Convergence Measures

Nils Klarlund*

TR 90-1106
March 1990

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501

*Partially supported by an Alice & Richard Netter Scholarship and Thanks to Scandinavia Foundation, Inc. and NSF grant CCR 88-06979. Author's electronic address is klarlund@cs.cornell.edu.

Convergence Measures

Nils Klarlund[1]

Cornell University

Abstract General methods of verification for programs defining *infinite* computations rely on measuring *progress* or *convergence* of finite computations towards satisfying the specification. Traditionally, progress is measured using *well-founded orderings*, but this often involves syntactic transformations.

Our main result is that program verification can take place by *direct measurement* of convergence for programs that are analytic ($\mathbf{\Sigma}_1^1$) sets and specifications that are coanalytic ($\mathbf{\Pi}_1^1$) sets. We use orderings that are *not* well-founded, but that ensure well-foundedness of limits of finite trees.

Our results can also be seen as a new approach to parts of descriptive set theory. In fact, Souslin's Theorem—that every set in $\mathbf{\Sigma}_1^1 \cap \mathbf{\Pi}_1^1$ is Borel—is a corollary of our main result.

1 Introduction

The *verification problem* is a fundamental issue in computer science. For *infinite computations*, it can be formulated:

> Given a program A and a specification C, each defining a set of computations, how can one determine that A satisfies C, i.e. $A \subseteq C$, reasoning only about *finite computations*?

For certain kinds of specifications, like those imposing *fairness* requirements on computations, dozens of methods have been suggested. Yet, the general problem has, to the author's knowledge, only been addressed in relatively

[1]Partially supported by an Alice & Richard Netter Scholarship of the Thanks to Scandinavia Foundation, Inc. and NSF grant CCR 88-06979.

Author's electronic address is `klarlund@cs.cornell.edu`.

few articles [DH86,Har86,Var87]. The earlier proposals, however, hinge on the practice of reducing the verification problem to the termination problem, which in turn is solved using *well-founded orderings*. These methods are *indirect* because they involve transformations of programs. The direct approaches in [AS87,AS89,Kla90b,RR88] only apply to sets at low levels of the Borel Hierarchy, namely finite Boolean combinations of $\mathbf{G}_\delta$ sets. In [Kla90a], a direct method is given for $\mathbf{F}_{\sigma\delta}$ programs and $\mathbf{G}_{\delta\sigma}$ specifications. Still, the question of whether there is a general direct method applicable to all Borel sets was open.

In this paper, we answer this question positively; in fact, we show a more general result. To do this, we represent programs and specifications using *approximation functions* that describe finite computations. Then the verification problem is addressed using a *convergence measure* on approximation functions. This measure—which is based on an ordering that is *not* well-founded—guarantees that any infinite computation of the program satisfies the specification. Our main result is that program verification can take place by such direct measurement of convergence for programs that are analytic ($\mathbf{\Sigma}_1^1$) sets and specifications that are coanalytic ($\mathbf{\Pi}_1^1$) sets.

As simple corollaries of our approach, we obtain the Boundedness Theorem for $\mathbf{\Pi}_1^1$ sets and the Souslin Theorem that a set is Borel if it is both analytic and coanalytic. Therefore, it is our hope that our work might inspire more set-theoretic studies based on finite approximations.

2 Our Results

Our contributions are the following:

- A representation of analytic and coanalytic sets based on limits of *approximation functions*, which assign a finite tree to each finite computation. We show that any analytic (resp. coanalytic) set can be represented as a limit, $\lim_{\neg\mathrm{WF}} \tau$ (resp. $\lim_{\mathrm{WF}} \tau$), where τ is an approximation function and $\lim_{\neg\mathrm{WF}}$ and $\lim_{\mathrm{WF}}$ are limit operators. Here, $\lim_{\mathrm{WF}} \tau$ is the set of computations for which the tree arising as the limit of finite approximations is well-founded (i.e. has no infinite paths), and $\lim_{\neg\mathrm{WF}} \tau$ is the set of computations for which the limit tree is not well-founded.

- The *WF ordering*, which—while not itself well-founded—ensures that the limit of any ordered sequence of trees is well-founded.

- The notion of *convergence measure*, which expresses that finite computations converging towards computations of program A also converge towards computations of specification C.

- A characterization of the question $A \subseteq C$ in terms of finite approximation functions, where $A = \lim_{\neg\mathrm{WF}} \tau^A$ and $C = \lim_{\mathrm{WF}} \tau^C$, to wit:
  $A \subseteq C$ *iff* (τ^A, τ^C) *is convergence measurable.*

- Elementary proofs of the Boundedness Theorem for $\mathbf{\Pi}^1_1$ sets and the Souslin Theorem. The former proof is based on a powerful class of automata, which we call *Borel automata.*

3 Previous Work

Earlier verification methods aiming at general properties [DH86,Har86, Var87] of infinite state systems relied on extensive modifications of the program to be verified in order to reduce progress to something that could be measured in terms of well-founded orderings. Another general approach [Kla90b,MP87] relies on the use of "and"-nondeterministic automata (a word is accepted if *all* runs are accepting), but such a view does not give satisfactory measures of convergence, because one is forced to look at all runs at the same time.

Direct methods based on measuring finite computations have so far only been shown for low levels of the Borel Hierarchy. The methods in [AS87,AS89,Kla90b,Kla90a,RR88] all apply to various kinds of finite Boolean combinations of $\mathbf{G}_\delta$ sets.

The approach in [Kla90a] gives a direct method for solving the verification problem for $\mathbf{F}_{\sigma\delta}$ programs and $\mathbf{G}_{\delta\sigma}$ specifications, and the results of the present paper generalize this method. The *liminf ordering* in [Kla90a] orders paths in a well-founded tree in a way that is reminiscent of the Kleene-Brouwer ordering. The WF ordering presented in this paper is a natural extension of the liminf ordering to embeddings of trees.

Souslin's Theorem was first proved in [LS18].

4 Generalized Limit Operators

To study analytic sets in the *Baire space* ω^ω, which consists of infinite sequences $\alpha = \alpha_0, \alpha_1, \dots$ of natural numbers, we first need some notation for trees.

A tree τ is a prefix-closed subset of ω^*, each sequence $t = \langle t^0, \dots, t^\ell \rangle$ representing a *node*, which has children $t \cdot \langle d \rangle \in \tau$. Here "$\cdot$" denotes catenation and $d \in \omega$ is the *direction* of $t \cdot \langle d \rangle$ from t. Any sequence of directions $\langle t^0, t^1, \dots \rangle$ (finite or infinite) denotes a path $\langle\rangle, \langle t^0 \rangle, \langle t^0, t^1 \rangle, \dots$ (finite or infinite) in τ, provided each $\langle t^0, \dots, t^\ell \rangle \in \tau$. The *level* $|t|$ of a node $t = \langle t^0, \dots, t^\ell \rangle$ is the number ℓ. We view trees as growing upwards with the children ordered from left to right in increasing order.

For a sequence $\tau_0, \tau_1, \dots$ of trees, we define $\lim_i \tau_i$ as:

$$t \in \lim_i \tau_i \text{ iff } \forall^\infty i : t \in \tau_i,$$

where $\forall^\infty$ means "for all but finitely many." It is not hard to see that $\lim_i \tau_i$ is a tree, which we call the *limit tree*. An *approximation function* τ assigns a finite tree $\tau(u)$ to each finite sequence $u \in \omega^*$. Let the limit operators $\lim_{\neg \mathrm{WF}}$

and $\lim_{\mathrm{WF}}$ be defined by: for $\alpha \in \omega^\omega$,

$$\alpha \in \lim_{\neg\mathrm{WF}} \tau \ \text{ iff } \ \neg\mathrm{WF} \lim_{u \to \alpha} \tau(u)$$

$$\alpha \in \lim_{\mathrm{WF}} \tau \ \text{ iff } \ \mathrm{WF} \lim_{u \to \alpha} \tau(u)$$

where $u \to \alpha$ denotes that u takes the values $\langle\rangle, \langle\alpha_0\rangle, \langle\alpha_0, \alpha_1\rangle, \ldots$ and $\mathrm{WF}\,T$ denotes that tree T is well-founded.

Theorem 1 (Representation Theorem) *Limit operators* $\lim_{\neg\mathrm{WF}}$ *and* $\lim_{\mathrm{WF}}$ *define the class* $\mathbf{\Sigma}^1_1$ *and* $\mathbf{\Pi}^1_1$ *of the Baire space, i.e.* $A \in \mathbf{\Sigma}^1_1 \Leftrightarrow \exists\tau : A = \lim_{\neg\mathrm{WF}} \tau$ *and* $C \in \mathbf{\Pi}^1_1 \Leftrightarrow \exists\tau : C = \lim_{\mathrm{WF}} \tau$.

Proof We give the proof for $\lim_{\neg\mathrm{WF}}$ (the proof for $\lim_{\mathrm{WF}}$ being obtainable by dualization) and use the fact that a set A is analytic iff it is representable as a tree T on $\omega \times \omega$ such that

$$A = \{\alpha \mid \exists\beta \in \omega^\omega : \forall n : (\alpha, \beta)\downarrow_n \in T\}$$

(see for example [Mos80, p.77]). Here, $\downarrow_n$ denotes the prefix up to index n, i.e. $(\alpha, \beta)\downarrow_n = \langle(\alpha_0, \beta_0), \ldots, (\alpha_n, \beta_n)\rangle$.

Now for such a representation T of an analytic set A, define for all $u = \langle u_0, \ldots, u_n\rangle \in \omega^*$:

$$\tau(u) = \{\langle\beta^0, \ldots, \beta^n\rangle \mid \langle(u_0, \beta^0), \ldots, (u_n, \beta^n)\rangle \in T\}.$$

Then it follows that $\neg\mathrm{WF} \lim_{u \to \alpha} \tau(u)$ iff $\alpha \in A$.

On the other hand, if $A = \lim_{\neg\mathrm{WF}} \tau$, then let T consist of all infinite paths $\langle(u_0, t^0), (u_1, t^1), \ldots\rangle$ such that $\langle t^0, t^1, \ldots\rangle \in \lim_{i \to \omega} \tau(\langle u_0, \ldots, u_i\rangle)$. Let A be the analytic set defined by T. Then we obtain again that $\neg\mathrm{WF} \lim_{u \to \alpha} \tau(u)$ iff $\alpha \in A$. $\square$

This characterization of $\mathbf{\Sigma}^1_1$ and $\mathbf{\Pi}^1_1$ relies on well-foundedness as do classic representations, but differs in using limits instead of projections or sequence mappings (cf [Mos80, pp. 84,193]). Also in analogy with classic results, we have:

Theorem 2 (Boundedness Theorem for $\mathbf{\Pi}_1^1$ sets) *Let $C = \lim_{\mathrm{WF}} \tau$ be a coanalytic set. If there is a countable ordinal ν such that for all $\alpha \in C$, $\lim_{u \to \alpha} \tau(u)$ is ν-rankable,[2] then C is Borel.*

We postpone the proof of Theorem 2 to Section 7.

5 The WF Ordering

To define the WF ordering, we need the concept of tree embeddings. Let T be a fixed tree. An *embedding* of a tree τ in T is an injective mapping $\rho : \tau \to T$ such that $\rho(\langle\rangle) = \langle\rangle$ and for all $t \cdot \langle d \rangle \in \tau$ there is d' with $\rho(t \cdot \langle d \rangle) = \rho(t) \cdot \langle d' \rangle$. Note that $|\rho(t)| = |t|$; in fact, ρ is just a structure-preserving relabeling of τ. Also note that $\mathrm{dom}\rho$, the domain of the mapping ρ, is the tree τ and that $\mathrm{rng}\rho$, the range of ρ, is the image in T of τ.

We can now define the *WF ordering*, which we denote by $\succeq_{\mathrm{WF}}$.

Definition 1 *$\rho \succeq_{\mathrm{WF}} \rho'$ if for all $s \in \mathrm{dom}\rho \cap \mathrm{dom}\rho'$, $\rho(s) \geq \rho'(s)$, where "$\geq$" is the lexicographic ordering, i.e. $\langle d^0, \ldots, d^n \rangle \geq \langle e^0, \ldots, e^n \rangle$ if either $\langle d^0, \ldots, d^n \rangle = \langle e^0, \ldots, e^n \rangle$ or there is a level $\lambda \leq n$ such that $d^\lambda > e^\lambda$ and for all $\ell < \lambda$, $d^\ell = e^\ell$.*

Intuitively, $\rho \succeq_{\mathrm{WF}} \rho'$ if for any node s in both $\mathrm{dom}\rho$ and $\mathrm{dom}\rho'$, the image in T of s under ρ' is the same as or to the left of the image under ρ. Although $\succeq_{\mathrm{WF}}$ is not a well-founded ordering, it ensures well-foundeness in the limit provided T is well-founded. This is a consequence of:

Proposition 1 *Let T be a fixed tree and let $\rho_0 \succeq_{\mathrm{WF}} \rho_1 \succeq_{\mathrm{WF}} \cdots$ be an infinite ordered sequence of embeddings in T. Then there is an embedding ρ of $\lim_i \mathrm{dom}\rho_i$ in $\lim_i \mathrm{rng}\rho_i$.*

Proof Let $s = \langle s^0, \ldots, s^\ell \rangle \in \lim_i \mathrm{dom}\rho_i$. Then there is K such that for all $k \geq K$, $s \in \mathrm{dom}\rho_k$. Hence by definition of $\succeq_{\mathrm{WF}}$, we have $\rho_K(\langle s^0, \ldots, s^\ell \rangle) \geq$

[2]Here, a well-founded tree T is *ν-rankable* if there is an assigment of ordinals to the nodes of T such that the root has rank ν and if a node t has rank γ then every child of t has rank less than γ.

$\rho_{K+1}(\langle s^0, \ldots, s^\ell \rangle) \geq \cdots$. Thus, there is a $H \geq K$ and directions $t^0, \ldots, t^\ell$ such that for all $k \geq H$, $\rho_k(\langle s^0, \ldots, s^\ell \rangle) = \langle t^0, \ldots, t^\ell \rangle$ and therefore, $\langle t^0, \ldots, t^\ell \rangle \in \lim_i \mathrm{rng}\rho_i$. Now define $\rho(t) = \langle t^0, \ldots, t^\ell \rangle$.

It is not hard to verify that ρ so defined is an embedding of $\lim_i \mathrm{dom}\rho_i$ in $\lim_i \mathrm{rng}\rho_i$. □

Corollary 1 *If* WF T *and* $\rho_0 \succeq_{\mathrm{WF}} \rho_1 \succeq_{\mathrm{WF}} \cdots$, *then* WF $\lim_i \mathrm{dom}\rho_i$.

Hence if T is well-founded, $\succeq_{\mathrm{WF}}$ measures progress of trees towards defining a well-founded tree. To state this more forcefully, we need a couple of definitions.

Definition 2 *A* tree graph $G = (V, E, \tau)$ *is a countable directed graph* (V, E) *with a* tree assignment τ *that defines a finite tree for each node in* V. *An infinite path* $v_0, v_1, \ldots$ *has the* WF property *if WF* $\lim_i \tau(v_i)$, *and* G *has the WF property if all paths have the WF property.*

A WF measure (μ, T) *of a tree graph* $G = (V, E, \tau)$ *is a finite path tree* T *and a mapping* $\mu : v \in V \rightarrow (\tau(v) \rightarrow T)$ *such that* $\mu(v)$ *is an embedding of* $\tau(v)$ *in* T *and* μ *respects the edge relation of* G, *i.e.* $(u, v) \in E$ *implies* $\mu(u) \succeq_{\mathrm{WF}} \mu(v)$. G *is* WF measurable *if it allows a WF measure. By abuse of language, we also call* μ *a measure (in* T*).*

A key result of this paper is the following characterization of graphs with the WF property.

Proposition 2 $G = (V, E, \tau)$ *has the WF property iff* G *is WF measurable.*

Proof ($\Leftarrow$) Let (μ, T) be a WF measure of G and let $v_0, v_1, \ldots$ be an infinite path in G. Then $\mu(v_0) \succeq_{\mathrm{WF}} \mu(v_1) \succeq_{\mathrm{WF}} \cdots$. Thus by Corollary 1, WF $\lim_i \mathrm{dom}\mu(v_i)$ and as $\mathrm{dom}\mu(v_i) = \tau(v_i)$, it follows that $v_0, v_1, \ldots$ has the WF property.

($\Rightarrow$) Given that G has the WF property, we show how to construct a finite path tree T and a measure μ in T. We need the following lemma, where $w \rightarrow_W^* W$ denotes that there is a path in W from w to any $w' \in W$.

`AssignWF`(W, t):

For each d:

(a) Let $\widehat{W} = \{v \in W \mid (\wp_2 t) \cdot \langle d \rangle \in \tau(v)\}$.
If $\widehat{W} = \emptyset$, then exit.

(b) Use Lemma 1 to obtain a partitioning $\mathcal{P} = W_0, W_1, \ldots$ of $\widehat{W}$.

(c) For each class W_k of $\mathcal{P}$:

i. $T := T \cup \{t \cdot \langle (k, d) \rangle\}$

ii. $W(t \cdot \langle (k, d) \rangle) = W_k$,

iii. `AssignWF`$(W_k, t \cdot \langle (k, d) \rangle)$

Figure 1: The algorithm `AssignWF`.

Lemma 1 *Let $G = (V, E)$ be a non-empty countable graph. Then there exists a finite or infinite partitioning $\mathcal{P} = W_0, W_1, \ldots$ of V and a mapping ι that to each class W of $\mathcal{P}$ associates a node $\iota(W) \in W$ such that* (a) *$\iota(W) \rightarrow^*_W W$ and* (b) *for all $(v, v') \in E$, if $v \in W_k$ and $v' \in W_{k'}$, then $k \geq k'$.*

Proof See [Kla90a]. $\square$

Now to construct the tree T, we use the algorithm in Figure 1. For now, T is defined as a tree with directions in $\omega \times \omega$, but later we view it as a tree on ω by using an appropriate pairing function. Each node $t = \langle (k^0, s^0), \ldots, (k^n, s^n) \rangle$ of T has a label $W(t)$, which is a subset of V constructed such that for all $v \in W(t)$, $\langle s^0, \ldots, s^n \rangle \in \tau(v)$. The algorithm `AssignWF` is initially invoked with $W = V, t = \langle \rangle$, and variable $T = \{\langle \rangle\}$.

The purpose of `AssignWF`(W, t) is for each d to define children of node t together with their labels. First in Step (a) of Figure 1, nodes v in W whose tree $\tau(v)$ does not contain $\langle s^0, \ldots, s^n, d \rangle$ are filtered out; here $\wp_2(\langle (k^0, s^0), \ldots, (k^n, s^n) \rangle) = \langle s^0, \ldots, s^n \rangle$. Second in Step (b), the resulting set $\widehat{W}$ is partitioned using Lemma 1. Third in Step (c), a child in direction (k, d) with label W_k is created for each class W_k of the partitioning and the algorithm is reapplied on W_k and node $t \cdot \langle k, d \rangle$.

It can be seen that the algorithm corresponds to a monotonic set operator w.r.t. the values of T. Thus, we take the final value of T to be the fixed point of the corresponding set operator. In addition, we define $W(\langle\rangle) = V$.

Note that to each label $W(t)$, where $t \neq \langle\rangle$, is associated a node $\iota(W(t))$ of G such that $\iota(W(t)) \rightarrow^*_{W(t)} W(t)$, because $W(t)$ is a class defined by an application of Lemma 1.

Claim 1

(a) *For all* $t \in T$, *for all* $v \in W(t)$, $\wp_2(t) \in \tau(v)$.

(b) *For any* $t \cdot \langle (k, d) \rangle \in T$, *it holds that* $W(t) \supseteq W(t \cdot \langle (k, d) \rangle)$.

(c) *For each* $v \in V$ *and each* $\langle s^0, \ldots, s^n \rangle \in \tau(v)$, *there is a unique list* $\langle k^0, \ldots, k^n \rangle$ *of length* n *such that* $v \in W(\langle (k^0, s^0), \ldots, (k^n, s^n) \rangle)$.

Proof Follows by induction. □

Now using Claim 1(c), we define an embedding $\mu(v)$ of $\tau(v)$ in T by $\mu(v)(s) = \langle (k^0, s^0), \ldots, (k^n, s^n) \rangle$ for all $s = \langle s^0, \ldots, s^n \rangle \in \tau(v)$. To prove that μ preserves order, assume that $(u, v) \in E$ and $s = \langle s^0, \ldots, s^n \rangle \in \mathrm{dom}\tau(u) \cap \mathrm{dom}\tau(v)$. Let $k^0, \ldots, k^n, h^0, \ldots, h^n$ be defined by

$$\begin{aligned}
\langle (k^0, s^0), \ldots, (k^n, s^n) \rangle &= \mu(u)(\langle s^0, \ldots, s^n \rangle) \\
\langle (h^0, s^0), \ldots, (h^n, s^n) \rangle &= \mu(v)(\langle s^0, \ldots, s^n \rangle)
\end{aligned}$$

Then either $\langle k^0, \ldots, k^n \rangle = \langle h^0, \ldots, h^n \rangle$ or there is a $\lambda \leq n$ such that $k^\lambda \neq h^\lambda$ and $k^\ell = h^\ell$ for all $\ell < \lambda$. Let $t = \langle (k^0, s^0), \ldots, (k^{\lambda-1}, s^{\lambda-1}) \rangle = \langle (h^0, s^0), \ldots, (h^{\lambda-1}, s^{\lambda-1}) \rangle$. Then $\texttt{AssignWF}(W(t), t)$ was invoked and $u, v \in W(t)$. This invocation defined $W(t \cdot \langle (k^\lambda, s^\lambda) \rangle$ and $W(t \cdot \langle (h^\lambda, s^\lambda) \rangle)$, which are disjoint subsets of $W(t)$ by assumption that $k^\lambda \neq h^\lambda$. Hence, $k^\lambda > h^\lambda$ by Lemma 1. Therefore, if we use a pairing function $\# : \omega \times \omega \rightarrow \omega$ that is monotonic in its first variable to code the directions of T, we obtain

$$\langle \#(k^0, s^0), \ldots, \#(k^n, s^n) \rangle \geq \langle \#(h^0, s^0), \ldots, \#(h^n, s^n) \rangle.$$

As this holds for all $s \in \mathrm{dom}\tau(u) \cap \mathrm{dom}\tau(v)$, it follows that $\mu(u) \succeq_{\mathrm{WF}} \mu(v)$.

Claim 2 *There is no infinite path in T.*

Proof Suppose for a contradiction that $\langle (k^0, s^0), (k^1, s^1), \ldots \rangle$ is an infinite path. Then by Claim 1(b), $W(\langle (k^0, s^0) \rangle) \supseteq W(\langle (k^1, s^1) \rangle) \supseteq \cdots$ and therefore for any $n > 0$, if $t = \langle (k^0, s^0), \ldots, (k^n, s^n) \rangle$ then $\iota(W(t)) \rightarrow^*_{W(t)} W(t \cdot \langle (k^{n+1}, s^{n+1} \rangle)$, because $\iota(W(t)) \rightarrow^*_{W(t)} W(t)$, by Lemma 1. In particular, $\iota(W(t)) \rightarrow^*_{W(t)} \iota(W(t \cdot \langle (k^{n+1}, s^{n+1}) \rangle))$. We conclude that there exists an infinite path $v_0, v_1, \cdots$ in G and a monotonic increasing function $i(j)$ such that $v_{i(j)} = \iota(W(\langle (k^0, s^0), \ldots, (k^j, s^j) \rangle))$ for all j, and for all $n \geq i(j)$, it holds by Claim 1(a) that $\langle s^0, \ldots, s^j \rangle \in \tau(v_n)$. But then $v_0, v_1, \cdots$ does not have the WF property, because $\langle s^0, s^1, \ldots \rangle$ is an infinite path in $\lim_i \tau(v_i)$. Contradiction. □

6 Convergence Measures

To formulate the notion of convergence measure, we need to "braid" the trees of approximation functions.

Definition 3 *Given finite trees τ and τ', the set $M^{\vee}(\tau, \tau')$ consisting of nodes $\langle d^0, e^0, \ldots, d^n, e^n \rangle$ and $\langle d^0, e^0, \ldots, e^{n-1}, d^n \rangle$, where $n \geq -1$, $\langle d^0, \ldots, d^n \rangle \in \tau$ and $\langle e^0, \ldots, e^n \rangle \in \tau'$, is called the* or-merge *of τ and τ'.*

It is not hard to see that $M^{\vee}(\tau, \tau')$ is a tree. The or-merge has the following properties:

Proposition 3 (a) *Let τ_i and τ'_i be infinite sequences of trees. Then* $\mathrm{WF}\lim_i M^{\vee}(\tau_i, \tau'_i)$ *iff* $\mathrm{WF}\lim_i \tau_i$ *or* $\mathrm{WF}\lim_i \tau'_i$. *Moreover,* (b) *if* $\lim M^{\vee}(\tau_i, \tau'_i)$ *is ν-rankable and* $\neg\mathrm{WF}\lim_i \tau_i$, *then* $\lim_i \tau'_i$ *is ν-rankable.*

Proof (a)($\Rightarrow$) By contraposition, assume that $\neg\mathrm{WF}\lim_i \tau_i$ and $\neg\mathrm{WF}\lim_i \tau_i'$. Thus, there are infinite paths $\langle d^0, d^1, \ldots\rangle$ and $\langle e^0, e^1, \ldots\rangle$ in $\lim_i \tau_i$ and $\lim_i \tau_i'$. Then it can be seen that $\langle d^0, e^0, d^1, e^1, \ldots\rangle$ is an infinite path in $\lim_i M^\vee(\tau_i, \tau_i')$.

(a)($\Leftarrow$) By contraposition, assume that $\langle d^0, e^0, d^1, e^1, \ldots\rangle$ is an infinite path in $\lim_i M^\vee(\tau_i, \tau_i')$. Then it follows that $\langle d^0, d^1, \ldots\rangle$ and $\langle e^0, e^1, \ldots\rangle$ are infinite paths in $\lim_i \tau_i$ and $\lim_i \tau_i'$.

(b) Assume $\lim M^\vee(\tau_i, \tau_i')$ is ν-rankable and $\neg\mathrm{WF}\lim_i \tau_i$. Then there is an infinite path $\langle d^0, d^1, \ldots\rangle$ in $\lim_i \tau_i$. But then for every node $\langle e^0, \ldots, e^n\rangle$ in $\lim_i \tau_i'$, $\langle d^0, e^0, \ldots, d^n, e^n\rangle$ is in $\lim_i M^\vee(\tau_i, \tau_i')$. Now let $\gamma(t)$ be the rank of $\lim_i M^\vee(\tau_i, \tau_i')$ in a ν-ranking of $\lim M^\vee(\tau_i, \tau_i')$ and define a ranking γ' of $\lim_i \tau_i'$ by $\gamma'(\langle e^0, \ldots, e^n\rangle) = \gamma(\langle d^0, e^0, \ldots, d^n, e^n\rangle)$. Then γ' is a ν-ranking of $\lim_i \tau_i'$. □

Now to study the problem whether $A \subseteq C$, where $A = \lim_{\neg\mathrm{WF}} \tau^A$ is analytic and $C = \lim_{\mathrm{WF}} \tau^C$ is coanalytic, we use the following:

Definition 4 *A* convergence measure (T, μ) *for* (τ^A, τ^C) *is a WF measure of the Baire space with tree assignment* $u \mapsto M^\vee(\tau^A(u), \tau^C(u))$ *for* $u \in \omega^*$.

Here (by abuse of language), the Baire space is viewed as a tree with edge relation $(u, v) \in E$ if $v = u \cdot \langle d\rangle$.

Our main result is:

Theorem 3 *For analytic* $A = \lim_{\neg\mathrm{WF}} \tau^A$ *and coanalytic* $C = \lim_{\mathrm{WF}} \tau^C$, $A \subseteq C$ *iff* (τ^A, τ^C) *is convergence measurable.*

Proof ($\Leftarrow$) Assume that (τ^A, τ^C) has measure (T, μ). Let $\alpha \in A$. Then $\neg\mathrm{WF}\lim_i \tau_i^A$, and because μ is a WF measure and $\langle\rangle, \langle\alpha_0\rangle, \langle\alpha_1\rangle, \langle\alpha_1, \alpha_2\rangle \cdots$ is an infinite path, we get an ordered sequence

$$\mu(\langle\rangle) \succeq_{\mathrm{WF}} \mu(\langle\alpha_0\rangle) \succeq_{\mathrm{WF}} \mu(\langle\alpha_0, \alpha_1\rangle) \succeq_{\mathrm{WF}} \cdots$$

Thus by Definition 4 and Proposition 2, $\mathrm{WF}\lim_{u\to\alpha} M^\vee(\tau^A(u), \tau^C(u))$. By Proposition 3(a), we deduce $\mathrm{WF}\lim_{u\to\alpha} \tau^C(u)$, whence $\alpha \in C$.

($\Rightarrow$) If $A \subseteq C$, then by Proposition 3(a) it holds for all $\alpha \in \omega^\omega$ that WF $\lim_{u \to \alpha} M^\vee(\tau^A(u), \tau^C(u))$. Use Proposition 2 to obtain T and μ. $\square$

Corollary 2 (Souslin's Theorem) *If A is analytic and coanalytic, then A is Borel.*

Proof If A is analytic, i.e. $A = \lim_{\neg \mathrm{WF}} \tau^A$ for some τ^A, and coanalytic, i.e. $A = \lim_{\mathrm{WF}} \tau^C$ for some τ^C, then by Theorem 3 (τ^A, τ^C) has a convergence measure (μ, T), because $A \subseteq A$. Let ν be a countable ordinal such that T is ν-rankable. Then by Proposition 3(b), for any $\alpha \in A$, $\lim_{u \to \alpha} \tau^C(u)$ is ν-rankable, because $\neg \mathrm{WF} \lim_{u \to \alpha} \tau^A(u)$. Then A is Borel by Theorem 2. $\square$
Note: in an expanded version of this article, we will give a simple proof of the other (easier) direction: every Borel set is analytic and coanalytic.

7 Borel Automata

In the Baire space, the class of Borel sets is the least class that contains all open sets[3] and is closed under enumerable unions and intersections. To describe these sets, we introduce a very powerful automaton concept.

Definition 5 *A* Borel automaton *$A = (Q, q^0, \to, \phi_\nu)$ on alphabet ω consists of a countable set of states Q, an initial state q^0, a deterministic transition relation $\to \subseteq Q \times \omega \times Q$ and a ranked formula ϕ_ν, where ν is a countable ordinal.*

Definition 6 *By transfinite induction, we define a* ranked formula *ϕ_γ to be either a* temporal predicate *$\Box\Diamond\Phi$ ("infinitely often Φ") or $\Diamond\Box\Phi$ ("almost always Φ"), where Φ is a predicate on Q, or a disjunction $\bigvee_{\gamma' < \gamma} \phi_{\gamma'}$ or a conjunction $\bigwedge_{\gamma' < \gamma} \phi_{\gamma'}$, where $\phi_{\gamma'}$ are ranked formulas.*

A sequence $q_0, q_1, \ldots$ satisfies *ϕ_γ, written $q_0, q_1, \ldots \models \phi_\gamma$, according to:*

[3] An open set is a countable union of basic open sets, which are on the form $\{u \cdot \alpha | \alpha \in \omega^\omega\}$ for $u \in \omega^*$.

$$q_0, q_1, \ldots \models \Diamond\Box\Phi \ \textit{iff} \ \exists H : \forall h > H : q_h \models \Phi$$

$$q_0, q_1, \ldots \models \Box\Diamond\Phi \ \textit{iff} \ \forall H : \exists h > H : q_h \models \Phi$$

$$q_0, q_1, \ldots \models \bigwedge_{\gamma'<\gamma} \phi_{\gamma'} \ \textit{iff} \ \forall\gamma' < \gamma : q_0, q_1, \ldots \models \phi_{\gamma'}$$

$$q_0, q_1, \ldots \models \bigvee_{\gamma'<\gamma} \phi_{\gamma'} \ \textit{iff} \ \exists\gamma' < \gamma : q_0, q_1, \ldots \models \phi_{\gamma'}$$

A *run* $q_0, q_1, \ldots$ of A over $\alpha \in \omega^\omega$ is a sequence of states such that $q_0 = q^0$ and for all i, $q_i \xrightarrow{\alpha_i} q_{i+1}$ (i.e. $(q_i, \alpha_i, q_{i+1}) \in \rightarrow$). We assume that A allows a run (which is unique because A is deterministic) over every $\alpha \in \omega^\omega$. A run $q_0, q_1, \ldots$ is *accepting* if $q_0, q_1, \ldots \models \phi_\nu$, and α is *accepted* if the run over α is accepting. The *language* $L(A) \subseteq \omega^\omega$ defined by A is the set of α that are accepted.

Proposition 4 *The class of languages defined by Borel automata is the class of Borel sets.*

Proof It is well-known that automata on the form $(Q, q^0, \rightarrow, \Box\Diamond\Phi)$ define the class of $\mathbf{G}_\delta$ sets[4] [Arn83,Lan69] (these automata are known as deterministic infinite state Büchi automata). The proof then follows by transfinite induction. $\Box$

Now to prove the Boundedness Theorem of Section 4, we assume that $C = \lim_{\mathrm{WF}} \tau^C$ is a coanalytic set and ν is a countable ordinal such that for all $\alpha \in C$, $\lim_{u \to \alpha} \tau^C(u)$ is ν-rankable. We define a Borel automaton with $Q = \{(u, \tau^C(u)) \mid u \in \omega^*\}$, $q^0 = (\langle\rangle, \tau^C(\langle\rangle))$, and transition relation $(u, \tau) \xrightarrow{d} (u', \tau')$ if $u' = u \cdot \langle d \rangle$. By transfinite induction, define ϕ^t_γ, where $t \in \omega^*$, as

$$\begin{aligned} \phi^t_0 &= \bigwedge_{d \in \omega} \Box\Diamond\neg\Phi^{t\cdot\langle d\rangle} \\ \phi^t_\gamma &= \bigwedge_{d \in \omega} (\Box\Diamond\neg\Phi^{t\cdot\langle d\rangle} \vee \bigvee_{\gamma'<\gamma} \phi^{t\cdot\langle d\rangle}_{\gamma'}), \quad \text{if } \gamma > 0 \end{aligned}$$

[4] $\mathbf{G}$ is the class of open sets and $\mathbf{G}_\delta$ is the class of countable intersections of open sets.

where Φ^t is a state predicate defined by $(u,\tau)\models\Phi^t$ iff $t \in \tau$. Then it is not hard to see that $(u_0,\tau_0),(u_1,\tau_1),\ldots\models\phi^t_\gamma$ iff the limit of $\tau_0[t],\tau_1[t],\ldots$ is γ-rankable, where $\tau[t]$ denotes the empty tree if $t \notin \tau$ and otherwise denotes the subtree of τ rooted at t.

Hence, if we let $A = (Q, q^0, \rightarrow, \phi^{\langle\rangle}_\nu)$, then $L(A) = C$, whence C is Borel by Proposition 4.

Acknowledgements

Thanks to Dexter Kozen for comments and suggestions which significantly improved the paper. Also thanks to Chet Murthy, Steve Rapkin, and Jim Russell for helpful discussions.

References

[Arn83] A. Arnold. Topological characterizations of infinite behaviors of transition systems. In *Proc. 10th Col. Automata, Languages and Programming*, pages 490–510. LNCS, Vol. 154, Springer-Verlag, 1983.

[AS87] B. Alpern and F.B. Schneider. Recognizing safety and liveness. *Distributed Computing*, 2:117–126, 1987.

[AS89] B. Alpern and F.B. Schneider. Verifying temporal properties without temporal logic. *ACM Transactions on Programming Languages*, 11(1):147–167, January 1989.

[DH86] I. Dayan and D. Harel. Fair termination with cruel schedulers. *Fundamenta Informatica*, 9:1–12, 1986.

[Har86] D. Harel. Effective transformations on infinite trees with applications to high undecidability, dominos, and fairness. *Journal of the ACM*, 33(1):224–248, 1986.

[Kla90a] N. Klarlund. Limit operators and convergence measures for ω-languages with applications to extreme fairness. Technical Report TR-1100, Cornell University, 1990.

[Kla90b] N. Klarlund. Verification conditions for ω-automata and applications to fairness. Technical Report TR-1080, Cornell University, 1990.

[Lan69] L.H. Landweber. Decision problems for ω-automata. *Math. System Theory*, 3:376–384, 1969.

[LS18] N. Lusin and W. Sierpinski. Sur quelques proprietés des ensembles (A). *Bull. Int. Acad. Sci. Cracovie*, Série A: Sciences Mathématiques:35–48, 1918.

[Mos80] Yinnis N. Moschovakis. *Descriptive Set Theory*, volume 100 of *Studies in Log. and the Found. of Math.* North-Holland, 1980.

[MP87] Z. Manna and A. Pnueli. Specification and verification of concurrent programs by $\forall$-automata. In *Proc. Fourteenth Symp. on the Principles of Programming Languages*, pages 1–12. ACM, 1987.

[RR88] O. Grumberg R. Rinat, N. Francez. Infinite trees, markings and well-foundedness. *Information and Computation*, 79:131–154, 1988.

[Var87] M. Vardi. Verification of concurrent programs: The automata-theoretic framework. In *Proc. Symp. on Logic in Computer Science.* IEEE, 1987.