Harvard CS 121 and CSCI E-121

Lecture 18: Undecidable Problems and Unprovable Theorems

Harry Lewis

November 5, 2013

Recursion Theory over $\mathcal{N}$

- We have presented this theory as a theory of languages
- Classically it is treated as a theory of sets of numbers
- The two are equivalent since strings can be converted to numbers (treating strings as numerals, for example) and v.v.
- So it makes sense to say "The set of primes is recursive"
- Similarly we can index the r.e. sets $S_0, S_1, \ldots$, where S_i is the r.e. set recognized [or, alternatively, enumerated] by the TM whose description is the binary numeral that represents i

Recursive functions

- A function f is recursive if f is computable
- e.g. if there is a TM that always leaves $f(w)$ on the tape when started with input w
- Similarly we can speak of a recursive function from numbers to numbers
- Thm: A nonempty set is r.e. iff it is the range of a recursive function

Partial Recursive Functions

- A partial recursive function is a function whose domain is a subset of Σ^* and which is computed by a TM
- That is, ϕ is a p.r.f. if there is a TM M, such that, when M is started with input w, M halts and leaves output u on the tape iff $u = \phi(w)$
- A set is r.e. iff it is the domain of a partial recursive function
- The p.r.f.s can be indexed $\phi_0, \phi_1, \phi_2, \ldots$

Degrees of unsolvability

- The (mapping) reduction $\leq_m$ is a partial order (reflexive and transitive)
- The equivalence classes are called *degrees*
- We have identified two degrees:
  - The recursive sets
  - The sets equivalent to the halting problem (the r.e.-complete sets)
- The degree structure of non-recursive sets is extremely rich ("Recursive function theory")
- The important question for us is: What other problems are r.e.-complete?

Unsolvability of Derivability in General Grammars

- **Theorem:** There is no algorithm to determine, given any grammar G and any string w, whether $w \in L(G)$.

  Proof: Suppose there were such a decision procedure.

  Then we could use it to solve the halting problem:

  Given M and w, to determine if M halts on input w, construct a grammar G such that $L(M) = L(G)$ and determine if $w \in L(G)$.

  G simulates computations of M run backwards!

  Since the halting problem is unsolvable, so is this problem.

- There is a particular grammar G_0 for which this problem is unsolvable: namely, the grammar for the universal TM.

Two-Counter Machines

- A counter machine can add and subtract 1 from its registers and check if they are zero.
- **Theorem:** The halting problem is unsolvable even for 2-counter machines.
- **Proof:**
  1. One TM tape to two pushdown stores
  2. One pushdown store to two counters
  3. Four counters to two counters

An Undecidable Problem about Context Free Grammars

Theorem: It is undecidable to determine, given CFGs G_1 and G_2, whether $L(G_1) \cap L(G_2) = \emptyset$.

Proof: Reduction from $\{\langle G, w\rangle : G$ is a general grammar generating $w\}$

- Given $\langle G, w\rangle$, we can construct grammars G_1, G_2 such that:

$$L(G_1) = \{C_1 \# D_1^R \# C_2 \# D_2^R \# \cdots \# C_n \# D_n^R : \\ n \geq 1, \text{ and for each } i,\ C_i \Rightarrow_G D_i\ \}.$$

$$L(G_2) = S \# C_2^R \# C_2 \# C_3^R \# C_3 \# \cdots \# C_n^R \# w^R : \\ n \geq 1 \text{ and the } C_i \text{ are arbitrary strings}\}.$$

- G_1 generates pairs of unrelated one-step derivations
- G_2 has S and w at beginning and end, and in between pairs match (even positions reversed)

Intersection of CFLs, continued

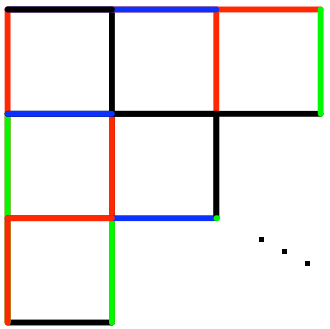
- Any string in $L(G_1)$ or $L(G_2)$ has an odd number of $\#$s
- Any string in $L(G_1) \cap L(G_2)$ is a derivation of w in G (every other intermediate string is reversed)
- So $L(G_1) \cap L(G_2)$ is nonempty iff w is derivable in G
- So $\langle G, w \rangle \mapsto \langle G_1, G_2 \rangle$ is a reduction from general grammar derivability to $\{\langle G_1, G_2 \rangle : L(G_1) \cap L(G_2) \neq \emptyset\}$.

Verifying computations is easier than carrying them out!

Tiling

Tiling: Given a finite set of patterns for square tiles:

Is it possible to tile the whole plane with tiles of these patterns in such a way that the abutting edges match?



Theorem: Tiling is undecidable.

Tiling, continued

Variant of tiling: fix the tile at the origin and ask whether the first quadrant can be tiled (easier to show undecidability).

Proof by reduction from $\overline{L_\varepsilon}$:

- $\langle M \rangle \overset{f}{\mapsto}$ sets of tiles so that:

  M does not halt on $\varepsilon \Leftrightarrow f(\langle M \rangle)$ tiles the first quadrant.

- View computation of M as "tableau", filling first quadrant with elements of $C = Q \cup \Gamma$, each row being a configuration of M.
- Computation valid iff every 2×3 window consistent with transition function of M (and bottom row is correct initial configuration).
- Each tile represents a 2×3 window of tableau. Edge colors force consistency with neighbors on overlap.

Post's Correspondence Problem

A correspondence system is a finite collection of ordered pairs of strings

$$(x_1, y_1), \ldots, (x_n, y_n) \qquad (x_i, y_i \in \Sigma^*)$$

A match in this C.S. is a sequence of pairs (likely with repetitions) such that the concatenation of the first components is the same string as the concatenation of the second components.

i.e. a sequence of indices $j_1, \ldots, j_k (1 \leq j_i \leq n)$ such that $x_{j_1} x_{j_2} \ldots x_{j_k} = y_{j_1} y_{j_2} \ldots y_{j_k}$

Thm: It is unsolvable to determine, given a C.S., whether that C.S. has a match.

Diophantine Equations

These are equations like

$$x^3y^3 + 13xyz = 4u^2 - 22$$

The coefficients and the exponents have to be integers. (No variables in the exponents!)

The question is whether the equation can be satisfied (made true) by substituting integers for the variables—this is known as Hilbert's 10th problem.

Diophantus of Alexandria (200-284 AD)

- “God gave him his boyhood one-sixth of his life, One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage, after attaining half the measure of his father’s life, chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.”

- Other problems concerning triangular arrays, etc., gave rise to quadratic equations.

- Fermat’s statement of his ”Last Theorem” was in the margin of his copy of Diophantus.

"Hilbert's 10th Problem"

10. Determination of the Solvability of a Diophantine Equation.

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Thm (Matiyasevich, 1970): Hilbert's 10th problem is unsolvable.

Diophantine sets

- A set of natural numbers is *Diophantine* iff it is $\{x : (\exists y_1, y_2, \ldots, y_n) P(x, y_1, y_2, \ldots, y_n)\}$ where P is some diophantine equation with $n + 1$ variables ranging over $\mathcal{N}$.
- A set is Diophantine iff is r.e.
- n can be restricted to 9!

Relation to Gödel's Incompleteness Theorem

- Axiom systems for mathematics, e.g.
  - Peano arithmetic — attempt to capture properties of $\mathcal{N}$
    - E.g. mathematical induction:

      If $P[0]$

      and, for all n, $P[n] \Rightarrow P[n+1]$,

      then for all n, $P[n]$
  - Zermelo-Frankel-Choice set theory (ZFC) — enough for all of modern mathematics
- Proofs of theorems from these axiom systems defined by (simple) rules of mathematical logic.

The Decision Problem (for Mathematics)

- **Entscheidungsproblem** is German for “Decision Problem”
- **The** Decision Problem is the problem of determining whether a mathematical statement is provable
- **Proposition:** Set of provable theorems is Turing-recognizable.
- **Is it decidable?**

Undecidability of mathematics

Theorem [Church, Turing]: Set of true statements of arithmetic (using just $+$ and $\times$) is undecidable.

Proof sketch:

- Reduce from $\text{HALT}^{\varepsilon}_{\text{TM}}$.
- $\langle M \rangle \mapsto$
  mathematical statement P_M = "$(\exists n) M$ halts on ε after n steps".
- M halts on ε iff P_M is true.

Incompleteness of Mathematics

Gödel's Incompleteness Theorem: Some true statement is not provable.

Proof sketch:

- For every statement ϕ, either ϕ or $\neg\phi$ is true.
- Suppose all true statements provable.

  $\Rightarrow$ For all statements ϕ, exactly one of ϕ and $\neg\phi$ is provable.

  $\Rightarrow$ Set of provable theorems r.e. and co-r.e.

  $\Rightarrow$ Set of provable theorems decidable.
- Contradiction.

See Sipser Chapter 6 for more on this & other advanced topics on computability theory.