COMP0009. Incompleteness

November 23, 2023

Gödel's Incompleteness Theorem

Countable Sets

Let $f : A \to B$ be any function.

- f is <u>surjective</u> if $\forall b(b \in B \to \exists a(a \in A \land f(a) = b))$.
- f is <u>injective</u> if $\forall a \forall a'((f(a) = f(a')) \to (a = a'))$
- A <u>bijection</u> $f : A \to B$ is injective and surjective (one-to-one and onto).
- If there is a bijection from A to B then $|A| = |B|$ (same cardinality)
- Set S is <u>countable</u> if either it is finite, or there is a bijection $f : \mathbb{N} \to S$.

Problems

Finite ordinals: $0 = \emptyset,\ 1 = \{0\}, \ldots,\ n = \{0, 1, \ldots, n-1\}$.
A set S is <u>inductive</u> if $0 \in S$ and $n \in S \Rightarrow (n+1) \in S$.
$\mathbb{N} = \{0, 1, \ldots\}$ is the intersection of all inductive sets.

1. Prove that if S and T are both countably infinite, then there is a bijection from S to T
2. Let $m, n \in \mathbb{N}$, finite natural numbers. When is there a bijection from m to n?
3. Prove that S is countable if and only if there is an injection from S to $\mathbb{N}$.
4. Prove that $\mathbb{N} \times \mathbb{N}$ is countably infinite.
5. Prove that the set of all rational numbers is countably infinite.
6. Let Σ be a finite alphabet. Prove that Σ^* is countably infinite.

$\mathbb{R}$ is not countable

Assume $f : \mathbb{N} \to \mathbb{R} \cap [0, 1]$ is a bijection (for contradiction).

n	$f(n)$						
0	$\cdot$	8	2	9	0	4	$\dots$
1	$\cdot$	2	2	8	7	1	$\dots$
2	$\cdot$	0	3	6	2	5	$\dots$
3	$\cdot$	6	4	8	9	1	$\dots$
4	$\cdot$	6	4	1	3	8	$\dots$
$\vdots$							

$\mathbb{R}$ is not countable

Assume $f : \mathbb{N} \to \mathbb{R} \cap [0, 1]$ is a bijection (for contradiction).

n	$f(n)$						
0	$\cdot$	8	2	9	0	4	...
1	$\cdot$	2	2	8	7	1	...
2	$\cdot$	0	3	6	2	5	...
3	$\cdot$	6	4	8	9	1	...
4	$\cdot$	6	4	1	3	8	...
$\vdots$							

$$0 \cdot 93719 \ldots \notin ran(f)$$

Let $r = 0 \cdot r_0 r_1 r_2 \ldots$ where r_n is one more than n'th decimal place of $f(n)$ if ≤ 9, else 1. Then $r \notin rng(f)$, contradicting surjectiveness of f.
Hence no bijection f exists and so $\mathbb{R}$ is uncountable.

Paradoxes

- Liar Paradox, “All Cretans are liars”

Paradoxes

- Liar Paradox, “All Cretans are liars”
- Russell's paradox. $R = \{S : S \notin S\}$. Does $R \in R$?

Paradoxes

- Liar Paradox, "All Cretans are liars"
- Russell's paradox. $R = \{S : S \notin S\}$. Does $R \in R$?
- Berry's paradox. Smallest natural number that cannot be defined uniquely by up to 80 characters.

Gödel's Incompleteness Theorem

Consider true statements of arithmetic.

$$\begin{aligned} C &= \{0, 1, 2, \ldots\} \\ F &= \{+, \times\} \\ P &= \{=, <\} \end{aligned}$$

Theorem (Gödel, 1931)

If S is any r.e. set of L-sentences then either

- *There is a statement ϕ which is true in arithmetic ($\mathbb{N}$) but $\phi \notin S$ (incompleteness), or*
- *There is a statement ϕ which is false in arithmetic and $\phi \in S$ (inconsistency).*

Proof Sketch

Idea: every character coded as a number

char	code		
p	112	x	120
(	040	)	041
$\wedge$	911	$\vee$	942
$\neg$	045	y	121
$\forall$	944	$\exists$	945
...			

e.g. $p(x)$ has code 112 040 120 041.
So can code a formula as a number.
Write $m +\!\!+ n$ for $(10 \times 10 \times \cdots \times 10 \times m) + n$ (concatenation).

Decoding

String property	first-order formula
$Form(n)$	$Atom(n) \vee Neg(n) \vee Disj(n) \vee Exist(n)$
$Atom(n)$	$\exists y \exists z((n = y{+\!+}040{+\!+}z{+\!+}041) \wedge (112 \leq y \leq 114) \wedge (120 \leq z \leq 122))$
$Neg(n)$	$\exists z(Form(z) \wedge n = 045{+\!+}z)$
$Disj(n)$	$\exists v \exists w((n = 040{+\!+}v{+\!+}942{+\!+}w{+\!+}041) \wedge Form(v) \wedge Form(w))$
$Exists(n)$	$\exists v((n = 945{+\!+}120/121{+\!+}v) \wedge Form(v))$

This recursion is well-founded.
This code number is called the "Gödel number" of the formula.

Gödel Coding

Similarly, every proof can be represented as a string using 000 as a delimeter, so every proof has a Gödel number.

We can express 'n is the code of a proof' by a first-order formula $Proof(n)$. Let G_f, G_p, F, P be coding and decoding functions, so if ϕ is a formula and $\bar{\phi}$ is a proof then $G_f(\phi)$ and $G_p(\bar{\phi})$ are their codes numbers. If $n \in \mathbb{N}$ and $Form(n)$ then $F(n)$ is the formula ϕ such that $G_f(\phi) = n$, and if $Proof(n)$ is true then $P(n)$ is the proof $\bar{\phi}$ such that $G_p(\bar{\phi}) = n$.

The proof

Can write formulas

$$\begin{aligned}\mu(n,m) &= P(n) \text{ is a proof of } F(m)\\ \lambda(n) &= F(n) \text{ is a formula with one free variable, } x\end{aligned}$$

Let

$$A_0(x), A_1(x), A_2(x), \ldots$$

be an enumeration of all the formulas with one free variable x. If $F(m)$ has just x as a free variable then $F(m) = A_k(x)$ (some k).
Can write

$$\mu(n,k,q) = (P(n) \text{ is a proof of } A_k(q))$$

Consider

$$\neg\exists n \mu(n,x,x)$$

This is a formula with one free variable. So there is some n_0 such that

$$A_{n_0}(x) = \neg\exists n \mu(n,x,x)$$

We have $\mathbb{N} \models A_{n_0}(m)$ iff "there is no proof of $A_m(m)$".
Finally, consider

$$A_{n_0}(n_0)$$

We have

$$\mathbb{N} \models A_{n_0}(n_0) \iff \text{ there is no proof of } A_{n_0}(n_0) \text{ !}$$

If $\mathbb{N} \models A_{n_0}(n_0)$ then there is no proof of $A_{n_0}(n_0)$ (incompleteness).
If $\mathbb{N} \not\models A_{n_0}(n_0)$ then there is a proof of $A_{n_0}(n_0)$. (inconsistency).

Decidable, semi-decidable

- Finite alphabet Σ, language $S \subseteq \Sigma^*$.
- S is decidable if there is a program that takes $s \in \Sigma^*$ as input, runs, always terminates, returns 1 if $s \in S$ else 0.
- S is recursively enumerable (re) or semi-decidable if there is a program that outputs only strings in S and any given string in S is eventually output.

What we've learnt

Validity

- Validity, for FOL, is semi-decidable
- The set of satisfiable first-order formulas is co-recursively enumerable (we can enumerate the unsatisfiable formulas).

Validity in $\mathbb{N}$

- The set of first order formulas valid in $\mathbb{N}$ is not even recursively enumerable.
- The theory $\Gamma = \{\phi : \mathbb{N} \models \phi\}$ has non-standard models.

Decidable, re, co-re

- Finite alphabet Σ, $S \subseteq \Sigma^*$, $\bar{S} = \Sigma^* \setminus S$,
- If S is re then $\bar{S}$ is co-re,
- If S is re and also co-re then S is decidable (how?)

First Order Logic

- Much more expressive than propositional logic
- Valdities are re but not decidable
- But first-order theories cannot define connectedness of graphs or finiteness of structures
- First-order validities of arithmetic not recursively enumerable.

First-order Logic Summary

- Syntax, $L(C, F, P)$, parsing
- Semantics: structure (D, I), valid in structure, valid over all structures.
- Axiomatic proof $\vdash$
- Tableau proof (close tableau for negated formula)
- Soundness and Strong Completeness $\Gamma \vdash \phi \iff \Gamma \models \phi$
- Recursive sets, recursively enumerable sets.
- Validities of FOL — recursively enumerable but not recursive.
- Compactness
- No first-order theory can define connectedness in graphs. No first-order theory can define $\mathbf{N} = (\mathbb{N}, \{0, 1, \ldots\}, \{+, \times\}, \{=\})$, non-standard models.
- Gödel incompleteness theorem — validities of $\mathbf{N}$ are not even recursively enumerable.
- First-order logic summary

- Syntax, $L(C, F, P)$, parsing
- Semantics: structure (D, I), valid in structure, valid over all structures.
- Axiomatic proof $\vdash$
- Tableau proof (close tableau for negated formula)
- Soundness and Strong Completeness $\Gamma \vdash \phi \iff \Gamma \models \phi$
- Recursive sets, recursively enumerable sets.
- Validities of FOL — recursively enumerable but not recursive.
- Compactness
- No first-order theory can define connectedness in graphs. No first-order theory can define $\mathbf{N} = (\mathbb{N}, \{0, 1, \ldots\}, \{+, \times\}, \{=\})$, non-standard models.
- Gödel incompleteness theorem — validities of $\mathbf{N}$ are not even recursively enumerable.
- First-order logic summary