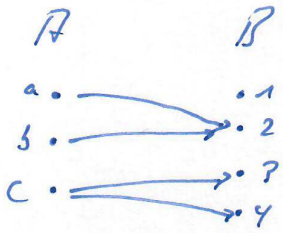
0. Einführung in das Beweisen

0.1 Objekte, Aussagen und Resultate

Objekte, über die man spricht:

(1) Mengen

(2) Relationen: $R \subseteq A \times B$ (auch nur Mengen)

$R =$ 

$= \{(a,2),(b,2),(c,3),(c,4)\}$.

(3) Funktionen: $F : A \to B$,

steht kurz für

$F \subseteq A \times B$, F linkstotal, F rechtseindeutig.

Also sind Funktionen auch nur Relationen

und somit auch nur Mengen.

Aussagen, die zu beweisen sind:

In der Regel Aussagen über Mengen:

(1) Inklusionen: $A \subseteq B$, falls (das ist ein definierendes Falls, alternativ sage "definitionsgemäß genau dann, wenn" gdw.

$$\forall x \in A : x \in B.$$

Eine äquivalente Definition wäre:

$$\forall x.\ x \in A \Rightarrow x \in B.$$

Das passt eher zur Prädikatenlogik,

ist aber in der Mathematik weniger üblich.

(2) Gleichheiten: $A = B$, falls $\forall x.\ x \in A \Leftrightarrow x \in B$.

Es gilt $A = B$ gdw. $A \subseteq B$ und $B \subseteq A$ gelten.

Damit ist das Beweisen von Gleichheiten
auch nicht schwieriger als das Beweisen von Inklusionen.

(3) Eigenschaften: $P : A \to \mathbb{B} = \{true, false\}$ // P = Property

Lese: $\forall x \in A : P(x) = true$

Lasse "= true" typischerweise weg
und schreibe:

$\forall x \in A : P(x)$.

Resultate, die erzielt werden:

Lemma: Einfache Aussage oder technische Hilfsaussage.
Das Beweisen ähnelt dem Programmieren.
Lemmata verhalten sich wie Prozeduren,
die man aufrufen kann.

Proposition: Nicht so einfache Aussage
oder Aussage von eigenständigem Interesse
(aber nicht super wichtig).

Satz: Wichtige Aussage.
Beweis nutzt vorher bewiesene Lemmata und Propositionen.

Korollar: Unmittelbare Folgerung
aus einem Lemma / Proposition / Satz.

0.2 Beweistechniken:

- **Umgang mit $\forall x \in A.\ P(x)$:**

  Der nächste Satz des Beweises lautet:

  > "Sei v aus A gegeben."

  Es wird also x zu v instantiiert.
  Über dieses v wissen wir nichts,
  außer dass es aus A stammt.
  Eben weil wir nichts über v wissen,
  wird die folgende Argumentationskette
  für alle ($\forall$) Werte gelten.
  Tatsächlich geht der Beweis jetzt damit weiter,
  dass wir

  > zeigen, dass $P(v)$ gilt.

- **Umgang mit $\exists x \in A.\ P(x)$:**

  In diesem Fall

  > ist ein konkretes v aus A anzugeben ($\exists$ = es gibt).

  Für dieses v muss man dann
  in der folgenden Argumentationskette

  > zeigen, dass $P(v)$ gilt.

Man kann sich den Unterschied der Quantoren
so vorstellen: $\forall x$ = der Wert v für x wird mir von außen gegeben.
$\exists x$ = ich bin verantwortlich, einen geeigneten Wert v für x zu finden.

Zeigen, dass etwas gilt:

- Sehe die Definition von P(x) ein.
- Argumentiere kleinschrittig, so dass jeder Schritt aus den vorherigen folgt.

Implikationen:

Oft hat P(x) die Gestalt:

"Wenn α gilt, dann gilt auch β."

Drei mögliche Beweisansätze / -strategien:

Direkter Beweis ($\alpha \Rightarrow \beta$):

- Beginne mit Aussage α.
- Nutze Definitionen und ziehe einfache Schlüsse.
- Finde Aussage β.

Kontraposition ($\neg\beta \Rightarrow \neg\alpha$):

- Beginne mit Aussage $\neg\beta$.
- Nutze Definitionen und ziehe einfache Schlüsse.
- Finde Aussage $\neg\alpha$.

Widerspruch ($\alpha \wedge \neg\beta \Rightarrow$ false):

- Beginne mit den Aussagen α und $\neg\beta$.
- Nutze Definitionen und ziehe einfache Schlüsse.
- Finde Widerspruch (also in der Form von $0=3$ oder $a \in \emptyset$ oder ähnlich falsches Zeug).

Äquivalenzen:

Manchmal möchte man zeigen, dass $\alpha \Leftrightarrow \beta \Leftrightarrow \gamma$.
Nutze Ringschluss und zeige: $\alpha \Rightarrow \beta$ und $\beta \Rightarrow \gamma$ und $\gamma \Rightarrow \alpha$.

0.3 Beweisen an einem Beispiel:

Ziel:
- Erläutere das Beweisen an einem Lemma aus der Vorlesung.
- Kommentare, die das Vorgehen beschreiben aber nicht zum eigentlichen Beweis gehören.

// sind so gekennzeichnet.

Bemerkung:
- Beweisen ist ein Handwerk, das man lernt, indem man es regelmäßig macht.
- Beweisen schult das folgerichtige Denken und das Abstraktionsvermögen.

Lemma: $\Sigma \in Folg(\Sigma)$.

Beweis:

Um $\Sigma \in Folg(\Sigma)$ zu zeigen,

// Wir brauchen die Definition von $\in$.

nutze die Definition.

$\forall A \in \Sigma : A \in Folg(\Sigma)$

// Das ist ein $\forall$-Quantor, nächster Satz ist klar.

Sei eine Formel A aus Σ gegeben.

Zu zeigen ist: $A \in Folg(\Sigma)$.

// Um Weiterzumachen, brauchen wir die Definition von $Folg(\Sigma)$.

Nutze die Definition von $Folg(\Sigma)$

als $\exists B$ Formel $\mid \Sigma \models B$.

Es ist also zu zeigen:

$A \in \{B \mid \Sigma \vdash B\}$,

// Damit A in der Menge liegt,
muss es die Bedingung der Menge erfüllen.

kurz $\Sigma \vdash A$.

// Wir brauchen die Definition von $\vdash$.

Per Definition gilt $\Sigma \vdash A$,
falls

$\forall\, \ell : \text{Formel} \to \mathbb{B}$:
Wenn ℓ die Menge Σ erfüllt,
dann erfüllt ℓ auch A.

// Das ist wieder ein $\forall$-Quantor,
der nächste Satz ist also festgelegt.

Sei eine Bewertung $\ell : \text{Formel} \to \mathbb{B}$ gegeben.
Zu zeigen ist: Wenn ℓ Σ erfüllt, dann auch A.

// Das ist eine Implikation,
dafür kennen wir drei Beweisansätze.

Direkter Beweis:

Angenommen ℓ erfüllt Σ.

// Wir brauchen die Definition.

Dann gilt für jedes $B \in \Sigma$,
dass ℓ B erfüllt.

// Jetzt kommt der einzige Moment,
wo wir selber einen Schluss ziehen müssen.
Der Rest des Beweises bis hierher
war rein mechanisch.

Da $A \in \Sigma$, gilt auch für A,
Das ist der Schluss
dass ℓ A erfüllt. □

Der Beweis lässt sich auch
mit den anderen beiden Beweisansätzen beenden:

Alternative 1: Kontraposition

Angenommen ℓ erfüllt A nicht.
Da $A \in \Sigma$, gibt es eine Formel aus Σ,
die ℓ nicht erfüllt.
Also erfüllt ℓ Σ nicht. □

Alternative 2: Widerspruch

Angenommen ℓ erfüllt Σ
aber ℓ erfüllt A nicht.
Da $A \in \Sigma$, muss ℓ insbesondere A erfüllen.
↯ ℓ kann nicht A erfüllen
(Widerspruch) und gleichzeitig A nicht erfüllen. □

Welcher Beweisansatz für eine Aussage am besten klappt,
lässt sich nicht sagen → Übung / Erfahrung hilft.

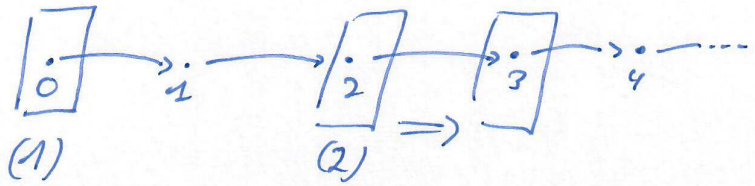
0.4 Induktiv definierte Mengen und strukturelle Induktion

Ziel: Beweise Aussagen

$$\forall x \in A : P(x),$$

wobei A eine unendliche Menge ist, die aber schrittweise aufgebaut ist.

Intuition:



$[\cdot] :=$ P gilt für das Element.

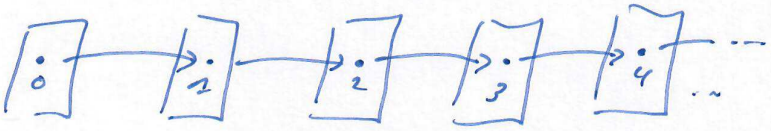
(1) Zeige $P(0)$.

(2) Zeige alle Varianten:

Angenommen $P(x)$ gilt schon,

folgere daraus $P(x+1)$.

- Dann hat man gezeigt:



Definition (induktiv definierte Menge):

Sei X eine Menge (elementarer Bausteine).

Sei O eine Menge von Operatoren mit Stelligkeit $k \geq 1$.

Die durch X und O induktiv definierte Menge ist die kleinste Menge A mit

(1) $X \subseteq A$

(2) Falls $o \in O$ Stelligkeit k hat und $a_1, \dots, a_k \in A$, dann gilt auch $o(a_1, \dots, a_k) \in A$.

Beispiele:

- Betrachte $\mathbb{N} = \{0, 1, 2, \ldots\}$.
  Dann ist $X = \{0\}$ und $O = \{+1_1\}$.

- Betrachte die Menge der aussagenlogischen Formeln über der Menge der atomaren Aussagen/aussagenlogischen Variablen P.
  Dann ist
  $$X = P \cup \{\top, \bot\} \text{ und } O = \{\neg_1, \wedge_2, \vee_2, \to_2, \leftrightarrow_2\}.$$

Das Induktionsprinzip:

Sei A durch X und O induktiv definiert.

Um zu zeigen:
$$\forall n \in A : P(n)$$
nutze folgendes Prinzip:

$$\underbrace{\forall x \in X : P(x)}_{\text{Induktionsanfang}} \wedge \underbrace{\forall o_k \in O \; \forall n_1, \ldots, n_k \in A : \underbrace{\underbrace{(P(n_1) \wedge \ldots \wedge P(n_k))}_{\text{Induktionsvoraussetzung}} \Rightarrow \underbrace{P(o(n_1, \ldots, n_k))}_{\text{Induktionsschluss}}}_{\text{Induktionsschritt}}.$$

Beispiele:

Zeige: Alle geraden Zahlen aus $\mathbb{N}$ sind durch zwei teilbar:
$$\forall x \in \{0, 2, 4, 6, \ldots\} : \exists y \in \mathbb{N} : 2y = x.$$

Die Menge der geraden Zahlen $\{0, 2, 4, 6, \ldots\}$
ist induktiv definiert durch

$$X = \{0\}$$
$$O = \{+2\}_2\{.$$

Beweis:

IA: $\forall x \in \{0\} : \exists y \in \mathbb{N} : 2y = x.$

(Induktions-anfang) Sei $x \in \{0\}$, also $x = 0$.
Wähle $y = 0$.
Dann gilt
$$x = 0 = 2 \cdot 0 = 2 \cdot y.$$

IV: Sei n eine gerade Zahl,

(Induktions-voraussetzung) für die es $y \in \mathbb{N}$ gibt
mit
$$n = 2y.$$

IS: Nun ist für $n+2$ ein $z \in \mathbb{N}$ zu finden,

(Induktions-schluss) so dass
$$n + 2 = 2z.$$

Es gilt
$$n + 2 \overset{(IV)}{=} 2y + 2 = 2(y+1).$$

Wähle
$$z = y + 1.$$

□

Folge: Jede aussagenlogische Formel
hat eine gerade Anzahl an Klammern:
$$\forall A \in \text{Formel} . \exists y \in \mathbb{N} : \#(A) = 2y.$$

Dafür ist

$$\#: \text{Formel} \to \mathbb{N}$$

eine Funktion, die die Klammern einer Formel zählt.

Beweis:

IA: Sei p eine aussagenlogische Variable.

Dann gilt

$$\#(p) = 0 = 2 \cdot 0.$$

Mit $y = 0$ gilt die Behauptung.

Für $\top$ und $\bot$ ist die Argumentation analog.

IV: Betrachte Formeln A und B

für die es y_1 und y_2 gibt mit

$$\#(A) = 2y_1 \text{ und } \#(B) = 2y_2.$$

IS: Fall 1: $\neg(A)$

Es gilt $\#(\neg(A))$

$$= 2 + \#(A)$$

$$\overset{(IV)}{=} 2 + 2 \cdot y_1$$

$$= 2(y_1 + 1).$$

Mit $z = y_1 + 1$ gibt es also eine natürliche Zahl,

so dass $\#(\neg(A)) = 2 \cdot z$.

Fall 2: $(A \text{ op } B)$ mit $\text{op} \in \{\wedge, \vee, \to, \leftrightarrow\}$

Es ist ein $z \in \mathbb{N}$ zu finden mit

$$\#((A \text{ op } B)) = 2z.$$

Wähle $z = y_1 + y_2 + 1$.

Tatsächlich gilt damit:

$$\begin{aligned} \#((A \,\mathrm{op}\, B)) &= 2 + \#(A) + \#(B) \\ &\overset{(IV)}{=} 2 + 2y_1 + 2y_2 \\ &= 2 \cdot (1 + y_1 + y_2) = 2 \cdot z. \end{aligned}$$

□