Computation Theory, Term II/2020–21

Lecture 2: Mathematical Preliminaries

built on 2021/01/05 at 16:34:51

The goals of this lecture are threefold:

- To remind you of some mathematical concepts that you have seen before but may have forgotten. Along the way, we'll try to agree upon notation that will be used in this class.
- To review proof techniques that you've mastered in the past but may feel a bit rusty. Along the way, we'll try to look at stylistic issues.
- To explore connections between proofs and computations. Why do some proofs translate (almost) directly to computer algorithms? Why some others don't—or take more efforts to do so?

1 Something Old, Something New

We review some mathematical concepts that will be pertinent to this course. You have seen most of these from other courses already.

1.1 Functions

A *function* is an object that defines an input/output behavior; that is, a function takes an input and produces an output. For a mathematical function, the same input will always lead to the same output, every time you invoke it.

A function takes input from a set of possible inputs called the *domain*—and produces an output from a set called the *range*. We often write $f : D \to R$ to indicate that f takes input from D (i.e., the domain is D) and produes an output in R (i.e., the range is R).

There are many ways to describe a specific function:

- One way is with a list of steps ("procedure") for computing the output for an input. A typical example is when we see $f(x) = 2x + 5$. What we really mean is, if the input is x, we'll multiply x by 2 and add 5 to it—and that will be our answer. In similar ways, the following is a function described in this manner:

```
int foo(int price) {
  if (price < 10) return 5;
  else {
    int baseShipping = 4*price;
    int tax = 0.07*price;
    return tax + baseShipping + price;
  }
}
```

- It is also possible with a table that lists all possible inputs and the corresponding output values. For example:

Example 1.1 *Consider the function* $f\colon \{0,1,2\} \to \{0,1,2\}$ *where*

n	$f(n)$
0	2
1	0
2	1

This function adds 2 *to the input and computes the result modulo* 3.

Example 1.2 *A function sometimes takes more than one input value as input. Let* $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. *Then, the following function is a function* $g\colon \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$, *given as a table:*

$g(\downarrow,\rightarrow)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

There are a few features worth pointing out:

1. *you call this function with, for instance,* $g(2,3)$*, which results in the value* 1*;*
2. *that* $(2,3)$ *is an element from the domain of g. The domain of g is the set* $\mathbb{Z}_4 \times \mathbb{Z}_4$*, so each element of it is a pair of values. By the way, the set* $A \times B$ *is called the Cartesian product of A and B. Nothing stops you from writing* $A \times B \times A$*. And there's the shorthand* A^k *for* $A \times A \times \cdots \times A$*, where there are k of As.*

1.2 Strings and Languages

Strings are the bread and butter of computing. To formally describe them, we'll define an *alphabet* to be any nonempty finite set. What goes into the alphabet set are the *symbols* of the alphabet. Most often, we use the Greek letter Σ for an alphabet. For example, we may write

$$\Sigma_1 = \{\mathtt{0}, \mathtt{1}\} \qquad \Sigma_2 = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f}, \mathtt{g}, \mathtt{h}, \mathtt{i}, \mathtt{j}, \mathtt{k}, \mathtt{l}, ..., \mathtt{z}\}$$

Strings are defined over an alphabet. A *string* over Σ is a finite sequence of symbols from Σ. The set Σ^* contains all possible strings on the alphabet Σ, including the empty string.

How can one formally define a language? Imagine giving a big baboon a typewriter with keys corresponding to the symbols in Σ. Whatever the baboon types away, that's a string. Is that a string in a language? Pretty much, if it appears in a predefined set, it's a language. Motivated by this, a language L is simply a set of strings, so $L \subset \Sigma^*$.

2 Proof Techniques

This is a quick recap of technologies you have seen and mastered from your previous courses but may have forgotten. In Math, a *theorem* is a statement that is demonstrably true. To demonstrate that it is true, we write a *proof*—a sequence of logical mathematical steps that form an irrefutable argument supporting the theorem.

As you can relate to firsthand, the task of finding proofs isn't easy (otherwise, your life would be too dull). To date, there is no fail-proof recipe for coming up with a proof although some strategies exist. Some useful tips from Pòlya *How to Solve It*:

1. Read and completely understand the statement of the theorem to be proved. Surprisingly, most often this is the hardest part.
2. Sometimes, theorems contain multiple theorems inside them. For example, "Property A if and only if property B", requires showing two statements: (1) $A \implies B$ and (2) $B \implies A$.
   Another one: To show that two sets A and B are equal, you can try showing that $A \subseteq B$ and $B \subseteq A$. By the same token, to show that X and Y have the same value, it is sometimes beneficial to show that $X \leqslant Y$ and $Y \leqslant X$.
3. Work out a few simple cases of the theorem just to get a grip on it (i.e., crack a few simple cases first).
4. Write down the proof once you have it. This is to ensure the correctness of your proof. Often, mistakes are caught at the time of writing.
5. Finding proofs takes time, we do not come prewired to produce proofs. Be patient, think, express and write clearly and try to be precise as much as possible.

Let's prove something simple: Here's a (easy) theorem that everyone of you knows how to prove.

Theorem 2.1 *There exists an* $x \in \mathbb{Z}_+$ *such that* $5x + 8 = 18$.

How do we go about proving such a statement? The "there exist" quantifier basically asks us to establish an x that (1) is a positive integer and (2) satisfies $5x + 8 = 18$. If we can exhibit such an x, we are set. So here's a proof:

Proof: Choose $x = 2$. It's easy to see that $x \in \mathbb{Z}_+$. Also, we can check that $5(2) + 8 = 18$. This concludes the proof of the theorem. ■

Notice that even though the process of coming up with $x = 2$ may involve solving the equation $5x + 8 = 18$, this doesn't necessarily show up in the proof. The act of solving for x could merely be part of the work in developing this proof. On a philosophical note, one may comment that the process of solving for x is perhaps more difficult (under some notion of difficulty) than verifying that an x satisfies the equation.

In real life, most theorems are more involved than that.

Theorem 2.2 (DeMorgan's Law) *For any two sets A and B,* $\overline{A \cup B} = \overline{A} \cap \overline{B}$

To prove this theorem, we must establish that the set $\overline{A \cup B}$ and the set $\overline{A} \cap \overline{B}$ are equal. You may remember that to show that $X = Y$, it suffices for you to show that every element of X belongs to Y and every element of Y belongs to X—in other words, $X \subseteq Y$ and $Y \subseteq X$.

Proof: Let A and B be any two given sets. We'll first prove that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. Let $x \in \overline{A \cup B}$. Then, $x \notin A \cup B$ by the definition of complement, so then $x \notin A$ and $x \notin B$, by the definition of union. This means that $x \in \overline{A}$ and $x \in \overline{B}$, by the definition of complement. Hence, x is in both $\overline{A}$ and $\overline{B}$, so $x \in \overline{A} \cap \overline{B}$.

We'll also show that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. Let $y \in \overline{A} \cap \overline{B}$, so y is in both $\overline{A}$ and $\overline{B}$, by the definition of intersection. This means $y \notin A$ and $y \notin B$, by the definition complement. It follows that $y \notin A \cup B$, and so $y \in \overline{A \cup B}$.

We conclude that $\overline{A \cup B} = \overline{A} \cap \overline{B}$. ■

2.1 Stylistic Note

We expect your proof to have *three* levels:

- The first level should be a one-word or one-phrase "hint" of the proof. For example, you'll say proof by contradiction, proof by induction, using pigeonhole principle, or "proof by induction using repeated applications of hypercontrativity theorem"
- The second level should be a short blurb of key idea(s).
- The third level should be your full proof.

Due to (time) constraints (and the fact that you'll be bored to tears), most proofs in the lectures will usually contain only the first two levels.

2.2 Proof by Contradiction

To prove that a proposition P, suppose the opposite of P and show that the world would come to an end, so P must be true.

Theorem 2.3 $\sqrt{2}$ *is irrational.*

Proof: Suppose for a contradiction that $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ and $b \neq 0$. Out of all possible a and b, we'll pick one that yields the least fraction—that is, if some $d > 1$ divides both a and b, we'll divide both of them by d.

Now, by squaring this equation, we have that $2 = \frac{a^2}{b^2}$. In other words,

$$a^2 = 2b^2.$$

This means a^2 is even, so a, too, must be even. That is, $a = 2k$ for some k. But then we have $4k^2 = 2b^2$, which means $2k^2 = b^2$. This, however, means b^2 must be even, and b itself must be even, too. Hence, $\frac{a}{b}$ isn't a least fraction[1] But then this is impossible because we made sure at the beginning that $\frac{a}{b}$ is the least fraction. ■

[1] At least 2 divides both a and b.

2.3 Induction

Induction is a simple and powerful technique for proving theorems. There are many variations, but the most simple form deals with the following:

> Let $P(n)$ be a mathematical statement that depends only on n—that $P(\cdot)$ is called the predicate. To prove that $P(n)$ is true for all n, a proof by induction requires that you prove the base case(s) and the inductive step—that is, showing if $P(n)$ is true, then $P(n+1)$ is true.

Claim 2.4 *For all integer $n \geqslant 1$, the summation*

$$1 + 2 + 3 + \cdots + n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

To proceed, we'll sketch a plan as follows. Since n is universally-quantified and a natural number, it seems natural to induct on n. But first, we need a predicate $P(\cdot)$ that we'll use for induction. We'll try the simplest one first—just repeat the claim.

$P(n) \equiv$ "$1 + 2 + 3 + \cdots + n = n(n+1)/2$."

What is the value of $P(1)$? Notice how, as defined, when we plug in a value of n into $P(n)$, we expect this function to return True or False—not a number or anything else.

Base Case. The smallest n we claim is $n = 1$, so let's check that $P(1)$ is indeed true. For this to be true, we must show that the left-hand side (LHS) of the equation is equal to the right-hand side (RHS). When $n = 1$, the LHS is 1 by itself. The RHS is $1(1+1)/2 = 1$. Hence, LHS is equal to RHS, and so $P(1)$ has been verified.

Inductive Step. We have verified the base case(s) up to $n = 1$. Therefore, we'll use the inductive step to show it for $n > 1$. Let $n \geqslant 2$. We will assume $P(n-1)$ is true and show that under this assumption, $P(n)$ is also true. By this assumption (that is, $P(n-1)$ is true), we know that

$$1 + 2 + 3 + \cdots + (n-1) = \frac{(n-1)n}{2}. \tag{2.1}$$

Like in the base case, to show that $P(n)$ holds, we need to verify that LHS equals RHS for the current n. Let's look at LHS first. On the left-hand side of the equation, we have $1 + 2 + 3 + \cdots + (n-1) + n$—the first n positive numbers. On the right hand side, we have $n(n+1)/2$.

But consider that LHS can be written as

$$\begin{aligned} 1 + 2 + 3 + \cdots + (n-1) + n &= \Big[1 + 2 + 3 + \cdots + (n-1)\Big] + n \\ &= \frac{(n-1)n}{2} + n && \text{[IH implies (2.1)]} \\ &= \frac{(n-1)n}{2} + \frac{2n}{2} && \text{[algebra]} \\ &= \frac{n(n-1+2)}{2} = \frac{n(n+1)}{2} && \text{[algebra]} \end{aligned}$$

which is equal to RHS, as we wish. Therefore, we conclude that $P(n-1) \implies P(n)$.

Conclusion: Having shown the base case and the inductive step, we conclude using the princicple of mathematical induction that $P(n)$ holds for all $n \geqslant 1$, hence proving the claim.

3 Provablility vs. Computability

The proof above that shows that there exists an $x \in \mathbb{Z}_+$ such that $5x + 8 = 18$ gives, as a side effect of the proof, a value of x that satisfies the conditions of the theorem. Many proofs you have seen in the past, mostly the inductive ones, also have this flavor: the proof gives a recipe to compute the solution.

Let's look at a slightly different example:

Theorem 3.1 *There exist irrational numbers a and b such that a^b is rational.*

How do we even go about proving this theorem? This is apparently difficult. We know a few irrational numbers, but recognizing whether a number is irrational is nontrivial. But if you play around a little bit, a few things are clear: we know that $\sqrt{2}$ is rational—and $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is clearly rational. However, is $\sqrt{2}^{\sqrt{2}}$ irrational or rational? We can't quite tell[2]. Still, can we take advantage of this idea?

Proof: Let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. We know a is a real number, so either a is rational or irrational. If a is irrational, then

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2,$$

and we've proved the theorem. Otherwise, a is rational. In this case, we have that if we let $x = \sqrt{2}$ and $y = \sqrt{2}$, then $x^y = \sqrt{2}^{\sqrt{2}} = a$ is rational. This concludes the proof. ■

Is this proof correct? Most mathematicians out there would say so. In terms of computation, there is something unsatisfying about how this proof works. Even though we're able to check the proof, at the end of the day, we don't know what a and what b make the theorem hold. The proof doesn't quite tell us how. Many proofs that are contradiction-based have the same issue: the argument just says something gotta be true because otherwise the world would fall apart. It doesn't exhibit the existence of such a thing.

4 Practice

Solve the following problems for practice:

(1) Remember that a positive integer a is *odd* if there exists a positive integer k such that $a = 2k + 1$. Show that if a is odd, then a^2 must be odd as well.

(2) Prove using mathematical induction that for $k \geqslant 1$,

$$1 + 3 + 5 + 7 + \cdots + (2k - 1) = k^2.$$

For more challenge (not to be handed in), prove the folowing theorem:

Theorem 4.1 *Let $n \in \mathbb{Z}_+$ For any set $A \subseteq \{1, 2, \ldots, 2n\}$ with $|A| = n + 1$, there are always two numbers in A such that one divides the other.*

(*Hints:* pigeonhole principle. Observe also that every number m can be written as $m = 2^i m'$. where m' is odd and $i \geqslant 0$.)

[2] it's actually irrational