

# Aspects of Computability Theory

Antonio Montalbán.  
University of Chicago

Kyoto, August 2006

- 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 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 programming language chosen.

**Examples:** The following sets are computable:

- The set of even numbers.
- The set of prime numbers.
- The set of strings 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  $A \leq_T B$ , 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  $A \leq_T B$  and  $B \leq_T A$ .

**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.

- 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

## Basic definitions

Given sets  $A, B \subseteq \mathbb{N}$  we say that  $A$  is **computable in  $B$** , and we write  $A \leq_T B$ , 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  $\mathbf{D} = (\mathcal{P}(\mathbb{N}) / \equiv_T)$ , and  $\mathcal{D} = (\mathbf{D}, \leq_T)$ .

**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,  $\mathbf{D}$  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  $A \leq_T A \oplus B$  and  $B \leq_T A \oplus B$ ,

and if both  $A \leq_T C$  and  $B \leq_T C$  then  $A \oplus B \leq_T C$ .

## Turing Jump

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

$$A' = \{\text{programs, with oracle } A, \text{ that HALT}\}.$$

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  $\mathbf{a} \leq_T \mathbf{b}$  then  $\mathbf{a}' \leq_T \mathbf{b}'$ .

# Operations on $\mathcal{D}$ .

## Definition

A **jump upper semilattice (JUSL)** is structure  $(A, \leq, \vee, j)$  such that

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

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

## The Picture

- Sets below  $\mathbf{0}'$  are classified from *Low* to *High*.
- Even though there are no computable completions  $C$  of PA there are Low ones, that is  $C' \equiv_T \mathbf{0}'$ .
- We have  $\mathbf{0} <_T \mathbf{0}' <_T \mathbf{0}'' <_T \dots <_T \mathbf{0}^{(\omega)}$ .
- A set is *arithmetic* if it is  $\leq_T \mathbf{0}^{(n)}$  for some  $n \in \omega$ .
- $\mathbf{0}^{(\omega)}$  is the set of true arithmetic formulas.
- We can continue along computable ordinals  $\alpha$   
 $\mathbf{0}^{(\omega+1)} <_T \dots <_T \mathbf{0}^{(\omega+\omega)} <_T \dots <_T \mathbf{0}^{(\alpha)} <_T \dots$
- A set is *hyperarithmetic* if it is  $\leq_T \mathbf{0}^{(\alpha)}$  for some computable ordinal  $\alpha$ .
- *Kleene's O*, the set of Halting Non-deterministic programs (where one is allowed 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 together? YES
- What about  $\aleph_1$  many? YES
- Is there a descending sequence of degrees  $\mathbf{a}_0, \geq_T \mathbf{a}_1 \geq_T \dots$ ? 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  $(A, \leq, ')$ . [Hinman, Slaman '91]  
 (For size  $\aleph_1$  it's independent of ZFC) [M. 03]
- Every ctble. jump upper semilattice  $(A, \leq, \vee, ')$  [M. '03]

## History of Decidability Results.

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

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

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

**Question:** Is  $\exists - \text{Th}(\mathbf{D}, \leq_T, \vee, ', 0)$  decidable?

**Question:** Is  $\forall \exists - \text{Th}(\mathbf{D}, \leq_T, ')$  decidable?

## Two famous open question

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

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

**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  $\times_A$  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 Structures

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

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

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 structure.

**Theorem:** Every linear ordering has two isomorphic presentations  $\mathcal{L}_1$  and  $\mathcal{L}_2$  such that if  $X \leq_T \mathcal{L}_1$  and  $X \leq_T \mathcal{L}_2$  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

$$DegSp(\mathcal{G}) = \{\mathbf{a} : \mathbf{x} \leq_T \mathbf{a}\}.$$

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

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

## Example: Represent Structures

**Theorem:** [Spector 55] Every hyperarithmetical 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 hyperarithmetical linear ordering  $\mathcal{L}$ , there is a computable linear ordering  $\mathcal{A}$  that is equimorphic to  $\mathcal{L}$   
that is,  $\mathcal{A} \preceq \mathcal{L}$  and  $\mathcal{L} \preceq \mathcal{A}$ .

- 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

# 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 exist in ZFC?

## Second Order Arithmetic

Simpson and Friedman's program of Reverse Mathematics 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 revisited

- 1 Fix a base theory.  
(We use  $\text{RCA}_0$  that essentially says that the computable sets exists)
- 2 Pick a theorem  $T$ .
- 3 What axioms do we need to add to  $\text{RCA}_0$  to prove  $T$ .
- 4 Suppose we found axioms  $A_0, \dots, A_k$  of  $\mathcal{Z}_2$  such that  
$$\text{RCA}_0 \text{ proves } A_0 \ \& \ \dots \ \& \ A_k \Rightarrow T.$$
How do we know these are necessary?
- 5 It's often the case that  $\text{RCA}_0$  also proves  $T \Rightarrow A_0 \ \& \ \dots \ \& \ A_k$
- 6 Then, we know that  $\text{RCA}_0 + A_0, \dots, A_k$  is the least system (extending  $\text{RCA}_0$ ) 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  $\varphi(n)$ ,  
 $IND(\varphi) \quad (\varphi(0) \ \& \ \forall n(\varphi(n) \Rightarrow \varphi(n+1))) \Rightarrow \forall n\varphi(n)$

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

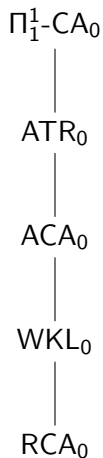
$RCA_0$  consists of:                      Semi-ring Axioms +  $\Sigma_1^0$ -IND+  $\Delta_1^0$ -CA.

$\Delta_1^0$ -CA is equivalent to: for every comp. program  $p$  any oracle  $Y$ ,  
 there is a set  $X$  such that

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

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

# The big five



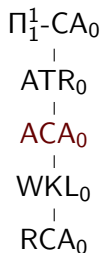
# ACA<sub>0</sub>

## Def:

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

$ACA_0$  is  $RCA_0$  + Arithmetic comprehension.

where *Arithmetic comprehension* is the scheme of axioms  
 $CA(\varphi) \quad \exists X \forall n (n \in X \Leftrightarrow \varphi(n))$   
 where  $\varphi$  is any arithmetic formula.



## Theorem

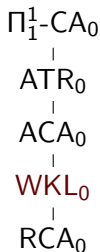
The following are equivalent over  $RCA_0$ :

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

# WKL<sub>0</sub>

*WKL<sub>0</sub>* is  $\text{RCA}_0$  + 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  $\text{RCA}_0$ :*

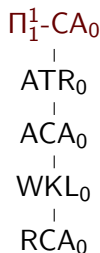
- *WKL<sub>0</sub>*
- *Every continuous function on  $[0, 1]$  is uniformly continuous.*

# $\Pi_1^1$ -separation

**Def:** A formula is  $\Pi_1^1$  if it has the form  $\forall X\psi$ , where  $\psi$  is an arithmetic formula.

$\Pi_1^1$ -CA<sub>0</sub> is RCA+  $\Pi_1^1$  comprehension.

where  $\Pi_1^1$  *comprehension* is the scheme of axioms CA( $\varphi$ )  $\exists X\forall n (n \in X \Leftrightarrow \varphi(n))$  where  $\varphi$  is any  $\Pi_1^1$  formula.



Theorem (The following are equivalent over RCA<sub>0</sub>):

- $\Pi_1^1$ -CA<sub>0</sub>
- 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.

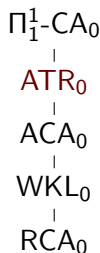
**Def:** A group  $G$  is *divisible*  $\forall a \in G \forall n \in \mathbb{N} \exists b (nb = a)$ .

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

# ATR<sub>0</sub>

$ATR_0$  is  $RCA_0$  + Arithmetic Transfinite Recursion.

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



## Theorem

*The following are equivalent over  $RCA_0$ :*

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

- 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



## 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  $\mu$  be the usual coin-tossing measure on  $2^\omega$ .

So, if  $\sigma \in 2^{<\omega}$ , and  $[\sigma] = \{X \in 2^\omega : \sigma \subseteq X\}$ , then,  $\mu([\sigma]) = 2^{-|\sigma|}$ .

**Note:** If  $U \subseteq 2^\omega$  is open, there is a sequence  $\{\sigma_j\}_{j \in \omega}$  s.t.  $U = \bigcup_{j \in \omega} [\sigma_j]$ , and if the  $\sigma_j$  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  $\mu(U_i) \leq 2^{-i}$  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  $d: 2^{<\omega} \rightarrow \mathbb{R}^+$  such that

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

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

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

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

**Thm**[Schnorr 71]  $X \in 2^\omega$  is Martin L\"of 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  $\tau$* ,  $K(\tau)$ , be the length of the shortest program that outputs  $\tau$  (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

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

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