

When a system is fairly correct

Hagen Völzer^{1,2}

*Institute for Theoretical Computer Science
Lübeck University
Germany*

Abstract

We give an overview over recent work on fairness in reactive and concurrent systems, including an abstract characterisation of fairness. We also derive a notion of a *fairly correct* system and sketch its application.

Keywords: Fairness, liveness, temporal properties, verification, model checking

Extended Abstract

Fairness is a convenient and popular tool when modelling and specifying concurrent systems. A large variety of fairness notions exists in the literature. Among them, we find well-known notions such as *weak fairness (justice)* [12], *strong fairness (compassion)* [12], and *extreme fairness* [15] and less-known notions such as *∞ -fairness* [4], *α -fairness* [13], and *hyperfairness* [3,11,17]. A fairness notion is often meant to represent a particular phenomenon. Phenomena expressed by fairness assumptions include progress of individual processes, general environment behaviour, behaviour of probabilistic choice, impartiality of arbiters and schedulers, and partial synchrony. Many fairness notions are geared to a particular application or specification language. Overviews over fairness can be found in [9,6,12]. More recent studies on fairness include [7,8,11,18].

In contrast to *safety* and *liveness*, which were characterised by Lamport [10] and Alpern and Schneider [1], there was no fully satisfactory abstract characterisation of fairness. However, Apt, Francez, and Katz [2] gave some criteria that must be met by any fairness assumption. Following Lamport [11], we think that their most important criterion is that a fairness assumption must be *machine closed* with respect to the safety property defined by the transition system under consideration.

¹ This extended abstract is based on joint work with Daniele Varacca, Imperial College London, UK and Ekkart Kindler, Paderborn University, Germany

² Email: voelzer@tcs.uni-luebeck.de

This, basically, means that fairness is imposed in such a way to the transition system that the system ‘cannot paint itself into a corner’ [2]; i. e. , whatever the system does, it is possible to continue in such a way that the fairness assumption is met. While machine closedness is necessary for a property to be a fairness property, it does not exclude some properties that are intuitively not fairness properties.

We propose (together with Varacca and Kindler [18]) a definition of fairness that refines machine-closure and excludes properties that are intuitively not fairness properties. One characterisation says: A fairness property with respect to a system is a property that contains a property of the form ‘If each prefix of a run can be extended to satisfy Q , then that run has always eventually a prefix satisfying Q ’, where Q is a property of finite runs. We show that fairness is then closed under arbitrary union and countable intersection and that most popular fairness notions satisfy our definition. We give independent characterisations in terms of game theory, language theory, and general topology [18]. It turns out that fairness as we define it coincides with the *co-meager* sets of the natural topology of runs, a subclass of the dense sets. This shows that our characterisation of fairness is in line with the definitions of safety and liveness given by Lamport [10] and Alpern and Schneider [1] since safety properties are the closed sets and liveness properties are the dense sets of that topology.

A co-meager set is a ‘large’ set in a topological sense. This gives rise to a notion of a ‘fairly correct’ system [16]: a system is *fairly correct* if its specification is a large set relative to the set of all runs of the system, i.e., most runs of the system satisfy the specification. Equivalently, a system is fairly correct if there exists a fairness assumption under which it is correct. Many distributed, especially fault-tolerant, systems are only fairly correct with respect to their actual specification since often, fully correct solutions are too expensive or do not exist [5].

Another natural way to formalise ‘large set’ is to mean *probabilistically large*, i.e., a set of measure 1 for a given probability measure. Note that this notion needs a concrete probability measure, which may be hard to justify for a given system. The notions of probabilistic and topological largeness share many properties. A classic mathematical text book [14] is devoted to study their similarities and differences. Although similar, these notions do not coincide in general—in fact, even for the most straightforward probability measure on the set of runs, there are topologically large sets that have probability 0. However, it turns out [16] that the two notions coincide for bounded Borel measures on finite state systems.

It follows that fair correctness of a finite system is decidable and can be checked with the same complexity as usual correctness for LTL and Büchi automata specifications. However, in contrast to usual correctness, for fair correctness, it is not necessary to specify any fairness assumption explicitly.

References

- [1] Alpern, B. and F. B. Schneider, *Defining liveness*, Information Processing Letters **21** (1985), pp. 181–185.
- [2] Apt, K. R., N. Francez and S. Katz, *Appraising fairness in languages for distributed programming*, Distributed Computing **2** (1988), pp. 226–241.

- [3] Attie, P. C., N. Francez and O. Grumberg, *Fairness and hyperfairness in multi-party interactions*, Distributed Computing **6** (1993), pp. 245–254.
- [4] Best, E., *Fairness and conspiracies*, Information Processing Letters **18** (1984), pp. 215–220, erratum ibidem 19:162.
- [5] Fich, F. E. and E. Ruppert, *Hundreds of impossibility results for distributed computing.*, Distributed Computing **16** (2003), pp. 121–163.
- [6] Francez, N., “Fairness,” Springer, 1986.
- [7] Joung, Y.-J., *On fairness notions in distributed systems, part I: A characterization of implementability*, Information and Computation **166** (2001), pp. 1–34.
- [8] Joung, Y.-J., *On fairness notions in distributed systems, part II: Equivalence-completions and their hierarchies*, Information and Computation **166** (2001), pp. 35–60.
- [9] Kwiatkowska, M. Z., *Survey of fairness notions*, Information and Software Technology **31** (1989), pp. 371–386.
- [10] Lamport, L., *Formal foundation for specification and verification*, in: M. Alford, J. Ansart, G. Hommel, L. Lamport, B. Liskov, G. Mullery and F. Schneider, editors, *Distributed Systems: Methods and Tools for Specification*, LNCS **190**, Springer-Verlag, 1985 .
- [11] Lamport, L., *Fairness and hyperfairness*, Distributed Computing **13** (2000), pp. 239–245.
- [12] Lehmann, D. J., A. Pnueli and J. Stavi, *Impartiality, justice and fairness: The ethics of concurrent termination.*, in: S. Even and O. Kariv, editors, *ICALP*, LNCS **115** (1981), pp. 264–277.
- [13] Lichtenstein, O., A. Pnueli and L. D. Zuck, *The glory of the past*, in: R. Parikh, editor, *Logic of Programs*, LNCS **193** (1985), pp. 196–218.
- [14] Oxtoby, J. C., “Measure and Category. A Survey of the Analogies between Topological and Measure Spaces,” Springer-Verlag, 1971.
- [15] Pnueli, A., *On the extremely fair treatment of probabilistic algorithms*, in: *Proc. 15th Annual Symposium on Theory of Computing (STOC)* (1983), pp. 278–290.
- [16] Varacca, D. and H. Völzer, *Temporal logics and model checking for fairly correct systems*, in: *LICS*, 2006.
- [17] Völzer, H., *Refinement-robust fairness*, in: *Proc. CONCUR 2002 – 13th International Conference on Concurrency Theory, Brno, Czech Republic*, LNCS **2421** (2002), pp. 547–561.
- [18] Völzer, H., D. Varacca and E. Kindler, *Defining fairness*, in: M. Abadi and L. de Alfaro, editors, *CONCUR*, LNCS **3653** (2005), pp. 458–472.