Applications of Computability Theory

Damir D. Dzhafarov
University of Notre Dame

13 January, 2012

“Turing got it right.” — Robert Soare

An incomplete history

1912 Turing is born in Paddington, London.

1936 Develops Turing machines, solves Entscheidungsproblem.

1938 Kleene proves recursion theorem.

1939 Turing defines oracle Turing machines.

1944 Post studies relative computability, formulates Post's problem.

1950 Davis and Robinson begin working on Hilbert's tenth problem.

1954 Kleene/Post introduce finite-extension forcing arguments.

1955 Medvedev writes about mass problems.

1957 Friedberg and Muchnik solve Post's problem.

1959 Shoenfield proves limit lemma.

1963 Sacks proves jump inversion theorem, density theorem.

Modern times

Study of algebraic structure of Turing degrees and combinatorial properties of subsets of ω.

Focus on development of powerful new techniques. Infinite injury, tree method.

Games introduced for understanding complicated constructions.

Generalized computability.

Automorphisms of the c.e. sets, definability, bi-interpretability.

Applications to models of Peano arithmetic. Π^0_1 classes and basis theorems. Computable model theory.

Computability theory applied to study of Ramsey's theorem.

Algorithmic randomness, mass problems, reverse mathematics.

Some early results of Turing and Church

1936 Turing gives an algorithm for computing a normal number, and shows that normal numbers have measure 1.

1940 Church writes about random sequences and computability.

These works mark the first applications of computability to randomness and complexity, as we know them today.

They demonstrate that the algorithmic properties of reals and sets of reals can offer insight about their analytic properties.

This leads to the need for a precise, formal notion of algorithmic randomness.

Passing all statistical tests

We can think of randomness as incompressibility, or as unpredictability, or as typicality (having no distinguishing features). Formalizing these intuitions results in several equivalent definitions.

A Martin-Löf test is a uniformly c.e. sequence $\mathcal{U} = (U_i)_{i\in\omega}$ of subsets of $2^{<\omega}$ such that $\lambda(U_i) \leq 2^{-i}$ for each i.

A sequence $A \in 2^\omega$ passes the test $\mathcal{U}$ if $A \notin \bigcap_{i\in\omega} U_i$.

A is Martin-Löf random if it passes every Martin-Löf test.

Example. Chaitin's Ω, or the halting probability, for a universal prefix-free Turing machine M is $\sum_{M(\sigma)\downarrow} 2^{-|\sigma|}$.

A selection of results

The class of random sequences has measure 1.

Martin-Löf. There exists a universal Martin Löf test, meaning one that is passed by precisely by the random sequences.

Van Lambalgen. A sequence $A = B \oplus C$ is random if and only if B and C are mutually random.

Some results of Kučera.

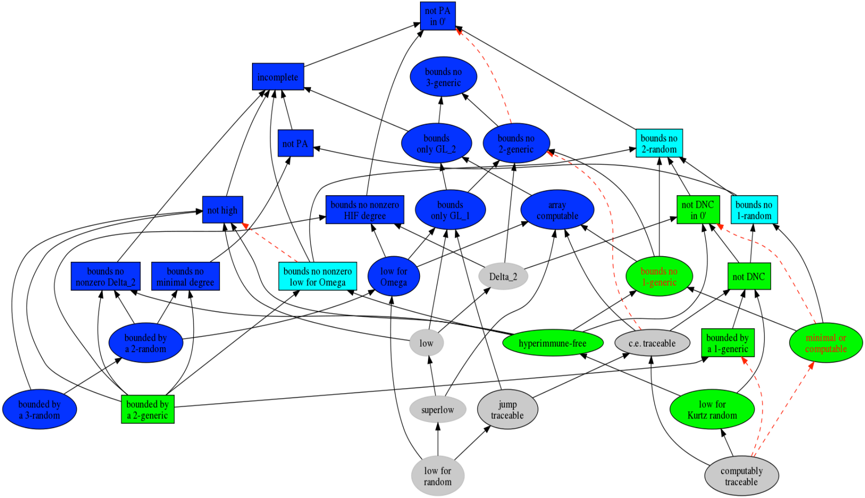
If A is a random sequence and P is a Π^0_1 class of positive measure, then P contains some shift of A.

Every set is computable from some random set.

No c.e. set is random, and the only c.e. random degree is $\mathbf{0}'$.

A myriad of related notions and connections

From The computability menagerie by J. Miller.



A foundational question

1944 Post refers to what will eventually be called Turing degrees as degrees of unsolvability.

The study of Turing degrees, especially c.e. degrees, played a crucial role in the development of computability theory as a robust subject.

But it is worth noting that, besides $\mathbf{0}, \mathbf{0}', \mathbf{0}'', \ldots$, there are no natural examples of Turing degrees, only of various classes of degrees.

Perhaps, then, "degrees of unsolvability" should be reserved for some more general notions than Turing degree and Turing reducibility.

A better notion of degree of unsolvability

A mass problem is a a collection of subsets of ω regarded as solutions to a particular problem.

Example. For an infinite tree $T \subseteq 2^{<\omega}$, the set $\{f \in 2^\omega : \forall n\, f \upharpoonright n \in T\}$ may be regarded as the set of solutions to the problem of finding an infinite path through T.

Given mass problems P and Q, we say:

P is weakly reducible or Muchnik reducible to Q, written $P \leq_w Q$, if every $f \in Q$ computes some $g \in P$;

P is strongly reducible or Medvedev reducible to Q, written $P \leq_s Q$, if there is a single reduction Φ such that $\Phi^f \in P$ for all $f \in Q$.

Equivalence classes under $\leq_w$ and $\leq_s$ give new notions of degree.

Examples of mass problems

Examples. Define the following weak degrees:

$\mathbf{PA}$ is the weak degree of the set of completions of Peano arithmetic.

$\mathbf{r}_n$ is the weak degree of the set of n-random reals.

$\mathbf{d}$ is the weak degree of the set of diagonally noncomputable functions.

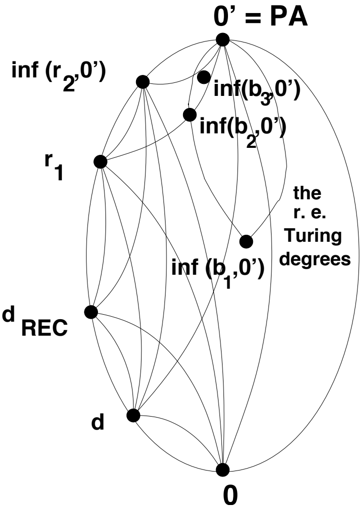
$\mathbf{d}_{\mathrm{REC}}$ is the weak degree of the set of computably bounded, diagonally noncomputable functions.

$\mathbf{b}_1$ is the weak degree of the set of almost everywhere dominating sets.

Let $\mathcal{E}_w$ be the collection of all weak degrees of Π^0_1 classes under $\leq_w$. All of the degrees above belong to $\mathcal{E}_w$, and $\mathbf{PA}$ is its greatest element.

A snapshot of $\mathcal{E}_w$

From Mass problems and degrees of unsolvability by S. Simpson.



Structural properties of $\mathcal{E}_w$

Binns. The analogue of Sacks's splitting theorem holds in $\mathcal{E}_w$.

Simpson and Binns. $\mathcal{E}_w$ is a countable distributive lattice.

Simpson. There is an embedding of $\mathcal{E}_T$ into $\mathcal{E}_w$ preserving $\mathbf{0}$ and $\mathbf{0}'$. The images of the non-zero degrees under this embedding are incomparable with the weak degrees defined above.

Simpson, Simpson and Binns. Natural properties only satisfied by Π^0_1 classes with weak degrees intermediate between $\mathbf{0}$ and $\mathbf{0}'$.

Open question. Does the analogue of the density theorem hold in $\mathcal{E}_w$?

Cenzer and Hinman. The answer is yes if the order is replaced by $\leq_s$.

From computability theory to proof theory

1948 Post proves what we now call Post's theorem.

1975 Friedman develops reverse mathematics.

Post's theorem gives a syntactic characterization of (relative) computability and computable enumerability. In particular, it says that the computable sets are precisely the Δ^0_1 sets in the arithmetical hierarchy.

Reverse mathematics builds a weak set theory with comprehension restricted to Δ^0_1-definable sets. Its goal is to calibrate the strength of (countable analogues of) mathematical theorems according to the minimal set-existence assumptions needed to prove them.

Second-order arithmetic, $\mathbb{Z}_2$

The language of $\mathbb{Z}_2$ is a two-sorted one, having:

variables of the first sort are intended to range over numbers, and are denoted $x, y, z, \ldots$;

variables of the second sort are intended to range over sets of numbers, and are denoted $X, Y, Z, \ldots$;

symbols for 0, 1, $+$, $\times$, $<$, and $=$ for first-order variables, and a symbol $\in$ connecting first-order and second-order variables.

The theory $\mathbb{Z}_2$ has the axioms of a discrete ordered ring, the full comprehension scheme, and the full induction scheme.

Reverse mathematics takes place in various subsystems of $\mathbb{Z}_2$.

The “big five” subsystems

Recursive comprehension axiom (RCA_0). Basic axioms of arithmetic, plus induction for Σ^0_1 formulas, and comprehension for Δ^0_1-definable sets.

Weak König’s lemma (WKL_0). RCA_0, plus the axiom that every infinite binary tree has an infinite path.

Arithmetical comprehension axiom (ACA_0). RCA_0, plus comprehension for sets definable by an arithmetical formula.

Arithmetical transfinite recursion (ATR_0). RCA_0, plus an axiom scheme that states that any arithmetically-defined functional $2^{\mathbb{N}} \to 2^{\mathbb{N}}$ may be iterated along any countable well-ordering, starting with any set.

Π^1_1 comprehension axiom (Π^1_1-CA_0). RCA_0, together with comprehension for Π^1_1-definable sets.

The "big five" subsystems

Intuitively, RCA_0 corresponds to computable mathematics, and as such is weak. It serves as a base system.

WKL_0 is the formalization of the existence, for every set A, of a set of PA degree relative to A.

ACA_0 corresponds to the assertion of the existence of jumps.

The restriction of induction to Σ^0_1 formulas means RCA_0 and WKL_0 cannot prove the infinitary pigeonhole principle.

Remarkably, most theorems of mathematics are either provable in RCA_0, or equivalent to one of the other four subsystems over RCA_0. Virtually all of non-set-theoretical mathematics is provable in Π^1_1-CA_0.

Some basic equivalences

Simpson. The following are provable in RCA_0:

Baire category theorem;

Intermediate value theorem;

Urysohn's lemma and the Tietze extension theorem.

The following are equivalent to WKL_0 over RCA_0:

Friedman. Heine/Borel theorem;

Simpson. Gödel's compactness theorem;

Brown and Simpson. Separable Hahn/Banach theorem;

Friedman, Simpson, and Smith. Every countable commutative ring has a prime ideal.

Some basic equivalences

The following are equivalent to ACA_0 over RCA_0:

Simpson. Ascoli lemma;

Friedman. Bolzano/Weierstrass theorem;

Folklore. The range of every $f : \mathbb{N} \to \mathbb{N}$ exists;

Friedman, Simpson, and Smith. Every countable commutative ring has a maximal ideal.

The following are equivalent to ATR_0 over RCA_0:

Friedman and Hirst. Any two countable well orderings are comparable;

Friedman, Simpson, and Smith. Ulm's theorem for countable reduced Abelian groups;

Steel; Simpson. Determinacy for open sets in the Baire space.

A sample proof

Theorem (Dzhafarov and Mummert). Over RCA_0, ACA_0 is equivalent to the statement that for every family $\langle A_0, A_1, \ldots \rangle$ there exists a maximal set I such that $A_i \cap A_j \neq \emptyset$ for all $i, j \in I$.

Proof. Given $\langle A_0, A_1, \ldots \rangle$, the obvious way to construct I can be carried out in ACA_0.

For the reversal, fix $f : \mathbb{N} \to \mathbb{N}$. We show that the range of f exists.

Define $\langle A_0, A_1, \ldots \rangle$ by letting A_i contain $2i$ and all odd numbers z such that $\exists x \leq z \; f(x) = i$. Thus A_i is either a singleton, or contains cofinitely many odd numbers.

Let I be as in the statement. Then $i \in I$ if and only if $i \in \mathrm{range}(f)$. Thus, the range of f exists by Δ^0_1-comprehension.

What does reverse mathematics offer?

Many implications $\varphi \to \psi$ in reverse mathematics consist in taking an instance A of ψ, computably in it building an instance B of φ, and then showing that every solution of B computes one of A.

Reverse mathematics offers more than just a different language for expressing computability-theoretic facts.

First order consequences: We can calibrate fine uses of induction in the proofs of various principles. This gives us greater insight into their strength, and raises questions leading to interesting new constructions.

Multiple applications. Certain implications $\varphi \to \psi$ may require more than one application of φ. We then have a clear proof-theoretic relationship that may be difficult to express using computability theory alone.

An example: Ramsey's theorem

For a set $S \subseteq \mathbb{N}$, let $[S]^n$ denote the set of all subsets of S of size n.

A k-coloring of n-tuples is a map $f : [S]^n \to k$.

A set $H \subseteq S$ is homogeneous for f if $f \restriction [H]^n$ is constant.

RT^n_k. For every infinite S, every $f : [S]^n \to k$ admits an infinite homogeneous $H \subseteq S$.

Obviously, RT^2_3 implies RT^2_2. The reverse implication can be proved as follows. Given $f : [\mathbb{N}]^2 \to 3$, define $g : [\mathbb{N}]^2 \to 2$ computable in f by $g(x, y) = 0$ if $f(x, y) = 0$ and $g(x, y) = 1$ otherwise.

If H is homogeneous for g with color 0, it is homogeneous for f.

If not, define $h : [H]^2 \to 2$ computable in $H \oplus f$ by $h(x, y) = f(x, y)$. Every homogeneous set for h is homogeneous for f.

Irregular principles

RT^2_2 is an interesting principle. It is irregular in that it is not captured by any of the "big five".

Jockusch; Simpson. RT^2_2 is not provable in WKL_0.

Seetapun. RT^2_2 is strictly weaker than ACA_0

Liu. RT^2_2 does not imply WKL_0.

The quest to understand the precise strength RT^2_2 has led to a more systematic study of irregular principles.

Cholak, Jockusch, and Slaman; Dzhafarov and Hirst. Variations of RT^2_2.

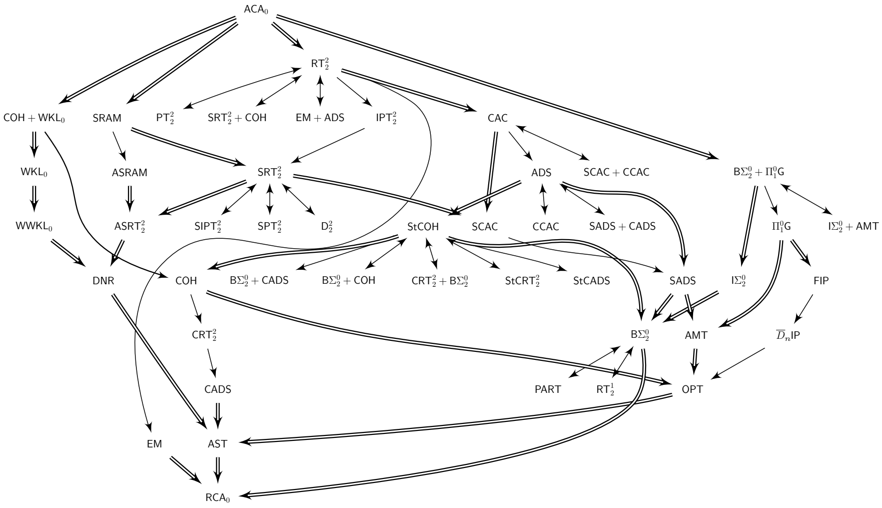
Hirschfeldt and Shore. Combinatorial principles.

Hirschfeldt, Shore, and Slaman. The atomic model theorem and AST.

Dzhafarov and Mummert. Equivalents of the axiom of choice.

Irregular principles

From the Reverse mathematics zoo by D. Dzhafarov.



“To really understand a mathematical principle, we have to study it using the tools computability theory, reverse mathematics, and algorithmic randomness.” — Denis Hirschfeldt

Thank you for your attention.