COMPSCI 3MI3 - Principles of Programming Languages

Topic 2 - Mathematical Preliminaries

NCC Moore

McMaster University

Fall 2021

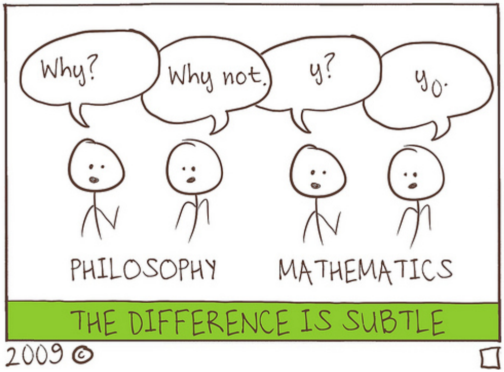
Adapted from Chapter 2 of "Types and Programming Languages" by Benjamin C. Pierce

Wait, this is a Math Class!?

Before we get started with the course proper, it will be useful to review some of the math we'll need.

- If you are unfamiliar with some of the concepts in this lecture, or don't feel you know the material very well, you are *strongly* encouraged to study these topics in preparation for the rest of this course.
- This course is pretty mathy, so a firm foundation is essential.

Sets, Relations, and Functions



Sets

We will use standard notation for sets.

- The elements of a set are delimited by curly braces:

$$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\} \tag{1}$$

  The above is the set of **Natural Numbers**.

- The empty set is denoted by $\emptyset$
- Set comprehensions are written as:

$$\{x \in S \mid \Phi(x)\} \tag{2}$$

  This is interpretted as "the collection of all elements of S satisfying the predicate $\Phi(x)$." In lecture, you will often hear me pronounce this as "such that".

Game Set Match

	Set Operators		Logical Operators
$s \in S$	Membership	$\exists$	Existential Quantifier
$S \cup T$	Union	$\forall$	Universal Quantifier
$S \cap T$	Intersection	$\neg$	Negation
$S \setminus T$	Difference	$\vee$	Or
$\lvert S \rvert$	Set Size	$\wedge$	And
$S \subseteq T$	Subset	$\rightarrow$	Implication
$S \supseteq T$	Superset	$\Longleftrightarrow$	"If and only if"
$S \subset T$	Strict Subset	$\vdash$	Proves
$S \supset T$	Strict Superset	$\models$	Models
$\mathcal{P}(S)$	Power Set of S	$\top \; \bot$	True and False

- $S \times T$ denotes the set of all possible tuples containing one element from S and one element from T.

Relations

An *n*-place **relation** on a collection of sets $S_1, S_2, S_3, \ldots, S_n$ is a set containing tuples of elements of from S_1 through S_n. R is a subset of the set of all possible such tuples.

$$R \subseteq S_1 \times S_2 \times S_3 \times \cdots \times S_n \tag{3}$$

If $s_1 \in S_1$ through $s_n \in S_n$, we say these elements are **related by** R if $(s_1, \ldots, s_n) \in R$

In Related News

A one place relation on a set S is called a **predicate** on S.

- We say a predicate P is true of an element $s \in S$ if $s \in P$.
- We will often write predicates in the form $P(s)$, like functions mapping elements of S to truth values.

A two-place relation R on sets S and T is called a **binary relation**.

- We will often write $s\,R\,t$ instead of the more proper $(s,t) \in R$.
- When we have a binary relation on elements of the same set U, we say that R is a binary relation *on* U

Relation Properties

The **domain** of a relation $R \subseteq S \times T$ is written $dom(R)$.

- The domain of R is the set of all elements $s \in S$ such that $(s, t) \in R$, for some t.

The **codomain** or **range** of R is written $range(R)$

- The codomain of R is the set of all elements $t \in T$ such that $(s, t) \in R$, for some s.

Functions

If a relation $R \subseteq S \times T$ has the following property, it is a **partial function**:

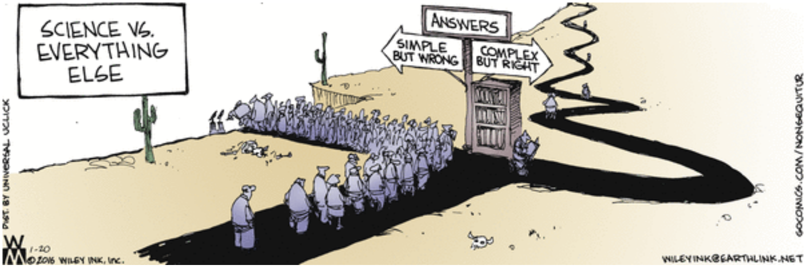
$$((s, t_1) \in R) \wedge ((s, t_2) \in R) \rightarrow (t_1 = t_2) \tag{4}$$

- If $s \in S$ is also in the domain of R, we say that "s is **defined on** R. We write this $R(s) \downarrow$
  - Otherwise, we say s is **undefined on** R, and write this $R(s) \uparrow$
- If, in addition, $dom(R) = S$, that is, if every element of S is in the domain of R, then R is a **total function**.

Supposing we have a binary relation R on S, and a predicate P on S, we say that P is **preserved on** R if:

$$P(s) \wedge s\,R\,t \rightarrow P(t) \tag{5}$$

Ordered Sets



“A proof is a repeatable experiment in persuasion.” -Jim Horning,

Binary Relation Properties

Reflexivity - If a relation R relates every element of S back to itself.

$$\forall s \in S \mid s \; R \; s \tag{6}$$

Symmetry - If the inverse of every tuple in R is also in R:

$$\forall s, t \in S \mid s \; R \; t \rightarrow t \; R \; s \tag{7}$$

Antisymmetry - If there are no tuples in R satisfying the above property, unless $s = t$

$$\forall s, t \in S \mid s \; R \; t \wedge t \; R \; s \rightarrow s = t \tag{8}$$

Transitivity - If a relation exibits the *transitive property*:

$$\forall s, t, u \in S \mid s \; R \; t \wedge t \; R \; u \rightarrow s \; R \; u \tag{9}$$

Binary Relation Properties Extended

- If a relation R on S is reflexive, transitive, and symmetric, the relation is called an **equivalence**.
- The **reflexive closure** of a relation R is the smallest reflexive relation R' such that $R \subseteq R'$.
- Similarly, the **transitive closure** of R is the smallest transitive relation R^+ such that $R \subseteq R^+$
- The **reflexive and transitive closure** of R is the smallest reflexive and transitive relation such that $R \subseteq R^*$

Another way to think of a **closure**, is as the set of all the tuples that would need to be added to R to satisfy the given property.

Preorders and Partial Orders

If a binary relation R on S is transitive and reflexive, we call it a **preorder on** S.

- We will use either $s \leq t$ or $s \sqsubseteq t$ to indicate a preorder.
- $s < t$ means that $s \leq t \wedge s \neq t$
- A preorder which is also antisymmetric is a **partial order**.

In some ways it's better to think of preorders and partial orders as graphs, with nodes as elements of S and tuples in the relation as edges of the graph.

Total Orders

- Over $\mathbb{N}$, $\mathbb{Z}$ or $\mathbb{R}$, we already know what orderings are intuitively.
- The usual ordering over the above sets is a **total order**.
- A total order is a partial order with one additional property: **strong connectivity** or **totality**.
- This means that, in addition to being transitive, reflexive and antisymmetric:

$$\forall s, t \in S \mid s \leq t \vee t \leq s \tag{10}$$

That is to say, every pair of elements in S is related by $\leq$.

Joins and Meets

If $\leq$ is a partial order on S, with $s, t \in S$, then $j \in S$ is the **join** (or *least upper bound*) of s and t if:

1. $s \leq j \wedge t \leq j$ and
2. if for any element $k \in S$, $s \leq k \wedge t \leq k \rightarrow j \leq k$

Similarly, $m \in S$ is the **meet** (or *greatest lower bound*) of $s, t \in S$ if:

1. $m \leq s \wedge m \leq t$
2. for any element $n \in S$, $n \leq s \wedge n \leq t \rightarrow n \leq m$

Chain Chain Chain

Suppose we have a preorder $\leq$ on S. A **decreasing chain** is a sequence of elements of S:

$$s_1, s_2, s_3, \ldots, s_n \tag{11}$$

Such that for every i:

$$s_i + 1 < s_i \tag{12}$$

- Chains can be **finite** or **infinite**.
- A set with no infinite decreasing chains is said to be **well founded**.
- For example, the total ordering over $\mathbb{N}$ is well founded, but the same ordering over $\mathbb{Z}$ is not.

Proof By Induction

IF YOU OBJECT TO MY CONJECTURE, I'LL PUT YOU INSIDE THIS COIL OF WIRES THAT'LL CREATE ELECTRICAL EDDY CURRENTS IN YOUR BODY UNTIL YOU *VAPORIZE!*

Professor Schmidt demonstrates the concept of proof by induction.

We're Going to Have to Induce!

[Principle of Ordinary Induction on Natural Numbers]
Suppose P is a predicate on $\mathbb{N}$. We take as axiomatic that:

$$P(0) \wedge (\forall i \in \mathbb{N} \mid P(i) \rightarrow P(i+1)) \rightarrow \forall n \in \mathbb{N} \mid P(n) \qquad (13)$$

In other words, if we can establish the *base case* of $P(0)$, and that $P(i+1)$ is a necessary consequence of $P(i)$, we can conclude that P holds for all $\mathbb{N}$

- For example, the following argument follows the above structure:
    - Premise: You were completely lost in this class in the first week of class.
    - Premise: For any week of class, if you were lost last week you will be lost this week.
    - Conclusion: You will always be lost in class.

Employee Induction Program

[Principle of Complete Induction on Natural Numbers]
Suppose P is a predicate on $\mathbb{N}$. We take as axiomatic that:

- If, for each natural number n, it is given that $P(i)$ holds for all $i < n$, and this demonstrates that P holds for n, we may conclude that P holds for all $\mathbb{N}$. In other words:

$$P(0) \wedge (P(0) \wedge P(1) \wedge \cdots \wedge P(n) \rightarrow P(n+1)) \rightarrow (\forall k \in \mathbb{N} | P(k)) \quad (14)$$

Complete or **Strong** Induction is so named because it uses a stronger hypothesis than simple induction.

- For example...
  - Premise: You were lost in this class for all weeks prior to a particular week.
  - Premise: Being lost for all weeks prior to a particular week implies you are lost in that particular week
  - Conclusion: You will always be lost in this class.

A Numerical Example

Consider the **Fundamental Theorem of Arithmetic**:

- Every natural number greater than 1 is the product of one or more prime numbers.

We can prove this using complete induction.

Base Case -

- In this case, we are concerned with the natural numbers greater than 1, so our base case will be 2.
- Is 2 the product of prime factors?
  - The only two factors of 2 are 1 and 2.
  - The definition of a prime number is a number which has no factors other than 1 and itself. $\therefore$ 2 is a prime number.
  - This argument also applies to 1. $\therefore$ 1 is a prime number.
  - 1 and 2 are prime, $\therefore$ 2 is the product of prime numbers.

A Numerical Example (cont.)

Iterative Case

- If $n \in \mathbb{N}$ is prime, then it is trivially the product of a prime number and 1.
- Otherwise, n has two factors, which must be less than n.

$$n = m_1 m_2 \tag{15}$$

  - If it is given that m_1 and m_2 are prime factorizable:

$$m_1 = p_1 p_2 \dots p_k \tag{16}$$

$$m_2 = q_1 q_2 \dots q_j \tag{17}$$

  Where all p_i and q_i are prime numbers.

$$\therefore n = p_1 p_2 \dots p_k q_1 q_2 \dots q_j \tag{18}$$

- n has no factor which is not prime, since primes are irreducible.
- $\therefore$ n is the product of prime factors.

Add to My Order

Lexicographic Ordering, or **dictionary ordering** is a way of generalizing an ordering to pairs, or even longer sequences of elements. For pairs:

$$(m, n) \leq (m', n') \iff m < m' \vee (m = m' \wedge n \leq n') \tag{19}$$

If you take the set of English letters, and alphabetical order as an ordering over them, lexicographic ordering is the way that words are arranged in the dictionary. Hence, *dictionary ordering*.

Inducted into the Math Hall of Fame

[Principle of Lexicographic Induction]
Supposing P is a predicate on pairs of natural numbers and $\leq$ is a lexicographic ordering relation, we take as axiomatic:

- If $P(0,0)$, and
- If, for each pair (m,n) of natural numbers:
  - given $P(m',n')$ for all $(m',n') < (m,n)$
  - we can conclude $P(m,n)$
- Then $P(m,n)$ holds for all $m,n \in \mathbb{N}$.

This method is also known as **nested** or **inner induction**.

- This method can be easily expanded to larger tuples.
- Induction on pairs is fairly common, triples are occasionally useful, and increasingly rare beyond that.

Structural Induction

[Principle of Structural Induction]
One form of induction we will be using frequently in this course is **structural induction**. Suppose P is a predicate on the members of a recursively defined structure (nodes in a tree, for example), we take as axiomatic that:

- For each member s:
  - If from $P(r)$ holding for all immediate submembers r of s
  - We may conclude $P(s)$
- We may conclude $P(s)$ holds for all members of the structure.

An Example Involving Beverages

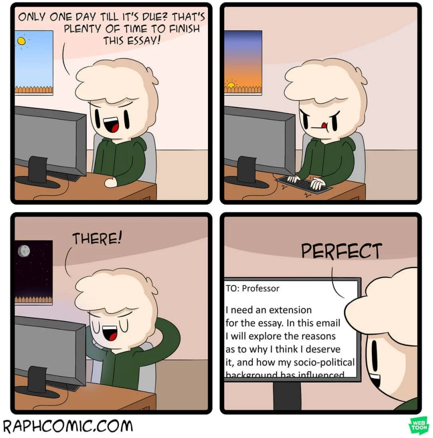
To demonstrate structural induction, let's argue that a cup contains tea and not coffee.

- Let's assume that we started off with n cups of tea.
- Let's also assume that a cup of tea is formed by pouring two other cups of tea together to form a larger one.

- Our predicate in this case is "the cup contains tea and not coffee". Since coffee cannot be produced by any tea combining process...
- We can conclude that, no matter where we are in the tea pouring process, or which combination of pours or cups we have used, there is no cup which contains coffee.

Last Slide Comic

Jokes at the students' expense time!


ONLY ONE DAY TILL IT'S DUE? THAT'S PLENTY OF TIME TO FINISH THIS ESSAY!
THERE!
PERFECT
RAPHCOMIC.COM
WEB TOON

TO: Professor

I need an extension for the essay. In this email I will explore the reasons as to why I think I deserve it, and how my socio-political background has influenced