Propagation of Partial Randomness

Stephen G. Simpson
Pennsylvania State University
http://www.math.psu.edu/simpson/
simpson@math.psu.edu

Proof Theory and Computability

Harumi Grand Hotel

Tokyo, Japan

February 20–23, 2012

Randomness.

We work with $\{0,1\}^{\mathbb{N}}$ = the *Cantor space*. Note that each point $X \in \{0,1\}^{\mathbb{N}}$ is an infinite sequence of 0's and 1's. Let μ be the *fair coin probability measure* on $\{0,1\}^{\mathbb{N}}$. Thus each point X is viewed by μ as the outcome of an infinite sequence of coin tosses. Consider sets $S \subseteq \{0,1\}^{\mathbb{N}}$ which are *effectively null*, i.e., effectively of measure 0. A point $X \in \{0,1\}^{\mathbb{N}}$ is defined to be *random* (in the sense of Martin-Löf 1966) if it belongs to no effectively null set.

Details: For each $\tau \in \{0,1\}^*$ we write $[\tau] = \{X \mid \tau \text{ is an initial segment of } X\}$. So $\mu([\tau]) = 2^{-|\tau|}$ where $|\tau|$ = the length of τ. For $A \subseteq \{0,1\}^*$ we write $[A] = \bigcup_{\tau \in A}[\tau]$. A set $S \subseteq \{0,1\}^{\mathbb{N}}$ is said to be *effectively null* if $S \subseteq \bigcap_n [A_n]$ where $\mu([A_n]) \leq 2^{-n}$ and the A_n's are *uniformly recursively enumerable* or *u.r.e.*. Here u.r.e. means that the set $\{(\tau, n) \mid \tau \in A_n\} \subseteq \{0,1\}^* \times \mathbb{N}$ is recursively enumerable.

Prefix-free Kolmogorov complexity.

We consider partial recursive functions Φ from $\{0,1\}^*$ to $\{0,1\}^*$. We say that Φ is *prefix-free* if the domain of Φ is prefix-free, i.e., there is no pair $\sigma_1, \sigma_2 \in \mathrm{dom}(\Phi)$ such that σ_1 is an initial segment of σ_2. For each $\tau \in \{0,1\}^*$ let $\mathrm{KP}_\Phi(\tau) = \min\{|\sigma| \mid \Phi(\sigma) = \tau\}$.

We can construct a Φ which is *universal*, i.e., for any prefix-free partial recursive function Ψ there exists a constant c such that for all τ, $\mathrm{KP}_\Phi(\tau) \leq \mathrm{KP}_\Psi(\tau) + c$. Then, the *prefix-free complexity* of τ is defined as $\mathrm{KP}(\tau) = \mathrm{KP}_\Phi(\tau)$ where Φ is a universal prefix-free partial recursive function.

Note that KP is well-defined up to $\pm O(1)$. Here "well-defined" means that KP is independent of the choice of Φ.

Roughly speaking, $\mathrm{KP}(\tau)$ is the number of bits of information which are needed to describe τ. In particular, one can prove that $\exists c \, \forall \tau \, (\mathrm{KP}(\tau) \leq |\tau| + 2\log_2|\tau| + c)$, etc.

Randomness and complexity.

The next theorem shows a connection between Martin-Löf randomness and Kolmogorov complexity. Namely, X is random if and only if the finite initial segments of X are (nearly) as complex as possible.

Let $X{\upharpoonright}n$ be the initial segment of length n.

Schnorr's Theorem. A point $X \in \{0,1\}^{\mathbb{N}}$ is random in the sense of Martin-Löf $\Longleftrightarrow$ $\exists c \, \forall n \, (\mathsf{KP}(X{\upharpoonright}n) \geq n - c)$.

Two recent books on randomness and Kolmogorov complexity:

1. André Nies, *Computability and Randomness*, Oxford University Press, 2009, XV + 433 pages.

2. Rodney G. Downey and Denis Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag, 2010, XXVIII + 855 pages.

Partial randomness.

Fix a recursive function $f : \{0,1\}^* \to [0,\infty)$.

The f-*weight* of $A \subseteq \{0,1\}^*$ is defined as

$$\mathrm{wt}_f(A) = \sum_{\tau \in A} 2^{-f(\tau)}.$$

A point $X \in \{0,1\}^{\mathbb{N}}$ is said to be f-*random* if $X \notin \bigcap_n [A_n]$ for all u.r.e. sequences of sets A_n, $n = 1, 2, \ldots$, such that $\mathrm{wt}_f(A_n) \leq 2^{-n}$.

Two special cases:

1. X is Martin-Löf random $\Longleftrightarrow$ X is "length-random," i.e., f-random where $f(\tau) = |\tau| =$ the length of τ.

2. For each rational number s, say that X is s-*random* if X is f_s-random with $f_s(\tau) = s|\tau|$.

The *effective Hausdorff dimension* of X is

$$\mathrm{effdim}(X) = \sup\{s \mid X \text{ is } s\text{-random}\}.$$

Fundamental results concerning s-randomness and effective Hausdorff dimension have been obtained by several researchers including Tadaki, Reimann, Terwijn, Miller, ...

Partial randomness and complexity.

We now generalize Schnorr's Theorem, replacing Martin-Löf randomness by partial randomness.

Theorem. For any recursive function $f : \{0,1\}^* \to [0,\infty)$, a point $X \in \{0,1\}^{\mathbb{N}}$ is f-random $\iff \exists c \forall n\, (\mathrm{KP}(X{\upharpoonright}n) \geq f(X{\upharpoonright}n) - c)$.

For example, X is 0.5-random if and only if the first n bits of X contain at least $n/2$ bits of information, modulo an additive constant.

Similarly, X is $\sqrt{|\cdot|}$-random if and only if the first n bits of X contain at least $\sqrt{n}$ bits of information, modulo an additive constant.

Randomness relative to a Turing oracle.

The purpose of this talk is to present some new results concerning partial randomness relative to a Turing oracle. We first present the original results, concerning randomness relative to a Turing oracle.

Recall that a point $Y \in \{0,1\}^{\mathbb{N}}$ may be used as a Turing oracle. This means that our Turing machines have the added capability of immediately accessing the value $Y(n)$ when n is known. For example, the function $\psi(m) =$ the least n such that $n > m$ and $Y(n) = 1$ is computable using Y as a Turing oracle.

We say that X is *Turing reducible to* Y if X is computable using Y as a Turing oracle.

We say that X is *random relative to* Y if $X \notin \bigcap_n [A_n]$ whenever $\mu([A_n]) \leq 2^{-n}$ and A_n is u.r.e. using Y as a Turing oracle.

Propagation of randomness.

Theorem 1 (Miller/Yu 2008)**.** Assume that X is random, and X is Turing reducible to Y, and Y is random relative to Z. Then X is random relative to Z.

We define a PA-*oracle* to be a Turing oracle Z such that some complete extension of Peano Arithmetic is Turing reducible to Z. Instead of PA we could use any recursively axiomatizable, essentially undecidable theory. E.g., ZFC or Z_2 or PRA or Robinson's Q.

Theorem 2. Assume that X is random. Then X is random relative to some PA-oracle.

Theorem 2 is due independently to Downey/Hirschfeldt/Miller/Nies (2005) and Reimann/Slaman (not yet published) and Simpson/Yokoyama (published in 2011).

Randomness relative to a PA-oracle.

Theorem 2, concerning randomness relative to a PA-oracle, has been very useful in the study of randomness.

Reimann/Slaman applied Theorem 2 to prove:

$X \in \{0,1\}^{\mathbb{N}}$ is nonrecursive $\Longleftrightarrow$
X is non-atomically random w.r.t. some probability measure on $\{0,1\}^{\mathbb{N}}$.

Simpson/Yokoyama applied a generalization of Theorem 2 to study the reverse mathematics of Loeb measures.

Recently Brattka/Miller/Nies applied Theorem 2 to prove:

$x \in [0,1]$ is random $\Longleftrightarrow$
every computable continuous function of bounded variation is differentiable at x.

Propagation of partial randomness.

In order to obtain sharp generalizations of Theorems 1 and 2, we must consider an alternative notion of f-randomness.

As before, fix a recursive function $f : \{0,1\}^* \to [0,\infty)$. For $A \subseteq \{0,1\}^*$ the *prefix-free f-weight* of A is defined as $\mathrm{pwt}_f(A) = \sup\{\mathrm{wt}_f(P) \mid P \text{ prefix-free}, P \subseteq A\}$.
We say that X is *strongly f-random* if $X \notin \bigcap_n [A_n]$ for all u.r.e. sequences A_n with $\mathrm{pwt}_f(A_n) \leq 2^{-n}$.
The notion of strong f-randomness relative to a Turing oracle is defined similarly.

Theorem 3. Assume that X is strongly f-random, and X is Turing reducible to Y, and Y is random relative to Z. Then X is strongly f-random relative to Z.

Theorem 4. Assume $\forall i\,(X_i$ is strongly f_i-random). Then $\forall i\,(X_i$ is strongly f_i-random relative to $Z)$ for some PA-oracle Z.

f-randomness vs. strong f-randomness.

Theorem 5. Theorems 3 and 4 fail if we replace strong f-randomness by f-randomness. Indeed, there exists a 0.5-random X which is not 0.5-random relative to any PA-oracle.

Thus strong f-randomness appears to be more "stable" than f-randomness. Nevertheless, there are close relationships between the two notions.

Theorem 6. Assume that X is f-random relative to some PA-oracle. Then X is strongly f-random.

Theorem 7. Assume that X is g-random where $g(\tau) = f(\tau) + 2\log_2 f(\tau)$. Then X is strongly f-random.

Theorems 3, 4, 5, 6, 7 were first proved in 2011. They will eventually appear in a paper by Higuchi/Simpson/Yokoyama.

A variant of prefix-free complexity.

Just as f-randomness can be characterized in terms of prefix-free complexity or KP, so strong f-randomness can be characterized in terms of a slightly different complexity notion, called a priori complexity or KA.

A *semimeasure* is a function $m : \{0,1\}^* \to [0,1]$ such that $m(\tau) \geq m(\tau 0) + m(\tau 1)$ for all $\tau \in \{0,1\}^*$. We say that m is *left r.e.* if the real numbers $m(\tau)$ are uniformly left recursively enumerable. One can construct a left r.e. semimeasure m which is *universal*, i.e., for any left r.e. semimeasure m_1 we can find c_1 such that $m_1(\tau) \leq c_1 \cdot m(\tau)$ for all τ. Then, the *a priori complexity* of τ is defined as $\mathrm{KA}(\tau) = -\log_2 m(\tau)$. As in the case of KP, the definition of KA is independent of the choice of a universal left r.e. semimeasure, modulo additive constants

These concepts are originally due to Levin.

Characterizing strong f-randomness.

Using KA (a priori complexity)
instead of KP (prefix-free complexity),
one obtains a Schnorr-like characterization
of strong f-randomness.

Theorem. For any recursive function
$f : \{0,1\}^* \to [0,\infty)$, a point $X \in \{0,1\}^{\mathbb{N}}$
is strongly f-random if and only if
$\exists c \, \forall n \, (\mathsf{KA}(X{\upharpoonright}n) \geq f(X{\upharpoonright}n) - c)$.

This theorem is essentially due to
Calude/Staiger/Terwijn (2006).
See also Reimann (2008).

Levin often says that KA
is "better behaved" than KP.

For instance, it is easy to show that
$\exists c \, \forall \tau \, (\mathsf{KA}(\tau) \leq |\tau| + c)$.

Partial randomness and mass problems.

Given a computable function $f : \{0, 1\}^* \to [0, \infty)$, there is an associated mass problem K_f, namely, the problem of finding some X which is f-random. Let $\mathbf{k}_f = \deg(K_f) =$ the *degree of unsolvability* (Muchnik degree) of K_f.
The next theorem shows that $\mathbf{k}_f < \mathbf{k}_g$ provided f is sufficiently "nice" and g grows significantly faster than f.

Theorem (Hudelson 2009)**.** Assume that $f(\tau) = F(|\tau|)$ and $F(n) \leq F(n+1) \leq F(n) + 1$ for all n and all τ. Assume also that $f(\tau) + 2\log_2 f(\tau) \leq g(\tau)$ for all τ. Then, there exists a strongly f-random X such that no g-random Y is Turing reducible to X.

Phil Hudelson, Mass problems and initial segment complexity, 20 pages, 2010, submitted for publication.

Joseph S. Miller, Extracting information is hard, Advances in Mathematics, 226, 2011, 373–384.

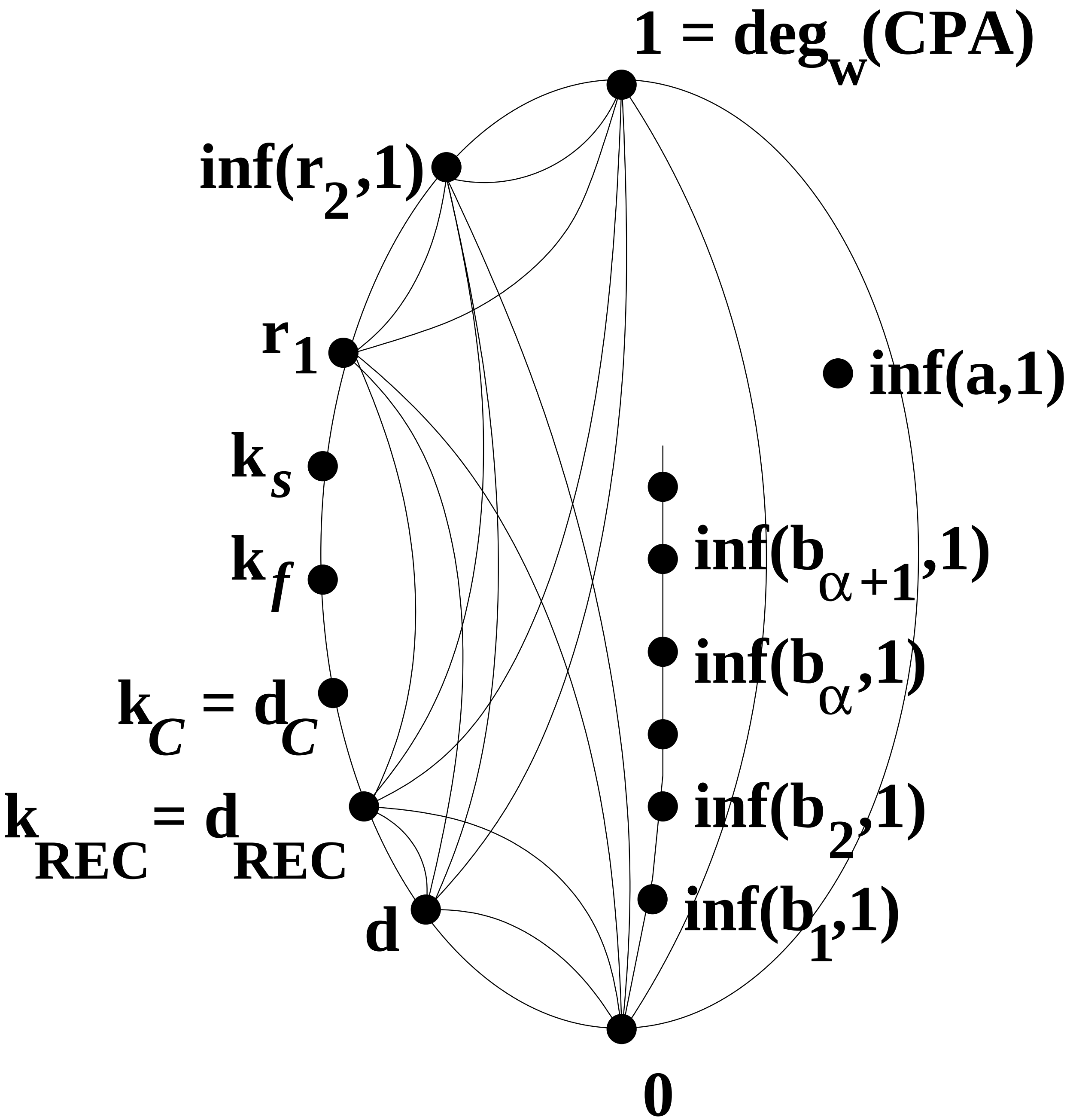
The lattice $\mathcal{E}_\mathrm{w}$.

Let $\mathcal{E}_\mathrm{w}$ be the lattice of Muchnik degrees of nonempty effectively closed sets in $\{0,1\}^\mathbb{N}$. See for instance my survey paper in the recent centennial issue of the Tohoku Mathematical Journal.

The lattice $\mathcal{E}_\mathrm{w}$ is a rich structure and contains many interesting degrees of unsolvability. On the next slide, each of the black dots except one represents a specific, natural degree of unsolvability.

In particular, for each computable function $f : \{0,1\}^* \to [0,\infty)$ such that $f(\tau) \leq |\tau|$ for all τ, we can show that the Muchnik degree $\mathbf{k}_f$ belongs to $\mathcal{E}_\mathrm{w}$. Thus Hudelson's theorem implies the existence of more such black dots.

For example, let $\mathbf{q}_n = \mathbf{k}_f$ where $f(\tau) = \sqrt[n]{|\tau|} =$ the nth root of $|\tau|$. Then for $n = 1, 2, 3, \ldots$ the Muchnik degrees $\mathbf{q}_n$ belong to $\mathcal{E}_\mathrm{w}$, and by Hudelson's theorem we have $\mathbf{r}_1 = \mathbf{q}_1 > \mathbf{q}_2 > \cdots > \mathbf{q}_n > \mathbf{q}_{n+1} > \cdots$.



A picture of $\mathcal{E}_w$. Here $\mathbf{a} =$ any r.e. degree, $\mathbf{r} =$ randomness, $\mathbf{b} =$ LR-reducibility, $\mathbf{k} =$ complexity, $\mathbf{d} =$ diagonal nonrecursiveness.

Embedding hyperarithmeticity into $\mathcal{E}_{\mathsf{w}}$.

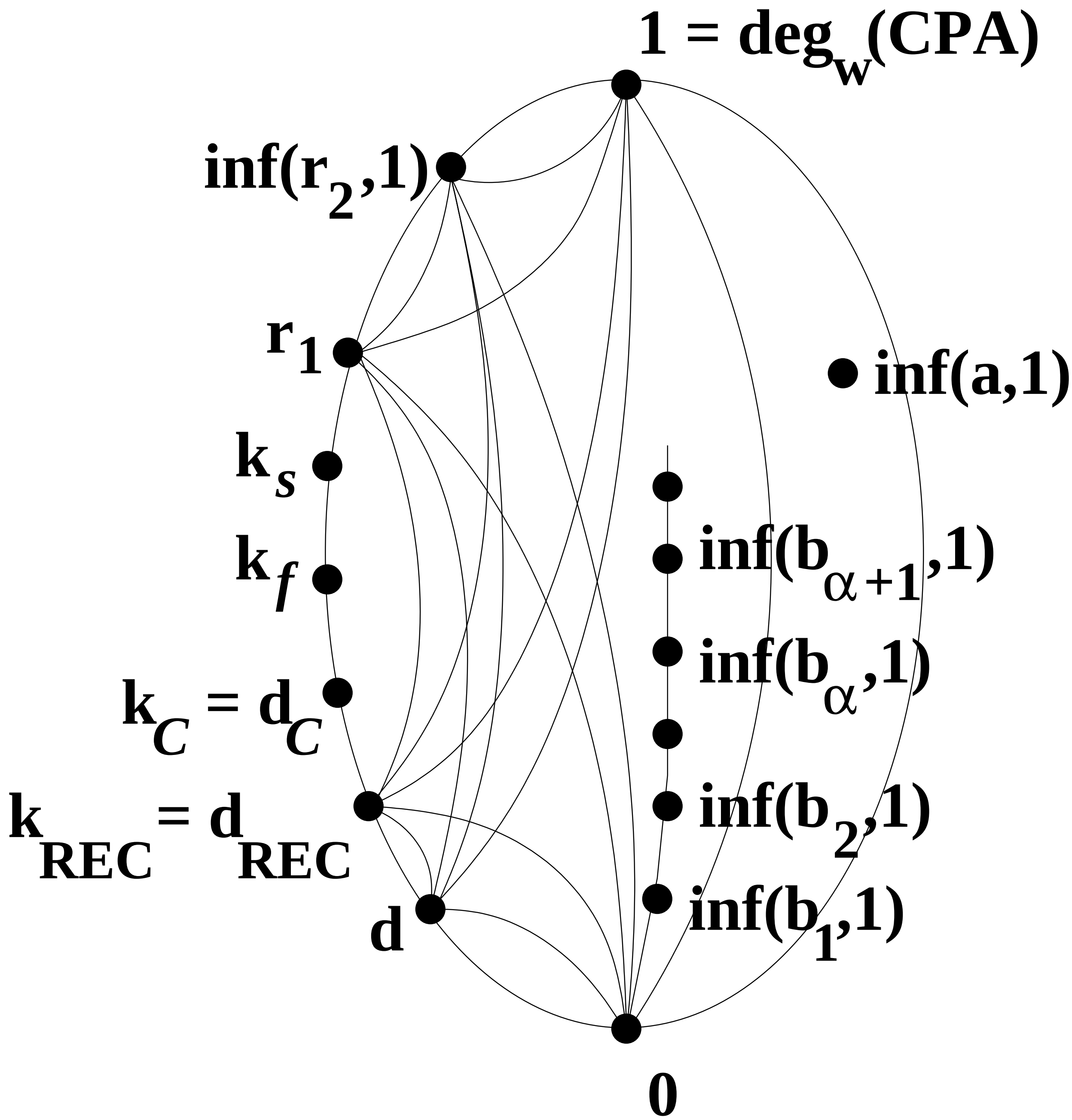
Given a Turing oracle Z, let
$\mathsf{MLR}^Z = \{X \mid X \text{ is random relative to } Z\}$ and
$\mathsf{KP}^Z(\tau) =$ the prefix-free complexity of τ relative to Z.

Define $Y \leq_{\mathsf{LR}} Z \iff \mathsf{MLR}^Z \subseteq \mathsf{MLR}^Y$ and
$Y \leq_{\mathsf{LK}} Z \iff \exists c \forall \tau \, (\mathsf{KP}^Z(\tau) \leq \mathsf{KP}^Y(\tau) + c)$.

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 <u>hyperarithmetical hierarchy</u>.
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 $\mathbf{b}_\alpha = \deg(\{Z \mid 0^{(\alpha)} \leq_{\mathsf{LR}} Z\})$ we have
$\inf(\mathbf{b}_\alpha, \mathbf{1}) \in \mathcal{E}_{\mathsf{w}}$ and $\inf(\mathbf{b}_\alpha, \mathbf{1}) < \inf(\mathbf{b}_{\alpha+1}, \mathbf{1})$.



A picture of $\mathcal{E}_w$. Here $\mathbf{a} =$ any r.e. degree, $\mathbf{r} =$ randomness, $\mathbf{b} =$ LR-reducibility, $\mathbf{k} =$ complexity, $\mathbf{d} =$ diagonal nonrecursiveness.

History: Kolmogorov 1932 developed his "calculus of problems" as a nonrigorous yet compelling explanation of Brouwer's intuitionism. Later Medvedev 1955 and Muchnik 1963 proposed Medvedev degrees and Muchnik degrees as rigorous versions of Kolmogorov's idea.

Some references:

Stephen G. Simpson, Mass problems and randomness, Bulletin of Symbolic Logic, 11, 2005, 1–27.

Stephen G. Simpson, An extension of the recursively enumerable Turing degrees, Journal of the London Mathematical Society, 75, 2007, 287–297.

Stephen G. Simpson, Mass problems and intuitionism, Notre Dame Journal of Formal Logic, 49, 2008, 127–136.

Stephen G. Simpson, Mass problems and measure-theoretic regularity, Bulletin of Symbolic Logic, 15, 2009, 385–409.

Stephen G. Simpson, Medvedev degrees of 2-dimensional subshifts of finite type, to appear in Ergodic Theory and Dynamical Systems.

Stephen G. Simpson, Entropy equals dimension equals complexity, 2011, 19 pages, submitted for publication.

THE END. THANK YOU!