THEORY OF COMPUTATION
Preliminaries - 1

Prof. Dan A. Simovici

UMB

These slides follow loosely the reference “Computability, Complexity and Languages” by M. D. Davis, R. Sigal, and E. Weyuker, published by Academic Press.

The main themes of this course are:

- the formalization of the notion of computable function;
- the study of important classes of computable function;
- the limits of the computability.

Basic notations

- The set of natural numbers is

$$\mathbb{N} = \{0, 1, \ldots, n, \ldots\}.$$

- $a \in S$ means that a is an element of a set S.
- If R and S the equality $R = S$ is equivalent with the inclusions $R \subseteq S$ and $S \subseteq R$.

Note that $\emptyset \subseteq S$ and $S \subseteq S$, where $\emptyset$ is the emptyset, and S is an arbitrary set.

Set-Theoretical Operations

Let R, S be two sets.

Definition

- The union of R and S is the set $R \cup S$ of all x that belong to R or to S.
- The intersection of R and S is the set $R \cap S$ of all x that belong to both R and S.
- The difference of R and S is the set $R - S$ of all x that belong to R but not to S.

Complements of Sets

In certain context we work with sets that are all subsets of a set D. If S is such a subset, the set $D - S$ is the *complement* of S and is denoted as $\overline{S}$.
We have De Morgan Laws:

$$\begin{aligned} \overline{R \cup S} &= \overline{R} \cap \overline{S}, \\ \overline{R \cap S} &= \overline{R} \cup \overline{S}. \end{aligned}$$

Finite Sets

A set consisting of $a_1, \ldots, a_n$ is denoted as $S = \{a_1, \ldots, a_n\}$. Sets that can be written in this manner, or the empty set, are said to be *finite* and we write $n = |S|$.

- Sets that are not finite are said to be *infinite*.
- Note the difference between a singleton $\{x\}$ and an element x.
- We can write either $x \in S$, or $\{x\} \subseteq S$.

Definition

A set S is *finite* only if it can be written as

$$S = \{x_1, \ldots, x_n\}.$$

Sets that are not finite (e.g. $\mathbb{N}$, the set of natural numbers) are said to be *infinite*.

Note that a and $\{a\}$ are different things.
In particular, $a \in S$ is true if $\{a\} \subseteq S$.
Since two sets are equal if and only if they have the same members, it follows that

$$\{a, b, c\} = \{b, a, c\} = \{c, b, a\}.$$

When the order is important we use n-tuples or *lists* written as

$$(a_1, a_2, \dots, a_n).$$

Lists may contain duplicate entries; sets may not.

Example

$\ell = (6, 1, 6, 2)$ is a list.

Note that

$$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$$

is equivalent to $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$.

The set of subsets of a set S is denoted by $\mathcal{P}(S)$.

Example

If $S = \{a, b, c\}$, the set $\mathcal{P}(S)$ consists of the sets:

$$\begin{array}{l} \emptyset, \\ \{a\}, \{b\}, \{c\}, \\ \{a, b\}, \{a, c\}, \{b, c\}, \\ \{a, b, c\}. \end{array}$$

A subset T of a finite set $S = \{x_1, \ldots, x_n\}$ can be represented as an array having n components.

Example

Let $S = \{x_1, x_2, x_3, x_4, x_5\}$ and $T = \{x_2, x_3, x_5\} \subseteq S$. The array representing T is

0	1	1	0	1
x_1	x_2	x_3	x_4	x_5

Since there are two choices (0 or 1) for each of the n entries of the array, there exists 2^n subsets of S.

Definition

A *function* is a set f whose members are ordered pairs and that has the special property

$$(a, b) \in f \text{ and } (a, c) \in f \text{ implies } b = c.$$

Intuitively, one writes $f(a) = b$ if $(a, b) \in f$.

- The set of all *a*s such that $(a, b) \in f$ for some b is called the *domain* of f.
- The set of all $f(a)$ for a in the domain of f is the *range* of f.

If A is the domain of f and B is the range of f we write

$$f : A \longrightarrow B.$$

Example

Let f the set of ordered pairs (n, n^2) for $n \in \mathbb{N}$. For each n, $f(n) = n^2$. The domain of f is $\mathbb{N}$. The range of f is the set of all perfect squares.

Definition

A *partial function* on a set S is a function whose domain is a subset of S.

Example

Let g be defined by $g(n) = \sqrt{n}$. The domain of g is the set of all perfect squares.

If f is a partial function on S and $a \in \mathrm{Dom}(f)$ we write $f(a)\downarrow$ to indicate that a is in the domain of f and we say that $f(a)$ is defined. If f is not defined on a we write $f(a)\uparrow$.

Let A and B be two finite sets such that $|A| = m$ and $|B| = n$.
How many functions exist of the form $f : A \longrightarrow B$?
To describe functions of the form $f : A \longrightarrow B$ imagine a table with m positions indexed by the elements of A:

$b_?$	$b_?$	$\cdots$	$b_?$	$b_?$
a_1	a_2	$\cdots$	a_{m-1}	a_m

For each box we have $|B|$ choices, so there are $|B|^{|A|}$ functions.

- The empty set $\emptyset$ is itself a function that is nowhere defined.
- For a partial function on a Cartesian product $S_1 \times S_2 \times \cdots \times S_n$ we write $f(a_1, \ldots, a_n)$ rather than $f((a_1, \ldots, a_n))$.
- A partial function of a set S_n is called an *n-ary partial function on S*.
- When $n = 1$ we use the term *unary function* for $f : S \longrightarrow S$; when $n = 2$ we use the term *binary function* for $f : S \times S \longrightarrow S$.

A function $f : A \longrightarrow B$ is

- *one-to-one* or an *injection* if $f(a) = f(a')$ implies $a = a'$;
- *onto* or a *surjection* if for each $b \in B$ there exists $a \in A$ such that $f(a) = b$;
- a *bijection* if it is both one-to-one and onto.

Definition

A *predicate* on a set S is a total function

$$P : S \longrightarrow \{TRUE, FALSE\},$$

where TRUE and FALSE are *truth values*.

We say that $P(a)$ is true if $P(a) = TRUE$ and $P(a)$ is false if $P(a) = FALSE$.
An alternative notation identifies TRUE with 1 and FALSE with 0, which allows us to identify predicates as function with values in the set $\{0, 1\}$.

Predicates are usually specified as by expressions that may become true or false.

Example

The expression $x < 5$ specifies a predicate P on $\mathbb{N}$ defined by

$$P(n) = \begin{cases} 1 & \text{if } x = 0, 1, 2, 3, 4, \\ 0 & \text{otherwise.} \end{cases}$$

Operations on Truth Values

Starting from two predicates P and Q on a set S define the predicates $\sim P$, $P\&Q$, and $P \vee Q$ by the following tables:

P	$\sim P$
0	1
1	0

P	Q	$P\&Q$	$P \vee Q$
1	1	1	1
0	1	0	1
1	0	0	1
0	0	0	0

- Given a predicate P on a set S there is subset R of S defined as

$$R = \{a \in S \mid P(a) = 1\}.$$

Conversely, given a subset R of S, the *characteristic function* of R is the predicate P defined by

$$P(x) = \begin{cases} 1 & \text{if } x \in R, \\ 0 & \text{if } x \notin R. \end{cases}$$

The Connection between Sets and Predicates

$$\{x \in S \mid P(x) \& Q(x)\} = \{x \in S \mid P(x)\} \cap \{x \in S \mid Q(x)\},$$
$$\{x \in S \mid P(x) \vee Q(x)\} = \{x \in S \mid P(x)\} \cup \{x \in S \mid Q(x)\},$$
$$\{x \in S \mid \sim P(x)\} = S - \{x \in S \mid P(x)\}.$$

To indicate that two expressions containing variables define the same predicate we place the symbol $\Leftrightarrow$ between them.

Example

Consider the equivalent expressions

$$x < 5 \Leftrightarrow x = 0 \vee x = 1 \vee x = 2 \vee x = 3 \vee x = 4.$$

The following equalities are known as the *De Morgan* identities:

$$P(x) \& Q(x) \quad \Leftrightarrow \quad \sim(\sim P(x) \vee \sim Q(x)),$$
$$P(x) \vee Q(x) \quad \Leftrightarrow \quad \sim(\sim P(x) \& \sim Q(x)).$$

We assume here that predicates have the form $P : \mathbb{N}^m \longrightarrow \{0, 1\}$ and, therefore we omit "on $\mathbb{N}$".

Definition

Let $P(t, x_1, \ldots, x_n)$ be an $(n + 1)$-ary predicate. The predicate $Q(y, x_1, \ldots, x_n)$ defined by

$$\begin{aligned} Q(y, x_1, \ldots, x_n) \quad = \quad & P(0, x_1, \ldots, x_n) \vee P(1, x_1, \ldots, x_n) \\ & \vee \cdots \vee P(y, x_1, \ldots, x_n) \end{aligned}$$

is true if and only if there is $t \leqslant y$ such that $P(t, x_1, \ldots, x_n)$ is true. We write Q as $(\exists t)_{\leqslant y} P(t, x_1, \ldots, x_n)$. The expression $(\exists t)_{\leqslant y}$ is called a *bounded existential quantifier*.

Definition

Let $P(t, x_1, \ldots, x_n)$ be an $(n+1)$-ary predicate. The predicate $Q(y, x_1, \ldots, x_n)$ defined by

$$\begin{aligned} Q(y, x_1, \ldots, x_n) &= P(0, x_1, \ldots, x_n) \& P(1, x_1, \ldots, x_n) \\ &\quad \& \cdots \& P(y, x_1, \ldots, x_n) \end{aligned}$$

is true if and only if for every t, $t \leqslant y$ $Q(t, x_1, \ldots, x_n)$ is true. We write Q as $(\forall t)_{\leqslant y} P(t, x_1, \ldots, x_n)$. The expression $(\forall t)_{\leqslant y}$ is called a *bounded universal quantifier*.

Example

The predicate

$$P(x, z) = (\exists y)_{\leqslant z}(x + y = 4)$$

is equivalent to the predicate

$$(x + z \geqslant 4) \& (x \leqslant 4).$$

Definition

We write

$$Q(x_1, \ldots, x_n) \Leftrightarrow (\exists t)P(t, x_1, \ldots, x_n)$$

for the predicate which is true if there exists some $t \in \mathbb{N}$ for which $P(t, x_1, \ldots, x_n)$ is true.
Similarly, $(\forall t)P(t, x_1, \ldots, x_n)$ is true if $P(t, x_1, \ldots, x_n)$ is true for all $t \in \mathbb{N}$.

Example

We have:

$$(\exists y)(x + y = 4) \Leftrightarrow x \leqslant 4$$
$$(\exists y)(x + y = 4) \Leftrightarrow (\exists y)_{\leqslant 4}(x + y = 4).$$

- An *alphabet* is a finite non-empty set of *symbols*.
- A *word* is an n-tuple of symbols $w = (a_1, a_2, \ldots, a_n)$ written as $a_1 a_2 \cdots a_n$. Here n is the *length* of w denoted by $n = |w|$.
- If $|A| = m$, there are m^n words of length n.
- There is a unique word of length 0 denoted as λ or just 0.

- The set of words over the alphabet A is denoted by A^*.
- A *language* over the alphabet A is any subset of A^*.
- We do not distinguish between the symbol a and the word a.
- If u, v are words, we write uv for the word obtained by placing v after u.

Example

If $A = \{a, b, c\}, u = bab, v = caba$, then

$$uv = babcaba \text{ and } vu = cababab.$$

We have $u0 = 0u = u$ for every $u \in A^*$.

Word product is *associative*, that is,

$$u(vw) = (uv)w$$

for $u, v, w \in A^*$.
If either $uv = uw$ or $vu = wu$, then $v = w$.

If u is a word and $n > 0$ we write

$$u^n = \underbrace{uu\cdots u}_{n}$$

and $u^0 = \lambda$.

Proof by Contradiction

Claim: the equation

$$\left(\frac{p}{q}\right)^2 = 2$$

has no solution for $p, q \in \mathbb{N}$.

Suppose that there is a solution (p, q) with $p, q \in \mathbb{N}$. Then, it has a solution in which p and q are not both even numbers (because if both p and q are even we can repeatedly cancel 2 until at least one of the numbers is odd).

If (p, q) is a solution with the property mentioned above, then $p^2 = 2q^2$, so p is even, say $p = 2k$. This implies that $q^2 = 2k^2$, so q^2 is even, so q is even. This contradicts the previous assumption (in red).

Mathematical Induction

Mathematical induction is a proof technique that allows us to prove statements of the form

$$(\forall n)P(n),$$

where P is a predicate on $\mathbb{N}$.
Variants of mathematical induction:

- simple induction;
- strong induction;
- course-of value induction,

and many others.
Recommended: *Mathematical Foundation of Computer Science by P. Fejer and D. Simovici, Springer*

Simple Induction

To prove $(\forall n)P(n)$ we need to prove:

- $P(0)$ (the basic step);
- $(\forall n)$(if $P(n)$ then $P(n+1)$) (the induction step).

This simplifies the proof because frequently is easier to show that $(\forall n)$(if $P(n)$ then $P(n+1)$ instead of proving $(\forall n)P(n)$.

Example

Let's prove that $\sum_{i=1}^{n}(2i+1) = (n+1)^2$ for all $n \in \mathbb{N}$.

- The basic step: for $n = 0$ the statement amounts to $1 = 1^2$, which is clearly true.
- The induction step: Suppose the statement holds for k, that is, $\sum_{i=1}^{k}(2i+1) = (k+1)^2$ (this supposition is called the inductive hypothesis). Then, we have

$$\begin{aligned}
\sum_{i=1}^{k+1}(2i+1) &= \sum_{i=1}^{k}(2i+1) + 2(k+1) + 1 \\
&= (k+1)^2 + 2(k+1) + 1 \\
&\quad \text{(by the inductive hypotheis)} \\
&= (k+2)^2.
\end{aligned}$$

Strong Induction

Principle of Strong Induction: Let n_0 be an integer and let P be a property of the integers that are at least equal to n_0. Suppose that

1. $P(n_0)$ is true, and
2. for all $k \geq n_0$, if $P(j)$ is true for every j with $n_0 \leqslant j \leqslant k$, then $P(k+1)$ is true.

Then, $P(n)$ is true for every integer greater or equal to n_0.

Example

We show that every integer greater or equal to 2 has a prime factorization (i.e., it can be obtained as the product of one or more prime numbers).

The basic step is for $n_0 = 2$. This is immediate since 2 is itself prime.

Suppose that $k \geqslant 2$, and that every natural number j with $2 \leqslant j \leqslant k$ has a prime factorization. We must show that $k+1$ has a prime factorization.

If $k+1$ is prime, then this is certainly true. If $k+1$ is not prime, then $k+1$ must be evenly divisible by some number r bigger than 1 and less than $k+1$, say, $k+1 = rs$. Then, we have $2 \leqslant r, s \leqslant k$, so by the induction hypothesis, both r and s can be written as products of primes. Combining these prime factorizations, we get a prime factorization for $k+1$.

Course-of-Values Induction

In the course-of-value induction we prove a single statement:

$$(\forall n)[\textbf{if } (\forall m)_{m<n} P(m) \textbf{then } P(n)].$$

Apparently, there is no initial statement $P(0)$. But in fact, this statement is implied by the previous statement because the case $n = 0$ is

$$\textbf{if} (\forall m)_{m<0} P(m) \textbf{then } P(0).$$

and the part $(\forall m)_{m<0} P(m)$ is entirely vacuous because there is no $m \in \mathbb{N}$ with $m < 0$.

Example

Let $P(n)$ be the property that n is the product of one or more prime numbers. We use course-of-value induction with $n_0 = 2$ to show that $P(n)$ is true for all $n \geqslant 2$. Suppose that $k \geqslant 2$ and that $P(j)$ is true for all j with $2 \leqslant j < k$. If k is prime, then $P(k)$ is obviously true. If not, then we can write $k = rs$, where $2 \leq r, s < k$, and we can use the inductive hypothesis to finish the proof, as we did before.