COMPUTABILITY, DECIDABILITY, INCOMPLETENESS

CDI XII

4 July 2023

LECTIO ULTIMA

Gödel's Incompleteness Theorem

Lecture XI, page 11

Gödel's Incompleteness Theorem in the land of sets

There is no decidable negation-complete S s.t. $\mathbb{HF} \models S$.

This means:

If S is any decidable axiom system then

$$P := \{\varphi \,;\, S \vdash \varphi\} \neq \{\varphi \,;\, \mathbb{HF} \models \varphi\} =: T$$

S-PROVABLE TRUE

We show this by:

1. P is Σ_1.
2. T is Π_1-hard

The theorem then follows from 1, 2, & the fact that $\Sigma_1 \neq \Delta_1$.

① $P = \{\varphi ; S \vdash \varphi\}$ is Σ_1.

Lecture XI page 12

Step 1 Prove that if S is decidable, then $P := \{\varphi ; S \vdash \varphi\}$ is Σ_1

In Lecture $\overline{\text{XI}}$ we reminded ourselves of the basic definitions of the proof predicate $\vdash$, or more precisely $\vdash_{\mathcal{R}}$ for a calculus $\mathcal{R}$:

Lecture XI page 13

A set $R \subseteq \mathrm{Fml}^{n+1}$ is called an <u>n-ary rule</u> and we interpret $(\varphi_0, \dots, \varphi_n) \in R$ as if $\varphi_0, \dots, \varphi_{n-1}$ have been derived, then φ_n can be derived.

Since $\mathrm{Fml} \subseteq \mathbb{W}$, rules are sets of sequences of words, which we know how to encode as words.

A rule R is <u>computable</u> if it is computable as a set of words.

A <u>calculus</u> is a finite set $\mathcal{R}$ of rules and it's called <u>computable</u> if all it's rules are computable.

<u>OBSERVE</u> (by inspection of the definitions) The standard proof predicate $\vdash$ has a computable calculus.

Lecture XI, page 14

Goal for next time:

If S is computable and $\mathcal{R}$ is computable, then

$$\{\varphi\,;\, S \vdash_{\mathcal{R}} \varphi\}$$

is Σ_1.

If we've proved that, Step 1 is complete.

An $\boxed{\mathcal{R}\text{-}S\text{-proof}}$ is a finite sequence $\vec{w}$ s.t. for every $i < |\vec{w}|$

- EITHER $w_i \in S$
- OR there is $R \in \mathcal{R}$, R is n-ary and $i_0, \ldots, i_{n-1} < i$ s.t. $(w_{i_0}, w_{i_1}, \ldots, w_{i_{n-1}}, w_i) \in R$.

Remember that we encoded sequences of words as words $\mathrm{code}(\vec{w})$;

similarly, encode a seq. of words $\vec{w}$ plus a nat. number i as a word $\mathrm{code}(\vec{w}, i)$.

(a) The set

$$\{(w, \mathrm{code}(\vec{w})) \,;\ w \text{ occurs in } \vec{w}\}$$

is computable.

(b) Fix a rule $R \in \mathcal{R}$

$$F(R) := \{\mathrm{code}(\vec{w}, i) \,;\ \exists i_0, \dots, i_{n-1} < i \ (w_{i_0}, \dots, w_{i_{n-1}}, w_i) \in R\}$$

FOLLOWS FROM

This set is computable since R is.

(c) Therefore

$$F(\mathcal{R}) := \bigcup_{R \in \mathcal{R}} F(R)$$

is computable since the computable sets are closed under finite unions.

(d) Also $A(S) := \{\mathrm{code}(\vec{w}, i) \,;\ w_i \in S\}$ is computable since S is.

(e) Then $\mathrm{Proof}(\mathcal{R}, S) := \{\mathrm{code}(\vec{w}) \,;\ \forall i < |\vec{w}| \ \mathrm{code}(\vec{w}, i) \in F(\mathcal{R}) \cup A(S)\}$

is computable.

Proof of ①

$$\{\varphi ; S \vdash \varphi\}$$

$$= \{\varphi ; \underbrace{\exists v \; \underbrace{\underbrace{O(\varphi, v)}_{(a)} \wedge \underbrace{v \in \mathrm{Proof}(\mathcal{R}, S)}_{(e)}}_{\Delta_1}}_{\Sigma_1}\}$$

$O(\varphi, v) :\Leftrightarrow \varphi$ occurs in the seq. coded by v

This finishes the proof of ①.

REMARK

1. This is fully general: choice of both $\mathcal{R}$ and S arbitrary as long as decidable
2. We don't even need that Proof (or S and $\mathcal{R}$ for that matter) are Δ_1; Σ_1 is sufficient to prove this.

② $T := \{\varphi \,;\, \mathbb{HF} \models \varphi\}$ is Π_1-hard

Lecture IX page 11

<u>Note</u>. The work done in Lecture II is a formalisation of "the machine coded by w halts at input w".
With some (not much) extra work, we could have formula σ_w s.t.

$$f_{w,1}(w)\downarrow \iff \sigma_w \text{ is true}$$

Note that this immediately gives us

$$\mathbb{K} \leq_m \{\varphi \,;\, \varphi \text{ is true}\}$$

by the reduction function

$$w \longmapsto \sigma_w.$$

Since Gödel's incompleteness theorem will show that
$\{\varphi \,;\, \varphi \text{ is true}\} \neq \{\varphi \,;\, \vdash \varphi\}$,
this is not an answer to the Entscheidungsproblem.
Need to work a little harder!

Our proof of ② will use precisely this idea, not reducing $\mathbb{K}$ but rather an arbitrary Π_1-set.

Arbitrary Π_1-set:

Note that $\neg \exists v \ (v,w) \in C$

$$\Longleftrightarrow \forall v \ \neg (v,w) \in C$$

$$\Longleftrightarrow \forall v \ \underbrace{(v,w) \notin C}$$

C computable $\Leftrightarrow W \setminus C$ computable

So an arbitrary Π_1 set is of the form

$$D = \{ w \,;\, \forall v \ (v,w) \in C \}$$

where C is computable.

$\Longleftrightarrow$ $w \in D \longleftrightarrow f_{d,2}(v,w)\downarrow = a$

$w \notin D \longleftrightarrow f_{d,2}(v,w)\downarrow = \varepsilon$

for some machine code d.

Write $\varphi(d,v,w)$ for the formula describing

"the machine with code d halts upon input (v,w) and produces output a".

$$\boxed{\begin{array}{l} w \in D \Longleftrightarrow HF \models \forall x \ \varphi(d,x,w) \\ w \notin D \Longleftrightarrow HF \models \neg \forall x \ \varphi(d,x,w) \end{array}} \quad (*)$$

Note that for a variable w (and fixed d)

$$h : w \longmapsto \forall x\, \varphi(d, x, w) \quad ,$$

is computable.

<u>Claim</u> h is a reduction function witnessing $D \leq_m T$.

[Follows directly from (*).]

This finishes the proof of ② and thus the proof of Gödel's (First) Incompleteness Thm. Q.E.D.

<u>REMARKS</u> 1. There is nothing special about Π_1. This proof shows that T is <u>hard</u> for any class of bounded complexity.

2. Hiding behind this is the famous TARSKI UNDEFINABILITY OF TRUTH THM.

<u>Note</u>: This proof is entirely non-constructive. It does <u>not</u> produce a true but non-provable formula.

<u>IN CONTRAST</u> Gödel's original proof did.

RECURSION THEOREM / FIXED POINT THEOREM

(50) Let φ be a total computable function. A word w is called a *fixed point of* φ if $f_{\varphi(w),1} = f_{w,1}$. Show using the following steps that such a fixed point exists.

(a) Argue that the function

$$g(u, v) := \begin{cases} f_{f_{u,1}(u)}(v) & \text{if } u \in \mathbf{K} \text{ and} \\ \uparrow & \text{otherwise} \end{cases}$$

is computable.

(b) By the s-m-n theorem, there is a total computable function h such that $f_{h(u),1}(v) = g(u, v)$. Let p be such that $f_{p,1} = \varphi \circ h$ and $w := h(p)$. Show that w is a fixed point of φ.

The relevant fixed point lemma can be found on moodle.

Find formula $\pi(\varphi)$ that expresses "φ is provable".

i.e., $\boxed{\exists v\ \overline{O}(\varphi, v) \wedge_{ve} \mathrm{Proof}(\mathcal{R}, S)}$

Consider map $\varphi \longmapsto \neg\pi(\varphi)$ and use the fixed pt theorem to obtain ψ s.t.

$$\boxed{\psi \longleftrightarrow \neg\pi(\psi)}$$

"I am not provable"

Such a ψ is usually called the GÖDEL SENTENCE

<u>Now:</u> The Gödel sentence ψ is either true or false in HF:

$$HF \models \psi$$

or

$$HF \models \neg\psi$$

if $HF \models \neg\psi$, then $HF \models \neg\neg\pi(\psi)$

$\Longrightarrow HF \models \pi(\psi)$ S

$\Longrightarrow$ there is a proof of ψ.

[since $HF \models S \Longrightarrow HF \vdash \psi$.]

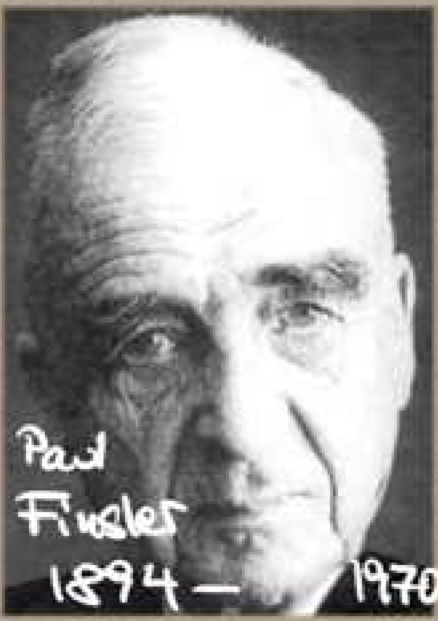
$\lightning$.

So $HF \models \psi$.

$\Longleftrightarrow HF \models \neg\pi(\psi)$

So, there is no proof of ψ.

- Pre-Gödel there were many attempts to show that the classical paradoxes of Greek antiquity apply in maths.
- Even using Liar's Paradox in light of "provability" is not entirely original.



Finsler did something like this and claimed priority over Gödel.

Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I[1]).

Von **Kurt Gödel** in Wien.

1.

Die Entwicklung der Mathematik in der Richtung zu größerer Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete von ihr formalisiert wurden, in der Art, daß das Beweisen nach einigen wenigen mechanischen Regeln vollzogen werden kann. Die umfassendsten derzeit aufgestellten formalen Systeme sind das System der Principia Mathematica (PM)[2]) einerseits, das Zermelo-Fraenkelsche (von J. v. Neumann weiter ausgebildete) Axiomensystem der Mengenlehre[3]) andererseits. Diese beiden Systeme sind so weit, daß alle heute in der Mathematik angewendeten Beweismethoden in ihnen formalisiert, d. h. auf einige wenige Axiome und Schlußregeln zurückgeführt sind. Es liegt daher die Vermutung nahe, daß diese Axiome und Schlußregeln dazu ausreichen, alle mathematischen Fragen, die sich in den betreffenden Systemen überhaupt formal ausdrücken lassen, auch zu entscheiden. Im folgenden wird gezeigt, daß dies nicht der Fall ist, sondern daß es in den beiden angeführten Systemen sogar relativ einfache Probleme aus der Theorie der gewöhnlichen ganzen Zahlen gibt[4]), die sich aus den Axiomen nicht

---

[1]) Vgl. die im Anzeiger der Akad. d. Wiss. in Wien (math.-naturw. Kl.) 1930, Nr. 19 erschienene Zusammenfassung der Resultate dieser Arbeit.

[2]) A. Whitehead und B. Russell, Principia Mathematica, 2. Aufl., Cambridge 1925. Zu den Axiomen des Systems PM rechnen wir insbesondere auch: Das Unendlichkeitsaxiom (in der Form: es gibt genau abzählbar viele Individuen), das Reduzibilitäts- und das Auswahlaxiom (für alle Typen).

[3]) Vgl. A. Fraenkel, Zehn Vorlesungen über die Grundlegung der Mengenlehre, Wissensch. u. Hyp. Bd. XXXI. J. v. Neumann, Die Axiomatisierung der Mengenlehre. Math. Zeitschr. 27, 1928. Journ. f. reine u. angew. Math. 154 (1925), 160 (1929). Wir bemerken, daß man zu den in der angeführten Literatur gegebenen mengentheoretischen Axiomen noch die Axiome und Schlußregeln des Logikkalküls hinzufügen muß, um die Formalisierung zu vollenden. — Die nachfolgenden Überlegungen gelten auch für die in den letzten Jahren von D. Hilbert und seinen Mitarbeitern aufgestellten formalen Systeme (soweit diese bisher vorliegen). Vgl. D. Hilbert, Math. Ann. 88, Abh. aus d. math. Sem. der Univ. Hamburg I (1922), VI (1928). P. Bernays, Math. Ann. 90. J. v. Neumann, Math. Zeitschr. 26 (1927). W. Ackermann, Math. Ann. 93.

[4]) D. h. genauer, es gibt unentscheidbare Sätze, in denen außer den logischen Konstanten: $\overline{}$ (nicht), $\vee$ (oder), (x) (für alle), $=$ (identisch mit) keine anderen Begriffe vorkommen als $+$ (Addition), . (Multiplikation), beide bezogen auf natürliche Zahlen, wobei auch die Präfixe (x) sich nur auf natürliche Zahlen beziehen dürfen.

Second Incompleteness Theorem: Under reasonable assumptions on S,

$S \nvdash \mathrm{Cons}(S)$

where $\mathrm{Cons}(S)$

is the formula

$$\boxed{\begin{array}{l}\forall v \;\; v \in \mathrm{Proof}(R_S) \\ \quad \longrightarrow \neg O(0=1, v)\end{array}}$$

4.

Aus den Ergebnissen von Abschnitt 2 folgt ein merkwürdiges Resultat, bezüglich eines Widerspruchslosigkeitsbeweises des Systems P (und seiner Erweiterungen), das durch folgenden Satz ausgesprochen wird:

Satz XI: Sei $\varkappa$ eine beliebige rekursive widerspruchsfreie[63]) Klasse von *Formeln*, dann gilt: Die *Satzformel*, welche besagt, daß $\varkappa$ widerspruchsfrei ist, ist nicht $\varkappa$-*beweisbar*; insbesondere ist die Widerspruchsfreiheit von P in P unbeweisbar[64]), vorausgesetzt, daß P widerspruchsfrei ist (im entgegengesetzten Fall ist natürlich jede Aussage beweisbar).

Der Beweis ist (in Umrissen skizziert) der folgende: Sei $\varkappa$ eine beliebige für die folgenden Betrachtungen ein für allemal gewählte rekursive Klasse von *Formeln* (im einfachsten Falle die leere Klasse). Zum Beweise der Tatsache, daß 17 Gen r nicht $\varkappa$-*beweisbar* ist[65]), wurde, wie aus 1. Seite 189 hervorgeht, nur die Widerspruchsfreiheit von $\varkappa$ benutzt, d. h. es gilt:

$$\mathrm{Wid}\,(\varkappa) \longrightarrow \overline{\mathrm{Bew}_{\varkappa}}\;(17 \text{ Gen } r) \tag{23}$$

d. h. nach (6·1):

$$\mathrm{Wid}\,(\varkappa) \longrightarrow (x)\;\overline{x\,B_{\varkappa}\,(17 \text{ Gen } r)}$$

Nach (13) ist $17 \text{ Gen } r = Sb\left(p \begin{smallmatrix}19\\ Z(p)\end{smallmatrix}\right)$ und daher:

$$\mathrm{Wid}\,(\varkappa) \longrightarrow (x)\;\overline{x\,B_{\varkappa}\,Sb\left(p \begin{smallmatrix}19\\ Z(p)\end{smallmatrix}\right)}$$

d. h. nach (8·1):

$$\mathrm{Wid}\,(\varkappa) \longrightarrow (x)\;Q\,(x, p) \tag{24}$$

Wir stellen nun folgendes fest: Sämtliche in Abschnitt 2[66]) und Abschnitt 4 bisher definierte Begriffe (bzw. bewiesene Behauptungen) sind auch in P ausdrückbar (bzw. beweisbar). Denn es wurden überall nur die gewöhnlichen Definitions- und Beweismethoden der klassischen Mathematik verwendet, wie sie im System P formalisiert sind. Insbesondere ist $\varkappa$ (wie jede rekursive Klasse) in P definierbar. Sei w die *Satzformel*, durch welche in P Wid $(\varkappa)$ ausgedrückt wird. Die Relation $Q\,(x, y)$ wird gemäß (8·1), (9), (10) durch das *Relationszeichen* q ausgedrückt, folglich $Q\,(x, p)$ durch r $\left[\text{da nach (12) } r^{4}_{1} = Sb\left(q \begin{smallmatrix}19\\ Z(p)\end{smallmatrix}\right)\right]$ und der Satz $(x)\,Q\,(x, p)$ durch 17 Gen r.

Wegen (24) ist also w Imp (17 Gen r) in P beweisbar[67]) (um so mehr $\varkappa$-*beweisbar*). Wäre nun w $\varkappa$-*beweisbar*, so wäre auch 17 Gen r $\varkappa$-*beweisbar* und daraus würde nach (23) folgen, daß $\varkappa$ nicht widerspruchsfrei ist.

A few remarks about this proof sketch:

The (ancient Greek) argument on page 10 can be transformed into:

$$\boxed{\mathrm{Cons}(S) \longrightarrow (\neg\psi \longrightarrow \psi)}$$

This needs some (reasonable) assumptions on S.

Note: by propositional logic $(\neg\psi \to \psi) \iff \psi$.

So $\boxed{\mathrm{Cons}(S) \longrightarrow \psi}$

So if $S \vdash \mathrm{Cons}(S)$, then $S \vdash \psi$ which we proved to be false.

Thus $S \nvdash \mathrm{Cons}(S)$.

This leads to the following definition:

$$S \leq_{\mathrm{Cons}} T$$

$$:\iff T \vdash \mathrm{Cons}(S)$$

CONSISTENCY STRENGTH HIERARCHY

Gödel's Second Incompleteness Thm implies that for reasonable S [e.g., PA, ZF, ZFC, ...]

$$S \nvdash \mathrm{Cons}(S);$$

thus
$$S <_{\mathrm{Cons}} S + \mathrm{Cons}(S)$$
$$<_{\mathrm{Cons}} S + \mathrm{Cons}(S) + \mathrm{Cons}(S + \mathrm{Cons}(S))$$
$$<_{\mathrm{Cons}} \cdots$$

<u>Strange example</u>.
Let's take $S := \mathrm{ZFC}$. By Gödel 2,
$$\mathrm{ZFC} \nvdash \mathrm{Cons}(\mathrm{ZFC}).$$
That means $\mathrm{ZFC} + \neg\mathrm{Cons}(\mathrm{ZFC})$ is consistent.

Consider $\mathrm{Cons}(\mathrm{ZFC} + \neg\mathrm{Cons}(\mathrm{ZFC}))$
which implies $\mathrm{Cons}(\mathrm{ZFC})$ since $\mathrm{ZFC} \subseteq \mathrm{ZFC} + \neg\mathrm{Cons}(\mathrm{ZFC})$

So $\mathrm{ZFC} + \neg\mathrm{Cons}(\mathrm{ZFC}) + \mathrm{Cons}(\mathrm{ZFC} + \neg\mathrm{Cons}(\mathrm{ZFC}))$
cannot be consistent.

⋮