Introduction to Mass Problems

Stephen G. Simpson

Pennsylvania State University
NSF DMS-0600823, DMS-0652637
http://www.math.psu.edu/simpson/
simpson@math.psu.edu

Logic Seminar

Department of Mathematics

Pennsylvania State University

October 16, 2007

Abstract:

In an important and influential 1932 paper, Kolmogorov proposed a "calculus of problems" and noted its similarity to the intuitionistic propositional calculus of Brouwer and Heyting. According to Kolmogorov's informal idea, one problem is said to be "reducible" to another if any solution of the second problem can easily be transformed into a solution of the first problem.

In 1955 Kolmogorov's doctoral student Medvedev developed a rigorous elaboration of Kolmogorov's informal idea, in terms of Turing's theory of computability and unsolvability. A mass problem was defined to be a set of Turing oracles, i.e., an arbitrary subset of the Baire space. A mass problem was said to be solvable if it contains at least one computable member. One mass problem was said to be reducible to another if there exists a partial computable functional carrying all members of the second problem to members of the first problem. This reducibility notion is now known as strong reducibility, in contrast to the weak reducibility of Muchnik 1963, who required only that for each member of the second problem there exists a member of the first problem which is Turing reducible to it. On this basis Medvedev and Muchnik respectively noted that the strong and weak degrees of unsolvability form Brouwerian lattices.

Subsequently these lattices turned out to be an extremely useful tool in the classification of unsolvable problems arising in several areas of mathematics, including most recently dynamical systems.

The purpose of this talk is to introduce these ideas, which will be elaborated further in subsequent talks.

A. N. Kolmogoroff, Zur Deutung der intuitionistischen Logik, *Mathematische Zeitschrift*, 35, 58–65, 1932.

English translation, commentary, additional references are in: Andrei N. Kolmogorov, On the interpretation of intuititionistic logic, pages 151-158 and 451-466 of: *Selected Works of A. N. Kolmogorov*, Volume 1, Kluwer, 1991, XIX + 551 pages.

He proposes a "calculus of problems" ("Aufgabenrechnung"). One problem is "reducible" to another if any solution of the second yields a solution of the first.

"Es gilt dann die folgende merkwürdige Tatsache: Nach der Form fällt die Aufgabenrechnung mit der Brouwerschen, von Herrn Heyting neuerdings formalisierten, intuitionistischen Logik zusammen."

Translation:

"We then have the following remarkable fact: The calculus of problems coincides formally with the Brouwerian intuitionistic logic as recently formalized by Mr. Heyting."

Kolmogorov's informal proposal is now known as the BHK or Brouwer/Heyting/Kolmogorov interpretation of intuitionistic logic.

Kolmogorov's informal proposal in 1932 was later elaborated rigorously by two authors:

Yuri T. Medvedev, Degrees of difficulty of mass problems, *Doklady Akademii Nauk SSSR*, 104, 1955, 501–504, in Russian.

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

Medvedev was one of Kolmogorov's many doctoral students. In his Ph.D. thesis, Medvedev proposed a rigorous elaboration of Kolmogorov's nonrigorous idea. See also Medvedev's 1955 Doklady paper.

According to Medvedev, a *mass problem* is any set of Turing oracles, i.e., a subset of the Baire space, $\mathbb{N}^{\mathbb{N}}$. We use letters such as $A, B, \ldots$ to denote mass problems.

Recall that a partial functional

$$\Phi :\subseteq \mathbb{N}^{\mathbb{N}} \longrightarrow \mathbb{N}^{\mathbb{N}}$$

is said to be *computable* if there exists a program $\mathcal{P}$ which computes Φ in the following sense: for all $f, g \in \mathbb{N}^{\mathbb{N}}$, $\Phi(f) = g$ if and only if for all $n \in \mathbb{N}$, the run of the program $\mathcal{P}$ with input n using f as a Turing oracle eventually halts with output $g(n)$.

Here are Medvedev's definitions.

Let A and B be mass problems, i.e., A and B are subsets of $\mathbb{N}^{\mathbb{N}}$.

We say that B *is reducible to* A if there exists a computable partial functional Φ as above such that $A \subseteq \mathrm{dom}(\Phi)$ and, for all $f \in A$, $\Phi(f) \in B$.

Intuitively, a "problem" is identified with its set of solutions. Thus, the "solutions" of the "problem" A are just the elements of A.

A problem A is said to be *solvable* if it has at least one computable solution. A problem B is said to be *reducible* to a problem A if there exists a computable partial functional which maps any solution of A to a solution of B.

Let A and B be mass problems. We say that A and B *are of the same degree of difficulty* if A is reducible to B and B is reducible to A.

A *degree of difficulty* is an equivalence class of mass problems under the above equivalence relation. The degree of difficulty of the mass problem A is denoted deg(A).

We use letters such as $\mathbf{a}, \mathbf{b}, \ldots$ to denote degrees of difficulty.

Let $\mathcal{D}$ denote the set of degrees of difficulty. The cardinality of $\mathcal{D}$ is the same as the cardinality of the set of mass problems, $2^{2^{\aleph_0}}$.

We partially order $\mathcal{D}$ by defining deg(B) $\leq$ deg(A) if and only if B is reducible to A. Thus $\mathcal{D}$ is a partially ordered set.

Indeed, Medvedev noted that $\mathcal{D}$ is a Brouwerian lattice. See below.

Review of lattice theory:

A *partially ordered set* is an ordered pair $(P, \leq)$ such that P is a set and $\leq$ is a binary relation on P with the following properties:

1. $a \leq a$ for all $a \in P$ (reflexivity).
2. $a \leq b$, $b \leq c$ imply $a \leq c$ (transitivity).
3. $a \leq b$, $b \leq a$ imply $a = b$ (antisymmetry).

A *lattice* is a partially ordered set $(L, \leq)$ such that any two elements $a, b \in L$ have a least upper bound in L and a greatest lower bound in L.

We use sup(a, b) to denote the least upper bound of a and b. We use inf(a, b) to denote the greatest lower bound of a and b.

An example of a lattice is the set of positive integers under divisibility: $a \leq b$ if and only if a is a divisor of b. Then sup(a, b) is the least common multiple of a and b, and inf(a, b) is the greatest common divisor of a and b.

Note that for any lattice $(L, \leq)$ there is also the *dual lattice* $(L, \geq)$.

A lattice $(L, \leq)$ is said to be *distributive* if

$$\sup(a, \inf(b, c)) = \inf(\sup(a, b), \sup(a, c))$$

for all $a, b, c \in L$.

It can be shown that the distributive law is *self-dual* in the sense that it is equivalent to the dual property

$$\inf(a, \sup(b, c)) = \sup(\inf(a, b), \inf(a, c))$$

for all $a, b, c \in L$. In other words, a lattice $(L, \leq)$ is distributive if and only if the dual lattice $(L, \geq)$ is distributive.

In any lattice L we define 0 and 1 to be the bottom and top elements of L, if they exist.

Medvedev 1955 noted that
the partial ordering of degrees of difficulty
is a distributive lattice with 0 and 1.

Let $\mathbf{a} = \text{deg}(A)$ and $\mathbf{b} = \text{deg}(B)$. Then

$$\text{sup}(\mathbf{a}, \mathbf{b}) = \text{deg}(A \times B)$$

where

$$A \times B = \{f \oplus g \mid f \in A, g \in B\}$$

and

$$\text{inf}(\mathbf{a}, \mathbf{b}) = \text{deg}(A + B)$$

where

$$A + B = \{\langle 0 \rangle^\frown f \mid f \in A\} \cup \{\langle 1 \rangle^\frown g \mid g \in B\}.$$

The bottom element 0 is $\text{deg}(A)$ for any A which contains a computable element, i.e., A is a solvable mass problem.

The top element 1 is $\text{deg}(\emptyset)$. Here $\emptyset$ is the empty set, i.e., the problem with no solutions whatsoever.

Review of lattice theory, continued:

Let L be a distributive lattice with 0 and 1.

For $a, b \in L$ let $a \Rightarrow b$ be the unique minimum $x \in L$ such that sup$(a, x) \geq b$, if it exists.

L is *Brouwerian* if $a \Rightarrow b$ exists for all $a, b \in L$.

Note that this property is not self-dual.

Fact: Each Brouwerian lattice is a model of intuitionistic propositional calculus:

$a \wedge b =$ sup(a, b), $a \vee b =$ inf(a, b),

$a \Rightarrow b$ as above, $\neg\, a = (a \Rightarrow 1)$,

$a \vdash b$ if and only if $a \geq b$.

Completeness Theorem (Tarski 1938)**:**
A first-order propositional formula is intuitionistically valid if and only if it is identically 0 in all Brouwerian lattices. This holds if and only if it is identically 0 in all <u>finite</u> Brouwerian lattices.

Medvedev 1955 noted that the lattice of all degrees of difficulty is Brouwerian.

For $\mathbf{a} = \deg(A)$ and $\mathbf{b} = \deg(B)$ we have

$$(\mathbf{a} \Rightarrow \mathbf{b}) \;=\; \deg(A \Rightarrow B)$$

where $A \Rightarrow B$ is the set of all $\langle n \rangle ^\frown h$ with the following properties: $n \in \mathbb{N}$, $h \in \mathbb{N}^{\mathbb{N}}$, and n is the Gödel number of a program which defines a computable partial functional Φ such that $\Phi(f \oplus h) \in B$ for all $f \in A$.

In other words, $A \Rightarrow B$ is the set of "codes" for continuous functionals which map each element of A to an element of B.

Letting $\mathbf{a}, \mathbf{b}, \mathbf{c}$ denote degrees of difficulty, it is straightforward to prove that $\mathbf{a} \Rightarrow \mathbf{b}$ is the least $\mathbf{c}$ such that $\sup(\mathbf{a}, \mathbf{c}) \geq \mathbf{b}$.

The proof uses the Enumeration Theorem. This is Turing's fundamental theorem which states the existence of universal programs.

The next important paper is:

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

This is the same Muchnik who in 1956 proved the famous Friedberg/Muchnik Theorem: there exist incomparable, recursively enumerable Turing degrees.

For $f, g \in \mathbb{N}^{\mathbb{N}}$ recall that g *is Turing reducible to* f, abbreviated $g \leq_T f$, if there exists a computable partial functional Φ such that $f \in \text{dom}(\Phi)$ and $\Phi(f) = g$. In other words, there exists a program $\mathcal{P}$ such that for all n, the run of $\mathcal{P}$ with input n using f as a Turing oracle eventually halts with output $g(n)$.
In other words, g is computable using f as an oracle.

Let $A, B \subseteq \mathbb{N}^{\mathbb{N}}$ be mass problems. We say that B *is weakly reducible to* A, abbreviated $B \leq_w A$, if for each $f \in A$ there exists $g \in B$ such that $g \leq_T f$.

This definition of Muchnik is a non-uniform variant of Medvedev's definition. Muchnik uses the term *strong reducibility*, abbreviated $\leq_s$, to refer to Medvedev's notion of reducibility as defined previously, in contrast to weak reducibility, $\leq_w$, as defined above.

From now on we write $\deg_s(A)$ for the *strong degree* of A, i.e., the degree of difficulty of A. This is also known as the *Medvedev degree* of A. The set of all strong degrees, previously denoted $\mathcal{D}$, is now denoted $\mathcal{D}_s$.

Let A and B be mass problems. We say that A and B *are of the same weak degree*, abbreviated $A \equiv_w B$, if $A \leq_w B$ and $B \leq_w A$. The *weak degrees* are the equivalence classs under $\equiv_w$. Weak degrees are also known as *Muchnik degrees*. The weak degree of A is denoted $\deg_w(A)$. The weak degrees are partially ordered by letting $\deg_w(B) \leq \deg_w(A)$ if and only if $B \leq_w A$. The partial ordering of all weak degrees is denoted $\mathcal{D}_w$.

Muchnik proved that the partial ordering $\mathcal{D}_w$ of weak degrees is a Brouwerian lattice. For $\mathbf{a} = \deg_w(A)$ and $\mathbf{b} = \deg_w(B)$ we have $\sup(\mathbf{a}, \mathbf{b}) = \deg_w(A \times B)$ and $\inf(\mathbf{a}, \mathbf{b}) = \deg_w(A + B)$ just as before. On the other hand, we also have $\inf(\mathbf{a}, \mathbf{b}) = \deg_w(A \cup B)$. Moreover, $(\mathbf{a} \Rightarrow \mathbf{b}) = \deg_w(A \Rightarrow B)$ where now $A \Rightarrow B$ is the set of $h \in \mathbb{N}^{\mathbb{N}}$ such that for all $f \in A$ there exists $g \in B$ such that $g \leq_T f \oplus h$. This is somewhat different from the Medvedev case.

Comparing the weak and strong degrees to the Turing degrees:

For $f, g \in \mathbb{N}^{\mathbb{N}}$ let $\deg_T(f)$ denote the *Turing degree* or *degree of unsolvability* of f, i.e., the equivalence class of f under the equivalence relation $f \equiv_T g$, i.e., $f \leq_T g$ and $g \leq_T f$. The Turing degrees are partially ordered by letting $\deg_T(g) \leq \deg_T(f)$ if and only if $g \leq_T f$. Let $\mathcal{D}_T$ be the partial ordering of Turing degrees.

It can be shown that $\mathcal{D}_T$ is an *upper semilattice*, i.e., for all $\mathbf{a}, \mathbf{b} \in \mathcal{D}_T$ we have $\sup(\mathbf{a}, \mathbf{b}) \in \mathcal{D}_T$. Moreover $\mathcal{D}_T$ has a bottom element, $\mathbf{0}$, the Turing degree of computable functions. On the other hand, $\mathcal{D}_T$ is not a lattice and does not have a top element.

There are obvious, natural embeddings of $\mathcal{D}_T$ into $\mathcal{D}_s$ and $\mathcal{D}_w$. Namely, we map $\deg_T(f)$ to $\deg_s(\{f\})$ and $\deg_w(\{f\})$ respectively. Here $\{f\}$ is the singleton set consisting of one element, f. These embeddings preserve the partial ordering and semilattice structure of $\mathcal{D}_T$ as well as the bottom element.

For any partially ordered set $(P, \leq)$, there is a complete distributive lattice $(P^*, \leq)$ consisting of the upward closed subsets of P partially ordered by $U \leq V$ if and only if $U \supseteq V$. It can be shown that $\mathcal{D}_w$ is isomorphic to $\mathcal{D}_T^*$. Moreover, any complete distributive lattice is Brouwerian. This is an alternative way to verify that $\mathcal{D}_w$ is Brouwerian.

Motivation:

We are primarily interested in $\mathcal{D}_s$ and $\mathcal{D}_w$ not so much because of intuitionistic logic, but rather as a framework for classifying unsolvable mathematical problems.

Let $\mathcal{D}_T$ be the upper semilattice of all Turing degrees, a.k.a., "degrees of unsolvability."

In $\mathcal{D}_T$ there are a great many specific, interesting Turing degrees, namely

$$\mathbf{0} < \mathbf{0}' < \mathbf{0}'' < \cdots < \mathbf{0}^{(\alpha)} < \mathbf{0}^{(\alpha+1)} < \cdots$$

where α runs through (a large initial segment of) the countable ordinal numbers (depending on whether V=L or not . . .). See my paper *The hierarchy based on the jump operator*, Kleene Symposium, North-Holland, 1980.

Historically, the original purpose of $\mathcal{D}_T$ (Turing 1936, Kleene/Post 1940's, 1950's) was to serve as a framework for classifying unsolvable mathematical problems.

In the 1950's, 1960's, and 1970's, it turned out that many specific, natural, well-known, unsolvable mathematical problems are indeed of Turing degree $\mathbf{0}'$:

- the Halting Problem for Turing machines (Turing's original example)

- the Word Problem for finitely presented groups

- the Triviality Problem for finitely presented groups, etc.

- Hilbert's 10th Problem for Diophantine equations

- and many others.

In addition, the **arithmetical hierarchy**

$$\mathbf{0}^{(n)}, \quad n < \omega$$

and the **hyperarithmetical hierarchy**

$$\mathbf{0}^{(\alpha)}, \quad \alpha < \omega_1^{\mathsf{CK}}$$

have been useful in studying the foundations of mathematics.

These hierarchies, based on iterating the Turing jump operator, have been useful precisely because of their ability to classify unsolvable mathematical problems.

This aspect of $\mathcal{D}_T$ is explored in my book *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1999, which is the basic reference on reverse mathematics.

On the other hand, there are many unsolvable mathematical problems which do not fit into the $\mathcal{D}_T$ framework at all.

For example, consider the following problem, which we call CPA:

> To find a complete, consistent theory which includes Peano Arithmetic.

Note that CPA is a very natural problem, in view of the Gödel Incompletness Theorem, which says that Peano Arithmetic itself is incomplete.

Moreover, by the work of Tarski, Gödel, and Rosser, the problem CPA is "unsolvable" in the sense that there is no *computable*, complete, consistent theory which includes Peano Arithmetic.

However (and this is the interesting point), it is not possible to assign a specific Turing degree ("degree of unsolvability") to the unsolvable problem CPA.

CPA is this unsolvable problem:

> To find a complete, consistent theory which includes Peano Arithmetic.

Although CPA is unsolvable, *there is no one specific Turing degree* associated to CPA. Thus, the Turing degree framework fails to classify CPA.

Digression: One may consider the Turing degree $\mathbf{0}^{(\omega)}$. It is reasonable to associate $\mathbf{0}^{(\omega)}$ to True Arithmetic, which is one particular, complete, consistent extension of Peano Arithmetic. However, it is unreasonable to associate $\mathbf{0}^{(\omega)}$ to the problem CPA as a whole. This is because, beyond True Arithmetic, there are many other complete, consistent extensions of Peano Arithmetic. Some of them even have Turing degree $< \mathbf{0}'$.

If we want to classify unsolvable problems such as CPA, we need a different framework.

The appropriate framework is:

MASS PROBLEMS.

Here are some more examples.

R_1: To find an infinite sequence of 0's and 1's which is *random* in the sense of Martin-Löf.

R_n: To find an infinite sequence of 0's and 1's which is n-*random*, $n = 1, 2, \ldots$.

DNR: To find a function f which is *diagonally nonrecursive*, i.e., $f(n) \neq \varphi_n^{(1)}(n)$ for all n.

$\mathsf{DNR}_{\mathsf{REC}}$: To find a function f which is diagonally nonrecursive and *recursively dominated*, i.e., there exists a recursive function g such that $f(n) < g(n)$ for all n.

AED: To find a Turing oracle A which is *almost everwhere dominating*, i.e., with probability 1, every function which is computable from a sequence of coin tosses is dominated by some function which is computable from A.

Each of the problems R_1, R_2, ..., DNR, $\mathsf{DNR}_{\mathsf{REC}}$, AED, ..., is similar to the problem CPA. In each case, the problem is *unsolvable* (i.e., there is no computable solution), but *there is no one specific Turing degree* that can be attached to the problem.

In other words, each of the problems

CPA, R_1, R_2, ..., DNR, DNR_{REC}, AED, ...,

is an example of an *unsolvable mass problem*.

If we wish to classify unsolvable problems of this kind, we need a concept of “degree of unsolvability” which is more general than the Turing degrees.

The appropriately generalized concept of “degree of unsolvability” is:

WEAK DEGREES,

also known as

MUCHNIK DEGREES.

This concept of “degree of unsolvability” is the one that has turned out to be most useful for classification and comparison of specific, natural, unsolvable mass problems.

The lattice $\mathcal{P}_w$:

We focus on Π^0_1 subsets of $2^{\mathbb{N}}$, i.e., $P = \{\text{paths through } T\}$ where T is a recursive subtree of $2^{<\mathbb{N}}$, the full binary tree of finite sequences of 0's and 1's. Two of the earliest pioneering papers on Π^0_1 subsets of $2^{\mathbb{N}}$ are by Jockusch/Soare 1972.

We define $\mathcal{P}_w$ to be the set of weak degrees of nonempty Π^0_1 subsets of $2^{\mathbb{N}}$, ordered by weak reducibility.

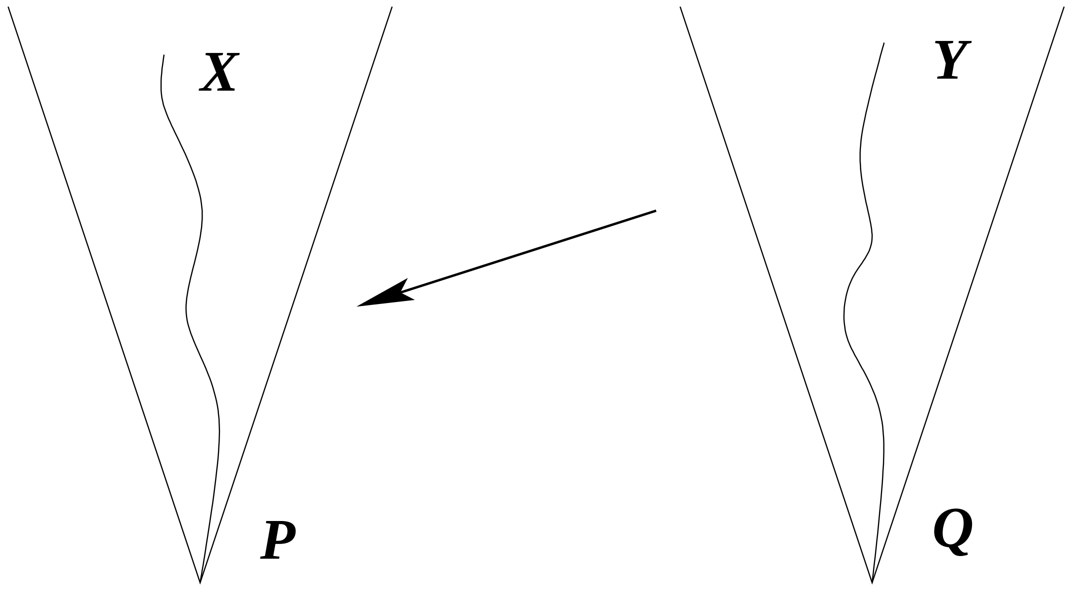
Basic facts about $\mathcal{P}_w$:

1. $\mathcal{P}_w$ is a distributive lattice, with l.u.b. given by $P \times Q = \{X \oplus Y \mid X \in P, Y \in Q\}$, and g.l.b. given by $P \cup Q$.

2. The bottom element of $\mathcal{P}_w$ is the weak degree of $2^{\mathbb{N}}$.

3. The top element of $\mathcal{P}_w$ is the weak degree of CPA $= \{\text{completions of Peano Arithmetic}\}$. (see Scott/Tennenbaum, Jockusch/Soare).

Weak reducibility of Π^0_1 subsets of $2^{\mathbb{N}}$:



$P \leq_w Q$ means:
$(\forall Y \in Q)\ (\exists X \in P)\ (X \leq_T Y)$.

P, Q are given by infinite recursive subtrees of the full binary tree of finite sequences of 0's and 1's.

X, Y are infinite (nonrecursive) paths through P, Q respectively.

The lattice $\mathcal{P}_w$ (review):

A *weak degree* is an equivalence class of subsets of ω^ω under the equivalence relation $P \leq_w Q$ and $Q \leq_w P$. The weak degrees have a partial ordering induced by $\leq_w$.

We define $\mathcal{P}_w$ to be the set of weak degrees of nonempty Π^0_1 subsets of 2^ω, partially ordered by weak reducibility.

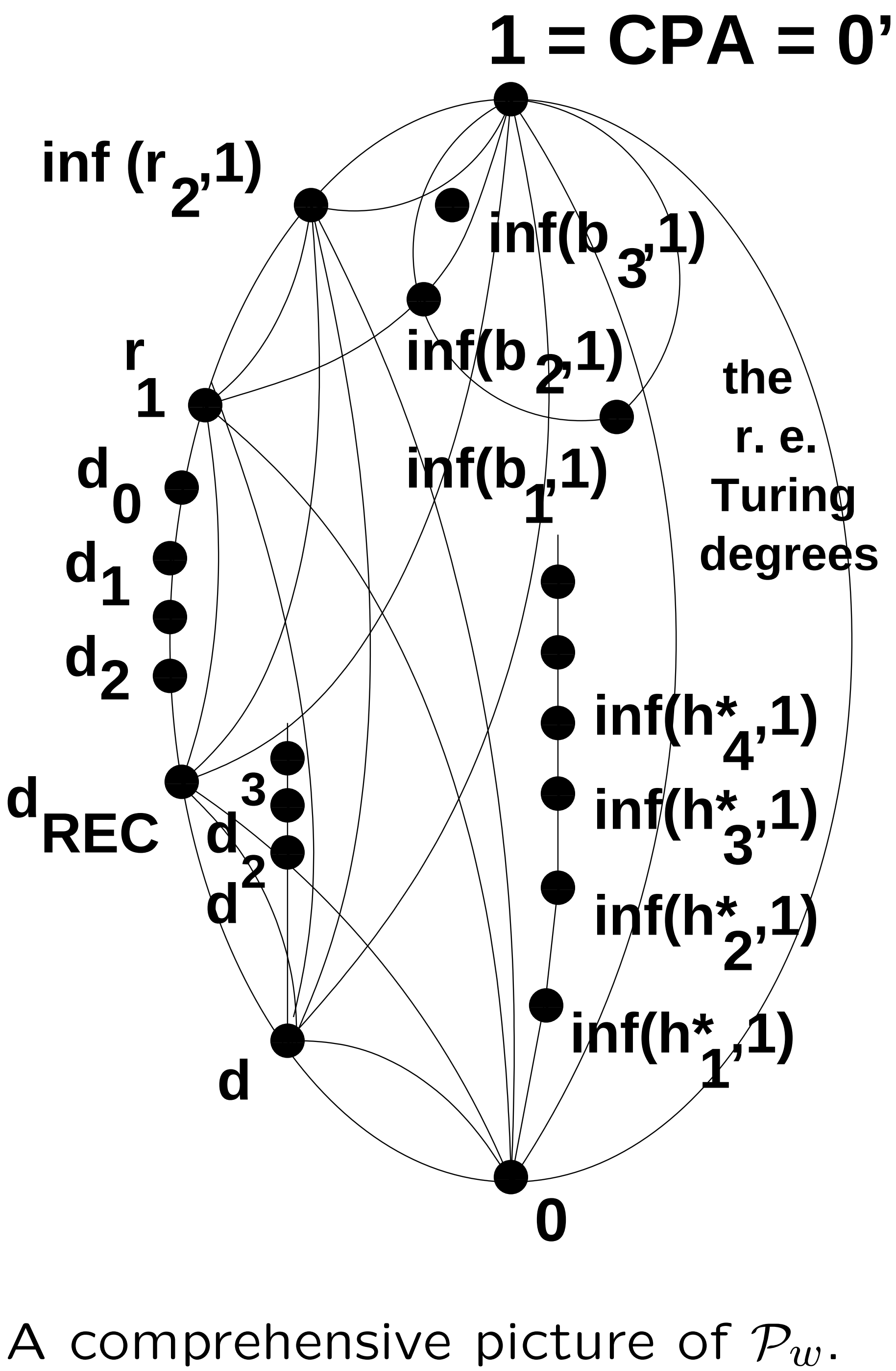
$\mathcal{P}_w$ is a countable distributive lattice.

The bottom element of $\mathcal{P}_w$ is the weak degree of 2^ω.

The top element of $\mathcal{P}_w$ is the weak degree of

$$\text{CPA} = \{\text{completions of Peano Arithmetic}\}.$$

We use $\mathbf{1}$ to denote this weak degree.



A comprehensive picture of $\mathcal{P}_w$.
$\mathbf{r} =$ randomness, $\mathbf{h} =$ hyperarithmeticity,
$\mathbf{b} =$ almost everywhere domination,
$\mathbf{d} =$ diagonal nonrecursiveness, etc.

Each of the big black dots in the previous slide represents a specific, interesting, weak degree in $\mathcal{P}_w$.

Subsequent talks in this series will explore the structure of $\mathcal{D}_w$ and $\mathcal{P}_w$ and the use of $\mathcal{D}_w$ and $\mathcal{P}_w$ in classifying unsolvable mathematical problems.

THE END