

# Prozessäquivalenz

Grundlegende Frage:

*Wann sollen zwei Prozesse mit unterschiedlicher Implementierung und unterschiedlichem internen Verhalten als gleich erachtet werden?*

Aspekte:

- Prozessalgebra: Gleiche Prozesse können in verschiedenen Kontexten durch gleiche ersetzt werden.
- Für welche Zwecke soll die Äquivalenz benutzt werden?
- Wie kann man Gleichheit von Prozessen beweisen?

**Beispiele:**

1.  $\text{protocol}(key) \mid \text{attacker} \approx \text{protocol}(key') \mid \text{attacker}$
2. Spezifikation und Verifikation: Spezifiziere gewünschtes Verhalten durch einen Prozess; leite aus Implementierung einen Prozess ab und prüfe Gleichheit mit der Spezifikation.

# Spuräquivalenz

Zwei Prozesse können die gleichen Folgen von Aktionen ausführen.

## **Problem:**

Damit sind folgende Prozesse gleich:

$$\epsilon.(coffee.0 + chocolate.0)$$
$$\epsilon.coffee.0 + \epsilon.chocolate.0$$

Spuräquivalenz kann nützlich sein, ist aber oft zu grob.

# Observationen

Wir betrachten stattdessen *observationelle Äquivalenz*, in der zwei Prozesse gleich sind, wenn sie von der Umgebung nicht unterschieden werden können.

# Observationen

Wir betrachten stattdessen *observationelle Äquivalenz*, in der zwei Prozesse gleich sind, wenn sie von der Umgebung nicht unterschieden werden können.

Als mögliche Observation betrachten wir ein **Strong Barb** genanntes Prädikat  $P \downarrow a$  (etwa: Widerhaken).

$P \downarrow a$  gilt falls  $P$  sofort auf dem Kanal  $a$  senden kann.

Formal:  $P \downarrow a$  falls  $P \equiv E[\bar{a}.P_1 + P_2]$  für geeignete Prozesse  $P_1, P_2$  und Auwertungskontext  $E[-]$ , der  $a$  nicht bindet.

## Beispiele:

$$\bar{a}.(b.0 + c.0) \downarrow a$$

$$\bar{a}.(b.0 + c.0) \not\downarrow b$$

# Observationen

Man könnte nun versuchen Prozesse  $P$  und  $Q$  als gleich auffassen, wenn sie in beliebigen Kontexten die gleichen Observationen zulassen, d.h.

$$E[P] \downarrow a \quad \text{gdw} \quad E[Q] \downarrow a$$

für alle Auswertungskontexte  $E[-]$  und alle  $a$ .

# Observationen

Man könnte nun versuchen Prozesse  $P$  und  $Q$  als gleich auffassen, wenn sie in beliebigen Kontexten die gleichen Observationen zulassen, d.h.

$$E[P] \downarrow a \quad \text{gdw} \quad E[Q] \downarrow a$$

für alle Auswertungskontexte  $E[-]$  und alle  $a$ .

Auf diese Art erfasst man aber nur einen Auswertungsschritt.

**Beispiel:**  $\bar{a}.b.0$  und  $\bar{a}.c.0$  wären äquivalent.

# Observationen

Man könnte nun versuchen Prozesse  $P$  und  $Q$  als gleich auffassen, wenn sie in beliebigen Kontexten die gleichen Observationen zulassen, d.h.

$$E[P] \downarrow a \quad \text{gdw} \quad E[Q] \downarrow a$$

für alle Auswertungskontexte  $E[-]$  und alle  $a$ .

Auf diese Art erfasst man aber nur einen Auswertungsschritt.

**Beispiel:**  $a.b.0$  und  $a.c.0$  wären äquivalent.

Auch wenn man sagt, dass die Prozesse eine beliebige Anzahl von Schritten ausführen dürfen, bevor die Observation gemacht wird, d.h.

$$\exists P'. E[P] \longrightarrow^* P' \downarrow a \quad \text{gdw} \quad \exists Q'. E[Q] \longrightarrow^* Q' \downarrow a$$

(für alle  $E[-]$  und  $a$ ), so kann man  $a.(b.0 + c.0)$  und  $a.b.0 + a.c.0$  nicht unterscheiden.

# Bisimulation

**Idee:** Jede Evolution von  $P$  muss sich einer äquivalenten von  $Q$  zuordnen lassen und umgekehrt.

## Beispiel:

Semaphore  $S_1$ , die *einen* Prozess in kritischen Bereich lässt.  
Semaphore  $S_2$ , die *zwei* Prozesse in kritischen Bereich lässt.

$$\begin{array}{ll} S_1 = p.S'_1 & S_2 = p.S'_2 \\ S'_1 = v.S_1 & S'_2 = p.S''_2 + v.S_2 \\ & S''_2 = v.S'_2 \end{array}$$

$S_1 \mid S_1$  und  $S_2$  sollten äquivalent sein.

Evolutionen dieses Prozesse können zugeordnet werden:

$$\begin{array}{ll} E[S_1 \mid S_1] \text{ und } E[S_2] & E[S'_1 \mid S_1] \text{ und } E[S'_2] \\ E[S_1 \mid S'_1] \text{ und } E[S'_2] & E[S'_1 \mid S'_1] \text{ und } E[S''_2] \end{array}$$



# Bisimulation

**Idee:** Jede Evolution von  $P$  muss sich einer äquivalenten von  $Q$  zuordnen lassen und umgekehrt.

## Beispiel:

Bei den Prozessen  $P = a.(\bar{b}.0 + \bar{c}.0) \mid \bar{a}.0$  und  $Q = (a.\bar{b}.0 + a.\bar{c}.0) \mid \bar{a}.0$  kann man die Redukte nicht äquivalent zuordnen.

Wir haben  $Q \longrightarrow \bar{b}.0$  und  $Q \longrightarrow \bar{c}.0$ , aber nur  $P \longrightarrow \bar{b}.0 + \bar{c}.0$ .

Es gilt  $(\bar{b}.0 + \bar{c}.0) \downarrow b$  aber  $\bar{c}.0 \not\downarrow b$  sowie  $(\bar{b}.0 + \bar{c}.0) \downarrow c$  aber  $\bar{b}.0 \not\downarrow c$ .

$\Rightarrow$  Kann die Redukte nicht so zuordnen, dass die zugeordneten Prozesse stets nur die gleichen Observationen zulassen.

# Barbed Equivalence

## Definition:

**Strong Barbed Equivalence**  $\simeq$  ist die größte symmetrische Relation mit folgenden Eigenschaften (für alle  $P, Q, P'$ ):

1. Aus  $P \simeq Q$  und  $P \downarrow a$  folgt  $Q \downarrow a$  für alle  $a$ .
2. Gilt  $P \simeq Q$  und  $P \longrightarrow P'$ , so gibt es  $Q'$  mit  $Q \longrightarrow Q'$  und  $P' \simeq Q'$ .
3. Aus  $P \simeq Q$  folgt  $E[P] \simeq E[Q]$  für jeden Auswertungskontext  $E[-]$ .

**Satz:**  $\simeq$  ist wohldefiniert und eine Äquivalenzrelation.

## Beispiele:

$$a.(\bar{b}.0 + \bar{c}.0) \not\simeq a.\bar{b}.0 + a.\bar{c}.0$$

$$S_1 \mid S_1 \simeq S_2$$

$$\nu a.(a.0) \simeq 0$$

# Labelled Transitions

Die Quantifizierung über (unendlich viele) Kontexte macht es schwierig, konkrete Äquivalenzen zu beweisen.

**Beweistechnik:** Bisimulationen mit „Labelled Transitions“.

Idee: Formalisiere nicht nur die tatsächlichen, sondern auch die *möglichen* Interaktionen mit der Umgebung.

Reduktionsrelation mit Labels  $P \xrightarrow{\alpha} Q$ , wobei  $\alpha \in \{a, \bar{a}, \tau \mid a \in \mathcal{N}\}$ .

- Bisherige Reduktion  $P \longrightarrow Q$  tauchen (bis auf  $\equiv$ ) als  $P \xrightarrow{\tau} Q$  auf.
- Eine Reduktion  $P \xrightarrow{a} Q$  sagt, dass  $P$  auf Kanal  $a$  senden kann (an einen bisher unbekanntem Prozess) und dann zu  $Q$  wird.
- Eine Reduktion  $P \xrightarrow{\bar{a}} Q$  sagt, dass  $P$  auf Kanal  $\bar{a}$  senden kann (an einen bisher unbekanntem Prozess) und dann zu  $Q$  wird.

# Labelled Transitions

Transitionsrelation wird induktiv durch folgende Regeln definiert.

$$\frac{}{a.P \xrightarrow{a} P}$$

$$\frac{}{\bar{a}.P \xrightarrow{\bar{a}} P}$$

$$\frac{P \xrightarrow{\alpha} P'}{P + Q \xrightarrow{\alpha} P'}$$

$$\frac{Q \xrightarrow{\alpha} Q'}{P + Q \xrightarrow{\alpha} Q'}$$

$$\frac{P \xrightarrow{\alpha} P'}{P | Q \xrightarrow{\alpha} P' | Q'}$$

$$\frac{Q \xrightarrow{\alpha} Q'}{P | Q \xrightarrow{\alpha} P' | Q'}$$

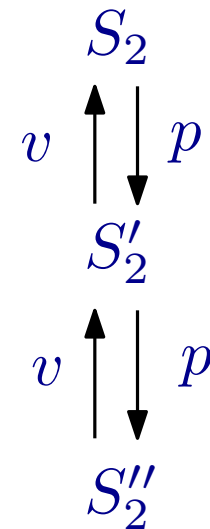
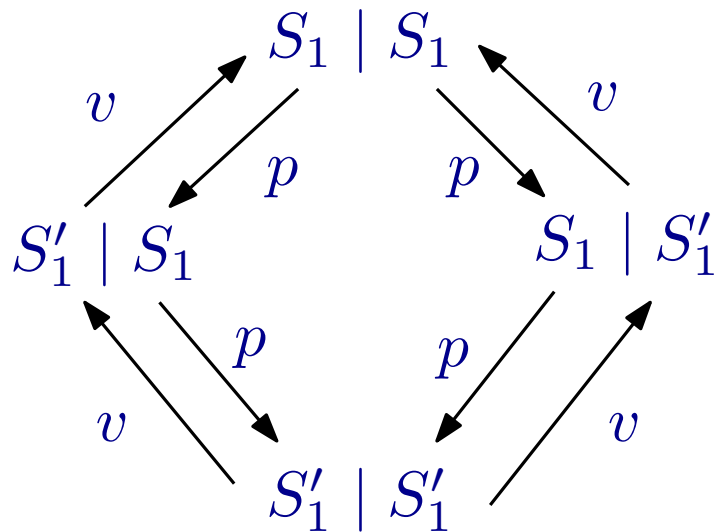
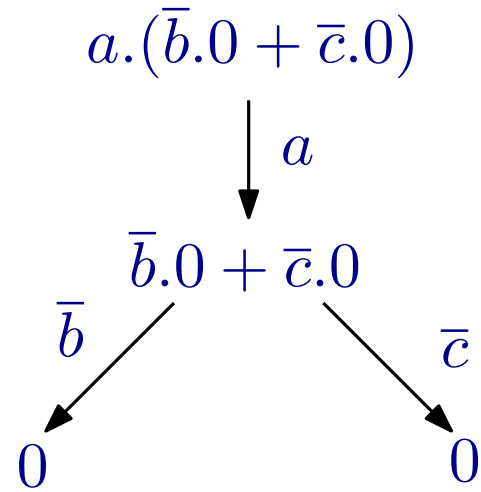
$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\bar{a}} Q'}{P | Q \xrightarrow{\tau} P' | Q'}$$

$$\frac{P \xrightarrow{\alpha} P'}{\nu a.P \xrightarrow{\alpha} \nu a.P'} \quad \alpha \notin \{a, \bar{a}\}$$

$\alpha$  läuft über  $\{a, \bar{a}, \tau \mid a \in \mathcal{N}\}$ .

# Labelled Transitions

Beispiele:



# Labelled Bisimulation

## Definition:

Eine Relation  $\mathcal{S}$  ist eine **starke Bisimulation** falls aus  $PSQ$  folgt:

1. Wenn  $P \xrightarrow{\alpha} P'$ , dann gibt es  $Q'$  mit  $Q \xrightarrow{\alpha} Q'$  und  $P'SQ'$ .
2. Wenn  $Q \xrightarrow{\alpha} Q'$ , dann gibt es  $P'$  mit  $P \xrightarrow{\alpha} P'$  und  $P'SQ'$ .

**Satz:** Es existiert eine **größte starke Bisimulationsrelation**  $\sim$ , die alle anderen Bisimulationsrelationen enthält, d.h. es gilt  $\mathcal{S} \subseteq \sim$  für jede Bisimulationsrelation  $\mathcal{S}$ .

## Definition:

Zwei Prozesse  $P$  und  $Q$  mit  $P \sim Q$  heißen **stark bisimilar**.

**Bemerkung:** Um zu zeigen, dass  $P$  und  $Q$  stark bisimilar sind, genügt es *eine Bisimulation*  $\mathcal{S}$  zu finden, für die  $PSQ$  gilt.

# Labelled Bisimulation

**Beispiel:**

$$S_2 \sim S_1 \mid S_1$$

Es genügt, eine Bisimulationsrelation  $\mathcal{S}$  mit  $S_2 \mathcal{S} (S_1 \mid S_1)$  zu finden.

Wähle:

$$\mathcal{S} = \{(S_2, S_1 \mid S_1), (S'_2, S'_1 \mid S_1), (S'_2, S_1 \mid S'_1), (S''_2, S'_1 \mid S'_1)\}$$

# Labelled Bisimulation

## Beispiel:

$$a.(b.0 + c.0) \not\sim a.b.0 + a.c.0$$

Angenommen es gäbe eine Bisimulation  $\mathcal{S}$  mit  $a.(b.0 + c.0) \mathcal{S} (a.b.0 + a.c.0)$ .

- Es gilt  $a.(b.0 + c.0) \xrightarrow{a} (b.0 + c.0)$ .
- Der zweite Prozess hat folgende  $a$ -Transitionen:  
 $(a.b.0 + a.c.0) \xrightarrow{a} b.0$  und  $(a.b.0 + a.c.0) \xrightarrow{a} c.0$ .
- Da  $\mathcal{S}$  eine Bisimulation ist, muss dann auch  $(b.0 + c.0) \mathcal{S} b.0$  oder  $(b.0 + c.0) \mathcal{S} c.0$  gelten.
- $(b.0 + c.0) \mathcal{S} b.0$  ist nicht möglich:  $(b.0 + c.0) \xrightarrow{c} 0$ , aber  $b.0 \not\xrightarrow{c}$ .
- $(b.0 + c.0) \mathcal{S} c.0$  ist nicht möglich:  $(b.0 + c.0) \xrightarrow{b} 0$ , aber  $c.0 \not\xrightarrow{b}$ .



# Barbed Equivalence und Labelled Bisimulation

**Satz:** Bisimulation  $\sim$  ist eine Kongruenz, d.h. aus  $P \sim Q$  folgt  $C[P] \sim C[Q]$  für alle Kontexte  $C[-]$ .

**Satz:** Es gilt  $\equiv \subseteq \sim$ .

Bisimulation kann benutzt werden, um Äquivalenzen zu zeigen:

**Satz:** Aus  $P \sim Q$  (Bisimulation) folgt  $P \simeq Q$  (Barbed Equivalence).

Unter vernünftigen Annahmen (Rekursion ist so eingeschränkt, dass jeder Prozess höchstens endlich viele Nachfolger haben kann) kann Bisimulation alle Äquivalenzen zeigen:

**Satz:** Aus  $P \simeq Q$  (Barbed Equivalence) folgt  $P \sim Q$  (Bisimulation).

Bisimulation quantifiziert nicht über alle Kontexte.