Aspects of Computability Theory

Antonio Montalbán.
University of Chicago

Kyoto, August 2006

Computable Sets

Definition: A set $A \subseteq \mathbb{N}$ is *computable* if there is a computer program that, on input n, decides whether $n \in A$.

Church-Turing thesis: This definition is independent of the programing language chosen.

Examples: The following sets are computable:

- The set of even numbers.
- The set of prime numbers.
- The set of stings that correspond to well-formed programs.

Recall that any finite object can be encoded by a natural number.

Examples of non-computable sets

The word problem: Consider the groups that can be constructed with a finite set of generators and a finite set of relations between the generators. The set of pairs (set-of-generators, relations), of **non-trivial** groups is **not** computable.

Simply connected manifolds: The set of finite triangulations of **simply connected** manifolds is **not** computable.

The Halting problem: The set of programs that **halt**, and don't run for ever, is **not** computable.

Basic definitions

Given sets $A, B \subseteq \mathbb{N}$ we say that *A is computable in B*, and we write $A \leqslant_T B$, if there is a computable procedure that can tell whether an element is in A or not using B as an *oracle*.

We say that *A is Turing equivalent to B*, and we write $A \equiv_T B$ if $A \leqslant_T B$ and $B \leqslant_T A$.

Example: The following sets are Turing equivalent.

- The set of pairs (set-of-generators, relations), of non-trivial groups;
- The set of finite triangulations of simply connected manifolds;
- The set of programs that halt.

The set of true arithmetic formulas is $>_T$ than the previous sets.

Basic definitions

Given sets $A, B \subseteq \mathbb{N}$ we say that A is computable in B, and we write $A \leqslant_T B$, if there is a computable procedure that can tell whether an element is in A or not using B as an *oracle*.

This defines a quasi-ordering on $\mathcal{P}(\mathbb{N})$.

We let $\mathbf{D} = (\mathcal{P}(\mathcal{D})/\equiv_T)$, and $\mathcal{D} = (\mathbf{D}, \leqslant_T)$.

Question: How does $\mathcal{D}$ look like?

Some simple observations about $\mathcal{D}$

- There is a least degree $\mathbf{0}$.
  The degree of the computable sets.
- $\mathcal{D}$ has the *countable predecessor property*,
  i.e., every element has at countably many elements below it.
  Because there are countably many programs one can write.
- Each Turing degree contains countably many sets.
- So, **D** has size $2^{\aleph_0}$.
  Because $\mathcal{P}(\mathbb{N})$ has size $2^{\aleph_0}$, and each equivalence class is countable.

Operations on $\mathcal{D}$

Turing Join

Every pair of elements $\mathbf{a}, \mathbf{b}$ of $\mathcal{D}$ has a least upper bound (or *join*), that we denote by $\mathbf{a} \cup \mathbf{b}$. So, $\mathcal{D}$ is an upper semilattice.

Given $A, B \subseteq \mathbb{N}$, we let $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$.
Clearly $A \leqslant_T A \oplus B$ and $B \leqslant_T A \oplus B$,
and if both $A \leqslant_T C$ and $B \leqslant_T C$ then $A \oplus B \leqslant_T C$.

Turing Jump

Given $A \subseteq \mathbb{N}$, we let A' be the *Turing jump of A*, that is,

$A' =$ {programs, with oracle A, thatHALT}.

For $\mathbf{a} \in \mathbf{D}$, let $\mathbf{a}'$ be the degree of the Turing jump of any set in $\mathbf{a}$

- $\mathbf{a} <_T \mathbf{a}'$
- If $\mathbf{a} \leqslant_T \mathbf{b}$ then $\mathbf{a}' \leqslant_T \mathbf{b}'$.

Operations on $\mathcal{D}$.

Definition

A jump upper semilattice (JUSL) is structure $(A, \leqslant, \vee, \mathrm{j})$ such that

- $(A, \leqslant)$ is a partial ordering.
- For every $x, y \in A$, $x \vee y$ is the l.u.b. of x and y,
- $x < \mathrm{j}(x)$, and
- if $x \leqslant y$, then $\mathrm{j}(x) \leqslant \mathrm{j}(y)$.

$\mathcal{D} = (\mathbf{D}, \leqslant_T, \vee, ')$ is a JUSL.

The Picture

- Sets below $\mathbf{0}'$ are classified from *Low* to *High*.
- Even thought there are no computable completions C of PA there are Low ones, that is $C' \equiv_T 0'$.
- We have $\mathbf{0} <_T \mathbf{0}' <_T \mathbf{0}'' <_T \ldots <_T \mathbf{0}^{(\omega)}$.
- A set is *arithmetic* if it is $\leqslant_T \mathbf{0}^{(n)}$ for some $n \in \omega$.
- $0^{(\omega)}$ is the set of true arithmetic formulas.
- We can continue along computable ordinals α $\mathbf{0}^{(\omega+1)} <_T \ldots <_T \mathbf{0}^{(\omega+\omega)} <_T \ldots <_T \mathbf{0}^{(\alpha)} <_T \ldots$
- A set is *hyperarithmetic* if it is $\leqslant_T \mathbf{0}^{(\alpha)}$ for some computable ordinal α.
- *Kleene's O*, the set of Halting Non-deterministic programs (where one is allows to choose natural numbers non-deterministically) computes all the hyperarithmetic sets.

Questions one may ask

- Are there incomparable degrees? YES
- Are there infinitely many degrees such that non of them can be computed from all the other ones toghether? YES
- What about $\aleph_1$ many? YES
- Is there a descending sequence of degrees $\mathbf{a}_0, \geqslant_T \mathbf{a}_1 \geqslant_T \ldots$.? YES

A more general question:

Which structures can be embedded into $\mathcal{D}$?

Embedding structures into $\mathcal{D}$

Theorem: The following structures can be embedded into the Turing degrees.

- Every countable upper semilattice. [Kleene, Post '54]
- Every partial ordering of size $\aleph_1$ with the countable predecessor property (c.p.p.). [Sacks '61]
  (It's open whether this is true for size $2^{\aleph_0}$.)
- Every upper semilattice of size $\aleph_1$ with the c.p.p. Moreover, the embedding can be onto an initial segment. [Abraham, Shore '86]
  (For size $\aleph_2$ it's independent of ZFC) [Groszek, Slaman 83]
- Every ctble. jump partial ordering $(A, \leqslant, ')$.[Hinman, Slaman '91]
  (For size $\aleph_1$ it's independent of ZFC) [M. 03]
- Every ctble. jump upper semilattice $(A, \leqslant, \vee, ')$ [M. '03]

History of Decidability Results.

- $\mathrm{Th}(\mathbf{D}, \leqslant_T)$ is undecidable. [Lachlan '68]
- $\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T)$ is decidable. [Kleene, Post '54]

Question: Which fragments of $\mathrm{Th}(\mathbf{D}, \leqslant_T, \vee, ')$ are decidable?

- $\exists\forall\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T)$ is undecidable. [Shmerl]
- $\forall\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, \vee)$ is decidable. [Jockusch, Slaman '93]
- $\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, ')$ is decidable. [Hinman, Slaman '91]
- $\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, \vee, ')$ is decidable. [M. 03]
- $\forall\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, \vee, ')$ is undecidable. [Slaman, Shore '05].

Question: Is $\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, \vee, ', 0)$ decidable?
Question: Is $\forall\exists - \mathrm{Th}(\mathbf{D}, \leqslant_T, ')$ decidable?

Two famous open question

Conjecture: [Sacks] There is no computable enumerable operator Φ such that for every $A, B \subseteq \omega$

- $A \equiv_T B \quad \Rightarrow \quad \Phi^A \equiv_T \Phi^B$,
- $A <_T \Phi^A <_T A'$.

Conjecture: [Slaman, Woodin] The structure of the Turing Degrees is *rigid*. That is, there are no automorphisms of $\mathcal{D}$ other than `id`.

1. Pure Computability Theory
   - Background
   - JUSL Embeddings

2. Computable Mathematics

3. Reverse Mathematics
   - Main question
   - The System $\mathcal{Z}_2$
   - The Main Five systems

4. Effective Randomness

Computable Mathematics

Study

1. how effective are constructions in mathematics;
2. how complex is to represent certain structures;

Various areas have been studied,

1. Combinatorics,
2. Algebra,
3. Analysis,
4. Model Theory

In many cases one needs to develop a better understanding of the mathematical structures to be able to get the computable analysis.

Example: effectiveness of constructions.

Theorem: Every Abelian ring has a maximal ideal.

Note: A countable ring $\mathcal{A} = (A, 0, 1, +_A, \times_A)$ can be encoded by three sets $A \subseteq \mathbb{N}$, $+_A \subseteq \mathbb{N}^3$ and $\times_A \subseteq \mathbb{N}^3$.
We say that $\mathcal{A}$ is *computable* if A, $+_A$ and $\times_\mathcal{A}$ are.

Theorem: Not every computable Abelian ring has a computable maximal ideal.
However, maximal ideals can be found computable in $\mathbf{0}'$.
Moreover, there are computable rings, all whose maximal ideals compute $\mathbf{0}'$.

Example: Represent Strucutres

Def: A linear ordering $\mathcal{L} = \langle L, \leqslant_L \rangle$ is *computable* if both $L \subseteq \mathbb{N}$ and $\leqslant_{\mathcal{L}} \subseteq \mathbb{N} \times \mathbb{N}$ are computable.

Def: The *degree* of the presentation $\langle L, \leqslant_L \rangle$ is $deg(L) \vee \deg(\leqslant_L)$.

Does every linear ordering have a computable presentation?
`No`. There are $2^{\aleph_0}$ isomorphism types of countable l.o.s.

Def: An isomorphism type of a structure $\mathcal{L}$ has *Turing Degree* X if X is the least degree of a presentation of $\mathcal{L}$

This doesn't work for any type of sructure.
Theorem: Every linear ordering has two isomorphic presentations $\mathcal{L}_1$ and $\mathcal{L}_2$ such that if $X \leqslant_T \mathcal{L}_1$ and $X \leqslant_T \mathcal{L}_2$ then $X \equiv_T 0$.

Degree Spectrum

Def: The *degree spectrum* of a structure $\mathcal{L}$ is
$$DegSp(\mathcal{L}) = \{deg(\mathcal{A}) : \mathcal{A} \cong \mathcal{L}\}.$$

Q: What are the possible spectrums of different structures.

Thm: For every Turing degree $\mathbf{x}$ there is a graph $\mathcal{G}$ such that
$$DegSp(\mathcal{G}) = \{\mathbf{a} : \mathbf{x} \leqslant_T \mathbf{a}\}.$$

Thm:[R. Miller] There is a linear ordering $\mathcal{L}$ such that every $\mathbf{a} <_T \mathbf{0}'$ is in $DegSp(\mathcal{L})$ exept for $\mathbf{0}$.

Thm: [Knight] If $\mathcal{L}$ is a non-trivial structure, then $DegSp(\mathcal{L})$ is closed uppwards.

Example: Represent Strucutres

Theorem: [Spector 55] Every hyperarithmetic well-ordering was a computable copy.

After a sequence of results of Feiner, Lerman, Jockusch, Soare, Downey, Seetapun:

Theorem: [Knight '00] For every non-computable set A, there is a linear ordering, Turing equivalent to A, without computable copies.

Theorem: [M.] For every hyperarithmetic linear ordering $\mathcal{L}$, there is a computable linear ordering $\mathcal{A}$ that is equimorphic to $\mathcal{L}$

that is, $\mathcal{A} \preccurlyeq \mathcal{L}$ and $\mathcal{L} \preccurlyeq \mathcal{A}$.

Reverse Mathematics

What axioms are necessary to do mathematics?

- Is the fifth postulate necessary for Euclidean geometry?
- Is Peano Arithmetic enough to prove all the true statements about the natural numbers?
- Which large cardinals can be proved to exists in ZFC?

Second Order Arithmetic

Simpson and Friedman's program of Reverse Mathematic deals with *Second Order Arithmetic ($\mathcal{Z}_2$).*

- In $\mathcal{Z}_2$ we can talk about finite and countable objects.
- $\mathcal{Z}_2$ is much weaker than ZFC,
- and its much stronger than PA.
- In $\mathcal{Z}_2$ one can talk about
  - Countable algebra,
  - (non-set theoretic) combinatorics,
  - Real numbers,
  - Manifolds, continuous functions, differential equations...
  - Complete separable metric spaces.
  - Logic, computability theory,...
  - ....

Main question revisted

1. Fix a base theory.
   (We use RCA_0 that essentially says that the computable sets exists)
2. Pick a theorem T.
3. What axioms do we need to add to RCA_0 to prove T.
4. Suppose we found axioms $A_0, \ldots, A_k$ of $\mathcal{Z}_2$ such that
   $$\mathsf{RCA}_0 \text{ proves } A_0 \ \& \ \ldots \ \& \ A_k \Rightarrow T.$$
   How do we know these are necessary?
5. It's often the case that RCA_0 also proves $T \Rightarrow A_0 \ \& \ \ldots \ \& \ A_k$
6. Then, we know that $\mathsf{RCA}_0 + A_0, \ldots, A_k$ is the least system (extending RCA_0) where T can be proved.

Axioms of $\mathcal{Z}_2$

Semi-ring Axioms: $\mathbb{N}$ is a ordered semi-ring.

Induction Axioms: For every formula $\varphi(n)$,
IND(φ) $(\varphi(0)\ \&\ \forall n(\varphi(n) \Rightarrow \varphi(n+1))) \Rightarrow \forall n \varphi(n)$

Comprehension Axioms: For every formula $\varphi(n)$
CA(φ) $\exists X \forall n\ (n \in X \Leftrightarrow \varphi(n))$

RCA_0 consists of: Semi-ring Axioms + Σ^0_1-IND+ Δ^0_1-CA.

Δ^0_1-CA is equivalent to: for every comp. program p any oracle Y, there is a set X such that

$$n \in X \Leftrightarrow p^Y(n) = yes$$

(where p can use information from sets that we know exist)

The big five

$$
\begin{array}{c}
\Pi^1_1\text{-CA}_0 \\
| \\
\text{ATR}_0 \\
| \\
\text{ACA}_0 \\
| \\
\text{WKL}_0 \\
| \\
\text{RCA}_0
\end{array}
$$

ACA_0

Def:
A formula is *arithmetic* if it has no quantifiers over sets.

ACA_0 is $\mathrm{RCA}_0 +$ Arithmetic comprehension.

where *Arithmetic comprehension* is the scheme of axioms

$\mathrm{CA}(\varphi)$ $\qquad \exists X \forall n\, (n \in X \Leftrightarrow \varphi(n))$

where φ is any arithmetic formula.

$$\begin{array}{c} \Pi^1_1\text{-}\mathrm{CA}_0 \\ | \\ \mathrm{ATR}_0 \\ | \\ \mathrm{ACA}_0 \\ | \\ \mathrm{WKL}_0 \\ | \\ \mathrm{RCA}_0 \end{array}$$

Theorem

The following are equivalent over RCA_0:

- *ACA_0*
- *For every set X, its jump X' exists.*
- *Every ab. ring has a maximal ideal.*

WKL_0

$$\begin{array}{c} \Pi^1_1\text{-}\mathrm{CA}_0 \\ | \\ \mathrm{ATR}_0 \\ | \\ \mathrm{ACA}_0 \\ | \\ \mathrm{WKL}_0 \\ | \\ \mathrm{RCA}_0 \end{array}$$

WKL_0 is RCA_0+ Weak König's lemma.

Weak König's lemma says: Every infinite subtree of the full binary tree has an infinite path.

Theorem

The following are equivalent over RCA_0:

- *WKL_0*
- *Every continuous function on $[0, 1]$ is uniformly continuous.*

Π^1_1-separation

Def: A formula is Π^1_1 if it has the form $\forall X \psi$, where ψ is an arithmetic formula.

Π^1_1-CA_0 is RCA+ Π^1_1 comprehension.

where Π^1_1 *comprehension* is the scheme of axioms CA(φ) $\exists X \forall n\ (n \in X \Leftrightarrow \varphi(n))$ where φ is any Π^1_1 formula.

Π^1_1-CA_0
|
ATR_0
|
ACA_0
|
WKL_0
|
RCA_0

Theorem (The following are equivalent over RCA_0:)

- Π^1_1-CA_0
- *For every set X, Kleene's O relative to X, O^X, exists.*
- *Every com. group is a sum of a divisible and a reduced group.*

Def: A group G is *divisible* $\forall a \in G \forall n \in \mathbb{N} \exists b (nb = a)$.

Def: A group G is *reduced* if it has no divisible subgroup.

ATR_0

ATR_0 is RCA_0+ Arithmetic Transfinite Recursion.

[Simposon] ATR_0 is the least system where one can develop a reasonable theory of ordinals.

Π^1_1-CA_0
|
ATR_0
|
ACA_0
|
WKL_0
|
RCA_0

Theorem

The following are equivalent over RCA_0:

- *ATR_0*
- *For every set X and every X-computable ordinal α, the αth jump of X, $X^{(\alpha)}$, exists.*
- *Given two ordinals, one is an initial segment of the other one.*

Motivating question

Consider an infinite sequence X of 0s and 1s. We call such sequences *reals*.

What does it mean to say that X is *random*?

Given two reals, which one is more random?

How does the level of randomness relate to the usual measures of computational complexity?

The measure-theoretic paradigm

Let μ be the usual coin-toasing measure on 2^ω.
So, if $\sigma \in 2^{<\omega}$, and $[\sigma] = \{X \in 2^\omega : \sigma \subseteq X\}$, then, $\mu([\sigma]) = 2^{-|\sigma|}$.

Note: If $\mathcal{U} \subseteq 2^\omega$ is open, there is a sequence $\{\sigma_j\}_{j\in\omega}$ s.t. $\mathcal{U} = \bigcup_{j\in\omega}[\sigma_j]$, and if the σ_j are incomparable, then $\mu(U) = \sum_{j\in\omega} 2^{-|\sigma_j|}$.

Def: When $\{\sigma_j\}_{j\in\omega}$ is computable, U is a *computable open set*.

Def: A set of reals $\mathcal{A} \subseteq 2^\omega$ has *effective measure 0* if there is a uniformly computable sequence $\{U_i\}_{i\in\omega}$ of computable open sets such that $\mu(U_i) \leqslant 2^{-n}$ and $\mathcal{A} \subseteq \bigcup_{i\in\omega} U_i$.

A real $X \in 2^\omega$ is *Martin-Löf random*, if it does not belong to any effective measure 0 set.

The unpredictability paradigm

Def: A *Martin Gale* is a function $d\colon 2^{<\omega} \to \mathbb{R}^+$ such that

$$\forall \sigma \in 2^{<\omega} \qquad d(\sigma) = d(\sigma^\frown 0) + d(\sigma^\frown 1).$$

A Martin Gale d *succeeds on* $X \in 2^\omega$ if $\limsup_{n\to\infty} d(X \upharpoonright n) = \infty$.

Def: A *c.e. Martin Gale* is a function $d\colon 2^{<\omega} \to \mathbb{R}^+$ such that the reals $d(\sigma)$ are uniformly computable enumerable, and

$$\forall \sigma \in 2^{<\omega} \qquad d(\sigma) \geqslant d(\sigma^\frown 0) + d(\sigma^\frown 1).$$

Thm[Schnorr 71] $X \in 2^\omega$ is Martin Löf random $\Leftrightarrow$
it doesn't succeed on any c.e. Martin Gale.

The incompressibility paradigm

Roughly, given $\tau \in 2^{<\omega}$ let the *Kolmogorov complexity of τ*, $K(\tau)$, be the length of the shortest program that outputs τ (on a universal prefix-free Turing Machine).

Def: $X \in 2^{\omega}$ is *Kolmogorov-Levin-Chatin random* if there is a constant c such that

$$\forall n \quad K(X \upharpoonright n) \geqslant n - c.$$

Thm:[Shnorr] $X \in 2^{\omega}$ is Kolmogorov-Levin-Chatin random $\Leftrightarrow$ it is Martin Löf random