Computer Science 513

Introduction to Post's Problem

Instructor: Wayne Eberly

Department of Computer Science
University of Calgary

Lecture #18

Goals for Today

Goals for Today:

- Introduce ***degrees of difficulty*** — "Q=degrees," for any reducibility Q
- Introduce ***Post's problem*** and some of the research that its investigation triggered
- Introduce ***recursive permutations*** and relate these to **1*-equivalence***
- Introduce ***cylinders*** and use these to relate 1-degrees to m-degrees

References:

- Hartley Rogers, Jr., *Theory of Recursive Functions and Effective Computability*
- *Computability, Complexity and Languages*, Section 8.9

Degrees of Difficulty of Computation

Recall, from Lecture #11, that if $\preceq_Q$ is a reducibility and $A, B \subseteq \mathbb{N}$, then A is ***Q-equivalent*** to B, $A \equiv_Q B$, if $A \preceq_Q B$ and $B \preceq_Q A$.

It is also easily proved that, for all $A, B, C \subseteq \mathbb{N}$,

- $A \equiv_Q A$ — that is, $\equiv_Q$ is ***reflexive;***
- if $A \equiv_Q B$ then $B \equiv_Q A$ — that is, $\equiv_Q$ is ***symmetric***, and
- if $A \equiv_Q B$ and $B \equiv_Q C$ then $A \equiv_Q C$ — that is, $\equiv_Q$ is ***transitive***.

Thus $\equiv_Q$ is an example of an ***equivalence relation***.

Degrees of Difficulty of a Computation

Definition: A ***Q-degree*** is a collection of subsets $\mathbb{N}$ with the form

$$\{A\}_Q = \{S \subseteq \mathbb{N} \mid S \equiv_Q A\}$$

for some set $A \subseteq \mathbb{N}$. That is, $\{A\}_Q$ is the collection of subsets of $\mathbb{N}$ that are Q-equivalent to A.

In other words, a Q-degree is an ***equivalence class*** of the equivalence relation $\equiv_Q$.

Definition: A ***Turing-degree*** is a T-degree, that is, an equivalence class of the equivalence relation $\equiv_T$.

Turing-Degrees

A ***counting argument*** can be used to establish that the number of different Turing-degrees is uncountable:

- Since the number $\mathcal{S}$-programs with an oracle (for some fixed total function) is countable, every Turing degree must be countable as well.
- Since $\mathbb{N} \times \mathbb{N}$ is countable, this could be used to show that the set of subsets of $\mathbb{N}$ would be countable as well, if there were only countably many Turing degrees.
- However, the set of subsets of $\mathbb{N}$ is uncountable, so the set of Turing degrees must be uncountable too.

Turing-Degrees

On the other hand, since $\mathcal{AH}$ is countable, the set of Turing degrees that are subsets of $\mathcal{AH}$ must be countable too.

- Recall that, for $n \geq 1$, Δ_{n+1} is the set of subsets $A \subseteq \mathbb{N}$ such that $A \preceq_T \emptyset^{(n)}$.
- This can be used to argue that $\{\emptyset^{(n)}\}_T \subseteq \Delta_{n+1} \setminus \Delta_n$.
- It follows that the Turing degrees

$$\{\emptyset^{(1)}\}_T, \{\emptyset^{(2)}\}_T, \{\emptyset^{(3)}\}_T, \dots$$

are distinct — so the set of Turing degrees that are subsets of $\mathcal{AH}$ is countable but infinite.

Turing-Degrees

There are at least ***two*** Turing degrees that include computably enumerable sets:

1. The Turing degree $\{\emptyset\}_T$ — which is the collection of all ***computable*** sets.
2. The Turing degree $\{\emptyset^{(1)}\}_T$. Since $\emptyset^{(1)}$ is a computably enumerable set that is Turing-complete for Σ_1 (and, indeed, for Δ_2), this includes all computably enumerable sets that are Turing-complete for Σ_1 — along with their complements, the sets that are Turing-complete for Π_1.

Post's Problem

In 1944 Emil Post asked the following question, which is now known as ***Post's problem:***

> *Does there exist a computably enumerable set that is not computable, and not T-complete for Σ_1?*

This is the same as the question

> *Does there exist a third Turing-degree that includes computably enumerable sets?*

as well as the question

> *Does there exist a computably enumerable set $A \subseteq \mathbb{N}$ such that $A \not\leq_T \emptyset$ and $\emptyset^{(1)} \not\leq_T A$?*

This question was open until 1956, when Friedberg and Muchnik independently (and almost simultaneously) proved that the answer is "Yes."

Post's Problem

Attempts to solve Post's problem lead to studies of 1-degrees, m-degrees, and Q-degrees for various other reducibilities $\preceq_Q$ as well.

The next set of lectures will include *some* of the results that were developed as part of this study.

One-One Equivalence

Recall that a total function $f : \mathbb{N} \to \mathbb{N}$ is ***one-one*** if $f(x) \neq f(y)$ for all $x, y \in \mathbb{N}$ such that $x \neq y$, and that if $A, B \subseteq \mathbb{N}$ then $A \preceq_1 B$ if there exists a one-one computable function $f : \mathbb{N} \to \mathbb{N}$ such that $x \in A$ if and only if $f(x) \in B$ for all $x \in \mathbb{N}$.

- It was noted, in Lecture #15, that $\preceq_1$ is a reducibility — so that **1*-degrees*** can be defined as described above.

Recursive Permutations

Definition: A total function $f : \mathbb{N} \to \mathbb{N}$ is a ***permutation*** if f is both one-one and onto, that is,

(a) For all $x, y \in \mathbb{N}$, if $x \neq y$ then $f(x) \neq f(y)$, and
(b) for all $z \in \mathbb{N}$ there exists $x \in \mathbb{N}$ such that $f(x) = z$.

A total function $f : \mathbb{N} \to \mathbb{N}$ is a ***recursive permutation*** if f is a permutation and f is computable.

It is not hard to show that if $f : \mathbb{N} \to \mathbb{N}$ then its ***inverse*** $f^{-1} : \mathbb{N} \to \mathbb{N}$, such that, for all $z \in \mathbb{N}$,

$$f^{-1}(z) = \min_x (z = f(x))$$

is a recursive permutation as well.

Recursive Isomorphism

Definition: Let $A, B \subseteq \mathbb{N}$. Then A is ***recursively isomorphic*** to B,

$$A \equiv B,$$

if there exists a recursive permutation $f : \mathbb{N} \to \mathbb{N}$ such that $x \in A$ if and only if $f(x) \in B$ for all $x \in \mathbb{N}$.

- Note that if f is a recursive permutation then f is a one-one computable function.
- It follows that if $A \equiv B$ then $A \equiv_1 B$ for all $A, B \subseteq \mathbb{N}$.

Codes of Finite Sequences of Ordered Pairs

Consider a finite sequence

$$(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n) \tag{1}$$

of ***ordered pairs*** of natural numbers.

- The ***code*** of this sequence is the number

  $$u = \langle n, [\langle a_1, b_1\rangle, \langle a_2, b_2\rangle, \ldots, \langle a_n, b_n\rangle]\rangle$$

  that is formed using the pairing function $\langle \cdot, \cdot \rangle$ and Gödel numbering.
- The sequence can be recovered from its code using the relationship

  $a_i = \ell((r(u))_i)$ and $b_i = r((r(u))_i)$ for $1 \leq i \leq \ell(u)$.

Codes of Finite Sequences of Ordered Pairs

Definition: Let $A, B \subseteq \mathbb{N}$. Then the finite sequence of ordered pairs, shown at line (1), ***associates*** A and B if the following properties are satisfied:

(a) $a_i \neq a_j$ for $1 \leq i < j \leq n$ — so that $a_1, a_2, \ldots, a_n$ are distinct;

(b) $b_i \neq b_j$ for $1 \leq i < j \leq n$ — so that $b_1, b_2, \ldots, b_n$ are distinct;

(c) for every integer i such that $1 \leq i \leq n$, ***either*** $a_i \in A$ and $b_i \in B$ ***or*** $a_i \neq A$ and $b_i \neq B$.

Codes of Finite Sequences of Ordered Pairs

Lemma #1: Let $A, B \subseteq N$ such that $A \preceq_1 B$. Then there exists a computable total function $k : \mathbb{N}^2 \to \mathbb{N}$ such that, for all $u, a \in \mathbb{N}$, if

- u codes the sequence shown at line (1), and this sequence associates A and B, and
- $a \notin \{a_1, a_2, \ldots, a_n\}$,

then there exists a number $b \in \mathbb{N}$ such that $k(u, a)$ is the code of the finite sequence

$$(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n), (a, b) \tag{2}$$

and this sequence also associates A and B.

The supplemental document includes a proof of this claim.

Myhill's Theorem

Theorem #2 (Myhill's Theorem): Let $A, B \subseteq \mathbb{N}$. Then $A \equiv_1 B$ if and only if $A \equiv B$.

As previously noted, if $A, B \subseteq \mathbb{N}$ and $A \equiv B$ then $A \equiv_1 B$, so it remains only to establish the converse. This can be established using Lemma #1, above. Once again, the supplemental document includes a proof of this result.

Implications of Myhill's Theorem

For $n \in \mathbb{N}$, let $[n] = \{1, 2, 3, \ldots, n\} \subseteq \mathbb{N}$.

It immediately follows that there are (countably) *infinitely* many 1-degrees that include computably enumerable sets, including (but not necessarily limited to) the following:

(a) $\{[n]\}_1$ — the collection of all finite subsets of $\mathbb{N}$ with size n, for all $n \in \mathbb{N}$

(b) $\{\mathbb{N} \setminus [n]\}_1$ — the collection of all subsets of $\mathbb{N}$ whose *complements* are finite sets with size n, for all $n \in \mathbb{N}$

(c) $\{E\}_1$, where $E = \{2n \mid n \in \mathbb{N}\}$

(d) $\{\emptyset^{(1)}\}_1$, the collection of all sets that are 1-complete for Σ_2.

m-Degrees vs. 1-Degrees

- Notice, however, that every computable set A such that $A \neq \emptyset$ and $A \neq \mathbb{N}$ is m-complete for the set of computable sets, so these are each m-equivalent, and included in the degree $\{[1]\}_m$.
- Since this includes $\{[n]\}_1$ and $\{\mathbb{N} \setminus [n]\}_1$ for all $n \geq 1$, along with $\{E\}_1$, a single m-degree (consisting entirely of computable sets) includes infinitely many 1-degrees.
- Since $A \preceq_1 B$ implies that $A \preceq_m B$ for all $A, B \subseteq \mathbb{N}$, every 1-degree is a subset of a single m-degree.
- ***Question:*** How many 1-degrees can be contained in a single m-degree? How are they organized?
- This question motivates the following.

Cylinders

Definition: Let $S \subseteq \mathbb{N}$. Then the ***cylindrication*** of S is the set

$$Cyl(S) = \{\langle a, b\rangle \mid a \in S \text{ and } b \in \mathbb{N}\}.$$

A set $A \subseteq \mathbb{N}$ is a ***cylinder*** if $A \equiv Cyl(S)$ for some set $S \subseteq \mathbb{N}$.

Theorem #3: Let $A \subseteq \mathbb{N}$.

(a) $A \preceq_1 Cyl(A)$.

(b) $Cyl(A) \preceq_m A$ (and, therefore, $A \equiv_m Cyl(A)$).

(c) A is a cylinder if and only if and only if the following is true for every set $B \subseteq \mathbb{N}$: If $B \preceq_m A$ then $B \preceq_1 A$.

(d) $A \preceq_m B$ if and only if $Cyl(A) \preceq_1 Cyl(B)$, for all $B \subseteq \mathbb{N}$.

Once again, a proof can be found in the supplementary document for this lecture.

Cylinders

Corollary #4: Let $A \subseteq \mathbb{N}$. Then the following are equivalent:

(a) A is a cylinder.

(b) $Cyl(A) \preceq_1 A$.

(c) $A \equiv Cyl(A)$.

Proof:

- If A is a cylinder then parts (b) and (c) of the above result establish that $Cyl(A) \preceq_1 A$. Thus condition (a) implies condition (b).
- If $Cyl(A) \preceq_1 A$ then, since $A \preceq_1 Cyl(A)$ as well, by part (a) of the above result, $A \equiv_1 Cyl(A)$. Myhill's Theorem now implies that $A \equiv Cyl(A)$, so that condition (b) implies condition (c).
- Finally, if $A \equiv Cyl(A)$, then it follows, by definition. that A is a cylinder. Thus condition (c) implies condition (a). $\square$

m-Degrees and 1-Degrees

- Recall that the set of computable subsets of $\mathbb{N}$, and the set of computably enumerable subsets of $\mathbb{N}$, are both 1-closed and *m*-closed. Thus each 1-degree or *m*-degree either
  - consists entirely of (some) computable sets, or
  - consists entirely of computably enumerable sets that are not computable, or
  - consists entirely of sets that are not computably enumerable.
- Since $A \preceq_1 B \implies A \preceq_m B$ for all sets $A, B \subseteq \mathbb{N}$, every 1-degree is contained in an *m*-degree.
- We have seen an *m*-degree, consisting of computable sets, that includes *infinitely many* 1-degrees.
- At this point, we have *not* proved whether (or not) *m*-degrees, consisting of computably enumerable sets that are not computable, can include more than a single 1-degree.

m-Degrees and 1-Degrees

The following — which is a reasonably easy exercise to solve, now — helps to explain why ***cylinders*** are of interest:

Exercise:

1. Prove that every m-degree S includes a ***maximal*** 1-degree, that is a 1-degree T such that, $A \preceq_1 B$ for all $A \in S$ and $B \in T$. In particular, this is true when

$$T = \{Cyl(A) \mid A \in S\}.$$

2. Prove that if every set A that is computably enumerable, but not computable, is also a cylinder, the every m-degree including sets that are computably enumerable, but not computable, is also a 1-degree.

m-Degrees and 1-Degrees

3. Prove if there exists a set $A \subseteq \mathbb{N}$ that is computably enumerable, but not computable, and A is also *not* a cylinder, then there exists an *m*-degree, consisting of sets that are computably enumerable, that contains more than one 1-degree.

Indeed, the next lecture will include a proof that a set A, with the properties given in Exercise #3, *does* exist — so that at least one *m*-degree, including sets that are computably enumerable but not computable, exists that contains more than a single 1-degree.