $B \subseteq D$ heißt abgeschlossen unter f, falls $f(b_1, b_2, \ldots, b_n) \in B$ für alle $b_1, b_2, \ldots, b_n \in B$.

Wenn wir $f: D^n \to D$ als eine Relation $R \subseteq D^{n+1}$ auffassen, dann kann "abgeschlossen unter f" als "abgeschlossen unter R" interpretiert werden.

◆

Ausgehend von einer Menge A betrachtet man häufig "die kleinste" Menge B, die A enthält und eine Eigenschaft P besitzt. Damit die Menge B wohldefiniert ist, muss "die kleinste" eine eindeutige Bedeutung besitzen. Üblicherweise bedeutet "die kleinste" nicht "die kleinste Größe haben", sondern "die minimale bezüglich der partiellen Ordnung bei Mengeninklusion".

Da eine Menge von Mengen verschiedene minimale Elemente oder keines besitzen kann, hängt die Wohldefiniertheit von B von der Art der Eigenschaft P und der Menge A ab.

Beispiel 1.25

Betrachte $A := \{a\}$ und

$P :=$ " besitzt entweder b oder c als Element ".

Dann ist B nicht wohldefiniert, da sowohl $\{a,b\}$ als auch $\{a,c\}$ minimale Mengen mit A als Teilmenge und mit Eigenschaft P sind.

Folgender Satz zeigt, dass für eine Abschlusseigenschaft P die Menge B immer wohldefiniert ist.

Satz 1.3

Sei P eine Abschlusseigenschaft, die durch Relationen auf einer Menge D definiert ist und sei $A \subseteq D$. Dann existiert eine eindeutige minimale Menge B mit $A \subseteq B$, die die Eigenschaft P besitzt.

Beweis:

Sei P definiert als Abschluss unter den Relationen $R_1, R_2, \dots, R_m$, wobei $R_i \subseteq D^{n_i+1}$ für ein n_i, $1 \leq i \leq m$.

Sei S die Menge alles Mengen, die unter $R_1, R_2, \dots, R_m$ abgeschlossen sind und A als Teilmenge haben.

Da D selbst unter jedem R_i abgeschlossen ist und $A \subseteq D$ gilt

$$S \neq \emptyset.$$

Betrachte

$$B := \bigcap S.$$

Beh.: B ist das eindeutige minimale Element von S.

Bew d. Beh.:

Zunächst beweisen wir, dass $B \in S$.

- Es gilt $A \subseteq B$, da $A \subseteq C \ \forall C \in S$.
- Betrachte $i \in \{1, 2, \dots, m\}$ beliebig aber fest. Seien $b_1, b_2, \dots, b_{n_i} \in B$ und $(b_1, b_2, \dots, b_{n_i+1}) \in R_i$.

Dann gilt

$$b_1, b_2, \dots, b_{n_i} \in C \quad \forall C \in S.$$

Da jeder $C \in S$ abgeschlossen ist unter R_i gilt

$$b_{u_i+1} \in C \quad \forall C \in S$$

$$\Rightarrow$$

$$b_{u_i+1} \in B$$

Also ist B abgeschlossen unter R_i.
Insgesamt haben wir gezeigt, dass $B \in S$.
Betrachte B' beliebig mit

$A \subseteq B'$ und B' ist abgeschlossen unter R_i, $1 \leq i \leq m$.

Dann gilt $B' \in S$. $\Rightarrow$ $B \subseteq B'$.
Also ist B minimal und auch das einzige minimale Element von S.

■

Das im Beweis von Satz 1.3 konstruierte B heißt <u>Abschluss von A</u> unter den Relationen $R_1, R_2, \ldots, R_m$.

Eine wichtige Anwendung des Satzes 1.3 ist der <u>reflexive, transitive Abschluss</u> R^* einer binären Relation $R \subseteq A \times A$. R^* ist der Abschluss von R unter den Relationen

$$Q := \{((a,b),(b,c),(a,c)) \mid a,b,c \in A\}$$

$$Q' := \{((a,a)) \mid a \in A\}.$$

Beispiel 1.26

Betrachte

$$R := \{(a,b) \mid \exists \text{ Straße zwischen } a \text{ und } b\}.$$

Dann ist

$$R^* = \{(a,b) \mid b \text{ ist von } a \text{ über Straßen erreichbar}\}.$$

Die Definition von R^* gemäß Satz 1.3 gibt uns eine Sicht "von oben". R^* ist minimal unter einer Klasse von Relationen mit ähnlichen Eigenschaften. Folgender Satz charakterisiert R^* "von unten":

Satz 1.4

Der reflexive, transitive Abschluss R^* einer zweistelligen Relation R ist gleich

$$R \cup \{(a,b) \mid \exists \text{ Kette in } R \text{ von } a \text{ nach } b\}.$$

Bemerkung:

Obiger Satz sagt aus, welche geordnete Paare zu R hinzugenommen werden müssen, um R^* zu erhalten.

Beweis:

Sei $\bar{R} := R \cup \{(a,b) \mid \exists$ Kette von a nach b in $R\}$

Zu zeigen: $R^* \subseteq \bar{R}$

Hierzu beweisen wir zunächst $R^* \subseteq \bar{R}$ und dann $R^* \supseteq \bar{R}$.

„$\subseteq$"

Betrachte $(a,b) \in R^*$ beliebig aber fest.
Zu zeigen: $(a,b) \in \bar{R}$.

Falls $(a,b) \in R$, dann gilt offensichtlich $(a,b) \in \bar{R}$.
Gemäß der Definition einer Kette existiert in jeder Relation R die Kette von a nach a.
$\Rightarrow$
$(a,a) \in \bar{R}$ $\forall a \in A$. Somit haben wir $(a,b) \in \bar{R}$ für den Fall $a = b$ bewiesen.

Annahme: $(a,b) \notin R$ und $a \neq b$.

$(a,b) \in R^* \Rightarrow$

(a,b) ist im Abschluss von R unter der Relation Q.

$\Rightarrow \exists\, c \in A$ mit $(a,c), (c,b) \in R^*$
D.h., wir haben nun die Folge

$$(a,c), (c,b)$$

Falls $(a,c) \in R$, dann terminiert unsere

Betrachtung bezüglich (a,c). Falls $(a,c) \in R$, dann setzen wir die Betrachtung von (a,c) rekursiv fort und ersetzen in obiger Folge (a,c) durch die aus (a,c) konstruierte Folge.

Genauso verfahren wir mit (c,b).

Insgesamt erhalten wir eine Folge

$$(a,c_1), (c_1,c_2), \ldots, (c_{k-1}, c_k), (c_k, b)$$

mit $k \geq 1$ und jedes Paar in obiger Folge ist in R enthalten.

$\Rightarrow$

Wir haben die Kette $(a, c_1, c_2, \ldots, c_k, b)$ von a nach b in R konstruiert.

$\Rightarrow$

$(a,b) \in \overline{R}$.

„$\supseteq$"

Übung

Mitunter verwendet man in der Literatur

„ reflexive, transitive Hülle" Synonym für
„ reflexiven, transitiven Abschluss".

Falls man nicht die Reflexivität verlangt, dann spricht man vom <u>transitiven Abschluss</u> R^+.

1.6 Endliche und unendliche Mengen

Zwei Mengen A und B sind gleichmächtig (in Zeichen: $|A| = |B|$), falls eine bijektive Abbildung $f: A \to B$ existiert.

Bemerkung:

a) Falls A eine endliche Menge ist, dann bedeutet $|A| = |B|$, dass B auch eine endliche Menge ist und B genauso viele Elemente enthält wie A.

b) Wenn $f: A \to B$ eine bijektive Abbildung ist, dann existiert eine bijektive Abbildung $f^{-1}: B \to A$. Also ist die Relation "gleichmächtig" symmetrisch.

Frage:
Sind die Mengen der Vielfachen von 1001 $A := \{1001, 2002, 3003, \ldots\}$ und die Menge $\mathbb{N}$ gleichmächtig?

Zur Beantwortung dieser Frage genügt es, entweder eine Bijektion $f: A \to \mathbb{N}$ anzugeben oder zu beweisen, dass solche nicht existiert.

$f: A \to \mathbb{N}$ mit $f(i \cdot 1001) := i$ ist eine bijektive Abbildung. (Überzeugen Sie sich).

Wenn A eine endliche Menge ist, dann ist die Kardinalität von A gleich der Elementanzahl von A. Es gibt unendliche Mengen, die nicht gleichmächtig sind (das werden wir noch beweisen). Dies wirft folgende Frage auf:

Frage:
Wie definiert man die Kardinalität von unendlichen Mengen?

Die Beantwortung dieser Frage geht über die Vorlesung hinaus. Jedoch werden wir zwischen zwei Arten von unendlichen Mengen unterscheiden.

Eine Menge A heißt abzählbar, wenn es eine injektive Abbildung $f: A \to \mathbb{N}_0$ gibt. Falls keine solche Injektion existiert, dann heißt A überabzählbar.

Bemerkung:
Abzählbare Mengen sind endlich oder gleichmächtig zu $\mathbb{N}_0$.

Übung:
Zeigen Sie, dass die Relation "gleichmächtig" eine Äquivalenzrelation ist.

Falls eine Menge A abzählbar und nicht endlich ist, dann sagen wir auch, dass A

abzählbar unendlich ist.

Übung:
Beweisen Sie, dass die Menge aller abzählbar unendlichen Mengen exakt diejenigen Mengen, die zu $\mathbb{N}$ gleichmächtig sind, enthält.

Ist $f: A \to \mathbb{N}_0$ injektiv, dann ist f auch auf jeder Teilmenge $S \subseteq A$ injektiv. Also ist jede Teilmenge einer abzählbaren Menge abzählbar.

Satz 1.5
Sei A eine abzählbar unendliche Menge. Dann sind A und $\mathbb{N}$ gleichmächtig.

Beweis:
Wir haben zu zeigen, dass eine bijektive Abbildung $f: A \to \mathbb{N}$ existiert.

A abzählbar unendlich $\Rightarrow$

$\exists$ injektive Abbildung $g: A \to \mathbb{N}_0$.

D.h., für $a, a' \in A$ mit $a \neq a'$ gilt $g(a) \neq g(a')$
Sei

$$g(A) := \{ n \in \mathbb{N}_0 \mid \exists\, a \in A \text{ mit } g(a) = n \}.$$

Da A abzählbar unendlich ist $g(A)$ unendlich.

Annahme:
Die Zahlen in $g(A)$ sind aufsteigend sortiert und in dieser Reihenfolge mit 1 beginnend durchnummeriert.

Bezeichne $g(A,i)$ die i-te Zahl in dieser Liste. Wir definieren dann für $a \in A$

$$f(a) := i \text{ , wobei } g(a) = g(A,i)$$

Da g injektiv ist, ist auch f injektiv. Da für jedes $j \in \mathbb{N}$ auch ein $a' \in A$ mit $f(a') = j$ existiert, ist f auch surjektiv.
$\Rightarrow$
f ist bijektiv.

Somit existiert für jede abzählbar unendliche Menge eine Bijektion $f: A \to \mathbb{N}$. Dies erleichtert uns nachfolgend die Arbeit.

Satz 1.6
Die Vereinigung von endlich vielen abzählbaren Mengen ist abzählbar.

Beweis:

Seien

$A_1, A_2, \dots, A_t$ abzählbare Mengen.

Falls A_i, $i \in \{1,2,\dots,t\}$ abzählbar unendlich ist,

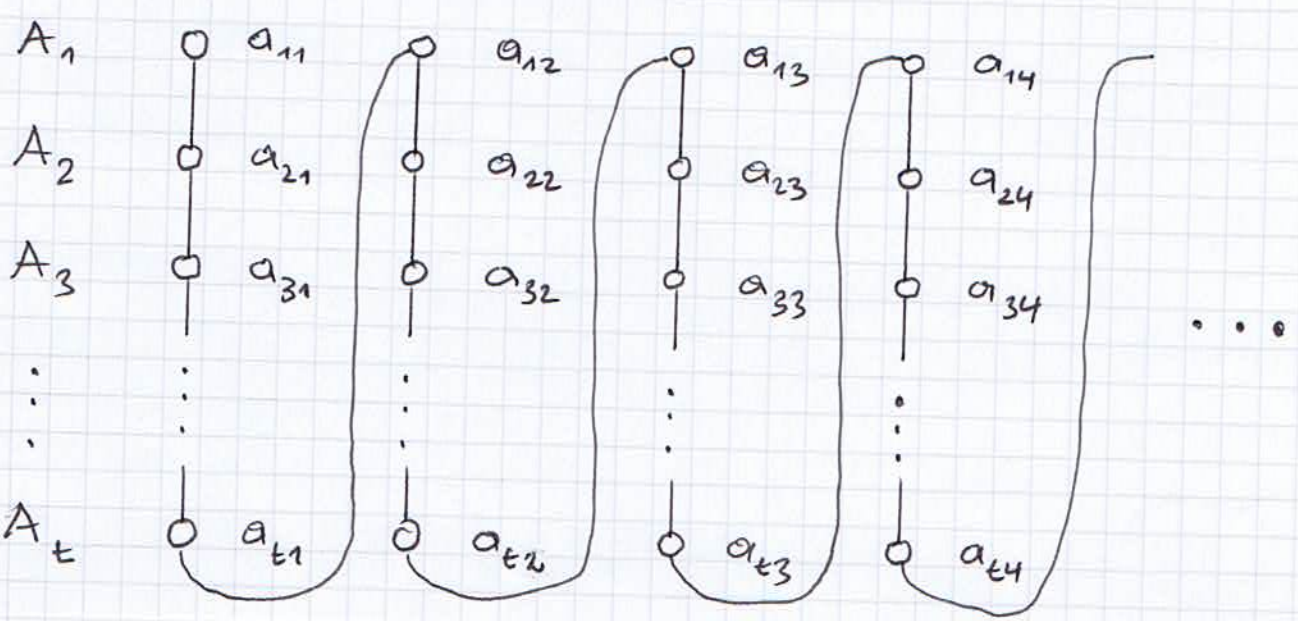
dann existiert eine Bijektion $f: A_i \to \mathbb{N}$.
Falls A_i endlich ist und n Elemente enthält, dann existiert eine Bijektion $f: A_i \to \{1, 2, \dots, n\}$. Dasjenige $a \in A_i$ mit $f(a) = j$ ist das j-te Element von A_i.

Nachfolgend bezeichnet a_{ij} das j-te Element der Menge A_i.

Ziel:
Konstruktion einer Injektion $g: \bigcup_{i=1}^{t} A_i \to \mathbb{N}$.

Idee:

Betrachte zunächst das erste Element von A_1, dann das erste Element von A_2, usw.
Nach dem ersten Element von A_t, betrachte das zweite Element von A_1, dann das zweite Element von A_2, u.s.w. D.h., wir betrachten die Elemente von $A_1, A_2, \dots, A_t$ in der nachfolgend skizzierten Reihenfolge:



Wir starten mit

$$j := 1$$

betrachten in obiger Reihenfolge das erste Element a_{11}, definieren

$$g(a_{11}) := j;$$
$$j := j+1$$

und betrachten das nächste Element.

Sei a_{akt} das aktuell betrachtete Element. Dann wird wie folgt verfahren:

Falls $g(a_{akt})$ nicht definiert,
dann

$$g(a_{akt}) := j;$$
$$j := j+1;$$

Betrachte das nächste Element.

Andernfalls betrachte das nächste Element.

Falls die Mengen $A_1, A_2, \ldots, A_t$ nicht paarweise disjunkt sind, dann kommt es vor, dass für ein aktuell betrachtetes Element a_{akt} der Wert $g(a_{akt})$ bereits definiert ist.

Aus der Konstruktion ergibt sich direkt, dass die Abbildung $g: \bigcup_{i=1}^{t} A_i \to \mathbb{N}$ injektiv ist.

■

Satz 1.7

$\mathbb{N} \times \mathbb{N}$ ist abzählbar.

Beweis:

$\mathbb{N} \times \mathbb{N}$ kann betrachtet werden als die Vereinigung von abzählbar unendlich vielen paarweise disjunkten Mengen

$$\{1\} \times \mathbb{N}, \{2\} \times \mathbb{N}, \{3\} \times \mathbb{N}, \ldots$$

Ziel:
Konstruktion einer Injektion $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Die Besuchsreihenfolge aus dem Beweis von Satz 1.6 kann hier nicht verwendet werden, da niemals das zweite Element einer Menge besucht werden würde.

Idee:

1. In der ersten Runde besuchen wir das erste Element der ersten Menge: $(1,1)$.
2. In der zweiten Runde besuchen wir das nächste Element der ersten Menge $(1,2)$ und dann das erste Element der zweite Menge: $(2,1)$.
3. In der dritten Runde besuchen wir das nächste nicht besuchte Element der ersten Menge, $(1,3)$ dann das nächste nicht besuchte Element der zweite Menge, $(2,2)$ und dann das erste Element der dritten Menge: $(3,1)$.

⋮

4. In der n-ten Runde besuchen wir das n-te Element der ersten Menge, $(1,n)$, dann das $(n-1)$-te Element der zweiten Menge, $(2,n-1)$, ..., und das erste Element der n-ten Menge.

Unter Verwendung obiger Besuchsreihenfolge können wir endlich zum Beweis von Satz 1.6 den Beweis zuende führen. ∎

Übung:

a) Arbeiten Sie den Beweis von Satz 1.7 aus.
b) Zeigen Sie, dass die Vereinigung von abzählbar vielen abzählbaren Mengen wieder abzählbar ist.

1.7. Drei grundlegende Beweistechniken

Wir werden drei grundlegende Beweistechniken, die in Beweisen immer wieder ihre Anwendung finden, kennen lernen. Diese sind:

die vollständige Induktion, das Schubfachprinzip und die Diagonalisierung.

1.7.1 Die vollständige Induktion

Die Grundidee der vollständigen Induktion beruht auf dem axiomatischen Aufbau der natürlichen Zahlen nach Peano: Man kann jede natürliche Zahl dadurch erhalten, dass man mit eins beginnend wiederholt eins addiert. D.h., wir können die Menge $\mathbb{N}$ der natürlichen Zahlen wie folgt induktiv definieren:

Sei A eine Menge von natürlichen Zahlen, so dass

i) $1 \in A$ und

ii) für jede natürliche Zahl n impliziert $n \in A$ auch $n+1 \in A$.

Dann gilt $A = \mathbb{N}$.

Obiges Prinzip kann man zum Beweis, dass eine Eigenschaft P für alle $n \in \mathbb{N}$ wahr ist, verwenden. Hierzu wendet man obiges Prinzip auf die Menge

$$A := \{ n \in \mathbb{N} \mid P \text{ ist wahr für } n \}$$

auf folgende Art und Weise an:

1) Induktionsanfang: Zeige $1 \in A$.

2) Induktionsvoraussetzung:
Nehmen wir an, dass $n \in A$, d.h., die Eigenschaft P gilt für n.

3) Induktionsschritt $n \rightsquigarrow n+1$:

Unter Verwendung der Induktionsvoraussetzung beweise, dass die Eigenschaft P auch für $n+1$ gilt.

Dann impliziert das Induktionsprinzip, dass $A = \mathbb{N}$, d.h., die Eigenschaft P gilt für jede natürliche Zahl. n heißt Induktionsvariable oder Induktionsparameter.

Beispiel 1.27

Beh.: Für $n \geq 1$ gilt: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Bew.:

$n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}. \quad \checkmark$$

Annahme:
Die Behauptung gilt für ein $n \geq 1$.
D.h., $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

$n \rightsquigarrow n+1$:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1) \underset{\text{Ind.Vor.}}{=} \frac{n(n+1)}{2} + (n+1)$$

$$= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

Beispiel 1.28

Beh.:
Für jede endliche Menge A gilt

$$|2^A| = 2^{|A|}$$

Bew.:
Wir beweisen die Behauptung mittels vollständiger Induktion über die Elementanzahl $|A|$ von A.

$|A| = 0$:

Dann ist $A = \emptyset$. Wegen $2^A = \{\emptyset\}$ gilt

$$|2^A| = |\{\emptyset\}| = 1.$$

Ferner gilt

$$2^{|A|} = 2^0 = 1. \quad \checkmark$$

Annahme:

$n \geq 0$ und $\forall A$ mit $|A| = n$ gilt

$$|2^A| = 2^{|A|}$$

$n \rightsquigarrow n+1$:

Sei A eine beliebige Menge mit $|A| = n+1$. Wegen $n \geq 0$ enthält A mindestens ein Element a. Sei

$$B := A \setminus \{a\}.$$

Dann gilt $|B| = n$.

Induktionsvoraussetzung $\Rightarrow$

$$|2^B| = 2^{|B|} = 2^n.$$

Betrachte 2^A. Zerlege 2^A wie folgt:

$$A_1 := \{ C \in 2^A \mid a \notin C \}$$

$$A_2 := \{ D \in 2^A \mid a \in D \}$$

A_1 und A_2 sind paarweise disjunkt und $2^A = A_1 \cup A_2$.

$\Rightarrow$

$$|2^A| = |A_1| + |A_2|$$

Wegen $A_1 = 2^B$ gilt

$$|A_1| = 2^n.$$

A_2 kann wie folgt geschrieben werden:

$$A_2 = \{ C \cup \{a\} \mid C \in 2^B \}.$$

Also gilt

$$|A_2| = |2^B| = 2^n.$$

Insgesamt gilt also

$$|2^A| = 2^n + 2^n = 2^{n+1} = 2^{|A|}.$$

■

Wir haben unseren Induktionsanfang für $|A| = 0$ und nicht für $|A| = 1$ bewiesen. Dennoch ist obiger Beweis korrekt.

Im obigen Beweis haben wir der Induktionsvariablen n folgendermaßen, in Abhängigkeit von der Anzahl der Elementen, Mengen zugeordnet:

$1 \;\hat{=}\;$ Menge mit null Elementen.
$2 \;\hat{=}\;$ Mengen mit einem Element
$3 \;\hat{=}\;$ Mengen mit zwei Elementen
$\vdots$
$n \;\hat{=}\;$ Mengen mit $n-1$ Elementen.

Dann haben wir vollständige Induktion über den Induktionsparameter durchgeführt.

Beispiel 1.29

Beh.:
Die Summe der ersten n, $n \geq 1$ ungeraden Zahlen ist gleich n^2.

Bew.:
n gibt uns hier die Anzahl der ersten ungeraden Zahlen, die aufaddiert werden, an.

$n = 1$:

$$1 = 1^2 \qquad \checkmark$$

Annahme:
Sei $n \geq 1$ und $\sum_{i=0}^{n-1} 2i + 1 = n^2$.

$n \rightsquigarrow n+1$:

$$\sum_{i=0}^{n} (2i+1) = \sum_{i=0}^{n-1} (2i+1) + 2n + 1$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2$$

■

Nicht immer ist es im Induktionsschritt einfach, alleine von n auf $n+1$ zu schließen. Betrachtet man den Induktionsschritt genauer, dann sieht man, dass sogar die Gültigkeit der Aussage für alle $\ell \leq n$ vorausgesetzt werden kann. Tut man dies, dann spricht man von der verallgemeinerten vollständigen Induktion.

Beispiel 1.30

Beh.:
Sei $n \geq 2$ eine natürliche Zahl. Dann ist n das Produkt von Primzahlen.

Erinnerung:
$p \in \mathbb{N}$ ist genau dann eine Primzahl, wenn $p \geq 2$ und p nur durch 1 und durch p teilbar ist.

Beweis:

$n = 2$:

2 ist triviales Produkt von sich selbst. Da 2 eine Primzahl ist, folgt damit die Behauptung

Annahme:

Sei $n \geq 2$. Seien alle Zahlen $2 \leq e \leq n$ Produkt von Primzahlen.

$n \rightsquigarrow n+1$:

1. Fall: $n+1$ ist Primzahl.

Dann erfüllt das triviale Produkt, das nur aus dem Faktor $n+1$ besteht, die Behauptung.

2. Fall: $n+1$ ist keine Primzahl.

Dann existieren $2 \leq a, b < n+1$ mit

$$n+1 = a \cdot b$$

Induktionsvoraussetzung $\Rightarrow$

$$a = p_1 \cdot p_2 \cdots p_r \text{ und } b = q_1 \cdot q_2 \cdots q_s,$$

wobei die Faktoren in beiden Produkten nicht notwendigerweise verschiedene Primzahlen sind.

$\Rightarrow$

$$n+1 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

erfüllt die Behauptung.

Beispiel 1.31

Beh.:
Jeder Geldbetrag von mindestens 4 Cents kann mit Zwei- und Fünfcentsstücken bezahlt werden.

Bew.:
Hier müssen wir aufgrund des Induktionsschrittes beim Induktionsanfang etwas aufpassen.

$4 \leq n \leq 6$:

Es gilt: $4 = 2+2$ und $6 = 2+2+2$ ✓

Annahme
$n \geq 6$ und jeder Betrag $4 \leq \ell \leq n$ kann mit Zwei- und Fünfcentsstücken bezahlt werden.

$n \rightsquigarrow n+1$:

Der Betrag $(n+1)-2$ liegt zwischen vier und n und kann somit gemäß Induktionsvoraussetzung mit Zwei- und Fünfcentsstücken bezahlt werden. Fügen wir ein weiteres Zweicentsstück hinzu, dann erhalten wir den Betrag $n+1$.

∎

1.7.2 Das Schubfachprinzip

Schubfachprinzip:
Seien A und B nichtleere endliche Mengen mit $|A| > |B|$. Dann gibt es keine injektive Funktion $f: A \to B$.

Hiervon müssen wir uns überzeugen. Wir interpretieren B als einen Schrank mit $|B|$ Schubfächer und f als eine Methode, die Elemente von A in die Schubfächer des Schrankes platzieren. Wir betrachten die Elemente von A in einer beliebigen, aber festen Ordnung und legen bei Betrachtung des Elements a in das Schubfach $f(a)$. Falls in dem Fach $f(a)$ bereits ein Element liegt, dann ist f nicht injektiv. Spätestens bei Betrachtung des $(|B|+1)$-ten Elements a (welches wegen $|A| > |B|$ existiert) muss sich in Fach $f(a)$ bereits ein Element befinden. Also kann f nicht injektiv sein.

Beim Beweis des folgenden einfachen Satzes verwenden wir das Schubfachprinzip.

Satz 1.8

Sei R eine binäre Relation auf einer endlichen Menge A. Falls in R eine Kette der Länge $|A|+1$ existiert, dann gibt es in R einen Kreis.

Beweis:

Seien $n := |A|+1$ und $(a_1, a_2, \dots, a_n)$ eine Kette in R. Betrachte die Funktion

$$f: \{1,2,\dots,n\} \to A \text{ mit } f(i) = a_i \ \forall i.$$

Schubfachprinzip $\Rightarrow$ f ist nicht injektiv.

Also existieren $1 \leq i < j \leq n$ mit $f(i) = f(j)$.

Betrachte $k > 0$ minimal, so dass $f(m) = f(m+k)$ für ein m, $1 \leq m < n$.

Dann ist $(a_m, a_{m+1}, \dots, a_{m+k-1})$ ein einfacher Kreis.

■

1.7.3 Die Diagonalisierung

Sei R eine binäre Relation auf einer Menge A. Die Diagonalmenge D der Relation R ist definiert durch

$$D := \{a \mid a \in A \text{ und } (a,a) \notin R\}.$$

Für jedes $a \in A$ sei R_a definiert durch

$$R_a := \{ b \mid b \in A \text{ und } (a,b) \in R \}.$$

Dann gilt $D \neq R_a \quad \forall\, a \in A$.

Dies ist der Fall, da $\forall\, a \in A$ gilt:

$$a \in R_a \iff a \notin D.$$

verwenden obiges Diagonalisierungsprinzip beim Beweis des folgenden Satzes.

Satz 1.9

Die Menge $2^{\mathbb{N}}$ ist überabzählbar.

Beweis:

Annahme: $2^{\mathbb{N}}$ ist aufzählbar unendlich.

$\Rightarrow$

$\exists$ Bijektion $f: \mathbb{N} \to 2^{\mathbb{N}}$.

$\Rightarrow$

$2^{\mathbb{N}}$ kann aufgezählt werden durch

$$S_1, S_2, S_3, \ldots,$$

wobei $S_i = f(i)$ für $i \in \mathbb{N}$.

Betrachte folgende Menge

$$D := \{ n \in \mathbb{N} \mid n \notin S_n \}.$$

Da D eine Menge von natürlichen Zahlen ist, gilt $D \in 2^{\mathbb{N}}$.

$\Rightarrow$

$\exists\, k \in \mathbb{N}$ mit $S_k = D$.

Frage: Gilt $k \in S_k$?

Annahme: $k \in S_k$

Definition von $D \Rightarrow k \notin D$.

Wegen $D = S_k$ impliziert dies $k \notin S_k$

Widerspruch

Annahme: $k \notin S_k$

Definition von $D \Rightarrow k \in D$

Wegen $D = S_k$ impliziert dies $k \in S_k$

Widerspruch

Somit führt die Annahme, dass $2^{\mathbb{N}}$ auf-zählbar unendlich ist, in jedem Fall zum Widerspruch

$\Rightarrow$ Diese Annahme ist falsch

$\Rightarrow$ $2^{\mathbb{N}}$ ist überabzählbar. ∎

Frage:
Wie haben wir obiges Diagonalisierungsprinzip im Beweis des Satzes 1.9 verwendet?

Betrachte die Relation

$$R = \{(i,j) \mid j \in f(i)\}.$$

Dann gilt

$$D = \{j \mid j \in \mathbb{N} \text{ und } j \notin f(i)\}$$

Sei

$$R_i := \{j \in \mathbb{N} \mid (i,j) \in R\}.$$

Wegen $S_i = f(i)$ gilt

$$R_i = S_i.$$

Da $D \neq S_i \; \forall \, i$ gilt $D \notin f(\mathbb{N})$.

$\Rightarrow$

f ist keine Bijektion.

2. Einführung in die Logik

Wir haben uns zu Beginn der Vorlesung informell mit Aussagen und einigen Dingen, die man mit solchen tun kann, beschäftigt. Dies war notwendig damit wir die Grundlagen legen und erste Beweise führen konnten. Wir hatten nicht definiert, was wir genau unter einer Aussage verstehen sondern uns auf unsere Intuition verlassen.

Eine Aussage ist ein sprachliches Gebilde, für das genau einer der Wahrheitswerte wahr oder falsch zutrifft. Gemäß dieser Definition gelten für Aussagen folgende grundlegende Prinzipien:

Prinzip der Zweiwertigkeit:
Jede Aussage ist wahr oder falsch.

Prinzip vom ausgeschlossenen Widerspruch:
Es gibt keine Aussage, die sowohl wahr als auch falsch ist.

Beispiel 2.1

"Die Sonne kreist um die Erde."
"Fünf ist eine Primzahl."
"Es gibt unendlich viele Primzahlzwillinge"

(Primzahlen, deren Differenz 2 ist)

sind Aussagen. Die erste ist falsch, die zweite ist wahr und der Wahrheitswert der dritten Aussage ist unbekannt.

"Heute ist schönes Wetter."
"x ist eine Primzahl."

sind keine Aussagen. Aufgrund des subjektiven Begriffes "schön" kann der Wahrheitswert des ersten Satzes nicht angegeben werden. Der Wahrheitswert des zweiten Satzes hängt von dem

Wert ab, den x annimmt.

Folgender Satz ist weder wahr noch falsch und somit keine Aussage.

"Dieser Satz ist falsch."

Angenommen, der Satz wäre wahr, dann müsste er falsch sein. Wenn wir davon ausgehen, dass der Satz falsch ist, dann müsste er wahr sein. (Paradoxon von Bertrand Russell).

Setzen wir mehrere Aussagen zu einer Aussage zusammen, dann hängt der Wahrheitswert der zusammengesetzten Aussage nur von den Wahrheitswerten der einzelnen Aussagen und nicht von etwaigen Sinnmöglichkeiten der Zusammensetzung ab.

Beispiel 2.2

"Wenn es eine ganze Zahl y mit $x = y+1$ für alle ganze Zahlen x gibt, dann gilt $w = z$ für alle ganze Zahlen w und z."

Wie wir bereits wissen, ist obige Aussage wahr, auch wenn diese trivial ist und völlig unsinnig aussieht.

Ziel:

Untersuchung, wie sich der Wahrheitswert von zusammengesetzten Aussagen aus den Wahrheitswerten der einzelnen Aussagen ergibt.

Zunächst werden wir uns in der sogenannten Aussagenlogik mit Aussagen, die sich aus elementaren Aussagen mit Hilfe der einfachen logischen Operationen "und", "oder" und "nicht" zusammensetzen lassen, beschäftigen. In der Aussagenlogik können eine Vielzahl von interessanten Aussagen nicht formuliert werden. Hierzu benötigt man zusätzlich sogenannte Prädikate und Quantoren. Fügt man diese zu den Operationen der Aussagenlogik hinzu, dann erhält man die sogenannte Prädikatenlogik. Mit dieser werden wir uns im Anschluss an die Aussagenlogik beschäftigen.

2.1 Die Aussagenlogik

2.1.1 Aussagenlogische Ausdrücke

Zunächst werden wir definieren, was wir unter einem aussagenlogischen Ausdruck verstehen.

Sei $X := \{x_1, x_2, \dots\}$ eine abzählbar (unendliche) Menge von Boole'schen Variablen. Dies sind Variablen, die die beiden Werte wahr und falsch annehmen können. Wir kombinieren Boole'sche Variablen

unter Verwendung der Boole'schen Operationen $\wedge$ (logisches und), $\vee$ (logisches oder) und $\neg$ (logisches nicht).

Ein aussagenlogischer Ausdruck ist

i) eine Boole'sche Variable $x_i \in X$ oder
ii) ein Ausdruck der Form $\neg \phi_1$, wobei ϕ_1 ein Boole'scher Ausdruck ist, oder
iii) ein Ausdruck der Form $(\phi_1 \wedge \phi_2)$, wobei ϕ_1 und ϕ_2 Boole'sche Ausdrücke sind, oder
iv) ein Ausdruck der Form $(\phi_1 \vee \phi_2)$, wobei ϕ_1 und ϕ_2 Boole'sche Ausdrücke sind.

Dies sind alle aussagenlogische Ausdrücke.

$\neg \phi_1$ heißt Negation von ϕ_1. Der Ausdruck $(\phi_1 \wedge \phi_2)$ ist die Konjunktion von ϕ_1 und ϕ_2. $(\phi_1 \vee \phi_2)$ ist die Disjunktion von ϕ_1 und ϕ_2. Ein Ausdruck der Form x_i oder $\neg x_i$ heißt Literal.

Was wir definiert haben ist die Syntax von aussagenlogischen Ausdrücken. Was einem Ausdruck Leben gibt ist seine Semantik. Die Semantik von aussagelogischen Ausdrücken ist relativ einfach. In Abhängigkeit der Wahrheitswerte der enthaltenen Variablen kann ein Ausdruck wahr oder falsch sein.

Wir haben aussagenlogische Ausdrücke induktiv definiert. Beginnend mit Variablen setzen wir diese unter Verwendung von Boole'schen Operationen zu komplizierteren Ausdrücken zusammen. Demzufolge werden unsere Definitionen von Eigenschaften von aussagelogischen Ausdrücken denselben induktiven Pfad der ursprünglichen Definition folgen. Auch werden wir bei unseren Beweisen <u>Induktion über die Struktur der Ausdrücke</u> verwenden.

Eine <u>Belegung</u> $\mathcal{B}$ ist eine Abbildung

$$\mathcal{B} : X' \longrightarrow \{\text{wahr}, \text{falsch}\},$$

die einer endlichen Menge $X' \subset X$ von Variablen jeweils einen Wahrheitswert zuordnet.

Sei ϕ ein aussagelogischer Ausdruck. Dann definieren wir wir wie folgt die Menge $X(\phi)$ von Boole'schen Variablen, die in ϕ vorkommt:

i) Falls $\phi = x_i \in X$, dann ist $X(\phi) := \{x_i\}$.
ii) Falls $\phi = \neg \phi_1$, dann $X(\phi) := X(\phi_1)$.
iii) Falls $\phi = (\phi_1 \wedge \phi_2)$ oder $\phi = (\phi_1 \vee \phi_2)$, dann $X(\phi) := X(\phi_1) \cup X(\phi_2)$.

Sei $\mathcal{B} : X' \longrightarrow \{\text{wahr}, \text{falsch}\}$ eine Belegung mit $X(\phi) \subseteq X'$. Dann heißt $\mathcal{B}$ <u>geeignet für</u> ϕ. Wir definieren nun induktiv, wann eine für ϕ geeignete Belegung $\mathcal{B}$ den Ausdruck ϕ <u>erfüllt</u>.

Wir schreiben dann $\mathcal{B} \models \phi$. Falls $\mathcal{B}$ den Ausdruck ϕ nicht erfüllt, dann schreiben wir $\mathcal{B} \not\models \phi$.

i) Falls $\phi = x_i \in \mathcal{B}(\phi)$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B}(x_i) =$ wahr.

ii) Falls $\phi = \neg \phi_1$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B} \not\models \phi_1$.

iii) Falls $\phi = (\phi_1 \wedge \phi_2)$, dann

$\mathcal{B} \models \phi$, falls sowohl $\mathcal{B} \models \phi_1$, als auch $\mathcal{B} \models \phi_2$.

iv) Falls $\phi = (\phi_1 \vee \phi_2)$, dann

$\mathcal{B} \models \phi$, falls $\mathcal{B} \models \phi_1$ oder $\mathcal{B} \models \phi_2$.

<u>Beispiel 2.3</u>

Betrachte $\phi := ((\neg x_1 \vee x_2) \wedge x_3)$ und die geeignete Belegung $\mathcal{B}$ mit

$\mathcal{B}(x_1) = \mathcal{B}(x_3) =$ wahr und $\mathcal{B}(x_2) =$ falsch.

<u>Frage:</u> Erfüllt $\mathcal{B}$ den Ausdruck ϕ?

Es gilt:

$\mathcal{B} \models x_1 \Rightarrow \mathcal{B} \not\models \neg x_1$ und $\mathcal{B} \not\models x_2$

$\Rightarrow \mathcal{B} \not\models (\neg x_1 \vee x_2) \Rightarrow \mathcal{B} \not\models \phi$

Wir verwenden zwei weitere Boole'sche Operationen:

$(\phi_1 \to \phi_2)$ für $(\neg \phi_1 \vee \phi_2)$

$(\phi_1 \leftrightarrow \phi_2)$ für $(\phi_1 \to \phi_2) \wedge (\phi_2 \to \phi_1)$

Zwei Ausdrücke ϕ_1 und ϕ_2 heißen äquivalent, falls für jede Belegung $\mathcal{B}$ mit $\mathcal{B}$ ist für ϕ_1 und für ϕ_2 geeignet, gilt:

$$\mathcal{B} \models \phi_1 \iff \mathcal{B} \models \phi_2.$$

Wir schreiben dann $\phi_1 \equiv \phi_2$.

Übung:
Beweisen Sie, dass die Relation $\equiv$ eine Äquivalenzrelation ist.

Lemma 2.1
Seien ϕ_1, ϕ_2 und ϕ_3 beliebige aussagenlogische Ausdrücke. Dann gilt

Idempotenz: $(\phi_1 \vee \phi_1) \equiv \phi_1$
$(\phi_1 \wedge \phi_1) \equiv \phi_1$

Kommutativität: $(\phi_1 \vee \phi_2) \equiv (\phi_1 \vee \phi_1)$
$(\phi_1 \wedge \phi_2) \equiv (\phi_2 \wedge \phi_1)$
$(\phi_1 \leftrightarrow \phi_2) \equiv (\phi_2 \leftrightarrow \phi_1)$

Assoziativität: $((\phi_1 \vee \phi_2) \vee \phi_3) \equiv (\phi_1 \vee (\phi_2 \vee \phi_3))$
$((\phi_1 \wedge \phi_2) \wedge \phi_3) \equiv (\phi_1 \wedge (\phi_2 \wedge \phi_3))$

Absorption: $(\Phi_1 \vee (\Phi_1 \wedge \Phi_2)) \equiv \Phi_1$
$(\Phi_1 \wedge (\Phi_1 \vee \Phi_2)) \equiv \Phi_1$

Distributivität: $(\Phi_1 \wedge (\Phi_2 \vee \Phi_3)) \equiv ((\Phi_1 \wedge \Phi_2) \vee (\Phi_1 \wedge \Phi_3$
$(\Phi_1 \vee (\Phi_2 \wedge \Phi_3)) \equiv ((\Phi_1 \vee \Phi_2) \wedge (\Phi_1 \vee \Phi_3$

Doppelte Negation: $\neg\neg\Phi_1 \equiv \Phi_1$

DeMorgan $\neg(\Phi_1 \vee \Phi_2) \equiv (\neg\Phi_1 \wedge \neg\Phi_2)$
$\neg(\Phi_1 \wedge \Phi_2) \equiv (\neg\Phi_1 \vee \neg\Phi_2)$

Beweis: Übung ■

Lemma 2.1 ermöglicht uns die Vereinfachung der Notation zur Repräsentation von aussagelogischen Ausdrücken. So vermeiden wir Klammern, wenn diese binäre Operationen ($\wedge$ oder $\vee$) derselben Art separieren.

Beispiel 2.4

Anstatt
$$(((x_1 \vee \neg x_3) \vee x_2) \vee (x_4 \vee (x_2 \vee x_5)))$$
schreiben wir
$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_2 \vee x_5)$$

◊

Dies bedeutet, dass wir "lange" Disjunktionen und Konjunktionen erlauben. Mittels Verwendung der Kommunität und Itempotenz können

wir dafür sorgen, dass lange Disjunktionen und lange Konjunktionen nur verschiedene Ausdrücke enthalten.

Beispiel 2.4 (Fortführung)

Anstatt

$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_2 \vee x_5)$$

schreiben wir

$$(x_1 \vee \neg x_3 \vee x_2 \vee x_4 \vee x_5).$$

♦

Des Weiteren verwenden wir folgende Schreibweisen:

$\bigwedge_{i=1}^{n} \varphi_i$ steht für $(\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n)$.

$\bigvee_{i=1}^{n} \varphi_i$ steht für $(\varphi_1 \vee \varphi_2 \vee \dots \vee \varphi_n)$.

Als nächstes werden wir zeigen, dass jeder aussagenlogischer Ausdruck φ in einen äquivalenten Ausdruck, der eine spezielle Form hat, transformiert werden kann.

Ein aussagenlogischer Ausdruck φ ist in konjunktiver Normalform (KNF), falls

$$\varphi = \bigwedge_{i=1}^{n} C_i,$$

wobei $n \geq 1$ und jedes C_i ist die Disjunktion von einem oder mehreren Literalen.

Φ ist in <u>disjunktiver Normalform</u> (DNF), falls

$$\Phi = \bigvee_{i=1}^{n} D_i ,$$

wobei $n \geq 1$ und jedes D_j ist die Konjunktion von einem oder mehreren Literalen. Die D_j's heißen <u>Implikanten</u> des Ausdrucks in DNF.

<u>Satz 2.1</u>

Jeder aussagenlogischer Ausdruck Φ ist äquivalent zu einem Ausdruck in KNF und zu einem Ausdruck in DNF.

<u>Beweis</u>:

Wir beweisen den Satz mittels Induktion über die Struktur von Φ.

<u>$\Phi = x_j \in X$</u>:

Φ ist eine einzelne Variable. Dann folgt aus der Definition von KNF und von DNF, dass Φ sowohl in KNF als auch in DNF bereits ist.

<u>Annahme</u>:

Φ_1 und Φ_2 sind aussagelogische Ausdrücke, zu den äquivalente Ausdrücke Φ_1' und Φ_2' in KNF sowie äquivalente Ausdrücke Φ_1'' und Φ_2'' in DNF existieren

Wir beweisen nun nacheinander, dass dann auch äquivalente Ausdrücke in KNF bzw DNF für

$\neg \phi_1$, $\phi_1 \vee \phi_2$ und $\phi_1 \wedge \phi_2$ existieren.

$\underline{\phi = \neg \phi_1}$:

Seien

$$\phi_1' := \bigwedge_{i=1}^{n} C_i \quad \text{und} \quad \phi_1'' := \bigvee_{i=1}^{m} D_i.$$

Dann gilt:

$$\neg \phi_1 \equiv \neg \phi_1' = \neg \left(\bigwedge_{i=1}^{n} C_i \right)$$

$$\overset{\text{DeM.}}{=} \bigvee_{i=1}^{n} \neg C_i$$

$$\overset{\text{DeM}}{=} \bigvee_{i=1}^{n} \tilde{D}_i,$$

wobei $\tilde{D}_i$ mittels Anwendung von DeMorgan auf $\neg C_i$ entsteht.

$\Rightarrow$

$\tilde{D}_i$ ist die Konjunktion der negierten Literalen in C_i.

$\Rightarrow \bigvee_{i=1}^{n} \tilde{D}_i$ ist in DNF.

Analog konstruiert man aus $\neg \phi''$ einen zu $\neg \phi_1$ äquivalenten Ausdruck in KNF.

Übung.

$\underline{\phi = (\phi_1 \vee \phi_2)}$:

Da $\phi_1'' \vee \phi_2''$ bereits in DNF ist, ist die Konstruktion des zu ϕ äquivalenten Ausdrucks

in DNF trivial.

Für die Konstruktion des zu Φ äquivalenten Ausdrucks in KNF betrachten wir $(\Phi_1' \vee \Phi_2')$.
Seien

$$\Phi_1' := \left(\bigwedge_{i=1}^{n} C_{1i}\right) \text{ und } \Phi_2' := \left(\bigwedge_{j=1}^{m} C_{2j}\right).$$

Dann gilt

$$\begin{aligned}
(\Phi_1' \vee \Phi_2') &= \left(\bigwedge_{i=1}^{n} C_{1i} \vee \bigwedge_{j=1}^{m} C_{2j}\right) \\
&\underset{\text{Dis}}{=} \left(\bigwedge_{j=1}^{m} \left(\left(\bigwedge_{i=1}^{n} C_{1i}\right) \vee C_{2j}\right)\right) \\
&\underset{\text{Dis}}{=} \left(\bigwedge_{j=1}^{m} \left(\bigwedge_{i=1}^{n} (C_{1i} \vee C_{2j})\right)\right) \\
&= \bigwedge_{j=1}^{m} \bigwedge_{i=1}^{n} (C_{1i} \vee C_{2j}) \\
&\qquad \uparrow \text{ KNF } \checkmark
\end{aligned}$$

$\underline{\Phi = (\Phi_1 \wedge \Phi_2)}$: analog (Übung)

Übung:

Vervollständigen Sie den Beweis von Satz 2.1.

2.1.2 Erfüllbarkeit und Gültigkeit

Ein aussagelogischer Ausdruck ϕ heißt erfüllbar, falls eine für ϕ geeignete Belegung $\mathcal{B}$ mit $\mathcal{B} \models \phi$ existiert. Andernfalls heißt ϕ nicht erfüllbar oder unerfüllbar. Ein Ausdruck ϕ heißt gültig oder eine Tautologie, falls $\mathcal{B} \models \phi$ für alle für ϕ geeignete Belegungen $\mathcal{B}$. Wir schreiben dann auch $\models \phi$. Falls ein Ausdruck ϕ unerfüllbar ist, dann gilt $\mathcal{B} \not\models \phi$ und somit $\mathcal{B} \models \neg\phi$ für alle für ϕ geeignete Belegungen $\mathcal{B}$. Also gilt

Lemma 2.2
Ein aussagelogischer Ausdruck ϕ ist genau dann unerfüllbar, wenn seine Negation $\neg\phi$ gültig ist.

Sei ϕ ein aussagelogischer Ausdruck und

$$X_n := \{x_1, x_2, \ldots, x_n\}$$

die Menge der Variablen, von denen ϕ abhängt.

Frage:
Wie können wir testen, ob ϕ erfüllbar ist oder nicht?

Idee:
Bestimme für jede Belegung von X_n den Wahrheitswert, den diese Belegung für Φ induziert.

Jede Variable $x_i \in X_n$ kann den Wert wahr oder den Wert falsch annehmen.
$\Rightarrow$
Es existieren 2^n verschiedene Belegungen von X_n.

Insbesondere, wenn Φ unerfüllbar ist, würde jede der 2^n Belegungen überprüft werden.
$\Rightarrow$
Bereits für relativ kleine n verbietet sich diese Vorgehensweise.

Ziel:
Entwicklung einer Methode, die in der Praxis "häufig schneller" feststellt, dass ein gegebener Ausdruck Φ nicht erfüllbar ist.

Zunächst benötigen wir einige Bezeichnungen.

Eine Klausel K ist eine endliche, möglicherweise leere Menge von Literalen. Jede Disjunktion C von Literalen korrespondiert zur Klausel

$$K_C := \{ y \mid y \text{ ist Literal in } C \}.$$

Umgekehrt korrespondiert jede nichtleere Klausel K zur folgenden Disjunktion C_K von Literalen:

$$C_K := \bigvee_{y \in K} y.$$

Wir schreiben $\square$ für die leere Klausel, die zu keinem Ausdruck korrespondiert.

Jede endliche nichtleere Menge $\mathcal{K} := \{K_1, K_2, \dots, K_s\}$ von Klauseln mit $\square \notin \mathcal{K}$ korrespondiert zum folgenden Ausdruck $\Phi_{\mathcal{K}}$ in konjunktiver Normalform.

$$\Phi_{\mathcal{K}} := \bigwedge_{i=1}^{s} C_{K_i}.$$

$\mathcal{K}$ heißt auch eine Klauselmenge.

Zu einem Ausdruck

$$\Phi = \bigwedge_{i=1}^{t} C_i$$

korrespondiert die Klauselmenge

$$\mathcal{K}_\Phi := \{K_{C_1}, K_{C_2}, \dots, K_{C_t}\}.$$

Seien K_1, K_2 und D Klauseln. Die Klausel D heißt genau dann Resolvente von K_1 und K_2, wenn es ein Literal y gibt mit

i) $y \in K_1$, $\neg y \in K_2$ und
ii) $D = (K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$.

Wir sagen, zwei Klauselmengen $\mathcal{K}_1$ und $\mathcal{K}_2$ sind äquivalent wenn die korrespondierenden Ausdrücke $\Phi_{\mathcal{K}_1}$ und $\Phi_{\mathcal{K}_2}$ äquivalent sind. Eine Klauselmenge $\mathcal{K}$ heißt genau dann erfüllbar, wenn $\Phi_{\mathcal{K}}$ erfüllbar ist.

Lemma 2.3 (Resolutionsregel)

Seien $\mathcal{K}$ eine Klauselmenge, $K_1, K_2 \in \mathcal{K}$ und D eine Resolvente von K_1 und K_2. Dann sind $\mathcal{K}$ und $\mathcal{K}' := \mathcal{K} \cup D$ äquivalent.

Beweis:

Sei $\mathcal{B}$ eine für $\Phi_{\mathcal{K}}$ geeignete Belegung. Offensichtlich gilt:

$$\mathcal{B} \models \Phi_{\mathcal{K}'} \Rightarrow \mathcal{B} \models \Phi_{\mathcal{K}}.$$

Annahme:

$$\mathcal{B} \models \Phi_{\mathcal{K}} \text{ und } D = (K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$$

zu zeigen: $\mathcal{B} \models \Phi_D$

Da $\mathcal{B}$ nicht gleichzeitig y und $\neg y$ erfüllen kann muss $\mathcal{B}$ mindestens ein Literal in $(K_1 \setminus \{y\}) \cup (K_2 \setminus \{\neg y\})$ erfüllen. Also gilt

$$\mathcal{B} \models \Phi_D.$$

∎

Die Resolutionsregel besagt, dass das Hinzufügen der Resolventen zweier Klauseln der betrachteten Klauselmenge zu einer äquivalenten Klauselmenge führt.

Übung:

Zeigen Sie, dass die Klauseln, mittels denen die Resolvente gebildet wurde, nicht aus der Klausel-

menge entfernt werden dürfen, da dann die resultierende Klauselmenge nicht mehr äquivalent zur ursprünglichen Klauselmenge sein muss.

Sei $\mathcal{K}$ eine Klauselmenge. Die Operation R ist dann definiert durch.

$$R(\mathcal{K}) := \mathcal{K} \cup \{D \mid D \text{ ist eine Resolvente in } \mathcal{K}\}.$$

D.h., R fügt zu $\mathcal{K}$ alle Resolventen von Klauseln aus $\mathcal{K}$ hinzu. Aus obiger Resolutionsregel folgt, dass $\mathcal{K}$ und $R(\mathcal{K})$ äquivalent sind.

Seien nun

$$R^0(\mathcal{K}) := \mathcal{K}$$
$$R^{i+1}(\mathcal{K}) := R(R^i(\mathcal{K})) \quad \text{für } i \geq 0$$
$$R^*(\mathcal{K}) := \bigcup_{i \geq 0} R^i(\mathcal{K}).$$

D.h., $R^*(\mathcal{K})$ ist der Abschluss von $\mathcal{K}$ unter der Operation R.

Bemerkung:
Falls $\mathcal{K}$ endlich ist, dann können von $\mathcal{K}$ ausgehend nur endlich viele unterschiedliche Klauseln konstruiert werden. Also existiert ein $n \geq 0$, so dass $R^{n+1}(\mathcal{K}) = R^n(\mathcal{K})$, womit $R^*(\mathcal{K}) = R^n(\mathcal{K})$.

Satz 2.2 (Resolutionssatz)

Eine Klauselmenge $\mathcal{K}$ ist genau dann unerfüllbar, wenn $\square \in R^*(\mathcal{K})$.

Beweis:

„$\Leftarrow$"

Annahme: $\square \in R^*(\mathcal{K})$

Wegen $\square \notin \mathcal{K}$ existiert ein $k \geq 1$ mit

i) $\square \notin R^{(k-1)}(\mathcal{K})$ und
ii) $\square \in R^{k}(\mathcal{K})$.

$\Rightarrow$ $\square$ ist Resolvente zweier Klauseln K_1 und K_2 aus $R^{(k-1)}(\mathcal{K})$.

$\Rightarrow$ $\exists$ Literal y mit

$$K_1 = y \text{ und } K_2 = \neg y$$

$\Rightarrow$

Der zu $R^{(k-1)}(\mathcal{K})$ korrespondierende Ausdruck ist nicht erfüllbar.

$\Rightarrow$ $\mathcal{K}$ ist unerfüllbar.

„$\Rightarrow$"

Annahme: $\mathcal{K}$ ist unerfüllbar.

Zu zeigen: $\square \in R^*(\mathcal{K})$.

Wir beweisen dies durch vollständige Induktion über die Anzahl n von unterschiedlichen Variablen in $\mathcal{K}$.

$\underline{n=1}$:

Sei x_1 diejenige Variable, die in $\mathcal{K}$ vorkommt. Dann sind

$$K_1 := \{x_1\}, \quad K_2 := \{\neg x_1\}, \quad K_3 = \{x_1, \neg x_1\}$$

die einzigen möglichen nichtleeren Klauseln in $\mathcal{K}$.

Da $\phi_{\mathcal{K}}$ unerfüllbar, muss $\mathcal{K}$ die Klauseln K_1 und K_2 enthalten. Da $\square$ die Resolvente von K_1 und K_2 ist, enthält $R^*(\mathcal{K})$ die leere Klausel $\square$.

$\underline{\text{Annahme}}$:

$n \geq 1$ und die Behauptung ist wahr für Klauselmengen, die n unterschiedliche Variablen enthalten.

$\underline{n \rightsquigarrow n+1}$:

Sei $\mathcal{K}$ eine Menge von nichtleeren Klauseln, in denen die Variablen $x_1, x_2, \ldots, x_{n+1}$ vorkommen, so dass $\phi_{\mathcal{K}}$ unerfüllbar.

Wir konstruieren zwei Klauselmengen $\mathcal{K}^+$ und $\mathcal{K}^-$, in denen x_{n+1} nicht vorkommt, durch:

Wir erhalten $\mathcal{K}^+$ aus $\mathcal{K}$, indem wir alle Klauseln, die das Literal x_{n+1} enthalten,