

# A Fixpoint Semantics of Event Systems With and Without Fairness Assumptions

Héctor Ruíz Barradas

*Universidad Autónoma Metropolitana Azcapotzalco, México*

Didier Bert

*LSR-IMAG, Grenoble, France*

December 2, 2005

# Contents

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

1. Introduction.
2. Set transformers and UNITY logic.
3. A general framework.
4. The case of minimal progress.
5. The case of weak fairness.
6. Conclusions.

## INTRODUCTION

- Action Systems
- Fairness
- Refinement
- Proposal
- Reachability and Termination

## NOTATION

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

# INTRODUCTION

# Action Systems

## INTRODUCTION

### ● Action Systems

- Fairness
- Refinement
- Proposal
- Reachability and Termination

## NOTATION

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

- Development of actions systems by stepwise refinement.
- The computational model of various approaches can be represented by a do od construction:

```
do
   $e_1 : g_1 \Longrightarrow s_1$ 
  ⋮
   $e_n : g_n \Longrightarrow s_n$ 
od
```

- Events with enabled guards are executed in a non deterministic way.

# Fairness

## INTRODUCTION

- Action Systems
- **Fairness**
- Refinement
- Proposal
- Reachability and Termination

## NOTATION

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

- Event B does not suppose fairness assumptions.
  - *minimal progress*.
- UNITY consider  $grd(e_i) \equiv true$  for any  $e_i$ .
  - *unconditional fairness*: events are executed infinitely often.
- Action Systems or TLA consider  $grd(e_i)$  as general predicates.
  - *weak fairness*: actions eventually enabled continuously are infinitely often executed.
  - *strong fairness*: actions enabled infinitely often are executed infinitely often.

# Refinement

## INTRODUCTION

- Action Systems
- Fairness
- **Refinement**
- Proposal
- Reachability and Termination

## NOTATION

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

- In UNITY or TLA, specifications and refinements are formulas in a temporal logic.
- In TLA, actions are specified by the “before-after” relation on the state variables.
- In UNITY, actions are modeled by assignments statements, derived from the last refinement.
- In Action Systems or Event B, specifications and refinements are specified in a programming like notation.

# Proposal

## INTRODUCTION

- Action Systems
- Fairness
- Refinement
- **Proposal**
- Reachability and Termination

## NOTATION

## GENERAL

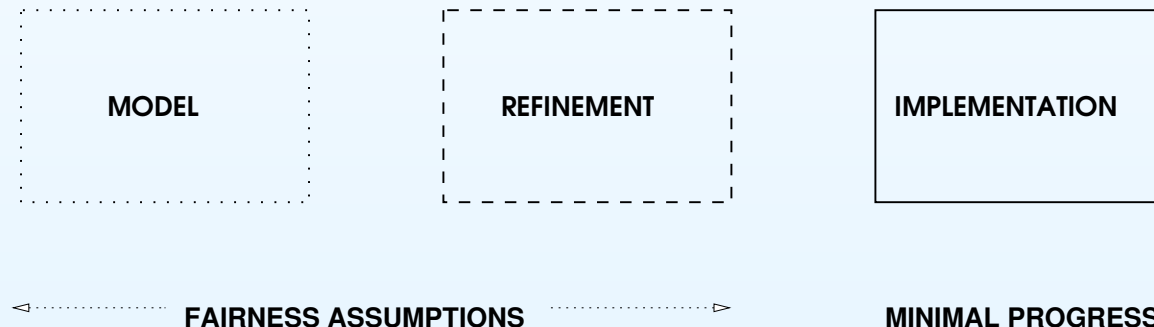
## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

### ■ An approach integrating:

- programming like notations in specifications and refinements (Event B / Action Systems),
- different fairness assumptions (TLA)



- explicit liveness specification and preservation (UNITY).

# Reachability and Termination

## INTRODUCTION

- Action Systems
- Fairness
- Refinement
- Proposal
- Reachability and Termination

## NOTATION

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

- Liveness in TLA or UNITY is specified by modalities:

“from a state satisfying  $P$ , the system eventually *reaches* a state satisfying  $Q$ ”

- In Event B or Action Systems, liveness is modeled by termination of iteration of events:

“execution of the iteration of events in a state satisfying  $P$  *terminates* into a state satisfying  $Q$ ”

- Reachability and termination are equivalent notions.

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- Dovetail
- UNITY-Like Logic
- Basic Properties
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

# NOTATION

# Set Transformers (1/4)

## INTRODUCTION

## NOTATION

### ● Model of Systems

- Definitions
- Primitives
- Dovetail
- UNITY-Like Logic
- Basic Properties
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

■ A model of a system  $\mathcal{S}$  is a structure  $\langle V, I, U, S \rangle$  where

- $V$  is a vector of variables,
- $I$  is the invariant of  $\mathcal{S}$ ,
- $U$  is an initialization statement and
- $S$  is the choice of events in  $\mathcal{S}$ :  $E_1 \parallel \dots \parallel E_n$

■ Each  $E_i$ , and therefore  $S$ , are modeled by conjunctive set transformers:

$$E_i \in \mathbb{P}(u) \rightarrow \mathbb{P}(u) \quad \text{where} \quad u = \{ z \mid I(z) \}$$

# Set Transformers (2/4)

## INTRODUCTION

### NOTATION

- Model of Systems
- **Definitions**
- Primitives
- Dovetail
- UNITY-Like Logic
- Basic Properties
- General Properties

### GENERAL

### MINIMAL PROGRESS

### WEAK FAIRNESS

### CONCLUSIONS

- Weakest precondition: for any event  $E$  and set  $r$  of  $\mathbb{P}(u)$ :

$$E(r) = \{z \mid z \in u \wedge wp(E, x \in r)\}$$

- Weakest liberal precondition:

$$\mathcal{L}(E)(r) = \{z \mid z \in u \wedge wlp(E, x \in r)\}$$

- Pairing Condition:

$$E(r) = \mathcal{L}(E)(r) \cap \text{pre}(E) \quad \text{where} \quad \text{pre}(E) = E(u)$$

# Set Transformers (3/4)

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- Dovetail
- UNITY-Like Logic
- Basic Properties
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

### ■ Primitive set transformers:

- $(\mathcal{L})(\text{skip})(r) = r$
- $(\mathcal{L})(F \parallel G)(r) = (\mathcal{L})(F)(r) \cap (\mathcal{L})(G)(r)$
- $(\mathcal{L})(F ; G)(r) = (\mathcal{L})(F)((\mathcal{L})(G)(r))$
- $(\mathcal{L})(p \implies F)(r) = \bar{p} \cup (\mathcal{L})(F)(r)$
- $(p \mid F)(r) = p \cap F(r)$
- $\mathcal{L}(p \mid F)(r) = (p \cup \{z \mid z \in u \wedge u \subseteq r\}) \cap \mathcal{L}(F)(r)$

### ■ Recursive definitions $(\mathcal{L})F(r) = \mathcal{F}((\mathcal{L})F(r))$

- $F(r) = \text{fix}(\mathcal{F})$  as the least solution.
- $\mathcal{L}(F)(r) = \text{FIX}(\mathcal{F})$  as the greatest solution.

# Set Transformers (4/4)

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- **Dovetail**
- UNITY-Like Logic
- Basic Properties
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

### ■ The dovetail operator:

- fair non deterministic choice operator ( $\nabla$ )
- Example:  $X = (n := 0 \nabla (X ; n := n + 1))$
- Definition:

$$\mathcal{L}(F \nabla G)(r) = \mathcal{L}(F)(r) \cap \mathcal{L}(G)(r)$$

$$\text{pre}(F \nabla G) = (F(u) \cap G(u)) \cup (\overline{F(\emptyset)} \cap F(u)) \cup (\overline{G(\emptyset)} \cap G(u))$$

$$\text{where } \text{grd}(F) = \overline{F(\emptyset)}$$

# UNITY-Like Logic (1/3)

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- Dovetail
- **UNITY-Like Logic**
- Basic Properties
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

### ■ Liveness is specified by two relations:

- *ensures* and
- *leads to*.

### ■ $P \gg Q$ specifies a basic property.

- Transition made by one event.

### ■ $P \rightsquigarrow Q$ specifies a general property

- Transition made by one or many events.

# UNITY-Like Logic (2/3)

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- Dovetail
- UNITY-Like Logic
- **Basic Properties**
- General Properties

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

■ Definition of *ensures* depends on fairness assumptions.

■  $P \gg_m Q$  under minimal progress follows from:

- MP0:  $I \wedge P \wedge \neg Q \Rightarrow wp(S, Q)$ .
- MP1:  $I \wedge P \wedge \neg Q \Rightarrow grd(S)$ .

■  $E \cdot P \gg_w Q$  under weak fairness follows from:

- WF0:  $I \wedge P \wedge \neg Q \Rightarrow wp(S, P \vee Q)$ .
- WF1:  $I \wedge P \wedge \neg Q \Rightarrow wp(E, Q) \wedge grd(E)$

where  $E$  is an event of the choice  $S$ .

# UNITY-Like Logic (3/3)

## INTRODUCTION

## NOTATION

- Model of Systems
- Definitions
- Primitives
- Dovetail
- UNITY-Like Logic
- Basic Properties
- **General Properties**

## GENERAL

## MINIMAL PROGRESS

## WEAK FAIRNESS

## CONCLUSIONS

■  $P \rightsquigarrow Q$  follows by a finite number of applications of the following rules:

- BRL:  $P \gg Q \vdash P \rightsquigarrow Q$ .
- TRA:  $P \rightsquigarrow R, R \rightsquigarrow Q \vdash P \rightsquigarrow Q$
- DSJ:  $\forall m \cdot (m \in M \Rightarrow P(m) \rightsquigarrow Q) \vdash$   
 $\exists m \cdot (m \in M \wedge P(m)) \rightsquigarrow Q$

INTRODUCTION

NOTATION

GENERAL

- Termination (1/2)
- Termination (2/2)
- Reachability (1/2)
- Reachability (2/2)
- Soundness and Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

**GENERAL**

# Termination (1/2)

INTRODUCTION

NOTATION

GENERAL

● Termination (1/2)

● Termination (2/2)

● Reachability (1/2)

● Reachability (2/2)

● Soundness and  
Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

■  $W$  models a *step* in the iteration of events.

- $W$  is a monotonic set transformer.
- $W$  is strict:  $W(\emptyset) = \emptyset$

■  $\mathcal{F}(r)$  models the body of the iteration:

$$\mathcal{F}(r) \hat{=} (\bar{r} \Longrightarrow W)$$

■ Iteration is modeled by the “opening” operator  $\hat{\phantom{x}}$ :

$$\mathcal{F}(r) \hat{=} = (\mathcal{F}(r) ; \mathcal{F}(r) \hat{=} ) \parallel \text{skip}$$

# Termination (2/2)

INTRODUCTION

NOTATION

GENERAL

- Termination (1/2)
- **Termination (2/2)**
- Reachability (1/2)
- Reachability (2/2)
- Soundness and Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

- Termination of  $(\bar{r} \Longrightarrow W)^\wedge$  is guaranteed into a state in  $r$ .

- The termination set of  $\mathcal{F}(r)^\wedge$  is a fixpoint:

$$\text{pre}(\mathcal{F}(r)^\wedge) = \text{fix}(\mathcal{F}(r))$$

- The *termination* relation  $\mathcal{T}$ :

$$\mathcal{T} \hat{=} \{ a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \subseteq \text{fix}(\mathcal{F}(b)) \}$$

# Reachability (1/2)

INTRODUCTION

NOTATION

GENERAL

- Termination (1/2)
- Termination (2/2)
- **Reachability (1/2)**
- Reachability (2/2)
- Soundness and Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

- The *reachability* relation  $\mathcal{L}$  is of type  $\mathbb{P}(u) \times \mathbb{P}(u)$
- $\mathcal{L}$  contains the basic relation  $\mathcal{E}$ :
  - Definition of  $\mathcal{E}$  depends on fairness assumptions.
  - First requirement:  $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}$ .
  - Second requirement:  $a \mapsto b \in \mathcal{E} \Rightarrow a \cap \bar{b} \subseteq W(b)$

# Reachability (2/2)

INTRODUCTION

NOTATION

GENERAL

- Termination (1/2)
- Termination (2/2)
- Reachability (1/2)
- **Reachability (2/2)**
- Soundness and Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

■  $\mathcal{L}$  is the smallest relation satisfying:

- SBR:  $\mathcal{E} \subseteq \mathcal{L}$

- STR:  $\mathcal{L}; \mathcal{L} \subseteq \mathcal{L}$

- SDR:  $\forall (q, l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \Rightarrow (l \times \{q\} \subseteq \mathcal{L} \Rightarrow \bigcup(l) \mapsto q \in \mathcal{L}))$

■ Relation between  $\mathcal{L}$  and *leads to*:

$$P \rightsquigarrow Q \equiv \text{set}(P) \mapsto \text{set}(Q) \in \mathcal{L}$$

# Soundness and Completeness

INTRODUCTION

NOTATION

GENERAL

- Termination (1/2)
- Termination (2/2)
- Reachability (1/2)
- Reachability (2/2)
- Soundness and Completeness

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

- *termination* and *reachability* relations are equal:

Considering

- $W$  a monotonic and strict set transformer,
- $\mathcal{F}(r) = (\bar{r} \Longrightarrow W)$ ,  $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}$ ,
- $a \mapsto b \in \mathcal{E} \Rightarrow a \cap \bar{b} \subseteq W(b)$ ,  $W(r) \mapsto r \in \mathcal{L}$

then the equality  $\mathcal{L} = \mathcal{T}$  holds.

- The inclusion  $\mathcal{L} \subseteq \mathcal{T}$  follows from definition of  $\mathcal{L}$ .
- The inclusion  $\mathcal{T} \subseteq \mathcal{L}$  follows from the property:

$$\forall r \cdot (r \in \mathbb{P}(u) \Rightarrow \mathcal{F}(r)^\alpha \mapsto r \in \mathcal{L})$$

INTRODUCTION

NOTATION

GENERAL

**MINIMAL PROGRESS**

- Termination MP
- Reachability MP
- Equality

WEAK FAIRNESS

CONCLUSIONS

# MINIMAL PROGRESS

# Termination under MP

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

● Termination MP

● Reachability MP

● Equality

WEAK FAIRNESS

CONCLUSIONS

- To establish a postcondition, a step needs:
  - any event must establish the postcondition and
  - the step must be executed in the guard of an event.

■ The step is defined as  $W_m \hat{=} \text{grd}(S) \mid S$

■ The body of the iteration is:  $\mathcal{F}_m(r) \hat{=} \bar{r} \Longrightarrow W_m$ .

■ The *termination* relation:

$$\mathcal{T}_m \hat{=} \{ a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \subseteq \text{fix}(\mathcal{F}_m(b)) \}$$

# Reachability under MP

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

- Termination MP
- **Reachability MP**
- Equality

WEAK FAIRNESS

CONCLUSIONS

- The basic relation considers MP0 and MP1 proof obligations:

$$\mathcal{E}_m \hat{=} \{ a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \cap \bar{b} \subseteq S(b) \cap \text{grd}(S) \}$$

- Reachability  $\mathcal{L}_m$  is the smallest relation satisfying:

- SBR:  $\mathcal{E}_m \subseteq \mathcal{L}_m$
- STR:  $\mathcal{L}_m ; \mathcal{L}_m \subseteq \mathcal{L}_m$
- SDR:  $\forall (q, l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \Rightarrow$   
 $(l \times \{q\} \subseteq \mathcal{L}_m \Rightarrow \bigcup(l) \mapsto q \in \mathcal{L}_m))$

# Equality between $\mathcal{T}_m$ and $\mathcal{L}_m$

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

- Termination MP
- Reachability MP
- Equality

WEAK FAIRNESS

CONCLUSIONS

## ■ Definitions of $W_m$ and $\mathcal{E}_m$ :

- $W_m \hat{=} \text{grd}(S) \mid S,$
- $\mathcal{E}_m \hat{=} \{ a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \cap \bar{b} \subseteq S(b) \cap \text{grd}(S) \}$

satisfy the conditions:

- $W_m$  is monotonic and strict,
- $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_m,$
- $a \mapsto b \in \mathcal{E}_m \Rightarrow a \cap \bar{b} \subseteq W_m(b),$
- $W_m(r) \mapsto r \in \mathcal{L}_m$

therefore, the equality  $\mathcal{T}_m = \mathcal{L}_m$  holds.

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

**WEAK FAIRNESS**

- A Fair Loop
- Termination WF
- Reachability WF
- Equality

CONCLUSIONS

# WEAK FAIRNESS

# Termination under WF (1/2)

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

• A Fair Loop

- Termination WF
- Reachability WF
- Equality

CONCLUSIONS

- A fair loop:

$$Y(q)(G) \hat{=} \bar{q} \implies ((S ; Y(q)(G)) \nabla (\text{grd}(G) \mid G))$$

- Termination set and weakest liberal precondition:

$$\text{pre}(Y(q)(G)) = \text{fix}(\bar{q} \cap G(\emptyset) \implies \overline{S(q)} \mid S)$$

$$\mathcal{L}(Y(q)(G))(r) = \text{FIX}(\bar{q} \implies (\text{grd}(G) \cap G(r) \mid S))$$

- As  $\mathcal{L}(Y(q)(G))(r) \subseteq \text{pre}(Y(q)(G))$ , the weakest precondition is:

$$Y(q)(G)(r) = \text{FIX}(\bar{q} \implies (\text{grd}(G) \cap G(r) \mid S))$$

## Termination under WF (2/2)

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

• A Fair Loop

• **Termination WF**

• Reachability WF

• Equality

CONCLUSIONS

- A step of the iteration under WF:

$$W_w \hat{=} \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r)))$$

- The body of the iteration under WF:

$$\mathcal{F}_w(r) \hat{=} \bar{r} \implies W_w$$

- The *termination* relation under WF:

$$\mathcal{T}_w \hat{=} \{ a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \subseteq \text{fix}(\mathcal{F}_w(b)) \}$$

# Reachability under WF

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

- A Fair Loop
- Termination WF
- **Reachability WF**
- Equality

CONCLUSIONS

- Basic relation for a helpful event:

$$\mathcal{E}(G) \hat{=} \{a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \cap \bar{b} \subseteq S(a \cup b) \cap \overline{G(\emptyset)} \cap G(b)\}$$

- Basic relation under WF:  $\mathcal{E}_w \hat{=} \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))$ .

- Reachability  $\mathcal{L}_w$  is the smallest relation satisfying:

- SBR:  $\mathcal{E}_w \subseteq \mathcal{L}_w$
- STR:  $\mathcal{L}_w ; \mathcal{L}_w \subseteq \mathcal{L}_w$
- SDR:  $\forall (q, l) \cdot (q \in \mathbb{P}(u) \wedge l \subseteq \mathbb{P}(u) \Rightarrow$   
 $(l \times \{q\} \subseteq \mathcal{L}_w \Rightarrow \bigcup(l) \mapsto q \in \mathcal{L}_w))$

# Equality between $\mathcal{T}_w$ and $\mathcal{L}_w$

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

- A Fair Loop
- Termination WF
- Reachability WF
- Equality

CONCLUSIONS

## ■ Definitions of $W_w$ and $\mathcal{E}_w$ :

- $W_w \hat{=} \lambda r \cdot (r \subseteq u \mid \bigcup G \cdot (G \in \mathcal{S} \mid Y(r)(G)(r)))$ ,
- $\mathcal{E}_w \hat{=} \bigcup G \cdot (G \in \mathcal{S} \mid \mathcal{E}(G))$  where  $\mathcal{E}(G) \hat{=} \overline{\{a \mapsto b \mid a \subseteq u \wedge b \subseteq u \wedge a \cap \bar{b} \subseteq S(a \cup b) \cap \overline{G(\emptyset)} \cap G(b)\}}$

satisfy the conditions:

- $W_w$  is monotonic and strict,
- $a \subseteq b \Rightarrow a \mapsto b \in \mathcal{E}_w$ ,
- $a \mapsto b \in \mathcal{E}_w \Rightarrow a \cap \bar{b} \subseteq W_w(b)$ ,
- $W_w(r) \mapsto r \in \mathcal{L}_w$

therefore, the equality  $\mathcal{T}_w = \mathcal{L}_w$  holds.

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

**CONCLUSIONS**

- Conclusions
- Future Work

# CONCLUSIONS

# Conclusions and Future Work (1/2)

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

● Conclusions

● Future Work

- A fixpoint semantics of event systems is presented.
- Minimal progress and weak fairness assumptions were considered.
- The development was structured: first a general framework was presented, then it was instantiated to two cases of fairness.
- Soundness and completeness were treated as equality between *termination* and *reachability*.
- The approach is a proposal of integration of programming like notations (as Event B or Action Systems) with temporal logic (UNITY) in event systems.

# Conclusions and Future Work (2/2)

INTRODUCTION

NOTATION

GENERAL

MINIMAL PROGRESS

WEAK FAIRNESS

CONCLUSIONS

● Conclusions

● Future Work

- In the paper we present sufficient conditions to derive liveness properties under MP:
  - All events decrement a variant under an loop invariant and
  - All events decrement a variant, and the property holds under WF.
  
- As a future work we consider to extend the approach:
  - to consider strong fairness and
  - to deal with composition of event systems.