Reference for Mathematical Notions

(Material covered in appendix A)

Xavier Rival and Kwangkeun Yi

Material provided with the book
"Static analysis: an abstract interpretation perspective"

2019

Basic mathematics

This set of slides covers the basic notions of mathematics required to read the book/follow the lectures supplied with it:

- sets
- logical connectors and formulas
- functions
- order relations, Galois connections
- use of induction in definitions and proofs, fixpoints

Note: this is just an introduction
more advanced material would be required for an in-depth lecture!

Sets

Sets define **finite or infinite collections of elements**

A few sets and their notations:

- $\emptyset$: empty set, containing no element
- $\{a_0, a_1, \ldots, a_n\}$: set comprising elements $a_0, a_1, \ldots, a_n$
- $S \cup T$: union of sets S and T, set containing exactly the elements that are either in S *or* in T
- $S \cap T$: intersection of sets S and T, set containing exactly the elements that are either in S *and* in T
- $S \times T$: set of pairs made of an element of S and an element of T
- $\wp(S)$: set of all subsets of S
- $\{x \in S \mid P(x)\}$: set of elements in S that satisfy logical predicate P
- $\mathbb{N}, \mathbb{R}$: sets of integers, of reals

Logical connectives

The following standard logical connectives are used throughout the book and the course (look for notes on mathematical logics for a formal introduction):

- **conjunction** $\wedge$:
  $A \wedge B$ holds if and only if both A and B hold
- **disjunction** $\vee$:
  $A \vee B$ holds if and only if either A or B holds
- **negation** $\neg$
- **implication** $\implies$: $A \implies B$ holds if and only if $\neg A \vee B$ holds
- **equivalence** $\iff$: $A \iff B$ is equivalent to $A \implies B \wedge B \longrightarrow A$
- **universal quantification** $\forall$:
  $\forall x \in A, P(x)$ holds if and only if $P(x)$ holds for any x in A
- **existential quantification** $\exists$:
  $\exists x \in A, P(x)$ holds if and only if there exists at least one x in A such that $P(x)$ holds

Definitions by induction

Definitions by **induction** allow to define mathematical objects of **unbounded size**, and **possibly arbitrarily deep with nesting** patterns.

Example: definition of very basic arithmetic expressions

$$
\begin{array}{rcl}
E & ::= & n \\
  & | & E \odot E
\end{array}
$$

An expression is

- either a base value
- or an operator applied to two expressions
  which in turn may be either a value or a binary operator applied to...

Proofs by recurrence

Principle of **proofs by induction**: cover all cases by exploiting the recursive structure of a set.

Most classical case: **proofs by recurrence over integers**
We assume a unary predicate P over integers.
Then, if we can prove:

1. that $P(0)$ holds
2. that for all integer n, if $P(n)$ holds, so does $P(n+1)$

then, **we can derive that, for all integer n, $P(n)$ holds**.

This principle generalizes to other inductively defined objects
e.g., the arithmetic expressions introduced previously:

1. prove $P(v)$ for each value $v \in n$
2. prove that for each operator $\odot$, and expressions E_0, E_1, if $P(E_0)$ and $P(E_1$ hold so does $P(E_0 \odot E_1)$

Functions

A **function** describes a **mapping from a set to another set**; very often this mapping may be seen **as a computation**.

Notation for function definitions:

$$\begin{array}{rcccl} f: & A & \longrightarrow & B & \\ & x & \longmapsto & e & \text{expression depending on } x \end{array}$$

Meaning: function called f, from set A to set B, which maps x into e.

Other notations:

- $f(a)$: application of function f to element a (i.e., it is an element of set B)
- $f \circ g$ composition of function g with function f
- $(x_n)_{n \in \mathbb{N}}$: sequence, i.e., function from $\mathbb{N}$ to some set (the image of n is x_n)

Order relations

An **order relation** over a set E is a binary relation $(\preceq) \subseteq E \times E$ which is

- **reflexive**: $\forall x \in E,\ x \preceq x$
- **transitive**: $\forall x, y, z \in E,\ x \preceq y$ and $y \preceq z \Longrightarrow x \preceq z$
- **anti-symmetric**: $\forall x, y \in E,\ x \preceq y$ and $y \preceq x \Longrightarrow x = y$

Furthermore it is **total** when any pair of elements can be compared in one direction or the other.

Examples:

- standard order over integers: $\ldots \leq -2 \leq -A \leq 0 \leq 1 \leq 2 \leq \ldots$
- lexicographic order ("dictionary ordering"): "ab" $\leq$ "b" $\leq$ "ba" $\leq$ "bad"
- set inclusion, *not total* ($\{1, 2\}$ and $\{2, 3\}$ cannot be compared)

Chain: subset of E that is a total ordering

Ordered sets

Distinguished elements of a subset F of a partially ordered set $(E, \preceq)$:

- **maximal element** y of F: $y \in F$ and $\forall z \in F,\ z \preceq y$
- **upper bound** y of F: $\forall z \in F,\ z \preceq y$
- **least upper bound**: minimal element of the upper bounds, noted $\sqcup F$
- dual notions: **minimal** element, **lower bound**, **greatest lower bound**

Lattice: set E with partial order $\preceq$ ($(E, \preceq)$ called partial order), such that

- pairs have a least upper bound and a greatest lower bound
- E has a minimal element $\bot$ and a maximal element $\top$

Complete lattice: lattice + any subset has a greatest lower bound and a least upper bound

Complete partial order (or **CPO**): partial order $(E, \preceq)$ such that

- there is a minimal element
- any chain has a least upper bound

Operators over ordered sets

We consider two partial orders $(E, \preceq)$ and $(F, \preceq)$ and $f : E \longrightarrow F$; then:

- f is **monotone** if and only if

$$\forall x, y \in E,\ x \preceq y \Longrightarrow f(x) \preceq f(y)$$

- f is **continuous** if and only if $(E, \preceq)$ and $(F, \preceq)$ are CPOs and

$$\forall G \subseteq E,\ G \text{ is a chain} \Longrightarrow \begin{cases} f(G) \text{ is a chain} \\ \sqcup\{f(x) \mid x \in G\} = f(\sqcup G) \end{cases}$$

If $E = F$ then f is **extensive** if and only if $\forall x \in E,\ x \preceq f(x)$

Fixpoints

We consider $f : E \longrightarrow E$, where $(E, \prec)$ is a partial order.

- $x \in E$ **is a fixpoint of** f if and only if

$$f(x) = x$$

- $x \in E$ **is the least fixpoint of** f if and only if x is a fixpoint of f and is smallest than all others

Existence: not guaranteed in general! (conditions + theorem needed!)

Unicity: not guaranteed for fixpoints in general!
if it exists, the least fixpoint is unique

Kleene's fixpoint theorem

An important **constructive existence theorem**:

Theorem

Let f be a continuous function from a CPO $(E, \preceq)$ to itself. Then f has a least fixpoint expressed as follows:

$$\mathbf{lfp} f = \bigcup_{n \in \mathbb{N}} f^n(\bot)$$

Proof main steps:

1. proof that the iterates form a chain, since $f^n(\bot) \preceq f^{n+1}(\bot)$
2. existence of the least upper bound CPO property
3. fixpoint by continuity
4. proof that any fixpoint is greater than $f^n(\bot)$ by induction over n

There exist **other fixpoint existence theorems** though we do not present them in this course.