Die intuitionistische Natur von Statecharts

Gerald Lüttgen
Department of Computer Science
The University of Sheffield
www.dcs.shef.ac.uk/~luettgen

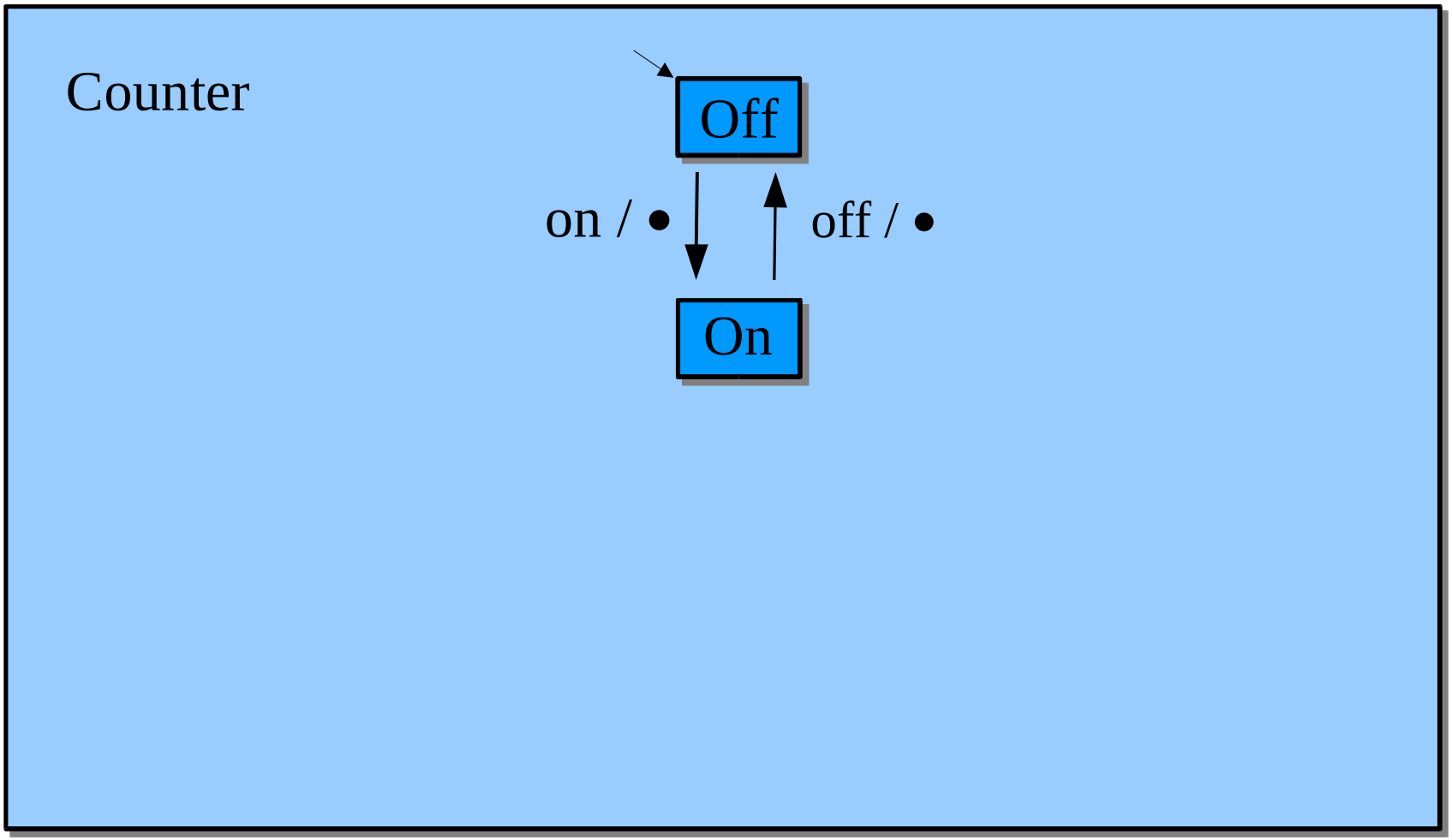
Gemeinsame Arbeit mit Michael Mendler,
The University of Sheffield

Statecharts [Harel 1987, Pnueli/Shalev 1991]

- Visuelle Entwurfssprache für reaktive Systeme mit global synchroner und lokal asynchroner Semantik
- Erweiterung von endlichen Automaten um
  - Hierarchie (ODER−Zustände)
  - Nebenläufigkeit (UND−Zustände)
  - Prioritäten (negierte Ereignisse)
- Vielfältige Anwendungen für eingebettete Systeme im Automobil− und Luftfahrtbereich
- Integration in zahlreichen Entwurfswerkzeugen, wie z.B. Statemate, Rhapsody, Matlab/Simulink, EsterelStudio

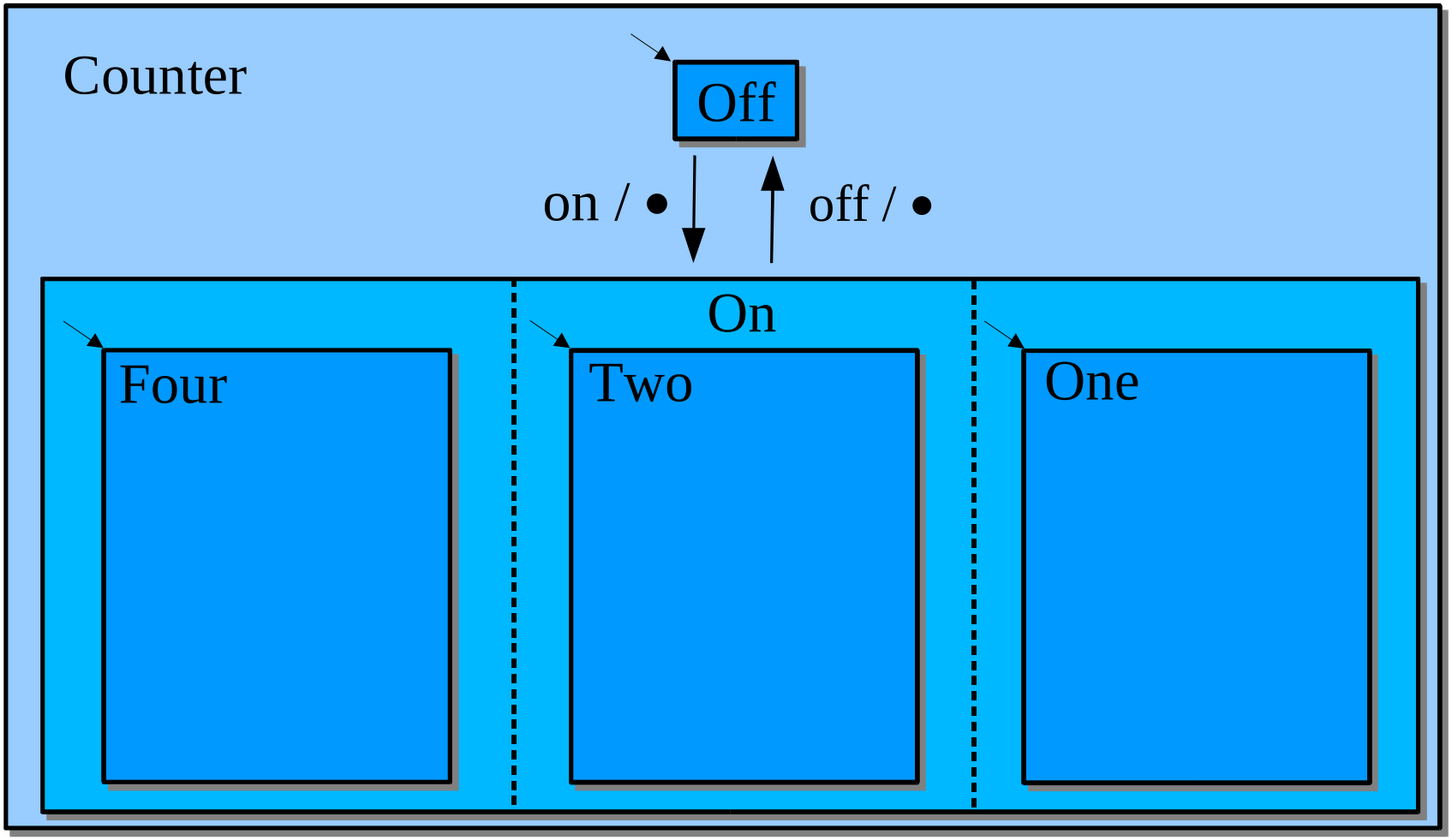
©2001 G. Lüttgen & M. Mendler

Beispiel: 3−Bit Zähler

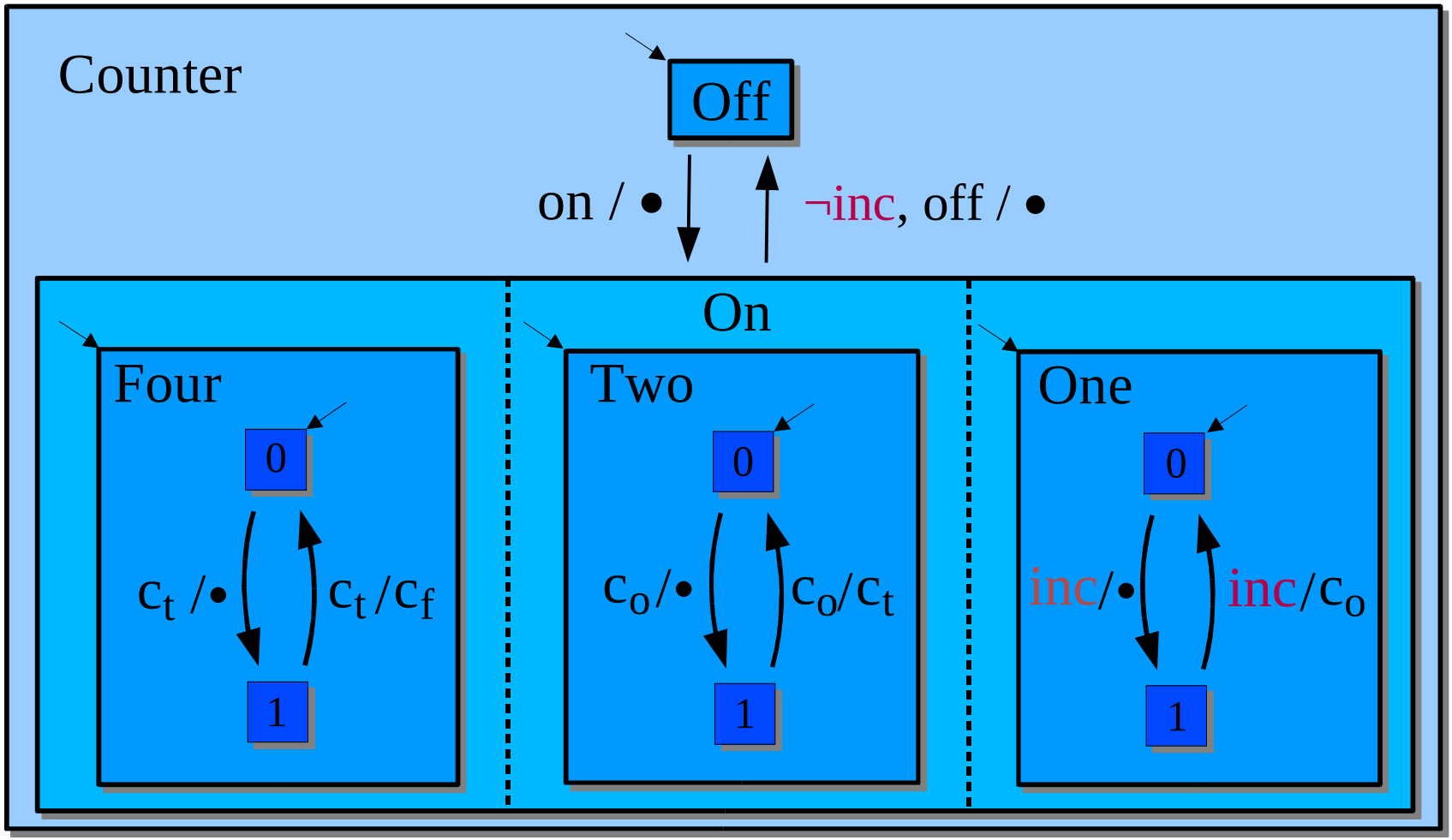


©2001 G. Lüttgen & M. Mendler

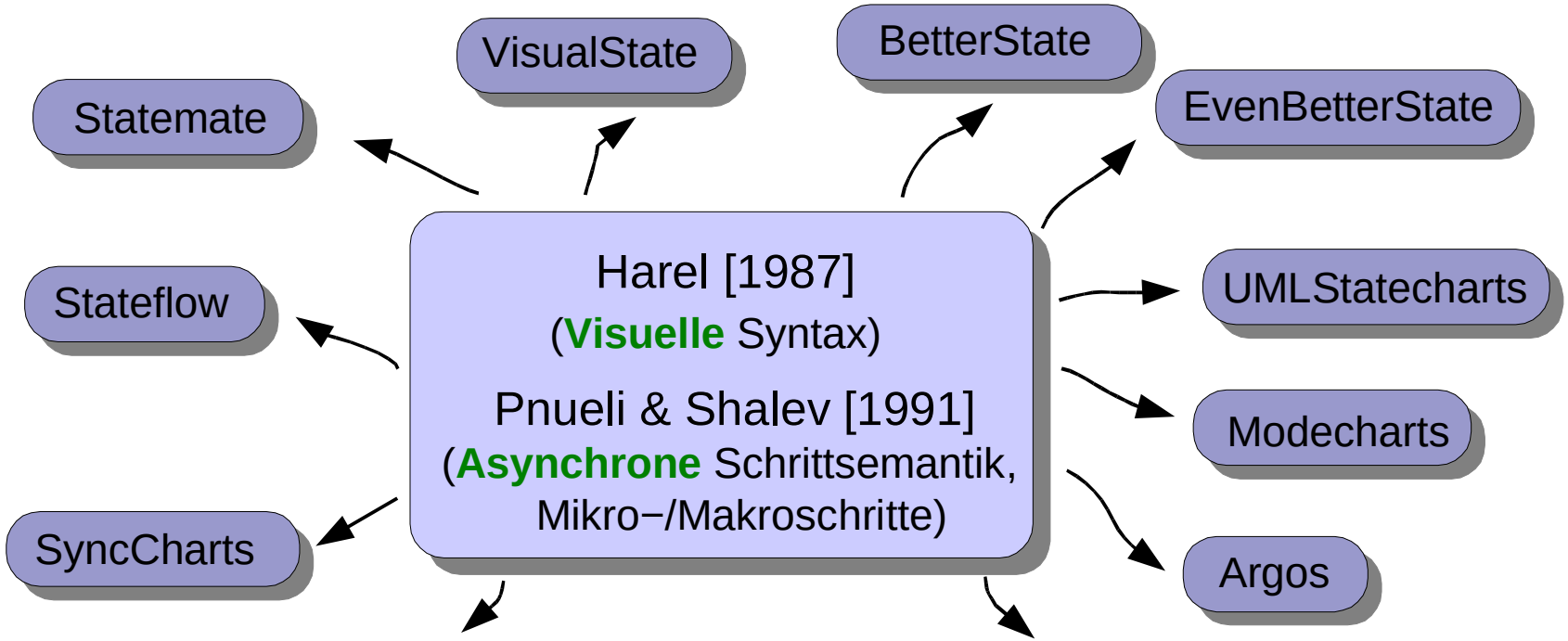
Beispiel: 3–Bit Zähler



Beispiel: 3–Bit Zähler



Statecharts



Heute: Vielzahl von Varianten (meist semantische Vereinfachungen, insbesondere synchron, weil einfacher zu implementieren).

Aber: Ist Pnueli/Shalevs asynchrone Semantik wirklich schwieriger?

©2001 G. Lüttgen & M. Mendler

Übersicht

Formalisierung:

Modelltheoretische Semantik für Pnueli/Shalev Statecharts

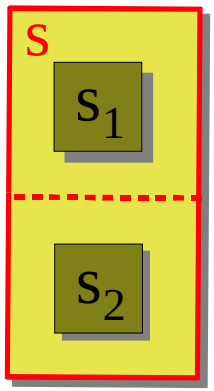
Eigenschaften:

- Shallow Embedding: "Syntax = Formel, Semantik = Modell"
  Jedes grafische Element entspricht logischem Prädikat.
- Inkrementell und kompositionell
- Kompakt: verwendet nur (intuitionistische) Aussagenlogik

⇒ "Ursprüngliche" Statecharts Semantik ist wesentlich einfacher zu handhaben als allgemein angenommen **...**

©2001 G. Lüttgen & M. Mendler

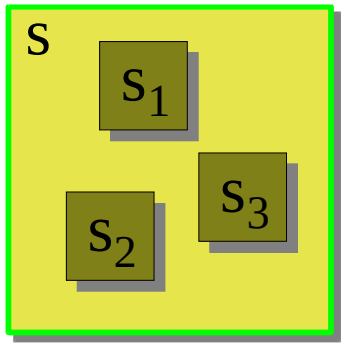
Statecharts Zustände



UND−Zustand s:

s aktiv ⇔ s_1 aktiv und s_2 aktiv

s inaktiv ⇔ s_1 und s_2 inaktiv



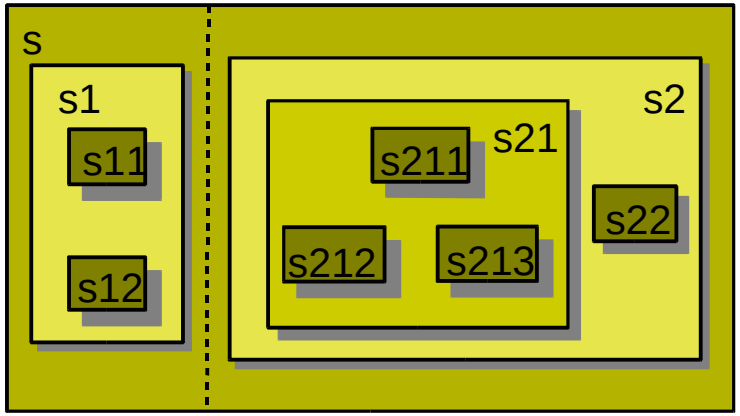
ODER−Zustand s:

s aktiv ⇔ entweder s_1 aktiv oder s_2 aktiv oder s_3 aktiv

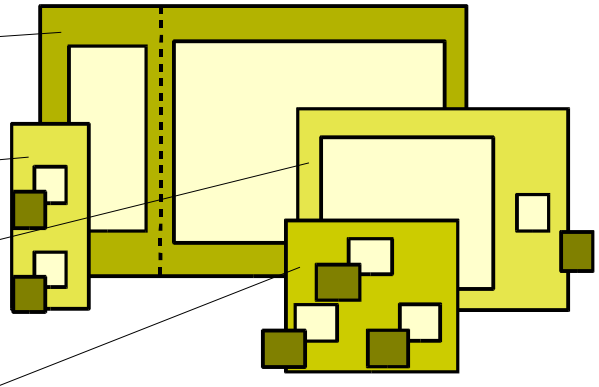
s inaktiv ⇔ s_1 und s_2 und s_3 inaktiv

©2001 G. Lüttgen & M. Mendler

Zustandssemantik = Konfigurationen



=



s≡s1 ∧ s≡s2

s1≡(s11∨s12) ∧
(s11∧s12)≡false

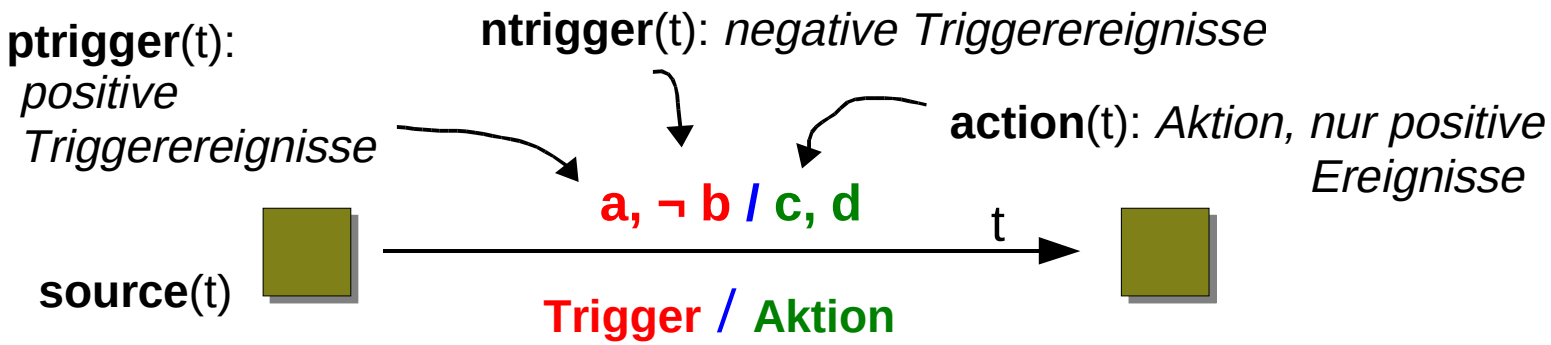
s2≡(s21∨s22) ∧ (s21∧s22)≡false

s21≡(s211∨s212∨s213) ∧
(s211∧s212)≡false ∧ (s211∧s213)≡false ∧
(s212∧s213)≡false

©2001 G. Lüttgen & M. Mendler

Statecharts Transitionen

Ereignisse $\mathcal{E}$ = {a, b, c, d, ...} **Transitionen** $\mathcal{T}$ = {t, t1, t2, t3, ...}



"wenn a anwesend und b abwesend, dann erzeuge c und d"

Transitionssemantik = Makroschritte

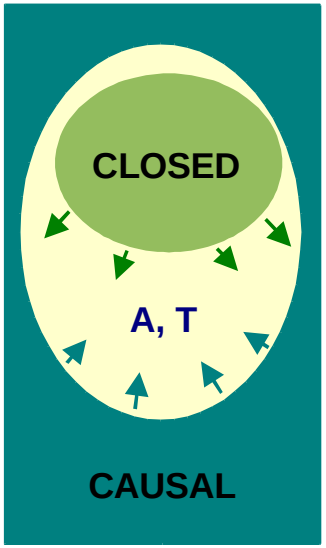
C: Konfiguration (aktive Zustände)
E: Umgebungsereignisse

A: Ereignisse im Makroschritt
T: Transitionen im Makroschritt

STEP (C,E,A,T) := **CLOSED** (C,E,A,T) $\wedge$ **CAUSAL** (C,E,A,T)

CLOSED: "*E und alle Aktionen von T sind in A, und alle durch A aktivierten Transitionen, die mit T schalten können, sind in T enthalten.*"

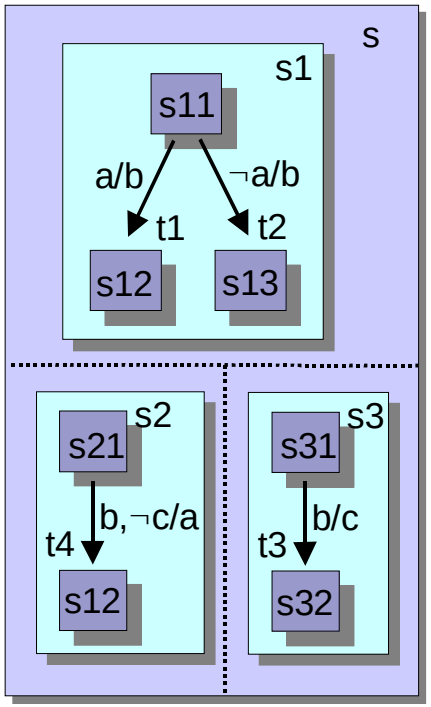
CAUSAL: "*A und T enhalten keine Aktionen oder Transitionen, die nicht kausal begründet werden können.*"



©2001 G. Lüttgen & M. Mendler

Beispiel

$E = \emptyset$



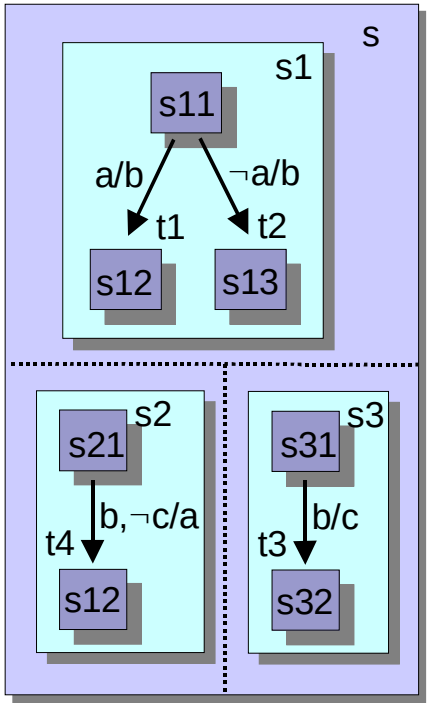
CLOSED (C, $\emptyset$, A, T) :=

$\forall e.$ **PRODUCED** ($\emptyset$, T, e) $\supset$ A(e) $\wedge$

$\forall t.$ **ENABLED** (C, A, T, t) $\supset$ T(t)

Beispiel

$E = \emptyset$



CLOSED (C, $\emptyset$, A, T) :=

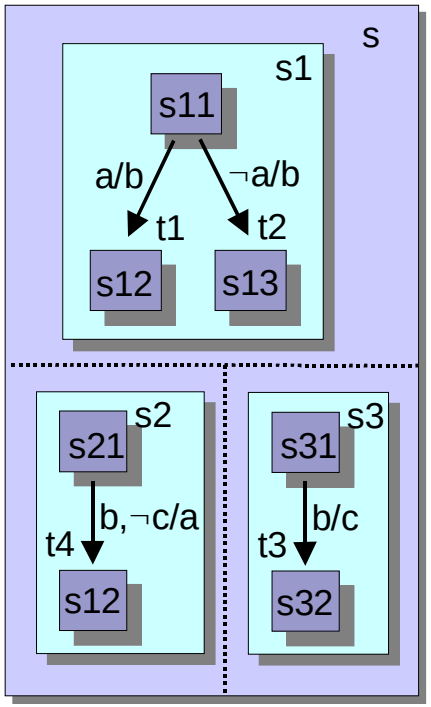
$\forall e.\ \emptyset(e) \supset A(e) \ \wedge$

$\forall e.\forall t.\ (T(t) \wedge \text{action}(e, t)) \supset A(e) \ \wedge$

$\forall t.$ **ENABLED** (C, A, T, t) $\supset$ T(t)

Beispiel

$E = \emptyset$



CLOSED (C, $\emptyset$, A, T) :=

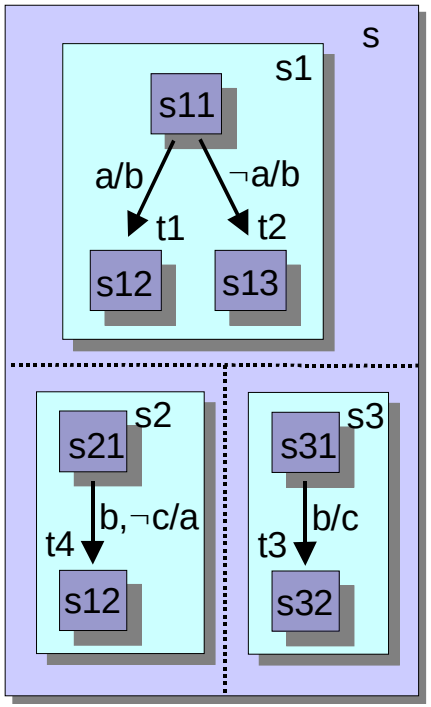
true $\wedge$

$\forall e.\forall t.\ (T(t) \wedge action(e, t)) \supset A(e) \ \wedge$

$\forall t.$ **ENABLED** (C, A, T, t) $\supset$ T(t)

Beispiel

E = ∅



CLOSED (C, ∅, A, T) :=

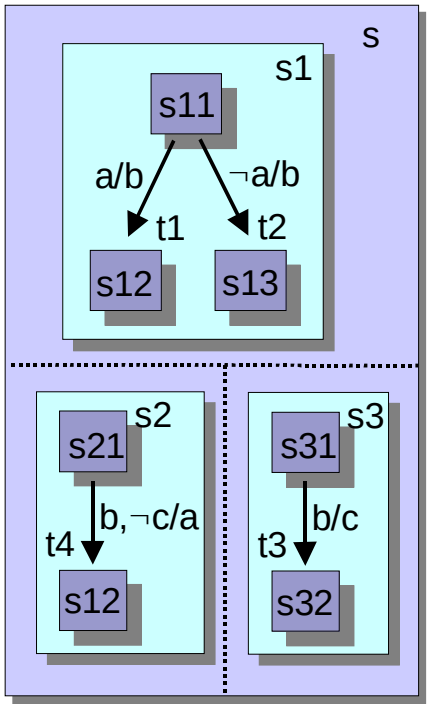
true ∧

t1 ⊃ b ∧ t2 ⊃ b ∧ t3 ⊃ c ∧ t4 ⊃ a ∧

∀t. **ENABLED** (C, A, T, t) ⊃ T(t)

Beispiel

E = ∅



CLOSED (C, ∅, A, T) :=

true ∧

t1 ⊃ b ∧ t2 ⊃ b ∧ t3 ⊃ c ∧ t4 ⊃ a ∧

ENABLED (C, A, T, t1) ⊃ t1 ∧

ENABLED (C, A, T, t2) ⊃ t2 ∧

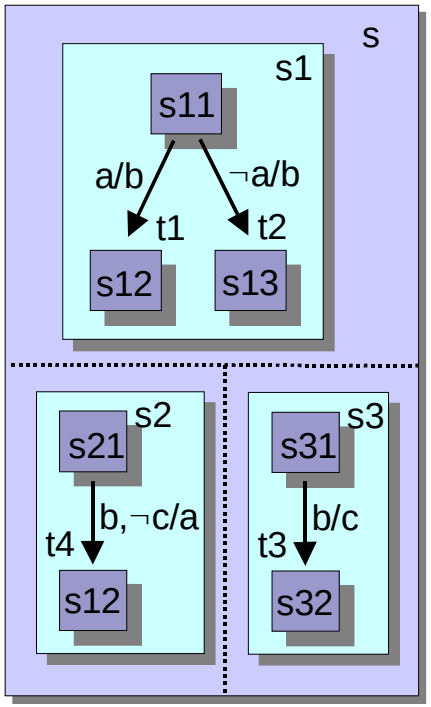
ENABLED (C, A, T, t3) ⊃ t3 ∧

ENABLED (C, A, T, t4) ⊃ t4

©2001 G. Lüttgen & M. Mendler

Beispiel

E = ∅



CLOSED (C, ∅, A, T) :=

true ∧

t1 ⊃ b ∧ t2 ⊃ b ∧ t3 ⊃ c ∧ t4 ⊃ a ∧

ENABLED (C, A, T, t1) ⊃ t1 ∧

ENABLED (C, A, T, t2) ⊃ t2 ∧

ENABLED (C, A, T, t3) ⊃ t3 ∧

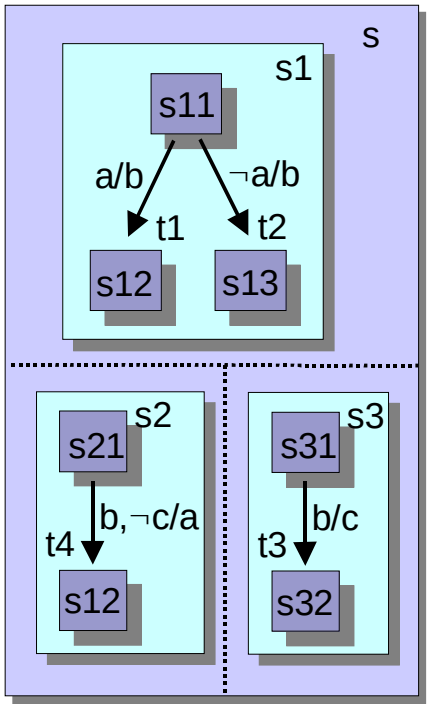
ENABLED (C, A, T, t4) ⊃ t4

RELEVANT **TRIGGERED** **ORTHOGONAL**

©2001 G. Lüttgen & M. Mendler

Beispiel

E = ∅



CLOSED (C, ∅, A, T) :=

true ∧

t1 ⊃ b ∧ t2 ⊃ b ∧ t3 ⊃ c ∧ t4 ⊃ a ∧

ENABLED (C, A, T, t1) ⊃ t1 ∧

ENABLED (C, A, T, t2) ⊃ t2 ∧

ENABLED (C, A, T, t3) ⊃ t3 ∧

ENABLED (C, A, T, t4) ⊃ t4

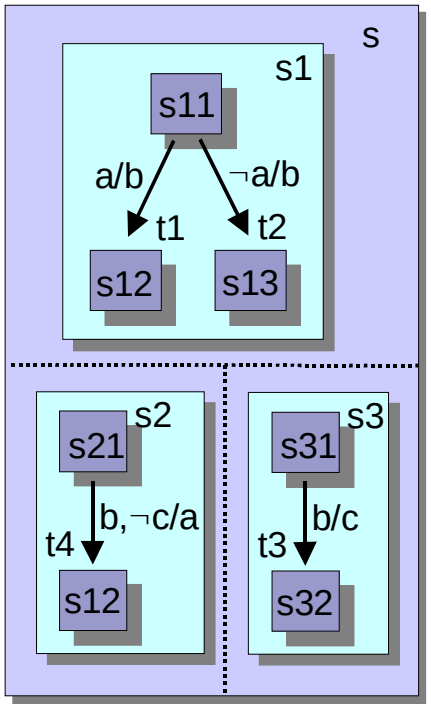
RELEVANT **TRIGGERED** **ORTHOGONAL**

(s21 ∧ b ∧ ¬c ∧ ⊥(t4)) ⊃ t4

©2001 G. Lüttgen & M. Mendler

Beispiel

$E = \emptyset$



CLOSED (C, $\emptyset$, A, T) :=

true $\wedge$

$t1 \supset b \wedge t2 \supset b \wedge t3 \supset c \wedge t4 \supset a \wedge$

$(s11 \wedge a \wedge \bot(t1)) \supset t1 \wedge$

$(s11 \wedge \neg a \wedge \bot(t2)) \supset t2 \wedge$

$(s31 \wedge b \wedge \bot(t3)) \supset t3 \wedge$

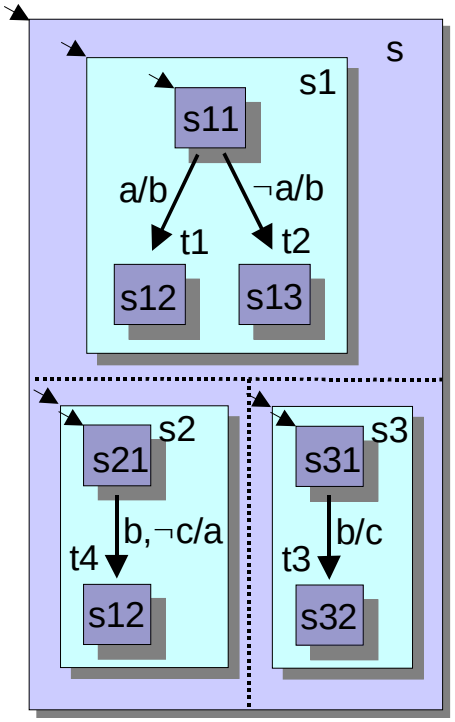
$(s21 \wedge b \wedge \neg c \wedge \bot(t4)) \supset t4$

Es bleibt noch zu beachten: Makroschritt = "minimales" Modell **...**

©2001 G. Lüttgen & M. Mendler

Nicht jedes minimale Modell ist kausal !

E = ∅



CLOSED (C, ∅, A, T) :=

true ∧

t1 ⊃ b ∧ t2 ⊃ b ∧ t3 ⊃ c ∧ t4 ⊃ a ∧

(s11 ∧ a ∧ ⊥(t1)) ⊃ t1 ∧

(s11 ∧ ¬a ∧ ⊥(t2)) ⊃ t2 ∧

(s31 ∧ b ∧ ⊥(t3)) ⊃ t3 ∧

(s21 ∧ b ∧ ¬c ∧ ⊥(t4)) ⊃ t4

Sei C = {s,s1,s11,s2,s21,s3,s31}. Dann sind

- X1 = C ∪ {b, c, t2, t3} kausal
- X2 = C ∪ {a, b, t1, t4} nicht kausal

beides minimale klassische Modelle!

©2001 G. Lüttgen & M. Mendler

Intuitionistische Semantik

Ersetze

STEP (C,E,A,T) := **CLOSED** (C,E,A,T) $\wedge$ **CAUSAL** (C,E,A,T)

durch

STEP(C,E,A,T) := (A,T) "minimales **intuitionistisches** Modell"
von **CLOSED** (C,E,A,T)

$\Rightarrow$ **STEP** ist durch **CLOSED** eindeutig bestimmt !

Intuitionistische Semantik

Semantik:

CLOSED = intuitionistische Spezifikation von Mikroschrittfolgen

Modelle:

Folgen von Mikroschritten = monotone Konstruktionsschritte

$$\mathbf{M} = (M_1, M_2, \ldots, M_n)$$

- $M_i \subseteq \mathcal{S} \cup \mathcal{E} \cup \mathcal{T}$ Mikrokonfiguration
- $\mathcal{S} \cap \mathcal{E} \cap \mathcal{T} = \emptyset$ eindeutige Namen
- $M_i \subseteq M_{i+1}$ Monotonie
- $M_i \cap \mathcal{S} = M_{i+1} \cap \mathcal{S}$ Zustände konstant

©2001 G. Lüttgen & M. Mendler

Modelltheoretische Semantik (klassisch)

Mikroschrittfolge $\mathbf{M} = (M_1, M_2, \ldots, M_n)$

$M_i \models p$	gdw	$p \in M_i \quad (p \in \mathcal{S} \cup \mathcal{E} \cup \mathcal{T})$
$M_i \models \perp(t)$	gdw	orthogonal(t, $M_i \cap \mathcal{T}$)
$M_i \models \neg\phi$	gdw	$M_i \not\models \phi$
$M_i \models \phi \wedge \psi$	gdw	$M_i \models \phi$ und $M_i \models \psi$
$M_i \models \phi \vee \psi$	gdw	$M_i \models \phi$ oder $M_i \models \psi$
$M_i \models \phi \supset \psi$	gdw	$M_i \models \phi \Rightarrow M_i \models \psi$

Modelltheoretische Semantik (intuitionistisch)

Mikroschrittfolge $\mathbf{M} = (M_1, M_2, \ldots, M_n)$

$M_i \models p$	gdw	$\forall j \geq i$	$p \in M_j$	$(p \in \mathcal{S} \cup \mathcal{E} \cup \mathcal{T})$
$M_i \models \bot(t)$	gdw	$\forall j \geq i$	orthogonal(t, $M_j \cap \mathcal{T}$)	
$M_i \models \neg\phi$	gdw	$\forall j \geq i$	$M_j \not\models \phi$	
$M_i \models \phi \wedge \psi$	gdw	$\forall j \geq i$	$M_j \models \phi$ und $M_j \models \psi$	
$M_i \models \phi \vee \psi$	gdw	$\forall j \geq i$	$M_j \models \phi$ oder $M_j \models \psi$	
$M_i \models \phi \supset \psi$	gdw	$\forall j \geq i$	$M_j \models \phi \Rightarrow M_j \models \psi$	

$\mathbf{M} \models \phi$ gdw $\forall j.\ M_j \models \phi$ Monotoniebedingung

Modelltheoretische Charakterisierung

Definition:

Es sei M = C∪A∪T (Mikroschrittfolge der Länge 1).

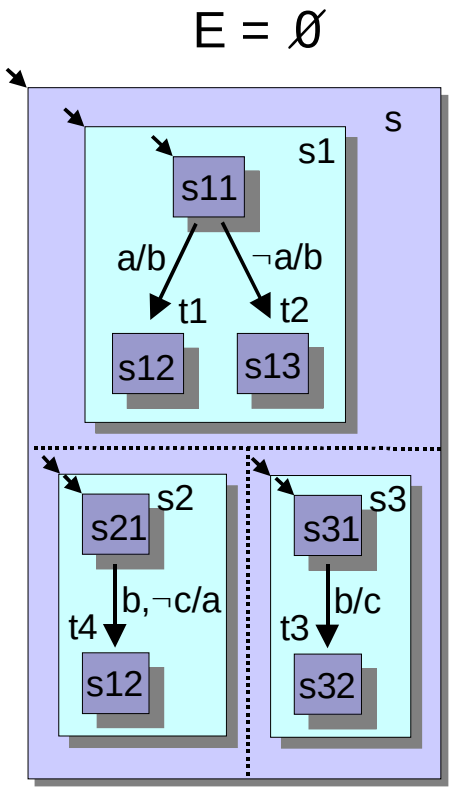
M heißt **Response−Modell** von ϕ, wenn

- $M \models \phi$
- Für alle Mikroschrittfolgen (M*, M) gilt:
  $(M^*, M) \models \phi \Rightarrow M^* = M$

Satz:

C∪A∪T ist ein Response−Modell von **CLOSED**
gdw **STEP** (C,Ø,A,T).

Beispiel



CLOSED (C, ∅, A, T) :=

$t1 \supset b \wedge\ t2 \supset b \wedge\ t3 \supset c \wedge\ t4 \supset a\ \wedge$

$(s11 \wedge a \wedge \perp(t1)) \supset\ t1\ \wedge$

$(s11 \wedge \neg a \wedge \perp(t2)) \supset\ t2\ \wedge$

$(s31 \wedge b \wedge \perp(t3)) \supset\ t3\ \wedge$

$(s21 \wedge b \wedge \neg c \wedge \perp(t4)) \supset\ t4$

Sei C = {s,s1,s11,s2,s21,s3,s31}. Dann gilt:

- X1 = C ∪ {b, c, t2, t3} Response–Modell
- X2 = C ∪ {a, b, t1, t4} kein Response–Modell

M = (C, X2) $\models$ **CLOSED**

©2001 G. Lüttgen & M. Mendler

Kompositionalität und volle Abstraktheit

Mikroschrittfolgensemantik: $[\![S]\!]_{\text{☺}} = \{ M : M \models S \}$

Satz:

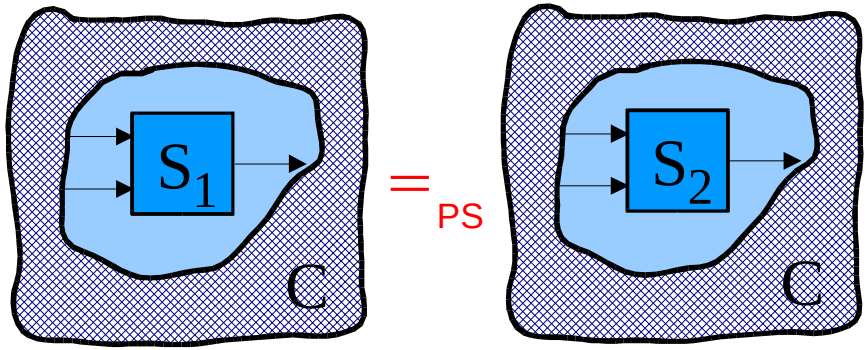
S_1, S_2 haben dieselbe intuitionistische Semantik.

$$[\![S_1]\!]_{\text{☺}} = [\![S_2]\!]_{\text{☺}}$$

gdw

Für alle (Parallel−)Kontexte C:

$C[S_1]$ und $C[S_2]$ haben dasselbe Verhalten im Sinne von Pnueli/ Shalev.



Zusammenfassung

- Pnueli/Shalevs Statechartssemantik verdient größere Aufmerksamkeit ! "Logischer Charakter"
- Ergebnis: kompakte Beschreibung von Mikroschrittverhalten; Shallow Embedding in Aussagenlogik
- Jedes grafische Element (Zustand, Transition) entspricht einem logischen Konstraint: inkrementell + kompositionell
- Intuitionistische Logik: spezielle Balance zwischen Syntax und Semantik; "mehr Semantik für weniger Syntax"

©2001 G. Lüttgen & M. Mendler

Vielen Dank!

Publikationen: (elektr. erhältlich via www.dcs.shef.ac.uk/~luettgen)

- G. Lüttgen and M. Mendler. The Intuitionism Behind Statecharts Steps. To appear in ACM Transactions on Computational Logic, 2001.
- G. Lüttgen and M. Mendler. Statecharts: From Visual Syntax to Model−theoretic Semantics. In Workshop on "Integrating Diagrammatic and Formal Specification Techniques," Wien, September 2001.

Workshopankündigung:

Semantic Foundations of Engineering Design Languages (SFEDL)

www.dcs.shef.ac.uk/~sfedl

Satellit zu ETAPS 2001, Grenoble, Frankreich, 14 April 2001.