CS121 Lecture 10: Gödel's Incompleteness Theorem

October 3rd, 2019

121.5 Friday 4pm: Theory of ML

Rice's Theorem

If $F: \{\text{Turing Machines}\} \to \{0,1\}$ has property that $F(M)$

Def. M and M' are **functionally equivalent** if for every $x \in \{0,1\}^*$, $M(x) = M'(x)$.

Notation: $M \cong M^*$

Q:

```
def f(n):
    return n+n
```

and

```
def g(n):
    i=0; r=0
    while i<n:
        r+=2; i+=1
    return r
```

Functionally equivalent?

Yes!

Def. $F: \{0,1\}^* \to \{0,1\}$ is **semantic** if for every $M \cong M'$, $F(M) = F(M')$

For every $F: \{0,1\}^* \to \{0,1\}$ if F is semantic then either $F = \text{one}$ or $F = \text{zero}$ or F is uncomputable.

What isn't a semantic function:

$$\text{LACONIC}(M) = \begin{cases} 1 & M \text{ has} \leq 100 \text{ states} \\ 0 & \text{o/w} \end{cases}$$

* not semantic $\neq$ computable!!

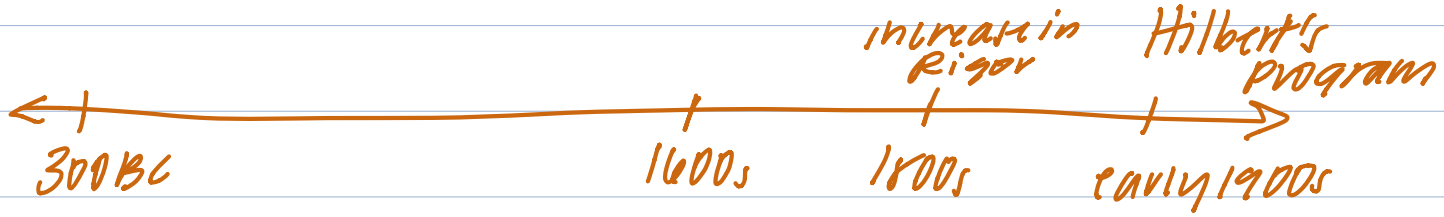
Q: HALTONSHORT(M) = 1 iff $M(x) = \perp$ whenever $|x| \leq 100$. Then HALTONSHORT is uncomputable.

$$M \cong M'$$

$$M(x) \neq \perp \leftrightarrow M'(x) = \perp$$

$$\forall x \in \{0,1\}^{\leq 100} \qquad \forall x \in \{0,1\}^{900}$$

Gödel's Incompleteness Theorem



Hilbert's Program

1) Find way to formalize all statements in math

2)

- sound: IF $A_1, \ldots A_n \vdash A$ then A is true
- complete: if A is true then $A_1, \ldots A_n \vdash A$

Gödel's 1st Incompleteness Theorem

For every axiomatic system rich enough to express quantified statements over integers if it is sound then it is not complete

Proof Systems

A **statement** is a string $x \in \{0,1\}^*$

Example: Fermat's Last Thm: "$\forall n>2\ \forall a,b,c>1$ $a^n+b^n \neq c^n$"

The statements are subset $T \subseteq \{0,1\}^*$

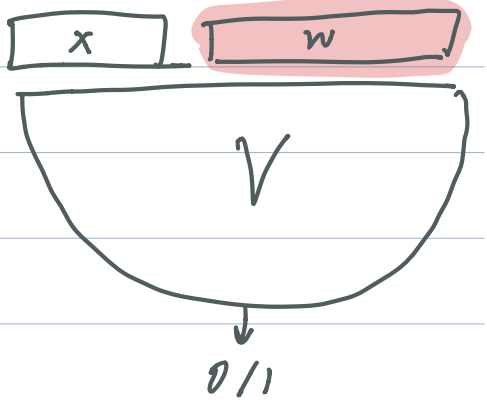
A **proof** for x is $w \in \{0,1\}^*$ that certifies $x \in T$

Denote $V(x,w)=1$ if w is a valid proof for x

↳ line by line proof

Proof system is:

- Effective if V is computable
- Sound if $V(x,w)=1 \rightarrow x \in T$
- Complete if $x \in T \rightarrow$ $\exists w \in \{0,1\}^*\ V(x,w)=1$



Gödel's: Let $T \subseteq \{0,1\}^*$ be the set of all true statements about natural numbers involving $\forall, \exists, \wedge, \vee, \neg, \times, +, =, >, <$. There does not exist an effective, sound, and complete proof for T.

↳ basically saying there are statements that are true and have no proof

♡ of Gödel: Let $QIS: \{0,1\}^* \to \{0,1\}$ defined as $QIS(x) = 1$ iff $x \in T$. Then QIS is uncomputable.

♡→ Theorem: Suppose (contradiction) V is system for T. Consider Alg A:

Alg A.

```
Input: x ∈ {0,1}*
for n = 1, 2, 3...:
    for w ∈ {0,1}^n:
        if V(x, w) = 1 return 1
        if V(¬x, w) = 1 return 0
```

Claim 1: If $x \in T$ then $A(x)$ halts and outputs 1

Claim 2: If $x \notin T$ then $A(x)$ halts and outputs 0

Immediate Corollary: (TM version)

Let $T \subseteq \{0,1\}^*$ be the set of all true statements about TMs of the form "Machine M halts / doesn't halt on input x". There does not exist an effective, sound, complete proof system for T.

♡ of Thm: Let $HALT: \{0,1\}^* \to \{0,1\}$ defined as $HALT(M, x) = 1$ iff M halts on x. Then $HALT$ is uncomputable.

encodes as ints

cellular automata / configurations

HALT is uncomputable → PUZZLE is uncomputable → QMS is uncomputable → QIS is uncomputable

↓ immediate

Gödel's for TM

↓ immediate

Gödel's for quantified integer statements

CAHALT: $\{0,1\}^* \to \{0,1\}$

input: rule $r: \Gamma^3 \to \{0,1\}$, starting conf $x_0 \dots x_n \in \Gamma$

output: 1 iff eventually reach $x_0 = 1$

Thm:

Proof: CAs can simulate TMs

PUZZLE: $\{0,1\}^* \to \{0,1\}$

input: puzzle pieces, aka $match_\downarrow, match_\rightarrow : \Sigma^2 \to \{0,1\}$

output: 1 iff $\exists$ smooth rectangle, aka

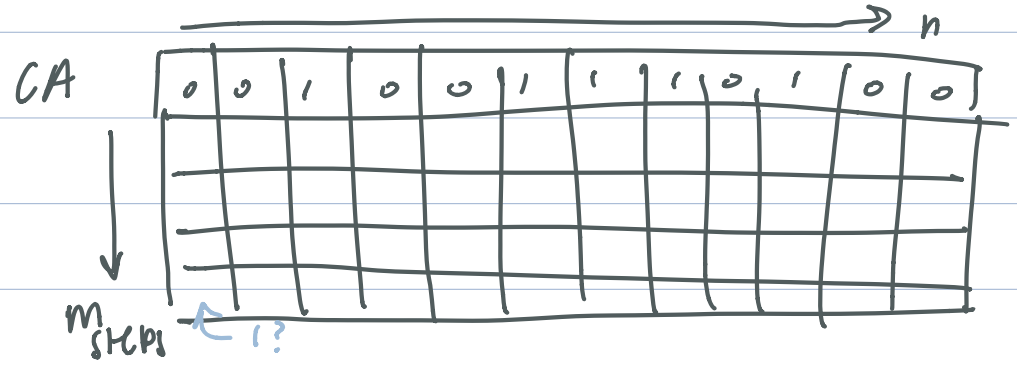
$$\exists x \in \Sigma^{m \cdot n} \text{ s.t. } \forall i \in [m-1], j \in [n-1]$$

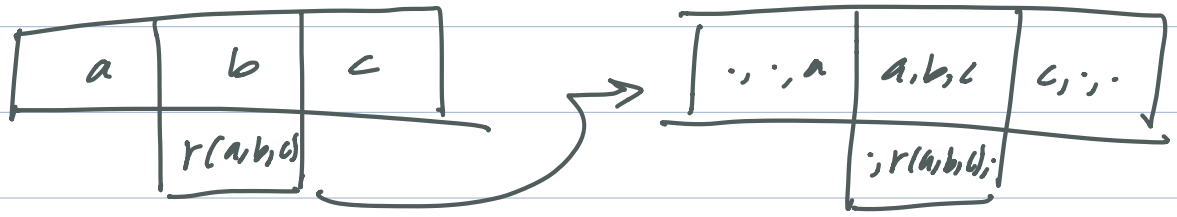
$$match_\downarrow(x_{ij}, x_{i+1,j}) \wedge match_\rightarrow(x_{ij}, x_{ij+1})$$

$$\text{and } x_{0,j} = x_{m-1,j} = x_{i,0} = x_{i,n-1} = \phi$$

Thm: PUZZLE is uncomputable.

Proof: if you could solve PUZZLE you could solve CAHALT.





QMS : $\{0,1\}^* \to \{0,1\}$ quantified mixed statements

input: statements about natural numbers and strings

$\forall, \exists, \vee, \wedge, \neg, \times, +, =, <, >$, and $|x|, x_i$

output: 1 iff s is true

Thm: QMS is uncomputable.

Proof: If you can compute QMS then you can compute PUZZLE.

QIS : $\{0,1\}^* \to \{0,1\}$ quantified integer statements

input: statements about natural numbers ~~and strings~~

$\forall, \exists, \vee, \wedge, \neg, \times, +, =, <, >$, and ~~$|x|, x_i$~~

Thm: QIS is uncomputable

Proof: If you can compute QIS then you could compute QMS.

Need: Encode string $x \in \{0,1\}^*$ as natural number $N(x) \in \mathbb{N}$

Come up w/ statements LEN, COORD satisfying

(1) LEN(N(x), n) true $\iff |x| = n$

(2) COORD(N(x), i) true $\iff x_i = 1$

Define $p_0, p_1, p_2 \ldots$ as follows: p_i is smallest prime # $> (i+1000)^3$

- encode 11 as $p_2 \cdot p_1 \cdot p_0$, 01001 as $p_4 \cdot p_3 \cdot p_0$, etc
- $LEN(N, n) := p_n | N \wedge \forall m > n \; p_m \nmid N$
- $COORD(N, i) := p_i | N$