1. Großübung (29.4.19)

Induktion

- zunächst: vollständige Induktion (über $\mathbb{N}$)

Def: $\mathbb{N}$ ist die kleinste Menge mit

- $0 \in \mathbb{N}$
- $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$ „impliziert"

Konsequenz: Jede natürliche Zahl lässt sich von 0 erreichen, in dem man endlich oft den Nachfolger bildet.

Um eine Aussage der Form „$\forall n \in \mathbb{N}$: $A(n)$ gilt" zu zeigen, zeige:

- Induktionsanfang (IA): Aussage gilt für $n=0$
- Induktionsvoraussetzung (IV): Angenommen, die Aussage gilt für ein festes, aber beliebiges $n \in \mathbb{N}$
  (n ist fest, wir wissen aber nichts darüber)
- Induktionsschritt (IS) „$n \to n+1$": Dann gilt die Aussage auch für $n+1$.

Wir haben also gezeigt:
- $A(0)$ gilt (IA)
- $\forall n: A(n) \Rightarrow A(n+1)$ (IV+IS)

Kombiniere:

$A(0)$ gilt, $A(0) \Rightarrow A(1)$ $\Rightarrow A(1)$ gilt
$\Rightarrow A(1)$ gilt, $A(1) \Rightarrow A(2)$ $\Rightarrow A(2)$ gilt
$\Rightarrow \dots$

$A(n)$ gilt $\forall n$ wie gewünscht.

Bsp: $\forall n: n < 2^n$

IA: $n=0$: $0 < 1 = 2^0$ ✓

IV: Für ein n gelte $n < 2^n$

IS: $n \to n+1$: z. z.: $n+1 < 2^{n+1}$

$$n+1 \overset{\text{IV: } n<2^n}{<} 2^n + 1 \overset{\forall n: 1 \leq 2^n, \text{„+“ monoton}}{\leq} 2^n + 2^n = 2(2^n) = 2^{n+1}$$ ✓

& „+“ ist monoton (größere Summanden $\Rightarrow$ größere Summe) □

Bsp:

Theorem: Alle Informatiker sind schlau.
(Alle Katzen sind schwarz.)
(Alle Frauen sind blond.)

Beweis:

Einschränkung ist wichtig, da sonst Induktion nicht funktioniert

Zeige: $\forall X$ endliche Menge von Informatikern:
X enthält schlauen Informatiker // Prämisse P
$\Rightarrow$ Alle Informatiker in X schlau // Konklusion K

Durch Wahl von X = alle Informatiker auf der Erde wird das Theorem gezeigt (unter der Annahme, dass es mindestens einen schlauen Informatiker gibt)

Zeige nun die Hilfsaussage durch Induktion nach $n = |X|$

IA: $n=0 \Rightarrow X = \phi \Rightarrow$ Aussage gilt, denn die Prämisse ist verletzt (Wahrheitstabelle für Implikation:

P	K	P⇒K
0	0	1
0	1	1
1	0	0
1	1	1

)

($n=1$: $X = \{x\}$. x schlau $\Rightarrow$ alle Informatiker in X schlau)

IV: Gelte die Aussage für ein n
(d.h. für alle Mengen der Größe n)

IS: $n \to n+1$ Betrachte X mit $|X| = n+1$
Schreibe $X = \{x_1, \dots, x_n, x_{n+1}\}$
Ang ein Informatiker aus X schlau (sonst Prämisse unwahr)
OBdA x_1 schlau (ggf. umsortieren)
↑ "ohne Beschränkung der Allgemeinheit"

Betrachte $X' = \{x_1, -, x_n\} = X \setminus \{x_{n+1}\}$

$X'' = \{x_1, -, x_{n-1}, x_{n+1}\} = X \setminus \{x_n\}$

$|X'| = |X''| = n$, $x_1 \in X'$, $x_1 \in X''$, x_1 nach Annahme schlau

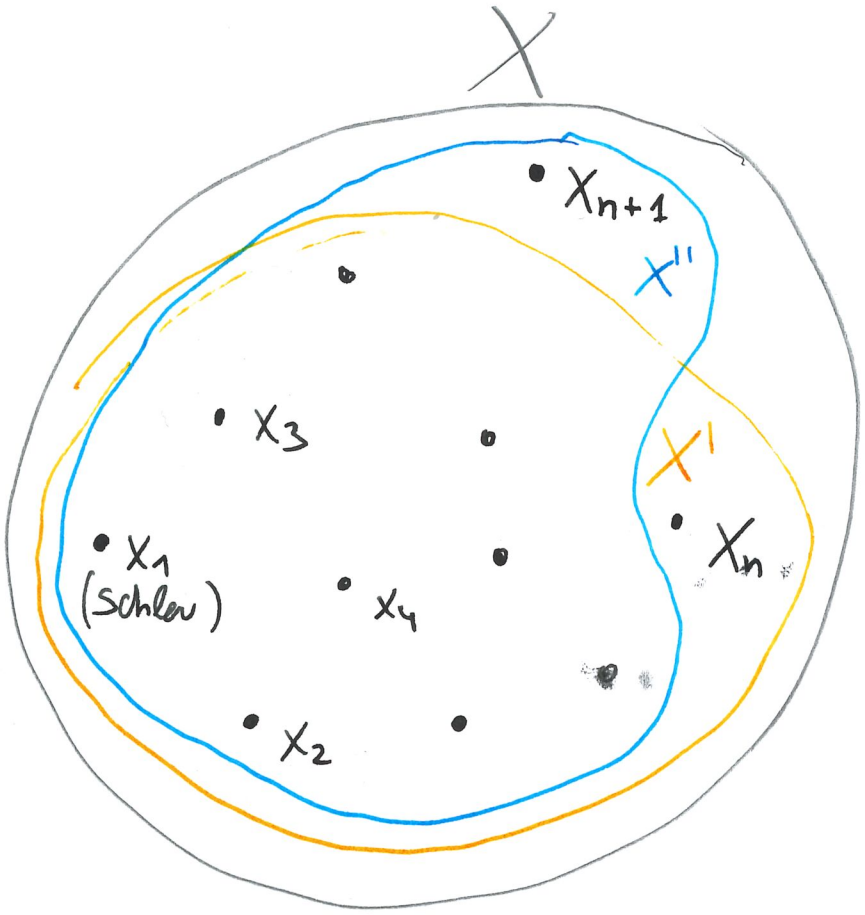
$\overset{IV}{\Rightarrow}$ Alle Informatiker in $X' \cap X''$ schlau

$\Rightarrow$ Alle " " $X' \cup X'' = X$ "

Nanu, das ist doch Quatsch...

Wo ist der Fehler?

Tipp: Wie sehen $X' \cap X''$ bei $n=2$ aus?



- nun: Strukturelle Induktion.

Def: Sei $\mathcal{A}$ Menge von (Aussagen-)Variablen.

$F(\mathcal{A})$ ist die kleinste Menge mit

- $p \in \mathcal{A} \Rightarrow p \in F(\mathcal{A})$ // Variablen
  $\bot, \top \in F(\mathcal{A})$ // false, true
  } Basisfälle, analog zu $0 \in \mathbb{N}$

- $B, C \in F(\mathcal{A}) \Rightarrow (\neg B), (B \wedge C), (B \vee C), (B \to C), (B \leftrightarrow C) \in F(\mathcal{A})$
  } Induktive Fälle, analog zu $n \in \mathbb{N} \Rightarrow n+1 \in \mathbb{N}$

Um eine Aussage der Form

$\forall A \in F(\mathcal{A}): \underbrace{D(A)}$ gilt"

" zu zeigen, bel. Aussage, die von $A \in F(\mathcal{A})$ abhängt

zeige

IA: $D(p)$ gilt $\forall p \in \mathcal{A}$, $D(\bot)$, $D(\top)$ gelten

IV: Angenommen $D(B)$, $D(C)$ gelten für feste, aber beliebige Formeln $B, C \in F(\mathcal{A})$

IS: Dann gelten auch

$D(\neg B)$, $D(B \wedge C)$, $D(B \vee C)$,
$D(B \to C)$, $D(B \leftrightarrow C)$

Bsp: Beweis einer semantischen Eigenschaft durch Induktion

Theorem: Alle Formeln, die nur aus Variablen, $\wedge, \vee$ bestehen, sind erfüllbar

Beweis: Umformulierung:

$\forall A \in \mathcal{F}(\mathbb{A})$: A besteht nur aus Variablen, $\wedge, \vee$
$\Rightarrow$ A erfüllbar (d.h. $\exists \varphi: \mathbb{A} \to \mathbb{B}$ Belegung mit $\hat{\varphi}(A) = 1$)

Versuch: Beweis durch Induktion

IA: $A \equiv p$: Wähle φ mit $\varphi(p)=1 \Rightarrow \hat{\varphi}(A) = \hat{\varphi}(p) = \varphi(p) = 1$

$A \equiv \bot$, $A \equiv \top$: Prämisse unwahr, also Aussage wahr

IV: Gelte die Aussage für B, C

IS: $A \equiv \neg B$, $A \equiv B \to C$, $A \equiv B \leftrightarrow C$: Prämisse unwahr

$A \equiv B \vee C$ (mit B, C bestehen nur aus Variablen, $\wedge, \vee$, sonst Prämisse unwahr)

IV: B erfüllbar
$\Rightarrow \exists \varphi$ mit $\hat{\varphi}(B) = 1$
$\hat{\varphi}(A) = \hat{\varphi}(B \vee C) = \max(\hat{\varphi}(B), \hat{\varphi}(C)) = \max(1, \underbrace{\hat{\varphi}(C)}_{\in\{0,1\}}) = 1$

$A \equiv B \wedge C$: IV: B, C erfüllbar
$\Rightarrow \exists \varphi, \psi$ mit $\hat{\varphi}(B) = 1, \hat{\psi}(C) = 1$

Problem: Wir wissen nun nichts über $B \wedge C$.

Bsp. $p \wedge \neg p$: $p, \neg p$ jeweils erfüllbar, aber $p \wedge \neg p$ unerfüllbar

Lösung: Zeige stärkere Eigenschaft

$\forall A \in \mathcal{F}(\mathcal{A})$: A besteht nur aus Variablen, $\wedge, \vee$

$\Rightarrow$ A wird von der Bewertung φ mit $\varphi(p) = 1 \; \forall p \in \mathcal{A}$ erfüllt

IA: $A \equiv p$: $\hat{\varphi}(A) = \varphi(p) = 1$

$A \equiv \bot$, $A \equiv \top$: Prämisse unwahr

IV: Ang. Aussage gilt für B, C

IS: $A \equiv \neg B$, $A \equiv B \to C$, $A \equiv B \leftrightarrow C$: Prämisse unwahr

$A \equiv B \vee C$: IV: $\hat{\varphi}(B) = 1$

Also $\hat{\varphi}(A) = \max(\underbrace{\hat{\varphi}(B)}_{1}, \underbrace{\hat{\varphi}(C)}_{\in\{0,1\}}) = 1$

$A \equiv B \wedge C$: IV: $\hat{\varphi}(B) = \hat{\varphi}(C) = 1$

Also $\hat{\varphi}(A) = \min(\hat{\varphi}(B), \hat{\varphi}(C)) = \min(1,1) = 1$ □

Also: Mit nur $\wedge, \vee$ lassen sich keine unerfüllbaren Formeln konstruieren

Def Eine **Bool'sche Funktion** ist eine Funktion mit Signatur $f: \mathbb{B}^n \to \mathbb{B}$ (für ein $n \in \mathbb{N}$)

Zeige Korrespondenz zwischen
- Bool'schen Fkt der Form $f: \mathbb{B}^{n \times m} \to \mathbb{B}$
- aussagenlogischen Formeln mit n Variablen

für alle $n \in \mathbb{N}$ $(n > 0)$.

Idee:
- Parameter der Funktion $\hat{=}$ Wahrheitswerte der Variablen
- Wert " " $\hat{=}$ Wahrheitswert oder Auswertung der Formel

Eine Richtung klar: Formel definiert Funktion

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

definiert $f_A : \mathbb{B}^3 \to \mathbb{B}$

$(p,q,r) \mapsto \max(\min(p,q), 1-r)$

Andere Richtung:

Finde zu jeder Fkt: $f: \mathbb{B}^n \to \mathbb{B}$ eine "äquivalente" Formel mit $\leq n$ Variablen.

Induktion nach n.

$n = 1$.

p	$f_1(p)$	$f_2(p)$	$f_3(p)$	$f_4(p)$
0	0	0	1	1
1	0	1	0	1

f_1, f_2, f_3, f_4 sind alle möglichen Boolschen Fkt. für $n = 1$

$f_1 \hat{=} \bot \hat{=} p \wedge \neg p$ $\quad f_3 \hat{=} \neg p$

$f_2 \hat{=} p$ $\quad f_4 \hat{=} \top \hat{=} p \vee \neg p$

Der Vollständigkeit halber:

$n = 2$:

p	q	$f_1(p,q)$	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Alle $|\mathbb{B}^2 \to \mathbb{B}| = (|\mathbb{B}|)^{|\mathbb{B}^2|} = 2^{(2^2)} = 2^4 = 16$ möglichen Funktionen der Form $\mathbb{B}^2 \to \mathbb{B}$

Wie bei $n = 1$:

$f_1 \hat{=} \bot$, $f_{16} \hat{=} \top$

$f_4 \hat{=} p$, $f_6 \hat{=} q$

$f_{13} = \neg p$, $f_{11} \hat{=} \neg q$

Außerdem:

$f_2 \hat{=} p \wedge q$, $f_8 \hat{=} p \vee q$

$f_{15} \hat{=} \neg(p \wedge q)$, $f_9 \hat{=} \neg(p \vee q)$

$f_{14} \hat{=} p \to q$, $f_{12} \hat{=} q \to p$, $f_3 \hat{=} \neg(p \to q)$, $f_5 \hat{=} \neg(q \to p)$

$f_{10} \hat{=} p \leftrightarrow q$

$f_7 \hat{=} \neg(p \leftrightarrow q) \hat{=} p \oplus q \hat{=} p \text{ XOR } q$ "exklusives Oder"

Nun $n \to n+1$:

Betrachte $f: \mathbb{B}^{n+1} \to \mathbb{B}$

$$(p_1, \dots, p_{n+1}) \mapsto f(p_1, \dots, p_{n+1})$$

Definiere $f_0: \mathbb{B}^n \to \mathbb{B}$

$$(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n, 0)$$

$f_1: \mathbb{B}^n \to \mathbb{B}$

$$(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n, 1)$$

Es gilt

$$f(p_1, \dots, p_n, p_{n+1}) = \begin{cases} f_0(p_1, \dots, p_n) & \text{, falls } p_{n+1} = 0 \\ f_1(p_1, \dots, p_n) & \text{, " } p_{n+1} = 1. \end{cases}$$

Induktion (IV): Es gibt zu f_0 bzw. f_1 "äquivalente" Formeln A_0 bzw. A_1.

Konstruiere:

$$A \equiv (p_{n+1} \wedge A_1) \vee (\neg p_{n+1} \wedge A_0)$$

Nachrechnen: f und A sind "äquivalent", d.h. für jede Belegung $\varphi: \{p_1, \dots, p_{n+1}\} \to \mathbb{B}$ gilt:

$$f(\varphi(p_1), \varphi(p_2), \dots, \varphi(p_{n+1})) = \hat{\varphi}(A) \qquad \square$$

Def: Eine Menge an Operatoren heißt vollständig, wenn man durch Formeln über diesen Operatoren alle Bool'schen Fkt. darstellen kann

- Beweis zeigt: $\{\bot, \top, \wedge, \vee, \neg, \rightarrow, \leftrightarrow, xor\}$ vollständig
- Beweis zeigt sogar: $\{\wedge, \vee, \neg\}$ vollständig
  (siehe $n = 1$ und $n \rightarrow n+1$)
- $\{\wedge, \vee\}$ ist nicht vollständig.
  Haben vorhin gezeigt, dass die Fk $f: \mathbb{B}^n \rightarrow \mathbb{B}$, $(p_1, \dots, p_n) \mapsto 0$ nicht darstellbar ist.
- Sogar $\{\wedge, \neg\}$ und $\{\vee, \neg\}$ sind vollständig

"Übungsaufgaben zum Knobeln"

- Beweise das!
  Tipp: De-Morgan'sche Regeln
- Welche Teilmengen von $\{\bot, \top, \vee, *, \neg, \rightarrow, \leftrightarrow, xor\}$ sind vollständig?
- Gibt es einen einzelnen binären Operator $*$, so dass $\{*\}$ bereits vollständig ist?
  Tipp: f_{15}.