Άλγεβρες Διεργασιών και Σχέσεις Ισοδυναμίας

Στην ενότητα αυτή θα μελετηθούν τα εξής θέματα:

Σχέσεις ισοδυναμίας

- *trace equivalence*
- *failure equivalence*
- *strong bisimulation*
- *weak bisimulation*

Σχέσεις ισοδυναμίας - κίνητρα

- Προδιαγραφή: Ένας χρονοδρομολογητής τύπου round-robin πρέπει να παράγει κυκλικά τα μηνύματα $\alpha_1, \alpha_2, \ldots, \alpha_n$ ξεκινώντας με το μήνυμα α_1.
- Αυτή η πρόταση δεν μπορεί να προσδιοριστεί σε χρονική λογική.
- Ουσιαστικά, ζητούμε η εξωτερική συμπεριφορά του χρονοδρομολογητή να "ισοδυναμεί" με

$$Spec \stackrel{def}{=} a_1.a_2.\ldots..a_n.Spec$$

- Πολλές προδιαγραφές μπορούν να διατυπωθούν με προτάσεις του τύπου "η συμπεριφορά του συστήματος πρέπει να είναι όμοια με". Για παράδειγμα, η χρήση telnet προς μια μηχανή πρέπει να παρουσιάζει "πανομοιότυπη" συμπεριφορά με τη χρήση της ίδιας μηχανής.
- Πως μπορούμε να ορίσουμε αυτού του είδους ισοδυναμίες συμπεριφοράς.

Σημαντικές ιδιότητες

1. Σχέσεις ισοδυναμίας πρέπει να είναι ανακλαστικές, συμμετρικές και μεταβατικές.

2. Διεργασίες που τερματίζουν δεν πρέπει να είναι ισοδύναμες με διεργασίες που δεν τερματίζουν.

3. Αν δύο διεργασίες είναι ισοδύναμες μεταξύ τους τότε η χρήση οποιασδήποτε από τις δύο ως κομμάτι ενός μεγαλύτερου συστήματος δεν πρέπει να επηρεάζει τη συμπεριφορά του συστήματος.

4. Δύο διεργασίες μπορούν να είναι ισοδύναμες αν ικανοποιούν τις ίδιες ιδιότητες που μπορούν να εκφραστούν σε μια λογική.

Ισοδυναμία Διεργασιών

- Πότε μπορούμε να θεωρούμε δύο διεργασίες ισοδύναμες;
- Έστω $E=a.(b.0 + c.0)$

  $F=a.b.0 + a.c.0$
- Έστω τα συστήματα μεταβάσεων τους όπου ας θεωρήσουμε κάθε κατάσταση ως αποδεκτή:

Ισοδυναμία ίχνους – trace equivalence

- Και οι δύο διεργασίες αποδέχονται τη γλώσσα $\{\varepsilon, a, ab, ac\}$ και θεωρούνται ισοδύναμες στη θεωρία των μη-ντετερμινιστικών πεπερασμένων αυτομάτων και των κανονικών γλωσσών.

- Όταν δύο διεργασίες αντιστοιχούν σε αυτόματα που αποδέχονται τις ίδιες γλώσσες, ή, με άλλα λόγια, έχουν τις ίδιες εκτελέσεις, ονομάζονται **ισοδύναμες ως προς την ισοδυναμία ίχνους** (trace equivalent).

- *Ερώτημα*: Ποιες ιδιότητες (Διαφάνεια 8-3) ικανοποιούνται από την ισοδυναμία ίχνους;

Trace equivalence

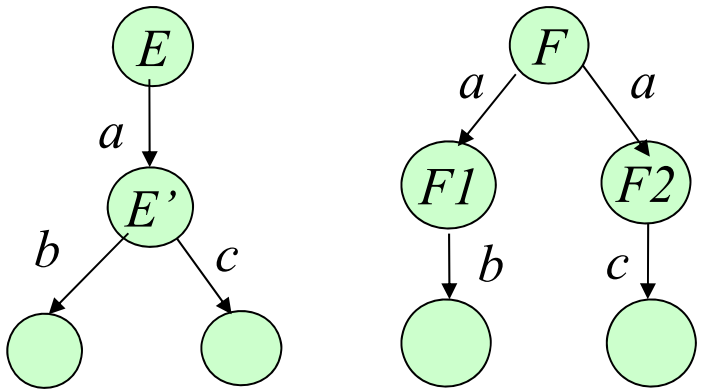
- Θεωρήστε μια τρίτη διεργασία "ελέγχου" $G = \overline{a}.\overline{b}.\overline{w}.0$ (η ετικέτα w υποδηλώνει "επιτυχία".
- Τοποθετώντας την G παράλληλα σε κάθε μια από τις E και F

$$(E \mid\mid G) \setminus L,\ (F \mid\mid G) \setminus L \qquad \text{όπου } L = \{a, b, c\}$$

  έχουμε ότι στην πρώτη περίπτωση ο έλεγχος τερματίζει με επιτυχία ενώ στη δεύτερη περίπτωση η αλληλεπίδραση ανάμεσα στις F και G δυνατόν να τερματίσει χωρίς επιτυχία.
- Αυτό οφείλεται στο *μη-ντετερμινισμό* της διεργασίας G.
- Επομένως η ισοδυναμία ίχνους δεν ικανοποιεί την ιδιότητα 3.

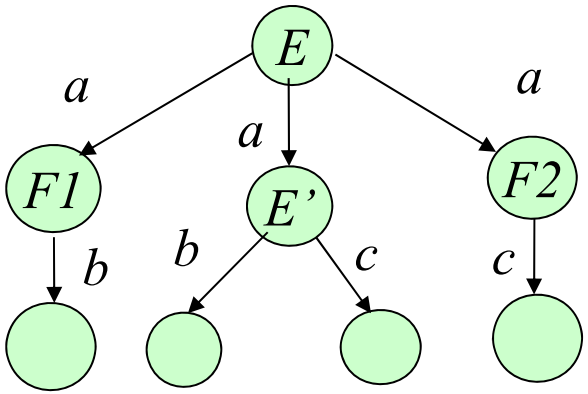
Ισοδυναμία με αποτυχίες

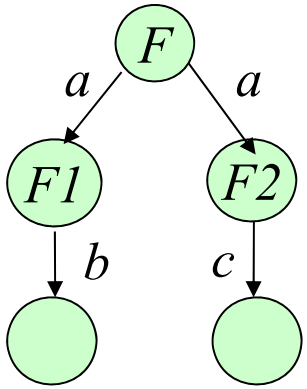
- Εκτός από τις εκτελέσεις σημειώνουμε επίσης τις "αποτυχίες" μιας διεργασίας.
- Μία *αποτυχία* είναι ένα ζεύγος (σ, X) όπου σ είναι μία λέξη και X ένα σύνολο από ενέργειες.
- Κάποια διεργασία εμφανίζει την αποτυχία (σ, X) αν μετά από την εκτέλεση της λέξης σ είναι ανίκανη να εκτελέσει κάποια ενέργεια από το σύνολο X.
- Η διεργασία F έχει αποτυχία (α, $\{c\}$) ενώ η διεργασία E δεν έχει αυτή την αποτυχία.



Ισοδυναμία με αποτυχίες

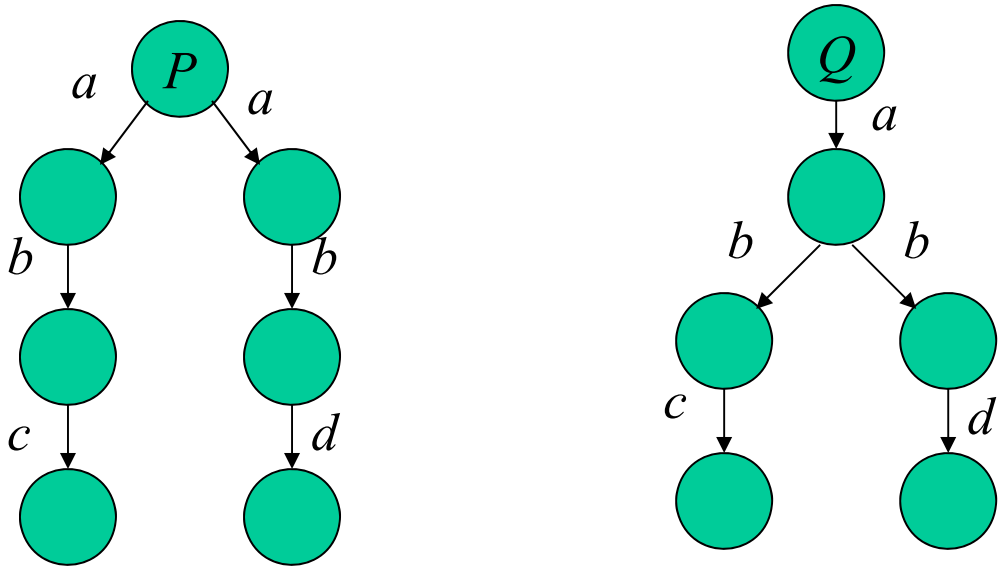
- Δύο διεργασίες ονομάζονται **ισοδύναμες ως προς την ισοδυναμία αποτυχίας** (failure equivalent) αν έχουν ακριβώς τις ίδιες αποτυχίες.
- Η σχέση αυτή επίσης δεν ικανοποιεί την ιδιότητα 3.





Ισοδυναμία προσομοίωσης

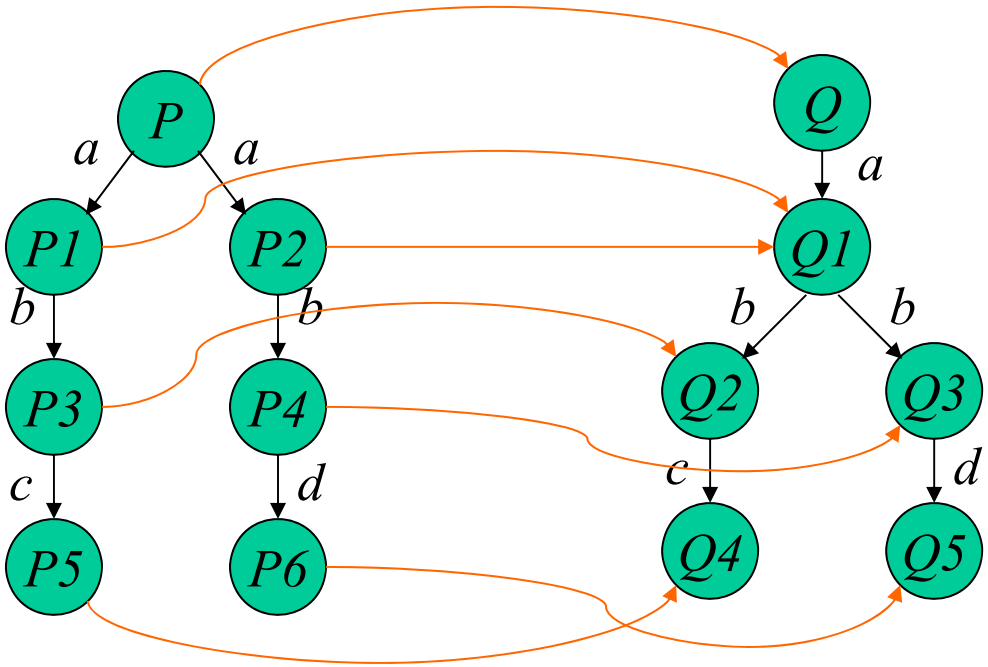
- Μία σχέση S⊆**P**×**P** ονομάζεται *ισοδυναμία προσομοίωσης* (simulation equivalence) αν για κάθε *(P,Q)*∈S, τότε για κάθε *α* ∈*Act*
  - Αν $P \xrightarrow{a} P'$ τότε υπάρχει *Q'* τέτοιο ώστε $Q \xrightarrow{a} Q'$ και (*P'*, *Q'*) ∈S.



Η Q προσομοιώνει την P

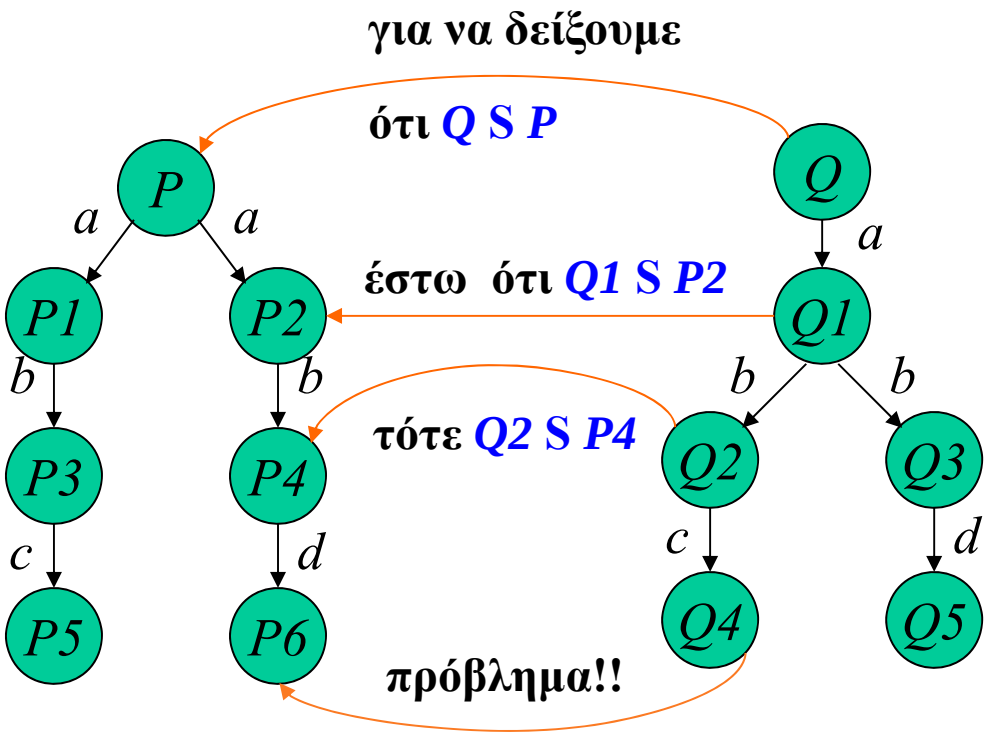
- Η σχέση που ψάχνουμε είναι η

$$S = \{(P,Q), (P1,Q1), (P2,Q1), (P3,Q2), (P4,Q3), (P5,Q4), (P6,Q5)\}$$

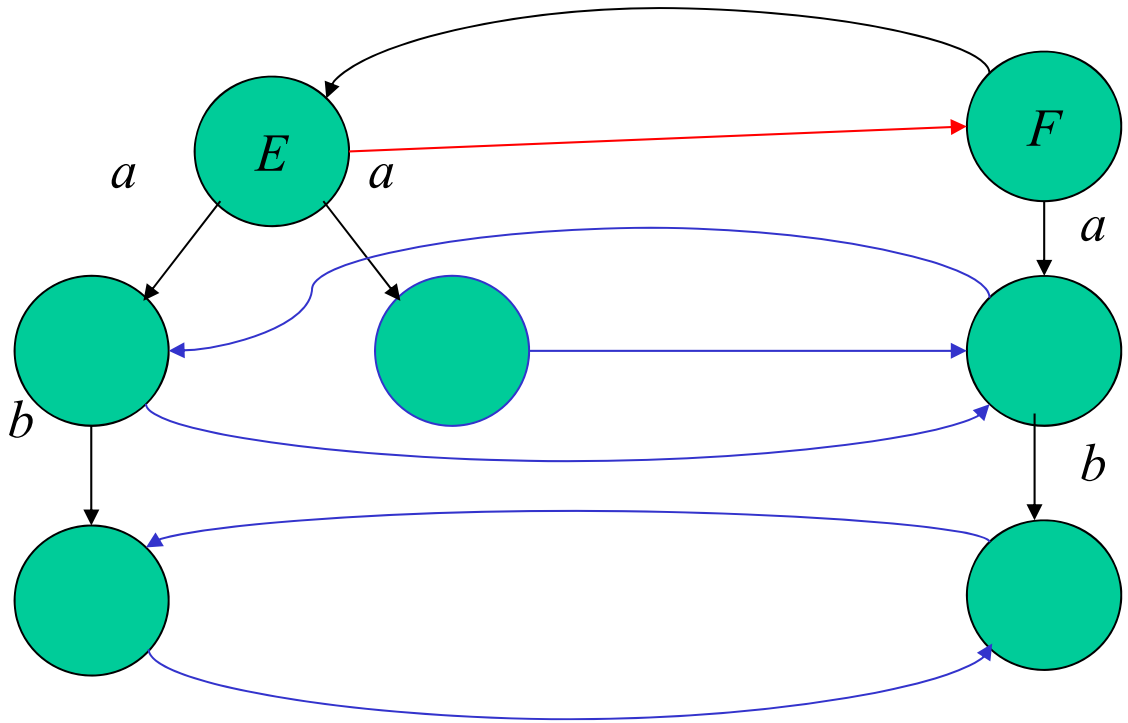


Η *P* προσομοιώνει την *Q* ;;;

- Για να δείξουμε ότι η *P* προσομοιώνει τη *Q* θα πρέπει είτε η *P1* είτε *η P2* να προσομοιώνει τη *Q1*. Αυτό όμως δεν ισχύει.



Ισοδυναμία προσομοίωσης vs ισοδυναμία αποτυχίας



Οι δύο διεργασίες προσομοιώνουν η μια την άλλη δεν έχουν όμως τις ίδιες αποτυχίες: η διεργασία $E = a.b.0 + a$, έχει την αποτυχία $(a, \{b\})$ που δεν ανήκει στις αποτυχίες της F.

Strong Bisimulation

- Μία σχέση $S \subseteq \mathbf{P} \times \mathbf{P}$ ονομάζεται *ισχυρή δυπροσομοίωση* αν για κάθε $(P,Q) \in S$, τότε για κάθε $\alpha \in Act$

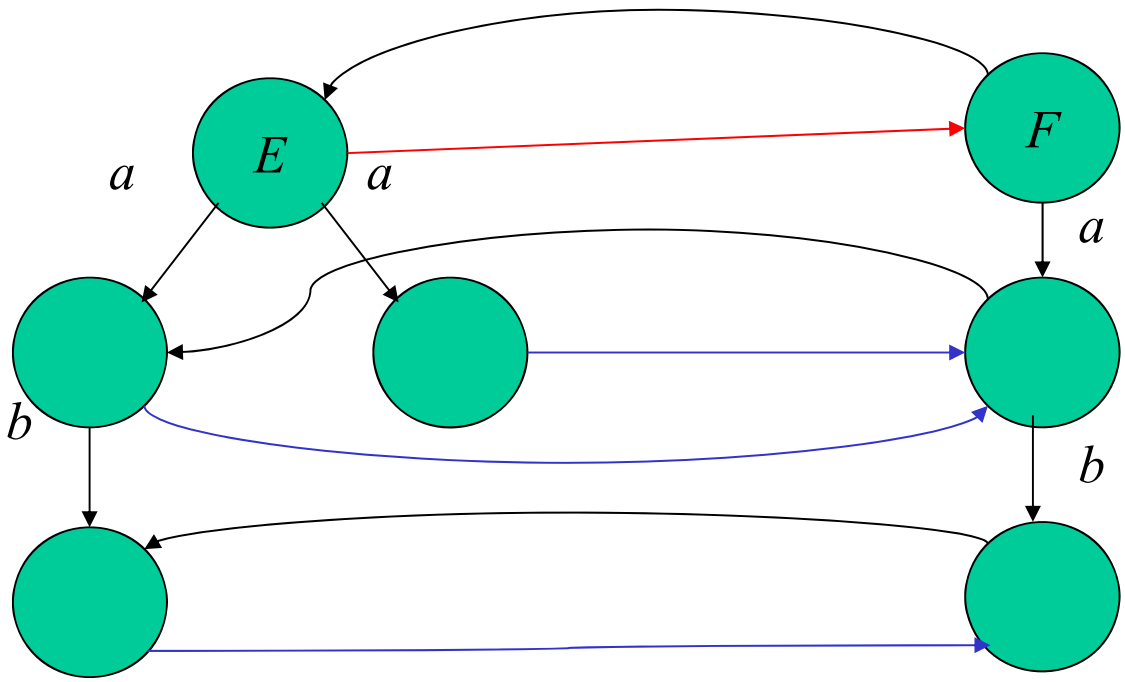
  1. Αν $P \xrightarrow{a} P'$ τότε υπάρχει Q' τέτοιο ώστε $Q \xrightarrow{a} Q'$ και $(P', Q') \in S$
  2. Αν $Q \xrightarrow{a} Q'$ τότε υπάρχει P' τέτοιο ώστε $P \xrightarrow{a} P'$ και $(P', Q') \in S$

- Σχηματικά

$$
\begin{tikzcd}
P \arrow[r, dashed, leftrightarrow] \arrow[d, "a"'] & \mathbf{S} \arrow[r, dashed, leftrightarrow] & Q \arrow[d, "a"] \\
P' \arrow[r, dashed, leftrightarrow] & \mathbf{S} \arrow[r, dashed, leftrightarrow] & Q'
\end{tikzcd}
$$

$\forall$ $\exists$

Προσοχή: η ίδια σχέση ισχύει και στις δύο κατευθύνσεις



Τα E και F σχετίζονται μέσω ισχυρής δυπροσομοίωσης;

Ισχυρή ισοδυναμία

- Δύο διεργασίες P και Q ονομάζονται *ισχυρά ισοδύναμες* (strongly equivalent or strongly bisimilar), αν υπάρχει σχέση ισχυρής δυπροσομοίωσης που τις συνδέει.

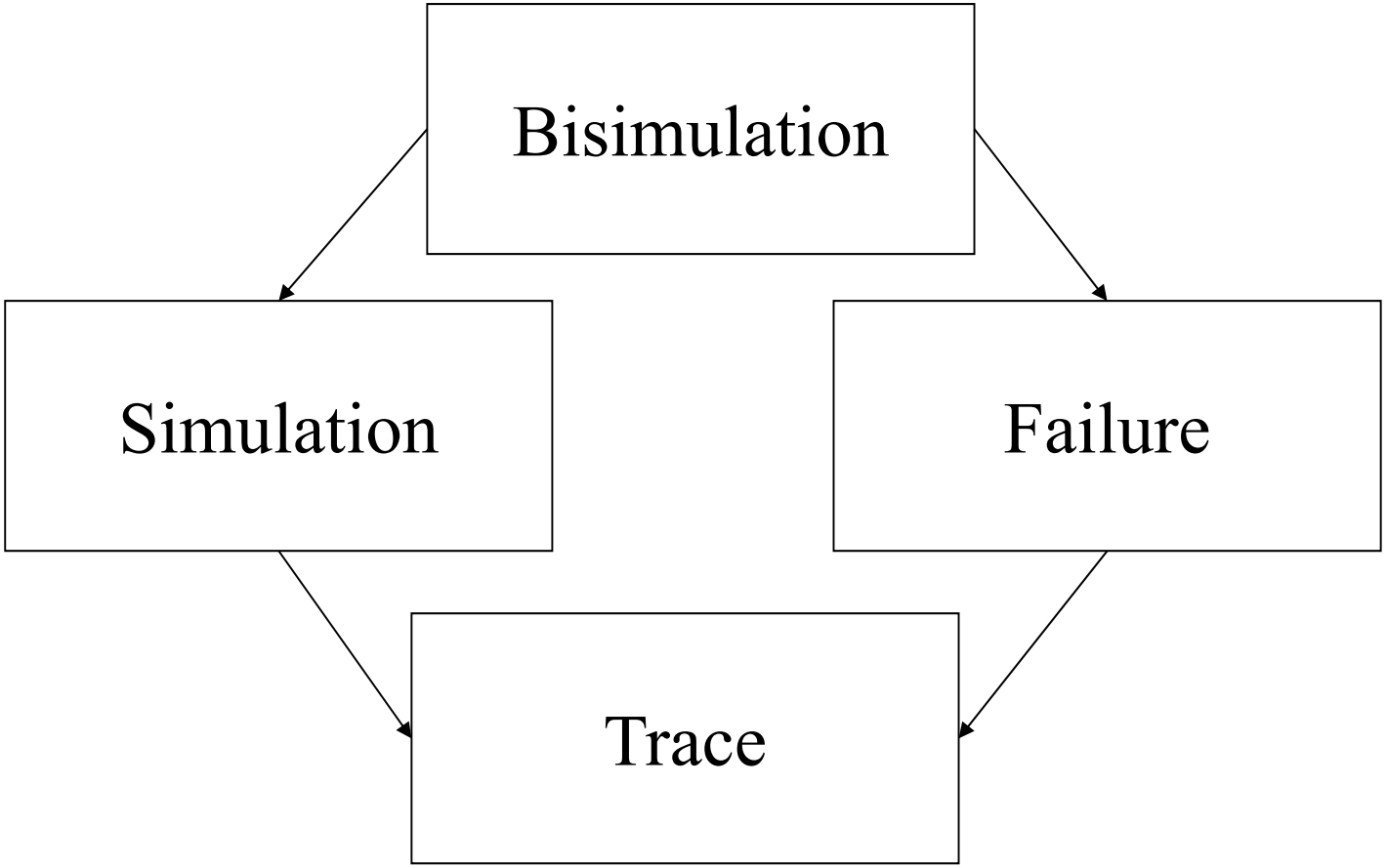
- Συμβολίζουμε το γεγονός ότι δύο διεργασίες είναι ισχυρά ισοδύναμες ως $P \sim Q$.

- Προφανώς

$$\sim \; = \cup \{ \text{ S} \mid \text{ S είναι σχέση ισχυρής δυπροσομοίωσης } \}$$

- *Αυτό εισηγείται πως για να αποφασίσουμε κατά πόσο δύο διεργασίες συνδέονται από τη σχέση ~ θα πρέπει να βρούμε μια σχέση ισχυρής δυπροσομοίωσης που τις συνδέει.*

Ιεραρχία ισοδυναμιών



Παραδείγματα

1. $a.c.0 + b.0 \sim (a.c.0 + b.0) + a.c.0$

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

3. $a.b.0 \not\sim a.b.0 + a.0$

Παράδειγμα: Σημαφόρη

$Sem_n\ (0) = get.\ Sem_n(1)$

$Sem_n\ (k) = get.\ Sem_n(k + 1) + put.\ Sem_n(k - 1) \qquad 0 < k < n$

$Sem_n\ (n) = put.\ Sem_n(n - 1)$

$Sem = get.\ Sem'$

$Sem' = put.\ Sem$

$$\boldsymbol{Sem_2\ (0) \sim Sem \mid Sem}$$

Αποδεικνύοντας ότι $P \sim Q$

- Ιδέα: Κτίσε μια ισχυρή δυπροσομοίωση που να περιέχει το ζεύγος (P, Q).

- Αυτό είναι ορθό αφού από τον ορισμό του ~:

  $P \sim Q$ αν και μόνο αν υπάρχει σχέση ισχυρής δυπροσομοίωσης S για την οποία $(P, Q) \in$ S.

Αποδείξτε ότι: $a.b.0 \sim a.b.0 + a.b.(0 + 0)$

Αποδεικνύοντας ότι $P \not\sim Q$

- $P \sim Q$ αν και μόνο αν υπάρχει σχέση ισχυρής δυπροσομοίωσης S για την οποία $(P, Q) \in S$.
- Επομένως για να δείξουμε ότι $P \not\sim Q$ πρέπει να δείξουμε ότι δεν υπάρχει σχέση ισχυρής δυπροσομοίωσης που να συνδέει τις δύο διεργασίες.
- Η απόδειξη είναι με αντίφαση:
  - Υπέθεσε ότι υπάρχει σχέση ισχυρής δυπροσομοίωσης ανάμεσα στις δύο διεργασίες
  - Δείξε ότι αυτό οδηγεί σε αντίφαση.

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

- Υποθέτουμε για να φθάσουμε σε αντίφαση ότι S είναι μια σχέση ισχυρής δυπροσομοίωσης για την οποία $(P, Q) \in$S όπου

$$P \equiv a.(b.0 + c.0)$$

$$Q \equiv a.b.0 + a.c.0$$

- Αφού η S είναι σχέση δυπροσομοίωσης και η διεργασία P με την ενέργεια α εξελίσσεται στη διεργασία $b.0 + c.0$ τότε θα πρέπει να υπάρχει εξέλιξη της διεργασίας Q, έστω Q' για την οποία $(b.0 + c.0, Q') \in$S. Υπάρχουν δύο υποψήφιες διεργασίες Q':
  1. Αν $(b.0 + c.0, b.0) \in$S, και αφού $b.0 + c.0 \xrightarrow{c} 0$ πρέπει $b.0 \xrightarrow{c} 0$ που είναι αδύνατη μετάβαση => αντίφαση.
  2. Αν $(b.0 + c.0, c.0) \in$S και αφού $b.0 + c.0 \xrightarrow{b} 0$ πρέπει $c.0 \xrightarrow{b} 0$ που είναι αδύνατη μετάβαση => αντίφαση.

- Επομένως δεν υπάρχει τέτοια σχέση S και το ζητούμενο έπεται.

Ζητούμενες ιδιότητες

- Ιδιότητα 1: Μπορούμε να επαληθεύσουμε ότι
  - $E \sim E$ για κάθε E
  - Αν $E \sim F$ τότε $F \sim E$
  - Αν $E \sim F$ και $F \sim G$ τότε $E \sim G$
- Ιδιότητα 2: Ικανοποιείται.
- Ιδιότητα 3: Μπορούμε να επαληθεύσουμε ότι αν $E \sim F$, τότε, για οποιαδήποτε ενέργεια a, σύνολο καναλιών L και συνάρτηση μετονομασίας f,
  - $a.E \sim a.F$ $\quad$ $E + G \sim F + G$
  - $E \mid G \sim F \mid G$ $\quad$ $E \setminus L \sim F \setminus L$
  - $E[f] \sim F[f]$
- Ιδιότητα 4: Υπάρχει λογική (η HML που θα μελετήσουμε αργότερα) για την οποία δυο διεργασίες είναι ισοδύναμες αν και μόνο αν ικανοποιούν τις ίδιες HML ιδιότητες.

Ισοδυναμία παρατήρησης

- Η ισχυρή ισοδυναμία επιβάλλει τον εξής περιορισμό:
  - Εξαναγκάζει τη θεώρηση εσωτερικών ενεργειών και την προσομοίωσή τους από ισοδύναμες διεργασίες:

    π.χ. $in.out.0 \not\sim in.\tau.\tau.out.0$

- Για να ξεπεράσουμε τον περιορισμό ορίζουμε μια σύνθετη σχέση μεταβάσεων που "απορροφά" τις εσωτερικές ενέργειες:

$$P \overset{\varepsilon}{\Longrightarrow} Q \qquad iff \qquad \underbrace{P \xrightarrow{\tau} \ldots \xrightarrow{\tau} Q}_{\geq 0}$$

$$P \overset{a}{\Longrightarrow} Q \qquad iff \qquad P \overset{\varepsilon}{\Longrightarrow} P' \xrightarrow{a} Q' \overset{\varepsilon}{\Longrightarrow} Q$$

$$\hat{a} = \begin{cases} \varepsilon, & \text{if} \quad a = \tau \\ a, & \text{otherwise} \end{cases}$$

Παραδείγματα

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\varepsilon}{\Rightarrow} \tau.\tau.b.0 + \tau.a.\tau.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\tau}{\not\Rightarrow} \tau.\tau.b.0 + \tau.a.\tau.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\varepsilon}{\Rightarrow} b.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\tau}{\Rightarrow} b.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\hat{\tau}}{\Rightarrow} b.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{a}{\Rightarrow} \tau.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{\hat{a}}{\Rightarrow} \tau.0$$

$$\tau.\tau.b.0 + \tau.a.\tau.0 \overset{a}{\Rightarrow} 0$$

Weak Bisimulation

- Μία σχέση S $\subseteq$ **P**×**P** ονομάζεται *ασθενής δυπροσομοίωση* αν για κάθε *(P,Q)*$\in$S, τότε για κάθε *α* $\in$*Act*
  1. Αν $P \xrightarrow{a} P'$ τότε υπάρχει *Q'* τέτοιο ώστε $Q \overset{\hat{a}}{\Rightarrow} Q'$ και (*P'*, *Q'*) $\in$S
  2. Αν $Q \xrightarrow{a} Q'$ τότε υπάρχει *P'* τέτοιο ώστε $P \overset{\hat{a}}{\Rightarrow} P'$ και (*P'*, *Q'*) $\in$S

- Σχηματικά

$$\begin{tikzcd}
P \arrow[r, dash] \arrow[d, "\forall\ a"'] & \mathbf{S} \arrow[r, dash] & Q \arrow[d, Rightarrow, "\exists\ \hat{a}"] \\
P' \arrow[r, dash] & \mathbf{S} \arrow[r, dash] & Q'
\end{tikzcd}$$

- Γράφουμε $P \approx Q$ αν υπάρχει σχέση ασθενής δυπροσομοίωσης S, με *(P,Q)*$\in$S.

Αποδεικνύοντας ότι $P \approx Q$ ή $P \not\approx Q$

- Οι τεχνικές είναι παρόμοιες με αυτές του ~:

- Για να δείξουμε ότι $P \approx Q$ κτίζουμε μια σχέση ασθενούς προσομοίωσης που περιέχει το ζεύγος (P, Q).

- Για να δείξουμε ότι $P \not\approx Q$ αποδεικνύουμε με αντίφαση πως δεν υπάρχει σχέση ασθενούς προσομοίωσης που περιέχει το ζεύγος (P, Q).

Αποδείξτε ότι: $a.\tau.b.0 \approx a.b.0$

Αποδείξτε ότι: $a.0 + \tau.b.0 \not\approx a.0 + b.0$

Παράδειγμα

Έστω

$$Sender = send.\ \overline{out}.\ ackin.\ Sender$$

$$Medium = out.\ \overline{in}.\ Medium + ackout.\ \overline{ackin}.\ Medium$$

$$Receiver = in.\ \overline{rec}.\ \overline{ackout}.\ Receiver$$

$$System = (\ Sender \mid Medium \mid Receiver\ ) \setminus \{\ in, out, ackin, ackout\}$$

$$Spec = send.\ \overline{rec}.\ Spec$$

Τότε $$System \approx Spec$$

Παράδειγμα (συν.): Ασθενής Δυπροσομοίωση

Ιδιότητες ασθενούς δυπροσομοίωσης

- Η ισοδυναμία παρατήρησης (observational equivalence), ή, ισοδυναμία ασθενούς δυπροσομοίωσης, (weak bisimilarity) έχει τα εξής θετικά στοιχεία:
  - Ο αναδρομικός ορισμός της επιτρέπει αναδρομικές διαδικασίες ελέγχου.
  - Η απόκρυψη εσωτερικών ενεργειών δίνει μια χρήσιμη έκφραση της σχέσης ότι ένα σύστημα *υλοποιεί* κάποια προδιαγραφή.
  - Κομψές τεχνικές που κληρονομούνται από την ισοδυναμία ισχυρής δυπροσομοίωσης.

- Μειονέκτημα:
  - δεν ικανοποιεί την ιδιότητα 3 (διαφάνεια 8-3), ή, σύμφωνα με την επικρατούσα ορολογία, δεν είναι *congruence* για τους τελεστές της CCS…

Ισοδυναμία παρατήρησης

- Μια σχέση ισοδυναμίας ονομάζεται *congruence* για μια γλώσσα αν μπορούμε να αντικαθιστούμε "ίσα" με "ίσα".
- Αυτό είναι χρήσιμο για *συνθετική* ανάλυση συστημάτων, δηλαδή για τη δυνατότητα εξαγωγής συμπερασμάτων σχετικά με ένα σύστημα από ιδιότητες των συνιστούντων κομματιών του.
- Για παράδειγμα, μια σχέση $\cong$ είναι congruence για τη γλώσσα CCS αν το γεγονός $P \cong Q$ συνεπάγεται ότι
  1. $a.P \cong a.Q$
  2. $P + R \cong Q + R$ για κάθε R
  3. $P \mid R \cong Q \mid R$ για κάθε R
  4. $P \setminus L \cong Q \setminus L$ για κάθε L
  5. $P[f] \cong Q[f]$ για κάθε f
- Για τη σχέση $\approx$ ισχύουν όλα τα πιο πάνω εκτός από το 2.

Το πρόβλημα με τον τελεστή +

- Ενώ $\tau.b.0 \approx b.0$

  $$a.0 + \tau.b.0 \not\approx a.0 + b.0$$

- Οφείλεται στην αρχική εσωτερική ενέργεια.
- Θα προσπαθήσουμε να λύσουμε το πρόβλημα με εκλέπτυνση της σχέσης $\approx$ σε μια νέα σχέση $\approx_C$.

Ισοδυναμία παρατήρησης – προσπάθεια 2

- $(P,Q) \in \approx_C$ αν για κάθε $\alpha \in Act$

  1. Αν $P \xrightarrow{a} P'$ τότε υπάρχει Q' τέτοιο ώστε $Q \overset{a}{\Rightarrow} Q'$ και $P' \approx Q'$
  2. Αν $Q \xrightarrow{a} Q'$ τότε υπάρχει P' τέτοιο ώστε $P \overset{a}{\Rightarrow} P'$ και $P' \approx Q'$

- Ο ορισμός αυτός ουσιαστικά επεκτείνει τη σχέση ≈ δηλώνοντας ότι οι αρχικές εσωτερικές ενέργειες πρέπει να αντιστοιχούνται (ασθενώς) από ισοδύναμες διεργασίες.

Η σχέση ισοδυναμίας $\approx_C$

1. $\tau.b.0 \not\approx_C b.0$
2. $\alpha.\tau.b.0 \approx_C \alpha.b.0$
3. Αν $P \approx Q$, $P \not\xrightarrow{\tau}$ και $Q \not\xrightarrow{\tau}$ τότε $P \approx_C Q$
4. Αν $P \approx Q$ τότε ισχύει ένα (τουλάχιστον) από τα ακόλουθα $P \approx_C Q$, $\tau.P \approx_C Q$ και $P \approx_C \tau.Q$.

- Πόσο καλή είναι η σχέση $\approx_C$;…
- …Είναι η μεγαλύτερη σχέση τύπου congruence που περιλαμβάνεται στην $\approx$. Δηλαδή
  - Αν $P \approx_C Q$ τότε $P \approx Q$
  - Για κάθε congruence $\approx_D \subseteq \approx$ ισχύει ότι $\approx_D \subseteq \approx_C$.