METRIC STRUCTURES AND PROBABILISTIC COMPUTATION

WESLEY CALVERT

Abstract. Continuous first-order logic is used to apply model-theoretic analysis to analytic structures (e.g. Hilbert spaces, Banach spaces, probability spaces, etc.). Classical computable model theory is used to examine the algorithmic structure of mathematical objects that can be described in classical first-order logic. The present paper shows that probabilistic computation (sometimes called randomized computation) can play an analogous role for structures described in continuous first-order logic.

The main result of this paper is an effective completeness theorem, showing that every decidable continuous first-order theory has a probabilistically decidable model. Later sections give examples of the application of this framework to various classes of structures, and to some problems of computational complexity theory.

1. Introduction

Continuous first-order logic was introduced in [4, 2] as a model-theoretic context sufficient to handle stability theory for so-called "metric structures." These are many-sorted structures in which each sort is a complete metric space of finite diameter. Key examples include Hilbert spaces, Banach spaces, probability spaces, and probability spaces with a distinguished automorphism.

For classical first-order model theory, there is a meaningful sense of computation and effectiveness: In a group, for instance, we have a reasonable algorithmic understanding of a group if the set of triples constituting the Caley table (equivalently, the set of words equal to the identity element) is decidable. Of course, there are often still many algorithmic unknowns in the group, such as the conjugacy problem and the isomorphism problem [12]. The aim of the present paper is to provide a similar framework for continuous first-order logic.

The framework suggested is probabilistic computation. This model of computation has seen wide use in complexity theory [18, 35], and there is some room for hope that an understanding of the relationship between continuous and classical first-order logic might yield insights into the relationship between probabilistic and deterministic computation. Section 7 gives reasons for such hope.

Not to get carried away in speculation, though, it is still cause for contentment that a way can be found to meaningfully talk about algorithmic information in the context of metric structures. The impossibility of finding an algorithm to solve arbitrary Diophantine equations (see [24]), the relationship of isoperimetric functions to the word problem [31, 6], and much more depend on a notion of computation adequate to the context of countable rings (in the case of Diophantine

Date: August 19, 2009.

Key words and phrases. Computable Model Theory, Probabilistic Computation, Randomized Computation, Continuous Logic, Metric Structures.

equations) and groups (in the case of the word problem). Some preliminary results on specific metric structures, given in Section 6, will suggest that there is ground for fruitful research in the effective theory of these structures.

A key argument that probabilistic computation is the *right* algorithmic framework for this context is that it admits an effective completeness theorem. The classical theorem is this.

Theorem 1.1 (Effective Completeness Theorem)**.** *A (classically) decidable theory has a (classically) decidable model.*

A full proof of this result may be found in [16], but it was known much earlier, at least to Millar [25]. The main theoretical contribution of the present paper will be to interpret the terms of this theorem in such a way as to apply to a continuous first-order theory and probabilistic computation. The main result of the present paper is the proof in Section 4 of the theorem naturally corresponding to Theorem 1.1.

Section 2 will describe the syntax and semantics for continuous first-order logic. The reader familiar with [3] or [2] will find nothing new in Section 2, except a choice of a finite set of logical connectives (no such choice is yet canonical in continuous first-order logic). Section 3 will define probabilistic Turing machines and the class of structures they compute. Section 4 will contain the proof of the main result. Section 6 will contain some examples, exhibiting different aspects of the information which is conveyed by the statement that a certain structure is probabilistically computable, and in Section 7 we will conclude with some remarks on time complexity of structures.

2. Continuous First-Order Logic

We will, in keeping with the existing literature on continuous first-order logic, adopt the slightly unusual convention of using 0 as a numerical value for True (or acceptance) and 1 as a numerical value for False (or rejection). The authors of [4] chose this convention to emphasize the metric nature of their logic.

Continuous first-order logic is an extension of Łukasiewicz propositional logic, which builds on work of Keisler and Henson (see [2] for a more detailed history). The following definitions are from [3].

2.1. **Semantics.**

Definition 2.1. A *continuous signature* is an object of the form $\mathcal{L} = (\mathcal{R}, \mathcal{F}, \mathcal{G}, n)$ where

1. $\mathcal{R}$ and $\mathcal{F}$ are disjoint and $\mathcal{R}$ is nonempty, and
2. n is a function associating to each member of $\mathcal{R} \cup \mathcal{F}$ its arity
3. $\mathcal{G}$ has the form $\{\delta_{s,i} : (0,1] \to (0,1] : s \in \mathcal{R} \cup \mathcal{F} \text{ and } i < n_s\}$

Members of $\mathcal{R}$ are called *relation symbols*, and members of $\mathcal{F}$ *function symbols*. We now define the class of structures.

Definition 2.2. Let $\mathcal{L} = (\mathcal{R}, \mathcal{F}, \mathcal{G}, n)$ be a continuous signature. A *continuous $\mathcal{L}$-pre-structure* is an ordered pair $\mathfrak{M} = (M, \rho)$, where M is a non-empty set, and ρ is a function on $\mathcal{R} \cup \mathcal{F}$ such that

1. To each function symbol f, the function ρ assigns a mapping $f^{\mathfrak{M}} : M^{n(f)} \to M$

(2) To each relation symbol P, the function ρ assigns a mapping $P^{\mathfrak{M}} : M^{n(P)} \to [0,1]$.
(3) The function ρ assigns d to a pseudo-metric $d^{\mathfrak{M}} : M \times M \to [0,1]$.
(4) For each $f \in \mathcal{F}$ for each $i < n_f$, and for each $\epsilon \in (0,1]$, we have

$$\forall \bar{a}, \bar{b}, c, e \left[d^{\mathfrak{M}}(c,e) < \delta_{f,i}(\epsilon) \Rightarrow d^{\mathfrak{M}}\left(f^{\mathfrak{M}}(\bar{a}, c, \bar{b}), f^{\mathfrak{M}}(\bar{a}, e, \bar{b}) \right) \leq \epsilon \right]$$

where $lh(\bar{a}) = i$ and $lh(\bar{a}) + lh(\bar{b}) = n_f - 1$.
(5) For each $P \in \mathcal{R}$ for each $i < n_P$, and for each $\epsilon \in (0,1]$, we have

$$\forall \bar{a}, \bar{b}, c, e \left[d^{\mathfrak{M}}(c,e) < \delta_{f,i}(\epsilon) \Rightarrow |P^{\mathfrak{M}}(\bar{a}, c, \bar{b}) - P^{\mathfrak{M}}(\bar{a}, e, \bar{b})| \leq \epsilon \right]$$

where $lh(\bar{a}) = i$ and $lh(\bar{a}) + lh(\bar{b}) = n_P - 1$.

Definition 2.3. A *continuous weak $\mathcal{L}$-structure* is a continuous $\mathcal{L}$-pre-structure such that ρ assigns to d a metric.

Since we are concerned here with countable structures, we will not use the stronger notion of a *continuous $\mathcal{L}$-structure* common in the literature, which requires that ρ be assigned to a *complete* metric. However, it is possible, given a continuous weak structure (even a pre-structure), to pass to a completion [3].

Definition 2.4. Let V denote the set of variables, and let $\sigma : V \to M$. Let φ be a formula.

(1) The *interpretation under σ* of a term t (written $t^{\mathfrak{M},\sigma}$) is defined by replacing each variable x in t by $\sigma(x)$.
(2) Let φ be a formula. We then define the *value of φ in $\mathfrak{M}$ under σ* (written $\mathfrak{M}(\varphi,\sigma)$) as follows:
  (a) $\mathfrak{M}(P(\bar{t}),\sigma) := P^{\mathfrak{M}}(\overline{t^{\mathfrak{M},\sigma}})$
  (b) $\mathfrak{M}(\alpha \dot{-} \beta, \sigma) := \max\left(\mathfrak{M}(\alpha,\sigma) - \mathfrak{M}(\beta,\sigma), 0\right)$
  (c) $\mathfrak{M}(\neg\alpha,\sigma) := 1 - \mathfrak{M}(\alpha,\sigma)$
  (d) $\mathfrak{M}(\frac{1}{2}\alpha,\sigma) := \frac{1}{2}\mathfrak{M}(\alpha,\sigma)$
  (e) $\mathfrak{M}(\sup_x \alpha, \sigma) := \sup\limits_{a \in M} \mathfrak{M}(\alpha, \sigma_x^a)$, where σ_x^a is equal to σ except that $\sigma_x^a(x) = a$.
(3) We write $(\mathfrak{M},\sigma) \models \varphi$ exactly when $\mathfrak{M}(\varphi,\sigma) = 0$.

Of course, if φ has no free variables, then the value of $\mathfrak{M}(\varphi,\sigma)$ is independent of σ.

2.2. **Syntax.**

Definition 2.5. Let $\mathcal{S}_0$ be a set of distinct propositional symbols. Let $\mathcal{S}$ be freely generated from $\mathcal{S}_0$ by the formal binary operation $\dot{-}$ and the unary operations $\neg$ and $\frac{1}{2}$. Then $\mathcal{S}$ is said to be a *continuous propositional logic.*

We now define truth assignments for continuous propositional logic.

Definition 2.6. Let $\mathcal{S}$ be a continuous propositional logic.

(1) if $v_0 : \mathcal{S}_0 \to [0,1]$ is a mapping, we can extend v_0 to a unique mapping $v : \mathcal{S} \to [0,1]$ by setting
  (a) $v(\varphi \dot{-} \psi) := \max\left(v(\varphi) - v(\psi), 0\right)$
  (b) $v(\neg\varphi) := 1 - v(\varphi)$
  (c) $v(\frac{1}{2}\varphi) = \frac{1}{2}v(\varphi)$

We say that v is the *truth assignment* defined by v_0.

(2) We write $v \models \Sigma$ for some $\Sigma \subseteq \mathcal{S}$ whenever $v(\varphi) = 0$ for all $\varphi \in \Sigma$.

Roughly, $\varphi \dot{-} \psi$ has the sense of $\psi \to \varphi$. We can also, of course, define $\varphi \wedge \psi$ as $\varphi \dot{-} (\varphi \dot{-} \psi)$, and $\varphi \vee \psi$ via deMorgan's law. We can also define something resembling equivalence, $|\varphi - \psi| = (\varphi \dot{-} \psi) \vee (\psi \dot{-} \varphi)$. Łukasiewicz propositional logic is the fragment of this logic which does not involve $\frac{1}{2}$.

To make a first-order predicate variant of this logic, we use sup in the place of $\forall$ and inf in the place of $\exists$ (with the obvious semantics, as will be described in what follows). We typically also include a binary function d, whose standard interpretation is generally a metric. Now we give the syntactic axioms for continuous first-order logic:

(A1) $(\varphi \dot{-} \psi) \dot{-} \varphi$
(A2) $((\chi \dot{-} \varphi) \dot{-} (\chi \dot{-} \psi)) \dot{-} (\psi \dot{-} \varphi)$
(A3) $(\varphi \dot{-} (\varphi \dot{-} \psi)) \dot{-} (\psi \dot{-} (\psi \dot{-} \varphi))$
(A4) $(\varphi \dot{-} \psi) \dot{-} (\neg\psi \dot{-} \neg\varphi)$
(A5) $\frac{1}{2}\varphi \dot{-} (\varphi \dot{-} \frac{1}{2}\varphi)$
(A6) $(\varphi \dot{-} \frac{1}{2}\varphi) \dot{-} \frac{1}{2}\varphi$.
(A7) $(\sup_x \psi \dot{-} \sup_x \varphi) \dot{-} \sup_x (\psi \dot{-} \varphi)$
(A8) $\varphi[t/x] \dot{-} \sup_x \varphi$ where no variable in t is bound by a quantifier in φ.
(A9) $\sup_x \varphi \dot{-} \varphi$, wherever x is not free in φ.
(A10) $d(x,x)$
(A11) $d(x,y) \dot{-} d(y,x)$
(A12) $(d(x,z) \dot{-} d(x,y)) \dot{-} d(y,z)$
(A13) For each $f \in \mathcal{F}$, each $\epsilon \in (0,1]$, and each $r,q \in \mathcal{D}$ with $r > \epsilon$ and $q < \delta_{f,i}(\epsilon)$, the axiom $(q \dot{-} d(z,w)) \wedge (d\,(f(\bar{x},z,\bar{y}), f(\bar{x},w,\bar{y})) \dot{-} r)$, where $lh(\bar{x}) + lh(\bar{y}) = n_f - 1$.
(A14) For each $P \in \mathcal{R}$, each $\epsilon \in (0,1]$, and each $r,q \in \mathcal{D}$ with $r > \epsilon$ and $q < \delta_{P,i}(\epsilon)$, the axiom $(q \dot{-} d(z,w)) \wedge ((P(\bar{x},z,\bar{y}) \dot{-} P(\bar{x},w,\bar{y})) \dot{-} r)$, where $lh(\bar{x}) + lh(\bar{y}) = n_P - 1$.

Axioms A1–A4 are those of Łukasiewicz propositional logic, and axioms A5–A6 are those of continuous propositional logic. Axioms A7–A9 describe the role of the quantifiers. Axioms A10–A12 guarantee that d is a pseudometric, and axioms A13–A14 guarantee uniform continuity of functions and relations. We write $\Gamma \vdash_Q \varphi$ whenever φ is provable from Γ in continuous first-order logic. Where no confusion is likely, we will write $\Gamma \vdash \varphi$.

3. Probabilisticly Computable Structures

If M is a Turing machine, we write $M^x(n)$ for the result of applying M to input n with oracle x. Excepting the polarity change to match the conventions above, the following definition is standard; it may be found, for instance, in [35].

Definition 3.1. Let 2^ω be the set of infinite binary sequences, with the usual Lebesgue probability measure μ.

(1) A *probabilistic Turing machine* is a Turing machine equipped with an oracle for an element of 2^ω, called the *random bits*, with output in $\{0,1\}$.
(2) We say that a probabilistic Turing machine M *accepts* n *with probability* p if and only if $\mu\{x \in 2^\omega : M^x(n) \downarrow= 0\} = p$.
(3) We say that a probabilistic Turing machine M *rejects* n *with probability* p if and only if $\mu\{x \in 2^\omega : M^x(n) \downarrow= 1\} = p$.

Definition 3.2. Let $\mathcal{L}$ be a computable continuous signature. Let $\mathfrak{M}$ be a continuous $\mathcal{L}$-structure. Let $\mathcal{L}(\mathfrak{M})$ be the expansion of $\mathcal{L}$ by a constant c_m for each $m \in M$ (i.e. a unary predicate $c_m \in \mathcal{R}$ where $c_m^{\mathfrak{M}}(x) := d(x, m)$). Then the *continuous atomic diagram* of $\mathfrak{M}$, written $D(\mathfrak{M})$ is the set of all pairs (φ, p), where φ is a quantifier-free (i.e. sup- and inf-free) sentence in $\mathcal{L}(\mathfrak{M})$ and $\mathfrak{M}(\varphi, \sigma) = p$. The continuous elementary diagram $D^*(\mathfrak{M})$ is the same, except that φ is not required to be quantifier-free.

Note that the definition is independent of σ, since a sentence has no free variables.

Definition 3.3. We say that a continuous pre-structure $\mathfrak{M}$ is *probabilistically computable* (respectively, *probabilistically decidable*) if and only if there is some probabilistic Turing machine T such that, for every pair $(\varphi, p) \in D(\mathfrak{M})$ (respectively, $D^*(\mathfrak{M})$) the machine T accepts φ with probability p.

Suppose T is a deterministic machine (i.e. one that makes no use of its random bits; a classical Turing machine) and $\mathfrak{M}$ a classical first-order structure. Then this definition corresponds exactly to the classical definition of a computable structure.

We cannot do entirely without the probabilistic machines (that is, we cannot thoroughly understand probabilistically computable structures using only classical Turing machines), as the follwoing result shows. Let $\mathcal{D}$ denote the dyadic numbers in the interval (i.e. those of the form $\frac{k}{2^n}$ for $k, n \in \mathbb{N}$).

Lemma 3.4 (No Derandomization Lemma)**.** *There is a probabilistically computable weak structure $\mathfrak{M}$ such that the set $\{(\varphi, p) \in D(\mathfrak{M}) : p \in \mathcal{D}\}$ is not classically computable.*

Proof. Let U be a computably enumerable set, and let S be the complement of U. We first construct a probabilistically computable function f such that

$$P(f^\sigma(x) = 0) = \frac{1}{2}$$

if and only if $x \in S$. Begin with $f_0 = \emptyset$. At stage t, if $x \notin U_t$, pick two strings σ_t, τ_t of length $t + 2$ such that $f_t(x)$ does not halt with random bits σ_t or τ_t. We define the function $f_{t+1} := f_t \cup \{f^{\sigma_t}(x) = 0, f^{\tau_t}(x) = 1\}$. On the other hand, if $x \in U_t$, then we arrange that $f_{t+1}^\sigma(x) = 0$ for all σ of length at most $t + 2$ where $f_t^\sigma(x)$ does not halt. Let $f = \bigcup\limits_{t \in \omega} f_t$. Now if $x \in S$, we never see $x \in U_t$, so $f(x) = 0$ with probability $\frac{1}{2}$. Otherwise, there is some t such that $x \in U_t - U_{t-1}$, and then $f(x) = 0$ with probability $1 - \sum\limits_{i=2}^{t} 2^{-i} > \frac{1}{2}$.

Now we let $\mathfrak{M}$ be the structure (ω, f), where f is interpreted as a unary predicate in the obvious way, and d is the discrete metric. If we could decide membership in $\{(\varphi, p) \in D(\mathfrak{M}) : p \in \mathcal{D}\}$ with a classical Turing machine, then we could also decide membership in U. □

Of course, this same argument could work for any other uniformly computable set of reals in place of $\mathcal{D}$. The following proposition, on the other hand, indicates a sense in which the diagrams of probabilistically computable structures may be approximated by Turing machines.

Proposition 3.5. *For any probabilistically computable pre-structure $\mathfrak{M}$, there is some (classically) computable function f, monotonically increasing in the second* *variable, and some (classically) computable function g, monotonically decreasing in the second variable, such that for any pair $(\varphi, p) \in D(\mathfrak{M})$, we have $\lim\limits_{s\to\infty} f(\varphi, s) = p$ and $\lim\limits_{s\to\infty} g(\varphi, s) = p$.*

Proof. Let $\mathfrak{M}$ be computed by the probabilistic Turing machine $T_{\mathfrak{M}}$. Let $(\sigma_s)_{s\in\omega}$ be an effective list of all strings in $2^{<\omega}$. Now we define

$$f(\varphi, s) := \sum_{i\leq s} \left(T^{\sigma_i}_{\mathfrak{M}}(\varphi) \cdot 2^{-lh(\sigma_i)} \right).$$

The definition of g is symmetric. These clearly have the correct properties. □

Functions similar to f and g are often seen in classical computable model theory [19, 17, 9, 10] (in the characterization of countable Abelian p-groups with classically computable copies, for instance).

Corollary 3.6. *For any probabilistically computable pre-structure $\mathfrak{M}$, the set of pairs, $(\varphi, p) \in D(\mathfrak{M})$ is the complement of a (classically) computably enumerable set.*

Proof. Follows immediately from Proposition 3.5. □

These limitations notwithstanding, the definition via probabilistic machines gives a more natural continuity with the established literature on continuous first-order model theory [2]. In addition, this definition is in any case not dispensable when, for instance, time complexity of computation is at issue (see Section 7).

4. Effective Completeness

Theorem 1.1 is an important piece of evidence that classical Turing computation (or any of the many equivalent concepts) is properly synchronized with classical first-order logic. In particular, it asserts that under the minimal, obviously necessary hypotheses, a classical first-order theory has a model which can be represented by a classical computation. The aim of the present section is to prove a similar result for continuous first-order logic and probabilistic computation. The following analogue to the classical concept of the decidability of a theory was proposed in [3].

Definition 4.1. Let $\mathcal{L}$ be a continuous signature and Γ a set of formulas of $\mathcal{L}$.

(1) We define
$$\varphi^\circ_\Gamma := \sup\{\mathfrak{M}(\varphi, \sigma) : (\mathfrak{M}, \sigma) \models \Gamma\}.$$

(2) If T is a complete continuous first-order theory, we say that T is *decidable* if and only if there is a (classically) computable function f such that $f(\varphi)$ is an index for a computable real number equal to φ°_T.

Theorem 4.2. *Let T be a decidable continuous first-order theory. Then there is a probabilistically decidable continuous pre-structure $\mathfrak{M}$ such that $\mathfrak{M} \models T$.*

Proof. The construction of a model $\mathfrak{M}$ is given in [3], by an analogue of Henkin's method. Our model will be essentially the same, except that some care must be taken with effectiveness. The principal content of the theorem consists in showing that this structure is probabilistically decidable. We will define a probabilistic Turing machine which, for any formula φ, accepts φ with probability $\mathfrak{M}(\varphi)$.

We begin by adding Henkin witnesses.

Definition 4.3. Let Γ be a set of formulae. Then Γ is said to be *Henkin complete* if for every formula φ, every variable x, and every $p < q \in \mathcal{D}$, there is a constant c such that

$$(\sup_x \varphi \dot{-} q) \wedge (p \dot{-} \varphi[c/x]) \in \Gamma.$$

Lemma 4.4. *We can effectively extend T to a consistent set Γ of formulae which is Henkin complete.*

Proof. Let $\mathcal{L}_0 = \mathcal{L}$. For each n, let $\mathcal{L}_{n+1}$ be the result of adding, for each formula φ in $\mathcal{L}_n$, and for each x, p, q as in the previous definition, a new constant $c_{(\varphi,x,p,q)}$. We can also extend the theory T, beginning with $\Gamma_0 = T$. For each n, the set Γ_{n+1} is produced by adding to T, for each formula φ in $\mathcal{L}_n$ and each x, p, q as in the previous definition, the formula $(\sup_x \varphi \dot{-} q) \wedge (p \dot{-} \varphi[c_{(\varphi,x,p,q)}/x])$. Let $\Gamma = \bigcup\limits_n \Gamma_n$. The consistency of Γ is demonstrated in [3].

Note that this construction is in every way effective. In particular, there is a (classically) computable function which will, given $p, q \in \mathcal{D}$ and Gödel numbers for φ and x, give us a Gödel number for $c_{(\varphi,x,p,q)}$. Moreover, the set Γ is (classically) computable. □

We write $\mathcal{L}^* = \bigcup\limits_n \mathcal{L}^n$, and $C = \{c_{(\varphi,x,p,q)}\}$.

Lemma 4.5. *We can effectively extend Γ to a consistent set Δ^0 such that for all formulae φ, ψ in $\mathcal{L}^*$ we have $\varphi \dot{-} \psi \in \Delta^0$ or $\psi \dot{-} \varphi \in \Delta^0$.*

Proof. We set $\Delta_0 = \Gamma$. At stage $s+1$, for each pair ψ, φ of sentences from $\mathcal{L}^*$ such that neither $\psi \dot{-} \varphi$ nor $\varphi \dot{-} \psi$ is in Δ_s, we proceed as follows. Let θ be the conjunction of all elements of Δ_s, and let $\bar{c}$ be the constants from C which occur in $(\psi \dot{-} \varphi) \dot{-} \theta$. We then check (effectively, since the theory is decidable), whether $(\forall \bar{x}\, ((\psi \dot{-} \varphi) \dot{-} \theta)\, (\bar{x}/\bar{c}))^{\circ}_{T} = 0$. If so, then we add $\psi \dot{-} \varphi$ to form Δ_{s+1}. Otherwise, we do so with $\varphi \dot{-} \psi$. Now $\Delta^0 = \bigcup\limits_s \Delta_s$ is as required. That this extension is consistent is established in [3]. □

Definition 4.6. Let Δ be a set of formulas. We say that Δ is *maximal consistent* if Δ is consistent and for all formulae φ, ψ we have

(1) If $\Delta \vdash \varphi \dot{-} 2^{-n}$ for all n, then $\varphi \in \Delta$, and
(2) $\varphi \dot{-} \psi \in \Delta$ or $\psi \dot{-} \varphi \in \Delta$.

Now let $\Delta^0 = \bigcup\limits_s \Delta_s$, and

$$\Lambda = \{\varphi : \forall n[\Delta^0 \vdash \varphi \dot{-} 2^{-n}]\}.$$

Now $\Delta = \Delta^0 \cup \Lambda$ is maximal consistent, by construction of Δ^0. Let $\mathfrak{M}$ be the model of T whose universe is the set of closed terms in C, as in [3].

We now define the probabilistic Turing machine G which will witness that $\mathfrak{M}$ is probabilistically computable. We set $K^A_0 = K^R_0 = A_0 = R_0 = \emptyset$. We define the functions $E(S) = \{\sigma \supseteq \tau : \tau \in S\}$ and

$$P(S) = \sum_{\sigma \in S} \frac{1}{2^{lh(a)}}.$$

At stage s, if $\Delta_s \vdash \varphi \dot{-} \frac{k}{2^n}$, then we will arrange that G accepts φ with probability at least $1 - \frac{k}{2^n}$. If $K^A_s = \emptyset$, then we find $2^n - k$ nodes $\sigma_1, \ldots, \sigma_{2^n - k}$ of length

n in $2^{<\omega} - E(K_s^R)$, and let $K_{s+1}^A = \{\sigma_1, \dots, \sigma_{2^n-k}\}$. If K_s^A is nonempty and $P(K_s^A) \geq 1 - \frac{k}{2^n}$, then we do nothing with K^A. If K_s^A is nonempty and $P(K_s^A) < 1 - \frac{k}{2^n}$, then we find some set Σ of elements of $2^{<\omega} - E(K_s^R)$ with length n so that $P(K_s^A \cup \Sigma) = 1 - \frac{k}{2^n}$, and let $K_{s+1}^A = K_s^A \cup \Sigma$.

If $\Delta_s \vdash \frac{k}{2^n} \dot{-} \varphi$ then we will arrange that G rejects φ with probability at least $\frac{k}{2^n}$. If $K_s^R = \emptyset$, then we find k nodes $\sigma_1, \dots, \sigma_k$ of length n in $2^{<\omega} - E(K_s^A)$, and let $K_{s+1}^R = \{\sigma_1, \dots, \sigma_k\}$. If K_s^R is nonempty and $P(K_s^R) \geq \frac{k}{2^n}$, then we do nothing with K^R. If K_s^R is nonempty and $P(K_s^R) < \frac{k}{2^n}$, then we find some set Σ of elements of $2^{<\omega} - E(K_s^A)$ with length n so that $P(K_s^R \cup \Sigma) = \frac{k}{2^n}$, and let $K_{s+1}^R = K_s^R \cup \Sigma$.

At this point, it is necessary to verify that certain aspects of the construction described so far are actually possible. In particular, we need to show that when we search for elements of $2^{<\omega} - E(K_s^A)$, for instance, there will be some. Now if $E(K_s^A)$ contains more than $2^n - k_1$ elements, we must have $P(K_s^A) < 1 - \frac{k_1}{2^n}$, so that we must have had $\Delta_s \vdash \varphi \dot{-} \frac{k_1}{2^n}$. (Note that if $\Delta_s \vdash \varphi \dot{-} p$ and $q > p$, then also $\Delta_s \vdash \varphi \dot{-} q$.)

Lemma 4.7. *If there is some s such that $\Delta_s \vdash \varphi \dot{-} \frac{k_1}{2^n}$ and $\Delta_s \vdash \frac{k}{2^n} \dot{-} \varphi$, then $(1 - \frac{k_1}{2^n}) + \frac{k}{2^n} \leq 1$.*

Proof. Suppose not. Then $2^n - k_1 + k > 1$, so that $k - k_1 > 0$ and $k > k_1$. However, we also have $\frac{k}{2^n} \dot{-} \frac{k_1}{2^n} = 0$, so that $k_1 \geq k$, a contradiction. □

The situation for finding elements of $2^{<\omega} - E(K_s^R)$ is symmetric.

Returning to the construction, at stage s, we will add more instructions. We will guarantee that for any $\sigma \in E(K_s^A)$, we will have $G^\sigma(\varphi) \downarrow = 0$, and for any $\sigma \in E(K_s^R)$ we will have $G^\sigma(\varphi) \downarrow = 1$.

Let φ be a sentence in $\mathcal{L}^*$, and suppose $\mathfrak{M}(\varphi) = p$. We need to show that G accepts φ with probability p. Since Δ is maximal consistent, for each $q_0, q_1 \in \mathcal{D}$ with $q_0 \leq \mathfrak{M}(\varphi) \leq q_1$, there was some s for which $\Delta_s \vdash \varphi \dot{-} q_1$ and for which $\Delta_s \vdash q_0 \dot{-} \varphi$, and at that stage, we ensured that G would accept φ with probability between q_0 and q_1. Since this is true for all $q_0 \leq p \leq q_1 \in \mathcal{D}$, it must follow that G accepts φ with probability p.

□

We can strengthen Theorem 4.2 to produce a continuous weak structure if we require T to be *complete*.

Definition 4.8. Let $\mathfrak{M}$ be a continuous $\mathcal{L}$-structure. We write $Th(\mathfrak{M})$ for the set of continuous $\mathcal{L}$-sentences φ such that $\mathfrak{M}(\varphi) = 0$. We say that T is *complete* if $T = Th(\mathfrak{M})$ for some $\mathfrak{M}$.

Corollary 4.9. *Let T be a complete decidable continuous first-order theory. Then there is a probabilistically decidable weak structure $\mathfrak{M}$ such that $\mathfrak{M} \models T$.*

Proof. If the signature has no metric, then Theorem 4.2 suffices. Otherwise, we note that T must contain the sentence $\sup\limits_{x,y} ((x = y) \dot{-} d(x, y))$, so that when we apply Theorem 4.2, the function $d^{\mathfrak{M}}$ is a metric on $\mathfrak{M}$. □

5. Probabilistically Effective Mathematics

In the present section, we will show, as a consequence of the effective completeness theorem, that "Probabilistically Computable Mathematics" — that is, the part of mathematics that can be carried out on probabilistically computable structures — is quite a lot more comprehensive than traditional effective mathematics. One key ingredient in the proof is the method of proof in Lemma 3.4. Another is the effective completeness theorem of the previous section. The third ingredient, to which we will turn in the following subsection, is the body of work known as "Reverse Mathematics."

5.1. **Some Relevant Reverse Mathematics.** The name "Reverse Mathematics" refers to a program, originating in work of Friedman, Simpson, and Smith [14] and later treated at length in Simpson's monograph [33] and the collection [34], which sought to classify mathematical theorems by the amount of "comprehension" necessary to prove them. The Simpson book [33] is the canonical reference for all of the material in this subsection. One represents all structures and all functions between them over a ground structure which will satisfy some fragment of second-order arithmetic. Typically, one tries to prove a familiar theorem (e.g. the Brouwer Fixed Point Theorem) in the smallest possible fragment of second-order arithmetic, and then proves that a set of axioms for that fragment is derivable from the theorem itself. It is for this second part of the practice that reverse mathematics is named.

The system RCA_0 is the fragment of second-order arithmetic axiomatized by the Peano axioms (excepting induction), induction on Σ^0_1 formulas, and a comprehension axiom stipulating that all Δ^0_1 sets exist (i.e. they are represented by an element in the "sets" sort — the second order sort — of the model of arithmetic). The mathematical statements which may be proved in RCA_0 are those which are effectively true, in the traditional sense. The Baire category theorem, the intermediate value theorem, Urysohn's lemma, the existence of an algebraic closure of a field, and the contraction mapping theorem are all provable in RCA_0.

The slightly stronger system WKL_0 consists of the axioms of RCA_0, with the additional axiom that every binary-branching tree has a path (the so-called "weak König lemma"). This additional axiom, guaranteeing the existence of many more sets, allows a much broader set of mathematical statements to be proved, as the following result demonstrates. Moreover, each of the theorems listed could be added to $\mathsf{RCA}_0$with identical results: each of them, when added to RCA_0, is equivalent to WKL_0. This list is wildly incomplete, and should primarily serve to exemplify the type of result which is possible. I have made no effort to credit the original sources of these results, as this information has been exhaustively documented in [33], from which this result is extracted.

Proposition 5.1. *Under the axioms of* RCA_0*, the following are equivalent:*

(1) WKL_0
(2) *The Heine–Borel theorem*
(3) *Every continuous real-valued function on a compact metric space has a supremum*
(4) *The local existence theorem for solutions of finite systems of ordinary differential equations*
(5) *Every countable field of characteristic 0 has a unique algebraic closure*
(6) *Brouwer's fixed point theorem.*

The third and final system which will concern us here is ACA_0, which consists of the axioms of RCA_0, plus the "arithmetic comprehension axiom", which guarantees the existence of all arithmetic sets (including, for instance, the Turing jump of any set in the model). Again, I extract the following summary from [33], and refer the reader there for the full history of these results.

Proposition 5.2. *Under the axioms of* RCA_0*, the following are equivalent:*

(1) ACA_0
(2) *the Bolzano-Weierstrass Theorem*
(3) *Every Cauchy sequence of real numbers is convergent*
(4) *Every countable field is isomorphic to a subfield of a countable algebraically closed field*
(5) *Every countable vector space over* $\mathbb{Q}$ *has a basis.*

Finally, and most importantly, Weak König's Lemma is provable in ACA_0, so that every model of ACA_0 is a model, too, of WKL_0.

5.2. **A Model of** ACA_0**.** We will show that the natural numbers with their usual first-order operations, together with the family of sets X for which there is some probabilistically computable structure $\mathcal{M}$ with universe $\mathbb{N}$ in which X is quantifier-free definable (i.e. X there is some continuous first-order formula φ such that X is the locus of all x such that $\mathcal{M}(\varphi(x)) = 0$), is a model of ACA_0. This will show that, among probabilistically computable structures, all of the results listed in Propositions 5.2 and 5.1 hold, in addition to those which are provable in RCA_0 (those which are true among classically computable structures). Consider the family $\mathcal{PC}$ of sets A of pairs (x, p) such that there is a probabilistic Turing machine, depending only on A, which will accept x with probability p.

Proposition 5.3. *The class* $\mathcal{PC}$ *is closed under the Turing jump.*

Proof. Let U be a Π^0_1 subset of W, where $W \in \mathcal{PC}$ (say that Φ is the Turing machine witnessing $W \in \mathcal{PC}$). Then U has a definition of the form

$$\forall y \ R((x, p), y).$$

Since the real numbers p must be uniformly computable, there are computable sequences $(q_{x\ell t})_{t\in\omega}$ and $(q_{xut})_{t\in\omega}$ of rationals such that $q_{\ell t}$ is strictly increasing with limit p and q_{ut} is strictly decreasing with limit p, and such that both converge faster than 2^{-t}.

We will construct a decidable CFO theory T_U describing a weak structure with two relations, $\hat{x}$ and $\hat{x}_1$ for each x which occurs as the first coordinate of an element (x, p) of W, such that $(\hat{x} \dot{-} \hat{x}_1) \wedge (\hat{x}_1 \dot{-} \hat{x})$ if and only if $(x, p) \in U$. Then, by Theorem 4.9, there will be a probabilistically computable weak structure satisfying T_U, in which U is defined by a quantifier-free formula. Thus, we will have $U \in \mathcal{PC}$.

We will work in a continuous signature with two unary relation symbols, $\hat{x}$ and $\hat{x}_1$, for each element x with some pair $(x, p) \in W$. Let $T_{U,0} = \emptyset$. At stage t, for each $x \leq t$, if $\Phi_t(x) \downarrow = 0$ with probability at least $q_{x\ell t}$ and for all $y \leq t$ we have $R((x, p), y)$, then we will include $q_{x\ell t} \dot{-} \hat{x}_1$ in $T_{U,t+1}$. If $\Phi_t(x) \downarrow = 1$ with probability at least $1 - q_{x\ell t}$ and for all $y \leq t$ we have $R((x, p), y)$, then we will include $\hat{x}_1 \dot{-} q_{x\ell t}$ in $T_{U,t+1}$. Meanwhile, we also include $q_{x\ell t} \dot{-} \hat{x}$, $\hat{x} \dot{-} q_{xut}$, and $\hat{x}_1 \dot{-} q_{xut}$. Let T_U be the union of the $T_{U,t}$'s.

Now T_U is decidable since $\hat{x}^\circ_T$ and $(\hat{x}_1)^\circ_T$, where x ranges over all first coordinates of W, must be uniformly computable. Thus, there is a probabilistically decidable weak structure $\mathcal{M}_U \models T_U$. Now for any $(x, p) \in W$, we have $(x, p) \in U$ if and only if $(\hat{x} \dot{-} \hat{x}_1) \wedge (\hat{x}_1 \dot{-} \hat{x})$, as required. □

Theorem 5.4. *Let $\mathcal{N}$ be the structure whose first-order part is* $(\mathbb{N}, +, \cdot, 0, 1)$*, and whose second order part consists of the sets X such that there exists some probabilistically computable structure $\mathcal{M}$ with universe $\mathbb{N}$ such that X is quantifier-free definable in $\mathcal{M}$. Then $\mathcal{N}$ is a model of* ACA_0.

Proof. It is clear that $\mathcal{N}$ satisfies the first-order Peano axioms. Moreover, recursive comprehension is satisfied, since we may define any Δ^0_1 subset by a quantifier-free formula. It remains to show that the second-order universe of $\mathcal{N}$ is closed under the Turing jump.

Let S be an infinite set in the second-order part of $\mathcal{N}$, defined by the quantifier-free continuous formula φ in $\mathcal{M}$ (if it is not infinite, we may replace it by a Turing-equivalent infinite set). Now S' is defined by $\{x : \Phi^S_x(x) \downarrow\}$, or, equivalently,

$$\{x : \exists t\ \Phi^{S \upharpoonright t}_{x,t}(x) \downarrow\}.$$

This set is 1-equivalent to a Σ^0_1 subset of S, and thus to a Σ^0_1 subset T of $D(\mathcal{M})$. Then, by Proposition 5.3, the complement of T is quantifier-free definable in a probabilistically computable structure on $\mathbb{N}$, and so both T and the complement of T are in the second-order part of $\mathcal{N}$. □

6. Examples

A full treatment of each of the following classes of examples suggests a paper — or many papers — of its own. However, in each case some suggestion is given of the kind of data given by the assumption that an element of the class is probabilistically computable.

It is perhaps useful at this point to comment on some other work in computable analysis that bears at least a superficial resemblance to the work of this paper. Ko [20] and Bosserhoff [7] have both investigated probabilistic computability of real-valued functions. Ko defined a real-valued function to be of class BPP_{RF}, roughly, if a probabilistic machine, executing in polynomial time, computed the value of the function, having errors which are bounded with high probability. Bosserhoff described three notions of probabilistic computability: computability except perhaps on a measure-zero set, Ko's model, and computability in the mean. Bosserhoff's context was most like the present one, in that the functions were viewed as having domains on computably presented (in the sense of the so-called "type-2 effectiveness" described, for instance, in [36]) metric spaces.

There have, to be sure, been many approaches to computable analysis. Work of Weihrauch [36], Brattka [8], and many others has used type-2 effectiveness, a model in which, very roughly, Turing machines compute functions by rational approximation. Pour-el and Richards (and others) have taken a more axiomatic approach [28], in which, for a given Banach space $\mathcal{X}$, one axiomatizes the notion of a computable sequence of points in $\mathcal{X}$. Other methods abound.

The use of probabilistically computable structures treated in continuous first-order logic comes through Theorem 4.9: The computability of various functions is now tied to a logic specifying their behavior. One family of applications of this comes, as we will see, through Theorem 5.4, but it is reasonable to expect others.

6.1. **Hilbert Spaces.** A pre-Hilbert space over a topological field F is a vector space with an inner product meeting all requirements of being a Hilbert space except perhaps that it may not be complete with respect to the norm. The authors of [2] identify a pre-Hilbert space H with the many-sorted weak structure

$$\mathcal{M}(H) = \left((B_n(H) : n \geq 1), 0, \{I_{mn}\}_{m<n}, \{\lambda_r\}_{r\in F}, +, -, \langle\cdot,\cdot\rangle\right)$$

where $B_n(H)$ is the closed ball of radius n, the map I_{mn} is inclusion of B_m in B_n, each λ_r is a scaling function, $+$ and $-$ are the standard vector operations, and $\langle\cdot,\cdot\rangle$ is the inner product. We also write $||x||$ for $\sqrt{\langle x, x\rangle}$, and the structure has a metric given by $d(x, y) = ||x - y||$. Of course, the normal case is to let $F = \mathbb{R}$, but this is not necessary. Now the pre-Hilbert space H is clearly a continuous weak structure in the obvious signature. A true Hilbert space is a continuous structure.

Theorem 6.1 ([2]). *There is a continuous first order theory, IHS, such that the following hold:*

1. *IHS is (classically) computably axiomatized*
2. *IHS is complete*
3. *Any two models of IHS with the same infinite cardinality are isomorphic.*
4. *The continuous first-order structures $\mathcal{M}$ that satisfy IHS are exactly the infinite-dimensional Hilbert spaces.*
5. *IHS admits quantifier elimination.*
6. *IHS is ω-stable.*

Since IHS is computably axiomatizable and complete, it must also be decidable. Consequently, Theorem 4.9 shows that there must exist some probabilistically computable weak structure satisfying IHS. Clearly one challenge of handling Hilbert spaces from a computational viewpoint is the essential uncountability of a true Hilbert space. However, computational scientists are generally undaunted by this feature, being satisfied with approximations in place of true limits of Cauchy sequences. We will adopt a similar approach. The following result is well known (see [22] for a proof).

Lemma 6.2. *For any p, the space $L^p(\mathbb{R})$ is separable (i.e. has a countable dense subset).*

Let F be a countable topological field dense in $\mathbb{R}$, let H be a separable Hilbert space over the reals, and let D be a countable dense subspace of H. We will write H^F for the restriction of D to the language which includes scalars only from F. It is well known that H must have a countable orthonormal basis (see, for instance, [29]).

Proposition 6.3. *If H^F is probabilistically computable, then there is a probabilistic Turing machine which will, given a probabilistically computable countable basis for H^F, produce a probabilistically computable orthonormal basis for H^F.*

Proof. The proof is precisely an implementation of the Gram–Schmidt process. Let $(u_i)_{i\in\omega}$ be a probabilistically computable countable basis. Set $v_1 := u_1$. For $s \geq 2$, at stage s, we set

$$v_s := u_s - \sum_{i=1}^{s-1} \frac{\langle u_s, v_i\rangle}{||v_i||}.$$

Now $(v_i)_{i\in\omega}$ is an orthogonal basis for H^F. We can normalize to an orthonormal basis $(\tilde{v}_i)_{i\in\omega}$ by setting $\tilde{v}_i := \frac{v_i}{||v_i||}$. □

6.2. **Banach Spaces and Banach Lattices.** Certainly, the framework of Section 6.1 is sufficient, without the inner product, to account for any normed vector space as a continuous pre-structure (and thus any Banach space as a continuous structure).

One also sometimes sees some Banach spaces with the additional structure of a lattice included. In such a structure, $f \vee g$ is the pointwise minimum of f and g, and $f \wedge g$ is the pointwise maximum. Such an approach is taken in [32, 23] and also in [2].

Fixed point theorems for operators on Banach spaces or appropriate subsets of them are an important technique for many non-linear differential equations [13, 15, 30, 29]. It is well-known that the classical Brouwer fixed point theorem is not effectively true (that is, roughly, if the convex hull C of a nonempty finite set of points in $\mathbb{R}^n$ and a continuous function $f : C \to C$ are given in a computable way, there may still be no algorithm to find a fixed point for f; see [1]). However, the probabilistically computable context is nearer to that of classical (non-effective) mathematics in this sense.

Proposition 6.4 (Probabilistically Effective Brouwer Fixed Point Theorem)**.** *Suppose that the convex hull of a nonempty finite set of points is defined by a quantifier-free continuous formula in a probabilistically computable structure $\mathcal{M}$. Then every continuous function which is quantifier-free definable in $\mathcal{M}$ has a fixed point $\hat{x}$. Further, the expansion of $\mathcal{M}$ to include a predicate for $\hat{x}$ is also probabilistically computable, uniformly in $\mathcal{M}, C$, and f.*

Proof. Given Theorem 5.4, the result follows directly from Theorem IV.7.6 of [33]. □

This shows that weak solutions to certain differential equations can be found in probabilistically computable structures [13]. There has been extensive work, especially by Weihrauch and Zhong [38, 37] in showing that solutions to some equations are computable in the type-2 framework. However, the improvement in the fixed point theorems provable (from Banach's to Brouwer's and Schauder's — on the latter, see Theorem IV.7.9 of [33]) should considerably improve the range of equations that can be effectively solved.

6.3. **Probability Spaces.** Let $\mathcal{X} = (X, \mathcal{B}, \mu)$ be a probability space. We say that $B \in \mathcal{B}$ is an *atom* if $\mu(B) > 0$ and there is no $B' \in \mathcal{B}$ with $B' \subseteq B$ and $0 < \mu(B') < \mu(B)$. We say that $\mathcal{X}$ is atomless if and only if $\mathcal{B}$ contains no atoms. Let $\hat{\mathcal{B}}$ be the quotient of $\mathcal{B}$ by the relation $B_1 \sim B_2$ if and only if $\mu(B_1 \triangle B_2) = 0$. The authors of [2] identified $\mathcal{X}$ with the structure

$$\left(\hat{\mathcal{B}}, 0, 1, \cdot^c, \cap, \cup, \mu\right)$$

with the metric $d(A, B) = \mu(A \triangle B)$.

Theorem 6.5 ([2])**.** *There is a continuous first-order theory APA such that*

1. *APA is finitely axiomatizable.*
2. *APA is complete.*
3. *APA admits quantifier elimination.*
4. *The continuous pre-structures satisfying APA are exactly the atomless probability spaces, represented as above.*

Since APA is finitely axiomatizable and complete, it is also decidable. Thus, Theorem 4.9 gives us a probabilistically decidable model. Of course, any separable probability structure can be approximated by a countable dense set.

Müller [26] has described probability spaces from the perspective of type-2 effectiveness. The present treatment likely offers improvements, at least due to Theorem 5.4.

A standard issue in effective model theory is whether two isomorphic structures must be isomorphic via a computable function. The following result shows that the answer for probability structures is affirmative.

Proposition 6.6. *Let $\mathfrak{B}$ and $\mathfrak{C}$ be isomorphic, probabilistically computable atomless probability structures with universes $\hat{\mathcal{B}}$ and $\hat{\mathcal{C}}$, respectively. Then there is a (classically) computable function witnessing the isomorphism.*

Proof. The isomorphism is constructed by a standard back-and-forth argument. Suppose that $f : \mathfrak{B} \to \mathfrak{C}$ is a finite partial isomorphism, and that $x \in \mathcal{B} - dom(f)$. We wish to find some $y \in \mathcal{C}$ such that $f \cup \{(x, y)\}$ is still a partial isomorphism. Without loss of generality, we may assume that x is not in the substructure of $\mathfrak{B}$ generated by $dom(f)$. Let $a_0, \dots, a_n$ be the atoms of the substructure of $\mathfrak{B}$ generated by $dom(f)$. We may assume, without loss of generality, that each a_i is in $dom(f)$. Now the isomorphism type of x is determined by the values $\mu(x \cap a_i)$. Since $\mathcal{B}$ is atomless, there is an element $y \in \hat{\mathcal{C}}$ such that for each i we have $\mu^{\mathfrak{B}}(x \cap a_i) = \mu^{\mathfrak{C}}(y \cap f(a_i))$, and since $\mathfrak{B}$ and $\mathfrak{C}$ are probabilistically computable, we can effectively find this y. The extension to a new element of $\mathfrak{C}$ is entirely symmetric. The union of the partial isomorphisms constructed in this way will be a computable function, and will be an isomorphism from $\mathfrak{B}$ to $\mathfrak{C}$. □

6.4. **Probability Spaces with a Distinguished Automorphism.** A standard sort of enrichment in stability theory is to expand a known structure by adding a new function symbol to define a new function, and to specify that this function be generic. Fix an interval I under the Lebesgue measure λ, and let $\mathfrak{L}$ be the algebra of measurable sets. Let G denote the group of measure preserving automorphisms of $(I, \mathfrak{L}, \lambda)$, modulo the relation of almost everywhere agreement. Let $\tau \in G$. Now τ induces an automorphism on $(\hat{L}, 0, 1, \cdot^c, \cap, \cup, \lambda)$ in a straightforward way (see [5, 2]). We say that $\tau \in G$ is *aperiodic* if for every positive integer n we have

$$\lambda\{x \in I : \tau^n(x) = x\} = 0.$$

To have a countable structure of this type, we could take a countable dense subset $I' \subseteq I$, and for $X \subseteq I'$, set $\lambda(X) = \lambda(cl(X))$.

In [5] and [2], an axiomatization is given for the theory of atomless probability spaces with a distinguished aperiodic automorphism. This theory is complete and admits elimination of quantifiers. The authors of [5] show that entropy arises as a model-theoretic rank.

The result below partially describes the degree of algorithmic control we can expect on iterations of such an automorphism. Before stating the result, though, a probabilistic analogue to computable enumerability should be given:

Definition 6.7. We say that a set is probabilistically computably enumerable if and only if there is some probabilistic Turing machine M such that

- If $x \in S$, then for any $q < 1$ the machine M accepts x with probability at least q, and

- If $x \notin S$, then there is some $q < 1$ such that M accepts x with probability at most q.

In particular (and especially in light of the time complexity considerations in Section 7), if we specify an error tolerance q, there is some s such that $M(s, x)$ is below q whenever $x \in S$, and (assuming the tolerance is sufficiently small) no such s otherwise.

Theorem 6.8. *Let $\mathcal{I} = (\hat{L}, 0, 1, \cdot^c, \cap, \cup, \lambda, \tau)$ be a probabilistically computable probability structure based on a dense subset of the unit interval, with a measure-preserving transformation τ. Let $A \subseteq I$ be a set of positive measure, defined without quantifiers in continuous first-order logic. Write $\mathfrak{A}$ for the set $\bigcup\limits_{n\in\omega} \tau^n(A)$. Then for any isomorphism $f : \mathcal{I} \to \mathcal{J}$ to a probabilistically computable structure $\mathcal{J}$, the set $f(\mathfrak{A})$ is probabilistically computably enumerable.*

Proof. Toward part 1, note that $\mathfrak{A}$ is defined by the infinitary disjunction

$$\varphi(x) = \bigvee_{n\in\omega} \tau^{-n}(x) \in \mathcal{A}$$

and that the set $\mathcal{A}$ is defined by a quantifier-free continuous first-order formula. The isomorphism f must preserve satisfaction of φ — that is, $\mathcal{I} \models \varphi(x)$ if and only if $\mathcal{J} \models \varphi(f(x))$. Now let M be a probabilistic Turing machine such that $M(x, s)$ is the minimum value of $\bigwedge\limits_{n\leq k} \tau^{-n}(x) \in \mathcal{A}$, where k ranges over all numbers less than or equal to s. Then M witnesses that $f(\mathfrak{A})$ is probabilistically computably enumerable. □

7. Time Complexity of Structures

One of the most important applications of probabilistic Turing machines is their role in computational complexity theory (see [21, 27, 18]). Let P be some decision problem. We say that Q is of class RP if and only if there is a probabilistic Turing machine M_Q, halting in time polynomial in the length of the input, such that if $x \in Q$, then M_Q accepts x with probability at least $\frac{3}{4}$, and if $x \notin Q$, then M_Q rejects x with probability 1. This class has the property that $\mathsf{P} \subseteq \mathsf{RP} \subseteq \mathsf{NP}$. [1]

Another complexity class of interest is the class BPP. We say that Q is of class BPP if and only if there is a probabilistic Turing machine M_Q, halting in time polynomial in the length of the input, such that if $x \in Q$, then M_Q accepts x with probability at least $\frac{3}{4}$, and if $x \notin Q$, then M_Q rejects x with probability at least $\frac{3}{4}$. Here we know that $\mathsf{RP} \subseteq \mathsf{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$.

Definition 7.1 (Cenzer–Remmel [11])**.** Let $\mathcal{A}$ be a computable structure. We say that $\mathcal{A}$ is uniformly polynomial time if the atomic diagram of $\mathcal{A}$ is a polynomial time set.

Clearly, $A \in \mathsf{P}$ if and only if the structure (ω, A) is polynomial time. Also, for any polynomial time structure $\mathfrak{M}$ and any quantifier-free definable $A \subseteq \mathfrak{M}^n$, we have $A \in \mathsf{P}$. We can extend Definition 7.1 in a routine way for probabilistically computable structures.

[1] In both this and the succeeding paragraph, the particular fraction $\frac{3}{4}$ is not critical. Using a so-called "Amplification Lemma," any fraction above and bounded away from $\frac{1}{2}$ will do [35].

Definition 7.2. We say that a probabilistically computable structure is polynomial time if and only if there is some probabilistic Turing machine T such that, for every pair $(\varphi, p) \in D(\mathfrak{M})$ the machine T halts in polynomial time and accepts φ with probability p.

Now we can characterize the members of BPP in terms of continuous weak structures.

Theorem 7.3. *The class* BPP *can be identified with the class of quantifier-free definable sets in polynomial time probabilistically computable structures in the following way:*

1. *Let $A \in \mathsf{BPP}$ be a subset of ω. Then there is a polynomial time probabilistically computable weak structure $\mathfrak{M}$ and a polynomial time computable function $f : \omega \to \mathfrak{M}$ such that there is a quantifier-free formula $\varphi(x)$ such that $\varphi(x) \leq \frac{1}{4}$ for $x \in f(A)$ and $\varphi(x) \geq \frac{3}{4}$ for $x \in \mathfrak{M} - f(A)$.*
2. *Let $\mathfrak{M}$ be a polynomial time probabilistically computable weak structure, and let A, B be quantifier-free disjoint definable subsets of $\mathfrak{M}^n$, where*
$$\inf \{d(x, y) : x \in A, y \in B\} > 0$$
and $A \cup B$ is classically computably enumerable. Then A and B are each of class BPP.

Proof. Toward the first point, let M be a probabilistic Turing machine witnessing that $A \in \mathsf{BPP}$. We let $\mathfrak{M}$ be the structure $(\omega, \mathcal{A})$, where $\mathcal{A}$ is a unary predicate and $\mathcal{A}(x)$ is the probability that M accepts x. We give $\mathfrak{M}$ the discrete metric.

For the second point, let A be defined by $\varphi(\bar{x})$, and B by $\psi(\bar{x})$. Now for $\bar{a} \in A \cup B$, to check whether $\bar{a} \in A$, we compute $\mathfrak{M}(\varphi(\bar{a}) \dot{-} \psi(\bar{a}))$. The computation runs in polynomial time, and $\bar{a}$ is accepted with probability at least $\frac{1}{2} + \inf \{d(\bar{a}, y) : y \in B\}$ when $\bar{a} \in A$ and with probability at most $\frac{1}{2} - \inf \{d(\bar{a}, y) : y \in B\}$ when $\bar{a} \in B$. □

References

1. M. J. Beeson, *Foundations of constructive mathematics*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3rd series, vol. 6, Springer, 1985.
2. I. Ben Yaacov, A. Berenstein, C. W. Henson, and A. Usvyatsov, *Model theory for metric structures*, To appear in a Newton Institute volume in the Lecture Notes series of the London Mathematical Society, 2007.
3. I. Ben Yaacov and A. P. Pedersen, *A proof of completeness for continuous first-order logic*, preprint, 2008.
4. I. Ben Yaacov and A. Usvyatsov, *Continuous first order logic and local stability*, to appear in *Transactions of the American Mathematical Society*, 2008.
5. A. Berenstein and C. W. Henson, *Model theory of probability spaces with an automorphism*, preprint, 2004.
6. J.-C. Birget, A. Yu. Ol'shanskii, E. Rips, and M. V. Sapir, *Isoperimetric functions of groups and computational complexity of the word problem*, Annals of Mathematics (2) **156** (2002), 467–518.
7. V. Bosserhoff, *Notions of probabilistic computability on represented spaces*, Journal of Universal Computer Science **14** (2008), 956–995.
8. V. Brattka, *Computability of banach space principles*, Tech. report, Informatik, FernUniversität Hagen, 2001.
9. W. Calvert, D. Cenzer, V. S. Harizanov, and A. Morozov, *Effective categoricity of equivalence structures*, Annals of Pure and Applied Logic **141** (2006), 61–78.
10. ———, *Effective categoricity of Abelian p-groups*, Accepted for publication in *Annals of Pure and Applied Logic*, 2008.

11. D. Cenzer and J. B. Remmel, *Complexity theoretic model theory and algebra*, Handbook of Recursive Mathematics (Yu. L. Ershov, S. S. Goncharov, A. Nerode, and J. B. Remmel, eds.), vol. 1, Studies in Logic and the Foundations of Mathematics, no. 138, North-Holland, 1998, pp. 381–513.
12. M. Dehn, *Über die Topologie des dreidimensionalen Raumes*, Matematische Annalen **69** (1910), 137–168.
13. L. C. Evans, *Partial differential equations*, Graduate Studies in Mathematics, no. 19, American Mathematical Society, 1998.
14. H. Friedman, S. G. Simpson, and R. Smith, *Countable algebra and set existence axioms*, Annals of Pure and Applied Logic **25** (1983), 141–181.
15. D. Gilbarg and N. S. Trudinger, *Elliptic partial differential equations of second order*, Gurndlehren der mathematischen Wissenschaften, no. 224, Springer, 1977.
16. V. S. Harizanov, *Pure computable model theory*, Handbook of Recursive Mathematics (Yu. L. Ershov, S. S. Goncharov, A. Nerode, and J. B. Remmel, eds.), vol. 1, Studies in Logic and the Foundations of Mathematics, no. 138, North-Holland, 1998, pp. 3–114.
17. D. R. Hirschfeldt, R. Miller, and S. Podsorov, *Order-computable sets*, Preprint, 2006.
18. R. Impagliazzo and W. Wigderson, $\mathsf{BPP} = \mathsf{P}$ *if E requires exponential circuits: derandomizing the* XOR *lemma*, Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, El Paso, Texas, ACM, 1997, pp. 220–229.
19. N. G. Khisamiev, *Constructive Abelian groups*, Handbook of Recursive Mathematics (Yu. L. Ershov, S. S. Goncharov, A. Nerode, and J. B. Remmel, eds.), vol. 2, Studies in Logic and the Foundations of Mathematics, no. 139, North-Holland, 1998, pp. 1177–1231.
20. K.-I. Ko, *Approximation ot measurable functions and its relation to probabilistic computation*, Annals of Pure and Applied Logic **30** (1986), 173–200.
21. D. C. Kozen, *Theory of computation*, Springer, 2006.
22. E. H. Lieb and M. Loss, *Analysis*, 2 ed., Graduate Studies in Mathematics, no. 14, American Mathematical Society, 2001.
23. J. Lindenstrauss and L. Tzafriri, *Classical banach spaces II: Function spaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 97, Springer, 1979.
24. Yu. Matiyasevich, *Hilbert's tenth problem: What was done and what is to be done*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (J. Denef, L. Lipshitz, T. Pheidas, and J. Van Geel, eds.), Contemporary Mathematics, vol. 270, American Mathematical Society, 2000, pp. 1–47.
25. T. S. Millar, *Foundations of recursive model theory*, Annals of Mathematical Logic **13** (1978), 45–72.
26. N. Muller, *Computability on random variables*, Theoretical Computer Science **219** (1999), 287–299.
27. C. H. Papadimitriou, *Computational complexity*, Addison-Wesley, 1994.
28. M. Pour-El and J. I. Richards, *Computability in analysis and physics*, Perspectives in Mathematical Logic, Springer, 1989.
29. M. Reed and B. Simon, *Methods of modern mathematical physics I: Functional analysis*, Academic Press, 1972.
30. T. L. Saaty and J. Bram, *Nonlinear mathematics*, International Series in Pure and Applied Mathematics, McGraw-Hill, 1964.
31. M. V. Sapir, J.-C. Birget, and E. Rips, *Isoperimetric and isodiametric functions of groups*, Annals of Mathematics (2) **156** (2002), 345–466.
32. H. H. Schaefer, *Banach lattices and positive operators*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, vol. 215, Springer, 1974.
33. S. G. Simpson, *Subsystems of second order arithmetic*, Perspectives in Mathematical Logic, Springer, 1999.
34. S. G. Simpson (ed.), *Reverse mathematics 2001*, Lecture Notes in Logic, no. 21, AK Peters, 2005.
35. M. Sipser, *Introduction to the theory of computation*, 2 ed., Thomson, 2006.
36. K. Weihrauch, *Computable analysis*, Texts in Theoretical Computer Science, Springer, 2000.
37. K. Weihrauch and N. Zhong, *Computable analysis of the abstract Cauchy problem in a Banach space and its applications I*, Mathematical Logic Quarterly **53** (2007), 511–531.
38. N. Zhong, *Computable analysis of a boundary-value problem for the Korteweg-de Vries equation*, Theory of Computing Systems **41** (2007), 155–175.

Department of Mathematics & Statistics, Faculty Hall 6C, Murray State University, Murray, Kentucky 42071

E-mail address: wesley.calvert@murraystate.edu