Computability Theory 2016F

杨睿之 Yang, Ruizhi

Thursday 11-12 [1-16] H2107

Lecture 1

Old name: Recursion Theory.

What is "computability theory" about?

1. Classical recursion theory: the concept of computability, relative computability (Turing reducibility, many-one reducibility, etc.), structure of degrees (based on different notions of relative computability), etc.;
2. Randomness theory (after 2000): the notions of randomness, relative randomness, the interaction between computability and randomness.

For this run, we will mainly focus on Randomness. Still, we will introduce some rudiments of computability theory, which form the preliminary of this course. You may find we are doing with classical computability theory half of our time (I hope not even more).

The main textbook: (Downey and Hirschfeldt, 2010).

Supplements: (Nies, 2009) (for randomness) and (Soare, 2016) (for computability).

Discussion section: After class, occasionally (every 2-3 lectures).

Final example: Problem set (take home).

Basically, we give definitions and we prove theorems in the lectures. BUT Why is this course given by the philosophy department?

1.1 Digitalization

The ultimate purpose of philosophy is no different than other intellectual enterprise of human. That is to understand the world (if it exists, and no matter whether it is physical or not). Nowadays, it seems convincing that every objects can be *coded by a number.* e.g.

1. A picture (.bmp), a pixel,
2. A song (.wav),
3. An article, and even a program.

Question: What is a coding?

An effective function mapping a space of "objects" to $\mathbb{N}$ or to finite 01-strings. E.g. the coding (system) of colors (say RGB).

By coding, we can treat *objects* as natural numbers and *concepts* of a space of objects as sets of natural numbers. This will only make difference if the total space is (countably) infinite. Otherwise, the total space (e.g. our physical universe as many believes) can be coded by a single natural number!

But, still, why does it matters?

By digitalization, it is how we can apply mathematics to the real world (again, not necessarily the physical one).

Two examples:

(Gödel, 1931): Coding of formal language and proofs. Then we can prove something is not provable, e.g. Gödel's incompleteness theorems.

(Turing, 1937): Coding of Turing machines (computer programs). Then we can prove something is not provable, e.g. the noncomputability of halting problem.

These illustrated how, by coding, fundamental concepts can be analyzed mathematically. Note, the case that the real world can be analyzed mathematically is itself an interesting problem for the philosophers.

Don't argue. Let's calculate!

– Leibniz

Now, we understand digitalization is important to philosophy. But, why computability, why randomness?

computability itself is important. At least it is essential for the understanding of randomness, which is the main purpose of this course. This left us to explain why randomness is important?

1.2 Why randomness?

Randomness is a crucial concept for us to understand the world.

1. Evolution theory: A basic assumption is mutations occur randomly. What is consequence in evolution theory if the mutations are random or not (the statistical properties of randomness), and in what sense they are random?
2. Thermodynamics and Fluid mechanics. The statistical properties of randomness.
3. Quantum mechanics. Randomness means unpredictability?
4. Does free will exist? If randomness is the opposite of determinism, then we have a dichotomy argument.
   (a) If determinism is true, then no free will.
   (b) Otherwise, it is random, no free will.
5. Computer sciense.
   (a) Cryptography. Need randomness to ensure security (randomness means unpredictability). Quantum randomness generator vs. pseudorandomness generator.
   (b) Artificial Intelligence. Machine learning need high quality randomness as feed.
6. Casino. The unpredictability and the statistical properties of randomness.

But this course may have nothing to do with all the above stuff! For example, everyone talks about Quantum randomness generator as the real randomness generator. But, is it true? This assertion is a physical one. Briefly, it asserts no *physical* way to predicate blablabla... Such an assertion can be enough for many applications, say to generate strong keys, to AI, or to design a game for the casino. But what we will talk about in this course may have nothing to do with this physical assertion. All the experience the whole human race had (on which surely the modern physics based) cannot prove any sequence in the physical world is random (in the sense we will discussed).

What we don't / do care either?

We don't care about the complexity (e.g. polynomial time / space). We do care about (relative) computability. So this course may not help you to improve the efficiency of your algorithm. In this course, what we do care about is the concept "randomness" itself. I presume it make fully sense why it is a course by the philosophy department.

That is all for philosophy!

1.3 Some set-theoretical notions

Natural numbers: $0 = \emptyset$,$1 = \{0\}$,$2 = \{0, 1\}$,etc.. Note, $n < m$ iff $n \in m$.

The set of all natural numbers: $\omega = \mathbb{N} =$ the smallest set contains 0 and is closed under successor. We write $n < \omega$ iff $n \in \omega$.

Ordered pair (or natural numbers): $(n, m) = \big\{\{n\}, \{n, m\}\big\}$. The key point: $(n_1, m_1) = (n_2, m_2)$ iff $n_1 = n_2$ and $m_1 = m_2$.

Cartesian product: $\omega \times \omega = \big\{(n, m) \bigm| n, m \in \omega\big\}$.

Relations: subsets of Cartesian product. When we say R is a (binary) relation, we mean $R \subset \omega \times \omega$. When we write nRm, we mean $(n, m) \in R$. Let R be a relation , we define $\operatorname{dom} R = \big\{n \bigm| \exists m(n, m) \in R\big\}$[1] and $\operatorname{ran} R = \big\{m \bigm| \exists n(n, m) \in R\big\}$.

Functions: Relations with single-value property, i.e. if f is a function and $(n, m_1), (n, m_2) \in f$, then $m_1 = m_2$. When we write $f : A \to B$, we mean f is a function $\operatorname{dom} f = A$, and $\operatorname{ran} f \subset B$.

[1] By $\exists m \ldots$, we mean there is an m such that ....

References

Downey, R. G. and Hirschfeldt, D. R. 2010. *Algorithmic Randomness and Complexity.* Springer.

Feferman, S., Dawson, John W., J., Kleene, S. C., Moore, G. H., Solovay, R. M., and van Heijenoort, J., editors 1986. *Kurt Gödel: Collected Works: Volume I Publications 1929-1936.* Oxford University Press, New York.

Gödel, K. 1931. Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i. In (Feferman et al., 1986), pages 144–195.

Nies, A. 2009. *Computability and randomness.* Oxford University Press.

Soare, R. I. 2016. *Turing computability: Theory and Applications.* Springer.

Turing, A. M. 1937. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265.