Computability Theory

Check List For Final Exam, Xiaofeng Gao's Section, 2015 Spring

Description:

This checklist covers all the contents for the final exam. It includes Chapter 6 to Chapter 9. (Note: Multiple options are available to prepare for the final exam. Reading the textbook is a must for success. Slides, assignments, and answer keys can be good supplements for all topics. For the notations, please refer to the Notations in the text book, page 241-245.)

Chapter 6. Decidability, undecidability and partial decidability

1. Decidability:
   (a) **Definition**. A predicate $M(\mathbf{x})$ is decidable if its characteristic function $c_M(\mathbf{x})$ given by $c_M(\mathbf{x}) = \begin{cases} 1, & \text{if } M(\mathbf{x}) \text{ holds,} \\ 0, & \text{if } M(\mathbf{x}) \text{ does not hold.} \end{cases}$ is computable.
   (b) The predicate $M(\mathbf{x})$ is undecidable if it is not decidable.
   (c) In literature $M(\mathbf{x})$ is decidable can be described as $M(\mathbf{x})$ is recursively decidable, $M(\mathbf{x})$ has recursive decision problem, $M(\mathbf{x})$ is solvable, $M(\mathbf{x})$ is recursively solvable, or $M(\mathbf{x})$ is computable.
2. Undecidable problems in computability:
   (a) **Theorem**. The problem '$x \in W_x$' is undecidable.
   (b) **Corollary**. There is a computable function h such that both '$x \in Dom(h)$' and '$x \in Ran(h)$' are undecidable.
   (c) **Theorem**. (the Halting problem) The problem '$\phi_x(y)$ is defined' is undecidable.
   (d) **Theorem**. The problem '$\phi_x = \mathbf{0}$' is undecidable.
   (e) **Corollary**. The problem '$\phi_x = \phi_y$' is undecidable.
   (f) **Theorem**. Let c be any number. The followings are undecidable.
      i. Acceptance Problem: '$c \in W_x$',
      ii. Printing Problem: '$c \in E_x$'.
   (g) **Theorem**. (Rice's theorem) '$\phi_x \in \mathscr{B}$' is undecidable for $\emptyset \subsetneq \mathscr{B} \subsetneq \mathscr{C}_1$.
3. Partially decidable predicates:
   (a) **Definition**. A predicate $M(\mathbf{x})$ of natural numbers is partially decidable if the function given by $f(\mathbf{x}) = \begin{cases} 1, & \text{if } M(\mathbf{x}) \text{ holds,} \\ \text{undefined}, & \text{if } M(\mathbf{x}) \text{ does not hold,} \end{cases}$ is computable.
   The function is called the partial characteristic function for M.
   (b) In the literature the terms partially solvable, semi-computable, and recursively enumerable are used with the same meaning as partially decidable.
   (c) partially decidable predicates:
      i. The halting problem is partially decidable. Its partial characteristic function is given by $f(x, y) = \begin{cases} 1, & \text{if } P_x(y)\downarrow, \\ \text{undefined}, & \text{otherwise.} \end{cases}$
      ii. The problem '$x \notin W_x$' is not partially decidable. The domain of its partial characteristic function differs from the domain of every computable function.
   (d) **Theorem**. A predicate $M(\mathbf{x})$ is partially decidable iff there is a computable function $g(x)$ such that $M(\mathbf{x}) \Leftrightarrow \mathbf{x} \in Dom(g)$.
   (e) **Theorem**. A predicate $M(\mathbf{x})$ is partially decidable iff there is a decidable predicate $R(\mathbf{x}, y)$ such that $M(\mathbf{x}) \Leftrightarrow \exists y.R(\mathbf{x}, y)$.
   (f) **Theorem**. If $M(\mathbf{x}, y)$ is partially decidable, so is $\exists y.M(\mathbf{x}, y)$.
   (g) **Corollary**. If $M(\mathbf{x}, \mathbf{y})$ is partially decidable, so is $\exists \mathbf{y}.M(\mathbf{x}, \mathbf{y})$.

(h) **Theorem**. $M(\mathbf{x})$ is decidable iff both $M(\mathbf{x})$ and $\neg M(\mathbf{x})$ are partially decidable.
(i) **Corollary**. The problem '$y \notin W_x$' is not partially decidable.
(j) **Theorem**. Let $f(\mathbf{x})$ be a partial function. Then f is computable iff the predicate '$f(\mathbf{x}) \simeq y$' is partially decidable.

Key Terms:

Decidability, Undecidability, the Halting problem, Rice's theorem, partial decidability.

Practice and Sources:

1. Slide08-Undecidability; 2. Textbook page 100-120

Chapter 7. Recursive And Recursively Enumerable Sets

1. Recursive Sets:
   (a) **Definition**. Let A be a subset of $\mathbb{N}$. The characteristic function of A is given by $c_A(x) = \begin{cases} 1, & \text{if } x \in A, \\ 0, & \text{if } x \notin A. \end{cases}$ A is recursive if $c_A(x)$ is computable.
   (b) Examples of recursive sets:
      i. $\mathbb{N}$, $\mathbb{Z}$.
      ii. $\mathbb{E}$ (even numbers).
      iii. $\mathbb{O}$ (odd numbers).
      iv. $\mathbb{O}$ (prime numbers).
      v. Any finite set.
   (c) Examples of unsolvable problems:
      i. $K = \{x \mid x \in W_x\}$, $\overline{K} = \{x \mid x \notin W_x\}$
      ii. $Fin = \{x \mid W_x \text{ is finite}\}$, $Inf = \{x \mid W_x \text{ is infinite}\}$,
      iii. $Cof = \{x \mid W_x \text{ is cofinite}\}$, $Tot = \{x \mid \phi_x \text{ is total}\}$,
      iv. $Rec = \{x \mid W_x \text{ is recursive}\}$,
      v. $Ext = \{x \mid \phi_x \text{ is extensible to total recursive function}\}$.
   (d) **Fact**. Recursive Set $\Leftrightarrow$ Solvable Problem $\Leftrightarrow$ Decidable Predicate.
   (e) **Theorem**. If A, B are recursive sets, then so are the sets $\overline{A}$, $A \cap B$, $A \cup B$, $A \backslash B$.
2. Recursively Enumerable Sets (r.e. set):
   (a) **Definition**. Let A be a subset of $\mathbb{N}$. Then A is recursively enumerable if the function f given by $f(x) = \begin{cases} 1, & \text{if } x \in A, \\ \text{undefined}, & \text{if } x \notin A. \end{cases}$ is computable.
   Notation 1. A is also called semi-recursive set, semi-computable set.
   Notation 2. Subsets of $\mathbb{N}^n$ can be defined as r.e. by coding to r.e. subsets of $\mathbb{N}$.
   (b) **Fact**. Partially Decidable Problem $\Leftrightarrow$ Partially Decidable Predicate $\Leftrightarrow$ R. E. Set
   (c) **Index Theorem**. A set is r.e. iff it is the domain of a unary computable function.
   (d) **Normal Form Theorem**. The set A is r.e. iff there is a primitive recursive predicate $R(\mathbf{x}, y)$ such that $\mathbf{x} \in A$ iff $\exists y.R(\mathbf{x}, y)$.
   (e) **Quantifier Contraction Theorem**. If $M(\mathbf{x}, \mathbf{y})$ is partially decidable, so is $\exists \mathbf{y}.M(\mathbf{x}, \mathbf{y})$ ($\{\mathbf{x} \mid \exists \mathbf{y}.M(\mathbf{x}, \mathbf{y})\}$ is r.e.).
   (f) **Uniformisation Theorem**. If $R(x, y)$ is partially decidable, then there is a computable function $c(x)$ such that $c(x) \downarrow$ iff $\exists y.R(x, y)$ and $c(x) \downarrow$ implies $R(x, c(x))$.
   (g) **Complementation Theorem**. A is recursive iff A and $\overline{A}$ are r.e.
   (h) **Graph Theorem**. Let $f(x)$ be a partial function. Then $f(x)$ is computable iff the predicate '$f(x) \simeq y$' is partially decidable iff $\{\pi(x, y) \mid f(x) \simeq y\}$ is r.e.
   (i) **Listing Theorem**. A is r.e. iff $A = \varnothing$ or $A = Ran(f)$ for a total function $f \in \mathscr{C}_1$.
   Equivalence Theorem. Let $A \subseteq \mathbb{N}$. Then the following are equivalent:
      i. A is r.e.
      ii. $A = \emptyset$ or A is the range of a unary total computable function.
      iii. A is the range of a (partial) computable function.
   Theorem. Every infinite r.e. set has an infinite recursive subset.
   Theorem. An infinite set is recursive iff it is the range of a total increasing computable

function (if it can be recursively enumerated in increasing order).
Theorem. The set $\{x \mid \phi_x \text{ is total}\}$ is not r.e.

(j) **Closure Theorem**. The recursively enumerable sets are closed under union and intersection uniformly and effectively.

(k) **Rice-Shapiro Theorem**. Suppose that $\mathcal{A}$ is a set of unary computable functions such that the set $\{x \mid \phi_x \in \mathcal{A}\}$ is r.e. Then for any unary computable function f, $f \in \mathcal{A}$ iff there is a finite function $\theta \subseteq f$ with $\theta \in \mathcal{A}$.
Corollary. The sets $\{x \mid \phi_x \text{ is total}\}$ and $\{x \mid \phi_x \text{ is not total}\}$ are not r.e.

(l) **Theorem**. If A and B are r.e., then so are $A \cap B$ and $A \cup B$.

3. Productive Sets:

(a) **Definition**. A set A is productive if there is a total computable function g such that whenever $W_x \subseteq A$, then $g(x) \in A \setminus W_x$. g is called a productive function for A.
Notation. A productive set is not r.e.

(b) Examples of productive sets:
i. $\{x \mid \phi_x \neq \mathbf{0}\}$ is productive.
ii. $\{x \mid c \notin W_x\}$ is productive.
iii. $\{x \mid c \notin E_x\}$ is productive.

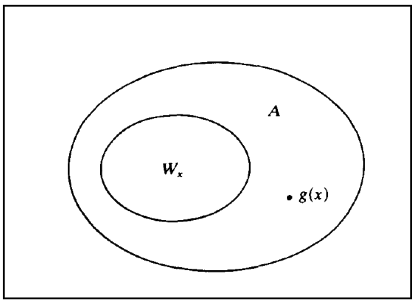

Fig. A productive set

(c) **Reduction Theorem**. Suppose that A and B are sets such that A is productive, and there is a total computable function such that $x \in A$ iff $f(x) \in B$. Then B is productive.

(d) **Theorem**. Suppose that $\mathscr{B}$ is a set of unary computable functions with $f_\varnothing \in \mathscr{B}$ and $\mathscr{B} \neq \mathscr{C}_1$. Then the set $B = \{x \mid \phi_x \in \mathscr{B}\}$ is productive.

4. Creative sets:

(a) **Definition**. A set A is creative if it is r.e. and its complement $\overline{A}$ is productive.
Example. K is creative. (The simplest example of a creative set).
Notation. From the theorem that A is recursive $\Leftrightarrow$ A and $\overline{A}$ are r.e. we can say that a creative set is an r.e. set that fails to be recursive in a very strong way. (Creative sets are r.e. sets having the most difficult decision problem.)

(b) **Theorem**. Suppose that $\mathscr{A} \subseteq \mathscr{C}_1$ and let $A = \{x \mid \phi_x \in \mathscr{A}\}$. If A is r.e. and $A \neq \emptyset$, $\mathbb{N}$, then A is creative.

(c) **Lemma**. Suppose that g is a total computable function. Then there is a total computable function k such that for all x, $W_{k(x)} = W_x \cup \{g(x)\}$.
Subset Theorem. A productive set contains an infinite r.e. subset.
Corollary. If A is creative, then $\overline{A}$ contains an infinite r.e. subset.

5. Simple Set:

(a) **Definition**. A set A is simple if A is r.e.,$\overline{A}$ is infinite and contains no infinite r.e. subset.

(b) **Theorem**. A simple set is neither recursive nor creative.

(c) **Theorem**. There is a simple set.

Key Terms:

Recursive Set, Recursively Enumerable Set, Productive Set, Creative Set, Simple Set.

Practice and Sources:

1. Slide09-RESet
2. Textbook page 121-142;
3. Lab08,Lab09.

Table 1: Various Sets

Set	Definition	Theorem	Example	Counter Example
Recursive Set	$c_A(x) = \begin{cases} 1, & \text{if } x \in A, \\ 0, & \text{if } x \notin A. \end{cases}$ is computable.	① Recursive Function Theorems ② Closure: A,B are r. $\Rightarrow$ $\overline{A}$, $A \cup B$, $A \cap B$ are r. ③ Rice Theorem: $\varnothing \subsetneq \mathscr{B} \subsetneq \mathscr{C}_1 \Rightarrow$ '$\phi_x \in \mathscr{B}$' is undecidable. ④ Any Theorems for Decidable Predicates.	$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{E}$, $\mathbb{O}$, $\mathbb{P}$ Any finite set	K, $\overline{K}$; Fin, Inf, Cof; Rec, Tot, Ext Any non-r.e. set
Recursively Enumerable Set (r.e. set)	$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A, \\ \uparrow, & \text{if } x \notin A. \end{cases}$ is computable.	① Index $\leftrightarrow$ ② Listing $\begin{cases} \text{③ Equvilence} \\ \exists \text{ infinite } r. \subseteq r.e. \\ r. \Leftrightarrow \exists f \in \mathscr{C}_1 \upuparrows, Ran(f) \end{cases}$ ④ Normal Form $\begin{cases} \text{⑤ Uniformization} \\ \text{⑥ Graph} \\ \text{⑦ Quantifier Constraction} \end{cases}$ ⑧ Complementation (A is $r.$ $\Leftrightarrow$ A, $\overline{A}$ are r.e.) ⑨ Closure (A,B are r.e. $\Rightarrow$ $A \cap B$, $A \cup B$ are r.e.) ⑩ Rice-Shapiro: $\mathscr{A} \subseteq \mathscr{C}_1$, $\{x \mid \phi_x \in \mathscr{A}\}$ is r.e., then $\forall f \in \mathscr{C}_1$, $f \in \mathscr{A} \Leftrightarrow \exists$ finite $\theta \subseteq f$ with $\theta \in \mathscr{A}$	all recursive set non-recursive r.e. set $\{x \mid x \in W_x\}$ $\{x \mid \phi_x(x) = 0\}$ $\{x \mid W_x \neq \varnothing\}$ $\{x \mid x\ 7's \text{ in } \pi\}$	$\overline{K}$; Fin, Inf, Cof; Tot, $\overline{Tot}$, Con; Rec, Ext
Productive Set	A is productive if $\exists$ total $g \in \mathscr{C}_1$ s.t. $\forall\ W_x \subseteq A$, $g(x) \in A \setminus W_x$	① Reduction Theorem A is productive and $A \leq_m B \Rightarrow B$ is productive ② Quasi-Rice Theorem $\mathscr{B} \subsetneq \mathscr{C}_1$, $f_\varnothing \in \mathscr{B} \Rightarrow \{x \mid \phi_x \in \mathscr{B}\}$ is productive ③ Quasi-Listing Theorem Productive set has r.e. subset	$\{x \mid \phi_x(x) \neq 0\}$ $\{x \mid c \notin W_x\}$ $\{x \mid c \notin E_x\}$ $\{x \mid \phi_x \text{ is not total}\}$	① r.e. set ② doesn't have r.e. subset
Creative Set	$\begin{cases} A \text{ is r.e.;} \\ \overline{A} \text{ is productive.} \end{cases}$	① Quasi-Rice Theorem $\mathscr{A} \subseteq \mathscr{C}_1$, $A = \{x \mid \phi_x \in \mathscr{A}\}$. If A is r.e., $A \neq \varnothing$, $\mathbb{N}$, then A is creative	$\{x \mid \phi_x(x) = 0\}$ $\{x \mid c \in W_x\}$ $\{x \mid c \in E_x\}$	① non-r.e. set ② simple set
Simple Set	$\begin{cases} A \text{ is r.e.;} \\ \overline{A} \text{ is infinite;} \\ \overline{A} \text{ contains no infinite} \\ \text{r.e. subset.} \end{cases}$	① Characteristic Theorem (A simple set is neither recursive nor creative) ② Existence Theorem (There is a simple set)	If A, B are simple: $A \oplus B$ is simple $A \otimes B$ is not simple $\overline{\overline{A} \otimes \overline{B}}$ is simple	Any recursive set Any creative set

Chapter 8. Arithmetic And Gödel's Incompleteness Theorem

1. Formal arithmetic:
   (a) **Definition**. The formalization of arithmetic is specifying an adequate formal logical language L and making statements of ordinary arithmetic of the natural numbers (First order logic with equality).
   Functional symbols (alphabet): $\mathsf{0}, \mathsf{1}, +, \times, =$.
   Logical notions: $\neg$ (not); $\wedge$ (and); $\vee$ (or); $\rightarrow$ (implies); $\forall$ (for all); $\exists$ (exists).
   Variables: $\mathsf{x}, \mathsf{y}, \mathsf{z}, \ldots$.
   Other symbols: brackets (and), $\neq$, etc.
   (b) **Definition**. The statements (formulas) of L are the meaningful finite sequences of symbols from the alphabet of L.
   $\mathscr{S}$ be the set of all possible meaningful statements.
   $\mathscr{T}$ be the set of all statements that are true in the ordinary arithmetic on $\mathbb{N}$.
   $\mathscr{F}$ be the set of all statements that are false in the ordinary arithmetic on $\mathbb{N}$.
   (c) Standard coding: It is straightforward to assign a Gödel number to every member of $\mathscr{S}$ in a uniform manner. $\mathscr{S} = \{\theta_0, \theta_1, \theta_2, \ldots\}$. We can use it to code any set of statements $\mathscr{X}$ by the set of number $\mathbf{X} = \{n \mid \theta_n \in \mathscr{X}\}$.
   We say that $\mathscr{X}$ is $\left\{\begin{array}{l} \textit{recursive} \\ \textit{r.e.} \\ \textit{productive} \\ \textit{creative} \\ \textit{etc.} \end{array}\right\}$ if $\mathscr{X}$ is $\left\{\begin{array}{l} \text{recursive} \\ \text{r.e.} \\ \text{productive} \\ \text{creative} \\ \text{etc.} \end{array}\right\}$
   (d) **Gödel's Lemma**. Suppose $M(x_1, \ldots, x_n)$ is a decidable predicate. Then it is possible to construct a statement $\sigma(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ that is a formal counterpart of $M(x_1, \ldots, x_n)$ in the following sense: for all $\mathsf{a}_1, \ldots, \mathsf{a}_n \in \mathbb{N}$, $M(\mathsf{a}_1, \ldots, \mathsf{a}_n)$ holds iff $\sigma(\mathsf{a}_1, \ldots, \mathsf{a}_n) \in \mathscr{T}$.
   Lemma. Foe any $n \in \mathbb{N}$,
   (a) $n \in K$ iff $n \in K \in \mathscr{T}$,
   (b)$n \notin K$ iff $n \notin K \in \mathscr{T}$
   (e) **Transform Lemma**. There is a total computable function g such that $\forall n$, $\theta_{g(n)}$ is $\mathsf{n} \notin \mathsf{K}$.
   (f) **Theorem**. $\mathscr{T}$ is productive.
2. Incompleteness:
   (a) **Definition**. A formal system $(\mathscr{A}, \mathscr{D})$ consists of a set $\mathscr{A} \subseteq \mathscr{S}$ (the axioms) and an explicit definition $\mathscr{D}$ of the notion of a formal proof of a statement in $\mathscr{S}$ from the axioms, satisfying the conditions:
      i. Proofs are finite objects.
      ii. Provability is decidable if $\mathscr{A}$ is recursive.
   (b) Is there a simple-minded subset of $\mathscr{T}$ (a set of axioms) from which all other statements in $\mathscr{T}$ can be proved? $\Longleftrightarrow$ Is there a formal system $(\mathscr{A}, \mathscr{D})$ for L such that
      i. $\mathscr{A}$ is recursive, and
      ii. the provable statements are precisely those in $\mathscr{T}$?
   (c) **Definition**. Consistency: There is no statement σ such that both σ and $\neg\sigma$ are provable; Completeness: For any statement σ, either σ is provable or $\neg\sigma$ is provable.
   (d) **Lemma**. In any recursively axiomatized formal system Pr (provable statements) is r.e.
   (e) **Simplified Gödel Theorem**. Suppose that $(\mathscr{A}, \mathscr{D})$ is a recursively axiomatized formal system in which all provable statements are true. Then there is a statement σ that is true but not provable (and consequently $\neg\sigma$ is not provable either).
3. Gödel's incompleteness theorem:
   (a) First Order Peano Axioms:

PA1	$\forall x.(\mathsf{s}(x) \neq 0)$
PA2	$\forall xy.(\mathsf{s}(x) = \mathsf{s}(y) \Rightarrow x = y)$
PA3	$\forall x.(x = 0 \vee \exists y.\mathsf{s}(y) = x)$
PA4	$\forall x.(x < \mathsf{s}(x))$
PA5	$\forall xy.(x < y \Rightarrow \mathsf{s}(x) \leq y)$
PA6	$\forall xy.(\neg(x < y) \Leftrightarrow y \leq x)$
PA7	$\forall xy.((x < y) \wedge (y < z) \Rightarrow x < z)$

(b) **Lemma**. (Gödel) Let $M(x_1, \ldots, x_n)$ be a decidable predicate, then there is a statement $\sigma(\mathsf{x}_1, \ldots, \mathsf{x}_n)$ in Peano arithmetic that satisfies the following properties: for any $a_1, \cdots, a_n \in \mathbb{N}$,

  i. If $M(a_1, \ldots, a_n)$ holds, then $\sigma(\mathsf{a}_1, \ldots, \mathsf{a}_n)$ is provable.
  ii. If $M(a_1, \ldots, a_n)$ does not hold, then $\neg\sigma(\mathsf{a}_1, \ldots, \mathsf{a}_n)$ is provable.

  Corollary. For any $n \in \mathscr{N}$, if $n \in K$ then $\mathsf{n} \in \mathsf{K}$ is provable in Peano arithmetic.

(c) **Definition**. A formal system is ω-consistent if there is no statement $\tau(\mathsf{y})$ such that all of the following are provable. $\exists \mathsf{y}.\tau(\mathsf{y}), \neg\tau(0), \neg\tau(1), \neg\tau(2), \ldots$

  Lemma. Suppose that Peano arithmetic is ω-consistent. Then for any natural number n, if $\mathsf{n} \in \mathsf{K}$ is provable then $n \in K$.

(d) **Theorem** (Gödel's Incompleteness Theorem, 1931).
  There is a statement σ of Peano arithmetic such that

  i. If Peano arithmetic is consistent, then σ is not provable;
  ii. If Peano arithmetic is ω-consistent, then $\neg\sigma$ is not provable

4. Rosser's Refinement:
   (a) **Definition**. Let $K_0 = \{x \mid \phi_x(x) = 0\}$ and $K_1 = \{x \mid \phi_x(x) = 1\}$.
   Definition. Two disjoint sets A, B are recursively inseparable if there is no recursive set C such that $A \subseteq C$ and $B \subseteq \overline{C}$.
   Proposition. Two disjoint sets A, B are recursively inseparable iff whenever $A \subseteq W_a$, $B \subseteq W_b$ and $W_a \cap W_b = \emptyset$ then there is a number $x \notin W_a \cup W_b$.
   Fact. K_0 and K_1 are recursively inseparable.
   (b) **Lemma**. For each natural number n, the following are valid in Peano arithmetic.
   i. If $n \in K_0$ then $\mathsf{n} \in \mathsf{K}_0$ is provable.
   ii. If $n \in K_1$ then $\mathsf{n} \in \mathsf{K}_1$ is provable.
   iii. If $\mathsf{n} \in \mathsf{K}_1$ is provable, then $\mathsf{n} \notin \mathsf{K}_0$ is also provable.
   (c) **Theorem**. (Gödel-Rosser Incompleteness Theorem) There is a statement τ such that if Peano arithmetic is consistent, then neither τ nor $\neg\tau$ is provable.
5. Undecidability:
   (a) **Theorem**. Suppose that $(\mathscr{A}, \mathscr{D})$ is an ω-consistent formal system of arithmetic in which all decidable predicates are representative. Then the set of provable statements is creative.
   (b) **Corollary**. If Peano arithmetic is ω-consistent, then the provable statements form a creative set.

Key Terms:

Formal Arithmetic, Gödel's Incompleteness Theorem, Rosser's Refinement, Undecidability.

Practice and Sources:

1. Slide12-Incompleteness;
2. Textbook page 143-156;
3. Lab12.

Chapter 9. Reducibility And Degrees

1. Many-One Reducibility:
   (a) **Definition**. The set A is many-one reducible (m-reducible) to the set B if there is a total computable function f such that $x \in A$ iff $f(x) \in B$ for all x.
   We shall write $A \leq_m B$ or more explicitly $f : A \leq_m B$.
   Notation. If f is injective, then we are talking about one-one reducibility, denoted by $f : A \leq_1 B$.
   (b) **Theorem**. Let A, B, C be sets.
      i. $\leq_m$ is reflexive: $A \leq_m A$.
      ii. $\leq_m$ is transitive: $A \leq_m B$, $B \leq_m C \Rightarrow A \leq_m C$.
      iii. $A \leq_m B$ iff $\overline{A} \leq_m \overline{B}$.
      iv. If A is recursive and $B \leq_m A$, then B is recursive.
      v. If A is recursive and $B \neq \varnothing, \mathbb{N}$, then $A \leq_m B$.
      vi. If A is r.e. and $B \leq_m A$, then B is r.e.
      vii. (i). $A \leq_m \mathbb{N}$ iff $A = \mathbb{N}$; (ii). $A \leq_m \varnothing$ iff $A = \varnothing$.
      viii. (i). $\mathbb{N} \leq_m A$ iff $A \neq \varnothing$; (ii). $\varnothing \leq_m A$ iff $A \neq \mathbb{N}$.
   (c) **Corollary**. Neither $\{x \mid \phi_x \text{ is total}\}$ nor $\{x \mid \phi_x \text{ is not total}\}$ is m-reducible to K.
   Corollary. If A is r.e. and is not recursive, then $\overline{A} \not\leq_m A$ and $A \not\leq_m \overline{A}$.
   Notation. It contradicts to our intuition that A and $\overline{A}$ are equally difficult.
   (d) **Theorem**. A is r.e. iff $A \leq_m K$.
   Notation. K is the most difficult partially decidable problem.
2. m-Degrees:
   (a) **Definition**. Two sets A, B are many-one equivalent, notation $A \equiv_m B$ (abbreviated m-equivalent), if $A \leq_m B$ and $B \leq_m A$.
   (b) **Theorem**. The relation $\equiv_m$ is an equivalence relation.
   (c) **Definition**. Let $d_m(A)$ be $\{B \mid A \equiv_m B\}$.
   Definition. An m-degree is an equivalence class of sets under the relation $\equiv_m$. It is any class of sets of the form $d_m(A)$ for some set A.
   (d) **Definition**. The set of m-degrees is ranged over by $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$.
   Definition. (Partial Order on m-Degree) Let $\mathbf{a}$, $\mathbf{b}$ be m-degrees.
      i. $\mathbf{a} \leq_m \mathbf{b}$ iff $A \leq_m B$ for some $A \in \mathbf{a}$ and $B \in \mathbf{b}$.
      ii. $\mathbf{a} <_m \mathbf{b}$ iff $\mathbf{a} \leq_m \mathbf{b}$ and $\mathbf{b} \not\leq_m \mathbf{a}$ ($\mathbf{a} \neq \mathbf{b}$).
   The relation $\leq_m$ is a partial order.
   Notation. From the definition of $\equiv_m$, $\mathbf{a} \leq_m \mathbf{b} \Leftrightarrow \forall A \in \mathbf{a}, B \in \mathbf{b}, A \leq_m B$.
   (e) **Theorem**. The relation $<_m$ is a partial ordering of m-degrees.
   (f) **Theorem**. Difficulty Class
      i. $\mathbf{o}$ and $\mathbf{n}$ are respectively the recursive m-degrees $\{\varnothing\}$ and $\{\mathbb{N}\}$.
      ii. The recursive m-degree $\mathbf{0}_m$ consists of all the recursive sets except $\varnothing, \mathbb{N}$. $\mathbf{0}_m \leq_m \mathbf{a}$ for any m-degree $\mathbf{a}$ other than $\mathbf{o}$, $\mathbf{n}$.
      iii. $\forall$ m-degree $\mathbf{a}$, $\mathbf{o} \leq_m \mathbf{a}$ provided $\mathbf{a} \neq \mathbf{n}$; $\mathbf{n} \leq_m \mathbf{a}$ provided $\mathbf{a} \neq \mathbf{o}$.
      iv. An r.e. m-degree consists of only r.e. sets.
      v. If $\mathbf{a} \leq_m \mathbf{b}$ and $\mathbf{b}$ is an r.e. m-degree, then $\mathbf{a}$ is also an r.e. m-degree.
      vi. The maximum r.e. m-degree $d_m(K)$ is denoted by $\mathbf{0}'_m$.
   (g) Algebraic Structure
      i. **Theorem**. m-degrees form an upper semi-lattice.
      ii. Lattice: A lattice is a partially ordered set (poset) $(L, \leq)$ in which any two elements have a unique supremum (also called a least upper bound or join) and a unique infimum (also called a greatest lower bound or meet).

To qualify as a lattice, the set and the operation must satisfy tow conditions: join-semilattice, meet-semilattice.
join-semilattice: $\forall a, b \in L$, $\{a, b\}$ has a join $a \vee b$. (the least upper bound)
meet-semilattice: $\forall a, b \in L$, $\{a, b\}$ has a meet $a \wedge b$. (the greatest lower bound)

iii. **Theorem**. Any pair of m-degrees $\mathbf{a}$, $\mathbf{b}$ have a least upper bound; i.e. there is an m-degree $\mathbf{c}$ such that
   A. $\mathbf{a} \leq_m \mathbf{c}$ and $\mathbf{b} \leq_m \mathbf{c}$ ($\mathbf{c}$ is an upper bound);
   B. $\mathbf{c} \leq_m$ any other upper bound of $\mathbf{a}$, $\mathbf{b}$.

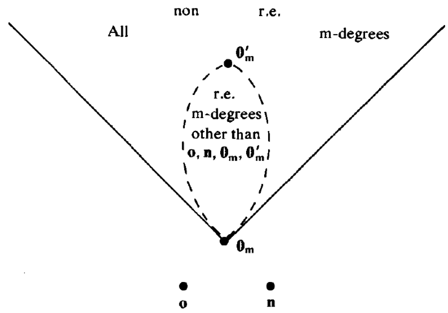

Fig. The m-degrees

3. m-complete r.e. sets:
   (a) **Definition**. An r.e. set is m-complete if every r.e. set is m-reducible to it.
   Notation. $\mathbf{0}'_m$, the m-degree of K is maximum among all r.e. m-degrees, and thus K is m-complete r.e. set (or just called m-complete set).
   (b) **Theorem**. The following statements are valid.
      i. K is m-complete.
      ii. A is m-complete iff $A \equiv_m K$ iff A is r.e. and $K \leq_m A$.
      iii. $0'_m$ consists exactly of all the m-complete sets.
   (c) **Myhill's Theorem**. A set is m-complete iff it is creative.
   Corollary. If $\mathbf{a}$ is the m-degree of any simple set, then $\mathbf{0}_m <_m \mathbf{a} <_m \mathbf{0}'_m$ (Simple sets are not m-complete).
4. Relative Computability:
   (a) Unlimited Register Machine with Oracle (URMO):
      i. **Definition**. Suppose χ is a total unary function.
      Informally a function f is computable relative to χ, or χ-computable, if f can be computed by an algorithm that is effective in the usual sense, except from time to time during computations f is allowed to consult the oracle function χ.
      Such an algorithm is called a χ-algorithm.
      ii. **Definition**. A URM with oracle, URMO for short, can recognize a fifth kind of instruction,$O(n)$, for every $n \geq 1$.
      If χ is the oracle, then the effect of $O(n)$ is to replace the content r_n of R_n by $\chi(r_n)$.
      P^χ denote the program P when used with the function χ in the oracle.
      $P^\chi(\mathbf{a}) \downarrow b$ means the computation $P^\chi(\mathbf{a})$ with initial configuration $a_1, a_2, \cdots, a_n, 0, 0, \cdots$ stops with the number b is register R_1.
      iii. **Definition**. Let χ be a unary total function, and f a partial function from $\mathbb{N}^n$ to $\mathbb{N}$.
         A. Let P be a URMO program, then P URMO-computes f relative to χ (or f is χ-computed by P) if, for every $\mathbf{a} \in \mathbb{N}^n$ and $b \in \mathbb{N}$, $P^\chi(\mathbf{a}) \downarrow b$ iff $f(\mathbf{a}) \simeq b$.
         B. The function f is URMO-computable relative to χ (or χ-computable) if there is a URMO program that URMO-computes it relative to χ.
      iv. **Theorem**.
         A. $\chi \in \mathscr{C}^\chi$.
         B. $\mathscr{C} \subseteq \mathscr{C}^\chi$.
         C. If χ is computable, then $\mathscr{C} = \mathscr{C}^\chi$.
         D. $\mathscr{C}^\chi$ is closed under substitution, recursion and minimalisation.
         E. If ψ is a total unary function that is χ-computable, then $\mathscr{C}^\psi \subseteq \mathscr{C}^\chi$.
   (b) χ-partial recursive function:

i. **Definition**. The class $\mathscr{R}^\chi$ of χ-partial recursive functions is the smallest class of functions such that

A. the basic functions are in $\mathscr{R}^\chi$.

B. $\chi \in \mathscr{R}^\chi$.

C. $\mathscr{R}^\chi$ is closed under substitution, recursion, and minimalisation.

ii. **Theorem**. For any χ, $\mathscr{R}^\chi = \mathscr{C}^\chi$.

(c) Numbering URMO programs

i. Let's fix an effective enumeration of all URMO programs: $Q_0, Q_1, Q_2, \ldots$. Let $\phi_m^{\chi,n}$ be the n-ary function χ-computed by Q_m.
ϕ_m^χ is $\phi_m^{\chi,1}$. $W_m^\chi = Dom(\phi_m^\chi)$ and $E_m^\chi = Ran(\phi_m^\chi)$.

ii. **The relativised s-m-n Theorem**. For each $m, n \geq 1$ there is a total computable $(m+1)$-ary function $s_n^m(e, \mathbf{x})$ such that for any χ, $\phi_e^{\chi,m+n}(\mathbf{x}, \mathbf{y}) \simeq \phi_{s_n^m(e,\mathbf{x})}^{\chi,n}(\mathbf{y})$.

(d) Universal programs for relative computability:
Universal Function Theorem. For each n, the universal function $\psi_U^{\chi,n}$ for n-ary χ-computable functions given by $\psi_U^{\chi,n}(e, \mathbf{x}) \simeq \phi_e^{\chi,n}(\mathbf{x})$ is χ-computable.

(e) χ-recursive and χ-r.e. sets :

i. **Definition**. Let A be a set

A. A is χ-recursive if c_A is χ-computable.

B. A is χ-r.e. if its partial characteristic function $f(x) = \begin{cases} 1 & \text{if } x \in A, \\ \uparrow & \text{if } x \notin A \end{cases}$ is χ-computable.

ii. **Theorem**. The following statements are valid.

A. For any set A, A is χ-recursive iff A and $\overline{A}$ are χ-r.e.

B. For any set A, the following are equivalent.

(1) A is χ-r.e.

(2) $A = W_m^\chi$ for some m.

(3) $A = E_m^\chi$ for some m.

(4) $A = \emptyset$ or A is the range of a total χ-computable function.

(5) For some χ-decidable predicate $R(x, y)$, $x \in A$ iff $\exists y.R(x, y)$.

C. $K^\chi \stackrel{\text{def}}{=} \{x \mid x \in W_x^\chi\}$ is χ-r.e. but not χ-recursive.

(f) Computability relative to set A means relative to characteristic function c_A.

5. Turing reducibility and Turing degrees:

(a) **Definition**. The set A is Turing reducible to B, notation $A \leq_T B$, if A has a B-computable characteristic function c_A.
Definition. A, B are Turing equivalent, notation $A \equiv_T B$, if $A \leq_T B$ and $B \leq_T A$.

(b) **Theorem**.

i. $\leq_T$ is reflexive and transitive.

ii. $\equiv_T$ is an equivalence relation.

iii. If $A \leq_m B$ then $A \leq_T B$.

iv. $A \equiv_T \overline{A}$ for all A.

v. If A is recursive, then $A \leq_T B$ for all B.

vi. If B is recursive and $A \leq_T B$, then A is recursive.

vii. If A is r.e. then $A \leq_T K$.

(c) **Definition**. A set A is T-complete if A is r.e. and $B \leq_T A$ for every r.e. set B.

(d) **Definition**. T-Degree

i. The equivalence class $d_T(A) = \{B \mid A \equiv_T B\}$ is the Turing degree (T-degree) of A.

ii. A T-degree containing a recursive set is called a recursive T-degree.

iii. A T-degree containing an r.e. set is called an r.e. T-degree.

(e) **Definition**. The set of degrees is ranged over by $\mathbf{a}, \mathbf{b}, \mathbf{c}, \ldots$.
   i. $\mathbf{a} \leq \mathbf{b}$ iff $A \leq_T B$ for all $A \in \mathbf{a}$ and $B \in \mathbf{b}$.
   ii. $\mathbf{a} < \mathbf{b}$ iff $\mathbf{a} \leq \mathbf{b}$ and $\mathbf{a} \neq \mathbf{b}$.

   Notation. The relation $\leq$ is a partial order.

(f) **Theorem**.
   i. There is precisely one recursive degree $\mathbf{0}$, which consists of all the recursive sets and is the unique minimal degree.
   ii. Let $\mathbf{0}'$ be the degree of K. Then $\mathbf{0} < \mathbf{0}'$ and $\mathbf{0}'$ is a maximum among all r.e. degrees.
   iii. $d_m(A) \subseteq d_T(A)$; and if $d_m(A) \leq_m d_m(B)$ then $d_T(A) \leq d_T(B)$.

(g) **Theorem**. The jump operation:
   i. $K^A \stackrel{\text{def}}{=} \{x \mid x \in W_x^A\}$. K^A is a T-complete A-r.e. set. Also called the completion of A, or the jump of A, and denoted as A'. $A <_T K^A$.
   ii. If B is A-r.e., then $B \leq_T K^A$.
   iii. If A is recursive then $K^A \equiv_T K$.
   iv. If $A \leq_T B$ then $K^A \leq_T K^B$.
   v. If $A \equiv_T B$ then $K^A \equiv_T K^B$.

(h) **Definition**. The jump of $\mathbf{a}$, denoted $\mathbf{a}'$, is the degree of K^A for any $A \in \mathbf{a}$.

   Notation. By Relativization jump is a valid definition because the degree of K^A is the same for every $A \in \mathbf{a}$. The new definition of $\mathbf{0}'$ as the jump of $\mathbf{0}$ accords with our earlier definition of $0'$ as the degree of K.

(i) **Theorem**. For any degree $\mathbf{a}$ and $\mathbf{b}$, the following statements are valid.
   i. $\mathbf{a} < \mathbf{a}'$.
   ii. If $\mathbf{a} < \mathbf{b}$ then $\mathbf{a}' < \mathbf{b}'$
   iii. If $B \in \mathbf{b}$, $A \in \mathbf{a}$ and B is A-r.e. then $\mathbf{b} \leq \mathbf{a}'$.

(j) **Theorem**. Any degrees $\mathbf{a}, \mathbf{b}$ have a unique least upper bound.

(k) **Theorem**. Any non-recursive r.e. degree contains a simple set.

(l) **Theorem**. There are r.e. sets A, B s.t. $A \not\leq_T B$ and $B \not\leq_T A$. Hence, if $\mathbf{a}$, $\mathbf{b}$ are $d_T(A)$, $d_T(B)$ respectively, $\mathbf{a} \not\leq \mathbf{b}$ and $\mathbf{b} \not\leq \mathbf{a}$, and thus $\mathbf{0} < \mathbf{a} < \mathbf{0}'$ and $\mathbf{0} < \mathbf{b} < \mathbf{0}'$.

(m) **Theorem**. For any r.e. degree $\mathbf{a} > \mathbf{0}$, there is an r.e. degree $\mathbf{b}$ such that $\mathbf{b} \mid \mathbf{a}$.

(n) **Sack's Density Theorem**. For any r.e. degrees $\mathbf{a} < \mathbf{b}$, $\exists$ r.e. degree $\mathbf{c}$ with $\mathbf{a} < \mathbf{c} < \mathbf{b}$.

(o) **Sack's Splitting Theorem**. For any r.e. degrees $\mathbf{a} > \mathbf{0}$ there are r.e. degrees $\mathbf{b}$, $\mathbf{c}$ such that $\mathbf{b} < \mathbf{a}$ $\mathbf{c} < \mathbf{a}$ and $\mathbf{a} = \mathbf{b} \cup \mathbf{c}$ (hence $\mathbf{b} \mid \mathbf{c}$).

(p) **Lachlan, Yates Theorem**.
   i. $\exists$ r.e. degrees $\mathbf{a}$, $\mathbf{b} > \mathbf{0}$ such that $\mathbf{0}$ is the greatest lower bound of $\mathbf{a}$ and $\mathbf{b}$.
   ii. $\exists$ r.e. degrees $\mathbf{a}$, $\mathbf{b}$ having no greatest lower bound (either among all degrees or among r.e. degrees).

(q) **Shoenfield Theorem**. There is a non-r.e. degree $\mathbf{a} < \mathbf{0}'$.

(r) **Spector Theorem**. There is a minimal degree. (A minimal degree is a degree $\mathbf{m} > \mathbf{0}$ such that there is no degree $\mathbf{a}$ with $\mathbf{0} < \mathbf{a} < \mathbf{m}$).

(s) **Corollary**. For any r.e. m-degree $\mathbf{a} >_m \mathbf{0_m}$, $\exists$ an r.e. m-degree $\mathbf{b}$ s.t. $\mathbf{b} \mid \mathbf{a}$.

<u>Key Terms:</u>

Many-one Reducibility, Many-one Equivalent, m-degrees, m-complete, Relative Computability, URMO, χ-computable, Turing Reducibility, Turing Degrees.

<u>Practice and Sources:</u>

1. Slide10-Reducibility; Slide11-NPReduction
2. Textbook page 157-181;
3. Lab10, Lab11

Chapter 10-11. Effective Operators and Recursion Theorems

1. **Function Operator**: An operator $\Phi : \mathscr{F}_m \to \mathscr{F}_n$ is a total function.
   (a) **Effectiveness**: the conversion can be effectively calculated in a finite time using a finite part of the input function f.
   (b) Check finite subfunction $\theta \subseteq f$. (A function θ is finite if its domain of definition is finite)
2. **Continuity and Monotonicity**: Let $\Phi : \mathscr{F}_m \to \mathscr{F}_n$ be an operator.
   (a) Φ is continuous if for any $f \in \mathscr{F}_m$ and all $\mathbf{x}, y$, $\Phi(f)(\mathbf{x}) \simeq y$ iff $\exists \theta \subseteq f.\Phi(\theta)(\mathbf{x}) \simeq y$.
   (b) Φ is monotone if $\Phi(f) \subseteq \Phi(g)$ whenever $f \subseteq g \in \mathscr{F}_m$.
3. **Lemma.** If Φ is continuous, then it is monotone.
4. **Definition.** $\Phi : \mathscr{F}_m \to \mathscr{F}_n$ is a recursive operator if there is a computable function $\phi(z, \mathbf{x})$ such that for all $f \in \mathscr{F}_m$ and $\mathbf{x} \in \mathbb{N}^n$, $y \in \mathbb{N}$, $\Phi(f)(\mathbf{x}) \simeq y$ iff $\exists \theta \subseteq f.\phi(\widetilde{\theta}, \mathbf{x}) \simeq y$.
5. **Theorem.** All recursive operators are continuous.
6. **Theorem.** Let $\Phi : \mathscr{F}_m \to \mathscr{F}_n$ be an operator. Then Φ is a recursive operator iff
   (a) Φ is continuous;
   (b) Function $\varphi(z, \mathbf{x}) = \begin{cases} \Phi(\theta)(\mathbf{x}), & \text{if } z = \widetilde{\theta} \text{ for some } \theta \in \mathscr{F}_m, \\ \uparrow, & \text{otherwise.} \end{cases}$ is computable.
7. **Corollary.** Suppose $\Phi : \mathscr{F}_m \to \mathscr{F}_n$ is a recursive operator with the computable function ϕ. Then $\Phi(\theta)(\mathbf{x}) \simeq y$ iff $\phi(\widetilde{\theta}, \mathbf{x}) \simeq y$.
8. **Extensional**. A total $h \in \mathscr{C}_1$ is extensional if, for all a, b, $\phi_{h(a)} = \phi_{h(b)}$ whenever $\phi_a = \phi_b$.
9. **Theorem (Myhill-Shepherdson, Part I).** Suppose that $\Psi : \mathscr{F}_m \to \mathscr{F}_n$ is a recursive operator. Then there is a total extensional computable function h such that $\Psi(\phi_e^{(m)}) = \phi_{h(e)}^{(n)}$.
10. **Theorem (Myhill-Shepherdson, Part II).** Suppose that h is a total extensional computable function. Then there is a unique recursive operator Ψ such that $\Psi(\phi_e^{(m)}) = \phi_{h(e)}^{(n)}$.
11. **The First Recursion Theorem.** Suppose that $\Phi : \mathscr{F}_m \to \mathscr{F}_m$ is a recursive operator. Then there is a computable function f_Φ that is the least fix point of Φ, i.e.
    - $\Phi(f_\Phi) = f_\Phi$;
    - if $\Phi(g) = g$, then $f_\Phi \subseteq g$.
12. **The Second Recursion Theorem.** Let f be a total unary computable function. Then there is a number n such that $\phi_{f(n)} = \phi_n$.
    (a) **Corollary.** If f is a total computable function, then there is a number n such that $W_{f(n)} = W_n$ and $E_{f(n)} = E_n$.
    (b) **Corollary.** If f is a total computable function, then there are arbitrarily large numbers n such that $\phi_{f(n)} = \phi_n$.
    (c) **Corollary.** Let $f(x, y)$ be a computable function, then there is an index e such that $\phi_e(y) \simeq f(e, y)$.
    (d) **Corollary.** There is a program P such that for all x, $P(x) \downarrow \gamma(P)$.
13. **Theorem.** K is not recursive.
14. **Rice Theorem.** Suppose $\emptyset \subsetneq \mathscr{A} \subsetneq \mathscr{C}_1$ and $A = \{x \mid \phi_x \in \mathscr{A}\}$. Then A is not recursive.
15. **Generalize Second Recursive Theorem**. If $f(x, z)$ is a total computable function. there is a total computable function $n(z)$ such that for all z, $\phi_{f(n(z),z)} = \phi_{n(z)}$. (diagonal argument)

Key Terms:

Operator, Finite Operator, Continuous Operator, Second Order Computable Function, Myhill-Shepherdson Theorem, The First/Second Recursion Theorem; Generalization of Diagonal Argument

Practice and Sources:

1. Slide-13
2. Textbook page 182-199 (except sec 4)

NP, NP-Complete and NP Reduction

1. **Decision Problem**: The "Yes" or "No" questions for any input instance.
   (a) For *maximization* problem: add a threshold k and determine whether there exists a solution with size/weight/measure $\geq k$.
   (b) For *minimization* problem: add a threshold k and determine whether there exists a solution with size/weight/measure $\leq k$.
2. **Polynomial Time Algorithm**: Algorithm A runs in poly-time if for every string s, $A(s)$ terminates in at most $p(|s|)$ "steps", where $p(.)$ is some polynomial.
3. **P** Problem: Decision problems for which there is a poly-time algorithm.
4. **NP** Problem: Decision problems for which there exists a poly-time certifier.
   (a) Certifier: a polynomial time algorithm to check whether a given string is a solution.
   (b) Certificate: a solution for a given instance.
5. **NP**-Completeness: a set of the hardest **NP** problems.
   (a) P is **NP**-Complete if i) $P \in \mathbf{NP}$; and ii) $\forall Q \in \mathbf{NP}$, $Q \leq_m^p P$.
   (b) P is **NP**-Hard if $\forall Q \in \mathbf{NP}$, $Q \leq_m^p P$.
6. **Polynomial Time Reduction**:
   (a) Cook Reduction: Problem X polynomial reduces (Cook) to problem Y if arbitrary instances of problem X can be solved using polynomial number of standard computational steps, plus polynomial number of calls to oracle that solves problem Y.
   (b) Karp Reduction: Problem X polynomial transforms (Karp) to problem Y if given any input $x \in X$, we can construct an input y such that x is a yes instance of X iff y is a yes instance of Y. Here we require $|y|$ to be of size polynomial in $|x|$. (Polynomial transformation is polynomial reduction with just one call to oracle for Y, exactly at the end of the algorithm for X.)

Key Terms:

Polynomial-time Reduction, P, NP, NP-Complete, NP-Hard, Certificate, Certifier, Decision Problem

Practice and Sources:

1. Slide11-NPReduction
2. Lab-11