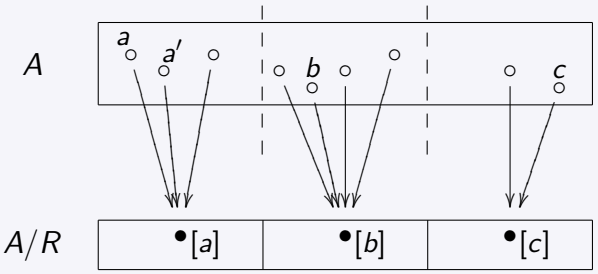
Äquivalenzklassen:

für Äquivalenzrelation $R \subseteq A^2$ auf A, $a \in A$:

$$[a]_R := \{b \in A \colon aRb\}$$
die **Äquivalenzklasse von a**

wichtig: A wird durch die Äquivalenzklassen in disjunkte Teilmengen zerlegt (Lemma 1.1.8), sodass

aRb gdw $[a]_R = [b]_R$



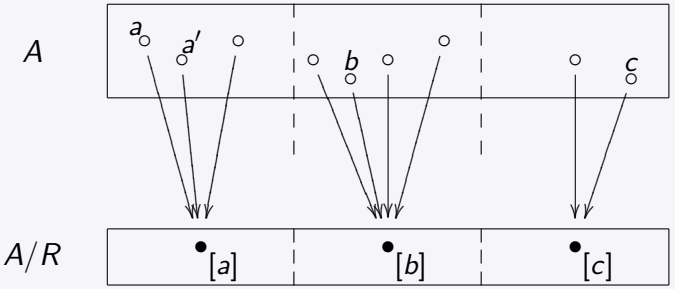
Äquivalenzrelationen: Quotient, natürliche Projektion

Quotient A/R : die Menge aller Äquivalenzklassen von R,

$$A/R := \{[a]_R \colon a \in A\}$$

die **natürliche Projektion**
$$\begin{array}{rcl} \pi_R \colon A & \longrightarrow & A/R \\ a & \longmapsto & [a]_R = \{b \in A \colon aRb\} \end{array}$$

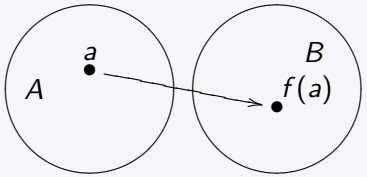
ordnet jedem Element seine Äquivalenzklasse zu



Funktionen und Operationen

→ Abschnitt 1.1.3

Funktion f von A nach B:
$$\begin{array}{rcl} f \colon A & \longrightarrow & B \\ a & \longmapsto & f(a) \end{array}$$



$f(a)$ ist das *Bild von* a unter f;
a ein *Urbild* von $b = f(a)$.

wesentlich: eindeutig definierter Funktionswert $f(a) \in B$ für jedes $a \in A$

A: **Definitionsbereich**

B: **Zielbereich**

$f(a)$ **Bild** von a unter f.

$f[A] := \{f(a) \colon a \in A\} \subseteq B$ **Bild(menge)** von f.

Funktionen, Operationen, Beispiele

n-stellige Funktion auf A: Funktion $f \colon A^n \to B$.

n-stellige Operation auf A: Funktion $f \colon A^n \to A$.

Beispiele: Addition, Multiplikation auf $\mathbb{N}$, $\mathbb{Z}$, ...

Beispiel **Konkatenation** auf Σ^*:
$$\begin{array}{rcl} \cdot \colon \Sigma^* \times \Sigma^* & \longrightarrow & \Sigma^* \\ (u, v) & \longmapsto & u \cdot v \ (= uv). \end{array}$$

Für $u = a_1 \dots a_n$; $v = b_1 \dots b_m$ ist $uv := \underbrace{a_1 \dots a_n}_{u} \underbrace{b_1 \dots b_m}_{v}$

Eigenschaften von zweistelligen Operationen

für 2-stellige Operation $*\colon A \times A \longrightarrow A$
$a, b \longmapsto a * b$ (infixe Notation)

assoziativ, falls für alle $a, b, c \in A$: $(a * b) * c = a * (b * c)$.

kommutativ, falls für alle $a, b \in A$: $a * b = b * a$.

neutrales Element: $e \in A$ neutrales Element für $*$
gdw für alle $a \in A$: $a * e = e * a = a$.

inverse Elemente (bzgl. $*$ mit neutralem Element e):
$a' \in A$ inverses Element zu $a \in A$, falls
$a * a' = a' * a = e$.

Beispiel Konkatenation: assoziativ, neutrales Element ε,
$w \neq \varepsilon$ hat kein inverses Element

(algebraische) Strukturen

→ Abschnitt 1.1.4

Struktur =

Trägermenge mit ausgezeichneten { **Konstanten**, **Operationen**, **Relationen**

typische Beispiele:

- **Standardstrukturen der Algebra**
  $(\mathbb{N}, +, 0)$, $(\mathbb{N}, +, \cdot, <, 0, 1)$, $(\mathbb{Z}, +, \cdot, 0, 1)$, ...
- **Graphen (Transitionssysteme)**
- **Wortmonoide**
- **Boolesche Algebren**
- später: Wortstrukturen, relationale Datenbanken, u.v.a.m.

Strukturtypen: Beispiele

Graphen (Transitionssysteme) als relationale Strukturen

(V, E) mit Knotenmenge V, Kantenrelation E
$E \subseteq V \times V$ eine 2-stellige Relation
$(a, b) \in E$ zu deuten als $a \xrightarrow{E} b$

Monoide als algebraische Strukturen

Monoid: assoziative 2-stellige Operation mit neutralem Element

Beispiel Wort-Monoid

das Wort-Monoid $(\Sigma^*, \cdot, \varepsilon)$ über Σ
$\cdot$, Konkatenation, als 2-stellige Operation
ε, das leere Wort, als Konstante

Beispiel: Boolesche Algebren

Axiome für Boolesche Algebra $(B, \cdot, +, ', 0, 1)$:

BA1: $+$ und $\cdot$ assoziativ und kommutativ.
Für alle x, y, z: $(x + y) + z = x + (y + z)$ $\quad x + y = y + x$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\quad x \cdot y = y \cdot x$

BA2: $+$ und $\cdot$ distributiv.
Für alle x, y, z: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
$x + (y \cdot z) = (x + y) \cdot (x + z)$

BA3: 0 und 1 als neutrale Elemente.
Für alle x: $x \cdot 1 = x$ $\quad x + 0 = x$

BA4: Komplement.
$0 \neq 1$ und für alle x: $x \cdot x' = 0$ $\quad x + x' = 1$

Beispiele: $(\mathcal{P}(M), \cap, \cup, ^-, \emptyset, M)$ für $M \neq \emptyset$; $(\mathbb{B}, \wedge, \vee, \neg, 0, 1)$

Homomorphismen → Abschnitt 1.1.5

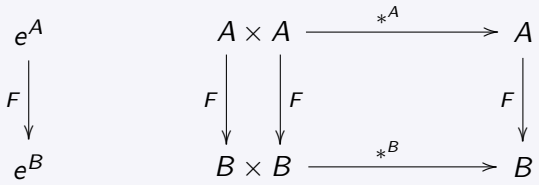
strukturerhaltende Abbildungen zw. Strukturen desselben Typs

z.B. für Strukturen $(A, *^A, e^A)$ und $(B, *^B, e^B)$
mit einer zweistelligen Operation $*$ und einer Konstanten e

$$\left.\begin{array}{rcl} F\colon A & \longrightarrow & B \\ a & \longmapsto & f(a) \end{array}\right\}$$ **Homomorphismus**, falls

(i) $F(e^A) = e^B$ (verträglich mit Konstante e)

(ii) $F(a_1 *^A a_2) = F(a_1) *^B F(a_2)$ (verträglich mit Operation $*$)



Homomorphismen: Beispiele

(1) $$\begin{array}{rcl} h\colon \Sigma^* & \longrightarrow & \mathbb{N} \\ w & \longmapsto & |w| \end{array}$$

Homomorphismus von $(\Sigma^*, \cdot, \varepsilon)$ nach $(\mathbb{N}, +, 0)$.

(2) $$\begin{array}{rcl} \hat{f}\colon \Sigma_1^* & \longrightarrow & \Sigma_2^* \\ w = a_1 \dots a_n & \longmapsto & a_1' \dots a_n' \end{array}$$

wobei $a_i' = f(a_i)$ für eine vorgeg. Funktion $f\colon \Sigma_1 \to \Sigma_2$

Homomorphismus von $(\Sigma_1^*, \cdot, \varepsilon)$ nach $(\Sigma_2^*, \cdot, \varepsilon)$.

(3) analog zu (2), zu $f\colon \Sigma_1 \to \Sigma_2^*$:
ersetze $a \in \Sigma_1$ durch ein Wort $f(a) \in \Sigma_2^*$.

Bemerkung: $\hat{f}$ in (2) und (3) eindeutig bestimmt durch f und die Forderung, dass $\hat{f}\colon (\Sigma_1^*, \cdot, \varepsilon) \stackrel{\text{hom}}{\longrightarrow} (\Sigma_2^*, \cdot, \varepsilon)$
und dass $\hat{f}$ Fortsetzung von f ist: $\hat{f}(a) := f(a)$ f.a. $a \in \Sigma_1$.

Isomorphie – Isomorphismen

Isomorphismus: bijektiver Homomorphismus, dessen Umkehrung auch ein Homomorphismus ist.

Beispiel

Für eine Bijektion $$\begin{array}{rcl} f\colon \Sigma_1 & \longrightarrow & \Sigma_2 \\ a & \longmapsto & f(a) =: a' \end{array}$$

ist $$\begin{array}{rcl} \hat{f}\colon \Sigma_1^* & \longrightarrow & \Sigma_2^* \\ w = a_1 \dots a_n & \longmapsto & a_1' \dots a_n' \end{array}$$

ein Isomorphismus zwischen $(\Sigma_1^*, \cdot, \varepsilon)$ und $(\Sigma_2^*, \cdot, \varepsilon)$.

Schreibweise: $\hat{f}\colon (\Sigma_1^*, \cdot, \varepsilon) \simeq (\Sigma_2^*, \cdot, \varepsilon)$

Beobachtung: $(\Sigma_1^*, \cdot, \varepsilon) \simeq (\Sigma_2^*, \cdot, \varepsilon)$ gdw. $|\Sigma_1| = |\Sigma_2|$

elementare Beweistechniken → Abschnitt 1.2

teilweise Vorgriff auf Teil II (Logik)

primäres Anliegen hier:

- normierte Verknüpfung von Aussagen, Aussagenlogik (AL)
- mathematische Präzision für Quantoren, Quantorenlogik
- Beweistechniken/-muster, insbesondere: Induktionsbeweise

Präzision des Ausdrucks / Strenge des Argumentierens
mathematische Grunddisziplin für den Werkzeugkasten

aussagenlogische Junktoren → Abschnitt 1.2.1

normierte Wahrheitswerte für aussagenlogische Operationen

Wahheitswerte (wahr bzw. falsch; 1 bzw. 0) zusammengesetzter Aussagen als Funktion der Wahrheitswerte der Teilaussagen

und $\wedge : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$\wedge$	0	1
0	0	0
1	0	1

oder $\vee : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$\vee$	0	1
0	0	1
1	1	1

Negation $\neg : \mathbb{B} \to \mathbb{B}$

	0	1
$\neg$	1	0

vgl. Boolesche Algebra $(\mathbb{B}, \wedge, \vee, \neg, 0, 1)$

weitere aussagenlogische Verknüpfungen

abgeleitete Junktoren , z.B.

Implikation $\to : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$\to$	0	1
0	**1**	1
1	0	1

Biimplikation $\leftrightarrow : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$\leftrightarrow$	0	1
0	1	0
1	0	1

sodass $(p \to q) \equiv (\neg p) \vee q$

$(p \leftrightarrow q) \equiv (p \wedge q) \vee ((\neg p) \wedge (\neg q))$

$\equiv (p \to q) \wedge (q \to p)$

aussagenlogische Äquivalenzen und Schlussregeln

Kontraposition: $(p \to q) \equiv ((\neg q) \to (\neg p))$

- beweise "$A \Rightarrow B$" über "$\neg B \Rightarrow \neg A$"

Indirekter Beweis/Widerspruchsbeweis: $p \equiv (\neg p \to 0)$

- beweise "A" über "$(\neg A)$ unmöglich"

Biimplikation/Äquivalenz: $(p \leftrightarrow q) \equiv \big((p \to q) \wedge (q \to p)\big)$

- beweise "$A \Leftrightarrow B$" über "$A \Rightarrow B$ und $B \Rightarrow A$"

Implikationsketten:

- beweise "$A \Rightarrow B$" z.B. über "$A \Rightarrow C$ und $C \Rightarrow B$" (Zwischenbehauptungen)

Quantoren: All- und Existenzaussagen → Abschnitt 1.2.2

$(\forall n \in \mathbb{N}) A(n)$ für die **Allaussage** "für alle $n \in \mathbb{N}$ gilt $A(n)$"

$(\exists n \in \mathbb{N}) A(n)$ für die **Existenzaussage** "$A(n)$ gilt für mindestens ein $n \in \mathbb{N}$"

Negationen von Allaussagen sind äquivalent zu Existenzaussagen und umgekehrt.

Beispiel

¬("alle Schnurze beissen") ≡ "es gibt mindestens einen Schnurz, der nicht beisst"

beachte: "alle Schnurze beissen" ist wahr,wenn es keine Schnurze gibt!

wichtig:

Allaussagen kann man durch ein Gegenbeispiel widerlegen, aber nicht durch Beispiele beweisen!

Induktionsbeweise → Abschnitt 1.2.3

Prinzip der vollständigen Induktion über $\mathbb{N}$:

beweise die Allaussage $(\forall n \in \mathbb{N})A(n)$ anhand von

(i) **Induktionsanfang**: $A(0)$.

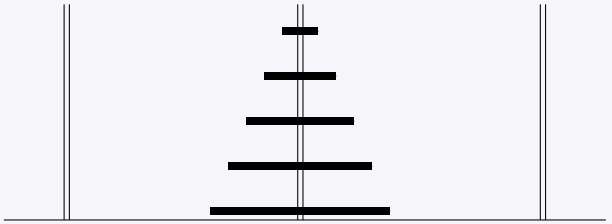
(ii) **Induktionsschritt**: für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$

Rechtfertigung:

für jedes feste n ergibt sich aus (ii) eine Implikationskette

$A(0) \Rightarrow A(1) \Rightarrow A(2) \Rightarrow \ldots \Rightarrow A(n-1) \Rightarrow A(n)$

Beispiel: Induktionsbeweis über $\mathbb{N}$ Beispiel 1.2.2



$A(n)$: n Scheiben lassen sich in $2^n - 1$ Schritten gemäß der Regeln umschichten, und nicht in weniger Schritten

Induktionsanfang: $A(0)$

Induktionsschritt: für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$

Induktionsprinzipien für andere Bereiche Beispiel 1.2.4

betrachte Menge M der Terme mit 2-st. Fktn $*$ und Konst. c
als Menge von Wörtern über $\Sigma = \{*, c, (,)\}$, $M \subseteq \Sigma^*$

$$M = \{c, c*c, c*(c*c), \ldots, (c*c)*(c*(c*c))), \ldots\}$$

systematische Erzeugung aller $t \in M$:

ausgehend vom Startelement $c \in M$
mit Operation $F\colon M \times M \longrightarrow M$

$$F(t_1, t_2) := \begin{cases} (t_1)*(t_2) & \text{für } t_1, t_2 \neq c \\ c*(t_2) & \text{für } t_1 = c, t_2 \neq c \\ (t_1)*c & \text{für } t_1 \neq c, t_2 = c \\ c*c & \text{für } t_1 = t_2 = c \end{cases}$$

Beweise damit z.B.: $\boxed{(\forall t \in M)\big(|t|_c = |t|_* + 1\big)}$

Induktionsprinzipien für andere Bereiche

M werde, ausgehend von $M_0 \subseteq M$,
durch Operationen $F \in \mathcal{F}$ erzeugt; dann lässt sich

$$(\forall x \in M)\, A(x)$$

beweisen anhand von

(i) **Induktionsanfang**: $A(x)$ gilt für alle $x \in M_0$.

(ii) **Induktionsschritt(e)** für $F \in \mathcal{F}$ (n-stellig):
aus $A(x_i)$ für $i = 1, \ldots, n$ folgt, dass auch $A(F(x_1, \ldots, x_n))$.

Induktionsprinzipien für andere Bereiche

Beispiele

Bereich M	$M_0 \subseteq M$	erzeugende Operationen
$\mathbb{N}$	$\{0\}$	S: $n \longmapsto n+1$
Σ^*	$\{\varepsilon\}$	($w \longmapsto wa$) für $a \in \Sigma$
$\{*, c\}$-Terme	$\{c\}$	$(t_1, t_2) \longmapsto (t_1 * t_2)$
endl. Teilmengen von A	$\{\emptyset\}$	($B \longmapsto B \cup \{a\}$) für $a \in A$

falscher Induktionsbeweis über $\mathbb{N}$ Übung 1.2.7

$A(n)$: { jede Gruppe von n Personen besteht aus gleichaltrigen Personen.

Induktionsanfang: $A(n)$ wahr für $n = 0$ und $n = 1$.

Induktionsschritt: $A(n) \Rightarrow A(n+1)$.

Sei $n \geqslant 1$, $|P| = n+1$; $p_1 \neq p_2$ beliebig aus P ausgewählt.

Betrachte $P_1 := P \setminus \{p_1\}$ und $P_2 := P \setminus \{p_2\}$. $|P_1| = |P_2| = n$.

Nach Induktionsannahme $A(n)$ bestehen also P_1 und P_2 jeweils aus gleichaltrigen Personen.

Jedes $p \in P \setminus \{p_1, p_2\}$ ist in P_1 *und* in P_2 vorhanden.

Also sind alle in P gleichaltrig. Also gilt auch $A(n+1)$.

Also gilt $(\forall n \in \mathbb{N})A(n)$?

Kapitel 2: Endliche Automaten Reguläre Sprachen

Reguläre Σ-Sprachen → Abschnitt 2.1

Operationen auf Σ-Sprachen

Komplement	$L \longmapsto \overline{L} := \Sigma^* \setminus L$	Boolesche Operationen
Schnitt	$(L_1, L_2) \longmapsto L_1 \cap L_2$	
Vereinigung	$(L_1, L_2) \longmapsto L_1 \cup L_2$	

Konkatenation von Sprachen

$(L_1, L_2) \longmapsto L_1 \cdot L_2 := \{u \cdot v : u \in L_1, v \in L_2\}$

Stern-Operation

$L \longmapsto L^* := \{u_1 \cdot \ldots \cdot u_n : u_1, \ldots, u_n \in L, n \in \mathbb{N}\}$