- *Prozeßkalküle* oder *Prozeßalgebren*: CSP, CCS, π-Kalkül
- Primäre Operation: Kommunikation
- Beschreibt ablauffähige Prozesse (vgl. Modallogik, temporale Logik, TLA: Spezifikation)

CSP: Syntax

Gegeben Prozeßalphabet Σ, besondere Ereignisse $\checkmark, \tau$

$P ::= \mathit{Stop} \mid a \to P \mid \mu\, P.F(P)$	fundamentale Operationen
$\mid\ ?x : A \to P(x)$	Präfixauswahl ($A \subseteq \Sigma$)
$\mid P \,\Box\, Q \mid P \sqcap Q$	externe und interne Auswahl
$\mid P \parallel Q \mid P \underset{X}{\parallel} Q \mid P \;{}_X\!\!\parallel_Y Q$	synchronisiert parallel
$\mid P \,\vert\vert\vert\, Q$	unsynchronisiert parallel
$\mid P \setminus X \mid f[P]$	hiding, Umbenennung (f injektiv)
$\mid \mathit{Skip} \mid P;\ Q$	sequentielle Komposition, Iteration

CSP: Beispiele

- Einfacher Schokoladenautomat:

$$\mu\, P.\mathit{1p} \to \mathit{choc} \to P$$

- Schokoladenautomat mit Auswahl:

$$P = \mathit{1p} \to \mathit{choc} \to P \mid \mathit{2p} \to \mathit{toffee} \to P$$

- Pufferprozess:

$$\mathit{COPY} = \mathit{left}?x \to \mathit{right}!x \to \mathit{COPY}$$

NB. Eingabe ($c?x$) und Ausgabe ($c!x$) sind *reine Konvention*.

CSP: Beispiele II

- Bankautomat:

$$\begin{aligned} ATM = \; & in?c : CARD \rightarrow pin.f_{pin}(c) \rightarrow req?n : WA \rightarrow \\ & ((dispense.n \rightarrow out.c ATM) \\ & \quad \sqcap (refuse \rightarrow (ATM \sqcap out.c \rightarrow ATM))) \end{aligned}$$

- Pantomimenpferd (fehlerhaft):

$$\begin{aligned} HORSE &= Front \;{}_F\|_B\; back \\ F &= \{forward, backward, nod, neigh\} \\ B &= \{forward, backward, wag, kick\} \\ Front &= forward \rightarrow Front' \,\square\, nod \rightarrow Front \\ Back &= backward \rightarrow Back' \,\square\, wag \rightarrow Back \end{aligned}$$

Operationale Semantik für CSP (I)

Defn: Ein *labelled transition system (LTS)* ist $L = (N, A, \rightarrow)$ mit Menge N der Knoten (Zustände), Menge A von Labels und Relation $\{\xrightarrow{a} \subseteq N \times N\}_{a \in A}$ von Kanten (Zustandsübergänge).

Hier $N = P, A = \Sigma \cup \{\checkmark, \tau\}$, $\rightarrow$ definiert wie folgt (NB. Keine Regel für *Stop*):

$$\frac{}{e \rightarrow P \ \xrightarrow{a}\ P[a/e]} \; a \in \texttt{comms(e)}$$

$$\frac{}{P \sqcap Q \xrightarrow{\tau} P} \qquad\qquad \frac{}{P \sqcap Q \xrightarrow{\tau} Q}$$

$$\frac{}{Skip \xrightarrow{\checkmark} \Omega}$$

Operationale Semantik für CSP (II)

$$\frac{P \xrightarrow{\tau} P'}{P \;\Box\; Q \xrightarrow{\tau} P' \;\Box\; Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P \;\Box\; Q \xrightarrow{\tau} P \;\Box\; Q'}$$

$$\frac{P \xrightarrow{a} P'}{P \;\Box\; Q \xrightarrow{a} P'}\, a \neq \tau \qquad \frac{Q \xrightarrow{a} Q'}{P \;\Box\; Q \xrightarrow{a} Q'}\, a \neq \tau$$

$$\frac{P \xrightarrow{x} P'}{P;\; Q \xrightarrow{x} P';\; Q}\, x \neq \checkmark \qquad \frac{\exists\, P'.\, P \xrightarrow{\checkmark} P'}{P;\; Q \xrightarrow{\tau} Q}$$

$$\frac{P \xrightarrow{\checkmark} P'}{P \setminus B \xrightarrow{\checkmark} \Omega} \qquad \frac{P \xrightarrow{x} P'}{P \setminus B \xrightarrow{\tau} P'}\, x \in B \qquad \frac{P \xrightarrow{x} P'}{P \setminus B \xrightarrow{x} P' \setminus B}\, x \notin B \cup \{\checkmark\}$$

Operationale Semantik für CSP (III)

$$\frac{P \xrightarrow{\tau} P'}{P \underset{X}{\parallel} Q \xrightarrow{\tau} P' \underset{X}{\parallel} Q} \qquad \frac{Q \xrightarrow{\tau} Q'}{P \underset{X}{\parallel} Q \xrightarrow{\tau} P \underset{X}{\parallel} Q'}$$

$$\frac{P \xrightarrow{a} P'}{P \underset{X}{\parallel} Q \xrightarrow{a} P' \underset{X}{\parallel} Q}\, a \notin X \qquad \frac{Q \xrightarrow{a} Q'}{P \underset{X}{\parallel} Q \xrightarrow{a} P \underset{X}{\parallel} Q'}\, a \notin X$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q'}{P \underset{X}{\parallel} Q \xrightarrow{a} P' \underset{X}{\parallel} Q'}\, a \in X$$

$$\frac{P \xrightarrow{\checkmark} P'}{P \underset{X}{\parallel} Q \xrightarrow{\tau} \Omega \underset{X}{\parallel} Q} \qquad \frac{Q \xrightarrow{\checkmark} Q'}{P \underset{X}{\parallel} Q \xrightarrow{\tau} P \underset{X}{\parallel} \Omega} \qquad \frac{}{\Omega \underset{X}{\parallel} \Omega \xrightarrow{\checkmark} \Omega}$$

Ziele der Semantik von Prozesskalkülen

- *Reasoning about processes by their external behaviour*
- Untersuchung von
  - Verfeinerung (Implementation)
  - *deadlock:* Keine Transition möglich
  - *livelock:* Divergenz
- Grundlegender Begriff: *Äquivalenz (Gleichheit) von Prozessen*

Äquivalenz für LTS: Bisimulation

Defn: Für LTS $L = (N, A, \rightarrow)$, eine *Bisimulation* ist eine Relation $R \subseteq N \times N$ auf den Knoten so daß

(i) wenn $n_1 \, R \, n_2$ und $n_1 \stackrel{x}{\rightarrow} m_1$ $(x \in \Sigma^{\tau,\checkmark})$,
dann gibt es m_2 so daß $n_2 \stackrel{x}{\rightarrow} m_2$ und $m_1 \, R \, m_2$

(ii) wenn $n_1 \, R \, n_2$ und $n_2 \stackrel{x}{\rightarrow} m_2$ $(x \in \Sigma^{\tau,\checkmark})$,
dann gibt es m_1 so daß $n_1 \stackrel{x}{\rightarrow} m_1$ und $m_1 \, R \, m_2$

Bisimularität: externe Ununterscheidbarkeit

Allerdings: CSP primär über denotationelle Semantik definiert

Denotationelle Semantik für CSP I: Das Pfad-Modell

Pfade: $\Sigma^{*\checkmark} \stackrel{def}{=} \Sigma^* \cup \{s ^\frown \langle \checkmark \rangle \mid s \in \Sigma^*\}$

$$
\begin{array}{lcl}
traces(Stop) & = & \langle\rangle \\
traces(a \to P) & = & \{\langle\rangle\} \cup \{\langle a \rangle ^\frown s \mid s \in traces(P)\} \\
traces(P \,\Box\, Q) & = & traces(P) \cup traces(Q) \\
traces(P \sqcap Q) & = & traces(P) \cup traces(Q) \\
traces(P \setminus B) & = & \{s \upharpoonright \Sigma \setminus B \mid s \in traces(P)\} \\
traces(Skip) & = & \{\langle\rangle, \langle \checkmark \rangle\} \\
traces(P;\ Q) & = & (traces(P) \cap \Sigma^*) \cup \\
 & & \{s ^\frown t \mid s ^\frown \langle \checkmark \rangle \in traces(P), t \in traces(Q)\} \\
traces(P \underset{X}{\|} Q) & = & \bigcup \{s \underset{X}{\|} t \mid s \in traces(P), t \in traces(Q)\}
\end{array}
$$

Denotationelle Semantik für CSP I: Das Pfad-Modell

Für $x \in X, y \in \Sigma \setminus X$:

$$\langle\rangle \underset{X}{\parallel} \langle\rangle = \langle\rangle \qquad \langle\rangle \underset{X}{\parallel} \langle x\rangle = \langle\rangle \qquad \langle\rangle \underset{X}{\parallel} \langle y\rangle = \langle y\rangle$$

$$\begin{aligned}
\langle x\rangle^\frown s \underset{X}{\parallel} \langle y\rangle^\frown t &= \{\langle y\rangle^\frown u \mid u \in \langle x\rangle^\frown s \underset{X}{\parallel} t\} \\
\langle x\rangle^\frown s \underset{X}{\parallel} \langle x\rangle^\frown t &= \{\langle x\rangle^\frown u \mid u \in s \underset{X}{\parallel} t\} \\
\langle x\rangle^\frown s \underset{X}{\parallel} \langle x'\rangle^\frown t &= \emptyset \;\; x \neq x' \\
\langle y\rangle^\frown s \underset{X}{\parallel} \langle y'\rangle^\frown t &= \{\langle y\rangle^\frown u \mid u \in s \underset{X}{\parallel} \langle y'\rangle^\frown t\} \cup \{\langle y'\rangle^\frown u \mid u \in \langle y\rangle^\frown s \underset{X}{\parallel} t\} \\
s \underset{X}{\parallel} t^\frown\langle\checkmark\rangle &= \emptyset \\
s^\frown\langle\checkmark\rangle \underset{X}{\parallel} t^\frown\langle\checkmark\rangle &= \{u^\frown\langle\checkmark\rangle \mid u \in s \underset{X}{\parallel} t\}
\end{aligned}$$

Denotationelle Semantik für CSP I: Das Pfad-Modell

- Für Rekursion: vollständige Ordnung auf Pfaden

  $P \sqsubseteq Q \stackrel{def}{=} P \subseteq Q, \quad \perp \stackrel{def}{=} \{\langle\rangle\}$

  $traces(\mu P.F(P)) = fix(F) = \bigcup_{i<\omega} F^i(\{\langle\rangle\})$

  Operatoren stetig und monoton. (Nicht der Fall für Präfixordnung $\sqsubseteq_T$.)

- Probleme des Pfad-Modells:
  - Keine Unterscheidung von interner und externer Auswahl.
  - Keine Unterscheidung von deadlocks.

Denotationelle Semantik für CSP II: Failure/Divergence

- Pfade beschreiben *mögliche* Aktionen, F/D beschreiben auch *erzwungene* Aktionen.
- Divergenz: Menge von Pfaden, *ab denen* der Prozess *divergieren* kann (unendliche Sequenz von τ).
- *Failures*: (s, X) wobei s ein Pfad des Prozesses ist und X eine Menge von *verweigerten* Aktionen (*refusals*) in einem *stabilen* Zustand nach s **oder** nach s kann $\checkmark$ auftreten (dann $X \subseteq \Sigma$) **oder** Prozess divergiert nach s.
- Stabiler Zustand: kein τ oder $\checkmark$ möglich.

Denotationelle Semantik für CSP II: Failure/Divergence Modell $\mathcal{N}$

$\mathcal{N}$ gegeben durch $P = (F, D)$ mit $F \subseteq \Sigma^{*\checkmark} \times \mathbb{P}(\Sigma^{\checkmark}), D \subseteq \Sigma^{*\checkmark}$ so daß

F1 $\quad traces(P) = \{t \mid (t, X) \in F\}$ ist nichtleer und präfixgeschlossen.

F2 $\quad (s, X) \in F \wedge Y \subseteq X \Rightarrow (s, Y) \in F$

F3 $\quad (s, X) \in F \wedge \forall\, a \in Y.\, s\,\hat{}\,\langle a\rangle \notin traces(P) \Rightarrow (s, X \cup Y) \in F$

F4 $\quad s\,\hat{}\,\langle\checkmark\rangle \in traces(P) \Rightarrow (s, \Sigma) \in F$

D1 $\quad s \in D \cap \Sigma^* \wedge t \in \Sigma^{*\checkmark} \Rightarrow s\,\hat{}\,t \in D$

D2 $\quad s \in D \Rightarrow (s, X) \in F$

D3 $\quad s\,\hat{}\,\langle\checkmark\rangle \in D \Rightarrow s \in D$

Denotationelle Semantik für CSP II: Eigenschaften von $\mathcal{N}$

Verfeinerung: $(F, D) \sqsubseteq_{FD} (F', D')$ gdw $F \supseteq F', D \supseteq D'$

Theorem: Für *endliches* Σ, $\mathcal{N}$ ist *cpo* mit $\sqsubseteq_{FD}$ und

$$\bot_{\mathcal{N}} = (\Sigma^{*\checkmark} \times \mathbb{P}(\Sigma^{*\checkmark}), \Sigma^{*\checkmark})$$

$$\bigsqcup_i (F_i, D_i) = (\bigcap_i F_i, \bigcap D_i)$$

Deadlockfreiheit: $\forall\, s.\, (s, \Sigma) \notin \mathit{failures}(P)$ (P kann nie alles verweigern)

Denotationelle Semantik für CSP II: Failure/Divergence

$$\mathit{failures}(\mathit{Stop}) = \{(\langle\rangle, X) \mid X \subseteq \Sigma^{\checkmark}\} \qquad \mathit{divergences}(\mathit{Stop}) = \emptyset$$

$$\mathit{failures}(a \to P) = \{(\langle\rangle, X) \mid a \notin X\} \cup \{(\langle a\rangle \hat{}\, s, X) \mid (s, X) \in \mathit{failures}(s)\}$$

$$\mathit{divergences}(a \to P) = \{(\langle a\rangle \hat{}\, s, X) \mid s \in \mathit{divergences}(P)\}$$

$$\mathit{failures}(P \sqcap Q) = \mathit{failures}(P) \cup \mathit{failures}(Q)$$

$$\mathit{divergences}(P \sqcap Q) = \mathit{divergences}(P) \cup \mathit{divergences}(Q)$$

$$\begin{aligned}\mathit{failures}(P \,\square\, Q) = \; & \{(\langle\rangle, X) \mid (\langle\rangle, X) \in \mathit{failures}(P) \cap \mathit{failures}(Q)\} \\ & \cup \{(s, X) \mid (s, X) \in \mathit{failures}(P) \cup \mathit{failures}(Q) \wedge s \neq \langle\rangle\} \\ & \cup \{(\langle\rangle, X) \mid \langle\rangle \in \mathit{divergences}(P) \cup \mathit{divergences}(Q)\} \\ & \cup \{(\langle\rangle, X) \mid X \subseteq \Sigma \wedge \langle\checkmark\rangle \in \mathit{traces}(P) \cup \mathit{traces}(Q)\}\end{aligned}$$

$$\mathit{divergences}(P \,\square\, Q) = \mathit{divergences}(P) \cup \mathit{divergences}(Q)$$

Denotationelle Semantik für CSP II: Failure/Divergence

$$
\begin{aligned}
\mathit{failures}(P \underset{X}{\parallel} Q) \;=\; & \{\, (u, Y \cup Z) \mid Y \setminus (X \cup \{\checkmark\}) = Z \setminus (X \cup \{\checkmark\}) \\
& \quad \wedge \exists\, s, t. (s, Y) \in \mathit{failures}(P) \wedge (t, Z) \in \mathit{failures}(Q) \\
& \quad \wedge u \in s \underset{X}{\parallel} t \} \\
& \cup \{ (u, Y) \mid u \in \mathit{divergences}(P \underset{X}{\parallel} Q) \} \\
\mathit{divergences}(P \underset{X}{\parallel} Q) \;=\; & \{\, u \hat{\ } v \mid \exists\, s \in \mathit{traces}(P), t \in \mathit{traces}(Q). \\
& \quad u \in (s \underset{X}{\parallel} t) \cap \Sigma^* \\
& \quad \wedge (s \in \mathit{divergences}(P) \vee t \in \mathit{divergences}(Q)) \}
\end{aligned}
$$

Denotationelle Semantik für CSP II: Failure/Divergence

$$
\begin{aligned}
\mathit{failures}(P \setminus X) &= \{(s \setminus X, Y) \mid (s, Y \cup X) \in \mathit{failures}(Y)\} \\
&\quad \cup \{(s, X) \mid s \in \mathit{divergences}(P \setminus X)\} \\
\mathit{divergences}(P \setminus X) &= \{(s \setminus X)\hat{\ }t \mid s \in \mathit{divergences}(P)\} \\
&\quad \cup \{(u \setminus X)\hat{\ }t \mid \; u \in \Sigma^{\omega} \wedge (u \setminus X)\text{finite} \\
&\qquad\qquad\qquad\qquad \wedge \forall s < u . s \in \mathit{traces}(P)\} \\
\mathit{failures}(P;\ Q) &= \{(s, X) \mid s \in \Sigma^{*} \wedge (s, X \cup \{\checkmark\}) \in \mathit{failures}(P)\} \\
&\quad \cup \{(s\hat{\ }t, X) \mid s\hat{\ }\langle\checkmark\rangle \in \mathit{traces}(P) \wedge (t, X) \in \mathit{failures}(Q)\} \\
&\quad \cup \{(s, X) \mid s \in \mathit{divergences}(P;\ Q)\} \\
\mathit{divergences}(P;\ Q) &= \mathit{divergences}(P) \cup \\
&\quad \{s\hat{\ }t \mid s\hat{\ }\langle\checkmark\rangle \in \mathit{traces}(P) \wedge t \in \mathit{divergences}(Q)\}
\end{aligned}
$$

Denotationelle Semantik für CSP II: Failure/Divergence

Lemma: Für *endliches* Σ, alle Operatoren sind stetig.

$\Rightarrow$ Existenz von Fixpunkten.

Nachteile: Endlichkeit des Alphabets, Divergenzmengen kostspielig zu berechnen aber meistens nicht nötig.

Nachteile können behoben werden durch *stable failures model* $\mathcal{F}$.

Tools für CSP

- **FDR2** (Formal Systems Europe Ltd.):
  - *model-checker:* für Prozesse mit *endlich* vielen Zuständen;
  - automatische Prüfung auf refinement (T, F, FD), deadlock, livelock; Debugging, Auswertung.
- **HOL-CSP** (Uni Bremen):
  - Kodierung von FD-Semantik in Isabelle
  - Interaktives Beweis beliebiger Aussagen über Prozesse mit unendlichen Zuständen, beliebigen Alphabeten etc.

Arbeiten mit FDR2