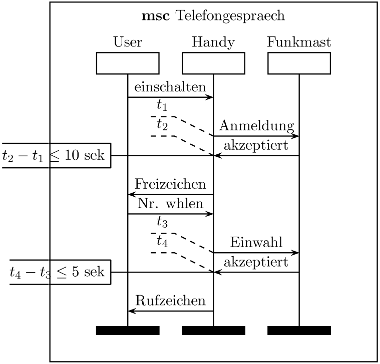
# Zeitliche und stochastische Sequenzdiagramme

Christoph Güdelhöfer
Betreuer: Professor Katoen

10. April 2007

# Gliederung

# Beispiel


msc Telefongespraech
User
Handy
Funkmast
einschalten
$t_1$
$t_2$
Anmeldung
akzeptiert
$t_2 - t_1 \leq 10$ sek
Freizeichen
Nr. whlen
$t_3$
$t_4$
Einwahl
akzeptiert
$t_4 - t_3 \leq 5$ sek
Rufzeichen

# Einführung

- Sequenzdiagramme bilden Kommunikationsflüsse ab
- bisher nur intuitiv definiert
- STAIRS liefert ein theoretisches Fundament für Sequenzdiagramme
- Erweiterung von STAIRS

# Gliederung

# grundlegende Funktionen I

- $\#\_ \in A^\omega \rightarrow N_0 \cup \{\infty\}$
  gibt die Anzahl der Elemente aus $a$ zurück.
- $\_[\_] \in A^\omega \times \mathbb{N} \rightarrow A$
  gibt n-tes Element aus $a$ zurück, für $n \leq \#a$.
- $\_ \frown \_ \in A^\omega \times A^\omega \rightarrow A^\omega$
  verbindet Folgen $a_1$ und $a_2$ zu neuer Folge mit Länge $\#a_1 + \#a_2$.
- $\_|\_ \in A^\omega \times \mathbb{N} \rightarrow A^\omega$
  bezeichnet Präfix der Länge $i$, für $0 \leq i \leq \#a$.

# grundlegende Funktionen II

- $\_ \circledS \_ \in \mathbb{P}(A) \times A^\omega \rightarrow A^\omega$
  ist Folge von *a* die nur Elemente aus *B* enthält.
- $\_ \circledast \_ \in \mathbb{P}(A \times B) \times (A^\omega \times B^\omega) \rightarrow A^\omega \times B^\omega$
  Filterfunktion
- $\pi_i$
  gibt Element *i* eines Tupels zurückgibt.

# Ereignisse Grundlagen

- $L$ Menge aller Lebenslinien
- $M$ Menge aller Nachrichten
  - Nachricht ist Tripel $(s, re, tr)$
  - $s$ Signal, $re$ Empfänger, $tr$ Sender
  - $re, tr \in L$
- $T$ Menge aller Bezeichnungen für Zeitstempel
  - $\mathbb{F}(v)$ Menge logischer Formeln mit freien Variablen $v$
  - $v \in T$
- Zwei Arten von Ereignissen $\{!, ?\}$
  - "!" Senden
  - "?" Empfangen

# Ereignisse Definition

- Ereignis ist Tripel: $(k, m, t) \in \{!, ?\} \times \mathcal{M} \times \mathcal{T}$
- $E$ Menge aller Ereignisse
- Interpretation der Ereignisse:

$$[\![\mathcal{E}]\!] \stackrel{\text{def}}{=} \{(k, m, t \mapsto r) | (k, m, t) \in \mathcal{E} \wedge r \in \mathbb{R}\}$$

- $k.\_ \in \mathcal{E} \to \{?, !\},\ m.\_ \in \mathcal{E} \to \mathcal{M},\ t.\_ \in \mathcal{E} \to \mathcal{T}$
  $tr.\_ \in \mathcal{E} \to \mathcal{L},\ re.\_ \in \mathcal{E} \to \mathcal{L},\ [r.\_ \in [\![\mathcal{E}]\!] \to \mathbb{R}$
  Funktionen um Art, Nachricht, Bezeichnung des Zeitstempels, Sender, Empfänger sowie Zeitstempel einer Ereignisinterpretation zu erhalten

# Spuren

- Spur $h \in [\![\mathcal{E}]\!]^\omega$ Folge von Ereignissen, zB. $\langle e_1, e_2, e_3 \rangle$.
- Spur entspricht Durchlauf durchs System
- Spur muss Wohlgeformtheitsbedingungen erfüllen
- $\mathcal{H}$ Menge der wohlgeformten Spuren

# Spuren Wohlgeformtheit I

- $\forall i, j \in [1..\#h] : i < j \Rightarrow r.h[i] \leq r.h[j]$
  Ereignisse sind zeitlich geordnet
- $\forall i, j \in [1..\#h] : i \neq j \Rightarrow r.h[i] \neq r.h[j]$
  Ereignis darf nur einmal pro Spur auftreten
- $e.l \stackrel{\text{def}}{=} \{e \in [\![\mathcal{E}]\!] | (k.e = ! \wedge tr.e = l) \vee (k.e = ? \wedge re.e = l)\}$
  alle Ereignisse, die auf Lebenslinie $l$ eintreten können

# Spuren Wohlgeformtheit II

- $\forall l \in \mathcal{L} : (\#e.l \circledS h = \infty \Rightarrow \forall t \in \mathbb{R} : \exists i \in \mathbb{N} : (r.(e.l \circledS h).[i] > t))$
  Zeit darf unendlich lang sein
  - $l$ beliebige Lebenslinie
  - $t$ beliebiger Zeitstempel
- mindestens soviele Sedungen wie Empfänge eines Sende-Ereignisses müssen aufgetreten sein:
  - $\forall i \in [1..\#h] : k.h[i] = ! \Rightarrow \#(\{!\} \times \{m.h[i]\} \times U) \circledS h|_i > \#(\{?\} \times \{m.h[i]\} \times U) \circledS h|_i]$
  - wobei $U \stackrel{\text{def}}{=} \{t \mapsto r | t \in \mathcal{T} \wedge r \in \mathbb{R}\}$.

# Gliederung

# Spezifikationspaar

- Spezifikationspaar $(p, n)$
  - $p$ positive Spuren
  - $n$ negative Spuren
  - $(p, n)$ ist widersprüchlich, falls $p \cap n \neq \emptyset$
- $\mathcal{O}$ Menge der Spezifikationspaare
- $[\![d]\!]$ ist Bezeichnung des Spezifikationspaars, das $d$ repräsentiert.

# Syntax zeitlicher Sequenzdiagramme

Menge $D$ der syntaktisch korrekten Sequenzdiagramme induktiv definiert:

- $\mathcal{E} \subset \mathcal{D}$
- $d \in \mathcal{D} \Rightarrow neg\ d \in \mathcal{D}$
- $d_1, d_2 \in \mathcal{D} \Rightarrow d_1\ par\ d_2 \in \mathcal{D} \wedge d_1\ seq\ d_2 \in \mathcal{D} \wedge d_1\ alt\ d_2 \in \mathcal{D}$
- $d \in \mathcal{D} \wedge C \in \mathbb{F}(tt.d) \Rightarrow d\ tc\ C \in \mathcal{D}$

Wobei $tt.d$ die Menge der Zeitstempel Bezeichnungen, die in $d$ auftreten, zurückgibt.

# Semantik zeitlicher Sequenzdiagramme I

- Semantik Ereignis:

$$[\![(k,m,t)]\!] \stackrel{\text{def}}{=} (\{\langle(k,m,t \mapsto r)\rangle | r \in \mathbb{R}\}, \emptyset), \text{ falls } (k,m,t) \in \mathcal{E}$$

- Semantik Negation:

$$[\![neg\ d]\!] \stackrel{\text{def}}{=} \neg[\![d]\!] \text{ wobei } \neg(p,n) \stackrel{\text{def}}{=} (\{\langle\rangle\}, n \cup p)$$

- Semantik Mögliche Auswahl:

$$[\![d_1\ alt\ d_2]\!] \stackrel{\text{def}}{=} [\![d_1]\!] \uplus [\![d_2]\!]$$

wobei

$$(p_1, n_1) \uplus (p_2, n_2) \stackrel{\text{def}}{=} (p_1 \cup p_2, n_1 \cup n_2)$$

# Parallele Ausführung

- Definition:
  $s_1, \ s_2 \in \mathcal{H}$

$$\begin{aligned} s_1 \| s_2 \stackrel{\text{def}}{=} \ & \{h \in \mathcal{H} | \exists \ or \in \{1,2\}^\infty : \\ & \pi_2((\{1\} \times [\![\mathcal{E}]\!]) \circledast (or, h)) \in s_1 \wedge \\ & \pi_2((\{2\} \times [\![\mathcal{E}]\!]) \circledast (or, h)) \in s_2\} \end{aligned}$$

- Semantik:

$$[\![d_1 \ par \ d_2]\!] \stackrel{\text{def}}{=} [\![d_1]\!] \| [\![d_2]\!]$$

wobei

$$(p_1, n_1) \| (p_2, n_2) \stackrel{\text{def}}{=} (p_1 \| p_2, (n_1 \| (p_2 \cup n_2)) \cup (p_1 \| n_2))$$

# Schwaches Sequenzieren/Ordnen

- Definition:

$$s_1 \precsim s_2 \stackrel{\text{def}}{=} \{h \in \mathcal{H} | \exists h_1 \in s_1,\ h_2 \in s_2 : \\ \forall l \in \mathcal{L} : el.l Ⓢ h = el.l Ⓢ h_1 \frown el.l Ⓢ h_2\}$$

- Semantik:

$$[d_1\ seq\ d_2] \stackrel{\text{def}}{=} [\![d_1]\!] \precsim [\![d_2]\!]$$

wobei

$$(p_1, n_1) \precsim (p_2, n_2) \stackrel{\text{def}}{=} (p_1 \precsim p_2, (n_1 \precsim (p_2 \cup n_2)) \cup (p_1 \precsim n_2))$$

# Zeitliche Beschränkung

- Definition
$$s \wr C \overset{\text{def}}{=} \{h \in s | h \models C\}$$
- Semantik:
$$[\![d \ tc \ C]\!] \overset{\text{def}}{=} [\![d]\!] \wr C$$

wobei
$$(p, n) \wr C \overset{\text{def}}{=} (p \wr C, n \cup (p \wr \neg C))$$

# Gliederung

# p-Obligationen

- $((p, n), Q)$ p-Obligation (engl. probability obligation)
  - $(p, n)$ Spezifikationspaar
  - $Q$ Menge von Wahrscheinlichkeiten
  - nur Spuren aus $\mathcal{H} \setminus n$ dürfen p-Obligationen implementieren
  - Spuren, die $((p, n), Q)$ implementieren
    - müssen mit Wahrscheinlichkeit von mind $Q$ auftreten
    - dürfen nur mit höheren Wahrscheinlichkeit als $Q$ auftreten, falls sie andere p-Obligationen erfüllen
  - $\mathcal{P}$ Menge der p-Obligationen
  - Multimenge von p-Obligationen definiert ein Sequenzdiagramm

# Syntax stochastischer Sequenzdiagramme

Menge $D$ der syntaktisch korrekten stochastischen Sequenzdiagramme induktiv definiert:

- zunächst die alte Definition:
  - $\mathcal{E} \subset \mathcal{D}$
  - $d \in \mathcal{D} \Rightarrow neg\ d \in \mathcal{D}$
  - $d_1, d_2 \in \mathcal{D} \Rightarrow d_1\ par\ d_2 \in \mathcal{D} \wedge d_1\ seq\ d_2 \in \mathcal{D} \wedge d_1\ alt\ d_2 \in \mathcal{D}$
  - $d \in \mathcal{D} \wedge C \in \mathbb{F}(tt.d) \Rightarrow d\ tc\ C \in \mathcal{D}$
- zusätzlich zur alten:

$$d_1, d_2 \in \mathcal{D} \wedge Q_1, Q_2 \subseteq [0..1] \Rightarrow d_1; Q_1\ palt\ d_2; Q_2 \in \mathcal{D}$$

# Semantik stochastischer Sequenzdiagramme I

- Semantik Ereignis

$$[\![(k,m,t)]\!] \stackrel{\text{def}}{=} \{(((\{\langle(k,m,t \mapsto r)\rangle | r \in \mathbb{R}\},\emptyset),\{1\})\} \text{ falls } (k,m,t) \in \mathcal{E}$$

- Semantik Negation

$$[\![neg\ d]\!] \stackrel{\text{def}}{=} \{(\neg o, Q) | (o, Q) \in [\![d]\!]\}$$

- Semantik zeitliche Beschränkung:

$$[\![d\ tc\ C]\!] \stackrel{\text{def}}{=} \{(o \wr C, Q) | (o, Q) \in [\![d]\!]\}$$

- Semantik Mögliche Wahl:

$$[\![d_1\ alt\ d_2]\!] \stackrel{\text{def}}{=} \{(o_1 \uplus o_2, Q_1 \cap Q_2) | (o_1, Q_1) \in [\![d_1]\!] \wedge (o_2, Q_2) \in [\![d_2]\!]\}$$

# Semantik stochastischer Sequenzdiagramme II

- Multiplikation von Wahrscheinlichkeiten:

$$Q_1 * Q_2 \stackrel{\text{def}}{=} \{q_1 * q_2 \mid q_1 \in Q_1 \wedge q_2 \in Q_2\}$$

- Semantik Parallele Ausführung:

$$\llbracket d_1 \; par \; d_2 \rrbracket \stackrel{\text{def}}{=} \{(o_1 \| o_2, Q_1 * Q_2) | (o_1, Q_1) \in \llbracket d_1 \rrbracket \wedge (o_2, Q_2) \in \llbracket d_2 \rrbracket\}$$

- Semantik schwaches Sequenzieren:

$$\llbracket d_1 \; seq \; d_2 \rrbracket \stackrel{\text{def}}{=} \{(o_1 \succsim o_2, Q_1 * Q_2) | (o_1, Q_1) \in \llbracket d_1 \rrbracket \wedge (o_2, Q_2) \in \llbracket d_2 \rrbracket$$

# *palt*-Operator

- Operand für *palt*:

$$[\![d;Q']\!] \stackrel{\text{def}}{=} \{(o, Q * Q') | (o, Q) \in [\![d]\!]\}$$

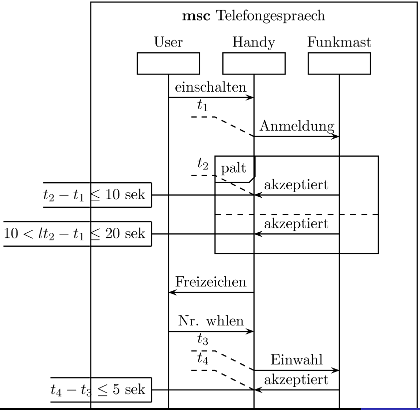
- Semantik *palt*:

$$[\![d_1 \ palt \ d_2]\!] \stackrel{\text{def}}{=} [\![d_1]\!] \cup [\![d_2]\!] \cup \{(\oplus([\![d_1]\!], [\![d_2]\!]), \{1\})\}$$

- Definition $\oplus$-Operator:

$$\oplus S \stackrel{\text{def}}{=} ((\bigcup_{((p,n),Q) \in S} p) \cap ((\bigcap_{((p,n),Q) \in S} p \cup n), \bigcap_{((p,n),Q) \in S} n)$$

# Beispiel


**msc** Telefongespraech
User
Handy
Funkmast
einschalten
$t_1$
Anmeldung
$t_2$
palt
akzeptiert
$t_2 - t_1 \leq 10$ sek
akzeptiert
$10 < lt_2 - t_1 \leq 20$ sek
Freizeichen
Nr. whlen
$t_3$
$t_4$
Einwahl
akzeptiert
$t_4 - t_3 \leq 5$ sek

# Zusammenfassung

- Wir haben Sequenzdiagramme auf der Basis von STAIRS weiter formalisiert, so dass sie nun
  - zeitliche und
  - stochastische Probleme darstellen können.
- Dabei konnten die Vorteile von STAIRS beibehalten werden ua.
  - strenger Formalismus
  - systematische Verfeinerung