Sequenzenkalkül allgemeiner Beweiskalkül

Sequenzen

$\Gamma \vdash \Delta$ $\Gamma, \Delta \subseteq \mathrm{AL}$, endlich
auch: $\Gamma; \Delta$ oder Γ, Δ
Γ, Δ als ungeordnete Listen ...

$\Gamma \vdash \Delta$ *allgemeingültig* gdw. $\bigwedge \Gamma \models \bigvee \Delta$

wichtig: links Konjunktion (der Voraussetzungen)
rechts Disjunktion (möglicher Konsequenzen)

Bsp.: $\varphi \vdash \psi$ allgemeingültig gdw. $\varphi \models \psi$.
$\emptyset \vdash \psi$ allgemeingültig gdw. ψ allgemeingültig.
$\varphi \vdash \emptyset$ allgemeingültig gdw. φ unerfüllbar.

Sequenzenkalkül
Regeln zur Erzeugung aller allgemeingültigen Sequenzen.

AL Sequenzenkalkül → Abschnitt 6.2

Erzeugung allgemeingültiger Sequenzen durch Sequenzenregeln

Sequenzenregeln

neue Sequenzen aus bereits abgeleiteten Sequenzen

Format: $\dfrac{\text{Prämissen}}{\text{Konklusion}}$

Beispiele: $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$ oder $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$

Korrektheit
des Kalküls: jede ableitbare Sequenz ist allgemeingültig.

einer Regel: sind die Prämissen allgemeingültig,
so auch die Konklusion.

AL Sequenzenkalkül $\mathcal{SK}$

(Ax) $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$

(0-Ax) $\dfrac{}{\Gamma, 0 \vdash \Delta}$ (1-Ax) $\dfrac{}{\Gamma \vdash \Delta, 1}$

$(\neg\mathrm{L})$ $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$ $(\neg\mathrm{R})$ $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$

$(\vee\mathrm{L})$ $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$ $(\vee\mathrm{R})$ $\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$

$(\wedge\mathrm{L})$ $\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$ $(\wedge\mathrm{R})$ $\dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

Korrektheit nachprüfen!

sogar rückwärts (ohne Informationsverlust!)

Beispiel

Ableitung der allgemeingültigen Sequenz $p \vdash (p \wedge q) \vee \neg q$:

$$\dfrac{\dfrac{\dfrac{}{p \vdash p, \neg q}\,(\mathrm{Ax}) \qquad \dfrac{\dfrac{}{p, q \vdash q}\,(\mathrm{Ax})}{p \vdash q, \neg q}\,(\neg\mathrm{R})}{p \vdash (p \wedge q), \neg q}\,(\wedge\mathrm{R})}{p \vdash (p \wedge q) \vee \neg q}\,(\vee\mathrm{R})$$

Ax: $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$ $\neg$R: $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$ $\wedge$R: $\dfrac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

Vollständigkeit

→ Abschnitt 6.3

Jede allgemeingültige Sequenz ist ableitbar.
Beweisidee: systematische Beweissuche rückwärts

> zu jeder Formel in einer Konklusions-Sequenz
> existiert (genau) eine Regel mit Prämissen,
> in der diese Formel abgebaut ist.

in rückwärts von der Zielsequenz generiertem Beweisbaum gilt:

Zielsequenz allgemeingültig ⇔ alle Sequenzen an den Blättern sind allgemeingültig

eine Sequenz aus Variablen ist allgemeingültig ⇔ Instanz von (Ax), Axiom

Beispiel Beweissuche

für eine *nicht* allgemeingültige Sequenz

$$(\vee L)\ \dfrac{(\wedge R)\ \dfrac{(\text{Ax})\ \dfrac{}{p \vdash p} \qquad \mathbf{p \vdash q}}{p \vdash p \wedge q} \qquad (\wedge R)\ \dfrac{\mathbf{q \vdash p} \qquad (\text{Ax})\ \dfrac{}{q \vdash q}}{q \vdash p \wedge q}}{p \vee q \vdash p \wedge q}$$

Man liest ab, dass z.B. die Interpretation $p \mapsto 1\,;\ q \mapsto 0$ ein Gegenbeispiel liefert.

Satz

Der AL Sequenzenkalkül ist korrekt und vollständig für die Ableitung aller allgemeingültigen AL Sequenzen.

Schnittregeln, von $\mathcal{SK}$ zu $\mathcal{SK}^+$

Hinzunahme weiterer *korrekter* Regeln erhält Korrektheit und Vollständigkeit

Schnittregel erlaubt direkte Nachbildung von $\left\{\begin{array}{l}\textbf{Kettenschlüssen}\\ \textbf{indirektem Beweis}\end{array}\right.$

- Kettenschluss: aus $(A \Rightarrow B)$ und $(B \Rightarrow C)$ gewinne $(A \Rightarrow C)$ klassische Schlussfigur des "modus ponens"
- indirekter Beweis: aus $(\neg A \Rightarrow \bot)$ gewinne A

$$\boxed{\text{(modus ponens)} \qquad \dfrac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}}$$

korrekt (nachprüfen!)

Bem.: Anwendung von modus ponens 'schluckt' Hilfsformel φ; problematisch für (rückwärtsgerichtete) Beweissuche

Schnittregeln, von $\mathcal{SK}$ zu $\mathcal{SK}^+$

→ Abschnitt 6.4

$$\boxed{\text{(modus ponens)} \qquad \dfrac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}}$$

Widerspruchsregel:

$$\boxed{\text{(Kontradiktion)} \qquad \dfrac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}}$$

jede konkrete Instanz von modus ponens oder Kontradiktion ist in $\mathcal{SK}$ eliminierbar (warum?)

Kontradiktion lässt sich direkt in $\mathcal{SK}$ + modus ponens herleiten

ebenso z.B. für die Schlussfigur des indirekten Beweises:

$$\boxed{\text{(Widerspruch)} \qquad \dfrac{\Gamma, \neg\varphi \vdash \psi \qquad \Gamma, \neg\varphi \vdash \neg\psi}{\Gamma \vdash \varphi}}$$

Teil 2: Logik erster Stufe (Prädikatenlogik), FO

Gegenstandsbereich:

S-Strukturen mit Belegungen für Element-Variablen

Ausdrucksmöglichkeiten:

atomare Aussagen über Terme Funktionen, Konstanten, Variablen

$\wedge, \vee, \neg$ (wie in AL)

Quantifizierung $\forall, \exists$ über Elemente

wesentliche Charakteristika von FO

- höheres Ausdrucksniveau
- strukturierte Formalisierung komplexerer Eigenschaften
- modulare Semantik
- korrekte und vollständige Beweiskalküle
- Kompaktheit
- nicht mehr entscheidbar

Strukturen zu Signatur S

$\rightarrow$ Abschnitt 1.1

Symbole:		
	$x, y, z, \ldots, x_1, x_2, x_3, \ldots$	Variablensymbole
	$c, d, e, \ldots$	Konstantensymbole
	$f, g, \ldots$	Funktionssymbole
	$P, Q, R, \ldots$	Relationssymbole

Signatur S: (vgl. *Klasse* beim OOP)
Auswahl von Konstanten-, $\underbrace{\text{Funktions- und Relationssymbolen}}_{\text{mit spezifizierten Stelligkeiten: Syntax!}}$

S-Struktur: (vgl. *Instanz* beim OOP)

$\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots, R^{\mathcal{A}}, \ldots)$ (Semantik)

besteht aus: Trägermenge $A \neq \emptyset$
für $c \in S$: ausgezeichnetes Element $c^{\mathcal{A}} \in A$.
für n-st. $f \in S$: n-st. Funktion $f^{\mathcal{A}} \colon A^n \to A$.
für n-st. $R \in S$: n-st. Relation $R^{\mathcal{A}} \subseteq A^n$.

Beispiel: $\mathcal{N} = \big(\mathbb{N}, +^{\mathcal{N}}, \cdot^{\mathcal{N}}, <^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}}\big)$ zu $S = \{+, \cdot, <, 0, 1\}$

Beispiele von Strukturtypen

unter vielen anderen

Wortstrukturen zu Signatur $S := \{<\} \cup \{P_a \colon a \in \Sigma\}$

$w = a_1 \ldots a_n \quad \longleftrightarrow \quad \mathcal{W} := \big(\{1, \ldots, n\}, <^{\mathcal{W}}, (P_a^{\mathcal{W}})_{a \in \Sigma}\big)$,
$<^{\mathcal{W}} := \{(i,j) \colon 1 \leqslant i < j \leqslant n\}$,
$P_a^{\mathcal{W}} := \{i \colon a_i = a\}$.

Graphen zu Signatur $S := \{E\}$

$u \bullet \xrightarrow{(u,v) \in E^{\mathcal{G}}} \bullet\, v$

$\mathcal{G} := \big(V, E^{\mathcal{G}}\big)$,
mit Knotenmenge V
Kantenrelation $E^{\mathcal{G}} \subseteq V \times V$.

Transitionssysteme (NFA) zu Signatur $S := \{E_a \colon a \in \Sigma\}$

$(\Sigma, Q, \Delta) \quad \longleftrightarrow \quad \mathcal{A} := \big(Q, (E_a^{\mathcal{A}})_{a \in \Sigma}\big)$,
$E_a^{\mathcal{A}} := \{(q, q') \colon (q, a, q') \in \Delta\}$.

Relationale Datenbanken, . . .

Beispiele von Strukturen

natürliche Zahlen:
$\mathcal{N} = (\mathbb{N}, +^{\mathcal{N}}, \times^{\mathcal{N}}, <^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}})$ zu Signatur $\{+, \times, <, 0, 1\}$
alternativ (Peano): $(\mathbb{N}, ++^{\mathcal{N}}, =^{\mathcal{N}}, 0^{\mathcal{N}})$ zu $\{\mathrm{succ}, =, 0\}$

ganze Zahlen:
$\mathcal{Z} = (\mathbb{Z}, -^{\mathcal{Z}}, \times^{\mathcal{Z}}, <^{\mathcal{Z}}, 1^{\mathcal{N}})$ zu Signatur $\{-, \times, <, 1\}$
aber auch zu Signatur $\{x^y, \div, \mathtt{prim}, \pi\}$ (!)

rationale Zahlen:
$\mathcal{Q} = (\mathbb{Q}, -^{\mathcal{Q}}, \times^{\mathcal{Q}}, \div^{\mathcal{Q}}, <^{\mathcal{Q}}, 0^{\mathcal{Q}}, 1^{\mathcal{Q}})$ zu Signatur $\{-, \times, \div, <, 0, 1\}$

ebenso **reelle Zahlen:** $\mathcal{R} = (\mathbb{R}, -^{\mathcal{R}}, \times^{\mathcal{R}}, \div^{\mathcal{R}}, <^{\mathcal{R}}, 0^{\mathcal{R}}, 1^{\mathcal{R}})$

komplexe Zahlen: $\mathcal{C} = (\mathbb{C}, -^{\mathcal{C}}, \times^{\mathcal{C}}, \div^{\mathcal{C}}, =^{\mathcal{C}}, 0^{\mathcal{C}}, 1^{\mathcal{C}})$

Bits: $\mathcal{B} = (\mathbb{B}, \mathtt{xor}, \wedge, \neq, 0, 1)$ zu $\{+, \times, <, 0, 1\}$

Terme

→ Abschnitt 1.2

Variablen aus $\mathcal{V} := \{x_1, x_2, \dots\}$ bzw. $\mathcal{V}_n := \{x_1, \dots, x_n\}$

S-Terme

$T(S)$ (über Variablen aus $\mathcal{V}$) induktiv erzeugt durch:

$x \in T(S)$ für $x \in \mathcal{V}$.
$c \in T(S)$ für $c \in S$.
$ft_1 \dots t_n \in T(S)$ für $f \in S$ (n-st.), $t_1, \dots, t_n \in T(S)$.

$T_n(S) \subseteq T(S)$: S-Terme über Variablen aus $\mathcal{V}_n$.

Beispiele wohlgeformter S-Terme

$S = \{f, c\}$, f 2-st.: c, $ffccc$, $fcfcc$, …, x_{17}, fx_1c, ffx_5cx_2, …

$S = \{+, \cdot, 0, 1\}$, $+, \cdot$ 2-st.: $\cdot + 11 + +111$,
$+ \cdot + + 111\, x_3\, x_1$, …

Konvention: Funktionsterme mit Klammern, 2-st. auch infix
$\big(((1+1)+1)\cdot x_3 + x_1\big)$ statt $+ \cdot + + 111 x_3 x_1$

Belegungen:

→ Abschnitt 1.3

weisen den Variablensymbolen Elemente einer S-Struktur zu

Belegung
über S-Struktur $\mathcal{A} = (A, c^{\mathcal{A}}, \dots, f^{\mathcal{A}}, \dots)$:

$$\begin{array}{rcl} \beta\colon \mathcal{V} & \longrightarrow & A \\ x & \longmapsto & \beta(x) \end{array}$$

Idee: eine Belegung liefert *Interpretation* der Variablensymbole in S-Struktur

diese Interpretation läßt sich natürlich auf alle S-Terme erweitern (wie?)

$\longrightarrow$ **die Semantik von Termen**

Semantik von S-Termen

→ Abschnitt 1.2/3

in **S-Interpretation:** S-Struktur + Belegung $\mathfrak{I} = (\mathcal{A}, \beta)$

Semantik von Termen

induktiv über $T(S)$ für gegebene S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$:

Interpretation von $t \in T(S)$: $t^{\mathfrak{I}} \in A$ induktiv geg. durch

- $t = x$ ($x \in \mathcal{V}$ Variable) : $t^{\mathfrak{I}} := \beta(x)$.
- $t = c$ ($c \in S$ Konstante) : $t^{\mathfrak{I}} := c^{\mathcal{A}}$.
- $t = ft_1 \dots t_n$ ($f \in S$, n-st.) : $t^{\mathfrak{I}} := f^{\mathcal{A}}(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}})$.

beachte Format dieser Interpretation als Abbildung

$$\boxed{\begin{array}{rcl} T(S) & \longrightarrow & A \\ t & \longmapsto & t^{\mathfrak{I}} \end{array}}$$

und Abhängigkeit von S-Struktur $\mathcal{A}$ *und* Belegung β.

Herbrand-Struktur: die syntaktische Interpretation

für funktionales S (ohne Relationssymbole)

Herbrand-Struktur

$\mathcal{T} = \mathcal{T}(S) = \big(T(S), \ldots, c^{\mathcal{T}(S)}, \ldots, f^{\mathcal{T}(S)}, \ldots\big)$

- $c \in S$: $\quad c^{\mathcal{T}} := c \in T(S)$.
- $f \in S$ (n-st.): $\quad \begin{array}{rcl} f^{\mathcal{T}}\colon T(S)^n & \longrightarrow & T(S) \\ (t_1, \ldots, t_n) & \longmapsto & ft_1 \ldots t_n. \end{array}$

(die einzig plausible Wahl ..., warum?)

Beobachtung (Übung 1.7, vgl. auch FGdI I)

für jede S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ ist die Abbildung

$$\begin{array}{rcl} h\colon T(S) & \longrightarrow & A \\ t & \longmapsto & t^{\mathfrak{I}} \end{array}$$

ein Homomorphismus von $\mathcal{T}(S)$ nach $\mathcal{A}$.

Logik erster Stufe: Syntax von $\mathrm{FO}(S)$ → Abschnitt 2.1

Symbole: Symbole in S zusammen mit Variablen $x \in \mathcal{V}$, AL-Junktoren, $=$, $\forall, \exists$, Klammern

induktive Definition der Menge der $\mathrm{FO}(S)$ Formeln:

- **atomare Formeln**: für $t_1, t_2 \in T(S)$: $\quad t_1 = t_2 \in \mathrm{FO}(S)$.

  für $R \in S$ (n-st.)*, $t_1, \ldots, t_n \in T(S)$: $\quad Rt_1 \ldots t_n \in \mathrm{FO}(S)$.

  * für $n = 2$: auch infixe Notation
- **AL-Junktoren**: für $\varphi, \psi \in \mathrm{FO}(S)$: $\quad \neg\varphi \in \mathrm{FO}(S)$.

  $(\varphi \wedge \psi) \in \mathrm{FO}(S)$.

  $(\varphi \vee \psi) \in \mathrm{FO}(S)$.
- **Quantifizierung**: für $\varphi \in \mathrm{FO}(S)$, $x \in \mathcal{V}$: $\quad \exists x\varphi \in \mathrm{FO}(S)$.

  $\forall x\varphi \in \mathrm{FO}(S)$.

Gleichheitsfreie Logik erster Stufe, $\mathrm{FO}^{\neq} \subseteq \mathrm{FO}$:
genauso, aber ohne Atome $t_1 = t_2$.

Syntax: freie Variablen (Definition 2.2)

induktiv über Aufbau der Formeln definiere Funktion

$$\boxed{\begin{array}{rcl} \mathrm{frei}\colon \mathrm{FO}(S) & \longrightarrow & \mathcal{P}(\mathcal{V}) \\ \varphi & \longmapsto & \mathrm{frei}(\varphi) \subseteq \mathcal{V} \end{array}}$$

induktiv gemäß: $\mathrm{frei}(\varphi) := \mathrm{var}(\varphi)$ für atomare φ.
$\mathrm{frei}(\neg\varphi) := \mathrm{frei}(\varphi)$.
$\mathrm{frei}(\varphi \wedge \psi) = \mathrm{frei}(\varphi \vee \psi) := \mathrm{frei}(\varphi) \cup \mathrm{frei}(\psi)$.
$\mathrm{frei}(\exists x\varphi) = \mathrm{frei}(\forall x\varphi) := \mathrm{frei}(\varphi) \setminus \{x\}$.

Formeln ohne freie Variablen: **Sätze**

$\mathrm{FO}_n(S) := \{\varphi \in \mathrm{FO}(S) \colon \mathrm{frei}(\varphi) \subseteq \mathcal{V}_n\}$.

Schreibweise: $\varphi(x_1, \ldots, x_n)$ für $\varphi \in \mathrm{FO}_n(S)$.

Variablen in φ, die nicht frei vorkommen: *gebunden*

Beispiele: $\mathrm{frei}(0 < fx) = \{x\}$ $\quad \mathrm{frei}(0 < fx \wedge \forall x \neg x = fx) = \{x\}$
$\mathrm{frei}(\forall x \neg x = fx) = \emptyset$

Syntax: Quantorenrang (Definition 2.3)

induktiv über Aufbau der Formeln definiere Funktion

$$\boxed{\begin{array}{rcl} \mathrm{qr}\colon \mathrm{FO}(S) & \longrightarrow & \mathbb{N} \\ \varphi & \longmapsto & \mathrm{qr}(\varphi) \in \mathbb{N} \end{array}}$$

induktiv gemäß: $\mathrm{qr}(\varphi) = 0$ für atomares φ.
$\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi)$.
$\mathrm{qr}(\varphi \wedge \psi) = \mathrm{qr}(\varphi \vee \psi) := \max(\mathrm{qr}(\varphi), \mathrm{qr}(\psi))$.
$\mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\forall x\varphi) := \mathrm{qr}(\varphi) + 1$.

Formeln von Quantorenrang 0 heißen *quantorenfrei*.

Beispiele: $\mathrm{qr}(0 < fx) = 0$
$\mathrm{qr}(\forall x \exists y\, x < y) = 2$
$\mathrm{qr}(0 < fx \wedge \forall x \exists y\, x < y) = 2$