Temporal logics and model checking for fairly correct systems

Hagen Völzer\textsuperscript{1}

joint work with Daniele Varacca\textsuperscript{2}

\textsuperscript{1}Lübeck University, Germany
\textsuperscript{2}Imperial College London, UK

LICS 2006
**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**
- $\text{SPEC}$ is probabilistically large
  
  i.e. $\mu(\text{SPEC}) = 1$

- needs probability measure $\mu$ on $S$

**Fairly Correct (New!)**
- $\text{SPEC}$ is topologically large
  
  i.e. $\text{SPEC}$ is a co-meager set in the natural topology on $S$

  $\iff$ there is a fairness assumption $F$ for $S$ such that $S \cap F \subseteq \text{SPEC}$
Road Map

Fairness and Topological Largeness
  Fairness: Examples
  Fairness: Language-theoretic Characterisation
  Fairness: Topological Characterisation

Topological vs Probabilistic Largeness
  Similarities
  Separation
  Coincidence

Model Checking for Fairly Correct Systems
  Linear Time
  Branching Time
  Complete Fairness
Strong Fairness

- Unwanted: e.g. \((ac)^\omega\)
- Assumption: Strong fairness wrt transition \(t\):
  \(\Box \Diamond enabled(t) \implies \Box \Diamond taken(t)\)
**k-Fairness** (E. Best 84)

- Unwanted: “Conspiracy”
- Assumption: \( k \)-Fairness wrt \( t \):
  \[ \square \Diamond enabled(k, t) \implies \square \Diamond taken(t) \]

\[ \begin{align*}
 &< k & t & < k \\
 &< k & t & < k \\
 &< k & t & < k \\
 &< k & t & < k \\
\end{align*} \]
$\infty$-Fairness

- $k$-Fairness wrt $t$: $\square \Diamond \text{enabled}(k, t) \implies \square \Diamond \text{taken}(t)$
- $\infty$-Fairness wrt $t$: $\square \text{enabled}(\infty, t) \implies \square \Diamond \text{taken}(t)$
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
$\infty$-Fairness wrt a State $s \in \Sigma$

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

\[ \square \text{enabled}_S(\infty, w) \implies \square \Diamond \text{taken}(w) \]
(Memoryless) $\infty$-Fairness wrt $Q \subseteq \Sigma^+$

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

$\Box \text{live}_S(Q) \iff '\Box \diamond Q'$

Examples:

- $Q = \Sigma^+ w$ ($\infty$-Fairness wrt $w$)
- $Q = "\#a = \#b"$ (truly memoryful)
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 \( Q \subseteq \Sigma^+ \).
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 $S$)
- **Closed set**: complement of an open set (*safety* relative to $S$)
Dense Set $L$

- $L$ intersects every (basic) open set
- $L$ = *Liveness* relative to $S$
- $L$ \iff ($S$, $L$) is *machine-closed*
Dense Open Set

- Finite extension suffices to reach the set
- "Observably" dense
- 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)
- Still a large set
- Game we play here: *Banach-Mazur game*
Topological Characterisation of Fairness

$E$ is a **co-meager** set iff it *contains* a dense $G_\delta$ set

- true in Baire spaces
- co-meager = topologically large
- co-meager = complement of a *meager* (small) set

**Theorem**

*E is a fairness property for S iff E is a co-meager set relative to S.*
Properties of Fairness

- Refines relative liveness (machine-closure)
- Closed under countable intersection (and superset)
- Maximal class having these two properties (in a strong sense)

- For more: V., Varacca, Kindler: *Defining Fairness*  
CONCUR 2005
Road Map

Fairness and Topological Largeness
  Fairness: Examples
  Fairness: Language-theoretic Characterisation
  Fairness: Topological Characterisation

Topological vs Probabilistic Largeness
  Similarities
  Separation
  Coincidence

Model Checking for Fairly Correct Systems
  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**: $\forall \alpha, \beta, s, s' : p_{\alpha s}^{s'} = p_{\beta s}^{s'}$
Generic Relaxations of Correctness

Fairly Correct

- SPEC is topologically large
  i.e. SPEC is a co-meager set in the natural topology on S

\[ \Leftrightarrow \text{there is a fairness assumption } F \text{ for } S \text{ such that } S \cap F \subseteq SPEC \]

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)

- \( E = \Box \Diamond 0 \)
- \( \mu(E) = 0 \) but \( E \) is co-meager
- \( \mu(\overline{E}) = 1 \) but \( \overline{E} \) is meager
- System is infinite!
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!
Theorem
If $S$ is finite-state, $E$ is $\omega$-regular, $\mu$ a bounded Borel measure on $S$ then

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

In particular true when $\mu$ is a positive Markov measure.
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 complexity for model checking fairly correct systems ...
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

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

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).
Model Checking $\omega$-regular Properties

Theorem

Checking whether a finite system is fairly correct wrt an $\omega$-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
Is there a strongest fairness property $F$ for $S$, i.e.,

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

**Advantage:** Reduces checking fair correctness to checking satisfaction conditioned on $F$. 
Answer

- No, not in general. (Fairness is not closed under arbitrary intersection.)
- Yes, if we are interested in a countable class of properties only (e.g. LTL, $\omega$-regular)
- Word fairness is complete for LTL and $\omega$-regular
- 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

- 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

- Also in paper: topological interpretation of general *path games* and the Pistore-Vardi logic