

Algebraische Spezifikation von Software und Hardware V

Markus Roggenbach

Mai 2008

6a. Spezifikationen

Beweis: \sim ist eine Äquivalenzrelation

(r): “ $A \sim A$,” da id_A die gewünschten Eigenschaften erfüllt.

(s): “ $A \sim B$ impliziert $B \sim A$:” Sei $A \sim B$.

Dann existieren $f : A \rightarrow B$ und $g : B \rightarrow A$ so dass:

$$f \circ g = id_B \quad g \circ f = id_A$$

Vertauschen der Rollen von f und g liefert $B \sim A$.

(t) “ $A \sim B$ und $B \sim C$ impliziert $A \sim C$:”

Übungsaufgabe.

Bsp: Isomorphismen zwischen Algebren

sort Bool

op not: Bool -> Bool

$$A(\text{Bool}) = \{0, 1\}, \quad A(\text{not})(0) = 1, \quad A(\text{not})(1) = 0$$

$$B(\text{Bool}) = \{tt, ff\}, \quad A(\text{not})(tt) = ff, \quad A(\text{not})(ff) = tt$$

Def: Fortsetzen einer Variablen Evaluation entlang eines Hom

Sei Σ eine Signatur.

Seien A, B Σ -Algebren,

Sei $g : A \rightarrow B$ ein Homomorphismus.

Sei X ein Variablen System.

Sei $\mu : X \rightarrow A$ eine Variablen Belegung.

Dann ist $g \circ \mu : X \rightarrow B$ eine Variablen-Belegung zu B mit

$$(g \circ \mu)_s(x : s) = g_s(\mu_s(x)).$$

Lemma: Termauswertung entlang eines Hom

Mit den Definitionen wie vor sei $t \in T_{\Sigma}(X)$ ein Term.

Dann gilt:

Wenn $\mu^{\sharp}(t)$ definiert ist, dann ist auch $(g \circ \mu)^{\sharp}(t)$ definiert.

In diesem Fall gilt zudem:

$$(g \circ \mu)^{\sharp}(t) = g(\mu^{\sharp}(t)).$$

Lemma: Erfülltheit für isomorphe Algebren

Sei Σ eine Signatur.

Seien $A \sim B$ Σ -Algebren mit

Isomorphismen $g : A \rightarrow B$ und $h : B \rightarrow A$.

Sei X ein Variablen System.

Sei $\mu : X \rightarrow A$ eine Variablen Belegung.

Dann gilt für alle $\varphi \in FOL(\Sigma)$:

$$\mu \models_A \varphi \quad \text{impliziert} \quad (g \circ \mu) \models_B \varphi$$

Beweis: Induktion über die Formelstruktur

$$\varphi \equiv p(t_1, \dots, t_n)$$

- gelte $\mu \models_A p(t_1, \dots, t_n)$

daraus folgt nach Def:

- $\mu^\#(t_i)$ definiert für $i = 1 \dots n$
- $(\mu^\#(t_1), \dots, \mu^\#(t_n)) \in A(p)$

daraus folgt mit Lemma und Hom Def:

- $(g \circ \mu)^\#(t_i)$ definiert für $i = 1 \dots n$
- $(g \circ \mu)^\#(t_i) = g(\mu^\#(t_i))$ für $i = 1 \dots n$
- $g(\mu^\#(t_1), \dots, \mu^\#(t_n)) \in B(p)$

daraus folgt $(g \circ \mu) \models_B p(t_1, \dots, t_n)$

Die übrigen Basisfälle: zu Ihrem Vergnügen

$$\underline{\varphi \equiv t_1 = t_2}$$

$$\underline{\varphi \equiv t_1 = e = t_2}$$

$$\underline{\varphi \equiv \text{False}}$$

$$\underline{\varphi \equiv \text{def } t}$$

Induktionsschritt:

$$\underline{\varphi \equiv \psi_1 \wedge \psi_2}$$

- gelte $\mu \models_A \psi_1 \wedge \psi_2$

daraus folgt nach Def:

- $\mu \models_A \psi_1$ und $\mu \models_A \psi_2$

daraus folgt via Induktion

- $(g \circ \mu) \models_B \psi_1$ und $(g \circ \mu) \models_B \psi_2$

daraus folgt nach Definition

- $(g \circ \mu) \models_B \psi_1 \wedge \psi_2$

Und was könnte bei der Implikation passieren?

sort s

ops $o : s$

$f : s \rightarrow? s$

$$A(s) = \{1\}, \quad A(o) = 1, \quad A(f)(1) = \perp$$

$$B(s) = \{1\}, \quad B(o) = 1, \quad B(f)(1) = 1$$

Klar: A und B sind nicht isomorph.

Aber: $g : A \rightarrow B$ mit $g_s(1) = 1$ ist Hom.

Betrachte $(\forall x : s \bullet \text{def } f(x)) \Rightarrow \text{not}(\forall x : s \bullet f(x) = o)$

$$\underline{\varphi \equiv \psi_1 \Rightarrow \psi_2}$$

Wir betrachten nur den Fall $(g \circ \mu) \models_B \psi_1$

daraus folgt via Induktion

$$\mu \models_A \psi_1 \text{ (da } (g \circ \mu) \models_B \psi_1\text{!)}$$

- gelte $\mu \models_A \psi_1 \Rightarrow \psi_2$

daraus folgt nach Def:

- $\mu \models_A \psi_1$ impliziert $\mu \models_A \psi_2$

daraus folgt via Modus Ponens

- $\mu \models_A \psi_2$

daraus folgt via Induktion

- $(g \circ \mu) \models_B \psi_2$

daraus folgt nach Definition $(g \circ \mu) \models_B \psi_1 \Rightarrow \psi_2$

Und was könnte beim Allquantor passieren?

sorts s, t

op $f: s \rightarrow? t$

$A(s) = \{a\}, A(t) = \{1\}, A(f)(a) = 1$

$B(s) = \{a, b\}, B(t) = \{1, 2\}, B(f)(a) = 1, B(f)(b) = \perp$

Klar: A und B sind nicht isomorph.

Aber: $g: A \rightarrow B$ mit $g_s(a) = a, g_t(1) = 1$ ist Hom.

Betrachte $(\forall x : s \bullet def f(x))$

Ausstehender Beweis: Übungsaufgabe

Hinweis: Betrachten Sie die Mengen von Variablen-Belegungen, die bei der Quantifizierung in A bzw. in B entstehen können.

Theorem: FOL ist abgeschlossen unter Isomorphie

Seien $A \sim B$ Σ -Algebren.

Dann gilt für alle geschlossenen Formeln $\varphi \in FOL^=$ über Σ :

$$A \models \varphi \quad \text{gdw} \quad B \models \varphi$$

Korrolar I

$Mod(sp)$ ist abgeschlossen unter Isomorphismus.

Beweis

Sei $A \in Mod(Sp)$.

Sei $B \sim A$.

Sei Φ die Formelmenge von Sp .

Aus $A \in Mod(Sp)$ folgt

$A \models \varphi$ für alle $\varphi \in \Phi$

daraus folgt mit dem vorherigen Theorem:

$B \models \varphi$ für alle $\varphi \in \Phi$

daraus folgt via Def der Modellklasse:

$B \in Mod(Sp)$.

Def

Eine Spezifikation Sp heisst monomorph, wenn für alle $A, B \in Mod(Sp)$ gilt: $A \sim B$.

Korollar II :

Für monomorphe Spezifikationen gilt:

$$Sp \models \varphi \vee Sp \not\models \varphi$$