When a system is fairly correct

Hagen Völzer

joint work with Daniele Varacca (London/Paris)

with contributions from Ekkart Kindler (Paderborn)

Lübeck University

EXPRESS 2006
Part I  Defining Fairness

Part II  Fairly correct systems —
          A generic relaxation of correctness
Part I

Defining Fairness
Road Map for Part I

What is fairness? – A: Examples
  Fair interleaving
  Fair synchronisation
  Fair choice

What is fairness? – B: Characterisation
  A first, language-theoretical characterisation
  A game-theoretical characterisation
  A topological characterisation
Specification of an Implementation

Safety as transition system

Liveness as fairness constraint

- Maximality $\cap$
- Strong fairness wrt $c$
Sequential Maximality

Linear time semantics

- All runs: \( a, ab, aba, \ldots, (ab)^\omega \)
- Unwanted: e.g. \( a \)
- Assumption: Maximality
- Only one maximal run: \( (ab)^\omega \)
Weak Fairness

- Unwanted: e.g. $(ab)^\omega, (cd)^\omega$
- Weak fairness wrt t: $\Diamond \Box enabled(t) \implies \Box \Diamond taken(t)$
What is fairness? – A: Examples

Strong Fairness

• Unwanted: e.g. \((ab)^\omega, (cd)^\omega\)

• Strong fairness wrt \(t\): □ ◊ \textit{enabled}(t) \Rightarrow □ ◊ \textit{taken}(t)
**$k$-Fairness** (E. Best 84)

- **Unwanted:** e.g. $(abcd)^\omega$
- **$k$-Fairness wrt $t$:** $\square \Diamond \text{enabled}(k, t) \Rightarrow \square \Diamond \text{taken}(t)$
- **Alternative:** *Hyperfairness* (Attie, Francez, Grumberg 1993) or (V. 2002)
$\infty$-Fairness

- $k$-Fairness wrt $t$: $\Box \Diamond \text{enabled}(k, t) \implies \Box \Diamond \text{taken}(t)$
- $\omega$-Fairness wrt $t$: $\bigcap_k k$-Fairness wrt $t$
- $\infty$-Fairness wrt $t$: $\Box \text{enabled}(\infty, t) \implies \Box \Diamond \text{taken}(t)$
Extreme Fairness (Pnueli 83)

- □ ◊(φ ∧ enabled(t)) → □ ◊(φ ∧ taken(t))
  where φ is a state formula
- e.g. φ = C and t = d
- E is satisfied under extreme fairness → E has probability 1
- converse not true
\(\alpha\)-Fairness (Lichtenstein, Pnueli, Zuck 85)

- \(\square \Diamond (A \land \Diamond(B \land \Diamond A))\) is not satisfied under extreme fairness, but has probability 1
- \(\alpha\)-Fairness wrt \(\Phi\) and \(t\):
  \[\square \Diamond (\Phi \land \text{enabled}(t)) \implies \square \Diamond (\Phi \land \text{taken}(t))\]
  where \(\Phi\) is a past formula
- e.g. \(\Phi = B \land \ominus A\) and \(t = d\)
- \(\phi\) is satisfied under \(\alpha\)-fairness \(\iff\) \(\phi\) has probability 1
  (in finite-state systems, \(\phi \in \text{LTL}\))
Map of Some Fairness Notions

SM(t) → WF(t) → SF(t) → SF(k,t) → SF(ω,t) → SF(α,t)

XF(t) → SF(ω,t) → SF(α,t)

αF(t) → αF(α,t)
Common Pattern

Sufficiently often enabled $\implies$ sufficiently often taken.

What is fairness?
Setting

- Run: finite or infinite sequence of states: \( x \in \Sigma^\infty = \Sigma^+ \cup \Sigma^\omega \) (Alternative \( x \in \Sigma^\omega \))
  - \( \alpha^\uparrow = \{ x \in \Sigma^\infty \mid \alpha \text{ is prefix of } x \} \)
  - \( x^\downarrow = \{ \alpha \in \Sigma^+ \mid \alpha \text{ is prefix of } x \} \)
- Temporal property: \( E \subseteq \Sigma^\infty \)
- System \( S \subseteq \Sigma^\infty \) all runs generated by a given transition system
What is fairness? – A: Examples

General Structure

Safety as transition system

Liveness as fairness constraint

- Given a system $S$
- $F \subseteq \Sigma^\infty$ is a fairness property for $S$ iff ...
- A fairness notion such as strong fairness maps each system to a fairness property for $S$

What properties do we want fairness to enjoy?
(1) Machine Closure of \((S, F)\)

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

- \(\triangle taken(b)\) is not m.c.
- \(\triangle taken(c)\) is m.c.

- If \((S, F)\) is an implementation \((S, F)\) should be m.c.

= Fairness does not rule out finite runs of the transition system

(Transition system cannot ‘paint itself into a corner’)
(2) Closure under Intersection

= intersection of two (countably many) fairness is fairness

- $x$-Fairness wrt transition 1 $\cap$
- $y$-Fairness wrt process 2 $\cap$
- $z$-Fairness wrt ...

\begin{figure}[h]
\centering
\begin{tikzpicture}
  \node (A) at (0,0) {A};
  \node (B) at (1,0) {B};
  \node (C) at (2,0) {C};
  \draw[->] (A) to [bend right=45] node[above] {a} (B);
  \draw[->] (A) to [bend left=45] node[below] {b} (B);
  \draw[->] (B) to node[right] {c} (C);
\end{tikzpicture}
\end{figure}
Machine Closure is not enough

- $E_1 = \square \Diamond taken(a)$
- $E_2 = \Diamond \square taken(b)$
- $E_1 \cap E_2 = \emptyset$

- $E_2$ prescribes that some choice is not taken sufficiently often
- $E_1, E_2$ are both machine closed
- $E_1 \cap E_2$ is not machine closed

$\implies$ machine-closed properties are not closed under intersection (bad for composition)
What do we want?

1. Machine-closed: not affecting safety
2. Modular: closed under intersection
3. Practical: existing notions fit
4. Otherwise as liberal as possible
$\infty$-Fairness wrt a State $s \in \Sigma$

\[ \square enabled_S(\infty, s) \implies \square \Diamond taken(s) \]
\( \infty \text{-Fairness wrt a Word } w \in \Sigma^+ \)

\[ \square \text{enabled}_S(\infty, w) \implies \square \Diamond \text{taken}(w) \]
What is fairness? – A: Examples

(Memoryless) $\infty$-Fairness wrt $Q \subseteq \Sigma^+$

$\square \ enabled_S(\infty, Q) \implies \square \ \Diamond \ taken(Q)$
Memoryful $\infty$-Fairness wrt $Q \subseteq \Sigma^+$

$\square \textrm{live}_S(Q) \longrightarrow \square \lozenge Q$

Examples:

- $Q = \Sigma^+ w$ ($\infty$-Fairness wrt $w$)
- $Q = "#a = #b"$ (truly memoryful)
Defining Fairness

Definition

$E \subseteq \Sigma^\infty$ is a fairness property for $S$ iff it contains a property of the form $\Box \text{live}_S(Q) \implies \Box \Diamond Q$ for some $Q \subseteq \Sigma^+$. 
What do we want? — Revisited

1. Machine-closed: not affecting safety ✓
2. Modular: closed under intersection ?
3. Practical: existing notions fit ✓

4. Otherwise as liberal as possible ?

5. Moreover:
   • Fairness is closed under superset (and arbitrary union) ✓
   • Is ◊ □ taken(b) a fairness property ?
Banach-Mazur Game

Two players: **Scheduler** and Opponent

- Opponent tries to produce an unfair run
- **Scheduler** wants to ensure fairness
Banach-Mazur Game

Run $x$: Run $x$:  

- Opponent
- Scheduler

• Target: $E \subseteq S$
  • Scheduler wins if $x \in E$
  • otherwise, opponent wins

$F$ is a fairness property for $S$ iff scheduler has a winning strategy for $F$
Scheduler has winning strategy for $F$

Examples

- Memoryful $\infty$-fairness wrt $Q \subseteq \Sigma^+$
- Any weaker property

Counterexamples

- $\Sigma^+$
- $\Diamond \Box \phi$, where $\phi$ is a state property
- $\{\alpha x | \alpha \in \Sigma^+\}$ for $x \in \Sigma^\omega$
- Finitary ‘fairness’ $\bigcup_k \Box (enabled(t) \implies taken(k, t))$
Closure under Intersection

Strategy: \( f : \Sigma^+ \rightarrow \Sigma^+ \) s.t. \( \alpha \) is prefix of \( f(\alpha) \).

Theorem

*Fairness is closed under countable intersection.*

Proof: Let \( f_i \) be a winning strategy for \( E_i \), \( i = 0, \ldots \). Define

\[
f(\alpha) = f_k(f_{k-1}(\ldots f_0(\alpha)\ldots)) \quad \text{where } k = |\alpha|
\]

\( f \) is a winning strategy for \( \bigcap_i E_i \)
What do we want? — Revisited

1. Machine-closed: not affecting safety ✓
2. Modular: closed under intersection ✓
3. Practical: existing notions fit ✓

4. Otherwise as liberal as possible ?

5. Moreover:
   - Fairness is closed under superset (and arbitrary union) ✓
   - □ taken(b) is not a fairness property! ✓
Determinacy

\[ E \subseteq \Sigma^\infty \text{ is determinate if either Scheduler or Opponent has a winning strategy for it.} \]

Existence of indeterminate property needs axiom of choice.

NB. Determinacy yields proof strategy for fairness.
Maximality theorem

Theorem

*Fairness is a maximal class of determinate properties such that fairness is machine-closed wrt the system and fairness is closed under finite intersection.*

Suppose: Scheduler has no strategy for $E$.

$\implies$ Opponent has winning strategy for $E$, let $\alpha$ be its first move.

$\implies$ Scheduler has strategy for $F = \overline{E} \cup \overline{\alpha}^\uparrow$

$\implies$ $\alpha$ has no extension into $E \cap F$.

$\implies$ $E \cap F$ is not machine-closed wrt the system.
What do we want? — Revisited

1. Machine-closed: not affecting safety ✓
2. Modular: closed under intersection ✓
3. Practical: existing notions fit ✓

4. Otherwise as liberal as possible ✓

5. Moreover:
   - Fairness is closed under superset (and arbitrary union) ✓
   - □ taken(b) is not a fairness property! ✓
Scott Topology on $S$

- **Basic open set**: $\alpha^\uparrow$ for $\alpha \in \Sigma^+ \cap S$

- **Open set**: arbitrary union of basic open sets (*guarantee* relative to $S$)
  e.g. $\Diamond \phi$ ($\phi$ is a state property)

- **Closed set**: complement of an open set (*safety* relative to $S$)
  e.g. $\Box \phi$. 
Dense Set $L$

- $L$ intersects every (basic) open set
- $L$ = Liveness relative to $S$
- $(S, L)$ is machine-closed
- e.g. $\Diamond \phi$, $\Diamond \Box \phi$, $\Box \Diamond \phi$ (in $\Sigma^\infty$, $\phi$ is not false)
Dense Open Set

- Finite extension suffices to reach the set (One-shot strategy for scheduler)

= "Observably" dense

e.g. $\diamond \phi$

- is a "large" set
**Dense $G_\delta$ Set $E$**

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

- $E$ is dense $\iff$ all $G_i$ are dense (in *Baire spaces*)

  e.g. $\square \Diamond$ *taken*($t$)

- Still a large set
Theorem

E is a fairness property for S iff E contains a dense $G_\delta$ set. relative to S.
Nowhere Dense Set

One hole = a nonempty open set in the complement of $E$

- Nowhere dense = Full of holes (holes reachable from everywhere)
- $\Leftrightarrow$ complement contains dense open set
- e.g. $\Sigma^k$, $\Box \phi$, $\Sigma^k \cdot \Box \phi$ ($\phi$ is a state formula)
Topological Characterisation of Fairness
Version 2

**Meager set (first Baire category) ‘small’:**

\[
\text{union of countably many nowhere dense sets}
\]

\[\Sigma^+ = \bigcup_{k \in \mathbb{N}} \Sigma^k, \quad \Box \square \phi = \bigcup_{k \in \mathbb{N}} \Sigma^k \cdot \square \phi\]

**Co-meager set (residual) ‘large’:**

\[
= \text{complement of a meager set} \]

\[\Leftrightarrow \text{contains a dense } G_\delta \text{ set (in every Baire space)} \]

\[\Leftrightarrow \text{fairness}\]
Conclusion Part I

- Three independent characterisations of fairness
- Machine-closed and closed under countable intersection and union
- Fairness properties are the large sets in a topological sense
- Characterisation carries over to any \(\omega\)-algebraic domain
Part II

Fair correctness
Road Map for Part II

Topological vs Probabilistic Largeness
Similarities
Separation
Coincidence

Checking Fair Correctness
Linear Time
Branching Time
Complete Fairness
Introduction

Five Philosophers

SPEC

- mutual exclusion and
- starvation-freedom

• System is not correct
  L and R may ‘conspire’ against Me
• However, system is almost correct
  ‘most’ runs satisfy SPEC
Generic Relaxations of Correctness

Let $S$ be the set of all runs of the system.

**Almost Correct**
- SPEC is probabilistically large
  
i.e. $\mu(SPEC) = 1$
- needs probability measure $\mu$ on $S$

**Fairly Correct (New!)**
- SPEC is topologically large
  
i.e. SPEC is a co-meager set in the natural topology on $S$
- there is a fairness assumption $F$ for $S$ such that $S \cap F \subseteq SPEC$
Road Map

Topological vs Probabilistic Largeness
  Similarities
  Separation
  Coincidence

Checking Fair Correctness
  Linear Time
  Branching Time
  Complete Fairness
Borel Measure $\mu$ over Scott Topology on $S$

- *measurable* sets are generated by *basic open sets* $\alpha \uparrow$ for $\alpha \in \Sigma^+ \cap S$
- $\mu(\alpha S \uparrow) = \mu(\alpha \uparrow) \cdot \mu(\alpha S \uparrow | \alpha \uparrow)$
- $\mu$ is determined by giving all $p^S_{\alpha} := \mu(\alpha S \uparrow | \alpha \uparrow)$ for all $\alpha S \in \Sigma^+ \cap S$

- positive: $\forall \alpha, s : p^S_{\alpha} > 0$
- bounded: $\exists \varepsilon \forall \alpha, s : p^S_{\alpha} > \varepsilon$
- Markov: $\forall \alpha, \beta, s, s' : p^s_{\alpha s} = p^s_{\beta s}$

We restrict to *non-leaking* measures, i.e. $\mu(S^{\text{max}}) = 1$ where $S^{\text{max}}$ is the set of all maximal runs of $S$. 
Generic Relaxations of Correctness

Fairly Correct
- SPEC is topologically large
  i.e. SPEC is a co-meager set in the natural topology on $S$
  $\iff$ there is a fairness assumption $F$ for $S$ such that $S \cap F \subseteq SPEC$

Almost Correct
- SPEC is probabilistically large
  i.e. $\mu(SPEC) = 1$
  • needs probability measure $\mu$ on $S$

One natural topology—many associated Borel measures.
Shared Properties of Topological and Probabilistic Largeness

- Here: \( E \) is large \( \implies \) \( E \) is dense
- Large sets form a \( \sigma \)-filter, i.e.:
  - \( E \) is large, \( E \subseteq F \implies F \) is large
  - \( E_i, i \in \mathbb{N} \) are large \( \implies \bigcap_{i \in \mathbb{N}} E_i \) is large
- \( E \) is large \( \implies \overline{E} \) is not large
  - not true for dense
  - call \( \overline{E} \) small when \( E \) is large
- \( E \) countable \( \implies \) \( E \) is small; there exist uncountable \( E \) that are small
- \( E \) is large \( F \) not small \( \implies \) \( E \cap F \) not small
Notions do not coincide! (1/2)

- $E = \square \Diamond 0$
- $\mu(E) = 0$ but $E$ is co-meager
- $\mu(\overline{E}) = 1$ but $\overline{E}$ is meager
- System is infinite!

$p \neq \frac{1}{2}$
Notions do not coincide! (2/2)

- $E = \Box \Diamond (\#A = \#B)$
- $\mu(E) = 0$ but $E$ is co-meager
- Property is not $\omega$-regular, hence not expressible in LTL!

$p \neq \frac{1}{2}$
Coincidence — Main Theorem

**Theorem**

If $S$ is finite-state, $E$ is $\omega$-regular, $\mu$ a bounded Borel measure on $S$ then

$$E \text{ is co-meager in } S \Leftrightarrow \mu(E) = 1$$

In particular true when $\mu$ is a positive Markov measure.
Proof Sketch \((E \text{ is co-meager in } S \Leftrightarrow \mu(E) = 1)\)

Suppose: Scheduler has strategy for \(E\).

\[\Rightarrow\] Scheduler has memoryless strategy for \(E\).
(Berwanger, Grädel, and Kreutzer 2003)

\[\Rightarrow\] Scheduler has bounded strategy for \(E\).

\[\Rightarrow\] \(\mu(E) = 1\)

Suppose: Scheduler has no strategy for \(E\).

\[\Rightarrow\] Opponent has winning strategy for \(E\), let \(\alpha\) be its first move.

\[\Rightarrow\] Scheduler has strategy for \(F = \overline{E} \cup \overline{\alpha} \uparrow\)

\[\Rightarrow\] \(\mu(\overline{E} \cup \overline{\alpha} \uparrow) = 1\) (furthermore: \(\mu(\overline{\alpha} \uparrow) < 1\))

\[\Rightarrow\] \(\mu(\overline{E}) > 0\) hence \(\mu(E) < 1\)
Some Consequences

- Any $\omega$-regular fairness property has probability 1 under randomised scheduling.
- Obtain alternative characterisations for probability 1 (language-theoretic, game-theoretic, topological) in the considered case.
- Obtain nice proof for the known fact that concrete values of probabilities do not matter in the considered case.
- Obtain complexity for model checking fairly correct systems ...
LTL Model Checking

Theorem

Checking whether a finite system is fairly correct wrt an LTL specification is PSPACE-complete.

- Use algorithm for finite Markov chains by Courcoubetis and Yannakakis 95
- Algorithm uses time linear in the system size
- PSPACE-hardness for checking for probability 1 is due to Vardi
Alternative: Reactivity

\[
\phi = \bigwedge_{i=1}^{n} (\Diamond \lozenge h_i \lor \Diamond \Box g_i)
\]

where \(h_i\) and \(g_i\) are past formulas.

- We have linear translation of largeness of \(\phi\) into satisfaction of a CTL+past formula
- Checking CTL+past is PSPACE-complete
- LTL can be translated into reactivity (possible exponential blowup)
- Linear checking when \(h_i\) and \(g_i\) are state formulas (above translation yields CTL formula)
Theorem

*Checking whether a finite system is fairly correct wrt an ω-regular property given by a Büchi automaton is PSPACE-complete.*

- Use algorithm for finite Markov chains by Vardi 85
- Algorithm uses time linear in the system size
- Completeness due to Vardi 85
Large-CTL*

Interpret path quantifier $A$ as "for almost all paths" in either sense

- Large-CTL* has complete axiomatisations
  - Lehmann and Shelah 82: in probabilistic sense
  - Ben-Eliyahu and Magidor 96: in topological sense
  - Axiomatisations for topological interpretation and for finite probabilistic models are the same!

- Model Checking is PSPACE-complete
Large-CTL

Theorem

The model checking problem for Large-CTL can be solved in linear time.

- Largeness can be translated into CTL satisfaction
- Size may blow up
- Blow-up does not affect checking complexity
Question

Is there a strongest fairness property $F$ for $S$, i.e.,

$S$ is fairly (almost) correct wrt $SPEC$ iff $F \cap S \subseteq SPEC$?

**Advantage:** Reduces checking fair correctness to checking satisfaction conditioned on $F$. 
Answer (1/2)

- No, not in general. (Fairness is not closed under arbitrary intersection.)
- Yes, if we are interested in a countable class $\mathcal{F}$ of properties only (e.g. LTL, $\omega$-regular)

$$F_{\mathcal{F}} = \bigcap \{F \in \mathcal{F} | F \text{ is a fairness property for } S\}$$

is complete for $\mathcal{F}$. 
Answer (2/2)

- Word fairness is complete for LTL and $\omega$-regular.

\[ \begin{array}{cccccc}
\text{w} & \text{w} & \text{w} \\
\text{w} & \text{w} & \text{w} \\
\end{array} \]

- $\alpha$-Fairness is also known to be complete.
- Word fairness is not $\omega$-regular.
- No $\omega$-regular-property is complete in general.
- There is no generic LTL formula that can be used to check fair correctness of $S$ for all $SPEC$. 

Conclusion Part II

- Generic relaxation of correctness
- Language-theoretic, topological, game-theoretic, and probabilistic interpretation
- Checking for fair correctness is better than weakening specification
- No need to specify any fairness assumption

- There are overall 8 *path quantifiers* (usual linear-time correctness + 7 generic relaxations)
- Can be interpreted as *path games* (Pistore and Vardi 2003, Berwanger et al 2003) ...
- ... or topologically (Varacca and V. 2006)
References

- Pistore and Vardi: The planning spectrum ..., LICS 2003
- Berwanger, Grädel, and Kreutzer: Once upon a time in a west ..., LPAR 2003
- Oxtoby: Measure and Category ..., Springer 1971
- V., Varacca, and Kindler: Defining Fairness. CONCUR 2005
- Varacca and V.: Temporal logics and model checking for fairly correct systems. LICS 2006
- V.: Refinement-Robust Fairness, CONCUR 2002