

Defining Fairness

Hagen Völzer

Lübeck University
Germany

joint work with

Daniele Varacca, Imperial College, London, UK

and

Ekkart Kindler, Paderborn University, Germany

August 26, 2005

CONCUR 2005, San Francisco

Decomposition of a specification

$$\text{Spec} = \text{Safety-Spec} \cap \text{Liveness-Spec}$$

writing Spec this way is useful for

- verification: correspondence to different proof techniques
- design: tradeoff between safety and liveness

Setting

- *Run*: finite or infinite sequence of states: $x \in \Sigma^\infty = \Sigma^+ \cup \Sigma^\omega$
- *Temporal property*: $E \subseteq \Sigma^\infty$
 - *finitary* if $E \subseteq \Sigma^+$
 - *infinitary* if $E \subseteq \Sigma^\omega$

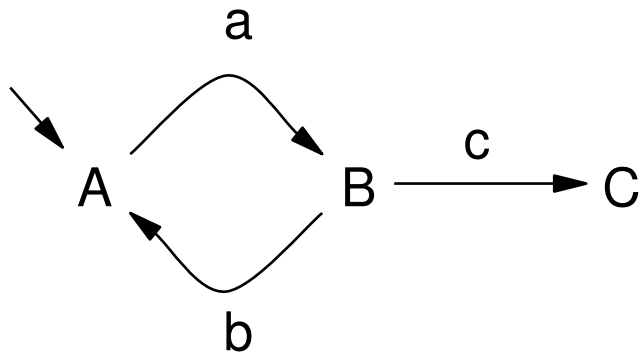
Live(ness) property L (Alpern/Schneider 1985)

= any finite run can be extended to a run satisfying L

- each superset of a liveness property is a liveness property
⇒ closed under arbitrary union
- not closed under intersection: $\Sigma^+ \cap \Sigma^\omega = \emptyset$

Specification of an implementation

Safety as transition system



Liveness as *fairness constraint*

- Maximality \cap
- Strong fairness wrt c

Examples of fairness notions

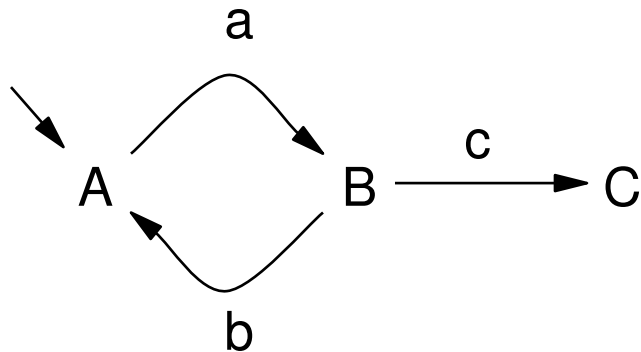
- Maximality: $\Box(\bigvee_t \text{enabled}(t) \Rightarrow \bigvee_t \Diamond \text{taken}(t))$
- Weak fairness: $\Diamond \Box \text{enabled}(t) \Rightarrow \Box \Diamond \text{taken}(t)$
- Strong fairness: $\Box \Diamond \text{enabled}(t) \Rightarrow \Box \Diamond \text{taken}(t)$
- Extreme fairness: $\Box \Diamond(\varphi \wedge \text{enabled}(t)) \Rightarrow \Box \Diamond(\varphi \wedge \text{taken}(t))$
- k -fairness: $\Box \Diamond \text{enabled}(k, t) \Rightarrow \Box \Diamond \text{taken}(t)$
- etc.

“Sufficiently often taken when sufficiently often possible.”

What is fairness?

Machine closure of (S, F)

= each finite run of S can be extended into $S \cap F$



• $\diamond \text{taken}(b)$ is not m.c.

• $\diamond \text{taken}(c)$ is m.c.

- if (S, F) is an implementation (S, F) should be machine closed
= fairness does not rule out finite runs of the transition system
(transition system cannot 'paint itself into a corner')

Machine closure is not enough



- $E_1 = \square \diamond \text{taken}(a)$
- $E_2 = \diamond \square \text{taken}(b)$
- $E_1 \cap E_2 = \emptyset$

- E_2 prescribes that some choice is not taken sufficiently often
- E_1, E_2 are both machine closed
- machine-closed properties are not closed under intersection (bad for composition)

Aim

Define fairness such that:

- fairness implies machine closure
- fairness is closed under intersection
- popular fairness notions fall into the class

Outline

1. Introduction
2. Constructive liveness
3. Fairness
4. A maximality theorem

Outline

1. Introduction

2. Constructive liveness

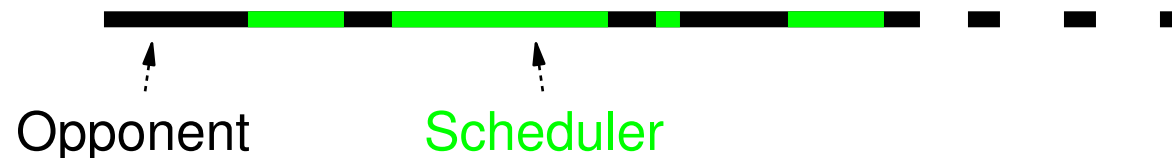
- game-theoretical
- language-theoretical
- topological

3. Fairness

4. A maximality theorem

Constructive liveness: game-theoretic

Run x :



- target: $E \subseteq \Sigma^\infty$
 - scheduler wins if $x \in E$
 - otherwise, opponent wins
- scheduler can enforce a choice to be taken infinitely often
- it cannot prevent another choice from being taken infinitely often

Constructive liveness property E

= scheduler has a winning strategy for target E

Examples

- Σ^ω
- $\square \diamond \phi$
- $\square(\psi \Rightarrow \diamond \phi)$
- $\diamond \square \psi \Rightarrow \square \diamond \phi$
- $\square \diamond \psi \Rightarrow \square \diamond \phi$

Counterexamples

- Σ^+
- $\diamond \square \phi$
- $\{\alpha x \mid \alpha \in \Sigma^+\}$ for $x \in \Sigma^\omega$.

ψ, ϕ are state formulas

Properties of constructive liveness

- is subclass of liveness
 - each superset of constructive liveness is constructive liveness
- ⇒ closed under arbitrary union
- closed under countable intersection

Outline

1. Introduction

2. Constructive liveness

- game-theoretical
- language-theoretical
- topological

3. Fairness

4. A maximality theorem

Constructive liveness: language-theoretic

For $Q \subseteq \Sigma^+$ let $R(Q) \subseteq \Sigma^\omega$ defined by:

$$R(Q) = \{x \mid x \text{ has } \infty \text{ many prefixes in } Q\}$$

= (Infinitary) *recurrence properties* (Manna/Pnueli 1990)

E is constructive liveness if and only if
it contains a live recurrence property

Outline

1. Introduction

2. Constructive liveness

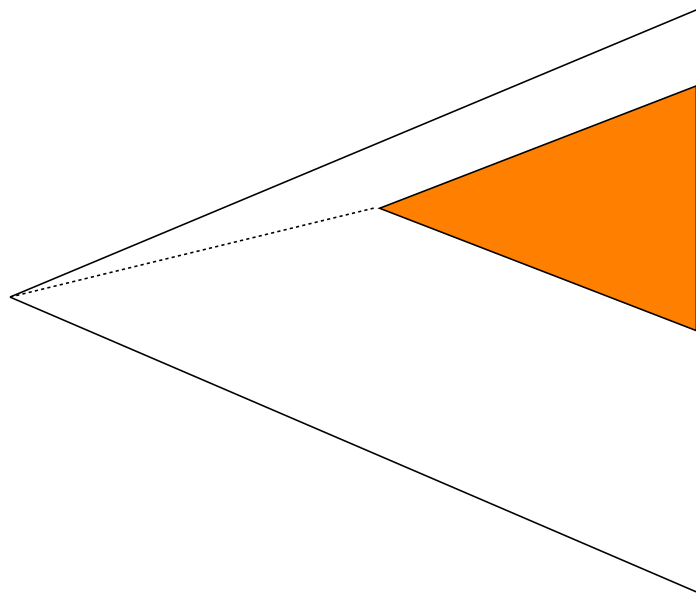
- game-theoretical
- language-theoretical
- topological

3. Fairness

4. A maximality theorem

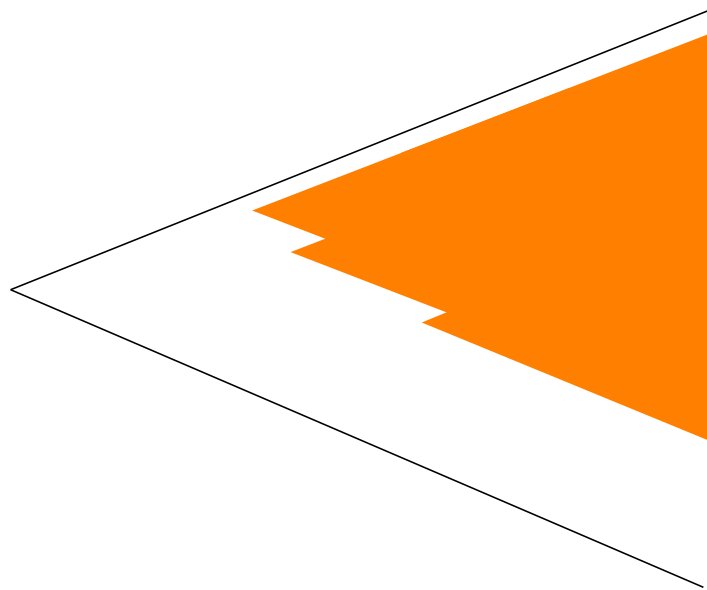
Scott topology on Σ^∞ : Basic open set

= any set $K(\alpha) = \{x \mid \alpha \text{ is a prefix of } x\}$ for $\alpha \in \Sigma^+$



Open set

= arbitrary union of basic open sets



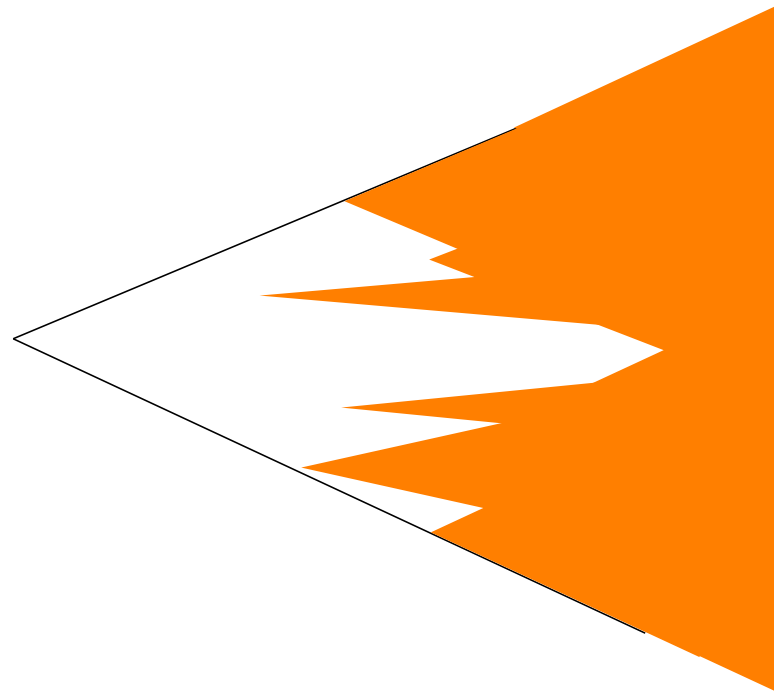
= *guarantee property* $\diamond \Phi$, Φ is a past formula

- requires one discrete good thing to happen once

Closed and dense sets

- *closed set*
 - = complement of an open set
 - = safety property
 - *dense set*
 - = intersects every nonempty open set
 - = liveness property
- ⇒ every property is the intersection of a safety and a liveness property (Alpern/Schneider 1985)

Dense open set



- E contains a dense open set
- \Leftrightarrow E has a one-shot winning strategy
- \Rightarrow E is constructive

G_δ set E

$$E = \bigcap_{i \in \mathbb{N}} G_i \quad G_i \text{ is open}$$

- requires countably many discrete things to happen once
- special case:
one discrete thing is required to happen infinitely often

Dense G_δ set E

$$E = \bigcap_{i \in \mathbb{N}} G_i \quad G_i \text{ is open}$$

- E is dense \Leftrightarrow all G_i are dense (true in every *Baire space*)
- E' contains a dense $G_\delta \Rightarrow E'$ is constructive
(on i -th turn, use one-shot strategy for G_i)

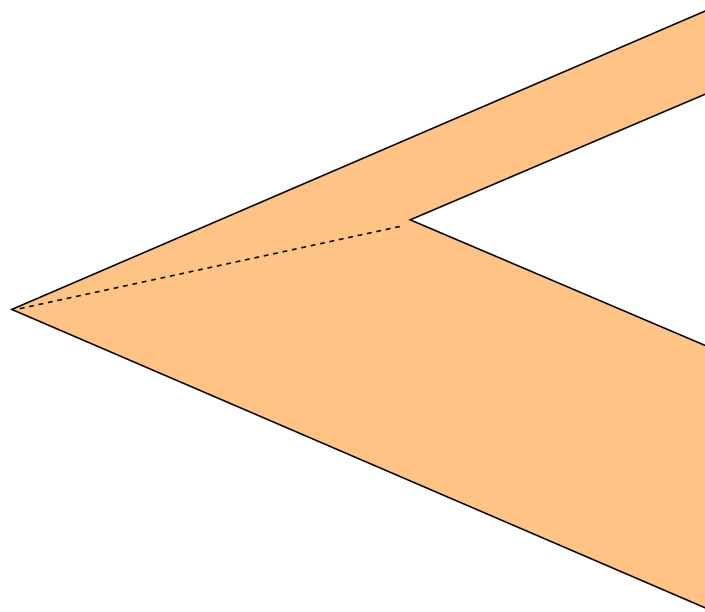
Constructive liveness: topological

E is constructive liveness if and only if it contains a dense G_δ set

$\Leftrightarrow E$ is *co-meager* (= topologically 'large')
(in every Baire space)

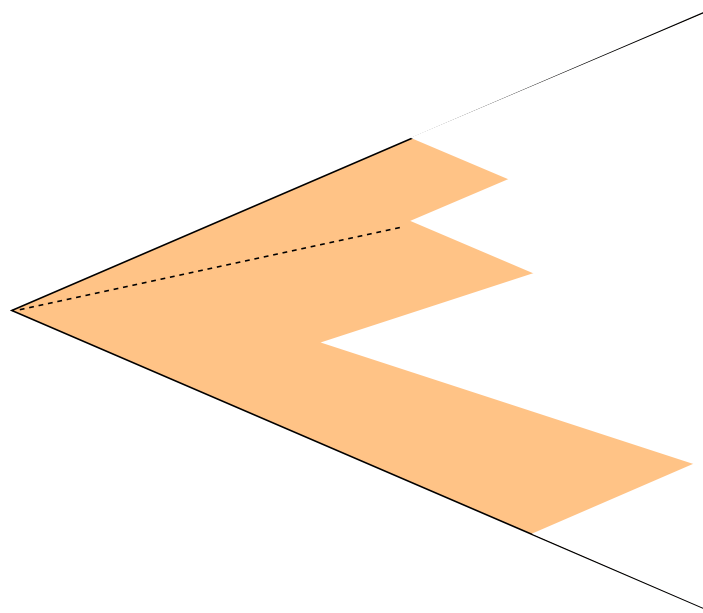
Some more topology: A hole in E

= a nonempty open set in the complement of E



Nowhere dense

= complement contains a dense open set



\Leftrightarrow full of holes (holes reachable from everywhere)

- e.g. Σ^k , $\Box \phi$, $\Sigma^k \cdot \Box \phi$ (ϕ is a state formula)

Co-meager set

Meager set (first Baire category) 'small':

= union of countably many nowhere dense sets

e.g. Σ^+ = $\bigcup_{k \in \mathbb{N}} \Sigma^k$, $\diamond \square \phi = \bigcup_{k \in \mathbb{N}} \Sigma^k \cdot \square \phi$

Co-meager set (residual) 'large':

= complement of a meager set

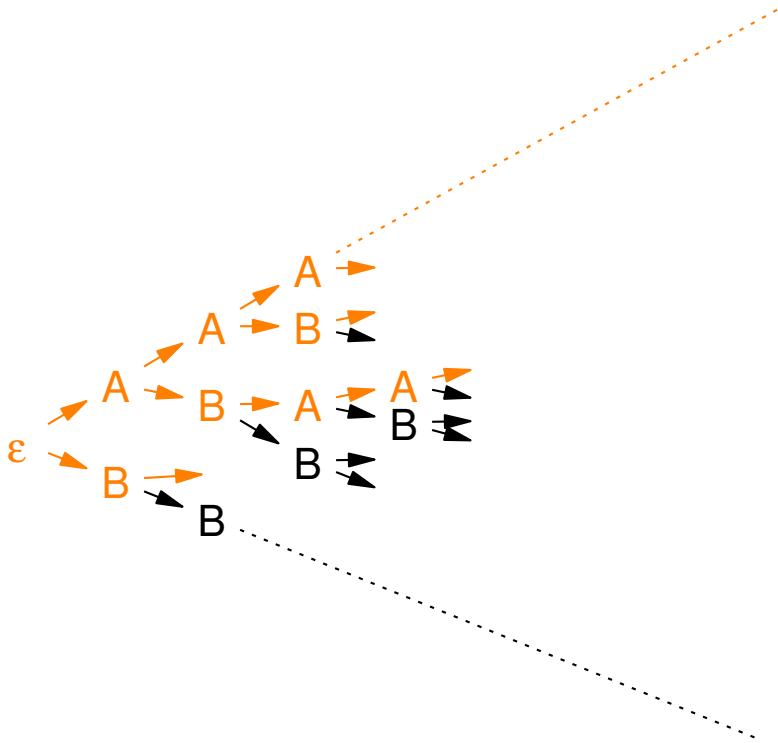
\Leftrightarrow contains a dense G_δ set (in every Baire space)

\Leftrightarrow constructive liveness

Outline

1. Introduction
2. Constructive liveness
3. Fairness
4. A maximality theorem

Fairness: game-theoretic



- given: a safety property S
- both players must play within S
- F is a *fairness property for S* if scheduler has a winning strategy for F

Strategies for popular fairness notions

- *Maximality*: just do something (if possible)
- *Strong fairness* wrt to a transition t : if possible, go to a state enabling t and let t occur
- same strategy can be used for many more fairness notions
- *Finitary fairness*: $\bigcup_k \square(\text{enabled}(t) \Rightarrow \text{taken}(k, t))$ is *not* a fairness notion

Aims revisited

- fairness implies machine closure
- fairness is closed under intersection
- popular fairness notions fall into the class

Fairness: other characterizations

- language-theoretic: see paper
- topological: co-meager sets in the Scott topology relativized to S
 - machine closure of (S, F) is density of F in that topology

Fairness and probability

- co-meager set = topologically 'large'
- set of measure 1 = probabilistically 'large'
- notions are similar (cf. Oxtoby 1971)

- in absence of a measure, you can at least prove that Liveness-Spec $\cap S$ is topologically large for your transition system S

Outline

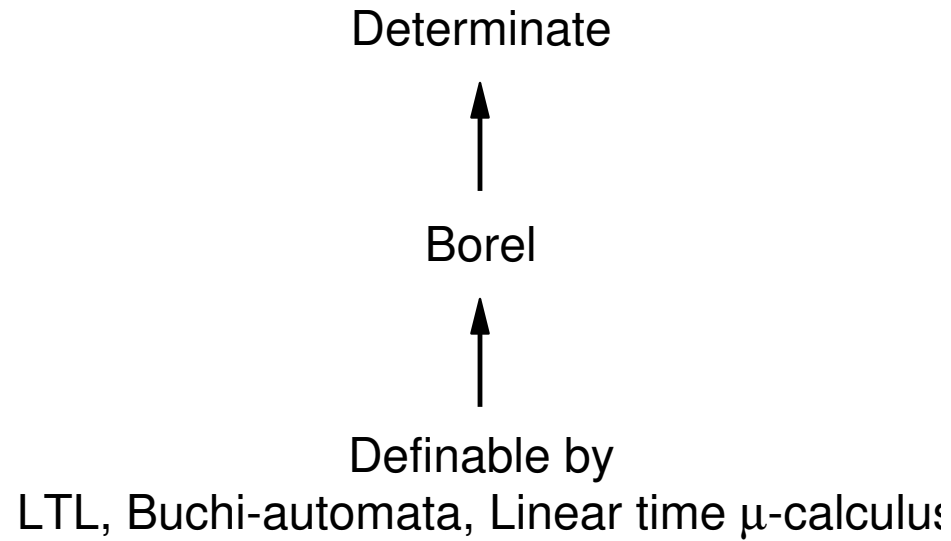
1. Introduction
2. Constructive liveness
3. Fairness
4. A maximality theorem

A maximality theorem

Our definition is, in a sense, the most liberal that meets our aims.

- Restrict to *determinate* properties
- = either scheduler or opponent has winning strategy
- constructive liveness is determinate

Generality of determinacy



need axiom of choice to show existence of indeterminate set

A maximality theorem

Constructive liveness is the largest class of determinate liveness properties that

- *includes dense G_δ sets* and
- *is closed under finite intersection.*

Each non-constructive, determinate liveness property is in conflict with some dense G_δ , i.e., intersecting the two results in a set that is not dense.

Summary

- *Fairness* formalizes
“Sufficiently often possible \Rightarrow sufficiently often taken”
- this assures closure under countable intersection
(and arbitrary union)
- most liberal definition in some sense
- fairness properties are topologically ‘large’

Belated acknowledgement

fairness as we define it appears as *local liveness*
(for infinitary properties)—(Alur and Henzinger 1995)

- easier to check than machine closure for *Streett constraints*

Conclusion

- notions/results carry over to non-sequential models (e.g. event structures), and any ω -algebraic domain
- Also in paper
 - link to Banach-Mazur game
 - a complete lattice of liveness properties
- Updated full version at my website