Gauging the complexity of mathematical theorems

Stephen G. Simpson, Pennsylvania State University

http://www.math.psu.edu/simpson/

simpson@math.psu.edu

Online Logic Seminar, Moscow State University

October 29, 2014

Abstract. Mathematical logic provides several frameworks for analyzing the "complexity" or "nonconstructivity" of a given mathematical theorem. Among these frameworks are: computable analysis, degrees of unsolvability, reverse mathematics, and algorithmic randomness. Each of these frameworks provides a different kind of information. In this talk I shall analyze a few nonconstructive mathematical theorems from each of these points of view.

In this talk we compare four methods for determining the "complexity" or "nonconstructivity" of a given mathematical theorem.

1. computable analysis (Markov school, . . . , Weihrauch school)
2. degrees of unsolvability (Kleene/Post, Muchnik, Sacks, . . .)
3. reverse mathematics (Kreisel, Friedman, Simpson, . . .)
4. algorithmic randomness (Martin-Löf, Nies, Downey/Hirschfeldt, . . .)

Each of these four approaches gives a different kind of information.

In order to compare these four approaches, we analyze a few mathematical theorems from all four points of view.

1. The theorem entails the existence of noncomputable objects.
2. We can measure the amount of noncomputability of these objects.
3. The proof of the theorem requires strong nonconstructive axioms, and we can measure the strength of these axioms.
4. The theorem entails randomness, Kolmogorov complexity, ...

We begin by analyzing the following well known theorem.

Theorem. Let (a_i, b_i), $i = 1, 2, 3, \ldots$ be a sequence of open intervals which cover the unit interval: $[0, 1] \subseteq \bigcup_{i=1}^{\infty} (a_i, b_i)$. Then there exists a finite subcovering: $[0, 1] \subseteq \bigcup_{i=1}^{n} (a_i, b_i)$ for some n.

This theorem is known as the Heine/Borel Covering Lemma.
It plays a fundamental role in real analysis, etc.

In order to analyze this theorem, we may consider the contrapositive:

If each finite subsequence (a_i, b_i), $i = 1, \ldots, n$ fails to cover $[0, 1]$,
then the entire sequence (a_i, b_i), $i = 1, 2, 3, \ldots$ fails to cover $[0, 1]$,
i.e., there exists a real number $x \in [0, 1] \setminus \bigcup_{i=1}^{\infty} (a_i, b_i)$.

1. COMPUTABLE ANALYSIS.

We construct a "*computable counterexample*":

a computable sequence of rational open intervals (a_i, b_i), $i = 1, 2, 3, \ldots$, such that $|a_i - b_i| = 1/2^{i+1}$ and for all i, if i is an index of a computable real number x, then $a_i < x < b_i$.

No finite subsequence (a_i, b_i), $i = 1, \ldots, n$ can cover all of the computable real numbers in $[0, 1]$, because $\sum_{i=1}^{n} |a_i - b_i| < \frac{1}{2}$.

However, the entire sequence (a_i, b_i), $i = 1, 2, 3, \ldots$ covers all of the computable real numbers. In other words, there is no computable real number $x \in [0, 1] \setminus \bigcup_{i=1}^{\infty} (a_i, b_i)$.

In this sense, the Heine/Borel Covering Lemma is "computably false," i.e., false in the computable world. Given a computable sequence of rational intervals (a_i, b_i), $i = 1, 2, 3, \ldots$ which does not cover $[0, 1]$, it is not always possible to compute a real number x as above.

2. DEGREES OF UNSOLVABILITY.

We now wish to measure the amount of noncomputability which is inherent in the Heine/Borel Covering Lemma.

Definition (Turing)**.** Let $x, y \in \{0,1\}^\infty$ be infinite sequences of 0's and 1's. We inscribe y on the left half of a Turing machine tape and use it as an "oracle." We say that x is computable from the oracle y if there exists a Turing program M with the following property: for each positive integer n, if we start M with (y on the left half of the tape and) n on the right half of the tape, then M will eventually halt with the nth bit of x on the right half of the tape. In this case we write $x = \Phi_M(y)$ and we say that x *is Turing reducible to* y.

Definition (Yu. T. Medvedev, 1955)**.** A mass problem is a set $P \subseteq \{0,1\}^\infty$. (Intuitively, P represents the "problem" of finding an element of the set P.) Given mass problems P and Q, we say that P is strongly reducible to Q if there exists a Turing program M such that for all $y \in Q$ there exists $x \in P$ such that $x = \Phi_M(y)$.

Definition (A. A. Muchnik, 1963)**.** Given mass problems P and Q, we say that P is weakly reducible to Q if for all $y \in Q$ there exist $x \in P$ and a Turing program M such that $x = \Phi_M(y)$.

The relations of strong reducibility and weak reducibility are transitive and reflexive. We can therefore make the following definitions.

Definition. A strong degree or Medvedev degree is an equivalence class of mass problems under the equivalence relation "P and Q are strongly reducible to each other." The set of all strong degrees is denoted $\mathcal{D}_{\mathsf{s}}$.

Definition. A weak degree or Muchnik degree is an equivalence class of mass problems under the equivalence relation "P and Q are weakly reducible to each other." The set of all weak degrees is denoted $\mathcal{D}_{\mathsf{w}}$.

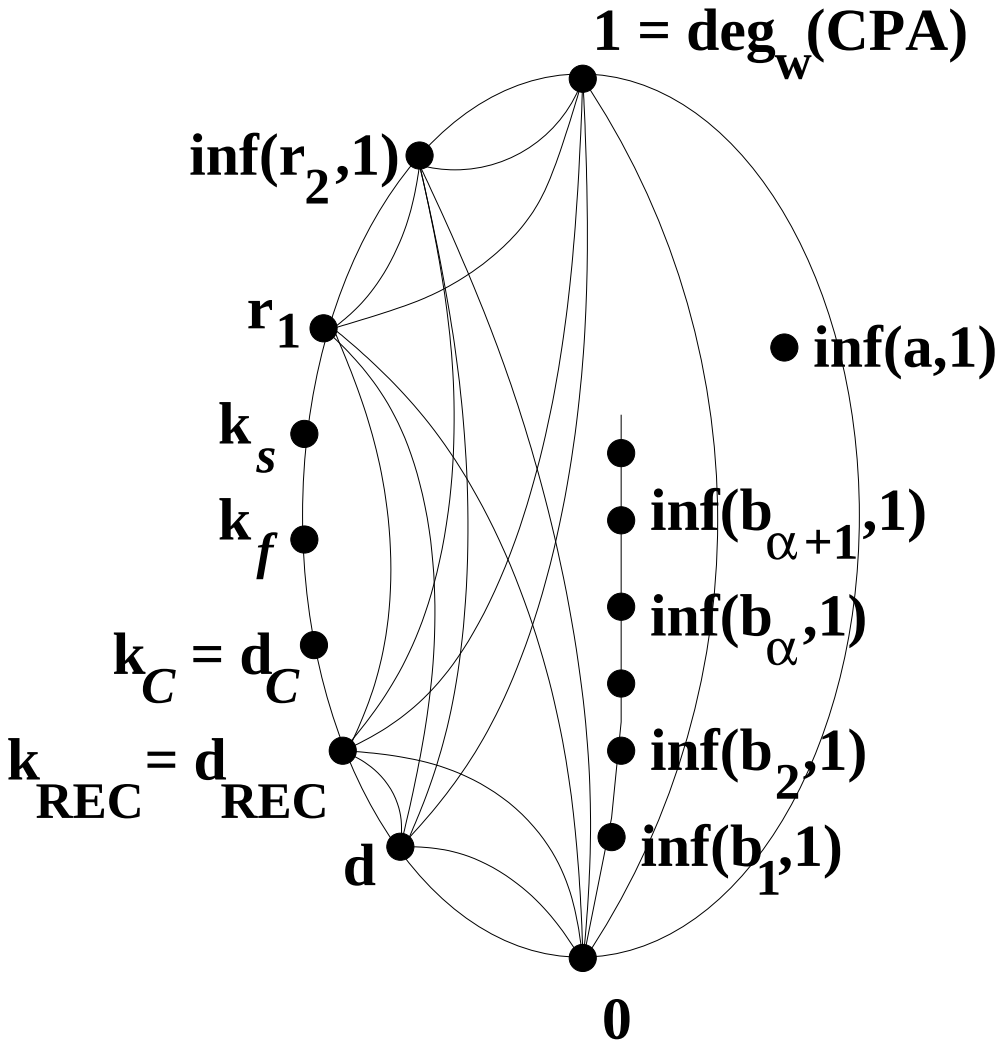
Remark. It can be shown that $\mathcal{D}_{\mathsf{s}}$ and $\mathcal{D}_{\mathsf{w}}$ are lattices, under strong and weak reducibility, respectively.

Given a computable sequence of open intervals (a_i, b_i), $i = 1, 2, 3, \ldots$, such that the set $P = [0, 1] \setminus \bigcup_{i=0}^{\infty} (a_i, b_i)$ is nonempty, we can ask:

What is the strong or weak degree of the mass problem P?

In other words, what kind of oracle would we need in order to compute (the binary expansion of) some real number $x \in P$?

Here is a picture of the weak degrees of this type.
This sublattice of $\mathcal{D}_{\mathsf{w}}$ is denoted $\mathcal{E}_{\mathsf{w}}$.



A picture of $\mathcal{E}_{\mathrm{w}}$.

Note. $\mathcal{E}_{\mathrm{w}}$ is the lattice of weak degrees of nonempty, effectively closed subsets of $[0,1]$.

From this picture we see that $\mathcal{E}_{\mathrm{w}}$ contains many specific, interesting degrees of unsolvability.

I am writing a book about $\mathcal{E}_{\mathrm{w}}$. A survey paper on $\mathcal{E}_{\mathrm{w}}$ is:

Stephen G. Simpson, Mass problems associated with effectively closed sets, Tohoku Mathematical Journal, 63, 2011, pp. 489–517.

The top degree $\mathbf{1} \in \mathcal{E}_{\mathrm{w}}$ is especially interesting. It can be described as the weak degree of the problem of finding an oracle y such that for any computable sequence of open intervals (a_i, b_i), $i = 1, 2, 3, \ldots$ as above, we can find an $x \in [0,1] \setminus \bigcup_{i=0}^{\infty} (a_i, b_i)$ such that $x = \Phi_M(y)$ for some Turing program M.

The degree $\mathbf{1} \in \mathcal{E}_{\mathrm{w}}$ can also be characterized as the weak degree of the problem of finding a complete, consistent extension of first-order Peano arithmetic. Or, replace Peano arithmetic by any consistent, recursively axiomatizable theory in which Robinson's Q is interpretable. For example, ZFC, assuming that ZFC is consistent.

3. REVERSE MATHEMATICS.

The goal of reverse mathematics is to answer questions of the following type. Given a mathematical theorem τ, what are the weakest axioms needed to prove τ?

Let Z_2 denote second-order arithmetic. Experience shows that reverse mathematics is best carried out in the context of subsystems of Z_2. In this context, the above question often has a precise answer. Namely, the axioms needed to prove τ are often *logically equivalent* to τ, over a weak base theory. Furthermore, there is a manageable hierarchy of axioms which frequently arise in this way.

Five subsystems of Z_2 which are crucially important for reverse mathematics are, in order of increasing strength:

$$\mathrm{RCA}_0, \quad \mathrm{WKL}_0, \quad \mathrm{ACA}_0, \quad \mathrm{ATR}_0, \quad \Pi^1_1\text{-CA}_0.$$

These are known as "The Big Five." The first system RCA_0 usually serves as the weak base theory. See my book:

Stephen G. Simpson, Subsystems of Second Order Arithmetic, Second Edition, Perspectives in Logic, Association for Symbolic Logic, 2009, XVI + 444 pages.

RCA_0 = a kind of formalized computable mathematics.

WKL_0 = RCA_0 + Weak König's Lemma.

ACA_0 = RCA_0 + arithmetical comprehension.

ATR_0 = RCA_0 + arithmetical transfinite recursion.

Π^1_1-CA_0 = RCA_0 + Π^1_1 comprehension.

It turns out that the Heine/Borel Covering Lemma is logically equivalent to WKL_0 over RCA_0. Furthermore, there is a long list of other famous mathematical theorems, each of which is logically equivalent to WKL_0 over RCA_0. Here is a partial list:

Every continuous real-valued function on $[0, 1]$ is uniformly continuous. Every continuous real-valued function on $[0, 1]$ is bounded. Every continuous real-valued function on $[0, 1]$ has a Riemann integral. Every continuous real-valued function on $[0, 1]$ has a maximum value. Every countable commutative ring has a prime ideal. Every countable field has a unique algebraic closure. Brouwer's Fixed Point Theorem. Peano's Existence Theorem for solutions of ordinary differential equations. The Hahn/Banach Theorem for separable Banach spaces. Etc., etc.

As is the case for the system WKL_0, each of the systems ACA_0 and ATR_0 and Π^1_1-CA_0 has an associated list of mathematical theorems, each of which is logically equivalent to the given system over RCA_0.

In this way, many mathematical theorems are grouped into a small number of "logical equivalence classes" over RCA_0. This outcome of reverse mathematics seems to be of general intellectual interest.

Remark 1. Weihrauch 1990 introduced another degree notion, the Weihrauch degrees, which provides detailed insight into many reverse mathematics constructions. The Weihrauch lattice is somewhat similar to the Medvedev lattice, but harder to define and more comprehensive.

Remark 2. Many subsystems of Z_2, including the Big Five, have been analyzed from a proof-theoretical point of view, using ordinal notations, etc. This proof-theoretic connection provides additional information which is not provided by computable analysis or degrees of unsolvability.

4. ALGORITHMIC RANDOMNESS.

Definitions (Martin-Löf, 1966)**.** A set $U \subseteq [0,1]$ is effectively open if it is of the form $U = [0,1] \cap \bigcup_{i=1}^{\infty}(a_i, b_i)$ where (a_i, b_i), $i = 1, 2, 3, \ldots$, is a computable sequence of rational open intervals. The complement $[0,1] \setminus U = [0,1] \setminus \bigcup_{i=1}^{\infty}(a_i, b_i)$ is said to be effectively closed.

A set $S \subseteq [0,1]$ is said to be effectively null or effectively of measure 0 if $S \subseteq \bigcap_{n=1}^{\infty} U_n = [0,1] \cap \bigcap_{n=1}^{\infty} \bigcup_{i=1}^{\infty}(a_{ni}, b_{ni})$ where (a_{ni}, b_{ni}), $n, i = 1, 2, 3, \ldots$, is a computable double sequence of rational open intervals, and each of the effectively open sets $U_n = [0,1] \cap \bigcup_{i=1}^{\infty}(a_{ni}, b_{ni})$ is of measure $\leq 1/2^n$.

A point $x \in [0,1]$ is random if $x \notin S$ for all effectively null sets S.

Theorem (Martin-Löf)**.** There is a universal effectively null set. In other words, the union of all effectively null sets is effectively null.

Corollary. Almost all points $x \in [0,1]$ are random. In fact, there exist effectively closed sets $P = [0,1] \setminus \bigcup_{i=0}^{\infty}(a_i, b_i)$ of measure arbitrarily close to 1 such that every point $x \in P$ is random in the sense of Martin-Löf.

Proof. Let $P = P_n = [0,1] \setminus U_n$ where $S = \bigcap_{n=1}^{\infty} U_n$ is univ. eff. null.

Recall that $\mathcal{E}_{\mathsf{w}}$ is the lattice of weak degrees of nonempty effectively closed sets in $[0,1]$.

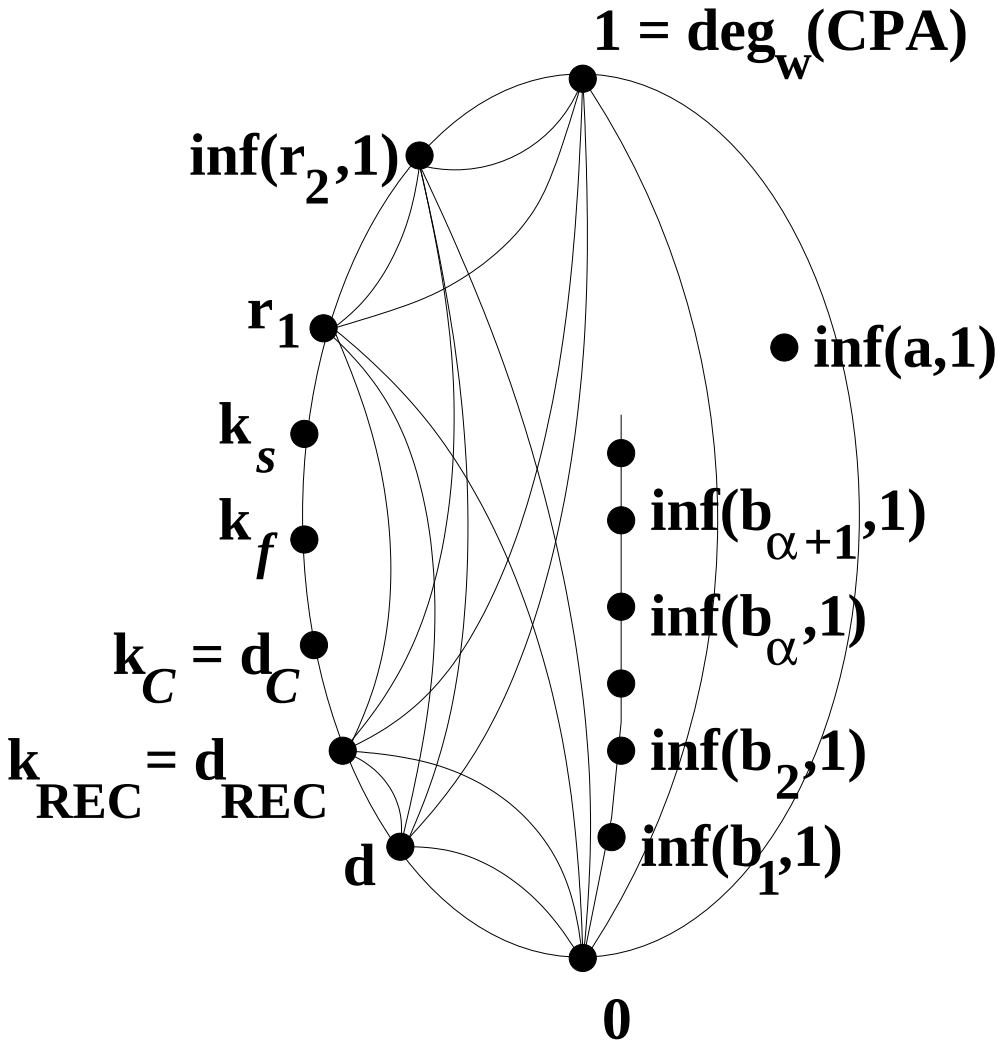
Remark. In our picture of $\mathcal{E}_{\mathsf{w}}$, $\mathbf{r}_1$ is the weak degree of the set $\mathsf{MLR} = \{x \in [0,1] \mid x \text{ is random in the sense of Martin-Löf}\}$.

In fact, most of the specific, named degrees in $\mathcal{E}_{\mathsf{w}}$ are in some way related to algorithmic randomness.

Remarkably, the only known exceptions are $\mathbf{0}$ and $\mathbf{1}$.

Remark. In our computable counterexample to Heine/Borel, we constructed an effectively closed set $P \subseteq [0,1]$ which is of positive measure yet contains no computable point. Kučera has shown that the weak degree of any such set is $\leq \mathbf{r}_1$.

Remark. There is a subsystem of Z_2 called WWKL_0 which arises in the reverse mathematics of measure theory. WWKL_0 is strictly intermediate between RCA_0 and WKL_0. WWKL_0 is equivalent over RCA_0 to the assertion that Heine/Borel holds for sequences of open intervals (a_i, b_i), $i = 1, 2, 3, \ldots$ such that $\sum_{i=1}^{\infty} |a_i - b_i| < 1$.



A picture of $\mathcal{E}_{\mathrm{w}}$.

Note. $\mathcal{E}_{\mathrm{w}}$ is the lattice of weak degrees of nonempty, effectively closed subsets of $[0,1]$.

We now explain some degrees in $\mathcal{E}_{\mathsf{w}}$. If P is any mass problem, let $\deg_{\mathsf{w}}(P)$ denote the weak degree of P.

The top degree in $\mathcal{E}_{\mathsf{w}}$ is $\mathbf{1} = \deg_{\mathsf{w}}(\mathrm{CPA})$ where CPA is the problem of finding a complete consistent theory which includes Peano arithmetic (or ZFC, etc.).

We also have $\inf(\mathbf{a}, \mathbf{1}) \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{a}$ is any recursively enumerable Turing degree. Moreover, $\mathbf{a} < \mathbf{b}$ implies $\inf(\mathbf{a}, \mathbf{1}) < \inf(\mathbf{b}, \mathbf{1})$

We have $\mathbf{r}_1 \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{r}_1 = \deg_{\mathsf{w}}(\mathrm{MLR})$, where $\mathrm{MLR} = \{x \in [0,1] \mid x$ is Martin-Löf random$\}$).

We also have $\inf(\mathbf{r}_2, \mathbf{1}) \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{r}_2 = \deg_{\mathsf{w}}(\{x \in [0,1] \mid x$ is 2-*random*$\}$), i.e., Martin-Löf random relative to the halting problem.

Also $\mathbf{d} \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{d} = \deg_{\mathsf{w}}(\{f \mid f$ is *diagonally nonrecursive*$\}$), i.e., $\forall n\, (f(n) \neq \varphi_n(n))$.

Let REC $= \{g \in \mathbb{N}^{\mathbb{N}} \mid g$ is recursive$\}$. Let C be any "nice" subclass of REC. For instance $C =$ REC, or $C = \{g \in$ REC $\mid g$ is primitive recursive$\}$. We have $\mathbf{d}_C \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{d}_C = \deg_{\mathsf{w}}(\{f \in \mathbb{N}^{\mathbb{N}} \mid f$ is diagonally nonrecursive and C-*bounded*$\})$, i.e., $(\exists g \in C)\, \forall n\, (f(n) < g(n))$.

Also, $\mathbf{d}_C = \deg_{\mathsf{w}}(\{x \in \{0,1\}^\infty \mid x$ is C-*complex*$\}$, i.e., $(\exists g \in C)\, \forall n\, (\mathsf{K}(x\restriction\{1,\ldots,g(n)\}) \geq n)\}$) where K denotes prefix-free Kolmogorov complexity. Moreover, $\mathbf{d}_{C'} < \mathbf{d}_C$ whenever C' contains a function which dominates all functions in C.

For $x \in \{0,1\}^\infty$ let effdim$(x) =$ the *effective Hausdorff dimension* of x, i.e., effdim$(x) = \liminf_{n\to\infty} \dfrac{\mathsf{K}(x\restriction\{1,\ldots,n\})}{n}$. Given a right recursively enumerable real number $s < 1$, we have $\mathbf{k}_s \in \mathcal{E}_{\mathsf{w}}$ where $\mathbf{k}_s = \deg_{\mathsf{w}}(\{x \in \{0,1\}^{\mathbb{N}} \mid \text{effdim}(x) > s\})$. Moreover, $s < t$ implies $\mathbf{k}_s < \mathbf{k}_t$ (Joseph S. Miller).

More generally, let $g : \mathbb{N} \to [-\infty, \infty)$ be an unbounded computable function such that $g(n) \leq g(n+1) \leq g(n) + 1$ for all n. For example, $g(n)$ could be $n/2$ or $n/3$ or $\sqrt{n}$ or $\sqrt[3]{n}$ or $\log n$ or $\log n + \log\log n$ or $\log\log n$ or the inverse Ackermann function. Define
$\mathbf{k}_g = \deg_{\mathsf{W}}(\{x \in \{0,1\}^\infty \mid x \text{ is } g\textit{-random}\})$, i.e.,
$\exists c \forall n \, (\mathsf{K}(x{\restriction}\{1,\ldots,n\} \geq g(n) - c)$.

Theorem (W. M. P. Hudelson, 2010)**.** $\mathbf{k}_g < \mathbf{k}_h$ provided $g(n) + 2\log g(n) \leq h(n)$ for all n. In other words, there exists a g-random real with no h-random real Turing reducible to it. This is a generalization of Miller's result.

Letting z be a Turing oracle, define $\mathsf{MLR}^z = \{x \in [0,1] \mid x$ is random relative to $z\}$ and $\mathsf{K}^z(\tau) =$ the prefix-free Kolmogorov complexity of τ relative to z. Define $y \leq_{\mathsf{LR}} z \iff \mathsf{MLR}^z \subseteq \mathsf{MLR}^y$ and $y \leq_{\mathsf{LK}} z \iff \exists c \forall \tau\, (\mathsf{K}^z(\tau) \leq \mathsf{K}^y(\tau) + c)$.

Theorem (Miller/Kjos-Hanssen/Solomon)**.** We have $y \leq_{\mathsf{LR}} z \iff y \leq_{\mathsf{LK}} z$.

For each recursive ordinal number α, let $0^{(\alpha)} =$ the αth iterated Turing jump of 0. Thus $0^{(1)} =$ the halting problem, and $0^{(\alpha+1)} =$ the halting problem relative to $0^{(\alpha)}$, etc. This is the hyperarithmetical hierarchy. We embed it naturally into $\mathcal{E}_{\mathsf{w}}$ as follows.

Theorem (Simpson 2009)**.** $0^{(\alpha)} \leq_{\mathsf{LR}} z \iff$ every $\Sigma^0_{\alpha+2}$ set includes a $\Sigma^{0,z}_2$ set of the same measure. Moreover, letting $\mathbf{b}_\alpha = \deg_{\mathsf{w}}(\{z \mid 0^{(\alpha)} \leq_{\mathsf{LR}} z\})$ we have $\inf(\mathbf{b}_\alpha, \mathbf{1}) \in \mathcal{E}_{\mathsf{w}}$ and $\inf(\mathbf{b}_\alpha, \mathbf{1}) < \inf(\mathbf{b}_{\alpha+1}, \mathbf{1})$.

Thank you for your attention!

Stephen G. Simpson, Pennsylvania State University

http://www.math.psu.edu/simpson/

simpson@math.psu.edu