Refinement-Robust Fairness

Hagen Völzer
Institut für Theoretische Informatik
Universität zu Lübeck

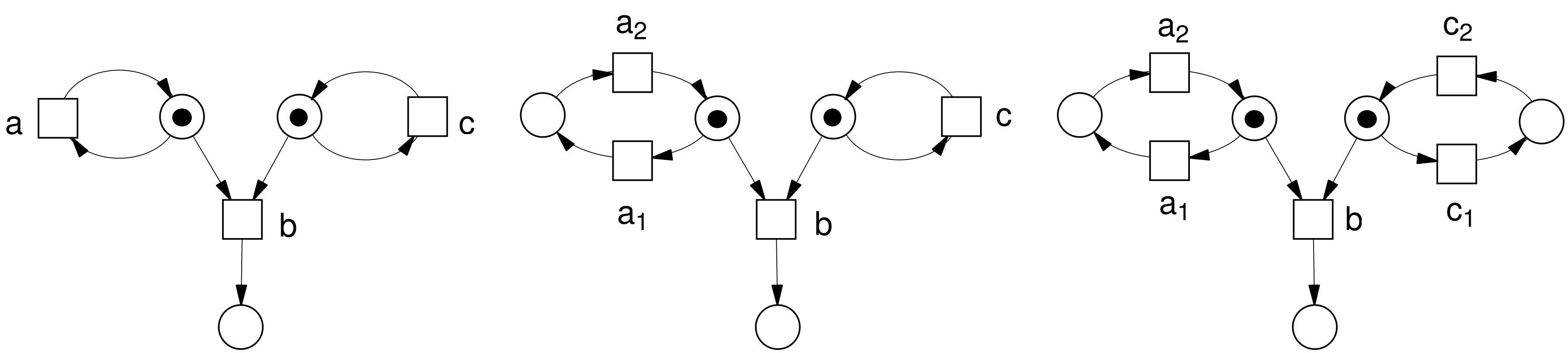
May 10, 2005

Overview

1. Problem
2. Formalization
3. Solution
4. Remarks

Problem

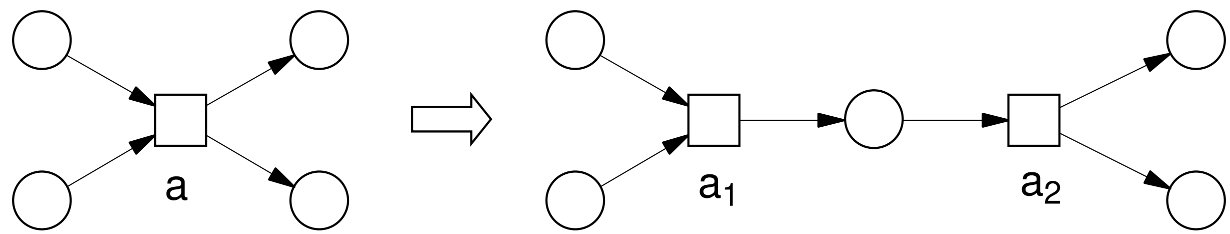
- weak fairness wrt t: $\Diamond \Box \text{enabled}(t) \Rightarrow \Box \Diamond \text{taken}(t)$
- strong fairness wrt t: $\Box \Diamond \text{enabled}(t) \Rightarrow \Box \Diamond \text{taken}(t)$



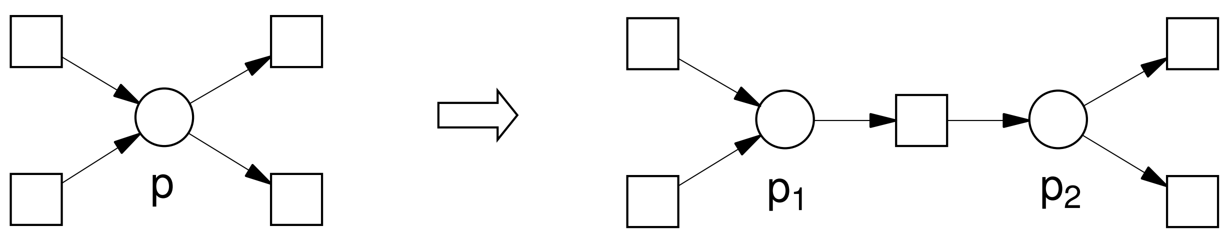
$\Rightarrow$ weak and strong fairness are not robust under refinement

Two refinements

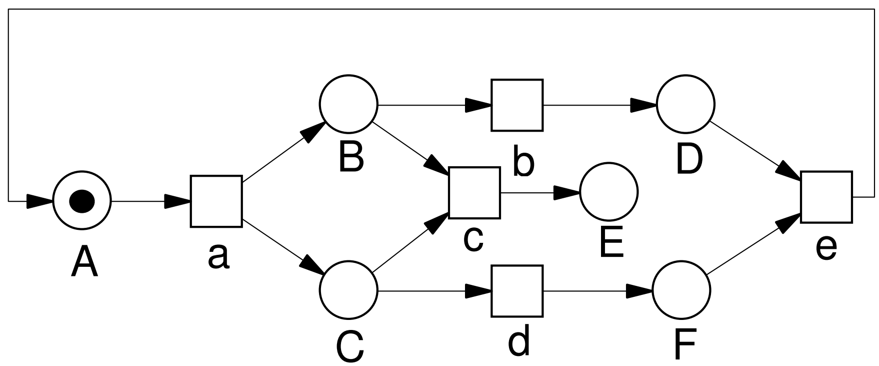
T-refinement:

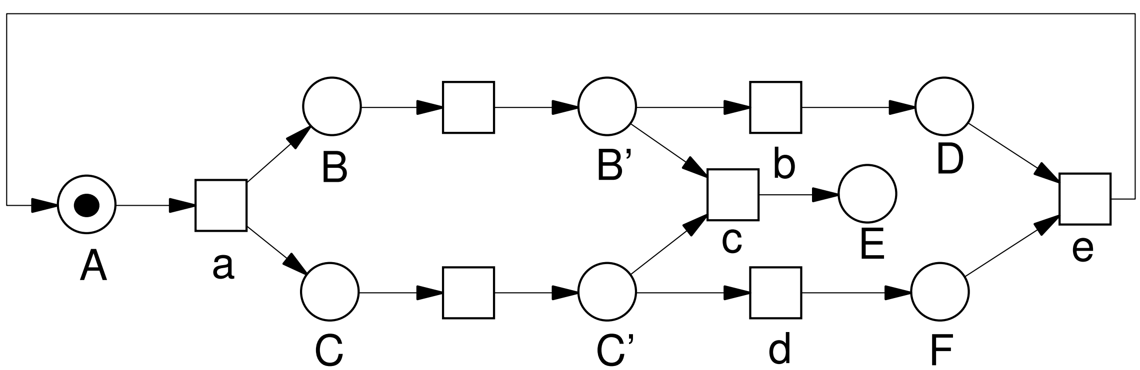


P-refinement:



Strong fairness and P-refinement





Outline

- recall *refinement-robust version* of weak fairness (Progress)
- introduce refinement-robust version of strong fairness (Simple Fairness)
- present other interesting refinement-robust fairness notions
- notions form a hierarchy
- hierarchy is based on *conflict structure* (free choice, asymmetric choice etc.)

Overview

1. Problem

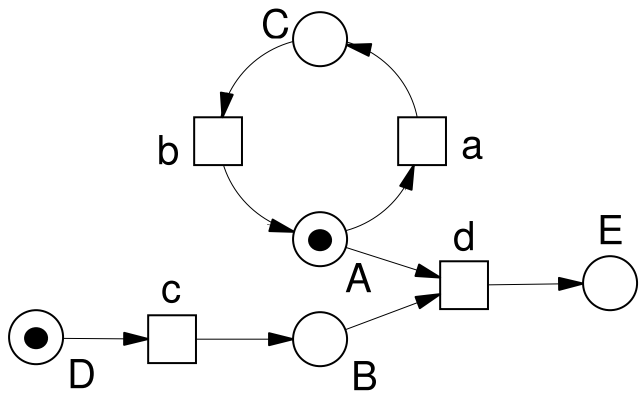
2. Formalization

3. Solution

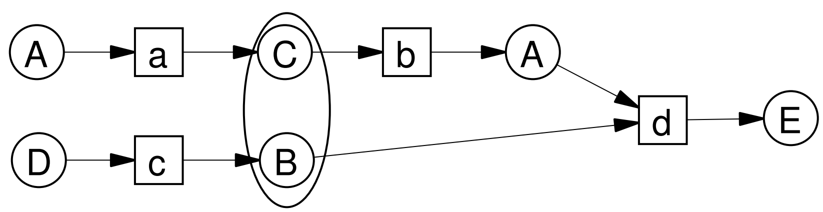
4. Remarks

Preliminaries

A (safe) system:

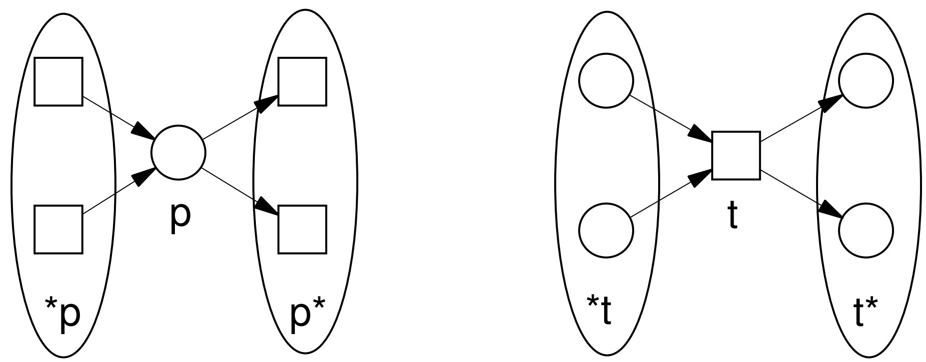


A non-sequential run:



Recall: *co-set* (of conditions)

Preliminaries (contd.)



$$^\bullet X = \bigcup_{x \in X} {}^\bullet x \qquad X^\bullet = \bigcup_{x \in X} x^\bullet$$

Refinement-Robustness

Refinement: φ : Nets $\longrightarrow$ Nets
(lifted: φ : Net systems $\longrightarrow$ Net systems)

Fairness assumption: $f : \Sigma \mapsto$ subset of non-sequential runs of Σ

Refinement-robustness: f is *φ-robust* if for all Σ, we have

$$f(\varphi(\Sigma)) = \varphi(f(\Sigma))$$

Refinement-Robustness

Implication: Linear-time semantics with refinement-robust fairness is preserved under refinement: f, g are φ-robust $\Rightarrow$

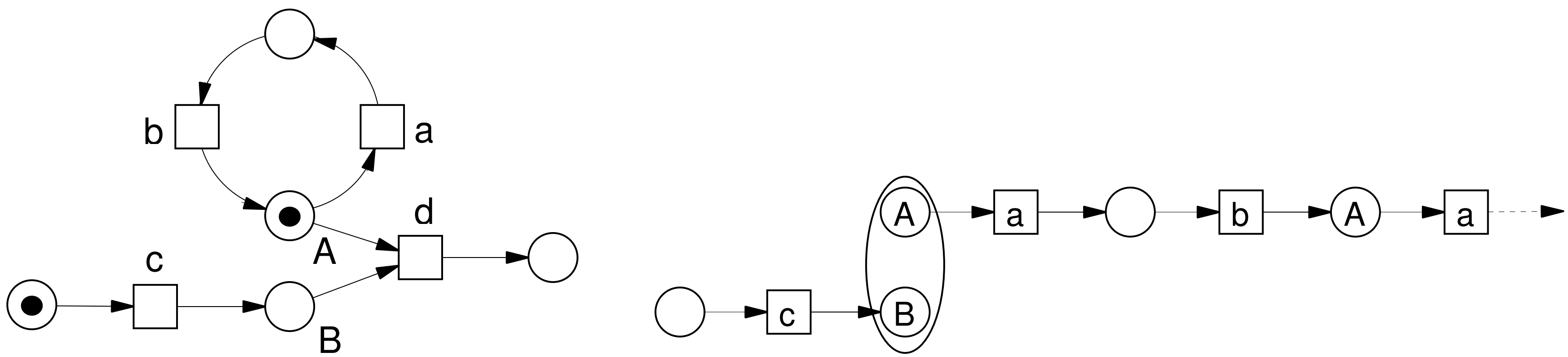
$$f(\Sigma_1) = g(\Sigma_2) \Rightarrow f(\varphi(\Sigma_1)) = g(\varphi(\Sigma_2))$$

In other words: Partial-order linear time semantics with refinement-robust fairness is a congruence for the algebra

(Net systems; T-refinement, P-refinement).

Weak and strong fairness for non-sequential runs

Recall: A non-sequential run represents a set of sequential runs (its *interleavings* or *observations*).



Definition: A non-sequential run is *weakly fair* (*strongly fair*) if it has an interleaving that is weakly fair (strongly fair).

Weak and strong fairness

Now we can formally prove:

Theorem: Weak and strong fairness are not refinement-robust.

Overview

1. Problem

2. Formalization

3. Solution

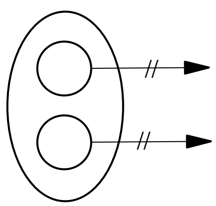
   - Refinement-robust versions of weak and strong fairness

   - Hyperfairness

4. Remarks

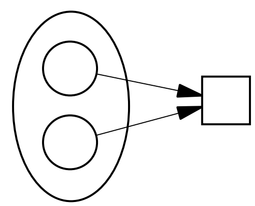
Persistence and Coexistence

of a co-set D of conditions



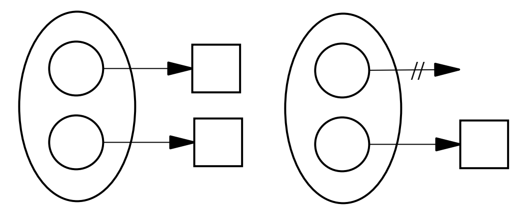
persistent

$D^\bullet = \emptyset$

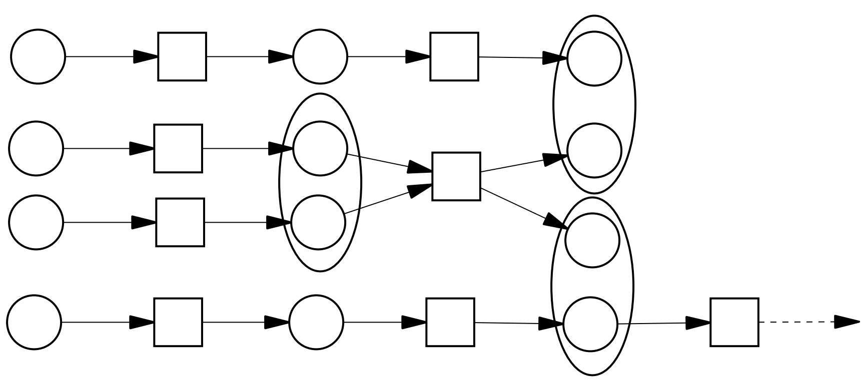


coexistent

$t \in D^\bullet \Rightarrow D \subseteq {}^\bullet t$



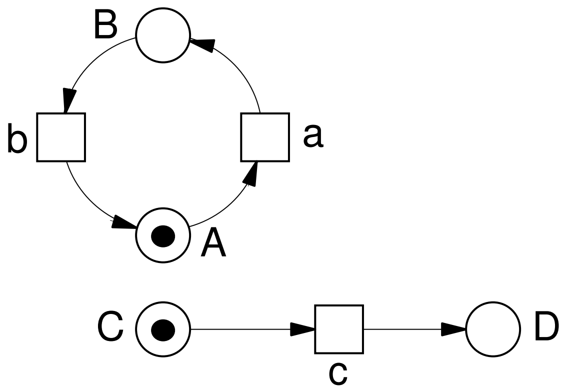
neither nor

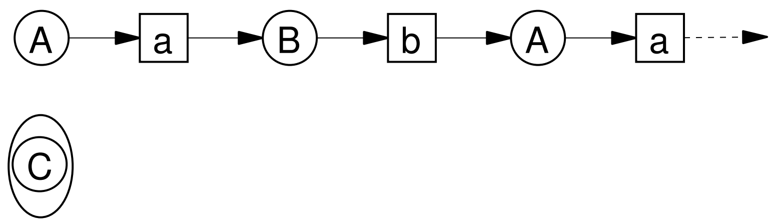


- persistence $\Rightarrow$ coexistence
- observer-independent
- refinement-robust

Progress wrt t

$= {}^\bullet t$ is not persistent
(i.e. there is no persistent co-set labelled with ${}^\bullet t$)

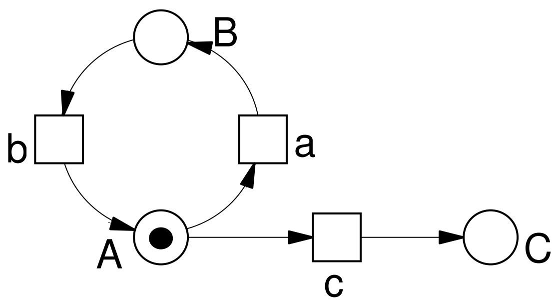


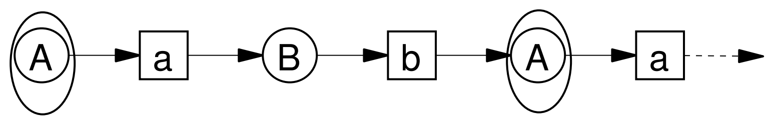


progress is known, e.g., as maximality of partial-order runs
weak fairness $\Rightarrow$ progress

Free Fairness wrt t

$\square \Diamond \text{coexistent}({}^\bullet t) \Rightarrow \square \Diamond \text{taken}(t)$

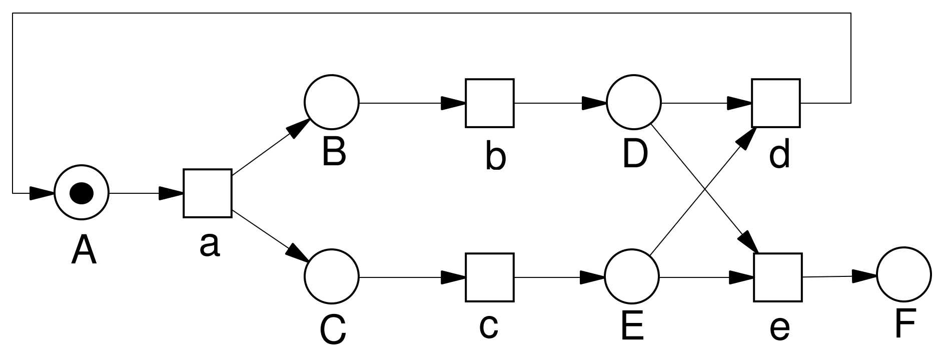


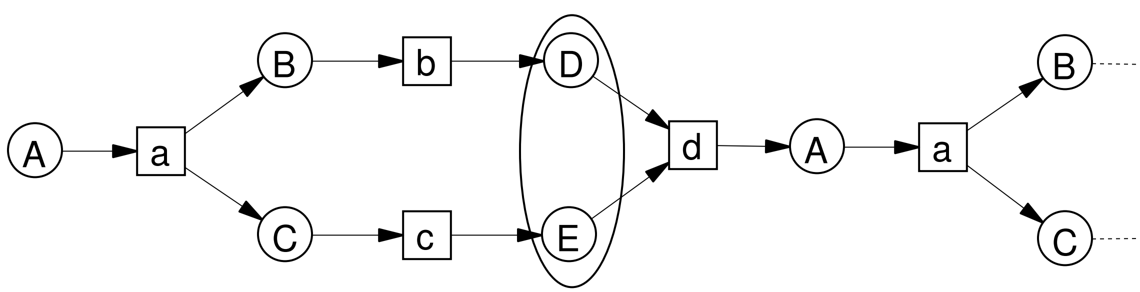


free fairness $\Rightarrow$ progress

Free Fairness wrt t (contd.)

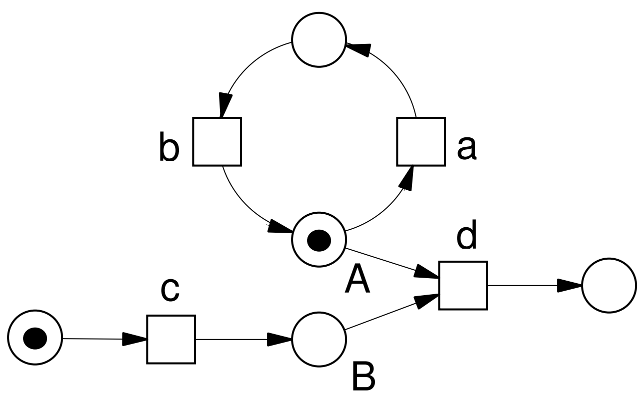
$\Box \Diamond \text{coexistent}({}^{\bullet}t) \Rightarrow \Box \Diamond \text{taken}(t)$

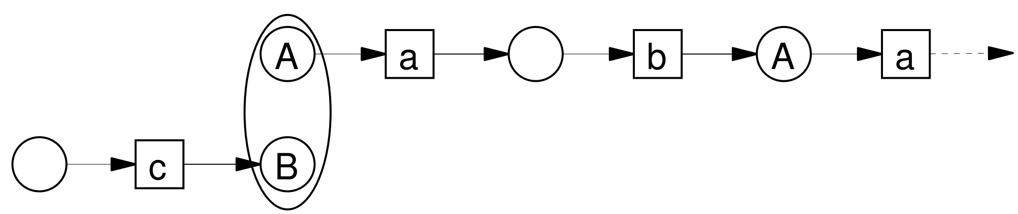




Simple Fairness wrt t

$$= \exists Q \subseteq {}^\bullet t : \text{persistent}(Q) \wedge \Box\Diamond\, \text{coexistent}({}^\bullet t \setminus Q) \Rightarrow \Box\Diamond\, \text{taken}(t)$$

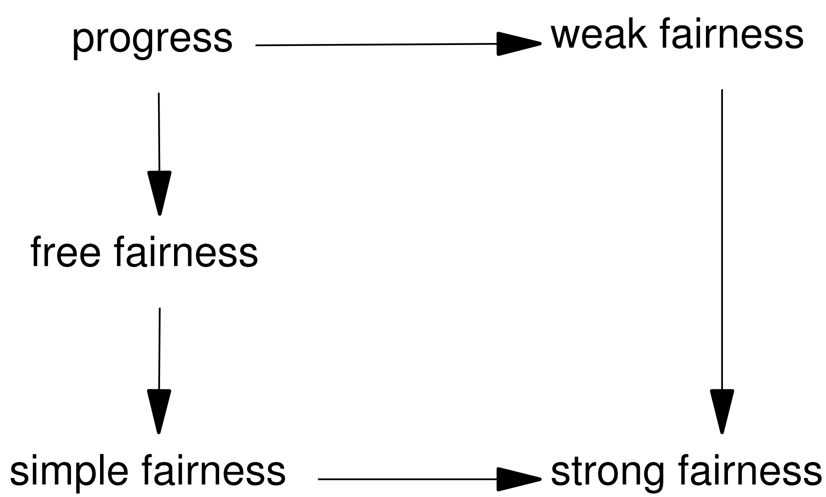




strong fairness $\Rightarrow$ simple fairness $\Rightarrow$ free fairness

fair arcs is a special case of simple fairness

Relationships



Refinement-Robust Fairness

Theorem:

Progress, free fairness, and simple fairness are refinement-robust.

Refinement-Robust Versions of Weak and Strong Fairness

Theorem: Given Σ and transition t of Σ.

1. Obtain Σ' by P-refining all $p \in {}^{\bullet}t$. Then
   - progress $\Leftrightarrow$ weak fairness (wrt t in Σ')
   - simple fairness $\Leftrightarrow$ strong fairness
2. Obtain Σ' by T-refining all conflict transitions of t. Then
   - progress $\Leftrightarrow$ weak fairness

Overview

1. Problem

2. Formalization

3. Solution

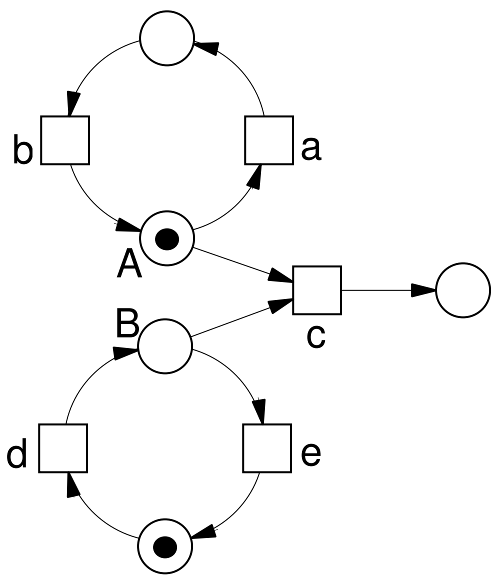
   - Refinement-robust versions of weak and strong fairness

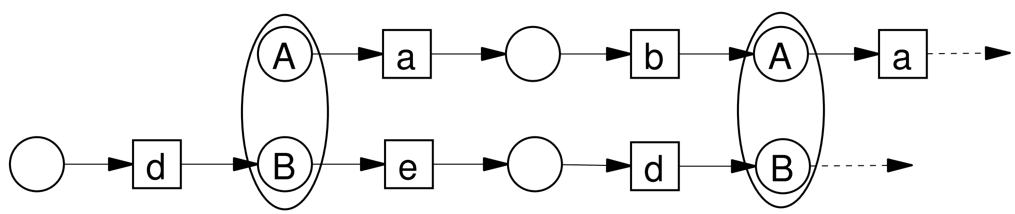
   - Hyperfairness

4. Remarks

Hyperfairness wrt t

$= \Box \Diamond {}^{\bullet}t \Rightarrow \Box \Diamond \text{taken}(t)$



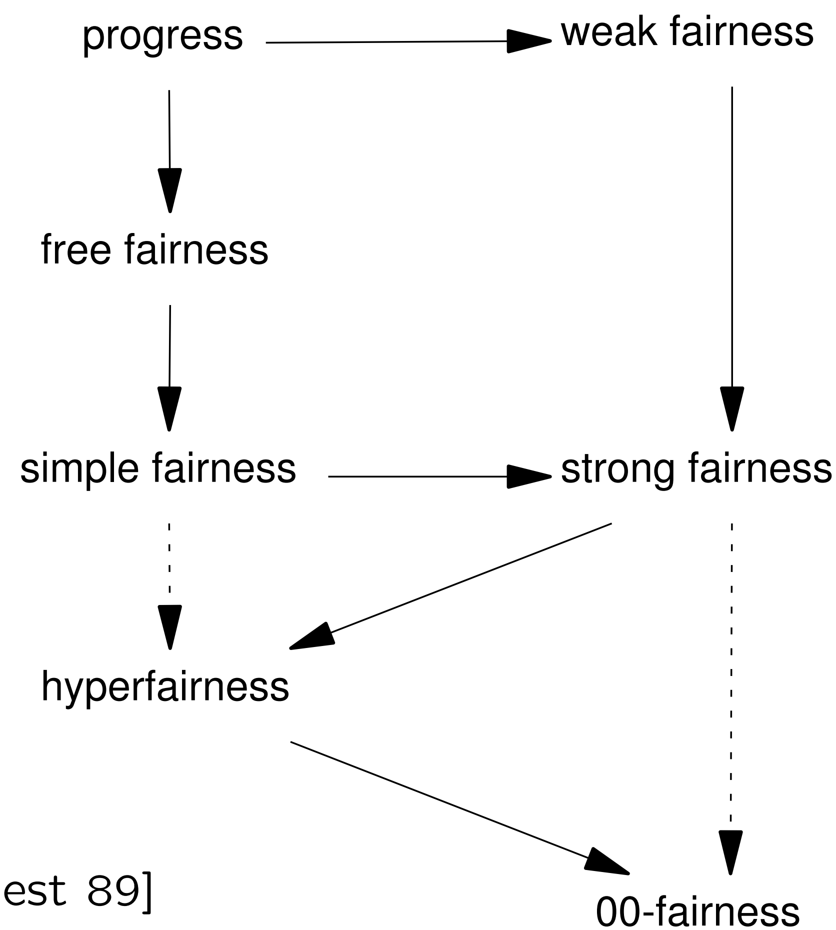


hyperfairness $\Rightarrow$ strong fairness

Hyperfairness

- rules out "conspiracies" that are due to race-conditions
- other notions with the same goal
  - ∞-fairness [Best 89] $= \Box$ reachable(t) $\Rightarrow \Box\Diamond$ taken(t)
  - hyperfairness [Attie, Francez, Grumberg 93] strongly tied to a particular process language
  - hyperfairness [Lamport 2000] identical with ∞-fairness

Relationships extended



∞-fairness wrt t [Best 89]
$= \Box$ reachable(t) $\Rightarrow \Box \Diamond$ taken(t)

Overview

1. Problem

2. Formalization

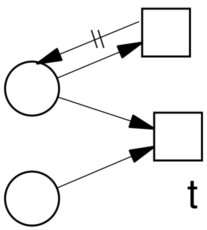
3. Solution

4. Remarks

   - hierarchy and conflict structure

   - Aspects of fairness

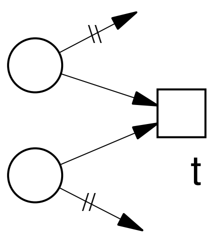
Conflict structure wrt t (1/4)



t is *loop-conflict free*: $\forall p, q \in {}^\bullet t : p^\bullet \cap {}^\bullet p \subseteq \{t\}$

t is loop-conflict free $\Rightarrow$ (weak fairness wrt $t \Leftrightarrow$ progress wrt t)

Conflict structure wrt t (2/4)

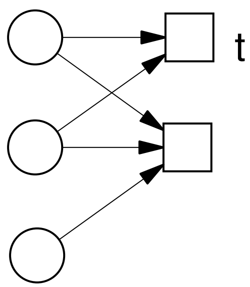


t is *conflict free*: $\forall p, q \in {}^{\bullet}t : p^{\bullet} = \{t\}$

A resource of t cannot be taken away

t is conflict free $\Rightarrow$ (free fairness wrt $t \Leftrightarrow$ progress wrt t)

Conflict structure wrt t (3/4)

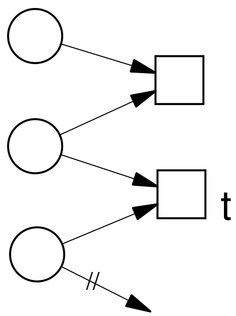


t is *free*: $\forall p, q \in {}^\bullet t : p^\bullet = q^\bullet$

A resource of t cannot be taken away unless t is enabled

t is free $\Rightarrow$ (simple fairness wrt t $\Leftrightarrow$ free fairness wrt t)

Conflict structure wrt t (4/4)



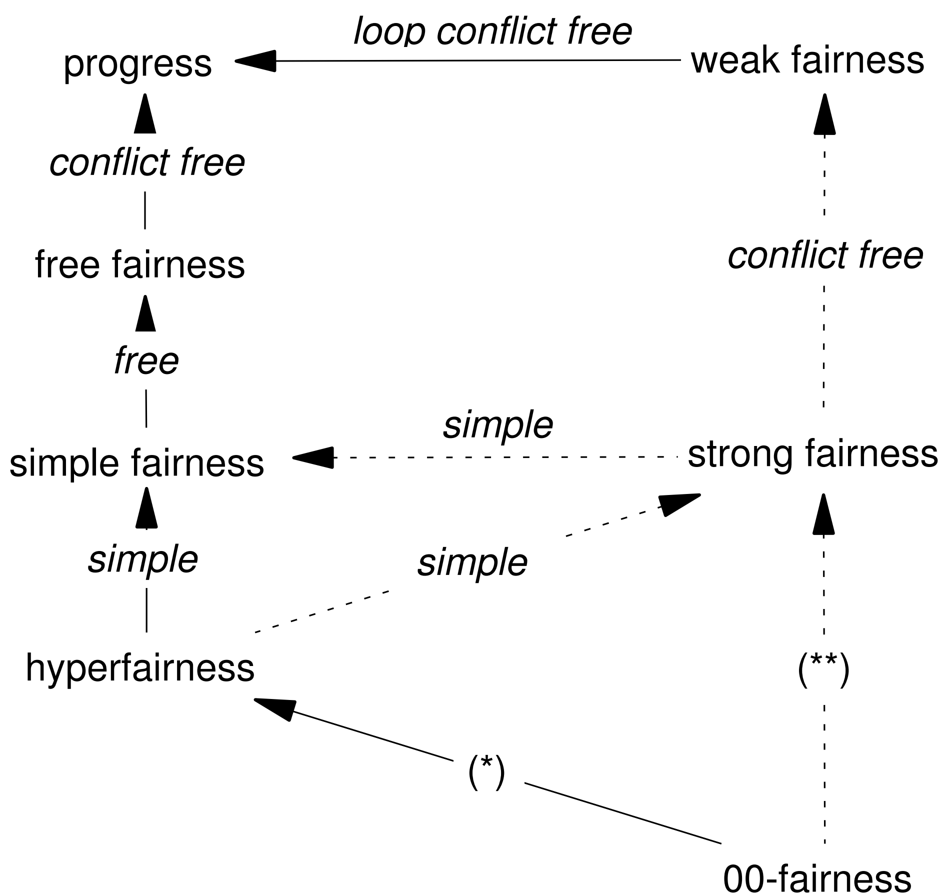
t is *simple*: $\forall p, q \in {}^\bullet t : p^\bullet \subseteq q^\bullet \vee q^\bullet \subseteq p^\bullet$

induces order on resources such that: If t has a token and all 'smaller' tokens then that token cannot be taken away unless t is enabled

t is simple $\Rightarrow$ (hyperfairness wrt t $\Leftrightarrow$ simple fairness wrt t)

conflict-free $\Rightarrow$ free $\Rightarrow$ simple

Collapse

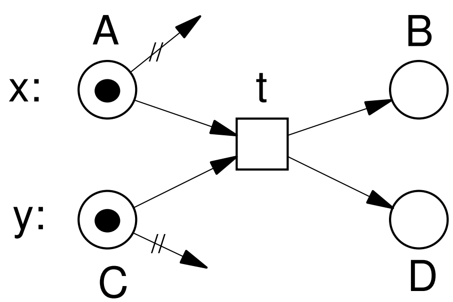


(*) = finite net; ∞-fairness assumed for all transitions; (**) = (*) + simple

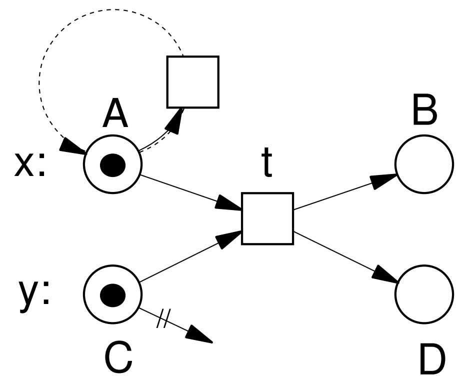
Aspects of Fairness

- *fairness wrt concurrency* = transition is not delayed by concurrent events = progress
- *fairness wrt choice* = each outcome of a recurrent choice is recurrent = free fairness $\setminus$ progress
- in simple fairness and hyperfairness, these aspects overlap ("confusion")

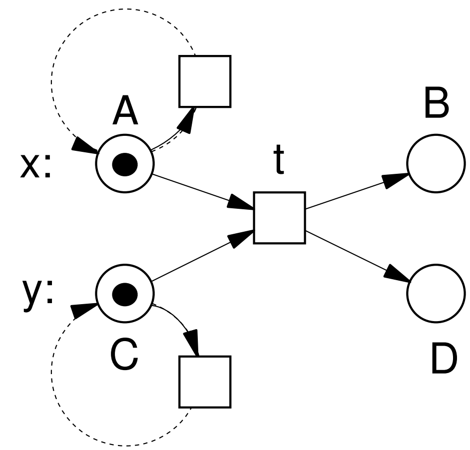
Synchronization assumptions



Progress

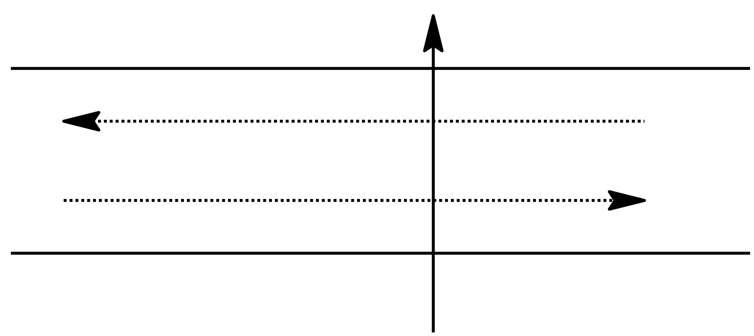


Simple fairness



Hyperfairness

An intuition



Conclusion

Summary:

– refinement-robust fairness can be derived from partial-order semantics

Additional remarks:

– the hierarchy separates computational power

– progress, free fairness, and simple fairness can be defined on sequential runs

Future work:

– fairness for unsafe and high-level nets

– fairness and composition