VII

SEVENTH LECTURE

of the Lecture Course

COMPUTABILITY, DECIDABILITY, INCOMPLETENESS

30 May 2023

Lecture VI

Definition A set $X \subseteq \mathbb{N}^k$ is called Σ_1 if there is a computable set $Y \subseteq \mathbb{N}^{k+1}$ s.t.

for all $\vec{w} \in \mathbb{N}^k$

$$\vec{w} \in X \Longleftrightarrow \exists v\ (\vec{w}, v) \in Y.$$

We say X is Π_1 if its complement is Σ_1.

We call X Δ_1 if it is both Σ_1 and Π_1.

Theorem TFAE

(i) A is c.e.

(ii) A is Σ_1

Corollary A is computable $\Longleftrightarrow$ A is Δ_1.

"$\Sigma_1 = \Delta_1 \Longleftrightarrow$ c.e. = computable"

Still Lecture VI

COMPUTABLY ENUMERABLE SETS

$$\mathbb{K} := \{ w ; f_{w,1}(w)\downarrow \} \subseteq \mathbb{W}$$

$$\mathbb{K}_0 := \{ (w,v) ; f_{w,1}(v)\downarrow \} \subseteq \mathbb{W}^2.$$

Both of these are usually called the Halting Problem or Turing's Halting

Prop. Both $\mathbb{K}$ and $\mathbb{K}_0$ are c.e.

Proof. Suppose U is a universal machine.

Neither $\mathbb{K}$ nor $\mathbb{K}_0$ is computable.

So, $\mathbb{K}$ is a Σ_1 set that is not Δ_1 and hence not Π_1.

$$\Sigma_1 \neq \Delta_1$$

Some people call this "Gödel's Incompleteness Theorem". We'll see in Part II why.

Still Lecture VI

We proved

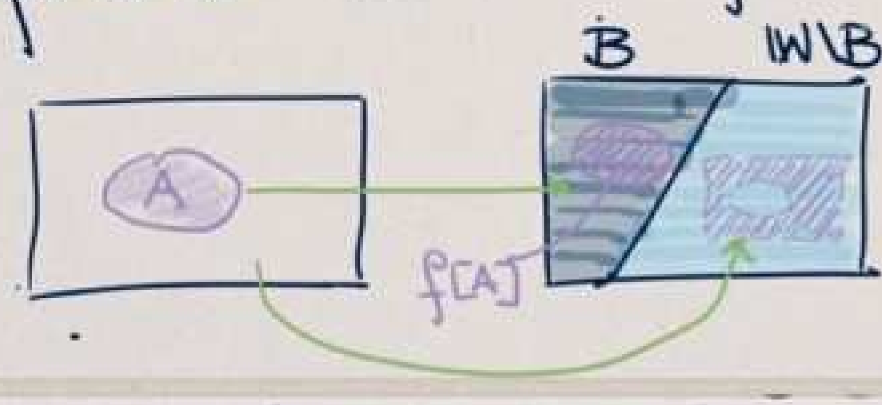
$A \leq_m B$ & B is computable $\Longrightarrow$ A is computable.

$A \leq_m B$ & B is c.e. $\Longrightarrow$ A is c.e.

Thus Σ_1 and Δ_1 are closed under reductions.

Def. A total function $f : \mathbb{W} \longrightarrow \mathbb{W}$ is called REDUCTION from A to B if

for all w $\quad w \in A \Longleftrightarrow f(w) \in B$.



Def. Let $\mathcal{C}$ be any collection of subsets of $\mathbb{W}$. [E.g., $\Sigma_1, \Pi_1, \Delta_1$, c.e., computable ...]

We say A is $\mathcal{C}$-hard if for all $X \in \mathcal{C}$ $\quad X \leq_m A$.

We say A is $\mathcal{C}$-complete if it is $\mathcal{C}$-hard & $A \in \mathcal{C}$.

Goal (Lecture VII): Prove that $\mathbb{K}$ is Σ_1-complete.

Note that $\mathbb{W} \setminus \mathbb{K}$ cannot be c.e.: if $\mathbb{W} \setminus \mathbb{K} \in \Sigma_1$, then $\mathbb{K} \in \Pi_1$, so $\mathbb{K} \in \Delta_1$ which we proved to be false.

Application If $\mathbb{K} \leq_m A$, then A is not computable.

If $\mathbb{W} \setminus \mathbb{K} \leq_m A$, then A is not c.e.

Theorem $\mathbb{K}$ is Σ_1- complete.

Proof. Let A be Σ_1, i.e., c.e.

Therefore let f be a computable partial fn s.t.

$$A = \mathrm{dom}(f). \quad (*)$$

$$g(w, v) := f(w)$$

Clearly, g is computable, so by s-m-n, find total h s.t.

CURRYING

$$\underline{f_{h(w)}}(v) = g(w, v) = \underline{f(w)}$$

Claim h is a reduction from A to $\mathbb{K}$.

$$\Longleftrightarrow \forall w \ \boxed{w \in A \longleftrightarrow h(w) \in \mathbb{K}}$$

Case 1 $w \in A \xrightarrow{(*)} f(w)\downarrow \longrightarrow f_{h(w)}$ halts for all v, so $f_{h(w)}$ is a total function $\longrightarrow f_{h(w)}(h(w))\downarrow \longrightarrow h(w) \in \mathbb{K}$.

Case 2 $w \notin A \xrightarrow{(*)} f(w)\uparrow \longrightarrow f_{h(w)}$ does not halt for any v $\longrightarrow f_{h(w)}(h(w))\uparrow \longrightarrow h(w) \notin \mathbb{K}$.

q.e.d.

If $A \leq_m B$ and $B \leq_m A$, we'll say that A and B are many-one-equivalent and write $\equiv_m$.

Easy to see that $\mathbb{K} \leq_m \mathbb{K}_0$, and so $\mathbb{K} \equiv_m \mathbb{K}_0$.

If $A, B \subseteq \mathbb{W}$, we can form a least upper bound to A & B as follows:

Assume $|\Sigma| \geq 2$, and pick a fixed $a \in \Sigma$.

$$A \oplus B := \{aw ; w \in A\} \cup \{bw ; b \neq a \text{ \& } w \in B\}.$$

Turing join of A & B

Prop. 1 $A, B \leq_m A \oplus B$.

Proof. If $b \neq a$, then both the functions

$$h_a : w \longmapsto aw$$
$$h_b : w \longmapsto bw$$

are computable & total

and h_a reduces A to $A \oplus B$ and h_b reduces B to $A \oplus B$.

[$w \in A \longrightarrow aw \in A \oplus B$; $w \notin A \longrightarrow aw \notin A \oplus B$;
$w \in B \longrightarrow bw \in A \oplus B$; $w \notin B \longrightarrow bw \notin A \oplus B$.]

q.e.d.

Corollary $\mathbb{K} \oplus \mathbb{N}\setminus\mathbb{K} =: X$

is a set that is neither Σ_1 nor Π_1.

Proof. By Prop 1, we have that

$$\mathbb{K} \leq_m X \quad \text{and}$$
$$\mathbb{N}\setminus\mathbb{K} \leq_m X.$$

Thus if it is Σ_1, then so is $\mathbb{N}\setminus\mathbb{K}$. $\lightning$.

& if it is Π_1, then so is $\mathbb{K}$ $\lightning$.

q.e.d.

Remark. This gives rise to a natural hierarchy of ever more complex sets. This mathematical object is called

DEGREES OF UNSOLVABILITY

Modern computability theory is mostly about understanding the structure

$$\left(\mathbb{N}/_{\equiv_m}, \leq_m\right):$$

how long are chains / antichains, is it dense etc.

Prop. 2 $A \oplus B$ is the least upper bound w.r.t. $\leq_m$;
(i.e., if $A, B \leq_m C$, then $A \oplus B \leq_m C$).

Proof. Suppose $A \leq_m C$ via f &
$B \leq_m C$ via g, i.e.,

computable total

$$\circledast \quad \boxed{w \in A \iff f(w) \in C}$$
$$\circledast \quad \boxed{w \in B \iff g(w) \in C}.$$

Define h by

$$h(xw) = \begin{cases} f(w) & \text{if } x = a \\ g(w) & \text{if } x \neq a \end{cases}$$

where $x \in \Sigma$. Clearly h is computable and total. We claim h reduces $A \oplus B$ to C:

Case 1
$w \in A \oplus B \longrightarrow$ (Case 1a) $w = av$ some $v \in A$
$\longrightarrow h(w) = f(v) \in C$ $\circledast$
$\longrightarrow$ (Case 1b) $w = bv$ some $b \neq a$, $v \in B$
$\longrightarrow h(w) = g(v) \in C$ $\circledast$

Case 2
$w \notin A \oplus B \longrightarrow w = av$ some $v \notin A$
$\longrightarrow h(w) = f(v) \notin C$ $\circledast$
$\longrightarrow w = bv$ some $b \neq a$ and $v \notin B$ $\longrightarrow h(w) = g(v) \notin C$ $\circledast$

q.e.d

INDEX SETS & RICE'S THEOREM

Reminder We said that $w, v \in \mathbb{W}$ are *weakly equivalent* if $W_w = W_v$.

$$W_w = \mathrm{dom}(f_{w,1}) = \{v ; f_{w,1}(v)\downarrow\} \qquad W_v = \mathrm{dom}(f_{v,1}) = \{v ; f_{v,1}(v)\downarrow\}$$

Def. A set $I \subseteq \mathbb{W}$ is called an *index set* if it is closed under weak equivalence, i.e.,

if $w \in I$ and $W_w = W_v$, then $v \in I$.

Remark We can think of index sets as "properties of c.e. sets":

For instance: $\mathbb{E}\mathrm{mp} := \{w ; W_w = \emptyset\}$

is the property of being empty.

$\mathbb{F}\mathrm{in} := \{w ; W_w \text{ is finite}\}$

$\mathbb{I}\mathrm{nf} := \{w ; W_w \text{ is infinite}\}$

Trivial index sets: $\emptyset, \mathbb{W}$.
These are called *trivial*.

Remark $\emptyset \neq \mathbb{E}\mathrm{mp}$.

In fact, $\mathbb{E}\mathrm{mp}$ contains lots of words: every single code of a RM that never halts.

Remember the padding lemma which told us that for every $w \in \mathbb{W}$ there are infinitely many weakly equivalent v.

Corollary Every nontrivial index set is infinite.

Theorem (RICE'S THEOREM)

Nontrivial index sets are not computable. More specifically, if I is nontrivial, then either $\mathbb{K} \leq_m I$ or

$$\mathbb{W} \setminus \mathbb{K} \leq_m I.$$

[Possibly both!]

(Cf. page 13)

Proof. Start by fixing some $e \in \mathbb{W}$ s.t.

$$W_e = \emptyset.$$

Clearly, either $e \in I$ or $e \notin I$.

We're going to show:

if $e \in I$, then $\mathbb{W} \setminus \mathbb{K} \leq_m I$;

if $e \notin I$, then $\mathbb{K} \leq_m I$.

Case 1 $e \in I$. By nontriviality of I, find $w \notin I$. [since $I \neq \mathbb{W}$!]

Define

$$g(u,v) := \begin{cases} f_{w,1}(v) & \text{if } u \in \mathbb{K} \\ \uparrow & \text{if } u \notin \mathbb{K} \end{cases}$$

Remember that the case distinction lemma requires the case distinction to be computable.
This is NOT the case here.

Claim: g is computable since I first calculate $f_{u,1}(u)$.
If this diverges, I have (accidentally) obtained the right behaviour, viz. $\uparrow$.
If it converges, we know that $u \in \mathbb{K}$; this happens after finitely many steps; I can then calculate $f_{w,1}(v)$.

$$g(u,v) := \begin{cases} f_{w,1}(v) & \text{if } u \in \mathbb{K} \\ \uparrow & \text{if } u \notin \mathbb{K}. \end{cases}$$

Since g is computable, find total computable h by s-m-n s.t.

$$f_{h(u)}(v) = g(u,v).$$

<u>Claim</u> h reduces $\mathbb{N} \setminus \mathbb{K}$ to I.

<u>Case 1a</u> $u \in \mathbb{K}$ $\longrightarrow f_{h(u),1}(v) = g(u,v) = f_{w,1}(v)$

$\longrightarrow f_{h(u),1} = f_{w,1}$

$\longrightarrow$ $h(u)$ & w are weakly eq.

$\longrightarrow$ $h(u) \notin I$ [since I index set & $w \notin I$].

<u>Case 1b</u> $u \notin \mathbb{K}$ $\longrightarrow f_{h(u),1}$ diverges for all v

$\longrightarrow \mathrm{dom}(f_{h(u),1}) = \emptyset$

$\quad \| $

$\quad W_{h(u)}$

$\longrightarrow$ $h(u)$ & e are weakly equivalent

$\longrightarrow$ $h(u) \in I$ [I index set & $e \in I$]

<u>Case 2</u> <u>$e \notin I$</u> By nontriviality, we find $w \in I$ [since $I \neq \emptyset$]

$$g(u,v) := \begin{cases} f_{w,1}(v) & \text{if } u \in \mathbb{K} \\ \uparrow & \text{o/w} \end{cases}$$

As before g is computable and therefore by s-m-n, we have h total and computable s.t.

$$f_{h(u)}(v) = g(u,v).$$

<u>Claim</u> h reduces $\mathbb{K}$ to I.

<u>Case 2a</u> $u \in \mathbb{K} \longrightarrow f_{h(u),1} = f_{w,1}$

$\longrightarrow h(u)$ & w are weakly eq.

$\longrightarrow h(u) \in I$ [I index set & $w \in I$]

<u>Case 2b</u> $u \notin \mathbb{K} \longrightarrow f_{h(u),1}$ is nowhere defined

$\longrightarrow W_{h(u)} = \mathrm{dom}(f_{h(u),1}) = \emptyset$

$\longrightarrow h(u)$ & e are weakly eq.

$\longrightarrow h(u) \notin I$ [I index set & $e \notin I$].

q.e.d.

<u>Corollary</u> $\mathbb{E}\mathrm{mp}$, $\mathbb{F}\mathrm{in}$, $\mathbb{I}\mathrm{nf}$ are all non-computable.

Note that the proof of Rice's Theorem tells us precisely in which case we are for which nontrivial index set:

① $e \in \mathbb{E}\mathrm{mp}$ for $W_e = \emptyset$,
so $\mathbb{N} \setminus \mathbb{K} \leq_m \mathbb{E}\mathrm{mp}$, so $\mathbb{E}\mathrm{mp}$ is not even c.e.

② $e \in \mathbb{F}\mathrm{in}$ for $W_e = \emptyset$,
so $\mathbb{N} \setminus \mathbb{K} \leq_m \mathbb{F}\mathrm{in}$.

③ $e \notin \mathbb{I}\mathrm{nf}$ for $W_e = \emptyset$,
so $\mathbb{K} \leq_m \mathbb{I}\mathrm{nf}$.

<u>Remark</u> $\mathbb{F}\mathrm{in}$ & $\mathbb{I}\mathrm{nf}$ are examples of the "possibly both" part of Rice's Theorem. It is possible to prove that

(Cf. page 9)

$$\mathbb{K} \leq_m \mathbb{F}\mathrm{in}.$$

and thus $\mathbb{N} \setminus \mathbb{K} \leq_m \mathbb{I}\mathrm{nf}$.

Remark next page will explain this "thus".

Remark If $A \leq_m B$, then

$$\mathbb{W} \setminus A \leq_m \mathbb{W} \setminus B$$

by the same reduction function.

$$\Big[w \in A \longleftrightarrow h(w) \in B$$

$$\Longleftrightarrow$$

$$w \notin A \longleftrightarrow h(w) \notin B . \Big]$$

Clearly $\mathbb{W} \setminus \mathbb{F}\mathrm{in} = \mathbb{I}\mathrm{nf}$.

So if $\mathbb{K} \leq_m \mathbb{F}\mathrm{in}$, then

$$\mathbb{W} \setminus \mathbb{K} \leq_m \mathbb{W} \setminus \mathbb{F}\mathrm{in} = \mathbb{I}\mathrm{nf}.$$

DECIDABILITY

Informally, we think of $A \subseteq \mathbb{W}$ as a "PROBLEM" in the form:

GIVEN $w \in \mathbb{W}$,
DECIDE WHETHER $w \in A$

The answer is supposed to be algorithmic, so there is an ALGORITHM / PROCEDURE that takes w as input and produces an answer: YES / NO.

One possible mathematical way to define "procedure" is to use our notion of computability:
Take RM M and feed w into M and interpret $f_M(w) = a$ as YES
and $f_M(w) = \varepsilon$ as NO.

This definition would make the notion of DECIDABILITY coincide with our notion of COMPUTABILITY:

a PROCEDURE is just a RM computing the characteristic function of the set A.

Next time: Informal (historical) argument for this identification

&

derive consequences of $\mathbb{C}$ for $\mathbb{D}$.