COMPSCI750: Computational Complexity Mathematically Prerequisites

Cristian S. Calude

Semester 2, 2022

Textbook

- M. Sipser. *Introduction to the Theory of Computation*, PWS, 2013.

Sets can be described by a specific property P, $\{n \mid P(n)\}$. For example, $\{n \in \mathbf{N} \mid n \text{ is prime}\} = \{2, 3, 5, 7, 11, \dots\}$. Note the difference between $\emptyset$ and $\{\emptyset\}$.

Sets can be combined with various operations, including *union* ($A \cup B$ consists of all elements in A **or** in B), *intersection* ($A \cap B$ consists of all elements in A **and** in B), *complement* ($\overline{A}$ consists of all elements **not in** A) and *power set* (2^A consists of **all** subsets of elements of A).

$$\{3, 4\} \cup \emptyset = \{3, 4\},$$

$$\{5, 1, 10\} \cap \{2, 3, 5, 7, 11, \dots\} = \{5\},$$

$$\overline{\{2, 3, 5, 7, 11, \dots\}} = \{0, 1, 4, 6, 8, \dots\},$$

$$2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

For every set A, $A \cap \overline{A} = \emptyset$.

For every set A, $2^A \neq \emptyset$.

A *function* (or a *mapping*) is a rule/process that takes an input and produces an output. *For every function, the same input always produces the same output.*

If f is a function that produces the output b on input a we write $f(a) = b$.

The set of inputs of a function f is called the *domain* (D) of f; the sets of outputs is called the *range* (R) of f. We write $f : D \to R$.

The function $f : D \to R$ is

- *injective or one-to-one* if for every $x \neq y$ in D, $f(x) \neq f(y)$;
- *surjective or onto* if for every $z \in R$ there exists $x \in D$ such that $f(x) = z$;
- *bijective* if it is both injective and surjective.

The function $f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ defined by

- $f(n) = 0$ for all $n \in \{0, 1, 2, 3, 4\}$ is not injective and not surjective;
- $f(n) = n + 1$ for $n \in \{0, 1, 2, 3\}$ and $f(4) = 0$ is bijective.

No function $f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ can be injective and not surjective (or surjective and not injective).

The function $f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4, \dots\}$ defined by $f(n) = n$ for all $n \in \{0, 1, 2, 3, 4\}$ is injective and not surjective.

The function $f : \{0, 1, 2, 3, \dots\} \to \{0, 1, 2\}$ where $f(n)$ is the remainder of the division of n by 3 for all $n \in \{0, 1, 2, 3, \dots\}$ is surjective and not injective.

A *sequence* is a list of elements in some order. We use parentheses to describe sequences like in $(4, 1, 44)$. As the order is important, $(4, 1, 44) \neq (44, 1, 4)$.

Finite sequences are also called *tuples*. A tuple with k elements is called k-tuple; if $k = 2$, we call it a *pair*.

The *cross product* of the sets A, B is defined by

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

For example,

$$\{a, b, c\} \times \{0, 1\} = \{(a, 0), (b, 0), (c, 0), (a, 1), (b, 1), (c, 1)\}.$$

A subset R of a set $A \times B$ is called a *(binary) relation*.

An equivalence relation $R \subseteq A \times A$ (also denoted by $\equiv$) has the following three properties:

1. *reflexivity*: for every $x \in A$, $(x, x) \in R$,
2. *symmetry*: for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$,
3. *transitivity*: for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

We now **prove** that the relation $n \equiv m$ defined on natural numbers by "$n - m$ is a multiple of 7" is an equivalence relation.

First, we have $n \equiv n$ because 7 divides $n - n = 0$. Second, if $n \equiv m$ then (by definition) $n - m$ is a multiple of 7, so $m - n = -(n - m)$ is also a multiple of 7, so $m \equiv n$. Third, if $n \equiv m$ and $m \equiv t$, then (by definition) $n - m$ and $m - t$ are multiples of 7, so $n - t = (n - m) + (m - t)$ is also a multiple of 7 because the sum of two multiples of 7 is also a multiple of 7, so $n \equiv t$.

Given an equivalence relation R on a set A, the equivalence class of an element $a \in A$ is

$$[a] = \{x \in A \mid (a, x) \in R\}.$$

There are 7 equivalence classes for the equivalence relation $n \equiv m$ defined on natural numbers by "$n - m$ is a multiple of 7":

$$[0], [1], [2], [3], [4], [5], [6].$$

Note that $[0] = [7] = [14] = [7k]$, for every $k \geq 0$.

If R is an equivalence relation on a set A, and $x, y \in A$, then the following statements are equivalent:

- $(x, y) \in R$,
- $[x] = [y]$,
- $[x] \cap [y] \neq \emptyset$.

Proof: Indeed, if $(x, y) \in R$ and $a \in [x]$, then by symmetry and transitivity $a \in [y]$. If $[x] = [y]$ then $[x] \cap [y] = [x] \neq \emptyset$. If $[x] \cap [y] \neq \emptyset$, then there is $a \in [x] \cap [y]$ so $a \in [x]$ and $a \in [y]$, hence by symmetry $x \in [a], y \in [a]$, so by transitivity $(x, y) \in R$.

Predicates

A *predicate* or *property* is a function $P : A \to \{\mathrm{TRUE}, \mathrm{FALSE}\}$. Sometimes we write $P : A \to \{0, 1\}$, where 0 stands for FALSE and 1 stands for TRUE.

For example, the predicate PRIME: $\{1, 2, 3, \dots\} \to \{0, 1\}$ is defined by PRIME(n)=0, if n is composite and PRIME(n)=1, if n is prime.

PRIME(13)=1, PRIME($2^{82,589,933} - 1$) = 1 (actually, this is the largest known prime since January 2020; this number has 24,862,048 digits when written in base 10),

PRIME($2^{82,589,933}$) = 0.

The values TRUE and FALSE are called *Boolean values* and are denoted by 1 and 0, respectively. The following operations with Boolean values are important:

- Negation (NOT): $\neg x = 1 - x$,
- Disjunction ($\vee$): $x \vee y = \max\{x, y\}$,
- Conjunction ($\wedge$): $x \wedge y = \min\{x, y\}$,
- Implication ($\rightarrow$): $x \rightarrow y = \neg(x) \vee y = \max\{1 - x, y\}$,
- Equivalence ($\leftrightarrow$): $x \leftrightarrow y = (x \rightarrow y) \wedge (y \rightarrow x)$,
- Exclusive OR ($\oplus$): $\oplus(x, y) = \neg(x \leftrightarrow y)$.

The two most common quantifiers are "for all" – $\forall$ and "there exists" – $\exists$. If P is a predicate, then

- $\forall x P(x)$ means "for all x, $P(x)$ is true".
- $\exists x P(x)$ means "there exists x such that $P(x)$ is true".

Informal	Formal
For each natural number n, $n \cdot 2 = n + n$.	$\forall n \in \mathbb{N}\ (n \cdot 2 = n + n)$.
There exists a natural number n, n^2 is equal to 25.	$\exists n \in \mathbb{N}\ (n^2 = 25)$.
For some natural number n, n^2 is equal to 25.	$\exists n \in \mathbb{N}\ (n^2 = 25)$.

The following important rules relate negation to quantifiers:

$$\neg(\forall x P(x)) = \exists x(\neg P(x)),$$

$$\neg(\exists x P(x)) = \forall x(\neg P(x)).$$

Informal.
All horses fly. Negation (All horses fly) = There is a horse that does not fly.
Formal.

$$\forall x(\text{horse}(x) \to \text{fly}(x)).$$

$$\begin{aligned}\neg(\forall x(\text{horse}(x) \to \text{fly}(x))) &= \exists x(\neg(\text{horse}(x) \to \text{fly}(x))) \\ &= \exists x(\text{horse}(x) \wedge \neg\text{fly}(x))\end{aligned}$$

because $\neg(A \to B) = A \wedge \neg B$.

"Theorems and proofs are the heart and soul of mathematics and definitions are its spirit" says Sipser.

Definitions describe clearly and precisely the objects and notions we use.

Mathematical statements express properties of defined objects. They may be true or false, but they always have to be *precise*.

A *proof* is a convincing – ideally, in an absolute sense – argument that a statement is true. It should not only be "beyond reasonable doubt", but "beyond any doubt".

A *theorem* is a mathematical statement proved to be true. A *lemma* is a proved mathematical statement useful in the proof of a more important mathematical statement. A *corollary* is a proved mathematical statement which can be easily derived from another mathematical statement, usually a theorem.

The only way to show the truth or falsity of a mathematical statement is via a *mathematical proof*. Finding proofs is not easy, even if we use a *proof-assistant* (like Isabelle or Coq), i.e. a sophisticated software designed to *assist* with the development of formal proofs by human-machine collaboration.

A proof is typically a formal argument showing the truth of an implication of the form "P implies Q". A proof of an equivalence is a proof of both implications "P implies Q" and "Q implies P".

In what follows we shall present some typical examples of proofs: they will appear in one form or another in what follows.

Theorem 0.10 *For any two sets A and B,*

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Proof. The theorem states that two sets are equal, hence we need to prove that every element in $\overline{A \cup B}$ is in $\overline{A} \cap \overline{B}$ and, conversely, every element in $\overline{A} \cap \overline{B}$ is in $\overline{A \cup B}$.

If $x \in \overline{A \cup B}$, then $x \notin A \cup B$ (by the definition of the complement), hence $x \notin A$ and $x \notin B$ (by the definition of the union), so $x \in \overline{A}$ and $x \in \overline{B}$ (by the definition of the complement), which means that $x \in \overline{A} \cap \overline{B}$ (by definition of the intersection). This shows that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

Next we shall prove the converse implication, i.e. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Try it!

A number is *rational* if it is a ratio of two integers, $\frac{n}{m}$, where $m \neq 0$. The number $\sqrt{2}$ is irrational.

Theorem. *There exist irrational numbers a and b such that a^b is rational.*

Non-constructive proof. The number $\sqrt{2}^{\sqrt{2}}$ is either rational **or** irrational. If it is rational, our statement is proved: $a = b = \sqrt{2}$. If it is irrational, then take $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$ and compute: $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$. The statement was proved.

This proof is *non-constructive* because we don't know whether $\sqrt{2}^{\sqrt{2}}$ is rational or not.

Theorem. *There exist irrational numbers a and b such that a^b is rational.*

Constructive proof. The numbers $a = \sqrt{2}$, $b = \log_2 9$ are irrationals and $a^b = 3$ is rational. The statement was proved.

Really? A simple analysis of the proof shows that in fact we have an implication:

$$\textit{If the numbers } a = \sqrt{2},\ b = \log_2 9 \textit{ are irrationals,}$$
$$\textit{then } a^b = 3 \textit{ is rational.}$$

To prove the theorem we need to prove that the implication is true. As the conclusion is true, we need to show that the hypothesis is true, that is two facts: a) $\sqrt{2}$ is irrational and b) $\log_2 9$ is irrational!

Theorem 0.14 $\sqrt{2}$ *is irrational.*

Proof. Assume by absurdity that $\sqrt{2}$ is rational, that is,

$$\sqrt{2} = \frac{N}{M},$$

where $M \neq 0$. If both N, M are divisible by the same integer t, then divide them by t; the value of the fraction will not change. Continue this (finite!) process till no such integer exists, so

$$\sqrt{2} = \frac{N}{M} = \frac{n}{m}.$$

Both n, m cannot be even. As $m \neq 0$, we can write $m\sqrt{2} = n$ and by squaring both members we get

$$2m^2 = n^2. \tag{1}$$

Continuation of the proof. From (1) we deduce that n^2 is even, so n is also even as the square of an odd number is odd. So, there exists an integer k such that $n = 2k$. Substituting in the equation (1) we get:

$$2m^2 = (2k)^2 = 4k^2.$$

This mean that $m^2 = 2k^2$, that is, m is even, a contradiction!

Theorem. $\log_2 9$ *is irrational.*

Proof. Assume by absurdity that $\log_2 9$ is rational, that is $\log_2 9 = \frac{n}{m}$, where n, m are integers and $m \neq 0$. By the properties of logarithms, 9^m would be equal to 2^n, a contradiction because the former is odd, and the latter is even.

Proof by induction is a method to show that all elements of an infinite countable set have a certain property.

Consider a property $P(i)$ of natural numbers; the goal is to show that $P(i)$ is true for every natural number i. As there are infinitely many i's, we cannot verify individually each of them, so the proof by induction comes handy.

The proof by induction consists in two steps:

1. *Basis*: Prove that $P(k)$ is true for a fixed natural number k.
2. *Induction step*: For each $i \geq k$ assume that $P(i)$ is true – the *induction hypothesis* –, and prove that $P(i+1)$ is also true.

The conclusion is that $P(i)$ is true for every $i \geq k$.

Theorem. $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Proof. For the basis we take $k = 1$: $1 = \frac{1 \cdot 2}{2}$ checks. Then, we assume that for every $i \geq k = 1$ we have

$$1 + 2 + 3 + \cdots + i = \frac{i(i+1)}{2}, \tag{2}$$

and we need to prove that

$$1 + 2 + 3 + \cdots + (i+1) = \frac{(i+1)(i+2)}{2}.$$

Indeed, using the induction hypothesis (2) we get:

$$1 + 2 + 3 + \cdots + i + (i+1) = (1 + 2 + 3 + \cdots + i) + (i+1)$$

$$= \frac{i(i+1)}{2} + (i+1) = \frac{(i+1)(i+2)}{2}.$$

An *alphabet* is a finite set. The elements of an alphabet are called *symbols*. Alphabets are usually denoted by capital (sometimes Greek) letters:

$$\Sigma = \{a\}, B = \{0, 1\}, \Gamma = \text{the set of 7-bit ASCII characters.}$$

A *string* over an alphabet is a finite sequence of symbols over the alphabet. For example, 1000 is a string over the alphabet B. The *length* of the string w over the alphabet Σ – denoted by $|w|$ – is the number of symbols it contains. The length of 00001 is 5. The string of length zero is called the *empty string* and is denoted by ε. Strings can be concatenated: from x and y we get xy; $|xy| = |x| + |y|$.

The set of all strings over the alphabet Σ is denoted by Σ^*. A string x is a *substring* of y if there exist two strings u, v such that $y = uxv$: *cad* is a substring of *abracadabra* over the alphabet $\{a, b, c, d, r\}$.

The *lexicographical order* of strings is defined in two steps: a) a shorter string precedes a longer string, and b) strings of the same length are ordered as in the dictionary (this assumes an ordering of the symbols in the alphabet).
If $B = \{0, 1\}$ and 0 precedes 1, then we have

$$\varepsilon < 0 < 1 < 00 < 01 < 10 < 11 < 000 < 001 < \ldots$$

A *language* is a set of strings. All set-theoretic operations can be applied to languages, but there are specific language-theoretic operations like *concatenation*:

$$AB = \{xy \mid x \in A, y \in B\}.$$

A typical question is in this area is:

> *Is the membership function of the set of strings with prime lengths computable by a Turing machine?*

The answer is affirmative. However, not all functions are computable and the Halting Problem is an (in)famous example.

Computability theory (from 1930s on) is an area of mathematics which studies the functions which are computable by Turing machines (or equivalent models of computation) and compares the objects which are not computable.

Church Turing Thesis

A function $f : \Sigma^* \to \Sigma^*$ is intuitively computable, i.e. computable by an algorithm, if and only if it is computable by a Turing machine.

If f is computable by a Turing machine, then it is intuitively computable because a Turing machine is an algorithm.

The converse implication cannot be proved mathematically because the definition "computable by an algorithm" is not a mathematical object as "algorithm" is not a mathematical object. This implication was verified empirically, but the problem is still open.

Church-Turing Thesis allows the use of algorithms instead of Turing machines, hence simplifying proofs.

Descriptional complexity theory (from the 1960s on) studies the complexity of expressing a property or naming an object.

Computational complexity (from the 1970s on) studies the time or space used in the computation and compares the difficulties of solving problems, even if the problems cannot be solved efficiently (intractable).