MLML VI

26. April 2021
Sommersemester 2021

INVARIANZ QUANTORENFREIER FORMELN UNTER EINBETTUNGEN

Lemma 1 Sei $\pi : \mathcal{A} \longrightarrow \mathcal{B}$ eine Einbettung von $\mathfrak{A}$ und $\mathfrak{B}$. Sei β eine Belegung in $\mathcal{A}$. Schreibe

$$\mathfrak{I} := (\mathfrak{A}, \beta)$$
$$\mathfrak{I}^{\pi} := (\mathfrak{B}, \beta^{\pi}).$$

Dann gilt:

(a) $\pi(\mathfrak{I}(t)) = \mathfrak{I}^{\pi}(t)$

(b) Sei φ ein Ausdruck, in dem keine Quantoren vorkommen [quantorenfreier Ausdruck]. Dann gilt

$$\mathfrak{I} \models \varphi \iff \mathfrak{I}^{\pi} \models \varphi.$$

Auszüge aus MLML V

(b) wird per Induktion über den Formelaufbau bewiesen. Allerdings, da wir die Beh. nur für quantorenfreie Ausdrücke formuliert haben, müssten wir Bed. (A5) nicht überprüfen.

Also verbleiben (A1), (A2), (A3), (A4):

(A3) und (A4) sind gänzlich trivial (folgt direkt aus Definition $\models$).

(A2) ist Bedingung (2) aus dem Begriff der Einbettung.

(A1) folgt direkt aus unserem Schritt (a).

Kurz etwas zu (A1) und Injektivität:

Sei $\varphi = t \equiv t'$

$$\begin{aligned}
\mathfrak{I} \models \varphi &\iff \mathfrak{I} \models t \equiv t' \\
&\overset{\text{Def.}}{\iff} \mathfrak{I}(t) = \mathfrak{I}(t') \\
&\iff \pi(\mathfrak{I}(t)) = \pi(\mathfrak{I}(t')) \\
&\overset{(a)}{\iff} \mathfrak{I}^{\pi}(t) = \mathfrak{I}^{\pi}(t') \\
&\overset{\text{Def.}}{\iff} \mathfrak{I}^{\pi} \models t \equiv t' \\
&\iff \mathfrak{I}^{\pi} \models \varphi
\end{aligned}$$

Äquivalenz hier verwendet die Injektivität von π.

Def. Wir nennen eine Folge von Zeichenketten $\xi_1, \dots, \xi_n$ eine U-Ableitung gdw für alle $1 \leq i \leq n$ gilt:

(U1) ξ_i ist ein quantorenfreier Ausdruck,

(U2) es gibt $j, k < i$ mit
$$\xi_i = (\xi_j \wedge \xi_k)$$

(U3) es gibt $j, k < i$ mit
$$\xi_i = (\xi_j \vee \xi_k)$$

(U4) es gibt $j < i$ und eine Variable x mit
$$\xi_i = \forall x \, \xi_j .$$

Falls ξ in einer U-Ableitung auftaucht, so heißt ξ universelle Formel.

Bem. ① Jede universelle Formel ist eine Formel [Beweis: Ind. über Formelaufbau].

② Universelle Formeln können keine Existenzquantoren enthalten.

Die rekursive Def. der universellen Formeln liefert unmittelbar ein

INDUKTIONSPRINZIP für universelle Formeln

Ang. E sei eine Eigenschaft von Zeichenketten, die

(U1) für alle qf. Formeln gilt

(A4∧) = (U2) falls sie für φ, φ' gilt, so für $(\varphi \wedge \varphi')$

(A4∨) = (U3) ebenso $(\varphi \vee \varphi')$

(A5∀) = (U4) falls sie für φ gilt und x eine Var. ist, so gilt sie für $\forall x \varphi$.

Dann hat jede universelle Formel Eigenschaft E.

Bsp. für universelle Formeln.

Def. Ein S-Satz φ heißt S-Gleichung falls es Terme t, t' gibt mit vorkommenden Variablen $x_1, \ldots, x_n$, so daß

$$\varphi = \forall x_1 \ldots \forall x_n\, t \equiv t'.$$

Bsp. $x^2+2x+3=0$

$$\forall x\ (x \otimes x) \oplus ((1 \oplus 1) \otimes x) \oplus (1 \oplus 1 \oplus 1) \equiv 0$$

Viele der Axiome in der Algebra sind Gleichungen:

A $\forall x \forall y \forall z\ (x \oplus y) \oplus z \equiv x \oplus (y \oplus z)$

ASSOZIATIV-GESETZ

N $\forall x\ \ x \oplus 0 \equiv x$

NEUTRALES ELEMENT $\forall x\ \ 0 \oplus x \equiv x$

I $\forall x \exists y\ (x \oplus y \equiv 0 \wedge y \oplus x \equiv 0)$

INVERSES ELEMENT

keine Gleichung

Nicht einmal eine universelle Formel !!

Gleichungen

UNIVERSELLE ALGEBRA

Falls S eine Sprache ist, für welche $S_R = \emptyset$ so nennen wir S-Strukturen auch

S-Algebren.

Eine Klasse $\mathcal{C}$ von S-Algebren heißt **gleichungsdefiniert**, falls es eine Menge Φ von S-Gleichungen gibt mit

$$\mathfrak{A} \in \mathcal{C} \Longleftrightarrow \mathfrak{A} \models \Phi .$$

In der Algebra wird so etwas auch als **Varietät** bezeichnet.

[Man beachte, daß in der Sprache der Körper, mit $+, \cdot, 0, 1$ die Terme exakt den Polynomen entsprechen. D.h. S-Gleichungen in dieser Sprache sind exakt die diophantischen Gleichungen.]

<u>Lemma 2</u> Falls $\pi: \mathfrak{A} \subseteq \mathfrak{B}$ [Einbettung von $\mathfrak{A}$ und $\mathfrak{B}$] und φ eine universelle Formel und $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation, so gilt

$$\underset{(\mathfrak{B}, \beta^{\pi}) =}{} \mathfrak{I}^{\pi} \models \varphi \Longrightarrow \mathfrak{I} \models \varphi . \quad {}_{= (\mathfrak{A}, \beta)}$$

$\mathfrak{I}^\pi \models \varphi \Rightarrow \mathfrak{I} \models \varphi$

Beweis Per Induktion nach Aufbau der universellen Formeln: (U1), (U2), (U3), (U4).

(U1) Lemma 1. zeigt bereits $\mathfrak{I}^\pi \models \varphi \Leftrightarrow \mathfrak{I} \models \varphi$ für qf. φ. ✓

(U2), (U3). Im Beweis von L1 hatten wir die Fälle (A4∧), (A4∨) bereits erledigt; aber (U2) = (A4∧) und (U3) = (A4∨).

(U4) Ang. $\varphi = \forall x \psi$ und die Beh. bereits gezeigt für ψ.

$\mathfrak{I}^\pi = (\mathfrak{B}, \beta^\pi)$

$$\mathfrak{I}^\pi \models \varphi \iff \mathfrak{I}^\pi \models \forall x \psi$$

$$\underset{\text{Def.}}{\iff} \text{für alle } b \in B \; (\mathfrak{I}^\pi)\tfrac{b}{x} \models \psi$$

(*)

nur eine Richtung, da π evtl. nicht surjektiv.

$$\implies \text{für alle } a \in A \; (\mathfrak{I}^\pi)\tfrac{\pi(a)}{x} \models \psi$$

$$\iff \text{f.a. } a \in A \; (\mathfrak{B}, \pi \circ \beta)\tfrac{\pi(a)}{x} \models \psi$$

$$\iff \text{f.a. } a \in A \; (\mathfrak{B}, \underbrace{\pi \circ (\beta\tfrac{a}{x})) }_{(\mathfrak{I}\frac{a}{x})^\pi} \models \psi$$

$$\iff \text{f.a. } a \in A \; (\mathfrak{I}\tfrac{a}{x})^\pi \models \psi$$

nur eine Richt. wg. IV

$$\overset{\text{IV}}{\implies} \text{f.a. } a \in A \; \mathfrak{I}\tfrac{a}{x} \models \psi \iff \mathfrak{I} \models \forall x \psi$$

q.e.d.

KOROLLAR

$[\pi = id]$

3.5.7 Substrukturlemma *Seien $\mathfrak{A}$ und $\mathfrak{B}$ S-Strukturen mit $\mathfrak{A} \subseteq \mathfrak{B}$, und sei $\varphi \in L_n^S$ universell. Dann gilt für alle $a_0, \ldots, a_{n-1} \in A$:*

$$\textit{Wenn } \mathfrak{B} \models \varphi[a_0, \ldots, a_{n-1}], \textit{ so } \mathfrak{A} \models \varphi[a_0, \ldots, a_{n-1}].$$

Korollar: Falls $\mathcal{E}$ eine Varietät ist und $\mathfrak{B} \in \mathcal{E}$ und $\mathfrak{A} \subseteq \mathfrak{B}$, so ist $\mathfrak{A} \in \mathcal{E}$.

M.a.W.: Varietäten sind unter Bildung von Substrukturen abgeschlossen.

Wichtiges Bsp. Im allgemeinen werden nicht-universelle Formeln nicht von Substrukturen erhalten. Standardbsp.

Sprache $S = \{+, \cdot, 0, 1\}$

Strukturen $(\mathbb{Q}, +, \cdot, 0, 1) = \mathfrak{Q}$

$(\mathbb{R}, +, \cdot, 0, 1) = \mathfrak{R}$

keine universelle Formel !!!

$\varphi = \boxed{\exists x}\; x \cdot x \equiv 1 + 1 \quad \longleftarrow \quad x^2 = 2$

Dann gilt $\mathfrak{R} \models \varphi$ und $\mathfrak{Q} \not\models \varphi$.

Aber $\mathfrak{Q} \subseteq \mathfrak{R}$, somit bleibt φ nicht beim Übergang auf Substr. erhalten.

Exkurs Substrukturen in der Algebra.

Gruppenaxiome in der Sprache $S=\{\underline{\oplus},\underline{\mathbb{O}}\}$

A $\forall x \forall y \forall z\ (x \oplus y) \oplus z \equiv x \oplus (y \oplus z)$

GLEICHUNG
$\Longrightarrow$ universell

N $\forall x\ \ x \oplus \mathbb{O} \equiv x$

$\forall x\ \ \mathbb{O} \oplus x \equiv x$

GLEICHUNGEN
$\Longrightarrow$ universell

$\forall x\,(x \oplus \mathbb{O} \equiv x \wedge \mathbb{O} \oplus x \equiv x)$
ist ebenfalls universell

I $\forall x \exists y\,(x \oplus y \equiv \mathbb{O} \wedge y \oplus x \equiv \mathbb{O})$

nicht universell

Was sind denn genau die S-Substrukturen einer Gruppe?

[Hoffnung: das sollten die Untergruppen der Gruppe sein.]

Bsp. Sei $(\mathbb{Z},+,0)$ die additive Gruppe der ganzen Zahlen. Dann ist

- $(\mathbb{N},+,0)$

eine S-Substruktur, aber natürlich keine Untergruppe von $\mathbb{Z}$.

Betrachte stattdessen die Sprache $S^* = \{\oplus, \mathbb{O}, \underset{\text{INVERSE}}{\ominus}\}$

$(\mathbb{Z}, +, 0, -)$ hat als S^*-Substrukturen exakt die Untergruppen von $\mathbb{Z}$.

<u>Beachte</u>: In S^* können wir I ersetzen durch:

$$I^* \quad \underbrace{\forall x \underbrace{\left(x \oplus \ominus x \equiv \mathbb{O} \wedge \ominus x \oplus x \equiv \mathbb{O} \right)}_{\text{qf}}}_{\text{universell}}$$

<u>Bem.</u> Sprache der Ringe $S := \{+, \cdot, 0\}$

$(\mathbb{Z}, +, \cdot, 0)$ als Ring betrachtet hat $(2\mathbb{Z}, +, \cdot, 0)$ als Unterring.

Aber in der Sprache der Eins-Ringe [unitale Ringe] $S^* = \{+, \cdot, 0, 1\}$ ist $2\mathbb{Z}$ keine S^*-Substruktur von $\mathbb{Z}$.

3.5.2 Isomorphielemma *Sind $\mathfrak{A}$ und $\mathfrak{B}$ isomorphe S-Strukturen, so gilt für alle S-Sätze φ:*

$$\mathfrak{A} \models \varphi \quad gdw \quad \mathfrak{B} \models \varphi.$$

Leichte Verstärkung, die man dann per Ind. beweisen kann:

Sei $\pi : \mathfrak{A} \cong \mathfrak{B}$ ein Isomorphismus, φ eine Formel [nicht notw. ein Satz] und $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation.

Da Teilausdrücke von Sätzen i.a. keine Sätze sind, gibt es kein natürliches Induktionsprinzip über den Formelaufbau, mit dem man etwas für alle Sätze beweisen könnte.

Dann gilt: $\mathfrak{I} \models \varphi \Leftrightarrow \mathfrak{I}^{\pi} \models \varphi$.

<u>Beweis</u> (der stärkeren Aussage):

Per Induktion nach dem Formelaufbau, also (A1), (A2), (A3), (A4), (A5).

Wir hatten im Beweis von Lemma 1 gesehen, daß die Induktionsschritte (A1) – (A4) alle bereits für π Einbettung gelten. Da jeder Iso eine Einbettung ist, gilt das hier also auch.

(A5) $\longrightarrow$ (A5$\forall$), (A5$\exists$)

Es gilt $\exists x \psi \dashv\models \neg \forall x \neg \psi$.

Somit reicht es (A3) und (A5$\forall$) zu zeigen, um (A5$\exists$) zu erhalten.

Es verbleibt (AS$\forall$).
Wir sehen uns den Beweis von (*) von S. 6 an und stellen fest, daß an zwei Stellen nur $\Rightarrow$ statt $\Leftrightarrow$ steht.
Bei einer liegt dies an der IV [das ist hier kein Problem], bei der anderen hatten wir gesehen, daß $\Leftrightarrow$ gilt, wenn π surjektiv ist. Und unser Iso π ist surjektiv. Somit ist (AS$\forall$) auch erledigt.

q.e.d.

Morgen in G3 betrachten wir eine nicht-triviale Anwendung des Isomorphielemmas: definierbare Teilmenge einer Struktur müssen unter Automorphismen erhalten bleiben.

§ 3.8 Substitution

[Letzter Abschnitt im ersten Teil der Logik]

Hier geht es um spitzfindige Syntaktische, die geschickt gelöst werden müssen.

Bsp. $\boxed{\varphi = \exists z \; z+z \equiv x}$ z

Dies ist eine Formel mit freier Variable x.

Als Bsp.struktur wähle $(\mathbb{N}, +) = \mathfrak{A}$,

$$\mathfrak{I} = (\mathfrak{A}, \beta)$$

Dann gilt:

$$\mathfrak{I} \models \varphi \Longleftrightarrow \beta(x) \text{ ist gerade.}$$

Dies sollte nicht von der Wahl der Variablen abhängen

z.B.
$$\varphi' = \exists z \; z+z \equiv y,$$

$$\mathfrak{I} \models \varphi' \Longleftrightarrow \beta(y) \text{ ist gerade.}$$

Idee: Substituiere x durch y in φ und erhalte φ': Analyse der Wahrheitsbedingung bleibt gültig.

Was geschieht, wenn ich x durch z substituiere?

$$\varphi'' = \exists z \; z+z = z$$

$\mathfrak{I} \models \varphi''$ ist immer wahr in der Struktur $\mathfrak{A} = (\mathbb{N}, +)$