Some Aspects of Reverse Mathematics

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

Reverse Mathematics Workshop

Department of Mathematics

University of Chicago

September 16-18, 2011

Gödel's Incompleteness Theorem.

Hilbert's concern for consistency proofs led to Gödel's Second Incompleteness Theorem.

Let T be a theory in the predicate calculus satisfying certain mild conditions. Then:

1. T is incomplete.

2. The statement "T is consistent" is not a theorem of T.

(Gödel 1931)

3. The problem of deciding whether a given formula is a theorem of T is algorithmically unsolvable.

(Gödel, Turing, Tarski, . . .)

The Gödel hierarchy.

Let T_1, T_2 be two theories as above. Define

$$T_1 \ < \ T_2$$

if "T_1 is consistent" is a theorem of T_2.

Usually this is equivalent to saying that T_1 is interpretable in T_2 and not vice versa.

This ordering gives a hierarchy of foundational theories, the Gödel hierarchy.

The Gödel hierarchy is often linear, and it exhibits other remarkable regularities.

The Gödel hierarchy is a central object of study in foundations of mathematics.

Reference.

Stephen G. Simpson, The Gödel hierarchy and reverse mathematics, in *Kurt Gödel: Essays for his Centennial*, ASL, Cambridge University Press, Lecture Notes in Logic 33, 2010, 128–141.

Stopping points in the Gödel hierarchy.

strong	⋮
	supercompact cardinal
	⋮
	measurable cardinal
	⋮
	ZFC (ZF set theory with choice)
	Zermelo set theory
	simple type theory
medium	Z_2 (2nd order arithmetic)
	⋮
	Π^1_2 comprehension
	Π^1_1 comprehension
	ATR_0 (arith. transfinite recursion)
	ACA_0 (arithmetical comprehension)
weak	WKL_0 (weak König's lemma)
	RCA_0 (recursive comprehension)
	PRA (primitive recursive arithmetic)
	EFA (elementary arithmetic)
	bounded arithmetic
	⋮

Foundational programs.

Several stopping points in the Gödel hierarchy correspond to venerable foundational programs in mathematics.

For instance, PRA corresponds to Hilbert's program of *finitism* (Tait 1981).

Since WKL_0 is Π^0_2-conservative over PRA, we may say that WKL_0 corresponds to a program of *finitistic reductionism*. This is interesting because WKL_0 suffices as a foundation for a remarkably large part of mathematics (Simpson 1988, 1999).

Similarly, there is a system IR (Feferman 1964) which corresponds to the outer limits of Hermann Weyl's program of predicativism.

Since ATR_0 is Π^1_1-conservative over IR, we may say that ATR_0 represents a program of *predicativistic reductionism* (Friedman/McAloon/Simpson 1982). This is interesting because ATR_0, like WKL_0, is one of the key theories in reverse mathematics.

Consequences for current research.

Reverse mathematics is ultimately a research program in the foundations of mathematics. Therefore, it is desirable to classify mathematical theorems with an eye to broad foundational programs corresponding to major stopping points in the Gödel hierarchy.

For instance, very little is known about the strength of the Dual Ramsey Lemma, a key lemma of Ramsey theory which deals with finite strings of symbols. It is known that the Dual Ramsey Lemma is provable in Π^1_1-CA_0 and not in WKL_0 (Miller/Solomon 2004). It would be desirable to close this very wide gap.

Similarly, we know that the first-order part of RT(2) (Ramsey's Theorem for pairs) includes Σ_2 bounding and is included in Σ_2 induction. There is an urgent need to close this gap, because Σ_2 bounding is finitistically reducible while Σ_2 induction is not.

Consequences, continued.

Similarly, it is unknown whether Hindman's Theorem is provable in ACA_0. Hindman's Theorem says that for every coloring of the positive integers with finitely many colors, there is an infinite set such that all the sums of finite nonempty subsets have the same color.

Similarly, let FC = Fraïssé's Conjecture. This is a theorem due to Laver 1969. It says that the countable linear orderings are well quasi-ordered under embeddability. It would be desirable to know whether FC is provable in ATR_0. Recently Marcone and Montalbán have made some progress, but the problem remains unsolved.

Announcement of recent results.

In the past two years, due to illness,
I have missed two important conferences.
Therefore, I now take this opportunity to
announce some miscellaneous recent results.

1. Reverse mathematics of the Lebesgue Differentiation Theorem.
2. Reverse mathematics of Peano systems.
3. Propagation of strong f-randomness.
4. Symbolic dynamics, Kolmogorov complexity, and $\mathcal{E}_{\mathsf{W}}$.
5. Hudelson's theorem on randomness extraction.
6. Embedding hyperarithmeticity into $\mathcal{E}_{\mathsf{W}}$ via LR-reducibility.

Reverse mathematics of the LDT.

Recall the Lebesgue Differentiation Theorem: For $f \in L_1([0,1]^d)$, for almost all $x \in [0,1]^d$,

$$(*) \qquad f(x) = \lim_{Q \to x} \frac{\int f \, d\mu}{\mu(Q)}$$

where Q is a cube containing x.

Theorem (Pathak/Rojas/Simpson 2010)**.** A point $x \in [0,1]^d$ is Schnorr random $\iff$ $(*)$ holds for all L_1-computable $f \in L_1([0,1]^d)$.

In the proof we exhibit a one-to-one correspondence between Schnorr tests and L_1-computable functions. This gives:

Theorem (Pathak/Rojas/Simpson 2010)**.** Given a computable sequence of L_1-computable functions in $L_1([0,1]^d)$, we can find a dense set of computable points $x \in [0,1]^d$ such that $(*)$ holds for all members of the sequence. Indeed, any effectively closed set of computable positive measure contains such computable points.

Reverse mathematics of Peano systems.

A *system* is an ordered triple A, c, f where A is a set, $c \in A$, and $f : A \to A$.

A system is said to be *inductive* if it has no proper subsystem.

A *Peano system* is an inductive system such that $c \notin \text{rng}(f)$ and f is one-to-one.

The standard example of a Peano system is $\mathbb{N}, 0, S$ where S is the *successor function*, i.e., $S(n) = n + 1$ for all $n \in \mathbb{N}$.

Theorem (Dedekind 1888)**.**
Any two Peano systems are isomorphic.

This is the beginning of Dedekind's set-theoretic foundation for mathematics (Dedekind cuts, etc.).

Theorem (Simpson/Yokoyama 2011)**.**
Dedekind's theorem is equivalent over RCA_0^* to WKL_0.

Recall from Simpson/Smith 1986 that $\text{RCA}_0^* = \text{RCA}_0 - \Sigma_1^0$-induction $+ \forall n \exists 2^n$.

Strong f-randomness.

Let $f : \{0,1\}^* \to (-\infty, \infty)$ be computable.
Say that $x \in \{0,1\}^{\mathbb{N}}$ is *strongly f-random* if
$\exists c \forall n \, (\mathrm{KA}(x\restriction\{1,\ldots,n\}) > f(x\restriction\{1,\ldots,n\}) - c)$.

Here KA = *a priori Kolmogorov complexity*,
i.e., $\mathrm{KA}(\sigma) = -\log_2 m(\sigma)$
where m is a universal left r.e. semimeasure.

Note that KA is similar but not identical to
KP = prefix-free Kolmogorov complexity.

Strong f-randomness has been studied by
Calude/Staiger/Terwijn, APAL, 2006, and
Reimann/Stephan, Proceedings of the 9th
Asian Logic Conference, 2006.

When $f(\sigma) = s|\sigma|$ this is closely related to
effective Hausdorff dimension as pioneered
in Reimann's Ph.D. thesis, 2004.

Propagation of strong f-randomness.

Theorem 1 (Simpson, 2011)**.**
Assume x is strongly f-random and $x \leq_{\mathsf{T}} y$ where y is Martin-Löf random relative to z. Then x is strongly f-random relative to z.

Remark. The special case $f(\sigma) = |\sigma|$, i.e., when x is Martin-Löf random, is due to Joseph S. Miller and Liang Yu, TAMS, 2008.

Theorem 2 (Simpson, 2011)**.**
Let I be a countable index set. Assume that

$$(\forall i \in I)\,(x_i \text{ is strongly } f_i\text{-random}).$$

Then, we can find a PA-oracle z such that $(\forall i \in I)\,(x_i$ is strongly f_i-random rel. to $z)$.

Remark. The special case $|I| = 1$, $f(\sigma) = |\sigma|$ is due to Rod Downey, Denis Hirschfeldt, Joseph S. Miller, and André Nies, JML, 2005.

Remark. I do not know whether Theorems 1 and 2 hold with KA replaced by KP.

Symbolic dynamics and complexity.

A *symbolic system* is a nonempty closed set $X \subseteq A^G$ which is *shift-invariant*,
i.e., $x \in X, g \in G \Rightarrow x^g \in X$.

Here A is a finite set of symbols, and G is one of the semigroups $\mathbb{Z}^d$ or $\mathbb{N}^d$ where $d \geq 1$.

If $G = \mathbb{Z}^d$ we write $F_n = \{-n, \ldots, n\}^d$.
If $G = \mathbb{N}^d$ we write $F_n = \{1, \ldots, n\}^d$.

Theorem (Simpson 2010)**.**

1. $\mathrm{effdim}(X) = \dim(X) = \mathrm{ent}(X)$.

2. $\dim(X) \geq \limsup_{n\to\infty} \dfrac{\mathrm{KP}(x\restriction F_n)}{|F_n|}$ for all $x \in X$.

3. $\dim(X) = \lim_{n\to\infty} \dfrac{\mathrm{KP}(x\restriction F_n)}{|F_n|}$ for many $x \in X$.

Here $\dim(X) =$ the Hausdorff dimension of X, and $\mathrm{ent}(X) =$ the *entropy* of X,
a well known conjugacy invariant
which goes back to Kolmogorov.

Remark. The proof of the above theorem involves ergodic theory (the Variational Principle, Shannon/McMillan/Breiman, etc.) plus a combinatorial argument which is similar to the proof of the Vitali Covering Lemma.

Remark. The above theorem seems so fundamental that it could have been noticed long ago. Nevertheless, I have not been able to find it in the literature. So far as I can tell, everything in the theorem is new, except the following result of Furstenberg 1967:

$$\dim(X) = \mathrm{ent}(X) \text{ provided } G = \mathbb{N}.$$

The proof of this special case is much easier.

Remark. The above theorem is an outcome of my discussions at Penn State during February–April 2010 with many people including John Clemens, Mike Hochman, Dan Mauldin, Jan Reimann, and Sasha Shen.

Degrees of unsolvability (Muchnik).

Let X be any set of reals. We view X as a *mass problem*, viz., the problem of "finding" some $x \in X$.

In order to interpret "finding," we use Turing's concept of computability.

Accordingly, we say that X is *algorithmically solvable* if X contains some computable real, or in other words, $X \cap \mathrm{REC} \neq \emptyset$.

Similarly, we say that X *is algorithmically reducible to* Y if each $y \in Y$ can be used as a Turing oracle to compute some $x \in X$.

The *degree of unsolvability* of X, $\deg(X)$, is the equivalence class of X under mutual algorithmic reducibility.

Reference:

Albert A. Muchnik, On strong and weak reducibilities of algorithmic problems, Sibirskii Matematicheskii Zhurnal, 4, 1963, 1328–1341, in Russian.

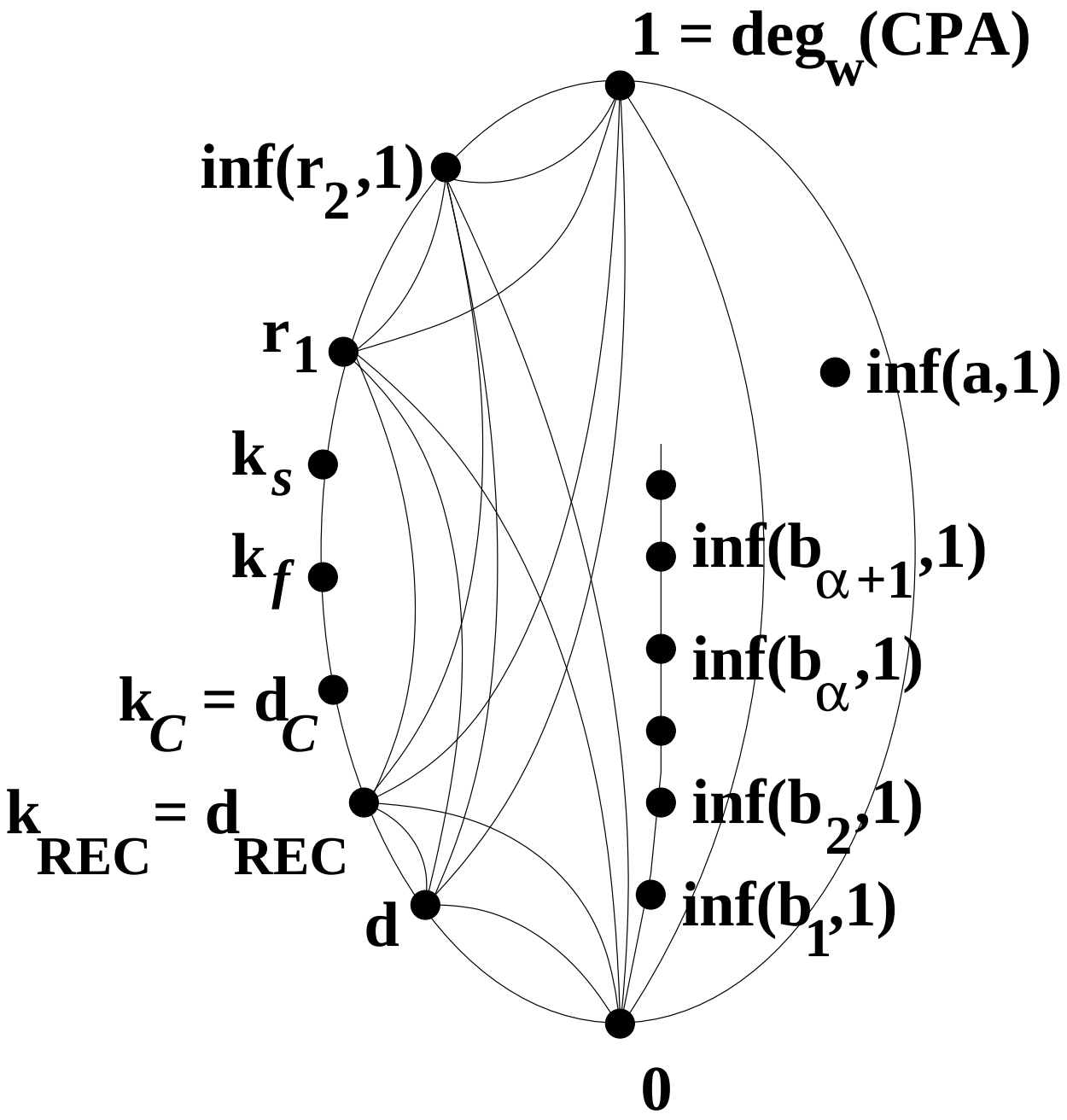
Symbolic dynamics, continued.

I have been applying recursion-theoretic concepts to obtain new results in symbolic dynamics. Given a symbolic system X, the program is to explore the relationship between familiar *dynamical properties* of X and the *degree of unsolvability* of X, i.e., its Muchnik degree, $\deg(X)$. Note that $\deg(X)$, like $\mathrm{ent}(X)$, is a conjugacy invariant.

For example, if X is of finite type and *minimal* (i.e., every orbit is dense), then $\deg(X) = \mathbf{0}$ (Hochman, 2009). More generally, this holds if X is effectively closed, i.e., not necessarily of finite type.

It is easy to see that if X is of finite type, then $\deg(X)$ belongs to $\mathcal{E}_{\mathrm{w}}$, the lattice of Muchnik degrees of nonempty effectively closed sets in the Cantor space. Conversely, every degree in $\mathcal{E}_{\mathrm{w}}$ is realized in this way (Simpson 2007).

This is interesting, because $\mathcal{E}_{\mathrm{w}}$ is very rich.



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

Randomness extraction.

Let $f : \mathbb{N} \to (-\infty, \infty)$ be an unbounded computable function such that $f(n) \leq f(n+1) \leq f(n) + 1$ for all n.

For example, $f(n)$ 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 $\mathbf{k}_f = \deg(\{x \in 2^{\mathbb{N}} \mid x \text{ is } f\textit{-random}\})$, i.e., $\exists c \forall n\, (\mathsf{KP}(x\restriction\{1, \ldots, n\} \geq f(n) - c)$.

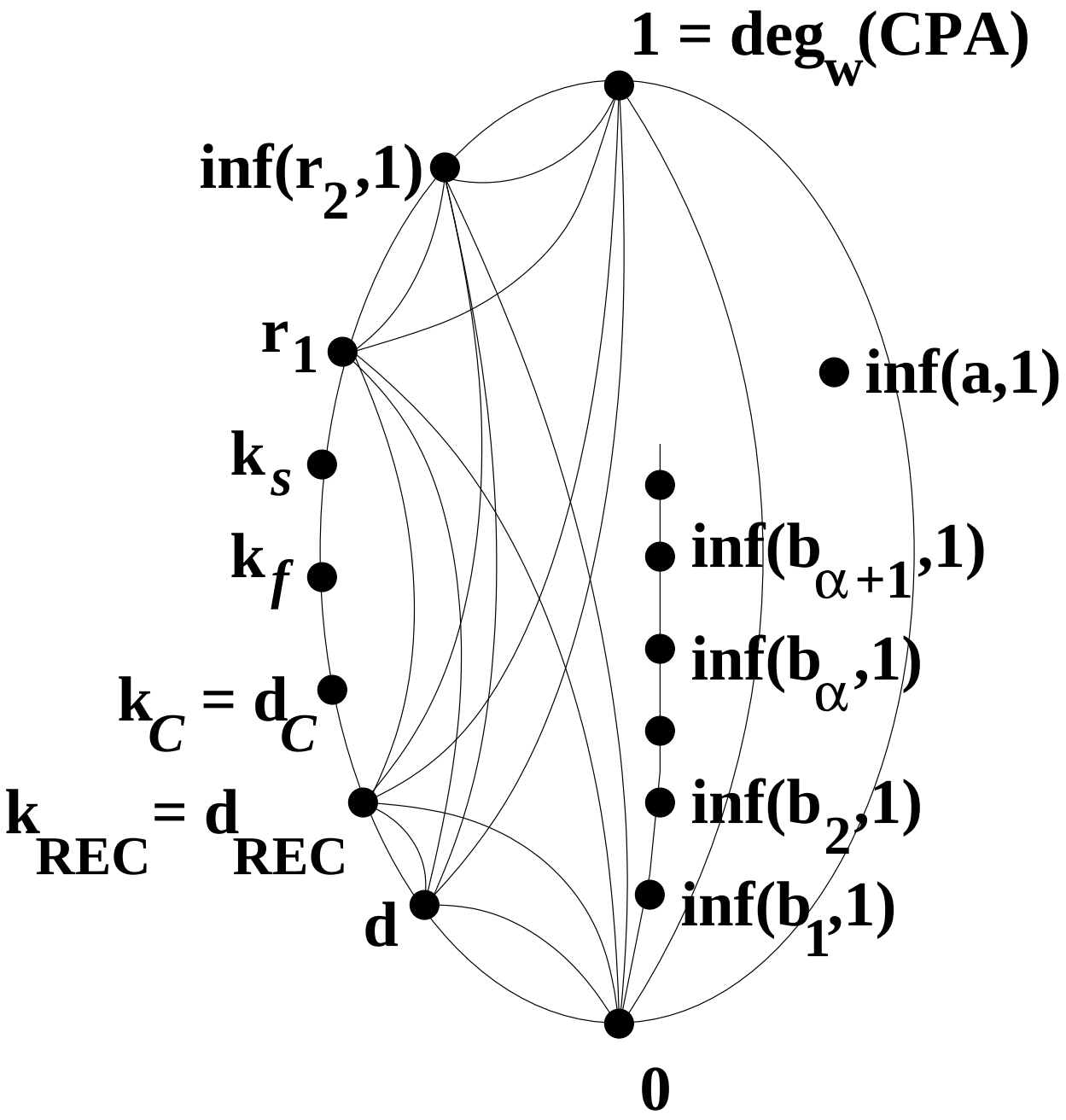
Theorem (Hudelson 2010)**.** $\mathbf{k}_f < \mathbf{k}_g$ provided $f(n) + 2\log f(n) \leq g(n)$ for all n.

In other words, there exists an f-random real with no g-random real Turing reducible to it.

References:

Phil Hudelson, Mass problems and initial segment complexity, 2010, in preparation.

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



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

Embedding HYP into $\mathcal{E}_{\mathsf{W}}$.

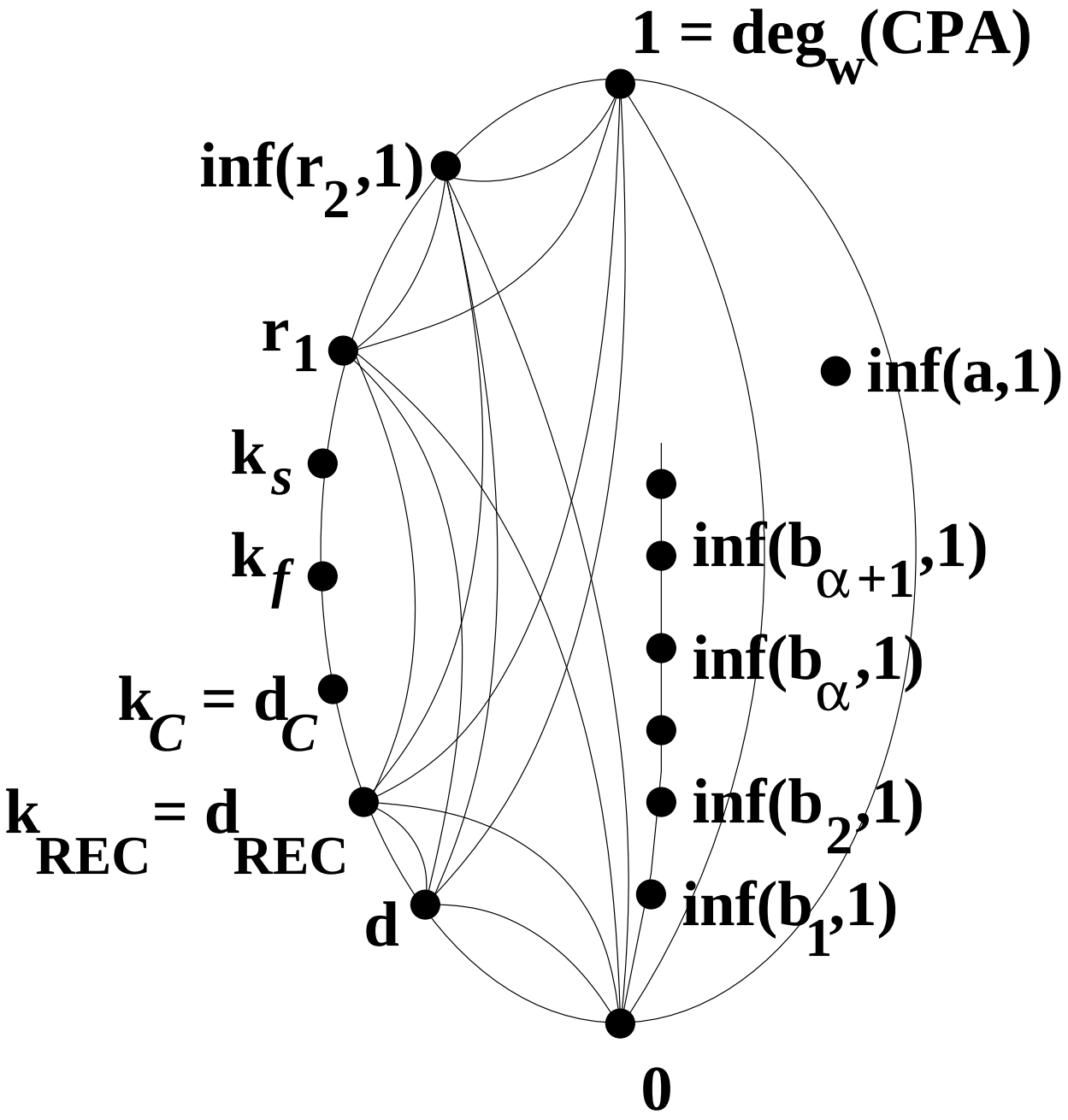
Let z be a Turing oracle. Define
$\mathsf{MLR}^z = \{x \in 2^{\mathbb{N}} \mid x \text{ is random relative to } z\}$
and $\mathsf{KP}^z(\tau) =$ the prefix-free Kolmogorov complexity of τ relative to z.

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

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 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 $\mathbf{b}_\alpha = \deg(\{z \mid 0^{(\alpha)} \leq_{\mathsf{LR}} z\})$ 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 $\mathcal{E}_{\mathrm{w}}$. 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, 2010, in preparation.

THE END. THANK YOU!