Aula 8

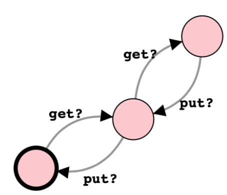
Bissimulação fraca e Congruência observável

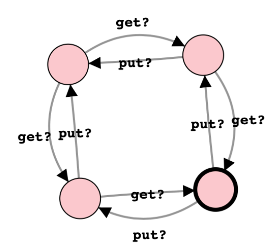
$2 - Buffer$

$$Buffer \quad := \quad put?.get?.Buffer$$

$$\begin{aligned} Buffer0 \quad &:= \quad put?.Buffer1 \\ Buffer1 \quad &:= \quad put?.Buffer2 + get?.Buffer0 \\ Buffer2 \quad &:= \quad get?.Buffer1 \end{aligned}$$

Será que $Buffer0 \sim (Buffer|Buffer)$?

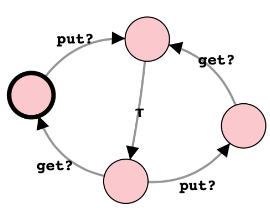


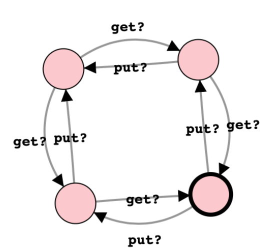


e

$$\begin{aligned} BufferL \quad &:= \quad put?.pass!.BufferL \\ BufferR \quad &:= \quad pass?.get?.BufferR \end{aligned}$$

Será que
$(BufferL|BufferR)\backslash\{pass!, pass?\} \sim (Buffer|Buffer)$?





1 Bissimilução fraca

Bissimulação Fraca

Ignora transições por τ. Seja $TS = (S, \longrightarrow, s_0)$. Uma relação $R \in S \times S$ é uma *bissimulação fraca* se $(s,t) \in R$ (ou $s\ R\ t$) implica para todo $\alpha \in Act$:

- se $s \xrightarrow{\alpha} s'$ então existe t' tal que $t \overset{\alpha}{\Rightarrow} t'$ e $(s', t') \in R$
- se $t \xrightarrow{\alpha} t'$ então existe s' tal que $s \overset{\alpha}{\Rightarrow} s'$ e $(s', t') \in R$.

Onde

Transições fracas

- $s \overset{\tau}{\Rightarrow} s'$ sse $\exists n \geq 0 : s \overset{\tau^n}{\rightsquigarrow} s'$
- $s \overset{a}{\Rightarrow} s'$ sse $\exists s'', s''' \in S : s \overset{\tau}{\Rightarrow} s'' \xrightarrow{a} s''' \overset{\tau}{\Rightarrow} s'$

Nota que

- $\longrightarrow \subseteq \Rightarrow$
- na definição de bissimulação fraca podemos usar sempre $\Rightarrow$.
- $s \overset{\tau}{\Rightarrow} s$ para todo o s.

Bissimilaridade fraca

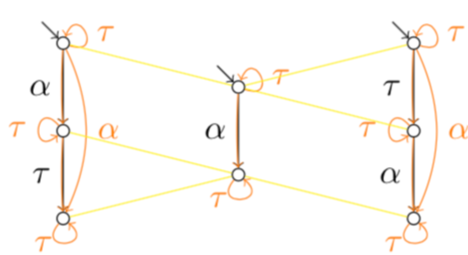
Dois estados s e t são *fracamente bissimilares*, e escreve-se $s \approx t$, se existe uma bissimulação fraca R que contêm (s,t), i.e $(s,t) \in R$.

Exemplo

Mostrar que

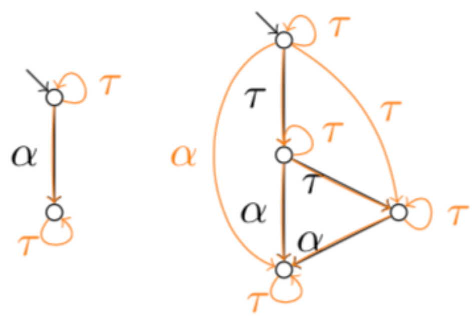
- $a.\tau.0 \approx a.0 \approx \tau.a.0$
- $\tau(a.0 + \tau.a.0) \approx a.0$

$$a.\tau.0 \approx a.0 \approx \tau.a.0$$



A laranja a relação $\Rightarrow$ e a amarelo a bissimulaçào R.

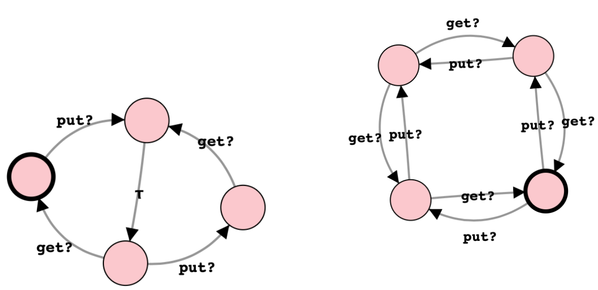
$$\tau(a.0 + \tau.a.0) \approx a.0$$



Exemplo dos Buffers

$$\begin{aligned} Buffer &:= put?.get?.Buffer \\ BufferL &:= put?.pass!.BufferL \\ BufferR &:= pass?.get?.BufferR \end{aligned}$$

$(BufferL|BufferR)\backslash\{pass!, pass?\} \approx (Buffer|Buffer)$



Não são fracamente bissimilares

$$(a!.b!.0) \not\approx (a!.b!.0 + \tau.0)$$

$$
\begin{tikzcd}
\arrow[r] & a!.b!.0 \arrow[d, "a!"] \\
& b!.0 \arrow[d, "b!"] \\
& 0
\end{tikzcd}
\qquad
\begin{tikzcd}
\arrow[r] & (a!.b!.0 + \tau.0) \arrow[d, "a!"] \arrow[dd, bend left, "\tau"] \\
& b!.0 \arrow[d, "b!"] \\
& 0
\end{tikzcd}
$$

- A: $a!.(b!.0 + \tau.0) \xrightarrow{\tau} 0$
- D: $a!.b!.0 \overset{\tau}{\Rightarrow} a!.b!.0$
- A: $a!.b!.0 \xrightarrow{a!} b!.0$
- D: não pode jogar com $a!$ porque 0 não tem transição fraca com $a!$.

Propriedades de $\approx$

$$\approx = \bigcup_{\text{R é bissimulação fraca}} R$$

Teorema 8.1. *A relação $\approx$ é de equivalência.*

Notar que se R é uma bissimulação fraca, R^{-1} também é (simetria).

Teorema 8.2. *A relação $\approx$ é maior bissimulação fraca .*

Mostrar que $\approx$ é uma bissimulação fraca.

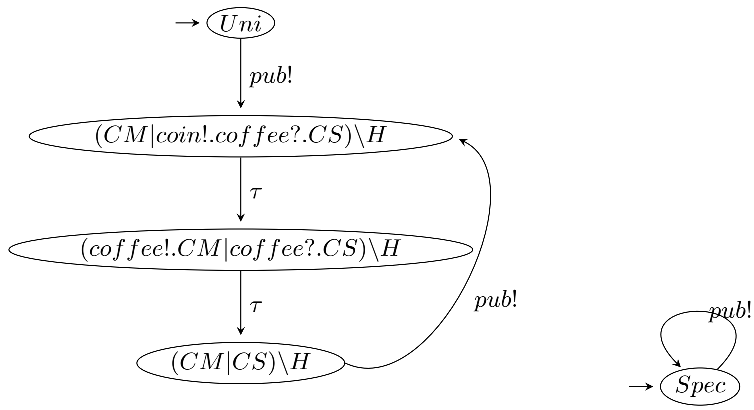
Teorema 8.3. *A bissimilaridade fraca é estritamente mais grosseira que a bissimilaridade forte, i.e $\sim \subsetneq \approx$.*

Cada bissimulação forte é uma bissimulação fraca. E vimos exemplos de processos que não bissimilares fortes mas que são bissimilares fracos. À bissimiliridade fraca também se chama *equivalência observável*.

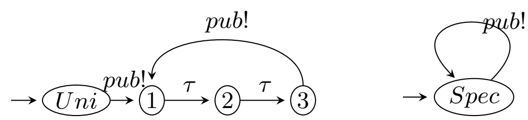
Será que $Spec \approx Uni$?

Seja $Spec := pub!.Spec$ e

$$
\begin{aligned}
CM &:= coin?.coffee!.CM \\
CS &:= pub!.coin!.coffee?.CS \\
Uni &:= (CM|CS)\backslash\{coin, coffee\}
\end{aligned}
$$



$Spec \approx Uni$



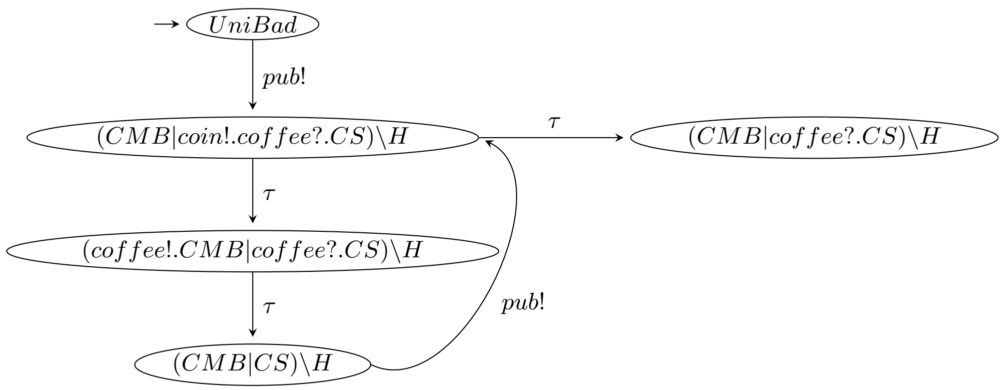
Jogo onde o defesa ganha. Configuração inicial $(Uni, Spec)$

- A: $Spec \xrightarrow{pub!} Spec$
- D: $Uni \overset{pub!}{\Rightarrow} 3$ $\qquad (3, Spec)$
- A: $3 \xrightarrow{pub!} 1$
- D: $Spec \xrightarrow{pub!} Spec$ $\qquad (1, Spec)$
- A: $1 \xrightarrow{\tau} 2$
- D: $Spec \overset{\tau}{\Rightarrow} Spec$ $\qquad (2, Spec)$
- A: $2 \xrightarrow{\tau} 3$
- D: $Spec \overset{\tau}{\Rightarrow} Spec$ $\qquad (3, Spec)$ (ciclo detectado)

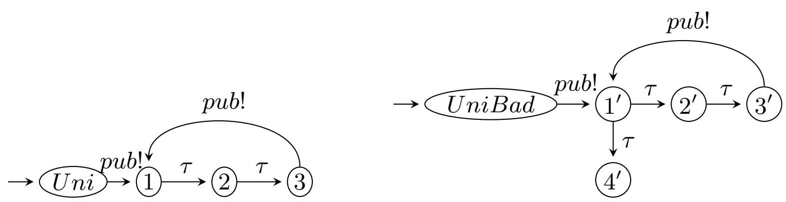
Será que $Uni \approx Unibad$?

$$\begin{array}{rcl} CM & := & coin?.coffee!.CM \\ CMB & := & coin?.coffee!.CMB + coin?.CMB \\ CS & := & pub!.coin!.coffee?.CS \\ Uni & := & (CM|CS)\backslash\{coin, coffee\} \\ UniBad & := & (CMB|CS)\backslash\{coin, cofee\} \end{array}$$

nestes caso não : $Uni \not\approx UniBad$ e é bom porque $UniBad$ pode entrar em deadlock e Uni não. (Verifica).



Jogo de bissimilaridade fraca entre $(Uni, UniBad)$.



O atacante ganha:

- A: $UniBad \xrightarrow{pub!} 1'$
- D: $Uni \overset{pub!}{\Rightarrow} 3$ $\qquad (3, 1')$
- A: $1' \xrightarrow{pub!} 4'$
- D: $3 \overset{\tau}{\Rightarrow} 3$ $\qquad (3, 4)$
- A: $3 \xrightarrow{pub!} 1$
- D: não pode jogar e perde.

A Bissimilaridade Fraca não é uma Congruência

Para todo $P, Q \in CCS$ se $P \approx Q$ e $\alpha \in Act$, $R \in CCS$ e $H \subseteq Com$,

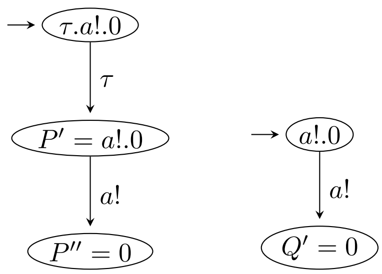
$$\begin{array}{rcl} \alpha.P & \approx & \alpha.Q \\ P|R & \approx & Q|R \\ R|P & \approx & R|Q \\ P\backslash H & \approx & Q\backslash H \end{array}$$

mas não implica que

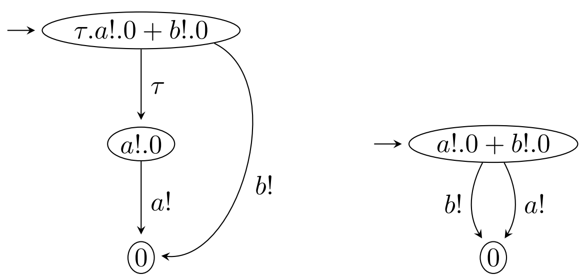
$$\begin{aligned} P + R &\approx Q + R \\ R + P &\approx R + Q \end{aligned}$$

Contraexemplo: $P = \tau.a!.0$, $Q = a!.0$ e $R = b!.0$.

- Mostrar que $P \approx Q$ considerando a relação $\mathcal{R} = \{(P, Q), (P', Q), (P'', Q')\}$ onde $P' = a!.0$ e $P'' = Q' = 0$ (mas em sistemas diferentes).



- Mostrar que $P + R \not\approx Q + R$.



- A: $\tau.a!.0 + b!.0 \xrightarrow{\tau} a!.0$
- D: $a!.0 + b!.0 \overset{\tau}{\Rightarrow} a!.0 + b!.0$
- A: $a!.0 + b!.0 \xrightarrow{b!} 0$
- D: não pode jogar porque não há nenhuma transição fraca de $a!.0$ por $b!$

O problema está nos processos não guardados! Neste caso o P.

Impondo a congruência do +

Congruência para a Escolha

Dois processos $P, Q \in CCS$ são *congruentes para a escolha*, e escreve-se $P \approx^{+} Q$ sse para todos os $R \in CCS$

$$P + R \approx Q + R$$

.

Pode-se provar que

- $\approx^+ \subsetneq \approx$ (tomando $R = 0$)
- $\approx^+$ é uma congruência e é a mais grosseira contida em $\approx$

Embora seja esta a noção de igualdade de processos que se pretende, não é fácil de usar por causa de *para todos os* $R \in CCS$. Vamos ver uma definição que é equivalente mas mais perto das outras definições de bissimulação.

Congruência Observável

Congruência Observável

Dois processos $P, Q \in CCS$ são congruentes para a observação, e escreve-se $P \simeq Q$ sse para todos $\alpha \in Act$ verifica-se que:

- se $P \xrightarrow{\alpha} P'$ então existe Q' tal que $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\alpha} \stackrel{\tau}{\Rightarrow} Q'$ e $P' \approx Q'$.
- se $Q \xrightarrow{\alpha} Q'$ então existe P' tal que $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\alpha} \stackrel{\tau}{\Rightarrow} P'$ e $P' \approx Q'$.

A diferença entre $\approx$ e $\simeq$ está que os passos internos iniciais não podem ser simulados por não haver movimento (lacete de τ).

Teorema 8.4. *Para todos os* $P, Q \in CCS$ $P \simeq Q$ *sse* $P \approx^+ Q$.

Exemplos

- $\tau.a \not\simeq a$
- $P|\tau.Q \not\simeq \tau.(P|Q)$

Igualdade de comportamento

- Dois processos $P, Q \in CCS$ *tem o mesmo comportamento* sempre que $P \simeq Q$.
- É chamada a *igualdade de comportamento*
- as propriedades pretendidas:
  - relação de equivalência
  - relação de congruência
  - ter o mesmo conjunto de traços *fracos*
  - seja sensível a deadlocks
- $\sim \subsetneq \simeq \subseteq \approx$
- em vez de $\simeq$ usa-se $=$.

Regras algébricas de = (leis τ de Milner)

Para além das satisfeitas por $\sim$ temos

$$\begin{array}{rcl} \alpha.\tau.P & = & \alpha.P \\ P+\tau.P & = & \tau.P \\ \alpha.(P+\tau.Q) & = & \alpha.(P+\tau.Q)+\alpha.Q \end{array}$$

Nota: as regras algébricas permitem provar a igualdade de processos pela aplicação das regras (em especial em CCS_0) ou considerá-las axiomas num sistema de dedução.

Representantes Minimais

- Para cada LTS podemos considerar o *representante minimal* o menor LTS cujo comportamento é igual ao LTS dado.
- O representante minimal é único a menos de isomorfismo se for estados-finito.
- É obtido pelo quociente induzido pela relação de equivalência ($\simeq$).
- cada classe de equivalência é um estado

Como obter o representante minimal

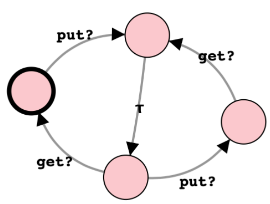
Dado um processo P do CCS estados-finito:

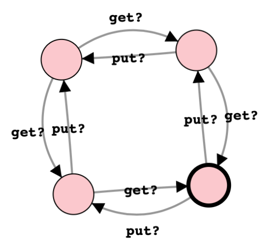
- Construir o LTS atíngível de P.
- Calcular a relação $\approx$
- Considerar a classe de equivalência de cada estado: $S = \{[s]_{\simeq} \mid s \in Reach(P)\}$
- Adicionar transições entre duas classes sempre que uma transição exista entre os elementos da respectiva classe.
- Podemos apagar as transições que seriam adicionadas por $\Rightarrow$ e não estavam em $\longrightarrow$.
- Adicionar um lacete com τ se P tem uma τ-transição para a sua classe $[P]_{\approx}$.

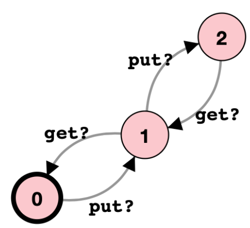
Exemplo:$2 - Buffer$

$$\begin{array}{rcl} Buffer & := & put?.get?.Buffer \\ BufferL & := & put?.pass!.BufferL \\ BufferR & := & pass?.get?.BufferR \end{array}$$

Será que $(BufferL|BufferR)\backslash\{pass!, pass?\} \simeq (Buffer|Buffer)$?







Sim e o LTS minimo equivalente é