Formelblatt FGDI 3 <Marco.Moeller@macrolab.de>
Stand: 06.03.2006 - Version: 1.0.0
Erhältlich unter HTTP://PRIVAT.MACROLAB.DE
Diese Formelsammlung basiert auf der Vorlesung "Formale Grundlagen der Informatik - 3" von Prof. Dr. Christoph Walther an der Technischen Universität Darmstadt im Wintersemester 2005/06.

1 Korrektheit Reaktiver Systeme

Transitionssystem $\mathcal{T} = (S, \rightarrow, r)$

Zustände S

Transitionsrelation $\rightarrow \subseteq S \times S$

- infix notiert: $s \rightarrow t \Leftrightarrow (s,t) \in \rightarrow$

Anfangszustand $r \in S$a

Pfad der Länge n, mit $\forall i, 0 \leq i \leq n : s_i \rightarrow s_{i+1}$

$$w = s_0 \dots s_n$$

Ausführung falls $\forall i, 0 \leq i : s_i \rightarrow s_{i+1}$

$$p = s_0 s_1 \dots$$

Wörter S^*sind endlich, S^ω sind unendlich

Element $\rho(i)$ ist das i-te Element von ρ (ab 0 Zählen!)

Suffix ρ^i ist das bei i beginnende suffix von ρ (ab 0 Zählen!)

Kripke Struktur $\mathcal{K} = (S, \rightarrow, r, AP, \nu)$

Transitionssystem das zugrunde liegt $(S, \rightarrow, r)$

Grundaussagen Menge AP

Interpretationen der Grundaussagen $\nu : AP \rightarrow 2^S$

- Die Zustände haben als eine Menge von Flags

Bild $\nu^{-1}(\rho) \in \left(2^{AP}\right)^\omega$ kann jeder Ausführung ρ zugeordnet werden: $\nu^{-1}(\rho)(i) = \{a \in AP | \rho(i) \in \nu(a)\}$

erfüllt $\mathcal{K}$ erfüllt eine LTL Formel ϕ (geschrieben $\mathcal{K} \models \phi$) falls für alle bei r beginnenden Ausführungen ρ gilt, dass $\nu^{-1}(\rho) \subseteq [[\phi]]$

- Es kann sowohl $\mathcal{K} \not\models \phi$ als auch $\mathcal{K} \models \phi$ gelten!

LTL Formeln

- Ist $a \in AP$ so ist a eine Formel
- Sind ϕ_1, ϕ_2 Formeln, so auch $\neg\phi_1, \phi_1 \vee \phi_2, \mathrm{X}\phi_1, \phi_1 \mathrm{U} \phi_2$
- Jede Formel definiert eine Menge von Wörtern aus $\left(2^{AP}\right)^\omega$. Sei $\sigma \in \left(2^{AP}\right)^\omega$
- Semantik $[[\phi]] = \{\sigma | \sigma \models \phi\}$

gilt	falls
$\sigma \models a$	$a \in \sigma(0)$
$\sigma \models \neg\phi$	$\sigma \not\models \phi$
$\sigma \models \phi_1 \vee \phi_2$	$\sigma \models \phi_1$ oder $\sigma \models \phi_2$
$\sigma \models \mathrm{X}\phi$	$\sigma^1 \models \phi$
$\sigma \models \phi_1 \mathrm{U} \phi_2$	$\exists i : \left(\sigma^i \models \phi_2 \wedge \forall k < i : \sigma^k \models \phi_1\right)$

- $\phi_1 \wedge \phi_2 \equiv \neg(\neg\phi_1 \vee \neg\phi_2)$
- $\mathrm{true} \equiv a \vee \neg a$
- $\mathrm{false} \equiv \neg\mathrm{true}$
- $\mathrm{F}\phi \equiv \mathrm{true}\,\mathrm{U}\phi$
- $\mathrm{G}\phi \equiv \neg\mathrm{F}\neg\phi$
- $\phi_1 \mathrm{W} \phi_2 \equiv (\phi_1 \mathrm{U} \phi_2) \vee \mathrm{G}\phi_1$
- $\phi_1 \mathrm{R} \phi_2 \equiv \neg(\neg\phi_1 \mathrm{U} \neg\phi_2)$
- $\mathrm{X}(\phi_1 \vee \phi_2) \equiv \mathrm{X}\phi_1 \vee \mathrm{X}\phi_2$
- $\mathrm{X}(\phi_1 \wedge \phi_2) \equiv \mathrm{X}\phi_1 \wedge \mathrm{X}\phi_2$
- $\mathrm{X}\neg\phi \equiv \neg\mathrm{X}\phi$
- $\mathrm{F}(\phi_1 \vee \phi_2) \equiv \mathrm{F}\phi_1 \vee \mathrm{F}\phi_2$
- $\mathrm{G}\neg\phi \equiv \neg\mathrm{F}\phi$
- $\mathrm{G}(\phi_1 \wedge \phi_2) \equiv \mathrm{G}\phi_1 \wedge \mathrm{G}\phi_2$
- $(\phi_1 \wedge \phi_2)\,\mathrm{U}\psi \equiv (\phi_1 \mathrm{U}\psi) \wedge (\phi_2 \mathrm{U}\psi)$
- $\phi \mathrm{U}(\psi_1 \vee \psi_2) \equiv (\phi \mathrm{U}\psi_1) \vee (\phi \mathrm{U}\psi_2)$
- $\mathrm{F}\phi \equiv \mathrm{FF}\phi$
- $\mathrm{G}\phi \equiv \mathrm{GG}\phi$
- $\phi \mathrm{U}\psi \equiv \phi\,\mathrm{U}(\phi \mathrm{U}\psi)$
- $\mathrm{F} \equiv \phi \vee \mathrm{XF}\phi$
- $\mathrm{G} \equiv \phi \wedge \mathrm{XG}\phi$
- $\phi \mathrm{U}\psi \equiv \psi \vee (\phi \wedge \mathrm{X}(\phi \mathrm{U}\psi))$
- $\phi \mathrm{W}\psi \equiv \psi \vee (\phi \wedge \mathrm{X}(\phi \mathrm{W}\psi))$

Büchi-Automat $\mathcal{B} = (Q, \Sigma, \delta, q_0, F)$

Zustandsmenge (endlich) Q

Alphabet (endlich) Σ

Übergangsrelation $\delta \subseteq Q \times \Sigma \times Q$

Anfangszustand $q_0 \in Q$

akzeptierende Zustände $F \subseteq Q$

akzeptiert $\mathcal{B}$ akzeptiert $a_0 a_1 \dots \in \Sigma^\omega$, gdw.

- $(q_i, a_i, q_{i+1}) \in \delta$ für alle $i \geq 0$
- Es gilt $q_i \in F$ für unendlich viele i

Sprache $\mathcal{L}(\mathcal{B}) = \{\sigma \in \Sigma^\omega | \mathcal{B} \text{ akzeptiert } \sigma\}$

- von Büchi Automaten erkannte Sprachen heißen ω-regulär

Generalisierter Büchi Automat hat eine Menge $\mathcal{F} = \{F_1, \dots, F_n\}$ von Akzeptanzmengen. Er akzeptiert, falls unenedlich viele zustände in F_i für *jedes* i.

markiertes Produckt $\mathcal{B}_1 \times \mathcal{B}_2 = (Q, \Sigma, \delta, q_0, F)$

gegeben $\mathcal{B}_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ und $\mathcal{B}_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$

- $Q = Q_1 \times Q_2 \times \{1, 2\}$

gilt $\in \delta$	falls $\in \delta_1$	falls $\in \delta_2$	
$(\langle s,t,1\rangle, a, \langle s',t',1\rangle)$	(s,a,s')	(t,a,t')	$s \notin F_1$
$(\langle s,t,1\rangle, a, \langle s',t',2\rangle)$	(s,a,s')	(t,a,t')	$s \in F_1$
$(\langle s,t,2\rangle, a, \langle s',t',2\rangle)$	(s,a,s')	(t,a,t')	$t \notin F_2$
$(\langle s,t,2\rangle, a, \langle s',t',1\rangle)$	(s,a,s')	(t,a,t')	$t \in F_2$

- $q_0 = \langle q_1, q_2, 1\rangle$
- $F = F_1 \times Q_2 \times \{1\}$

LTL →generalisierter Büchi

gegeben LTL-Formel ϕ in Normalform, d.h. Negationen sind nach Innen geschoben.

gesucht $\mathcal{B}_\phi = (Q, \Sigma, \delta, q, F)$

Abschluss $Cl(\phi)$ einer Formel ϕ ist die Menge aller Unterformeln von ϕ und ihrer Negierungen

Alphabet $\Sigma = 2^{AP}$ mit AP den Atomen von ϕ

Zustände $Q =$ Elemente von $2^{Cl(\phi)}$, die folgende Zusatzbedingungen erfüllen

- $\forall \phi_1 \in Cl(\phi) : \neg\phi_1 \in Q \Leftrightarrow \phi_1 \notin Q$
- $\forall \phi_1 \wedge \phi_2 \in Cl(\phi) : \phi_1 \wedge \phi_2 \in Q \Leftrightarrow \phi_1 \in Q \wedge \phi_2 \in Q$
- $\forall \phi_1 \vee \phi_2 \in Cl(\phi) : \phi_1 \vee \phi_2 \in Q \Leftrightarrow \phi_1 \in Q \vee \phi_2 \in Q$

Anfangszustände, alle die ϕ enthalten

Übergänge $s \xrightarrow{l}_{\rightarrow} t$, falls $l = \{p \in AP | p \in s\}$, sowie

- $\forall \mathrm{X}\phi_1 \in Cl(\phi) : \mathrm{X}\phi_1 \in s \Leftrightarrow \phi_1 \in t$
- $\forall \phi_1 \mathrm{U} \phi_2 \in Cl(\phi) : \phi_1 \mathrm{U}\phi_2 \in s \Leftrightarrow \phi_2 \in s \vee (\phi_1 \in s \wedge \phi_1 \mathrm{U}\phi_2 \in t)$
- $\forall \phi_1 \mathrm{R} \phi_2 \in Cl(\phi) : \phi_1 \mathrm{R}\phi_2 \in s \Leftrightarrow \phi_1 \wedge \phi_2 \in s \vee (\phi_2 \in s \wedge \phi_1 \mathrm{R}\phi_2 \in t)$

Akzeptierende Zustände Für jede Unterformel der Form $\psi \equiv \phi_1 \mathrm{U} \phi_2$ gibt es eine Akzeptanzmenge F_ψ wie folgt:

- F_ψ ist die Menge der Zustände, die ϕ_2 oder $\neg\phi_1 \mathrm{R} \neg\phi_2$ enthalten

Kripke → Büchi

- gegeben: $\mathcal{K} = (S, \rightarrow, r, AP, \nu)$
- gesucht: $\mathcal{B}_\mathcal{K} = (Q, \Sigma, \delta, q, F)$
- $F = Q = S$
- $\Sigma = 2^{AP}$
- $(s, A, s') \in \delta \Leftrightarrow s \rightarrow s'$ und $A = \{p \in AP | s \in \nu(p)\}$
- $q = r$
- $\mathcal{K} \models \phi \Leftrightarrow \mathcal{L}(\mathcal{B}_\mathcal{K}) \subseteq [[\phi]] \Leftrightarrow \mathcal{L}(\mathcal{B}_\mathcal{K} \times \mathcal{B}_{\neg\phi}) = \emptyset$
  - $\mathcal{L} \neq \emptyset$ wenn Graph von ... enthält als Kreise mit Enzustand drin die erreichbar vom Start sind

SCC starke Zusammenhangskomponente heißt $S \subseteq Q$ gdw. für alle $q, q' \in S$ gilt $q \rightarrow^* q'$

- SCC heitßt *trivial* wenn $|S| = 1$ und für $q \in S$ gilt $q \nrightarrow q$
- $\mathcal{L} \neq \emptyset$ wenn Graph von ... nicht-trivial SCC enthält die erreichbar vom Start ist

Aktionen $\mathcal{K} = (S, A, \rightarrow, r, AP, \nu)$

- S, r, AP, ν wie bei Kripkestruktur
- A sei eine Menge von Aktionen
- $\rightarrow \subseteq S \times A \times S$
- Sei $(s, a, s') \in \rightarrow$ deterministisch, so dass sich schreiben lässt $s' = a(s)$
- $enabled(s) = \{a | \exists s' : (s, a, s') \in \rightarrow\}$

Unabhängigkeit $I \subseteq A \times A$ heißt *Unabhängigkeitsrelation* für $\mathcal{K}$, falls

- $\forall a \in A : (a, a) \notin I$
- $\forall (a, b) \in I : (b, a) \in I$
- $\forall (a, b) \in I, s \in S$: *Aktiviertheit*: $a, b \in enabled(s) \Rightarrow a \in enabled(b(s)) \wedge b \in enabled(a(s)) \wedge a(b(s)) = b(a(s))$
- a und b heißen unabhängig, falls $(a, b) \in I$

stotter äquivalenz sind zwei Abläufe einer Kripke Struktur σ und ρ, falls es Sequenzen $0 = i_0 < i_1 < i_2 < \ldots$ und $0 = j_0 < j_1 < j_2 < \ldots$ gibt, so dass für alle $k \geq 0$ gilt:
$\nu^{-1}(\sigma(i_k)) = \nu^{-1}(\sigma(i_k + 1)) = \ldots \nu^{-1}(\sigma(i_{k+1} - 1))$
$=$
$\nu^{-1}(\rho(j_k)) = \nu^{-1}(\rho(j_k + 1)) = \ldots \nu^{-1}(\rho(j_{k+1} - 1))$

- Eine LTL-Formel ϕ heißt *stotter-invariant*, gdw. für alle äquivalenten Abläufe σ und ρ gilt

$$\sigma \models \phi \Leftrightarrow \rho \models \phi$$

- Alle Formeln der LTL Logik ohne den X-Operator sind stotter-invariant
- Zwei Kripke $\mathcal{K}$ und $\mathcal{K}'$ Strukturen heißen stotter-äquivalent gdw.
  - sie den gleichen Anfangszustand haben
  - für jeden Ablauf σ in $\mathcal{K}$ es einen stotter-äquivalenten Ablauf ρ in $\mathcal{K}'$ gibt und umgekehrt.
- Stotter-invariante Formeln können stotter-äquivalente Kripkestrukturen nicht unterscheiden

Sichtbarkeit Eine Aktion a heißt *unsichtbar*, falls für alle $s, s' \in S$ gilt: Falls $(s, a, s') \in \rightarrow$, dann gilt $\nu^{-1}(s) = \nu^{-1}(s')$.

Ample sets $ample(s) \subseteq enabled(s)$ ist die Menge an Nachfolgerzuständen die tatsächlich überprüft werden muss, beim Testen auf Leerheit der Sprache. $\mathcal{K}$ wird also auf $\mathcal{K}_R$ reduziert.

- $C0$: $ample(s) = \emptyset \Leftrightarrow enabled(s) = \emptyset$
- $C1$: Auf jedem Pfad beginnend in s in $\mathcal{K}$ gilt: keine Aktion, die von einer Aktion in $ample(s)$ abhängt, kann vor einer Aktion in $ample(s)$ ausgeführt werden.
  Eine Aktion b, die von einer Aktion $a \in ample(s)$ abhängt, d.h. $(a, b) \notin I$, kann erst nach der Ausführung einer Aktion $c \in ample(s)$ ausgeführt werden.
- $C2$: Falls $ample(s) \subsetneq enabled(s)$, sind alle Aktionen in $ample(s)$ unsichtbar
- $C3$: Für alle Zyklen in $\mathcal{K}_R$gilt: falls $a \in enabled(s)$ für einen Zustand im Zyklus, dann $a \in ample(s')$ für einen Zustand s' im Zyklus

2 Korrektheit Sequentieller Systeme

Alle volgenden Sysmbole müssen eindeutig zuordbar sein $\Leftrightarrow$ alle Mengen sind disjunkt. Bei $\subset$ ist die gleichheit *nicht* ausgeschlossen

Sorten $S = (s_1, \ldots, s_n)$ wie Liste von Datentypen

Signatur $\Sigma = (\Sigma_{ws})_{ws \in S^* S}$ Angabe über Fuktionssymbole mit dazugehörigen Stelligkeiten und Sorten.
0-stellig = Konstante

Variablensymbole $\mathcal{V} = (\mathcal{V}_s)_{s \in S}$

- $\mathcal{V}(\phi)$ Menge aller Variablen Symbole in ϕ
- $\mathcal{V}_f(\phi) \subset \mathcal{V}(\phi)$ Menge aller freien Variablen Symbole in ϕ, also die nicht abquantifizierten

Terme $\mathcal{T}(\Sigma, \mathcal{V}) \subset (\mathcal{V} \cup \Sigma)^*$ Menge der syntaktisch korrekten Terme aus den angegebenen Funktionen und Variablen

Grundterme $\mathcal{T}(\Sigma)$ Terme ohne Variablen

sensible Signatur hat von jeder Sorte mindestens ein Konstantensymbol

Σ-**Algebra** ist paar $A = (\mathcal{A}, \alpha)$ mit

Trägermengen $\mathcal{A} = (\mathcal{A}_s)_{s \in S}$

Deutungsfunktionen $\alpha = (\alpha_f)_{f \in \Sigma}$ die Signatur von f respektiert

Deutung $A : \mathcal{T}(\Sigma) \to_S \mathcal{A}$ bei gegebener Σ-Algebra A

Formeln $\mathcal{F}(\Sigma, \mathcal{V}) \subset (\mathcal{V} \cup \Sigma \cup \{\equiv, \neg, \wedge, \forall\})^*$

- Sprache wird auch um andere gewohnte boolsche Operatoren erweitert
- $\mathcal{F}_g$ Menge der geschlossenen Formeln, enthalten *keine* freien Variablen

Atomare Formeln $\mathcal{AT}(\Sigma, \mathcal{V}) \ni t_1 \equiv t_2$ mit $t_1, t_2 \in \mathcal{T}(\Sigma, \mathcal{V})$

pränexe Normalform ist eine Formel ϕ wenn alle Quantoren $(\forall, \exists)$ ganz links stehen.

universelle Formeln wenn pränex und alle Quantoren $\forall$
$\mathcal{F}_\forall(\Sigma, \mathcal{V})$ ist Menge aller solcher Formeln über geg. Signatur

Gleichung siehe Atomate Formel $\mathcal{E}(\Sigma, \mathcal{V}) = \mathcal{AT}(\Sigma, \mathcal{V})$

universelle Gleichung universelle Formel, die hinter den Quantoren nur nich genau ein $=$ steht
$\mathcal{E}_\forall(\Sigma, \mathcal{V})$ ist die Menge aller solcher universellller Geichungen

Allabschluss für ein $e \in \mathcal{E}(\Sigma, \mathcal{V})$ ist $\forall e$ die Gleichung, in der alle freien Variablen abquantifiziert wurden. Analog für Formelmengen.

Σ-**Interpretation** ist ein Paar $I = (A, \mathfrak{a})$ mit der Σ-Algebra A und $\mathfrak{a} : \mathcal{V} \to_S \mathcal{A}$.

Deutung von Formel: α auf Funktionen und $\mathfrak{a}$ auf Variablen rekursiv anwenden. Atomare Formeln liefern bool. Dieses mit Boolschen Funktionen verknüpfen.
$I \models_{Alg(\Sigma)} \phi \Leftrightarrow$ die Σ-Interpretation I erfüllt eine Formel $\phi \in \mathcal{F}(\Sigma, \mathcal{V})$ gdw. die Auswertung true liefert.

erfüllbar ist ϕ gdw. es einer Σ-Interpreation I gibt die Formel ϕ erfüllt

allgemeingültig ist ϕ gdw. jede Σ-Interpreation I die Formel ϕ erfüllt

folgt $\Phi \models_{\mathcal{F}(\Sigma,\mathcal{V})} \phi \Leftrightarrow$ eine Formel ϕ folgt aus einer Formelmenge Φ, gdw. alle Interpretationen die Φ wahr machen, auch ϕ wahr machen.

Folgerungen $\Phi^{\models \mathcal{F}(\Sigma,\mathcal{V})}$ ist die Menge aller Folgerungen aus Φ

allgemeingültig wenn $\emptyset \models_{\mathcal{F}(\Sigma,\mathcal{V})} \phi$

äquivalent $\phi_1 \approx \phi_2$ gdw. $\phi_1 \leftrightarrow \phi_2$ allgeimeingültig

Theorie $Th(A) := \{\phi \in \mathcal{F}_g(\Sigma, \mathcal{V}) \,|\, A \models \phi\}$ zu gegebener Σ-Algebra A

- ist angeschlossen und vollständig ϕ oder $\neg\phi$sind (nicht)enthalten in $Th(A)$
- $Th(A) \subset Th(B) \Rightarrow Th(A) = Th(B)$

Substitution $\sigma : \mathcal{V} \to_S \mathcal{T}(\Sigma, \mathcal{V})$

- rekursiv erweitern für gesamte Terme

Grundsubstitution $\sigma(x) \in \mathcal{T}(\Sigma, \mathcal{V}) \cap \{x\}$ für alle $x \in \mathcal{V}$

Substitutionlemma $\mathfrak{a}(\sigma(t)) = \mathfrak{a}[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)](t)$

- $A \models \forall l \equiv r \Rightarrow A \models \sigma(l) \equiv \sigma(r)$ für bel. Substitution σ

Klasse der Σ-Algebren Alg_Σ

- Für $\Phi \subset \mathcal{F}_g(\Sigma, \mathcal{V})$ ist $\mathrm{Mod}_\Sigma(\Phi) \subset \mathrm{Alg}_\Sigma$ die Klasse aller Σ-Algebren A mit $A \models \Phi$

Σ-**Homomorphismus** Für A, B Σ-Algebren ist $h : \mathcal{A} \to_S \mathcal{B}$ ein Homomorphismus wenn

$$h_s(\alpha_f(a_1, \ldots, a_n)) = \beta_f(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$$

- $id^A : A \to A$ ist Homomorphismus
- Verkettung von Homomorphismen ist wieder Homomorphismus
- $h(A(t)) = B(t)$ für alle $t \in \mathcal{T}(\Sigma)$

Äquivalenzrelation ist $\sim \in M \times M$ wenn

reflexiv $m \sim m$

symmetrisch $m \sim n \Leftrightarrow n \sim m$

transitiv $m \sim n \wedge n \sim k \Rightarrow m \sim k$

- Für Mengen M, N und $f : M \to N$ ist $\sim_F$ definiert durch $m_1 \sim_F m_2 \Leftrightarrow F(m_1) = F(m_2)$ eine Äquivalenzrelation
- Äquivalenzklassen sind disjunkte Zerlegung der Gesamtmenge

Äquivalenzklasse $[m]_\sim = \{n \in M | n \sim m\} \subset 2^M$

Quotientenmenge $M/_\sim = \left\{[m]_\sim \in 2^M | m \in M\right\}$

Σ-**Isomorphismus** ist eine bijektiver Homomorphismus

- $A \simeq_\Sigma B$ sind zwei Σ-Algebren, wenn ein isomorphismus zwischen ihnen exisitert
- $\simeq_\Sigma$ ist Äquivalenzrelation
- Isomorphe Algebren haben gleiche Theorie

Abstrakter Datentyp für eine Signatur Σ ist eine Klasse $\mathrm{C} \subset \mathrm{Alg}_\Sigma$ von Σ-Algebren, die unter Isomorphie abgeschlossen ist, d.h. es gilt für alle $A, B \in \mathrm{Alg}_\Sigma$

- $A \in \mathrm{C} \Rightarrow (A \simeq_\Sigma B \Rightarrow B \in \mathrm{C})$

monomorph heißt C falls $A \in \mathrm{C} \Rightarrow (B \in \mathrm{C} \Rightarrow A \simeq_\Sigma B)$

polymorph andernfalls

initial ist eine Σ-Algebra $A \in \mathrm{Alg}_\Sigma$ gdw. gilt: Für jede Σ-Algebra B existiert *genau ein* Σ-Homomorphismus von A nach B.

- gilt $A \simeq_\Sigma B$ ist auch B initial

Termalgebren Sei Σ eine Signatur bzgl. einer Sortenmenge S. Dann ist die Termalgebra $T_\Sigma = (\mathcal{T}(\Sigma), \tau)$ definiert durch

$$\tau_f(t_1, \ldots, t_n) := f t_1 \ldots t_n$$

- Diese Termalgebra ist inital in der Klasse aller Σ-Algebren

Kongruenzrelation ist $\approx \subset (\mathcal{A}_s \times \mathcal{A}_s)_{s \in S}$ wenn:

- $\approx_s$ ist Äquivalenzrelation
- Kongruenzeigenschaft
$a_1 \approx_{s_1} a_1' \wedge \ldots \wedge a_n \approx_{s_n} a_n' \Rightarrow \alpha_f(a_1, \ldots, a_n) \approx_s \alpha_f(a_1', \ldots, a_n')$

Kongruenzklasse $[a]_{\approx_s}$ analog Äquivalenzklasse

Quotientenmenge $\mathcal{A}_s/_{\approx_s}$ analog ...

Quotientenalgebra ist eine Σ-Algebra zu gegebenen A und $\approx$: $A/_\approx := \left(\mathcal{A}/_\approx, \tilde{\tilde{\alpha}}\right)$ mit

$$\tilde{\tilde{\alpha}}_f\left([a_1]_{\approx_{s_1}}, \ldots, [a_n]_{\approx_{s_n}}\right) := [\alpha_f(a_1, \ldots, a_n)]_{\approx_s}$$

Quotiententermalgebra Für eine Σ-Algebra A sei $\approx_A \subset \mathcal{T}(\Sigma) \times \mathcal{T}(\Sigma)$ für alle $t_1, t_2 \in \mathcal{T}(\Sigma)$ definiert durch

$$t_1 \approx_A t_2 \Leftrightarrow A(t_1) = A(t_2)$$

die Quotiententermalgebra von A ist dann definiert als $T_\Sigma/_{\approx_A} = \left(\mathcal{T}(\Sigma)/_{\approx_A}, \overset{\approx_A}{\tau}\right)$

- Für Variablenbelegung t und Term t gilt $\mathrm{t}(t) = [t]_{\approx_A}$

kanonische Termalgebra heißt $A(\mathcal{A}, \alpha)$ gdw.: $\mathcal{A} \subset \mathcal{T}(\Sigma)$ und $\forall t \in A : A(t) = t$

Teilsignatur ist eine Signatur, bei der einige Funktionssymbole weggleassen wurden

Erzeugte Σ-Algebra Seien Σ^c und Σ S-Signaturen mit $\Sigma^c \subset \Sigma$ und sei $A = (\mathcal{A}, \alpha)$ eine Σ-Algebra. Dann ist A durch Σ^c *erzeugt* gdw. gilt: $\forall s \in S, a \in \mathcal{A}_s : \exists q \in \mathcal{T}(\Sigma_s^c) : a = A(q)$

- bei erzeugter Algebra sind alle Trägermengen abzählbar
- A initial $\Rightarrow$ A erzeugt
- A erzeugt $\Rightarrow$ $A \simeq_\Sigma T_\Sigma/_{\approx_A}$
- Sei $h : A \to B$ Homomorphismus ist eindeutig, falls A erzeugt
- erzeugte Algebren mit gleicher Theorie sind isomorph

frei erzeugt wenn zusätzlich gilt $\forall s \in S, q_1, q_2 \in \mathcal{T}(\Sigma_s^c) : A(q_1) = A(q_2) \Rightarrow q_1 = q_2$
$\mathrm{Gen}_\Sigma \subset \mathrm{Alg}_\Sigma$ bezeichnet die Klasse aller erzeugten Σ-Algebren

- (frei) erzeugtheit vererbt sich durch Isomorphie und Quotiententermalgebra bildung
- alle Konstruktoren werden als injektive Funktionen gedeutet
- Es existiert eine isomorphe kanonische Termalgebra T_A zu A

Redukt ist Reduzierte Algebra zu kleinerer Signatur

- A durch $\Sigma^c \subset \Sigma$ erzeugt und sei A^c das Σ^c Redukt von A
  A freu erzeugt durch $\Sigma^c \Leftrightarrow A^c \simeq_{\Sigma^c} T_{\Sigma^c}$

Expansion ist vollständige Algebra zu großer Signatur

Kongruenz aus Relation Sei A eine Σ-Algebra, und $R =\subset (\mathcal{A}_s \times \mathcal{A}_s)$. Es existiert eine kleinste Kongruenzrelation $\approx_R$ die R noch enthält

Kongruenz aus Gleichung Für $E \subset \mathcal{E}(\Sigma, \mathcal{V})$ ist

$$R_E : = \{(\theta(l), \theta(r)) \in \mathcal{T}(\Sigma) \times \mathcal{T}(\Sigma) \mid l \equiv r \in E \wedge \theta \text{ ist Substitution}\}$$

und $\approx_E := \approx_{R_E}$

- Für alle $E \subset \mathcal{E}(\Sigma, \mathcal{V})$gilt $T_\Sigma/_{\approx_E} \models \forall E$
- Sei $E \subset \mathcal{E}(\Sigma, \mathcal{V})$ .Dann ist $T_\Sigma/_{\approx_E}$ initial in $\mathrm{Mod}_\Sigma(\forall E)$

Vorgehen Gegeben sei S, $\Sigma^c \subset \Sigma$ und $E \subset \mathcal{E}(\Sigma, \mathcal{V})$, so dass $T_{\Sigma/\approx_E}$ eine durch Σ^c freu erzeugte Quotiententermalgebra ist.

- Wir erweitern S zu S', Σ^c zu $\Sigma^{c'}$, Σ^d zu $\Sigma^{d'}$und E zu $E' \subset \mathcal{E}'(\Sigma', \mathcal{V})$
- Wir benötigen Gleichungen nur, wenn wir Σ^d um ein neues Funktionssymbol f zu $\Sigma^{d'}$ erweitern.
- Solch eine Gleichungsmenge $E' \backslash E$ muß garantieren, daß $T_{\Sigma'}/_{\approx_{E'}}$ durch Σ^c frei erzeugt ist, d.h. für alle $q_i \in \mathcal{T}(\Sigma^c)$ein $q \in \mathcal{T}(\Sigma^c)$mit
  $$T_{\Sigma'}/_{\approx_{E'}}(f q_1 \ldots q_n) \in [q]_{\approx_{E'}}$$
  existiert und für alle $q \in \mathcal{T}(\Sigma^c)$
  $$\mathcal{T}(\Sigma^c) \cap [q]_{\approx_{E'}} = \{q\}$$
  gilt. Wir nennen solche Gleichungsmengen $E' \backslash E$ *zulässig*.
- $\overset{E}{\tau}_f(q_1, \ldots, q_n) := q$ gdw. $\overset{\approx_E}{\tau}_f([q_1]_{\approx_E}, \ldots, [q_n]_{\approx_E}) = [q]_{\approx_E}$ definiert eine frei erzeugte kanonische Termalgebra $T_{\Sigma,E} = \left(\mathcal{T}(\Sigma^c), \overset{E}{\tau}\right)$ für die gilt $T_{\Sigma,E} \simeq_\Sigma T_\Sigma/_{\approx_E}$

structure struct $<= cons_1(sel_{1,1} : sct_{1,1}, \ldots, sel_{1,n_1} : sct_{1,n_1}), \ldots$

- $sct_{i,h} \in (S \backslash \{bool\}) \cup \{struct\}$ für alle $i \in \{1, \ldots, k\}$ und alle $h \in \{1, \ldots, n_i\}$. $(sct = struct)$
- $n_i \geq 0$ für alle $\{1, \ldots, k\}$
- Anzahl der Konstruktoren: $k \geq 1$

Axiome EQ_{struct}

- Gleichheit von Konstanten $eq_{struct}(cons_i, cons_i) \equiv true$
- Gleichheit von längeren Konstruktoren (geschachtelt, allquantifiziert) $eq_{struct}(cons_i(\ldots), cons_i(\ldots)) \equiv eq(eq(\ldots))$
- Nichgleichheit bei führenden Konstruktoren $eq_{struct}(cons_i(\ldots), cons_j(\ldots)) \equiv false$
- Falsch angewendete Selektoren liefern Beispielterm (Konstante)
- Selektoren $\forall x_1 : struct_{i,1} \ldots . sel_{i,h}(cons_i(\ldots)) \equiv x_h$
- $if_{struct}(true, x, y) \equiv x$
  $if_{struct}(false, x, y) \equiv y$

function $proc(x_1 : struct_1, \ldots, x_k : struct_k) : struct <= R_{proc}$

- x_i Parameter vom Typ $struct_i$
- name $Proc$ und Rückgabe vom Typ $struct$
- R_{proc} ist Rumpf und muss sich zu $struct$ auswerten lassen

konstruktive Spec. S ist eine Folge $\langle D_0, \ldots, D_n \rangle$ von Datenstruktur- und Prozedurdefinitionen.

- $S(0) = \{bool\}$, $\Sigma(0)^c_{bool} = \{true, false\}$, $\Sigma(0)^c_{bool,bool,bool,bool} = \{if_{bool}\}$
- $S, \Sigma^c, \Sigma^d, E, \mathcal{V}$ sind Funktionen von $i \to$ nummer der konstruktionsiteration
- $\langle D_0, \ldots, D_n \rangle \oplus D = \langle D_0, \ldots, D_n, D \rangle$

zulässige Spec. Eine Konstruktive Spezifikation $S = \langle D_0, \ldots, D_n \rangle$ ist zulässig, gdw. die $\Sigma(n)$-Algebra $T_{\Sigma(n)}/_{\approx_{E_n}}$ frei erzeugt durch $\Sigma(n)^c$ ist

- Datenstrukturdefinitionen sind automatisch zulässig in Verifun

prozedur Relation für gegebenes $proc$ ist

$$>_{proc} \subset \left(\mathcal{T}(\Sigma^c)_{struct_1} \times \ldots \times \mathcal{T}(\Sigma^c)_{struct_n}\right)^2$$

$(q_1, \ldots, q_n) >_{proc} (q'_1, \ldots, q'_n)$ gdw. beim Aufruf von $proc(q_1, \ldots, q_n)$ wird $proc(q'_1, \ldots, q'_n)$ rekursiv aufgerufen

- Eine Prozedur terminiert und damit ist ihre Definition zulässig, gdw. $>_{proc}$ fundiert ist.

Fundierte Relation Eine Relation $\succ \subset M \times M$ heißt fundiert gdw. es gibt keine unendliche Folgen $m_0, m_1, \ldots$ mit $m_i \succ m_{i+1}$ für alle $i \in \mathbb{N}$