Defining Fairness in Reactive and Concurrent Systems

HAGEN VÖLZER, IBM Research — Zurich, Switzerland
DANIELE VARACCA, PPS - CNRS and Univ Paris Diderot, France

We define when a linear-time temporal property is a *fairness property* with respect to a given system. This captures the essence shared by most fairness assumptions that are used in the specification and verification of reactive and concurrent systems, such as weak fairness, strong fairness, k-fairness, and many others. We provide three characterizations of fairness: a language-theoretic, a game-theoretic, and a topological characterization. It turns out that the fairness properties are the sets that are "large" from a topological point of view, that is, they are the *co-meager* sets in the natural topology of runs of a given system.

This insight provides a link to probability theory where a set is "large" when it has measure 1. While these two notions of largeness are similar, they do not coincide in general. However, we show that they coincide for ω-regular properties and bounded Borel measures. That is, an ω-regular temporal property of a finite-state system has measure 1 under a bounded Borel measure if and only if it is a fairness property with respect to that system.

The definition of fairness leads to a generic relaxation of correctness of a system in linear-time semantics. We define a system to be *fairly correct* if there exists a fairness assumption under which it satisfies its specification. Equivalently, a system is fairly correct if the set of runs satisfying the specification is topologically large. We motivate this notion of correctness and show how it can be verified in a system.

Categories and Subject Descriptors: F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs

General Terms: Languages, Theory, Verification

Additional Key Words and Phrases: Fairness, concurrent systems, temporal properties, temporal logic, machine closure, game theory, topology, model checking

ACM Reference Format:
Völzer, H. and Varacca, D. 2012. Defining fairness in reactive and concurrent systems. J. ACM 59, 3, Article 13 (June 2012), 37 pages.
DOI = 10.1145/2220357.2220360 http://doi.acm.org/10.1145/2220357.2220360

1. INTRODUCTION

A mathematical model of a reactive and concurrent system usually comes with one or more *fairness* assumptions. A fairness assumption usually stipulates that if a particular behavior of the system is sufficiently often possible during a given run of the system, then that behavior occurs sufficiently often in that run. Depending on what exactly we mean by "behavior", "sufficiently often" and "possible", many different fairness notions arise.

Some results in this article have been previously published as conference contributions [Varacca and Völzer 2006; Völzer et al. 2005]. An unreviewed informal presentation of some results was included in the concurrency column of the Bulletin of the EATCS, Vol. 90, pp. 90–108.

Authors' addresses: H. Völzer, IBM Research – Zurich, Säumerstrasse 4, CH-8803 Rüschlikon, Zurich, Switzerland; email: hvo@zurich.ibm.com; D. Varacca, Université Paris Diderot, 5 rue Thomas-Mann, 75205 Paris Cedex 13, France; email: varacca@pps.jussieu.fr.

DOI 10.1145/2220357.2220360 http://doi.acm.org/10.1145/2220357.2220360

For example, a run is said to be *weakly fair* with respect to an action A when the following implication is true: If A is eventually always enabled during the run, then it must be taken infinitely many times. Consider a process with two parallel threads. In principle, a scheduler could only give CPU time to one of the two threads. Such a scheduler is clearly not fair, and indeed it violates weak fairness with respect to the first action of the other thread.

In contrast to other important classes of temporal properties, such as *safety* and *liveness* [Alpern and Schneider 1985; Lamport 1977], no general characterization of fairness has so far been proposed, that is, there is no agreed definition of what the class of all fairness properties is. Apt et al. [1988] gave some criteria that must be met by fairness. Following Lamport [2000], we think that their most important criterion is that a fairness assumption must be *machine closed*[1] with respect to the safety property defined by the underlying transition system. This, basically, means that fairness is imposed in such a way to the transition system that the system "cannot paint itself into a corner" [Apt et al. 1988]; that is, whatever the system does in finite time, it is possible to continue in such a way that the fairness assumption is met. (To recall the precise definition, see Section 2.2.) However, machine closure does not exclude some properties that, we think, should not be considered to be fairness properties. For example, given a system M and an action A of the system, consider the two properties:

F_M—Action A is always eventually taken if it is always eventually enabled, and
E_M—Action A is eventually henceforth never taken.

Whereas F_M (called *strong fairness* with respect to A in M) is a typical fairness assumption that enforces an action to be taken sufficiently often, E_M rather prevents a particular choice, viz. action A, from being taken sufficiently often. E_M is therefore not a fairness property from our point of view. However, both properties are machine closed with respect to any safety property.[2]

Another issue is that fairness should be closed under intersection, that is, the intersection of finitely many, or better, countably many fairness assumptions should be a fairness assumption. This is because fairness assumptions are usually imposed stepwise and componentwise, for example, with respect to a particular process, state, or transition. The fairness assumption for the system is then the intersection of all fairness assumptions for its components.

Thus, for a given system M or, more generally, for a given safety property S, we want to define when a temporal property F should be called *a fairness property in* S such that

(1) when F is a fairness property in S, then F is machine closed with respect to S;
(2) fairness properties are closed under (countable) intersection;
(3) popular fairness notions from the literature such as *strong fairness* (see Section 3.3) should correspond to fairness properties in our sense.

Machine closure is not sufficient to guarantee closure under intersection: The intersection of F_M and E_M is the empty set in some systems M, and the empty set is not machine closed with respect to any nonempty safety property. Kwiatkowska [1991]

[1] *Machine closure* was originally called *feasibility* [Apt et al. 1988]. The term "*machine closed*" was introduced by Abadi and Lamport [1991].
[2] E_M also meets the other criteria proposed by Apt et al. [1988].

proposes a definition of fairness[3] that is closed under countable intersection. However, important popular fairness notions, such as strong fairness, are not covered by her definition, as we will show in Section 8.

In this article, we propose a definition of when a linear-time temporal property is a fairness property with respect to a given system, such that the requirements (1–3) are met. We give three characterizations for the family of all fairness properties: a language-theoretic, a game-theoretic and a topological characterization. The language-theoretic characterization is a general formalization of the standard intuition: if something is sufficiently often possible, it will happen sufficiently often. In the game-theoretic characterization, a fairness property is a property that can be guaranteed by a scheduler that gets control over the system infinitely often for a finite amount of time. Finally, it turns out that the fairness properties are the "large" sets from a topological point of view, that is, they are the co-meager sets in the natural topology of runs of a given system.

The topological insight provides a link to probability theory, where a set is "large" when it has measure 1. While these two notions of largeness are very similar, they do not coincide in general. However, we show that they coincide for ω-regular properties and bounded Borel measures. That is, an ω-regular temporal property of a finite-state system has measure 1 under a bounded Borel measure if and only if it is a fairness property with respect to that system.

The characterization of fairness directly leads to a generic relaxation of when a system is correct with respect to a linear-time specification. This notion of correctness, which we call *fair correctness*, has again a language-theoretic, a topological and a game-theoretic interpretation. We motivate this notion of correctness and discuss how a system can be shown to be fairly correct.

This article is structured as follows. Section 2 defines basic preliminary notions that are used throughout the article. In Section 3, we review the most popular fairness notions from the literature. That leads us to derive a first general definition of fairness in Section 4 using language-theoretic terms. In Section 5, we provide the first equivalent characterization of fairness in terms of a two-player game, called the *Banach-Mazur game*. The game-theoretic characterization allows us to prove some important properties of the class of fairness properties in Section 6. In Section 7, we identify the relationship of fairness with the Safety-Progress classification of properties proposed by Manna and Pnueli [1990], which refines our intuition about which temporal properties are fairness properties. In Section 8, we give another equivalent characterization of fairness, now in topological terms. It relates to the topological characterization of safety and liveness that was proposed by Alpern and Schneider [1985]. The insight that fairness properties are the properties that are "large" from a topological point of view then leads to a link to probabilistic systems and properties that have measure one. This link is explored in Section 9. Finally, Section 10 introduces fair correctness and discusses proof and model checking techniques for its verification.

2. BASIC NOTATIONS AND DEFINITIONS

In this chapter, we collect basic preliminary definitions, which include sequential runs, temporal properties and transition systems.

[3]Kwiatkowska [1991] works on the domain of Mazurkiewicz traces. She defines a fairness property for a system to be a G_δ set of maximal traces that is machine closed with respect to the safety property of the system.

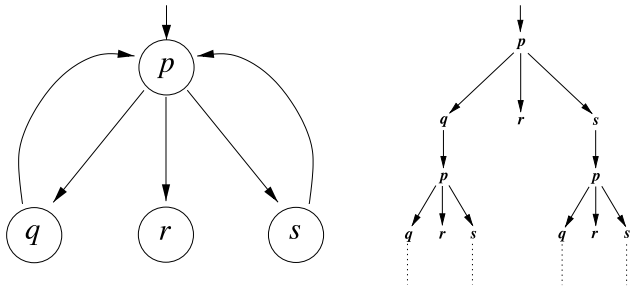

Fig. 1. A four-state system and the set of its runs represented as an infinite tree.

2.1. Systems and Runs

Let Σ be a nonempty set, whose elements will be thought of as *states*. Σ^* and Σ^ω denote the set of finite and infinite sequences over Σ, respectively. The set of all sequences $\Sigma^* \cup \Sigma^\omega$ is denoted as Σ^∞. We use the symbols α, β for denoting finite sequences, and x, y for arbitrary sequences. The empty sequence is denoted by ϵ. The length of a sequence x is denoted by $|x|$ ($= \omega$ if x is infinite). The set of all sequences of length k is denoted by Σ^k. Concatenation of sequences is denoted by juxtaposition; $\sqsubseteq$ denotes the usual *prefix order* on sequences. As usual, we write $x \sqsubset y$ when $x \sqsubseteq y$ and $x \neq y$.

Two sequences x, y are *compatible* if $x \sqsubseteq y$ or $y \sqsubseteq x$. Given a set $X \subseteq \Sigma^\infty$, we denote by $\max(X)$ the set of maximal elements of X under the prefix order. By $x\uparrow = \{y \mid x \sqsubseteq y\}$ and $x\downarrow = \{y \mid y \sqsubseteq x\}$ we denote the sets of all *extensions* and *prefixes* of a sequence x, respectively. The least upper bound of a sequence $(\alpha_i)_{i=0,1,\ldots}$ of finite sequences, where $\alpha_i \sqsubseteq \alpha_{i+1}$, is denoted by $\sup_i \alpha_i$. For a sequence $x = s_0, \ldots, s_n, \ldots$ and an index i where $0 \leq i < |x|$ of x, x_i denotes the finite prefix $s_0, \ldots, s_{i-1}$ of x and $x(i)$ denotes the state s_i. If $x \neq \epsilon$ and $0 \leq i < |x|$, then i is called a *position* of x.

An *action* or *transition relation* over Σ is a nonempty relation $A \subseteq \Sigma \times \Sigma$. Action A is *enabled* in a state s if there exists an s' such that $(s, s') \in A$; A is *taken* in a sequence x if there is a position i of x such that $(x(i), x(i+1)) \in A$. A *system* is a tuple $M = (\Sigma, R, \Sigma_0)$, where $R \subseteq \Sigma \times \Sigma$ is a transition relation over Σ and $\Sigma_0 \subseteq \Sigma$ is a set of *initial states*. The system is *finite* if Σ is finite. A *path* or *word* of a system M is a sequence x such that $(x(i-1), x(i)) \in R$ for each $i, 0 < i < |x|$. A *run* of a system M is a path of M such that if it is nonempty, then $s_0 \in \Sigma_0$. The set of all runs of M is denoted by S_M.

Remark 2.1. A run is thought of as an observation of global states. The empty run stands for the observation in which the initial state has not yet been observed. We could also develop the theory for sequences of alternating states and transitions or of transitions only. Modulo some technical details, these alternatives would differ very little.

Example 2.2. Figure 1 shows a system M over $\Sigma = \{p, q, r, s\}$, where $\Sigma_0 = \{p\}$, $R = \{(p, q), (p, r), (p, s), (q, p), (s, p)\}$. The sequences $x_1 = pq$, $x_2 = (pq)^\omega$, and $x_3 = pr$ are three runs of this system. We have $x_1 \sqsubseteq x_2$ and $x_2, x_3 \in \max(S_M)$. The infinite tree in Figure. 1 represents S_M, the set of all finite and infinite runs of M.

2.2. Temporal Properties

A *temporal property* (*property* for short) is a set $E \subseteq \Sigma^\infty$ of sequences of states. We say that some sequence x *satisfies* a property E if $x \in E$; otherwise we say that x *violates* E. We say that E is *finitary* if $E \subseteq \Sigma^*$ and E is *infinitary* if $E \subseteq \Sigma^\omega$. Furthermore, E is *upward-closed* if $x \in E$ and $x \sqsubseteq y$ implies $y \in E$; E is *downward-closed* if $x \in E$

and $y \sqsubseteq x$ implies $y \in E$; E is *complete*, sometimes also called *limit-closed*, if $\alpha_i \in E$ for $i \in \mathbb{N}$ with $\alpha_i \sqsubseteq \alpha_{i+1}$ implies $\sup_i \alpha_i \in E$.

A property S is a *safety property* if for any sequence x violating S, there exists a finite prefix α of x that violates S and each extension of a sequence violating S also violates S, that is,

$$\forall x \notin S : \exists \alpha \sqsubseteq x : \alpha\uparrow \cap S = \varnothing.$$

Equivalently, a property is a safety property precisely when it is *downward-closed* and *complete*. We can think of a safety property S as a tree, because $(S \cap \Sigma^*, \sqsubset_1)$ is a tree with root ϵ, where $\alpha \sqsubset_1 \beta$ if there exists a state s such that $\alpha s = \beta$. S corresponds to the set of all (finite and infinite) paths of the tree that start in the root (cf. also Figure 1). The set S_M is a safety property for each system M. Therefore, in the following, we will think of a safety property as a generalized system. In particular, we call an element of a safety property also a *run*. The set of all sequences Σ^∞ is also a safety property and can be seen as the set of runs of a "universal" system.

Consider a safety property S and a finite sequence $\alpha \in S$. A property E is *live in α with respect to S* if there exists a sequence x such that $\alpha \sqsubseteq x \in S \cap E$. Intuitively, E is live in a finite run of a system if the system has still a chance to satisfy E in the future. A property E is a *liveness property in S* if E is live in every $\alpha \in S \cap \Sigma^*$. In this situation, we also say that (S, E) is *machine-closed* [Abadi and Lamport 1991; Apt et al. 1988]. If $S = \Sigma^\infty$, then we simply say that E is a *liveness* property. Hence, E is a liveness property if and only if

$$\forall \alpha \in \Sigma^* : \alpha\uparrow \cap E \neq \varnothing.$$

A property is *ω-regular* if it is a property accepted by some Büchi automaton, or, equivalently a property definable in Monadic Second Order logic (see, e.g., Thomas [1990]).

Example 2.3. $\Sigma^{\leq k} = \{\alpha \in \Sigma^* \mid |\alpha| \leq k\}$ is a safety property for each $k \in \mathbb{N}$; Σ^* and Σ^ω are examples of liveness properties. Whereas Σ^* is a liveness property with respect to each safety property S, Σ^ω is a liveness property with respect to S only if $\max(S) \subseteq \Sigma^\omega$; $\max(S)$ is always a liveness property with respect to S. Σ^∞ is the only property that is a safety as well as a liveness property.

Remark 2.4. A temporal property is often (e.g. [Alpern and Schneider 1985; Manna and Pnueli 1990]) defined to be a subset of Σ^ω. It is then argued that finite runs can be mimicked by infinite ones by repeating the last state infinitely often. This often leads to a simplification of the presentation. The difference between the two approaches is not really essential. We will indicate when notable differences between the two approaches arise. Including finite runs, as we do here, gives rise to a more natural generalization to other domains such as nonsequential runs.

2.3. Linear-Time Temporal Logic

Some temporal properties can be expressed by formulas of a *linear-time* temporal logic such as LTL (see Manna and Pnueli [1992] and Emerson [1990]).

Let Σ be a set of states, AP a countable set of *atomic propositions*, and $v : AP \to 2^\Sigma$ a mapping that assigns each atomic proposition the set of states at which it is *satisfied*. We assume here that v is given implicitly and hence we will also refer to an atomic proposition as a *state property*. In particular, we will use in many examples, a state s as an atomic proposition that is satisfied at s and only at s.

The formulae ϕ of the logic *LTL* are defined as follows:

$$\begin{aligned}\phi, \psi \ :=& \\ &\mid \ \Phi \text{ where } \Phi \text{ is a state property} \\ &\mid \ \top, \neg\phi, \phi \wedge \psi \\ &\mid \ \bigcirc\phi, \phi \ \mathrm{U} \ \psi\end{aligned}$$

The temporal operators are pronounced as follows: $\bigcirc\phi$ as "next time" ϕ and $\phi \ \mathrm{U} \ \psi$ as ϕ "until" ψ.

Satisfaction is defined as follows (cf. Emerson [1990] and Clarke et al. [1986]). Let x be a sequence, and i a position of x. We define:

(1) $x, i \models \Phi$ if $x(i) \in v(\Phi)$,
(2) $x, i \models \top$ always; $x, i \models \neg p$ if $x, i \not\models p$; $x, i \models p \wedge q$ if $x, i \models p$ and $x, i \models q$,
(3) $x, i \models \bigcirc\phi$ if $i + 1$ is a position of x and $x, i + 1 \models \phi$,
(4) $x, i \models \phi \ \mathrm{U} \ \psi$ if there exists a position $j \geq i$ of x such that $x, j \models \psi$ and for each k, we have $i \leq k < j \Rightarrow x, k \models \phi$.

Then, for a system M, we say that ϕ is *satisfied* in M, denoted $M \models \phi$, if for all $x \in S_M$ we have $x, 0 \models \phi$. Furthermore, we define $\mathrm{sat}(\phi) = \{x \in \Sigma^\infty \mid x, 0 \models \phi\}$. A temporal property E is said to be *LTL-expressible* if there exists an LTL formula ϕ such that $E = \mathrm{sat}(\phi)$. It is well known that all LTL-expressible properties are ω-regular [Emerson 1990; Thomas 1990].

Additional Boolean operators can be defined as usual. Additional temporal operators are defined as abbreviations as follows.

$\Diamond\phi = \top \ \mathrm{U} \ \phi$ ("eventually" ϕ),
$\Box\phi = \neg\Diamond\neg\phi$ ("always" ϕ).

RLTL (restricted LTL) refers to the subset of those LTL formulas that do not contain the operators $\bigcirc$ and U, but may contain $\Diamond$ and $\Box$.

Example 2.5. With respect to the system M depicted in Figure 1, $\Box(\bigcirc q \Rightarrow p)$ denotes a safety property that is satisfied in M, whereas $\Box(p \Rightarrow \bigcirc q)$ denotes a safety property that is not satisfied in M; $\Diamond p$ is a liveness property that is satisfied in M, whereas $\Diamond q$ is a liveness property that is not satisfied in M; $\Diamond q$ is live in $\alpha = ps$, but not in pr. $\Diamond r$ is a liveness property in S_M, that is, machine-closed with respect to S_M, whereas $\Box\Diamond p$ is not, because it is not live in pr.

3. SURVEY OF FAIRNESS NOTIONS

The distinction of safety and liveness properties in the specification and verification of reactive systems is also reflected in the operational model of a reactive system: Some sort of state machine or transition system defines the set of all possible runs of the system, which is a safety property. To guarantee something to happen at all and to guarantee that some particular choices will eventually be made, there is an additional liveness property. That liveness property is usually called the *fairness assumption* of the reactive system.

Fairness usually means that a particular choice is taken sufficiently often provided that it is sufficiently often possible [Apt et al. 1988]. Depending on the interpretation of "choice", "sufficiently often", and "possible", many different fairness notions arise (cf., e.g., Lehmann et al. [1981], Francez [1986], and Kwiatkowska [1989]).

Before we propose a general definition of fairness, we review the most popular and some additional notable fairness assumptions that are used in the literature. To do so, we will represent some example systems as Petri nets, assuming the reader to be

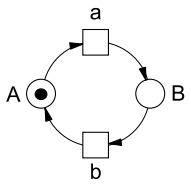

Fig. 2. A simple process.

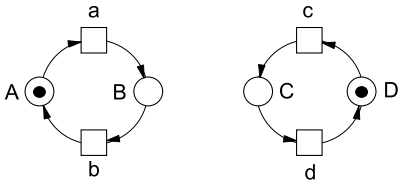

Fig. 3. Two independent processes.

familiar with the basic firing rule of a Petri net (see, e.g., Reisig [1985] and Murata [1989]).

The fairness properties we discuss are actually parametric on the systems at hand. For instance, for any given system and any given transition, there is a corresponding "strong fairness" property. Therefore rather than talking of fairness *properties*, we more precisely present fairness *notions*, that can be defined as maps from systems, transitions, and other parameters, to actual properties.

3.1. Sequential Maximality

Consider the system in Figure 2, represented as a Petri net. As such, the system specification only says what can and what cannot happen, that is, its semantics is the set of all its sequential runs. It does not say that something must happen at all. To say that something must happen, we can use the *maximality assumption*, which says that the system does not arbitrarily stop the computation.

A run x is *maximal with respect to an action* A if it is infinite or if its final state does not enable A. Hence, given a system $M = (\Sigma, R, \Sigma_0)$ and a partition of R into actions $A_1, \ldots, A_n$, a run of M is maximal iff it is maximal with respect to each A_i, $i = 1, \ldots, n$. In the system considered, this means that after every a, there must be a b and that after every b, there must be an a. This leaves only the run $(ab)^\omega$, which is the unique maximal run of the system. Therefore, the system satisfies the property "infinitely often a" under the maximality assumption.

3.2. Weak Fairness

Consider now the system in Figure 3 and assume maximality. Then, that system does not satisfy "infinitely often a" because the maximal run $(cd)^\omega$ does not. Although the overall system does not stop in this run, one of its components does. To rule out such a behavior, we assume *weak fairness*, also known as *justice* [Lehmann et al. 1981].

A run x is *weakly fair* with respect to an action A if A is taken infinitely often or A is always eventually disabled, that is, for each position i of x there exists a position $j \geq i$ such that A is not enabled in $x(j)$. Therefore, the maximal run $(cd)^\omega$ is not weakly fair with respect to a. The system does in fact satisfy "infinitely often a" under weak fairness with respect to a and b. Weak fairness with respect to an action A is obviously strictly stronger than maximality with respect to A.

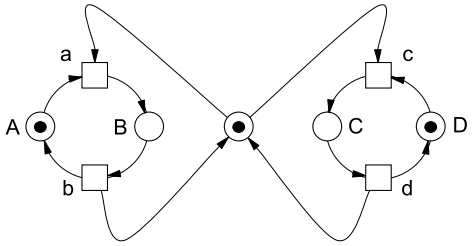

Fig. 4. Two processes sharing a resource.

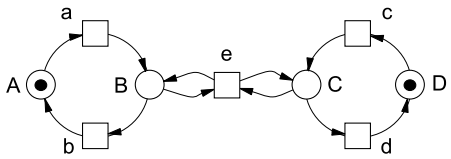

Fig. 5. Two processes sharing an action.

3.3. Strong Fairness

In the next system, see Figure 4, weak fairness is not sufficient to establish "infinitely often a" because the run $(cd)^\omega$ is weakly fair with respect to all transitions of the system. In particular, it is weakly fair with respect to a because a is always eventually disabled.

However, we can consider $(cd)^\omega$ unfair with respect to a because a is infinitely often enabled but never taken. This kind of unfairness is captured by the notion of *strong fairness*, which is also known as *compassion* [Lehmann et al. 1981].

A run is *strongly fair* with respect to an action A if A is taken infinitely often in x or A is eventually henceforth never enabled in x, that is, there is a position i of x such that A is not enabled in $x(j)$ for each position $j \geq i$. Strong fairness with respect to a together with maximality with respect to b and d then establish "infinitely often a" in the system. Strong fairness is obviously strictly stronger than weak fairness.

3.4. k-Fairness

In the next system, see Figure 5, strong fairness with respect to all transitions fails to establish "infinitely often e", because the run $(ab\,cd)^\omega$ violates it but is strongly fair with respect to all transitions. In particular, it is strongly fair with respect to e because e is never enabled in that run.

Among the fairness notions that establish "infinitely often e", there is the notion of *strong k-fairness* [Best 1984] for $k \geq 1$, cf. also *hyperfairness* as discussed by Lamport [2000].

Let $M = (\Sigma, R, \Sigma_0)$ be a system. An action A is *k-enabled* in a state s of a system M, $k \in \mathbb{N}$ if there exists a (finite nonempty) word $w = s_0, \ldots, s_n$ of M such that $s_0 = s$, $n \leq k$ and A is enabled in s_n. A run x is *strongly k-fair* with respect to action A if A is infinitely often taken in x or A is eventually henceforth never k-enabled, that is, there is a position i of x such that A is not k-enabled in $x(j)$ for each position $j \geq i$.

Weak fairness for all transitions together with strong 1-fairness for e indeed establish "infinitely often e". Strong $(k+1)$-fairness is clearly stronger than strong k-fairness, and strong 0-fairness coincides with strong fairness.

Remark 3.1. The "unfairness" arising in the system in Figure 5 is also known from the variant of the Dining Philosophers, in which a philosopher picks up both his forks

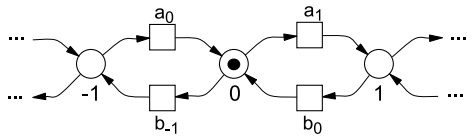

Fig. 6. A nondeterministic walk on the integer line.

at the same time to eat. There, a philosopher may starve because his two neighbors "conspire" against him by eating alternately in such a way that his two forks are never available at the same time. Note that transition e in Figure 5 needs two resources (B and C) at the same time. There are more complex fairness notions that better capture the "unfairness" in this example [Attie et al. 1993; Völzer 2002, 2005].

3.5. ∞-Fairness

Consider now the infinite-state system in Figure 6. Suppose we are interested here in the property "state 0 is visited infinitely often". This property is not established by strong k-fairness for any k because the diverging run $a_1a_2\ldots$ is strongly k-fair with respect to any transition for any $k \geq 0$. However, we can use the stronger notion of *strong ∞-fairness* [Best 1984].

An action A is *∞-enabled* in a state s of a system M if there exists a word $w = s_0, \ldots, s_n$ of M such that $s_0 = s$, and A is enabled in s_n. A run x is *strongly ∞-fair* with respect to action A if A is infinitely often taken in x or A is eventually henceforth never ∞-enabled, that is, there is a position i of x such that A is not ∞-enabled in $x(j)$ for each position $j \geq i$.

It is easy to see that ∞-fairness with respect to a_0 and b_0 establishes the preceding specification.

3.6. Word Fairness

While strong ∞-fairness with respect to transitions is very strong, there are still some useful specifications that are not established by it. As an example, consider the system in Figure 7 and the specification "the finite word $abca$ occurs infinitely often". The run $(abcd)^\omega$ does not satisfy the specification but it is strongly ∞-fair with respect to every transition, because every transition is taken infinitely often in this run. In such a case, we can extend the above fairness notions and define them with respect to finite words of transitions rather than with respect to a single transition only.

Let M be a system. We say that a word w of M is *enabled* in a state s of M if sw is also a word of M. We say that w is *taken* in x at position i if $x_iw \sqsubseteq x$. A run x of M is *strongly fair* with respect to w if w is taken infinitely often in x or w is eventually henceforth never enabled, that is, there exists a position i of x such that $x(j)$ does not enable w for each position $j \geq i$. A run x of M is *word fair* if it is strongly fair with respect to every finite word w of M; x is *state fair* (*transition fair*) if it is strongly fair with respect to every word of length 1 (length 2) of M.

Clearly, strong fairness with respect to the word $abca$ establishes the considered specification.

3.7. Other Notions of Fairness

Another remarkable notion is *equifairness* [Francez 1986]. A run x is *equifair* with respect to a pair (A_1, A_2) of actions if it is strongly fair with respect to both and the following holds: If x has infinitely many positions i such that both A_1 and A_2 are enabled in $x(i)$, then x has infinitely many positions j such that A_1 is taken k times in x_j implies that A_2 is taken k times in x_j.

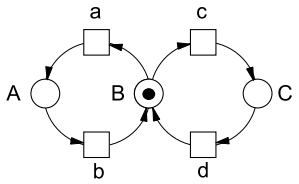

Fig. 7. A recurrent free choice.

Equifairness with respect to a and c in Figure 7 prescribes that each fair run has infinitely many positions such that the number of previous occurrences of a equals the number of previous occurrences of c.

Remark 3.2. In the literature, we usually find the additional intuitive assumption that for each state s of M, A_1 is enabled in s iff A_2 is enabled in s.

Other fairness notions found in the literature include those that were developed for the verification of randomized systems, for example, *extreme fairness* [Pnueli 1983] and *α-fairness* [Lichtenstein et al. 1985]. There are many more fairness notions in the literature, which we cannot all mention here. Overviews can be found elsewhere [Apt et al. 1988; Francez 1986; Joung 2001; Kwiatkowska 1989; Lamport 2000].

4. A LANGUAGE-THEORETIC CHARACTERIZATION OF FAIRNESS

All the examples of fairness notions that we have presented in Section 3 require that some finite behavior must be taken "sufficiently" often, provided that it is "possible". The most general notion of a finite behavior is a finitary property $Q \subseteq \Sigma^*$, where Q "is taken" in a finite prefix α of a sequence if $\alpha \in Q$.

The weakest form of "Q is possible" that we encountered is "there exists an extension into Q". The strongest form of "sufficiently often" that we encountered is "infinitely often". We therefore obtain the following generalization of ∞-fairness as the strongest fairness notion with respect to some finitary property Q.

Definition 4.1 (∞-*Fairness with respect to* Q). Let S be a safety and Q a finitary property. A run x is ∞-*fair* with respect to Q if

— there are infinitely many $i \in \mathbb{N}$ such that $x_i \in Q$ or
— Q is not *strictly live* with respect to S in some finite prefix α of x, that is, there is no finite run β such that $\alpha \sqsubset \beta \in Q \cap S$.

The set of ∞-fair runs in S with respect to Q is denoted as $\mathrm{F}_S(Q)$.

Thus, Definition 4.1 says that a run x is ∞-fair with respect to Q if each finite prefix of x that has a proper extension within S into Q is properly extended along x into Q. This implies that any finite run in $\max(S)$ is ∞-fair because it has no proper extension.

Example 4.2. If Q is the set of all finite sequences that end with an occurrence of a given action A, that is, $Q = \{\alpha s s' \mid \alpha \in \Sigma^*, (s, s') \in A\}$, then $\mathrm{F}_S(Q)$ is exactly strong ∞-fairness with respect to A as introduced in Section 3.5. This is easily generalized to ∞-fairness with respect to a word.

Definition 4.1 presents the strongest form of fairness we consider with respect to some finitary property Q. Any weaker form of fairness, such as strong and weak fairness, can be obtained by weakening. We thus define that a property is a fairness property if it *contains* all ∞-fair runs with respect to some Q.

Definition 4.3 (*Fairness*). Let S be a safety property. A temporal property E is a *fairness property in* S with respect to some finitary property Q if $\mathrm{F}_S(Q) \subseteq E$. We say that E is a *fairness property* in S if there exists a Q such that $\mathrm{F}_S(Q) \subseteq E$.

Example 4.4. Any property weaker than ∞-fairness (such as strong k-fairness etc.) is a fairness property according to Definition 4.3. Furthermore, let $Q = \{\alpha \mid A_1$ is taken exactly k times in α implies A_2 is taken exactly k times in $\alpha\}$. Then, $\mathrm{F}_{S_M}(Q)$ is a subset of equifairness in M with respect to (A_1, A_2). Hence, equifairness in S_M is a fairness property in S_M. Therefore all fairness notions introduced in Section 3 generate fairness properties with respect to a given system.

The class of ∞-fairness properties with respect to some Q (Definition 4.1) is, in general, not closed under weakening and thus Definition 4.3 is not redundant. To show this, a simple cardinality argument suffices: the class of ∞-fairness properties on a finite system has at most the cardinality of the continuum c (as there are at most c finitary properties), whereas the class of fairness properties has in general cardinality 2^c. Indeed, consider the complete graph over three states $\{p, q, r\}$, and consider the set P to be ∞-fairness with respect to the set of all finite runs that end with p. P is the set of runs with infinitely many occurrences of p. The complement of P is the set of runs with finitely many occurrences of p and has cardinality c. Therefore there are 2^c distinct supersets of P.

More interestingly, we can show that important fairness notions, such as strong fairness, are not covered without weakening, that is, by Definition 4.1.

PROPOSITION 4.5. *Consider the complete system over two states* $S = \{p, q\}^\infty$. *Let* F *denote strong fairness with respect to action* $A = \{(p, p)\}$. *There is no finitary property* Q *such that* $F = \mathrm{F}_S(Q)$. *Let* F' *denote* F *intersected with maximality with respect to all other transitions. There is no* Q *such that* $F' = \mathrm{F}_S(Q)$.

PROOF. Deferred to Section 8.7. □

5. A GAME-THEORETIC CHARACTERIZATION OF FAIRNESS

The language-theoretic characterization can be used to prove that a given property E is indeed a fairness property: We display a finitary property Q such that $\mathrm{F}_S(Q) \subseteq E$. However, the language-theoretic characterization does not give us a useful tool for proving that a given property is not a fairness property. The game-theoretic characterization of fairness, presented in this section, will give us such a tool. In particular, this characterization implies that a fairness assumption can never prevent a particular finite behavior from occurring sufficiently often and thus allows us to prove that the property E_M in Section 1 is not a fairness property. The game-theoretic characterization also turns out to be useful for proving some properties of our definition of fairness.

5.1. The Banach-Mazur Game

Let S be a safety property, and E any property. The game $G(S, E)$ is played by two players called *Alter* and *Ego*. The state of a play is a finite run of S. At every move, one player extends the current run by a finite, possibly empty, sequence. Alter has the first move. The two players move alternately. The play goes on forever, converging to a finite run α or an infinite run x in S. Ego wins if $x \in E$ (resp. $\alpha\uparrow \cap S \subseteq E$), otherwise Alter wins.

Definition 5.1 (*Banach-Mazur Game*). Let S be a safety property, and E any temporal property. A *play* of the game $G(S, E)$ is an infinite sequence of finite runs $(\alpha_i)_{i\in\mathbb{N}}$ of

S such that $\alpha_0 = \epsilon$ and $\alpha_i \sqsubseteq \alpha_{i+1}$ for each $i \geq 0$. Given a play $(\alpha_i)_{i\in\mathbb{N}}$, we say that *Ego wins* if $(\sup_i \alpha_i)\uparrow \cap S \subseteq E$. Otherwise, *Alter wins*.

A *partial play* is a finite prefix $(\alpha_i)_{i\leq n}$ of some play. The set of partial plays on S is denoted as PL_S. A *strategy* in S is a mapping $f : PL_S \to \Sigma^* \cap S$ such that if $\alpha = f(\alpha_0, \ldots, \alpha_i)$, then $\alpha_i \sqsubseteq \alpha$. We say that *Ego plays* f in a play $(\alpha_i)_{i\in\mathbb{N}}$ if for every $j \geq 0$, $f(\alpha_0, \ldots, \alpha_{2j+1}) = \alpha_{2j+2}$. Likewise, we say that *Alter plays* f in the play $(\alpha_i)_{i\in\mathbb{N}}$ if for every $j \geq 0$, $f(\alpha_0, \ldots, \alpha_{2j}) = \alpha_{2j+1}$. A strategy f is *winning* for Ego (Alter) in $G(S, E)$ if Ego (Alter) wins each play where he (she) plays f.

The game $G(S, E)$, henceforth called the *Banach-Mazur game*,[4] defines an intermediate version of nondeterminism between *daemonic* and *angelic* nondeterminism.

Suppose that the correctness of a system is specified by a temporal property E. Saying that nondeterminism is *daemonic* means that we define a system M to be correct if each run of M satisfies E. This corresponds to a game in which Alter chooses an arbitrary, possibly infinite run in S—Ego, who wants to prove correctness, is guaranteed to win only if every run of the system S is in E. Saying that nondeterminism is *angelic* means that we define a system M to be correct if there is a run of M that satisfies E. This corresponds to a game in which Ego chooses the entire run. Then, Ego has a winning strategy only if $S \cap E \neq \emptyset$. In the Banach-Mazur game, the nondeterminism is resolved alternately between Alter and Ego. In the following, we will prove that Ego has a winning strategy in the Banach-Mazur game $G(S, E)$ if and only if E is a fairness property for S.

The definition of strategy we have given is the most general one: players play remembering the full history of the play. As long as we are interested only in knowing whether there is a winning strategy for one of the players, we can use a simpler notion of strategy that does not decrease the power of the players. In this simplified version, players only know the current state of the play, but not the moves that led to it.

Definition 5.2. A strategy f in S is *decomposition invariant* [Grädel 2008] if for any $\alpha_0, \ldots, \alpha_i$ and $\beta_0, \ldots, \beta_j$, we have that $\alpha_i = \beta_j$ implies $f(\alpha_0, \ldots, \alpha_i) = f(\beta_0, \ldots, \beta_j)$.

We denote a decomposition-invariant strategy as a mapping $f : \Sigma^* \cap S \to \Sigma^* \cap S$ such that $\alpha \sqsubseteq f(\alpha)$ for all $\alpha \in \Sigma^* \cap S$.

PROPOSITION 5.3 ([GRÄDEL 2008]). *Given a Banach-Mazur game $G(S, E)$, Ego (Alter) has a winning strategy if and only if he (she) has a decomposition-invariant winning strategy.*

PROOF. Grädel [2008] gives a proof for a slightly different setting using topological arguments that we will introduce later. We could reproduce his proof for our setting using arguments from below. Instead we provide an alternative, more direct proof here.

Given a winning strategy f, we want to define a decomposition-invariant winning strategy g for the same game. To this end, we need to define $g(\alpha)$ for any finite run α. To apply f, we first need to decompose α into some partial play $\alpha_0, \ldots, \alpha_i$. We do this for Ego, the construction for Alter being essentially the same.

Let $\alpha_0 = \epsilon$. Define α_1 to be the smallest prefix of α such that $f(\alpha_0, \alpha_1)$ is compatible with α. Let $\alpha_2 = f(\alpha_0, \alpha_1)$. Recursively, define α_{2j+1} to be the smallest prefix of α such that $f(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{2j+1})$ is compatible with α. Define $\alpha_{2j+2} = f(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{2j+1})$. Let k be the first index for which $\alpha \sqsubseteq \alpha_{2k}$. Define $g(\alpha) = \alpha_{2k}$. To prove that g is a winning strategy, consider now a play $(\beta_i)_{i\in\mathbb{N}}$, where Ego plays g. This means that

[4]The naming will be explained in Section 8.6.

each β_{2j+1} is decomposed into $(\alpha_0^j, \ldots, \alpha_{2h_j+1}^j)$ and $\beta_{2j+2} = g(\beta_{2j+1}) = f(\alpha_0^j, \ldots, \alpha_{2h_j+1}^j)$. We claim that all such decompositions are "compatible" in the sense that for each $j < k$, $(\alpha_0^j, \ldots, \alpha_{2h_j+1}^j)$ is a prefix of $(\alpha_0^k, \ldots, \alpha_{2h_k+1}^k)$. It is sufficient to show this for $k = j+1$.

Let thus $(\alpha_0, \ldots, \alpha_{2l+1})$ be a decomposition of β_{2j+1} and $(\alpha'_0, \ldots, \alpha'_{2m+1})$ be a decomposition of β_{2j+3}. We show that for $i < 2l+1$, $\alpha_i = \alpha'_i$ by induction on i. By definition, $\alpha_0 = \alpha'_0 = \epsilon$. The prefix α_1 is defined as the smallest prefix such that $f(\alpha_0, \alpha_1)$ is compatible with β_{2j+1}.

If $f(\alpha_0, \alpha_1)$ is a strict prefix of β_{2j+1}, then $f(\alpha_0, \alpha_1)$ is compatible with β_{2j+3}. Moreover, α_1 is the shortest prefix such that $f(\alpha_0, \alpha_1)$ is compatible with β_{2j+3}. In fact, if there were a shorter one, call it $\hat{\alpha}$, then $f(\alpha_0, \hat{\alpha})$ would be also compatible with β_{2j+1}, thus contradicting the definiton of α_1 . Thus, $\alpha_1 = \alpha'_1$.

If $\beta_{2j+1} \sqsubseteq f(\alpha_0, \alpha_1)$, then $\beta_{2j+2} = g(\beta_{2j+1}) = f(\alpha_0, \alpha_1)$. Thus, $f(\alpha_0, \alpha_1)$ is compatible with β_{2j+3}, and again $\alpha_1 = \alpha'_1$. As $\alpha_0 = \alpha'_0$ and $\alpha_1 = \alpha'_1$, $\alpha_2 = f(\alpha_0, \alpha_1) = f(\alpha'_0, \alpha'_1) = \alpha'_2$. The inductive step is analogous, for both even and odd indices.

The limit of all the decompositions is a play $(\alpha_h)_{h\in\mathbb{N}}$ where Ego plays f, and therefore he wins. But $\sup_i \beta_i = \sup_j \beta_{2j+1} = \sup_j \alpha_{2h_j+1}^j = \sup_h \alpha_h$, and this shows that g is also a winning strategy. □

In the following, we will only consider decomposition-invariant strategies, but for brevity not mention it explicitly. We will now give a simplified characterization of the games in which Ego has a winning strategy. To this end, we will use the following definition:

Definition 5.4. We consider the game $G(S, E)$ and a strategy f in S. A run $x \in S$ is *f-compliant* (for Ego) if x is the result of a play in which Ego plays f. The set of all f-compliant runs is denoted by R_f.

Hence, a strategy f is winning for Ego iff $R_f \subseteq E$. We provide an alternative, easier characterization of compliant runs:

PROPOSITION 5.5. *Let f be a strategy in S. A run $x \in S$ is f-compliant iff for each position i of x, there exists a position $j \geq i$ of x such that $f(x_j) \sqsubseteq x$.*

PROOF. Trivially f-compliant runs satisfy the condition. Consider now a run x that satisfies the condition. In other words, for every prefix α of x, there exists a prefix β, such that $\alpha \sqsubseteq \beta$ and $f(\beta) \sqsubseteq x$. Also if $\alpha \neq x$, we can take β to be a proper extension of α. Let $h(\alpha)$ be one of such β, say, the shortest. Consider the play $(\alpha_n)_{n\in\mathbb{N}}$ defined as follows:

— $\alpha_{2h+1} = h(\alpha_{2h})$,
— $\alpha_{2h+2} = f(\alpha_{2h+1})$.

Clearly, the limit of the play is x, and this shows that x is f-compliant. □

A second, simpler characterization for infinite runs is the following:

PROPOSITION 5.6. *Let $x \in S$ be an infinite run and f a strategy. Then x is f-compliant iff for infinitely many i, x_i belongs to the image of f.*

PROOF. As previously mentioned, f-compliant runs satisfy the condition trivially. Consider now a run x that has infinitely many prefixes belonging to the image of f. We show that x satisfies the condition of Proposition 5.5. For any position i, consider the set $H = \{f(x_h) \mid h \leq i\}$. Take j to be the smallest position such that $f(x_j) \sqsubseteq x$ and $f(x_j) \notin H$. Such j must exists because H is finite, and clearly $j > i$. □

We now arrive at the final simplification of the notion of strategy.

Definition 5.7. A strategy f is *progressive* if $f(\alpha) = \alpha \Rightarrow \alpha \in \max(S)$

Note that a strategy f is progressive if and only if $R_f \subseteq \max(S)$. As Alter can always enforce the result of the play to be a maximal run of S, it is not restrictive to require that Ego plays progressively. More precisely:

LEMMA 5.8. *Ego has a winning strategy in $G(S, E)$ iff he has a progressive winning strategy in $G(S, E \cap \max(S))$.*

PROOF. Let f be a winning strategy for Ego in $G(S, E)$. Define f' to be a strategy such that $f'(\alpha) = f(\alpha)$ if $f(\alpha) \in \max(S)$ and otherwise $f'(\alpha) = f(\alpha)s$ for some state s such that $f(\alpha)s \in S$; f' is clearly progressive. Now consider a run $x \in R_{f'}$. If it is finite, it is maximal and then $x \in R_f$. If it is infinite, there are infinitely many indices j such that $f'(x_j) \sqsubseteq x$. But since $f'(\alpha) \sqsubseteq f(\alpha)$, for the same indices, $f(x_j) \sqsubseteq x$, and $x \in R_f$.

Thus, we have $R_{f'} \subseteq R_f$, and hence if f is winning for Ego, f' must also be winning for Ego. The converse is trivial. □

5.2. The Game-Theoretic Characterization of Fairness

We are now ready to state and prove the main result of the section.

THEOREM 5.9. *Ego has a winning strategy in $G(S, E)$ iff E is a fairness property for S.*

PROOF. ($\Leftarrow$) Suppose $\mathrm{F}_S(Q) \subseteq E$. Define a strategy f by $f(\alpha) = \beta$ where $\alpha \sqsubset \beta \in Q \cap S$ if there exists such a β and $f(\alpha) = \alpha$ otherwise. We have $R_f \subseteq \mathrm{F}_S(Q) \subseteq E$, hence, f is a winning strategy for Ego in $G(S, E)$.

($\Rightarrow$) Let f be a progressive winning strategy for Ego in $G(S, E)$. Define $Q = f(\Sigma^*)$. Let $x \in \mathrm{F}_S(Q)$. We want to show that $x \in E$. If $x = \alpha$ is a finite maximal run of S, then $f(\alpha) = \alpha$ and $\alpha \in R_f$. By definition of a progressive strategy, any other finite run has a proper extension in Q and thus it cannot be in $\mathrm{F}_S(Q)$. If x is infinite, since any finite prefix $\alpha \sqsubseteq x$ can be properly extended to Q, there must be infinitely many i such that $x_i \in Q$. By Proposition 5.6, we obtain $x \in R_f$. From $R_f \subseteq E$ follows $x \in E$. □

The intuition behind this game-theoretic characterization of fairness is that, while fairness restricts the allowed behavior, it should not restrict it too much. Ego, who wants to produce a fair run, can enforce some (live) choice to be taken infinitely often but he cannot prevent other choices being taken infinitely often (by Alter).

Example 5.10. Consider $S = \Sigma^\infty$ for this paragraph. Then, Σ^ω is a fairness property in S, whereas Σ^* is a liveness but not a fairness property in S because Alter can enforce the outcome of the play to be infinite. Similarly, for any sequence x, the property $\{\alpha x \mid \alpha \in \Sigma^*\}$ is a liveness property but not a fairness property in S. The property $\Box\Diamond\Phi$ is a fairness property whereas $\Diamond\Box\Phi$ is a liveness but not a fairness property—for any *nontrivial* state property Φ, that is, $\varnothing \neq \mathrm{sat}(\Phi) \neq \Sigma$. Hence, the property E_M in Section 1 is not a fairness property in general.

More examples for fairness properties in $S = \Sigma^\infty$ are $\Box(\Phi \Rightarrow \Diamond\Psi)$, $\Diamond\Box\Phi \Rightarrow \Box\Diamond\Psi$, and $\Box\Diamond\Phi \Rightarrow \Box\Diamond\Psi$.

Call a run *periodic* if it is of the form $\alpha\beta^\omega$ for $\alpha, \beta \in \Sigma^*$ and *aperiodic* otherwise. The set of aperiodic runs is a fairness property, whereas the set of periodic runs is a liveness but not a fairness property; f defined by $f(\alpha) = \alpha s^k r$, where $k = |\alpha|, s, r \in \Sigma, s \neq r$ is a winning strategy for Alter with respect to aperiodic runs.

It is clear that at most one of the two players has a winning strategy in a given Banach-Mazur game. In the examples, we have shown that Ego does not have a winning strategy by showing that Alter has a winning strategy. A property E such that either Ego or Alter has a winning strategy in $G(S, E)$ is called *determinate* with respect to S. Hence, for a given determinate property E, we have a complete proof strategy for showing whether E is a fairness property or not—either we display a winning strategy for Ego or one for Alter.

The family of determinate properties is quite large. It includes all *Borel properties* [Oxtoby 1971, Thms. 4.3 and 6.3], which will be defined and explained later in Section 8.3. It can be argued that we are usually not interested in properties that are not determinate. In fact, indeterminate properties do exist, but to prove their existence, one needs to invoke the axiom of choice [Oxtoby 1971, Ch. 6]. For our purposes, it shall suffice to state that each ω-regular property is a Borel property (see Thomas [1990]) and hence determinate.

6. PROPERTIES OF FAIRNESS PROPERTIES

In Section 1, we discussed three requirements for a general definition of fairness. We required popular notions of fairness to be covered by our definition. Furthermore, each fairness property should be machined-closed with respect to the system and the class of all fairness properties should be closed under countable intersection. By help of the game-theoretic characterization, we can now prove that the latter two requirements are met by our definition of fairness.

PROPOSITION 6.1. *Let S be a safety property and F a fairness property in S. Then, (S, F) is machine-closed.*

PROOF. Let $\alpha \in S \cap \Sigma^*$. We have to show that there exists a run x such that $\alpha \sqsubseteq x \in S \cap F$, which is clear because Ego has a winning strategy in the game $G(S, F)$, in particular for those plays in which Alter starts with move α. □

PROPOSITION 6.2. *Let S be a safety property and F_i fairness properties in S for each $i \in \mathbb{N}$. Then $\bigcap_i F_i$ is a fairness property in S.*

PROOF. Let f_i be a progressive winning strategy for Ego in $G(S, F_i)$ for each $i \in \mathbb{N}$. Define for $\alpha \in \Sigma^k$, $f(\alpha) = f_k(f_{k-1}(\cdots f_0(\alpha)\cdots))$. It is straightforward to verify that any f-compliant run is f_i-compliant for every $i \in \mathbb{N}$, and therefore f is a winning strategy for Ego with respect to $\bigcap_{i\in\mathbb{N}} F_i$. □

Example 6.3. Let F_k, $k \in \mathbb{N}$ be strong k-fairness with respect to some action of a system as defined in Section 3.4 and let $F = \bigcap_{k\in\mathbb{N}} F_k$. F is a fairness property that in general is clearly strictly stronger than any F_k but strictly weaker than strong ∞-fairness as was shown in Section 3.5.

Proposition 6.2 cannot be generalized to arbitrary intersections: for any $x \in S = \{p, q\}^\infty$, let $F_x = S \setminus \{x\}$. Clearly F_x is a fairness property, but $\bigcap_{x\in S} F_x$ is empty. An interesting subclass of fairness properties that forms a complete lattice is discussed elsewhere [Völzer et al. 2005].

We have already argued in Section 5.2 that the third requirement—that most popular fairness notions produce fairness properties—is also satisfied by our definition. While checking several other fairness notions in the literature, we either proved that the notion falls into the class we have defined or violates already the first requirement (machine closure). An example of this is *unconditional fairness*, which prescribes a particular action to be taken infinitely often regardless of the choices the system provides. The literature contains an extensive discussion why those properties should not

be considered fairness properties (cf. Apt et al. [1988] and Lamport [2000]). Another such example is *bounded fairness*, which requires that an action has to be taken within some fixed time after it has been enabled. More precisely, a run x is *k-bounded-fair* for $k \in \mathbb{N}$ if the following is true for each position i of x: If A is enabled at i then A is taken at some position j of x such that $i \leq j \leq i + k$. It is easy to see that k-bounded fairness is a safety property and therefore not a liveness property in general in a given system.

The notion of *finitary fairness* [Alur and Henzinger 1994] is an exception in our survey of "fairness" notions found in the literature: A run x is *finitary-fair* with respect to an action A if there exists a $k \in \mathbb{N}$ such that x is k-bounded-fair with respect to A. Finitary fairness is, in contrast to k-bounded fairness, a liveness property (i.e., machine-closed) in a given system. However, it is not a fairness property in general. For instance consider $S = \{p, q\}^\infty$, and finitary fairness with respect to the transition (p, q). A winning strategy for Alter is defined by $f(\alpha) = \alpha s^k$, where $k = |\alpha|$ and $s \in \{p, q\}$ is the last state of α. Note that for the system in Figure 6, no run is finitary-fair with respect to all transitions, that is, the intersection of the properties finitary fairness with respect to a_i and finitary fairness with respect to b_i for $i \in \mathbb{N}$ is empty.

However, given an action A, consider the following property $F_k(A)$: If A is infinitely often enabled, then A must be taken infinitely often within k steps. It is not difficult to verify that $F_k(A)$ is a fairness property.

This leads to the question whether we could have defined fairness in a different way and still satisfy our requirements. In particular: could have we defined fairness in a more liberal way, that is, as a larger family of properties? Again, thanks to the game-theoretic characterization, we can answer negatively to this question. Indeed we will now show that we cannot enlarge the class of fairness properties without giving up the first or the second requirement. We do not have a proof for this statement in full generality, but we can prove it if we restrict it to determinate properties. As argued above, this can be considered as a mild restriction.

THEOREM 6.4. *Let S be a safety property. The family $\mathcal{F}_S = \{F \mid F$ is a fairness property in $S\}$ is a maximal family of determinate properties with respect to S such that*

(1) $F \in \mathcal{F}_S$ implies (S, F) is machine-closed and
(2) $F, F' \in \mathcal{F}_S$ implies $F \cap F' \in \mathcal{F}_S$.

PROOF. Suppose by contradiction that $\mathcal{F}_S$ is not maximal, and consider a strictly larger familiy $\mathcal{F}'$ of determinate properties that satisfies (1) and (2). Take $E \in \mathcal{F}' \setminus \mathcal{F}_S$. Since $E \notin \mathcal{F}_S$, Ego has no winning strategy in $G(S, E)$, but since E is determinate, Alter has a winning strategy f in that game. Let $\alpha = f(\epsilon)$ be its first move. Consider the property

$$F = \neg E \cup \bigcup_{\beta \text{ is incompatible with } \alpha} \beta\uparrow,$$

where $\neg E$ denotes $S \setminus E$.

Ego has a winning strategy in the game $G(S, F)$, defined as follows: If the play is in a state that is compatible with α, then Ego can use f to guarantee $\neg E$. Otherwise, the play is in a state β that is incompatible with α, in which Ego does not have to do anything to win. Thus, $F \in \mathcal{F}_S \subseteq \mathcal{F}'$. Since $\mathcal{F}'$ satisfies (2), we have that $E \cap F \in \mathcal{F}'$. But by definition of F, α has no extension into $S \cap E \cap F$. Hence, $(S, E \cap F)$ is not machine-closed, contradicting (1). □

7. FAIRNESS AND THE SAFETY-PROGRESS HIERARCHY

With the *safety-progress classification*, Manna and Pnueli [1990] gave a classification of temporal properties that is in some sense orthogonal to the safety-liveness classification. Whereas safety and liveness define a partition of all temporal properties (safety properties, liveness properties, and those that are neither safety nor liveness), the members of the safety-progress classification form a hierarchy. Manna and Pnueli [1990] presented a language-theoretic, a topological, a temporal-logical and an automata-theoretic view of their hierarchy. In this section, we study the relationship of fairness properties with the safety-progress hierarchy in the language-theoretic view. In this way, we complement our insights into which properties are fairness properties.

7.1. The Safety-Progress Hierarchy

Manna and Pnueli [1990] define four operators that construct temporal properties from finitary properties. While they consider only infinitary properties as temporal properties, we generalize their operators here to our setting in a natural way. Let Q be a finitary property. Define

$$\mathrm{A}(Q) = \{x \mid \forall \alpha \sqsubseteq x : \alpha \in Q\} \tag{1}$$

$$\mathrm{E}(Q) = \{x \mid \exists \alpha \sqsubseteq x : \alpha \in Q\} \tag{2}$$

$$\mathrm{R}(Q) = \{x \mid \forall \alpha \sqsubseteq x : \exists \beta : \alpha \sqsubseteq \beta \sqsubseteq x \wedge \beta \in Q\} \tag{3}$$

$$\mathrm{P}(Q) = \{x \mid \exists \alpha \sqsubseteq x : \forall \beta : \alpha \sqsubseteq \beta \sqsubseteq x \Rightarrow \beta \in Q\}. \tag{4}$$

Properties of the form $\mathrm{A}(Q)$ are exactly the safety properties. Properties of the form $\mathrm{E}(Q)$, $\mathrm{R}(Q)$, and $\mathrm{P}(Q)$ are called *guarantee*, *recurrence*, and *persistence properties*, respectively.

We have the following dualities:

$$\neg\mathrm{A}(Q) = \mathrm{E}(\neg Q) \text{ and } \neg\mathrm{E}(Q) = \mathrm{A}(\neg Q) \tag{5}$$

$$\neg\mathrm{R}(Q) = \mathrm{P}(\neg Q) \text{ and } \neg\mathrm{P}(Q) = \mathrm{R}(\neg Q), \tag{6}$$

where $\neg X$ denotes the complement of X with respect to the appropriate universe. As $\mathrm{A}(Q) = \mathrm{R}(\mathrm{A}(Q) \cap \Sigma^*)$ and $\mathrm{E}(Q) = \mathrm{R}(\mathrm{E}(Q) \cap \Sigma^*)$, we have that each safety property and each guarantee property is also a recurrence property. Similarly, each safety and each guarantee property is also a persistence property.

Example 7.1. Let Φ be a state property. Then $\mathrm{sat}(\Box\Phi)$, $\mathrm{sat}(\Diamond\Phi)$, $\mathrm{sat}(\Box\Diamond\Phi)$ and $\mathrm{sat}(\Diamond\Box\Phi)$ are examples of safety, guarantee, recurrence and persistence properties, respectively.

7.2. Liveness and the Safety-Progress Hierarchy

We know already that Σ^∞ is the only property that is a safety as well as a liveness property. More generally, a safety property is a liveness property relative to another safety property S if and only if it contains S. The following proposition also clarifies when a guarantee, recurrence or persistence property is a liveness property (relative to a given safety property S).

PROPOSITION 7.2. *Let Q be a finitary property and S a safety property.*

(1) $\mathrm{A}(Q)$ *is a liveness property in S iff* $\Sigma^* \cap S \subseteq Q$.
(2) $\mathrm{E}(Q)$ *is a liveness property in S iff Q is a* pseudoliveness property in *S, where E is a* pseudo-liveness property in *S if for each $\alpha \in \Sigma^* \cap S$ there exists an $x \in E \cap S$ that is compatible with α.*

(3) $\mathrm{R}(Q)$ *is a liveness property in* S *iff* Q *is a liveness property in* S.
(4) $\mathrm{P}(Q)$ *is a liveness property in* S *iff* Q *is a liveness property in* S.

PROOF. All claims are proved by a straightforward application of the definitions. □

7.3. Fairness and the Safety-Progress Hierarchy

Which properties in the safety-progress hierarchy are fairness properties? We know already that a property is a fairness property in S only if it is a liveness property in S. We now show that each live guarantee as well as each live recurrence property is a fairness property. To do this, we use special classes of strategies.

Definition 7.3. Let S be a safety property, and f be a strategy in S. We say that f is *idempotent* if $f(f(\alpha)) = f(\alpha)$ for all $\alpha \in S \cup \Sigma^*$. We say that f is *stable* if $f(\alpha) \sqsubseteq \beta \Rightarrow f(\beta) = \beta$ for all $\alpha, \beta \in S \cup \Sigma^*$.

Clearly, each stable strategy is idempotent.

PROPOSITION 7.4. *Let* S *be a safety property.*

(1) *A subset of* S *is a live guarantee property if and only if it is the set of* f*-compliant runs of some stable strategy* f *in* S.
(2) *A subset of* S *is a live recurrence property if and only if it is the set of* f*-compliant runs of some idempotent strategy* f *in* S.

PROOF.

(1) To prove one direction, let Q be a finitary pseudoliveness property (cf. Proposition 7.2), define f such that $f(\alpha) = \alpha$ if $\alpha \in \mathrm{E}(Q)$ and let otherwise $f(\alpha)$ be any extension of α into Q; f is then stable and $R_f = \mathrm{E}(Q)$. For the other direction, given a stable strategy f, we have that $f(\Sigma^*)$ is a pseudoliveness (it actually is a liveness property) and $R_f = \mathrm{E}(f(\Sigma^*))$.
(2) For a given finitary liveness property Q, define f such that $f(\alpha) = \alpha$ if $\alpha \in Q$ and let otherwise $f(\alpha)$ be any extension of α into Q; f is then idempotent and $R_f = \mathrm{R}(Q)$. For a given idempotent f, $f(\Sigma^*)$ is a liveness property and $R_f = \mathrm{R}(f(\Sigma^*))$. □

It follows from Proposition 7.4 that each property that contains a live guarantee property or a live recurrence property is a fairness property. We show now that live persistence properties are not fairness properties in general.

PROPOSITION 7.5. *Let* S *be a safety property. A persistence property* P *is a fairness property in* S *if and only if there exists a guarantee property* $\mathrm{E}(Q)$ *that is live in* S *such that* $\mathrm{E}(Q) \cap S \subseteq P$.

PROOF.
($\Leftarrow$) is clear from Proposition 7.4.
For ($\Rightarrow$), let f be a winning strategy for $\mathrm{P}(Q)$ in S and let $\alpha \in \Sigma^*$. Let $\alpha_0 = \alpha$ and let α_{i+1}, for each $i \in \mathbb{N}$, be any extension of $f(\alpha_i)$ into $S \cap \neg Q$, provided that such an extension exists. If such an extension exists for each $i \in \mathbb{N}$, we obtain a run $x = \sup_{i \in \mathbb{N}} \alpha_i$ where $x \in \mathrm{R}(\neg Q)$ and hence $x \notin \mathrm{P}(Q)$. However, $x \in R_f$, which contradicts f being a winning strategy for $\mathrm{P}(Q)$. Therefore, there is an $i \in \mathbb{N}$ such that $\beta_\alpha := f(\alpha_i)$ has no extension into $S \cap \neg Q$, hence all extensions of β_α in S satisfy Q. Define $Q' = \{\beta_\alpha \mid \alpha \in S \cap \Sigma^*\}$; Q' is clearly live in S. Furthermore, we have $\mathrm{E}(Q') \cap S \subseteq \mathrm{P}(Q)$. □

We have shown in Proposition 7.4 that each property that contains a live recurrence property is a fairness property. The converse does not hold. (As a counterexample

consider $S = \Sigma^\infty$ and $X = \Sigma^\omega$. X contains no recurrence property because it contains no finite runs.) However, we can give a characterization of fairness in terms of recurrence properties.

PROPOSITION 7.6. *A property F is a fairness property in S iff there exists a finitary property Q that is live in S such that* $\mathrm{R}(Q) \cap \max(S) \subseteq F$.

PROOF.
($\Leftarrow$) is due to Lemma 5.8.
For ($\Rightarrow$), let f be a winning strategy for Ego in $G(S, F)$. Let $Q = f(S \cap \Sigma^*)$. We have $\mathrm{R}(Q) \cap \max(S) \subseteq R_f \subseteq F$. □

8. A TOPOLOGICAL CHARACTERIZATION OF FAIRNESS

This section presents a topological characterization of fairness. It turns out that fairness properties are exactly the sets that are *large* in a topological sense, that is, they are the *co-meager* sets in the natural topology of runs of the system. This insight will provide us with an important link to probability theory, where a set is large if it has measure 1. We will explore that link in Section 9.

Furthermore, the topological characterization liberates us from our concrete choice of semantical domain, that is, sequences of states, as other semantic domains are equipped with a natural topology, which then immediately provides a notion of fairness.

Of course, the topological characterization potentially gives us access to a large body of results in topology. This is even more interesting as other important concepts such as safety, liveness, guarantee, persistence and recurrence were given topological characterizations.

Last but not least, the topological characterization will provide us additional confidence that we have found a natural definition of fairness.

In Section 8.1, we will briefly introduce the use of topology in our context, which is based on a presentation by Smyth [1992]. In Section 8.2, we recall the observation, made by Alpern and Schneider [1985], that safety properties correspond to *closed* sets, whereas liveness properties correspond to *dense* sets. In Section 8.3, we discuss some important topological notions that constitute the *Borel Hierarchy*. In Section 8.4, we discuss the topological notion of "largeness". In Section 8.5, we introduce the Scott topology on systems. Finally, in Section 8.6, we show that fairness properties correspond to large sets in the Scott topology. For a classic introduction to topology, see Dugundji [1966].

8.1. Observable Properties

Given an observer of a system who can see the entire state and its evolution, what temporal properties are observable? By this we shall mean that the observer can detect the presence of the property in finite time. Therefore, a temporal property E is *observable* iff

$$x \in E \Rightarrow \exists \alpha \sqsubseteq x : \alpha\uparrow \subseteq E.$$

The observation of the finite prefix α *guarantees* that the observed run satisfies E. In fact, it is easy to see that a property is observable if and only if it is a guarantee property $\mathrm{E}(Q)$ as defined in Section 7.1. We may think of the observer as having a (possibly infinite) set Q of finite runs, which she uses to detect the property $E = \mathrm{E}(Q)$. Note that the operator $\mathrm{E}(\cdot)$ defines a bijection between observable and finitary properties.

Note that we only require the presence of an observable property to be detectable, but not its absence. In fact, for no nontrivial property E (i.e., $\varnothing \neq E \neq \Sigma^\infty$) it is the

case that E and $\neg E$ are both observable. (Then, the empty run would belong to one of the two, which implies that both are trivial.)

Observable properties have two important closure properties.

(1) The intersection of finitely many observable properties is observable.
(2) The union of arbitrarily many observable properties is observable.

To see this, note that an observable property can be decomposed into *cones*, that is, properties of the form $\alpha\uparrow, \alpha \in \Sigma^*$:

$$\mathrm{E}(Q) = \bigcup_{\alpha \in Q} \alpha\uparrow.$$

Closure under union follows immediately. Closure under finite intersection follows from the fact that

$$\alpha\uparrow \cap \beta\uparrow = \sup(\alpha, \beta)\uparrow$$

if α and β are compatible and $\alpha\uparrow \cap \beta\uparrow = \varnothing$ otherwise.

These two closure properties say that the family of observable properties is a *topology* on Σ^∞, that is, a *topology* on a nonempty set Ω is defined to be a family $\mathcal{T} \subseteq 2^\Omega$ that is closed under union and finite intersection. This implicitly requires $\Omega, \varnothing \in \mathcal{T}$. The pair $(\Omega, \mathcal{T})$ is called a *topological space*. A member of $\mathcal{T}$ is called an *open set*. Hence, observable properties are the open sets of our topology, which is called the *Scott topology* on Σ^∞.

A *base* of a topology $\mathcal{T}$ is a family $\mathcal{B} \subseteq \mathcal{T}$ such that each open set is the union of members of $\mathcal{B}$. Hence, the family

$$\mathcal{B} = \{\alpha\uparrow \mid \alpha \in \Sigma^*\}$$

is a base of the Scott topology on Σ^∞. A member of $\mathcal{B}$ is called a *basic open set*.

A set X is called a *neighborhood* of x if $x \in G \subseteq X$ for some open set G. Hence, a neighborhood of a run x is a property E such that some finite observation of it guarantees E.

8.2. Safety and Liveness Properties

As noted in Section 7.1, the complement of a guarantee property is a safety property. The complement of an open set of a topology is called a *closed* set. Thus safety properties are the closed sets of the Scott topology. By duality, safety properties are closed under arbitrary intersection and finite union. The *closure* of a set X, denoted $\overline{X}$, is the smallest closed set that contains X. For the Scott topology, we will call $\overline{E}$ the *safety closure* of the property E. We have

$$\overline{E} = \mathrm{A}(\{\alpha \mid \alpha \text{ is a finite prefix of some } x \in E\}).$$

For a safety property, the absence of the property is detectable. The safety closure of a set E can be viewed as the smallest tree that contains all runs of E.

Liveness properties are exactly the *dense* sets of the Scott topology: Recall that a set X is *dense* if it intersects every nonempty open set, or equivalently, every nonempty basic open set, that is, a property E is dense in the Scott topology iff for each finite run α,

$$E \cap \alpha\uparrow \neq \varnothing,$$

that is, precisely iff E is a liveness property. Equivalently, X is dense iff $\overline{X} = \Omega$, that is, E is a liveness property iff $\overline{E} = \Sigma^\infty$.

For a property E, we define its *liveness extension* $\mathrm{L}(E)$ by

$$\mathrm{L}(E) = E \cup \bigcup_{\alpha \in \Sigma^*, \alpha\uparrow \cap E = \varnothing} \alpha\uparrow.$$

Clearly, $\mathrm{L}(E)$ is a liveness property for any E.

The correspondence of safety and liveness to closed and dense sets was pointed out by Alpern and Schneider [1985]. As each set can be written as the intersection of a closed and a dense set, each temporal property can be written as the intersection of a safety and a liveness property. We have, for any temporal property E,

$$E = \overline{E} \cap \mathrm{L}(E).$$

8.3. The Borel Hierarchy

Guarantee properties are not closed under countable intersection. For example, we have

$$\bigcap_{k \in \mathbb{N}} \mathrm{E}(\Sigma^k) = \Sigma^\omega,$$

and Σ^ω is clearly not a guarantee property. By duality, safety properties are not closed under countable union. A set that can be written as the intersection of countably many open sets is called a G_δ *set*; a set that can be written as the union of countably many closed sets is called an F_σ *set*. More generally, let G denote the family of open sets and F the family of closed sets and define for a family $\mathcal{F} \subseteq 2^\Omega$,

$$\mathcal{F}_\delta = \left\{ \bigcap_{i \in \mathbb{N}} X_i \mid X_i \in \mathcal{F} \text{ for all } i \right\}$$

and

$$\mathcal{F}_\sigma = \left\{ \bigcup_{i \in \mathbb{N}} X_i \mid X_i \in \mathcal{F} \text{ for all } i \right\}.$$

Thus, for example $\mathrm{G}_{\delta\sigma}$ denotes the family of all sets that can be written as the countable union of G_δ sets. The families defined in that way form an infinite hierarchy, called the *Borel hierarchy*. The union of all families of the Borel hierarchy is called *Borel σ-field* (with respect to the Scott topology on Σ^∞). It is the smallest family of sets that contains the open sets and is closed under complementation and countable union. A member of the Borel σ-field is called a *Borel set*.

It is worth recalling that ω-regular properties belong to both $G_{\delta\sigma}$ and $F_{\sigma\delta}$ [Thomas 1990]. LTL-expressible properties belong to the same level of the Borel hierarchy [Manna and Pnueli 1990].

We will mainly be interested in G_δ sets. Previously, the property Σ^ω was shown to be a G_δ property. To see more examples, define for $k \in \mathbb{N} \cup \{\omega\}$ and a finitary property Q:

$$R^k(Q) = \{x \mid |\{i \mid x_i \in Q\}| \geq k\}.$$

Clearly, for $k \in \mathbb{N}$, $R^k(Q)$ is a guarantee property. For $k = \omega$, we observe

$$R^\omega(Q) = \bigcap_{k \in \mathbb{N}} R^k(Q).$$

Thus, $R^\omega(Q)$ is a G_δ set. Also, each guarantee property is a G_δ set, and hence the union $R^\omega(Q) \cup \mathrm{E}(Q')$ is a G_δ set.

8.4. Topologically Large Sets

As announced, we will prove that fairness properties with respect to a safety property S are the "large sets" in a topological sense. This means that *most* runs of S are fair.

In a topological space, we say that a set E is *somewhere dense* if there exists an open set G such that E intersects every nonempty open subset of G. A set is *nowhere dense* if it is not somewhere dense, or equivalently, if its closure does not contain any nonempty open set—or again equivalently, if its complement contains a dense open set [Dugundji 1966].

For an intuition on nowhere dense sets, imagine D to be a set of "dirty" points. If D is a dense set, then it pollutes the whole topological space: wherever we go in the topological space, we will have some dirty point in the neighborhood. If D is a somewhere dense set, then it pollutes part of the space. There are regions in which you will be always near a dirty point, but possibly also clean neighborhoods. Finally, if D is nowhere dense, then every clean point lives in a clean neighborhood. Intuitively, a nowhere dense set is small because the remainder of the topological space can stay clear of it. In this geometric sense, it can be thought of as a set that is full of holes.

A set is *meager* (or of *first category*), if it is the countable union of nowhere dense sets. Topologically, a countable union of small sets is still small. This was observed by René-Louis Baire, who proved that the unit interval of the real line cannot be obtained as the countable union of nowhere dense sets. This result can be thought of as a generalization of Cantor's theorem, which states that the unit interval is not obtained as the countable union of points [Oxtoby 1971].

The complement of a "small" set is therefore to be thought of as "large". The complement of a meager set is called *co-meager* (or *residual*).

In some topological spaces, co-meager sets can be equivalently characterized through G_δ sets. A topological space is called a *Baire space* if the intersection of countably many dense open sets is dense. In a Baire space, a set is a dense G_δ set if and only it can be written as the intersection of countably many dense open sets. Therefore, co-meager sets can equivalently be characterized as follows.

PROPOSITION 8.1. *In a Baire space, a set is co-meager if and only if it contains a dense* G_δ *set.*

PROOF. Straightforward, see Oxtoby [1971]. □

8.5. The Natural Topology of a System

If $\mathcal{T}$ is a topology on Ω and $Z \subseteq \Omega$ is a nonempty set, then the family $\mathcal{T}_Z = \{X \cap Z \mid X \in \mathcal{T}\}$ is also a topology, called the *relative topology* with respect to $\mathcal{T}$ and Z or $\mathcal{T}$ *relativized* to Z. Therefore, each system, or more generally each safety property S has a natural topology, viz. the Scott topology relativized to S, which is thus the family

$$\mathcal{T}_S = \{\mathrm{E}(Q) \cap S \mid Q \subseteq \Sigma^*\}.$$

The family $\mathcal{B} = \{\alpha\uparrow \cap S \mid \alpha \in \Sigma^*\}$ is a base for $\mathcal{T}_S$ and likewise we have: E is a member of a particular class of the Borel hierarchy generated by the Scott topology if and only if $E \cap S$ is a member of the same class of the Borel hierarchy generated by the Scott topology relativized to S.

A set $E \subseteq S$ is dense in the relative topology iff it is live with respect to S, that is, if (S, E) is machine-closed. However, if E is a liveness property (i.e., a dense set), then $E \cap S$ is not necessarily live with respect to S (a dense set in the relative topology)—and the converse is also not true in general: Consider $\Sigma = \{p, q\}$, $S = p^\omega\downarrow$ and $E = \mathrm{sat}(\Diamond q)$. E is a liveness property but not live with respect to S. Furthermore, $S = S \cap S$ is live with respect to S but not a liveness property.

PROPOSITION 8.2. *The Scott topology on Σ^∞ (relativized to some safety property S) is a Baire space.*

PROOF. Let $E = \bigcap_{i\in\mathbb{N}} \mathrm{E}(Q_i)\cap S$ such that Q_i is dense (i.e., live) in S and let $\alpha \in S\cap\Sigma^*$. As Q_0 is live in S, there exists α_0 such that $\alpha \sqsubseteq \alpha_0 \in S\cap Q_0$. Likewise, since Q_1 is live in S, there exists α_1 such that $\alpha_0 \sqsubseteq \alpha_1 \in S\cap Q_1$ and hence $\alpha_1 \in S\cap \mathrm{E}(Q_0)\cap \mathrm{E}(Q_1)$. Doing this for all $i \in \mathbb{N}$, we obtain $x = \sup_i \alpha_i \in S\cap\bigcap_{i\in\mathbb{N}} \mathrm{E}(Q_i)$. Therefore, E is dense (i.e., live) in S. □

It is essential that S be a safety property. The Scott topology relativized to Σ^* is not a Baire space. $\Sigma^{\geq k} = \{x \mid |x| \geq k\}$ is a dense open set for each k. The intersection is the empty set, which is not dense relative to Σ^*.

8.6. The Topological Characterization of Fairness

In this section, we show that fairness properties are precisely the co-meager sets. First, we give a topological characterization of ∞-fairness with respect to some Q.

THEOREM 8.3. *Given a safety property S and a property F, we have $F = \mathrm{F}_S(Q)$ for some finitary property Q (cf. Definition 4.1) if and only if F is a dense G_δ relative to S.*

PROOF.

($\Rightarrow$) Suppose $F = \mathrm{F}_S(Q)$ for some Q. We know it is dense; it remains to show that it is a G_δ set. The property $\mathrm{F}_S(Q)$ is defined to be the union of $R^\omega(Q)$, which was shown previously to be a G_δ set, and an open set: the set of all runs that cannot be extended into Q. An open set is also a G_δ set, and the union of two G_δ sets is a G_δ set.

($\Leftarrow$) If F is a dense G_δ set, it can be written as the intersection of dense open sets, that is, $F = \bigcap_{i\in\mathbb{N}} \mathrm{E}(Q_i) \cap S$, where each $\mathrm{E}(Q_i)$ is dense in S. Now, let $\min X$ denote the set of minimal elements of a set X in the prefix order. Without loss of generality, we can suppose the following:

(1) $Q_i = \min \mathrm{E}(Q_i)$. This is because $\mathrm{E}(Q_i) = \mathrm{E}(\min \mathrm{E}(Q_i))$ (the open sets are the upward closure of their minimal elements).
(2) $i < j \Rightarrow \mathrm{E}(Q_i) \supseteq \mathrm{E}(Q_j)$. This is because the finite intersection of open sets is an open set, and thus if for some $i < j$, we had $\mathrm{E}(Q_i) \not\supseteq \mathrm{E}(Q_j)$, we could take $Q'_j = \min \mathrm{E}(Q_i) \cap \mathrm{E}(Q_j)$.
(3) $Q_0 = \{\epsilon\}$ so that $\mathrm{E}(Q_0) = \Sigma^\omega$.

Define $Q = \bigcup_{i\in\mathbb{N}} Q_i$. We claim that $F = \mathrm{F}_S(Q)$. We prove the double inclusion.

First, let $x \in F$. Therefore, $x \in \mathrm{E}(Q_i)$ for each $i \in \mathbb{N}$. By assumption 1, for each i, there is exactly one element of Q_i that is a prefix of x. Either there are infinitely many such prefixes, and thus $x \in R^\omega(Q)$, or there are finitely many such prefixes. In the latter case, the longest such prefix, call it α (there is at least one by assumption 3), cannot be strictly extended into Q. To show this, let h be such that $\alpha \in Q_h$. Suppose that there is an α' that is strictly longer than α such that $\alpha' \in Q$. Let k be such that $\alpha' \in Q_k$. By assumption 1, $\alpha \notin Q_k$ and by assumption 2, $k > h$ and $\mathrm{E}(Q_h) \supset \mathrm{E}(Q_k)$, where the inclusion is strict. As $F = \bigcap_{i\in\mathbb{N}} \mathrm{E}(Q_i) \cap S$, there must be an element $\alpha'' \in Q_k$ such that α'' is a prefix of x. But as $\alpha \notin Q_k$ and $\mathrm{E}(Q_h) \supset \mathrm{E}(Q_k)$, α'' must be strictly longer than α, contradicting the fact that α is the longest prefix of x that is in Q. This shows that x has a prefix that cannot be extended into Q, and thus $x \in \mathrm{F}_S(Q)$.

For the other inclusion, let $x \in \mathrm{F}_S(Q)$. Suppose first $x \in R^\omega(Q)$. Therefore, for infinitely many i, $x \in \mathrm{E}(Q_i)$, and because of assumption 2, $x \in \mathrm{E}(Q_i)$ for all i.

Suppose now x has a prefix α that does not have a strict extension into Q. Because F is dense, there is an extension x' of α into F. As $x' \in \mathrm{E}(Q_i)$ for each i, there is an $\alpha_i \in Q_i$ that is a prefix of x'. As α_i is compatible with α and α has no strict extension

into Q, we have $\alpha_i \sqsubseteq \alpha$ for each $i \in \mathbb{N}$. Hence, $\alpha_i \sqsubseteq x$, and therefore $x \in \mathrm{E}(Q_i)$ and $x \in F$.[5] □

THEOREM 8.4. *A property F is a fairness property for S if and only if $F \cap S$ is co-meager in the Scott topology relativized to S.*

PROOF. By definition, F is a fairness property if and only if it contains some ∞-fairness property with respect to some Q. By Theorem 8.3, this is equivalent to containing a dense G_δ. And by Propositions 8.1 and 8.2, this is equivalent to being co-meager. □

Remark 8.5. The Banach-Mazur game first appeared in the *Scottish Book* [Mauldin 1981]—a notebook with an interesting history and contributions from now well-known mathematicians such as S. Banach, S. Mazur, S. Ulam, H. Steinhaus and others. Problem No. 43 in that book was posed by Stanisław Mazur. Given a nonempty set E of real numbers, Alter and Ego play the following game. Alter chooses a nonempty interval d_1, then Ego chooses a nonempty subinterval d_2 of d_1, then Alter chooses a subinterval d_3 of d_2, and so on. Alter wins if the intersection of the intervals $d_i, i \in \mathbb{N}$, intersects E, otherwise Ego wins. Mazur observed that Alter has a winning strategy if E is co-meager in some interval and Ego has a winning strategy if E is meager, and asked whether these conditions are also necessary for the existence of a winning strategy. This was affirmed by Stefan Banach, but no proof was ever published.

Oxtoby [1957] proved this theorem in a more general setting, for a generalization of the game in any complete metric space. Thus, essentially, the equivalence between co-meagerness and existence of a winning strategy for Ego was known. For an outline of the history and variants of the Banach-Mazur game, we refer to the survey by Telgársky [1987]. The Banach-Mazur game was recently studied as a special case of a *path game* by Berwanger et al. [2003] and Pistore and Vardi [2003]. We borrowed the names of the players from Berwanger et al. [2003].

Remark 8.6. If we restrict ourselves to infinitary temporal properties $E \subseteq \Sigma^\omega$, then the natural topology is the Scott topology relativized to Σ^ω, which is known as the *Cantor topology*. The Cantor topology is metrisable; a standard metric over Σ^ω is defined by

$$d(x, y) = \frac{1}{2^n},$$

where n is the length of the longest common prefix of x and y. The Cantor topology has therefore better separation properties than the Scott topology, which does not meet the separation axiom T_0 (cf. Dugundji [1966] and Smyth [1992]).

The fairness properties within Σ^ω are also the co-meager sets in a given safety property, and the Banach-Mazur game is also essentially the same because of Lemma 5.8. Recurrence properties and G_δ sets coincide in that setting [Manna and Pnueli 1990].

8.7. On the Necessity of Weakening

Kwiatkowska [1991] had proposed to define a fairness property for a system to be a dense G_δ set. However, strong fairness with respect to a particular transition is in general not a dense G_δ set, as we will now prove. By Theorem 8.3, this also proves then Proposition 4.5, for which we postponed the proof.

[5] A similar argument was used by Landweber [1969] to characterize the G_δ subsets of $\{0, 1\}^\omega$.

PROPOSITION 8.7. *Consider the complete system over two states* $S = \{p, q\}^\infty$. *Let* F *denote strong fairness with respect to action* $A = \{(p, p)\}$ *and let* F' *denote* F *intersected with maximality with respect to to all other transitions. Then* F *and* F' *are not* G_δ *sets.*

PROOF. Without maximality, the proof is easy: it is enough to observe that strong fairness by itself is not upward closed, whereas each G_δ set is. However, maximality is a basic implicit assumption for many authors, including Kwiatkowska [1991].

Suppose, by contradiction, that F' is a G_δ set. Then, there exist open sets $G_i, i \in \mathbb{N}$, such that $F' = \bigcap_{i\in\mathbb{N}} G_i$. Observe that we have, by definition of F',

$$pq^\omega \in F'$$

and hence $pq^\omega \in G_0$. As G_0 is open, there exists a $k_0 > 0$ such that

$$pq^{k_0}\uparrow \subseteq G_0.$$

Furthermore, we have

$$pq^{k_0} pq^\omega \in F',$$

and hence $pq^{k_0} pq^\omega \in G_0 \cap G_1$. As G_1 is open, there exists a $k_1 > 0$ such that

$$pq^{k_0} pq^{k_1}\uparrow \subseteq G_1,$$

and hence $pq^{k_0} pq^{k_1}\uparrow \subseteq G_0 \cap G_1$. We repeat the operation for all natural numbers, and obtain a sequence of finite runs that converges to an infinite run

$$x = pq^{k_0} pq^{k_1} pq^{k_2} \ldots$$

that belongs to the intersection of all G_i, and hence is contained in F'. However, x has infinitely many p's, and therefore infinitely many positions in which t is enabled, but t is never taken in x. Therefore, x is not strongly fair, that is, it is not in F' – a contradiction. □

Interestingly, a similar argument was used by Landweber [1969] (Lemma 3.1) to show that the set of sequences of $\{0, 1\}^\omega$ that contain finitely many 1's is not a G_δ set of the Cantor topology over $\{0, 1\}^\omega$.

9. FAIRNESS AND PROBABILITY

In this section, we provide a probability-theoretic view of fairness. In Section 8, we showed that fairness properties are exactly the sets that are large in a topological sense. In probability theory, a set is large if it has measure 1. Although these two notions of largeness are very similar, they do not coincide in general. However, we will prove that topological largeness and probabilistic largeness of temporal properties coincide for finite-state systems, ω-regular properties and bounded Borel measures. Thus, in the finite case and under mild assumptions, a property is a fairness property if and only if it has probability 1.

We start by pointing out some characteristics of the family of fairness properties.

9.1. Characteristics of Fairness

Let S be a safety property. The family $\mathcal{F}_S$ of all fairness properties in S, that is, of all—in the topological sense—large sets in S, has the following properties, which appeal to our intuition of largeness.

(1) Any superset of a large set is large. Hence the union of arbitrarily many large sets is large.
(2) The intersection of countably many large sets is large. Together with 1., this says that $\mathcal{F}_S$ is a *σ-filter*.

(3) Every large set is dense (in S) and therefore nonempty.
(4) If a set is large, its complement is not. Call a set *small* if its complement is large. A set may be neither large nor small. In that case we call it *medium-sized*.
(5) Intersection with a large set preserves size, that is., if F is large and X is small (medium-sized) [large] then $F \cap X$ is small (medium-sized) [large].
(6) If $S = \Sigma^\infty$ and $|\Sigma| \geq 2$, then every countable set is small, but there are also uncountable sets that are small.

Statement 1 follows immediately from the definition of fairness. Statement 2 was proved in Proposition 6.2. Statement 3 was proven in Proposition 6.1. Statement 4 follows immediately from statements 2 and 3. Statement 5 follows straight forwardly from statements 1 and 2. For the first part of statement 6, first observe that any singleton set is small because Ego has a strategy to avoid it. By duality, the union of countably many small sets is small. For part 2 of statement 6, consider $\Sigma = \{p, q, r\}$ and $E = \text{sat}(\Diamond\Box(p \vee q)) = \neg\text{sat}(\Box\Diamond r)$. E is clearly uncountable but small because Ego has a winning strategy for $\text{sat}(\Box\Diamond r)$. A similar example can be constructed for $|\Sigma| = 2$. Statement 6 can be generalized to safety properties S such that for each finite $\alpha \in S$, we have that $\alpha\uparrow$ is uncountable.

9.2. Probabilistic Largeness

To define probabilistic largeness, we first recall the standard setting of how probability is adjoined to systems.

A *σ-field* over a nonempty set Ω is a family $\mathcal{A}$ of subsets of Ω that contains the empty set and is closed under complementation and countable union. The intersection of arbitrarily many σ-fields is again a σ-field. Hence, for each family $\mathcal{F} \subseteq 2^\Omega$, there exists the smallest σ-field that contains $\mathcal{F}$. Given a topology $\mathcal{T}$ on Ω, the *Borel* σ-field of $\mathcal{T}$ is the smallest σ-field that contains $\mathcal{T}$. A member of the Borel σ-field is called a *Borel set*, which is precisely what we have introduced already in Section 8.3.

A *probability measure* on a σ-field $\mathcal{A}$ over Ω is a function $\mu : \mathcal{A} \to [0, 1]$ such that $\mu(\Omega) = 1$ and for any sequence of pairwise disjoint sets $(X_i)_{i\in\mathbb{N}}$, $\mu(\bigcup_{i\in\mathbb{N}} X_i) = \sum_{i\in\mathbb{N}} \mu(X_i)$. A *Borel* probability measure of a topology is a probability measure over the Borel σ-field of the topology. Given a probability measure μ on $\mathcal{A}$, and two sets $X, Y \in \mathcal{A}$, the *probability of X conditional to Y* is defined as $\mu(X \mid Y) = \mu(X \cap Y)/\mu(Y)$, provided $\mu(Y) > 0$.

A probabilistic system, or more general a *probabilistic safety property*, is a pair of a safety property S and a Borel measure μ of the Scott topology relativized to $\max(S)$. We can think of it as the tree that S represents in which at each branching a multisided coin is flipped to determine how the run is extended. We assume here maximality for convenience, that is, we assume that an enabled coin flip is eventually executed and each outcome of the coin flip properly extends the current run. We will write $\mu(X)$ for $\mu(X \cap \max(S))$ and $\mu(X \mid Y)$ for $\mu(X \cap \max(S) \mid Y \cap \max(S))$. Let $\alpha \in \Sigma^*$ and $s \in \Sigma$ such that $\alpha s \in S$. The conditional probability

$$p^s_\alpha = \mu(\alpha s\uparrow \mid \alpha\uparrow) = \mu(\alpha s\uparrow)/\mu(\alpha\uparrow) \tag{7}$$

is the probability that the outcome of the coin flip at the branching at α is s. Equation (7) implies $\mu((s_0 \cdots s_n)\uparrow) = p^s_\epsilon \cdot \cdots \cdot p^{s_n}_{s_0,\ldots,s_{n-1}}$. For each $\alpha \in S$, we have

$$\sum_{\alpha s\in S} p^s_\alpha = 1. \tag{8}$$

The Borel measure is determined by the p^s_α, that is, given $p^s_\alpha \in [0, 1]$ for each α and s with $\alpha s \in S$ such that (8) holds, there is a unique Borel measure μ of the Scott topology relativized to $\max(S)$ such that (7) holds.

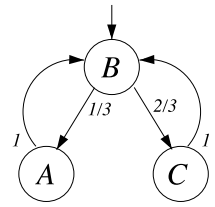

Fig. 8. A three-state system.

Let (S, μ) be a probabilistic safety property. We say that μ is a *Markov measure* if

$$p^{s'}_{\alpha s} = p^{s'}_{\beta s}$$

for all $\alpha, \beta \in S \cap \Sigma^*$ and $s, s' \in \Sigma$ such that $\alpha s s', \beta s s' \in S$, that is, if the coin-flip probabilities only depend on the last state. We say that μ is *positive* if all $p^s_\alpha > 0$ and therefore $\mu(\alpha\uparrow) > 0$ for each $\alpha \in S$; μ is said to be *bounded (away from zero)* if there exists a constant $c > 0$ such that $p^s_\alpha > c$ for each $\alpha s \in S$.

Example 9.1. Consider the system S, represented in Figure 8, which corresponds to the Petri net in Figure 7. For each $\alpha \in S \cap \Sigma^*$ such that $\alpha B \in S$, we define $p^A_{\alpha B} = 1/3$ and $p^C_{\alpha B} = 2/3$. Also, we are forced to have $p^B_{\beta A} = 1$ when $\beta A \in S$ and $p^B_{\beta C} = 1$ when $\beta C \in S$. This defines a Markov measure on S.

Topological and probabilistic largeness are very similar notions. Oxtoby's classic book [Oxtoby 1971] is devoted to the study of this similarity. All six statements in Section 9.1 are also true for probabilistic largeness, where for statement 3, we naturally have to assume that μ is positive. To see that statement 3 is true, let $\mu(F) = 1$ and $\alpha \in S$. If there is no extension of α into $S \cap F$, then $\alpha\uparrow \cap S \subseteq \neg F$. As $\mu(\alpha\uparrow) > 0$, we have $\mu(\neg F) > 0$ and hence $\mu(F) < 1$, a contradiction. All other statements follow from the laws of probability theory.

9.3. Separation

Although similar, the two notions of largeness do not coincide in general: there are sets that are large in one sense but not in the other.

Consider an (unrestricted and asymmetric, i.e., biased,) random walk on the integer line starting at 0. At each state the probability of going right is $p \neq 1/2$, and the probability of going left is $1 - p$ (cf. also Figure 6). The property X_1 = "The walk returns to 0 infinitely often" has probability 0 (see for instance Spitzer [2001]), but is co-meager (one easily displays a winning strategy for Ego in the Banach-Mazur game). On the other hand, the complement of X_1 has probability 1, but is meager.

A similar set can be displayed in a finite-state system: Consider the system in Figure 8. Note that the probability of going from B to C is not the same as the probability of going from B to A. The property X_2 = "The number of previous A's equals the number of previous C's infinitely often" has probability 0, but is co-meager.

Note that in both cases the winning strategies for Ego are unbounded, that is, the length of the sequences Ego adds is unbounded because he has to be able to compensate for unbounded moves by Alter.

More generally, we have the following result.

Definition 9.2. Let S be a safety property. A run x of S is said to *have infinitely many choices* if for infinitely many positions i, the prefix x_i has more than one extension in S.

LEMMA 9.3. *Let (S, μ) be a probabilistic safety property such that μ is a bounded Borel measure. Let x be a run of S with infinitely many choices. Then, for every $\varepsilon > 0$, there exist an i such that $\mu(x_i\uparrow) < \varepsilon$. In particular, $\mu(\{x\}) = 0$.*

PROOF. Let $c > 0$ be the bound of the Markov measure. Let $a = (1 - c)$. Let $k > 0$ be such that $a^k < \varepsilon$. Consider a prefix x_i that contains at least k choices. At each choice, the probability of the prefix is multiplied at most by a, and therefore $\mu(x_i\uparrow) \leq a^k < \varepsilon$. □

PROPOSITION 9.4. *Let M be a finite-state system and μ a bounded Borel measure on S_M. Suppose every maximal run of S_M has infinitely many choices. Then, S_M can be partitioned into a co-meager set and a set of measure 1.*

PROOF. The proof is essentially an adaptation from Oxtoby [1971, Thm. 1.6]. Take a dense countable subset X of S_M, for instance the set of periodic runs. Let x^i be the ith run of X for $i \in \mathbb{N}$. For every $i, j \in \mathbb{N}$, consider the prefix $x^i_{k_j}$ such that $\mu(x^i_{k_j}\uparrow) < (1/2)^{i+j+1}$. Let $G^i_j = x^i_{k_j}\uparrow$. Let $G_j = \bigcup_{i\in\mathbb{N}} G^i_j$, and let $G = \bigcap_{j\in\mathbb{N}} G_j$. Each G_j is open (as union of basic open sets) and contains the dense set X. Thus, G is a dense G_δ, and therefore co-meager. On the other hand, $\mu(G_j) \leq \sum_{i\in\mathbb{N}} \mu(G^i_j) < \sum_{i\in\mathbb{N}} (1/2)^{i+j+1} = (1/2)^j$. Therefore, $\mu(G) = 0$ and the complement of G has measure 1. □

9.4. Coincidence

We now prove that for bounded Borel measures on finite systems and ω-regular properties, the two notions of largeness coincide. Note that the property X_2 described in the counterexample in Section 9.3 is not accepted by any finite-state automaton.

PROPOSITION 9.5. *Let M be a finite-state system, μ a bounded Borel measure on S_M, and E an ω-regular property. If E is co-meager in S_M, then $\mu(E) = 1$.*

PROOF. If E is co-meager, Ego has a progressive winning strategy for E in the Banach-Mazur game $G(S_M, E)$. Berwanger et al. [2003] have shown that Ego then has also a *positional* winning strategy, that is, a strategy f such that

$$f(\alpha s) = \alpha s w \Rightarrow f(\beta s) = \beta s w$$

for all $\alpha, \beta \in \Sigma^*$. We will now show that $\mu(R_f) = 1$, and because $R_f \subseteq E$, we will have $\mu(E) = 1$.

As there are only finitely many states, the positional strategy f is also *bounded*, that is, there exists a $k \in \mathbb{N}$ such that

$$|f(\alpha)| - |\alpha| \leq k$$

for each $\alpha \in \Sigma^*$.

Let $c > 0$ be the bound on probabilities of transitions, and let E_i be the event: "at position $i \cdot k$, the run follows the strategy f", that is,

$$E_i = \{x \in S \mid f(x_{i\cdot k}) \sqsubseteq x\}.$$

Clearly, the probability of each E_i is at least c^k.

Then $\sum_n \mu(E_n) = +\infty$. If the E_n were independent, by the second Borel-Cantelli lemma (see, for instance, Williams [1991]), we would have that the set of infinitely many occurrences of E_n:

$$\limsup E_n = \bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} E_k$$

has probability 1. Clearly, $\limsup E_n \subseteq R_f$.

Unfortunately, the E_n are not independent, as the exact probability of playing the strategy at some position may depend on whether the strategy had been played before or not. However, while the exact probability may vary, we still know a lower bound for it: independently on whether the strategy has been played elsewhere, at position $i \cdot k$ the strategy is played with probability at least c^k. This form of "lower bound independence" is enough for our purposes. Indeed we use the following variant of the second Borel-Cantelli Lemma (see also Schmalz [2007, page 29]).

LEMMA 9.6. *Let E_n be events in some probability space. Denote by E'_n the complement of E_n. Suppose there exist a sequence $c_n > 0$ such that $\sum_{n=0}^{\infty} c_n = +\infty$ and such that the events are "lower bound independent" with respect to c_n, in the following sense: for each pair of finite disjoint sets of natural numbers I, J, for each $n \notin I \cup J$, if $\mu(E_n \mid \bigcap_{i\in I} E_i \cap \bigcap_{j\in J} E'_j)$ is defined, then $\mu(E_n \mid \bigcap_{i\in I} E_i \cap \bigcap_{j\in J} E'_j) \geq c_n$.*

Then, the probability that infinitely many E_n occur is 1.

We recall that $\mu(A \mid B)$ is defined as $\mu(A \cap B)/\mu(B)$. Therefore, it is defined only if $\mu(B) > 0$.

Define $a_n = 1 - c_n$. Then $\mu(E'_n \mid \bigcap_{i\in I} E_i \cap \bigcap_{j\in J} E'_j) \leq a_n$, if it is defined. By induction on k, we can easily prove that for each $n \geq 0$, $\mu(\bigcap_{n\leq i\leq n+k} E'_i) \leq \prod_{n\leq i\leq n+k} a_i$. The basis is $\mu(E'_n) \leq a_n$, which is a special case of lower bound independence. For the step, if $\mu(\bigcap_{n\leq i\leq n+k} E'_i)$=0, then trivially $\mu(\bigcap_{n\leq i\leq n+k+1} E'_i) = 0 \leq \prod_{n\leq i\leq n+k+1} a_i$. Otherwise,

$$\begin{aligned}
\mu\Big(\bigcap_{n\leq i\leq n+k+1} E'_i\Big) &= \mu\Big(E'_{n+k+1} \mid \bigcap_{n\leq i\leq n+k} E'_i\Big) \cdot \mu\Big(\bigcap_{n\leq i\leq n+k} E'_i\Big) \\
&\leq a_{n+k+1} \cdot \prod_{n\leq i\leq n+k} a_i \\
&= \prod_{n\leq i\leq n+k+1} a_i.
\end{aligned}$$

The first equality is by definition of conditional probability, whereas the inequality is by induction hypothesis and by lower bound independence.

Using logarithms one shows that $\sum_{n\leq i} c_i = +\infty$ implies $\prod_{n\leq i} a_i = 0$ and thus $\mu(\bigcap_{n\leq i} E'_i) = 0$ for any n. Therefore, $\mu(\bigcup_{n=1}^{\infty} \bigcap_{k=n}^{\infty} E'_k) = 0$, which implies $\mu(\bigcap_{n=1}^{\infty} \bigcup_{k=n}^{\infty} E_k) = 1$. □

Alternative proofs of Proposition 9.5 can be found in Schmalz [2007] and Varacca and Völzer [2006]. The converse of Proposition 9.5 also holds.

PROPOSITION 9.7. *Let M be a finite-state system, μ a bounded Borel measure on S_M, and E an ω-regular property. If $\mu(E) = 1$, then E is co-meager in S_M.*

PROOF. If E is not co-meager, then Alter has, owing to determinacy of ω-regular properties, a winning strategy f in the Banach-Mazur game $G(S_M, E)$. Let $\alpha_0 = f(\epsilon)$ be the first move of Alter in that strategy. We have $\mu(\alpha_0\uparrow) > 0$. As f is a winning strategy for Alter, f is also a winning strategy for Ego in the Banach-Mazur game $G(S_M, \neg(\alpha_0\uparrow \cap E))$. From Proposition 9.5, now follows $\mu(\neg(\alpha_0\uparrow \cap E)) = 1$, hence $\mu(\alpha_0\uparrow \cap E) = 0$. Because of $\mu(\alpha_0\uparrow) > 0$, we obtain $\mu(E) < 1$. □

We obtain that topological and probabilistic largeness coincide under the conditions discussed.

THEOREM 9.8. *In a finite system M under a bounded Borel measure μ, we have, for each ω-regular property E, $\mu(E) = 1$ if and only if E is co-meager in the Scott topology on S_M .*

In particular, topological and probabilistic largeness also coincide for properties expressible in LTL.

We observe that the requirement on boundedness could be further weakened. For instance, we could consider *slowly vanishing* measures, that is, measures that are not bounded but such that there exists a function $h(n)$ such that $\prod_n(1 - h(n)) = 0$ and for any prefix α of length n $p^s_\alpha > h(n)$ if $\alpha s \in S$.

10. FAIR CORRECTNESS

A system is *correct* with respect to a linear-time specification, that is, a temporal property E, if each run of the system satisfies E. If the system comes with a fairness assumption, we only have to check that each fair run satisfies the specification. The fairness assumption can be seen as a rely specification for the system that is guaranteed by the environment.

Traditionally only simple, well-understood fairness assumptions are employed, such as maximality, weak fairness and, occasionally, strong fairness. Proof calculi and model-checking algorithms have been optimized to deal with such simple fairness assumptions.

However, sometimes, a system does not satisfy a desired specification even under the assumption of strong fairness. As an example, we can consider again Dijkstra's dining philosophers and the "conspiracy" scenario mentioned in Section 3.4. For this particular example, there is also a starvation-free, although more complex, solution under strong fairness. However, for many problems, a system satisfying the actual specification is impossible, too difficult, or too expensive to obtain, cf. Fich and Ruppert [2003]. Still, simple systems may exist for those problems that satisfy the specification "well enough" and which actually work in practice.

However, in such cases, an appropriate fairness assumption, or more generally, an appropriate rely specification may be more difficult to find, more expensive to specify, and proof calculi and model-checking algorithms may not work well under them. For these cases, we can use a generic relaxation of correctness that allows us to verify a system that satisfies the specification "well enough", that is, for most, but not necessarily all, runs. To formalize "most" runs, we use topological largeness, that is, fairness.

Definition 10.1. A system M is *fairly correct* with respect to a temporal property E if E is co-meager in S_M.

Equivalently, M is fairly correct with respect to E if there exists a fairness assumption for M under which it is correct with respect to E, that is, there exists a fairness property F for S_M such that $S_M \cap F \subseteq E$. Thus, we abstract from the concrete fairness assumption that is required to guarantee the specification E. Note that the difference between traditional and fair correctness is small (in a topological sense). In particular, fair correctness guarantees that the system does not violate safety, that is, the safety property implied by the specification: M is fairly correct with respect to E implies that M is correct with respect to $\overline{E}$, that is, $S_M \subseteq \overline{E}$, where $\overline{E}$ denotes the safety closure of E introduced in Section 8.2. This implication follows from the fact that a co-meager set is dense.

Fair correctness occurs implicitly in the literature, in game-theoretic, topological and probabilistic form as will be explained in this article. In particular, it turns out that fair correctness is one of the seven relaxations of linear-time correctness

considered by Pistore and Vardi [2003] and Berwanger et al. [2003]. Pistore and Vardi [2003] provide an independent motivation of these relaxations of correctness in planning scenarios. They argue that such intermediate versions of correctness are adequate for specifying goals for automated task planning in nondeterministic domains.

We will now discuss how fair correctness can be verified.

10.1. Proving Fair Correctness

If ϕ is an LTL formula, then $\mathsf{A}\phi$ is a formula of the branching-time logic CTL*, cf. Emerson [1990], where A stands for "for all paths". If we reinterpret A in CTL* as "for most paths" in the topological sense, we obtain a language that can express fair correctness for LTL and which has been studied by Ben-Eliyahu and Magidor [1996]. They provide a sound and complete proof system for that language. The same proof system has been introduced before by Lehmann and Shelah [1982] for a version of CTL* in which the path quantifier A is interpreted as "for almost all paths" in the probabilistic sense. Lehmann and Shelah [1982] showed soundness and completeness of the proof system for finite probabilistic systems with bounded measures.

Alternatively, we can prove fair correctness, using deduction in linear-time temporal logic, by proving that the specification is implied by some well-known fairness property in the system—such as those presented in Section 3. One can then ask whether there is a fairness notion that is *complete* for proving fair correctness in this way, that is, a fairness notion F that implies all temporal properties that are fairly correct in the system, that is, M is fairly correct with respect to to E if and only if $F \cap S_M \subseteq E$. It is easy to see that, if such property existed, it should be obtained as the intersection of all fairness properties. This intersection may be the empty set in some systems as was shown in Section 6.

However, if one is interested in a particular class of specifications, then it is possible to find a fairness property that is complete—for that class.

Definition 10.2. Let S be a safety property and $\mathcal{F} \subseteq 2^{\Sigma^\infty}$ a family of linear-time properties. A fairness property F in S is *$\mathcal{F}$-complete* with respect to S if for each property $E \in \mathcal{F}$, we have: If E is co-meager in S, then $F \cap S \subseteq E$.

A complete fairness property, or a corresponding winning strategy for Ego, can be used to prove fair correctness with respect to each specification in $\mathcal{F}$. The following is a trivial consequence of the definition.

PROPOSITION 10.3. *Given a family $\mathcal{F}$, there is a $\mathcal{F}$-complete fairness property with respect to S if and only if*

$$\bigcap\{F \in \mathcal{F} \mid F \text{ is a fairness property in } S\} \tag{9}$$

is a fairness property in S.

Note that if F is complete for a family $\mathcal{F}$, then it is also complete for every subfamily of $\mathcal{F}$. Also note that if F is $\mathcal{F}$-complete and F' is a fairness property in S such that $F' \subseteq F$, then F' is also $\mathcal{F}$-complete.

Even if a $\mathcal{F}$-complete fairness property exists, it need not be a member of the family $\mathcal{F}$.

Definition 10.4. Let F be a fairness property. We say that F is *initial* in $\mathcal{F}$ with respect to S if F is $\mathcal{F}$-complete and $F \in \mathcal{F}$.

If $\mathcal{F}$ has an initial fairness property, then this is essentially unique:

PROPOSITION 10.5. *If F and F' are initial in $\mathcal{F}$, then $F \cap S = F' \cap S$.*

PROOF. From the definition of initiality follows $F \cap S \subseteq F'$ and $F' \cap S \subseteq F$. □

We are usually interested in countable families $\mathcal{F}$, such as the family of all ω-regular properties or the family of all LTL-expressible properties. The characterization of completeness in (9) then implies that there is a complete fairness property because fairness is closed under countable intersection.

In particular, completeness with respect to ω-regular and LTL-expressible properties can be characterized through word fairness (as defined in Section 3.6).

THEOREM 10.6. *Let $\mathcal{F}_1$ denote the family of all ω-regular properties or LTL-expressible properties. Let M be a finite system. A fairness property F is $\mathcal{F}_1$-complete with respect to M if and only if each run in $F \cap S_M$ is word fair. In particular, word fairness is $\mathcal{F}_1$-complete with respect to M.*

PROOF.
($\Leftarrow$) If E is an ω-regular property that is co-meager in S_M, then it follows—as in the proof of Proposition 9.5—that Ego has a positional winning strategy f in the Banach-Mazur game $G(S_M, E)$. Let $x \in S_M$ be word fair. If x is finite, then it must be maximal because of word fairness. As each finite maximal run is fair, we have $x \in E$. If x is infinite, some state s is repeated infinitely often. It follows that the word $w = sf(s)$ is enabled infinitely often in x. As x is word-fair, w is taken infinitely often in x. This, in turn, implies that $x \in R_f$. As f is winning for Ego, we have $x \in E$.
($\Rightarrow$) It is easy to see that word fairness with respect to a particular word w is LTL-expressible. As word fairness is indeed a fairness property in S_M, as argued in Section 4, the claim follows from the characterization in (9). □

The assumption in Proposition 10.6 that M is finite is essential. Consider the nondeterministic walk on the integer line in Figure 6 and the run $x = 0, 1, \ldots$; x is word fair but violates $\mathrm{sat}(\Diamond - 1)$, which is topologically large.

Another fairness notion that is complete for ω-regular properties is *α-fairness*, which was introduced by Lichtenstein et al. [1985] to prove probabilistic largeness. They also proved completeness with respect to probabilistic largeness in finite-state systems.

Although there exist complete fairness notions for ω-regular properties and therefore for LTL-expressible properties, those are not ω-regular themselves.

PROPOSITION 10.7. *Let $\mathcal{F}_1$ denote the family of all ω-regular properties or the family of LTL-expressible properties. There are finite systems M such that there is no initial fairness property in $\mathcal{F}_1$ with respect to S_M.*

PROOF. Consider $M = (\Sigma, R)$, with $\Sigma = \{p, q\}$ and $R = \Sigma \times \Sigma$. Suppose there were an ω-regular fairness property F that is $\mathcal{F}_1$-complete with respect to $S_M = \Sigma^\infty$. Then Ego has a positional winning strategy f in $G(S_M, F)$. Let $f(p) = pw_p$ and $f(q) = qw_q$. Let $x = (w_p w_q)^\omega$. Since f is winning and $x \in R_f$, we have $x \in F$. Let $k = |w_p| + |w_q|$ and let $w = p^k q$. This word w does not occur in x: p^k occurs in x only if $w_p w_q = p^k$. In that case $p^k q$ cannot occur in x. It follows that x is not strongly fair with respect to w. However, strong fairness with respect to w can be expressed in LTL. Hence F is not $\mathcal{F}_1$-complete, which contradicts our supposition. □

Proposition 10.7 shows that largeness of an LTL formula ϕ can in general not be checked by expressing a complete fairness property as LTL formula ψ and then checking the formula $(\psi \rightarrow \phi)$.

However, there are natural families that have an initial fairness property.

PROPOSITION 10.8. *Let $\mathcal{F}_2$ be the family of all RLTL-expressible properties and M a finite system. Then state fairness* (*as defined in Section* 3.6) *is initial in $\mathcal{F}_2$ with respect to S_M.*

PROOF. Zuck et al. [2002] point out that state fairness is complete for showing probabilistic largeness of properties that are expressible in RLTL. A direct, detailed proof for this result is given by Schmalz [2007]. State fairness for a finite system $M = (\Sigma, R)$ can be expressed by the following RLTL formula:

$$\bigwedge_{(s,s')\in R} \Box\Diamond s \rightarrow \Box\Diamond s' \tag{10}$$

□

10.2. Model Checking Fair Correctness

Proposition 10.8 shows that checking a finite system against fair correctness with respect to an RLTL formula can be reduced to classical model checking of an RLTL formula. In fact, it can be shown that, using this approach, checking fair correctness of RLTL is co-NP-complete [Schmalz et al. 2007]. Proposition 10.7 shows that the same approach cannot be taken for LTL and ω-regular properties.

Berwanger et al. [2003] showed that checking fair correctness with respect to an LTL specification for a finite system is decidable. They show that the existence of a winning strategy for Ego in the corresponding variation of the Banach-Mazur game for LTL-expressible objectives can be expressed as satisfaction of a CTL* formula. Their translation however is of nonelementary complexity and hence not suitable for complexity analysis.

We have shown elsewhere [Varacca and Völzer 2006] that fair correctness of an LTL formula can be expressed in CTL+past, a language that is strictly less expressive than CTL*. One can then model check the translation. However, the translated formula incurs a double exponential blowup, and therefore this is not an optimal algorithm.

Pistore and Vardi [2003] provide a translation of fair correctness for LTL into the logic EGCTL* of Kupferman [1999], whose model-checking complexity is double exponential [Kupferman 1999].

The exact complexity of checking fair correctness was so far still an open question (see also Kupferman and Vardi [2006]). In the light of Theorem 9.8, we can use probabilistic model checking to check fair correctness for ω-regular specifications on finite systems. In particular we can now answer the open question:

COROLLARY 10.9. *Checking fair correctness of a finite-state system against an ω-regular or an LTL specification is PSPACE-complete in the size of the specification, that is, in the size of the Büchi automaton or the LTL formula respectively. It can be done in linear time with respect to the size of the system.*

Together with Theorem 9.8, the result follows from the corresponding results on qualitative probabilistic model checking [Courcoubetis and Yannakakis 1995; Vardi 1985].

Additional results on model checking fair correctness can be obtained for specific fragments of LTL (see Schmalz et al. [2007]). In particular, there exist natural fragments of LTL for which it is easier to check fair correctness than (classical) correctness [Schmalz et al. 2007]. Fair correctness can be extended to branching-time semantics, incorporating it into branching-time logics, such as CTL and CTL*. We studied their model checking problems in detail elsewhere [Varacca and Völzer 2006].

11. CONCLUSIONS

We have proposed a definition of fairness that is in line with the well-known formalizations of safety and liveness. We have given three equivalent characterizations of fairness: one that generalizes the standard notion of strong fairness, one in terms of the Banach-Mazur game, and one in terms of topological largeness. The game-theoretic characterization stresses the intuition that fairness guarantees that some finite behavior will always eventually happen, while fairness can never prevent any finite behavior from happening recurrently. The topological characterization confirms the intuition that most runs of a system are fair. To strengthen this intuition, we have shown that in some cases, topological largeness coincides with probabilistic largeness. In these cases, the set of unfair runs has probability 0.

The definition of fairness led to a generic relaxation of linear-time correctness, which we called fair correctness. Verifying fair correctness of a system can be useful whenever the specification is satisfied only under some, possibly strong, fairness assumption and the fairness assumption is either unknown, expensive to specify, or impossible to specify in the temporal logic. We have shown that the model-checking problem for fair correctness has the same complexity for LTL and ω-regular specification as the corresponding problem for classical correctness. This also answered an open question posed by Pistore and Vardi.

One prominent topic in the literature on fairness is the *implementability* of a fairness notion (cf., e.g., Joung [2001]), in which one asks whether a scheduler exists that can be superimposed onto the system to realize a given fairness assumption. In this article, we have chosen the simplest possible setting to study fairness, aligned with earlier related contributions [Alpern and Schneider 1985; Manna and Pnueli 1990], in which a system has only one source of nondeterminism, which is then restricted by the fairness assumption. In the corresponding setting of a scheduler that implements a fairness assumption, the scheduler has access to all nondeterministic choices of the system. Besides our abstract study of fairness, such a simple setting can be adequate, for example, for studying some nondistributed multitasking operating systems. Then, Theorem 9.8 implies that any ω-regular fairness assumption on a finite system can be generically implemented with probability 1 through coin flipping. This includes the implementation of very strong fairness assumptions such as ∞-fairness over finitary properties (Def. 4.1). Alternatively, one can use a deterministic scheduler for word fairness, for example, repeatedly scheduling all enabled finite words of the system, to implement any ω-regular fairness notion in a finite system (cf. Theorem 10.6). One could then still ask whether some fairness assumption can be implemented in some sense more efficiently in a given finite system or whether it can be implemented at all in a given infinite system.

However, often the question of implementability arises in a specific system model, for example, a finite set of distributed processes that communicate asynchronously by message passing. In such models, we often have more than one source of nondeterminism, such as the uncertain order of message receipt or the unknown inputs from the environment. These sources of nondeterminism need to be distinguished in the system model because usually not all of them can be influenced by a superimposed scheduler. Studying implementability then requires a more complex setting to reflect this. A natural generalized setting to study implementability are *open systems* with two kinds of nondeterministic choices, one controlled by a scheduler and the other by an adversary, that is, the environment. A direction for further work is to formalize fairness in that setting, which is tightly related to the notion of *realizability* as introduced by Abadi et al. [1989] and to two-player games, similar to the ones presented in Asarin et al. [2010].

It is clear that some of the fairness notions discussed in this article cannot be implemented in such a generalized setting as they stand. For example, if an action is k-enabled, it does not necessarily mean that a scheduler can ensure its execution in the future because it may not have access to all the actions that lead to the enabledness. Complications can also arise in distributed systems where the scheduler may require nontrivial distributed computations to obtain the global knowledge needed to guarantee a certain fairness notion [Joung 1999]. Studying such issues requires further specialization of the system model to reflect distribution and the fact that the scheduler has only partial knowledge of the system state.

We mentioned related work throughout this article. Some authors used the notion that we have described as fairness in different contexts without actually attempting to define fairness: Ben-Eliyahu and Magidor [1996] observed that some popular fairness notions describe co-meager sets. Alur and Henzinger [1995] argue that for the compositional modeling of reactive systems, machine closure should be strengthened to what they call *local liveness*, which is the same as what we have defined as fairness. They gave the game-theoretic definition. As mentioned above, a generalized form of the Banach-Mazur game had been considered by Pistore and Vardi [2003] as well as Berwanger et al. [2003]. Thus, our results link different strands of research that were developed independently.

In addition, we would like to mention two related works whose relations with ours should be further studied. One is the recent work by Jaeger [2009] who finds connections between a more concrete, intensional fairness notion and Martin-Löf randomness. Jaeger [2009] also extends earlier work of Baier and Kwiatkowska [1998] by providing a deeper analysis of the relationship of his fairness notion and probability beyond bounded measures. The second work by Darondeau et al. [1992], where another, rather different, point of view on fairness is provided. For them, fairness properties are characterized as the Π^0_3 sets in Kleene's hierarchy. Thus, the class of fairness properties is not closed under superset. No topological characterization is provided, although there are analogies between Π^0_3 sets and $F_{\sigma\delta}$ sets.

Some follow-up work on our proposal has already appeared. Schmalz et al. [2007] show, for various subclasses of LTL, that model checking fair correctness has either the same complexity as checking classical correctness or is even strictly less expensive. Furthermore we show elsewhere [Schmalz et al. 2009] that the game-theoretic characterization can be used to present counterexamples in probabilistic model checking. Asarin et al. [2010] study the notion of fairness in the context of two-player games. A generalization of the Banach-Mazur game is proposed, and the equivalence between two-player games with fairness and Markov decision processes is shown. Baier et al. [2008] apply our framework to timed automata. There, a coincidence result between topological and probabilistic largeness is also shown.

ACKNOWLEDGMENTS

We would like to thank Matthias Schmalz for carefully reviewing various versions of this paper, Ekkart Kindler for earlier collaborations on the topic of fairness, and the anonymous reviewers for numerous suggestions for improving the presentation in this article.

REFERENCES

ABADI, M. AND, LAMPORT, L. 1991. The existence of refinement mappings. *Theoret. Comput. Sci. 82*, 253–284.

ABADI, M., LAMPORT, L., AND WOLPER, P. 1989. Realizable and unrealizable specifications of reactive systems. In *Proceedings of the 16th International Colloquium on Automata, Languages and Programming*. Springer-Verlag, 1–17.

ALPERN, B. AND SCHNEIDER, F. B. 1985. Defining liveness. *Inf. Proc. Lett. 21*, 181–185.

ALUR, R. AND HENZINGER, T. A. 1994. Finitary fairness. In *Proceedings of 9th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, 52–61.

ALUR, R. AND HENZINGER, T. A. 1995. Local liveness for compositional modeling of fair reactive systems. In *Proceedings of 7th International Conference on Computer Aided Verification*. Lecture Notes in Computer Science Series, vol. 939, Springer, 166–179.

APT, K. R., FRANCEZ, N., AND KATZ, S. 1988. Appraising fairness in languages for distributed programming. *Dist. Comput. 2*, 226–241.

ASARIN, E., CHANE-YACK-FA, R., AND VARACCA, D. 2010. Fair adversaries and randomization in two-player games. In *Proceedings of 13th FOSSACS*. Lecture Notes in Computer Science Series, vol. 6014, Springer, 64–78.

ATTIE, P. C., FRANCEZ, N., AND GRUMBERG, O. 1993. Fairness and hyperfairness in multi-party interactions. *Dist. Comput. 6*, 245–254.

BAIER, C. AND KWIATKOWSKA, M. Z. 1998. On the verification of qualitative properties of probabilistic processes under fairness constraints. *Inf. Proc. Lett. 66,* 2, 71–79.

BAIER, C., BERTRAND, N., BOUYER, P., BRIHAYE, T., AND GRÖSSER, M. 2008. Almost-sure model checking of infinite paths in one-clock timed automata. In *Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, 217–226.

BEN-ELIYAHU, R. AND MAGIDOR, M. 1996. A temporal logic for proving properties of topologically general executions. *Inf. Comput. 124,* 2, 127–144.

BERWANGER, D., GRÄDEL, E., AND KREUTZER, S. 2003. Once upon a time in a west - determinacy, definability, and complexity of path games. In *Proceedings of 10th LPAR*. Lecture Notes in Computer Science Series, vol. 2850, Springer, 229–243.

BEST, E. 1984. Fairness and conspiracies. *Inf. Proc. Lett. 18*, 215–220. (Erratum ibidem 19:162).

CLARKE, E. M., EMERSON, E. A., AND SISTLA, A. P. 1986. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Trans. Prog. Lang. Sys. 8,* 2, 244–263.

COURCOUBETIS, C. AND YANNAKAKIS, M. 1995. The complexity of probabilistic verification. *J. ACM 42*, 4, 857–907.

DARONDEAU, P., NOLTE, D., PRIESE, L., AND YOCCOZ, S. 1992. Fairness, distances and degrees. *Theoret. Comput. Sci. 97,* 1, 131–142.

DUGUNDJI, J. 1966. *Topology*. Allyn and Bacon.

EMERSON, E. A. 1990. Temporal and modal logic. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B)*. MIT Press and Elsevier, 995–1072.

FICH, F. E. AND RUPPERT, E. 2003. Hundreds of impossibility results for distributed computing. *Dist. Comput. 16,* 2-3, 121–163.

FRANCEZ, N. 1986. *Fairness*. Springer.

GRÄDEL, E. 2008. Banach-Mazur games on graphs. In *Proceedings of the 28th FSTTCS*. LIPIcs 2 Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik.

JAEGER, M. 2009. On fairness and randomness. *Inf. Comput. 207,* 9, 909–922.

JOUNG, Y.-J. 1999. Localizability of fairness constraints and their distributed implementations. In *Proceedings of 10th CONCUR*. Lecture Notes in Computer Science Series, vol. 1664, Springer, 336–351.

JOUNG, Y.-J. 2001. On fairness notions in distributed systems, part I: A characterization of implementability. *Inf. Comput. 166*, 1–34.

KUPFERMAN, O. 1999. Augmenting branching temporal logics with existential quantification over atomic propositions. *J. Logic. Comput. 9,* 2, 135–147.

KUPFERMAN, O. AND VARDI, M. Y. 2006. Memoryful branching-time logic. In *Proceedings of 21st Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, 265–274.

KWIATKOWSKA, M. Z. 1989. Survey of fairness notions. *Inf. Softw. Tech. 31,* 7, 371–386.

KWIATKOWSKA, M. Z. 1991. On topological characterization of behavioural properties. In *Topology and Category Theory in Computer Science*, G. Reed, A. Roscoe, and R. Wachter Eds., Oxford University Press, 153–177.

LAMPORT, L. 1977. Proving the correctness of multiprocess programs. *IEEE Trans. Softw. Eng. 3*, 2, 125–143.

LAMPORT, L. 2000. Fairness and hyperfairness. *Dist. Comput. 13*, 4, 239–245.

LANDWEBER, L. H. 1969. Decision problems for omega-automata. *Math. Syst. Theory 3*, 4, 376–384.

LEHMANN, D. AND SHELAH, S. 1982. Reasoning with time and chance. *Inf. Control 53*, 3, 165–198.

LEHMANN, D. J., PNUELI, A., AND STAVI, J. 1981. Impartiality, justice and fairness: The ethics of concurrent termination. In *Proceedings of 8th International Colloquium on Automata, Languages and Programming*. Lecture Notes in Computer Science Series, vol. 115, Springer, 264–277.

LICHTENSTEIN, O., PNUELI, A., AND ZUCK, L. D. 1985. The glory of the past. In *Proceedings of the Conference on Logic of Programs*. Lecture Notes in Computer Science Series, vol. 193, Springer, 196–218.

MANNA, Z. AND PNUELI, A. 1990. A hierarchy of temporal properties. In *Proceedings of the 9th Annual ACM Symposium on Principles of Distributed Computing*. ACM, 377–408.

MANNA, Z. AND PNUELI, A. 1992. *The Temporal Logic of Reactive and Concurrent Systems – Specification*. Springer.

MAULDIN, R. D. 1981. *The Scottish Book: Mathematics from the Scottish Cafe*. Birkhäuser.

MURATA, T. 1989. Petri nets: Properties, analysis and applications. *Proc. IEEE 77,* 4, 541–580.

OXTOBY, J. C. 1957. The Banach-Mazur game and Banach category theorem. In *Contributions to the Theory of Games, Vol. III*. Annals of Mathematical Studies Series, vol. 39, Princeton University Press, 159–163.

OXTOBY, J. C. 1971. *Measure and Category. A Survey of the Analogies between Topological and Measure Spaces*. Springer.

PISTORE, M. AND VARDI, M. Y. 2003. The planning spectrum - one, two, three, infinity. In *Proceedings of 18th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, 234–243.

PNUELI, A. 1983. On the extremely fair treatment of probabilistic algorithms. In *Proceedings of the 15th Annual Symposium on Theory of Computing*. ACM, 278–290.

REISIG, W. 1985. *Petri Nets: An Introduction*. Monographs in Theoretical Computer Science. An EATCS Series Series, vol. 4, Springer.

SCHMALZ, M. 2007. Extensions of an algorithm for generalised fair model checking. M.S. thesis, Technisch-Naturwissenschaftliche Fakultät, Universität zu Lübeck, Germany.

SCHMALZ, M., VÖLZER, H., AND VARACCA, D. 2007. Model checking almost all paths can be less expensive than checking all paths. In *Proceedings of 27th FSTTCS*. Lecture Notes in Computer Science Series, vol. 4855, Springer, 532–543.

SCHMALZ, M., VARACCA, D., AND VÖLZER, H. 2009. Counterexamples in probabilistic LTL model checking for Markov chains. In *Proceedings of 20th CONCUR*. Lecture Notes in Computer Science Series, vol. 5710, Springer, 587–602.

SMYTH, M. B. 1992. Topology. In *Handbook of Logic in Computer Science*, S. Abramsky, D. M. Gabbay, and T. Maibaum Eds. Vol. 1: Background: Mathematical Structures. Oxford University Press, 641–761.

SPITZER, F. 2001. *Principles of Random Walk*. Springer.

TELGÁRSKY, R. 1987. Topological games: On the 50th anniversary of the Banach-Mazur game. *Rocky Mountain J. Math. 17,* 2, 227–276.

THOMAS, W. 1990. Automata on infinite objects. In *Handbook of Theoretical Computer Science*, J. van Leeuwen Ed., Vol. B: Formal Models and Semantics. Elsevier.

VARACCA, D. AND VÖLZER, H. 2006. Temporal logics and model checking for fairly correct systems. In *Proceedings of 21st LICS*. IEEE Computer Society, 389–398.

VARDI, M. Y. 1985. Automatic verification of probabilistic concurrent finite-state programs. In *Proceedings of 26th Foundation of Computer Science*. 327–338.

VÖLZER, H. 2002. Refinement-robust fairness. In *Proceedings of 13th CONCUR*. Lecture Notes in Computer Science Series, vol. 2421, Springer, 547–561.

VÖLZER, H. 2005. On conspiracies and hyperfairness in distributed computing. In *Proceedings of 19th DISC*. Lecture Notes in Computer Science Series, vol. 3724, Springer, 33–47.

VÖLZER, H., VARACCA, D., AND KINDLER, E. 2005. Defining fairness. In *Proceedings of 16th CONCUR*. Lecture Notes in Computer Science Series, vol. 3653, Springer, 458–472.

WILLIAMS, D. 1991. *Probability with Martingales*. Cambridge University Press.

ZUCK, L. D., PNUELI, A., AND KESTEN, Y. 2002. Automatic verification of probabilistic free choice. In *Proceedings of 3rd VMCAI, Revised Papers*. Lecture Notes in Computer Science Series, vol. 2294, Springer, 208–224.

Received March 2011; revised December 2011; accepted February 2012