SCHOOL FOR ADVANCED STUDIES LUCCA

Some preliminary math

Set Notation

$A \subseteq B$ every element of A is in B

$A \subset B$ if $A \subseteq B$ and there is one element of B not in A

$A \subseteq B$ and $B \subseteq A$ implies $A = B$

$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$ $(\bigcup_{i \in I} A_i)$

$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$ $(\bigcap_{i \in I} A_i)$

$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ *ordered pairs* $(\times_{i=1}^{n} A_i)$

$2^A = \{X \mid X \subseteq A\}$ *powerset*

Relations

$R \subseteq A \times B$ is a relation on sets A and B $\quad (R \subseteq \times_{i=1}^{n} A_i)$

$(a,b) \in R \;\equiv\; R(a,b) \;\equiv\; aRb$ *notation*

$Id_A = \{(a,a) \mid a \in A\}$ (identity)

$R^{-1} = \{(y,x) \mid (x,y) \in R\} \subseteq B \times A$ (inverse)

$R_1 \cdot R_2 = \{(x,z) \mid \exists y \in B.\ (x,y) \in R_1 \wedge (y,z) \in R_2\} \subseteq A \times C$ (composition)

Some basic constructions

$$\begin{array}{lcl} R^0 & = & Id_A \\ R^{n+1} & = & R \cdot R^n \\ R^* & = & \bigcup_{n \geq 0} R^n \\ R^+ & = & \bigcup_{n \geq 1} R^n \end{array}$$

Note that: $R^1 = R \cdot R^0 = R$, $\quad R^* = Id_A \cup R^+$ and

$R^+ = \{(x,y) \mid \exists n, \exists x_1, \ldots, x_n \text{ with } x_i R x_{i+1}\ (1 \leq i \leq n-1),\ x_1 = x,\ x_n = y\}$

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

Properties of Relations

Binary Relations

A binary relation $R \subseteq A \times A$ is (same set A)

reflexive:	$\forall x \in A$: $(x, x) \in R$,
symmetric:	$\forall x, y \in A$: $(x, y) \in R \Rightarrow (y, x) \in R$,
antisymmetric:	$\forall x, y \in A$: $(x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$;
transitive:	$\forall x, y, z \in A$: $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Closure of Relations

$S = R \cup Id_A$	the reflexive closure of R
$S = R \cup R^{-1}$	the symmetric closure of R
$S = R^{+}$	the transitive closure of R
$S = R^{*}$	the reflexive and transitive closure of R

Special Relations

A relation R is

- an **order** if it is reflexive, antisymmetric and transitive
- an **equivalence** if it is reflexive, symmetric and transitive
- a **preorder** if it is reflexive and transitive

Examples

- **orders**: less-than-or-equal-to ($\leqslant$) on $\mathbb{R}$, set inclusion ($\subseteq$),...
- **equivalences**: equal-to ($=$) on $\mathbb{R}$, congruent-mod-n ($\equiv \mod n$),...
- **preorders**: reachability in graphs, subtyping or behavioural relations, ...

Kernel relation

- Given a preorder R its **kernel**, $K = R \cap R^{-1}$, is an equivalence relation

Equivalence Classes and Quotient Set

Example: $R = \{(x,y) \in \mathbb{N}\times\mathbb{N} \mid (x \equiv y) \bmod 3\}$

$R(7,7)$, $R(7,1)$, $R(1,7)$, $R(7,10)$, $R(1,10)$, ...

$[0] = \{0, 3, 6, 9, \ldots\}$ — *equivalence classes:*

$[1] = \{1, 4, 7, 10, \ldots\}$ — *- have a representative*

$[2] = \{2, 5, 8, 11, \ldots\}$ — *- are disjoint*

An **equivalence class** is a subset C of A such that

$$x, y \in C \Rightarrow (x,y) \in R \quad \textit{consistent} \quad \text{and}$$

$$x \in C \wedge (x,y) \in R \Rightarrow y \in C \quad \textit{saturated}$$

The **quotient set** Q^R_A of A modulo R is a partition of A

is the set of equivalence classes induced by R on A

Example: $R = \{(x,y) \in \mathbb{N}\times\mathbb{N} \mid (x \equiv y) \bmod 3\}$

$Q^R_{\mathbb{N}} = \{ [0], [1], [2] \}$

Functions

Partial Functions

A *partial function* is a relation $f \subseteq A \times B$ such that

$$\forall x, y, z.\ (x, y) \in f \wedge (x, z) \in f \Rightarrow y = z$$

We denote partial function by $f : A \rightharpoondown B$

Total Functions

A (total) *function* is a partial function $f : A \rightharpoondown B$ such that

$$\forall x\ \exists y.\ (x, y) \in f$$

We denote total function by $f : A \rightarrow B$

Functions (total or partial) can be *monotone*, *continuous*, *injective*, *surjective*, *bijective*, *invertible*...

Induction Principle

Mathematical Induction

To prove that $P(n)$ holds for every natural number $n \in \mathbb{N}$, prove

1. $P(0)$
2. for any $k \in \mathbb{N}$, $P(k)$ implies $P(k+1)$

Example: Show that $sum(n) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for every $n \in \mathbb{N}$

(1) $sum(0) = \frac{0(0+1)}{2} = 0$ *base case*

(2) to show: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ implies $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$

assume $sum(n) = \frac{n(n+1)}{2}$, for a generic n

$sum(n+1) = sum(n) + (n+1) =$ *properties of summation*

$= \frac{n(n+1)}{2} + (n+1)$ *inductive hypothesis*

$= \frac{(n+1)(n+2)}{2}$ $\square$

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

Playful digression

Some “advanced” proof methods

1. Proof by obviousness: So evident it need not to be mentioned
2. Proof by general agreement: All in favor?
3. Proof by majority: When general agreement fails
4. Proof by plausibility: It sounds good
5. Proof by intuition: I have this feeling...
6. Proof by lost reference: I saw it somewhere
7. Proof by obscure reference: It appeared in the Annals of Polish Math. Soc. (1854, in polish)
8. Proof by logic: It is on the textbook, hence it must be true
9. Proof by intimidation: Who is saying that it is false!?
10. Proof by authority: Don Knuth said it was true
11. Proof by deception: Everybody please turn their backs ...
12. Proof by divine word: Lord said let it be true

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

Inductively Defined Sets

basis: the set I of initial elements of S
induction: rules R for constructing elements in S from elements in S
closure: S is the least set containing I and closed w.r.t. R

$\mathbb{N}$ = Natural numbers

$I = \{0\}, \quad R_1: \text{ if } X \in \mathbb{N} \text{ then } s(X) \in \mathbb{N}$

$\mathbb{N} = \{0, s(0), s(s(0)), \ldots\}$

$L_{\mathbb{N}}$ = lists of elements of $\mathbb{N}$

$I = \{[\,]\}, \quad R_1: \text{ if } X \in L_{\mathbb{N}} \text{ and } n \in \mathbb{N} \text{ then } [n|X] \in L_{\mathbb{N}}$

$L_{\mathbb{N}} = \{[\,], [0], [1], [2], \ldots, [0,0], [0,1], [0,2], \ldots, [1,0], [1,1], [1,2], \ldots\}$

Tr = n-ary trees

$I = \{\varepsilon\}, \quad R_1: \text{ if } X_1, \ldots, X_n \in Tr \text{ for any n, then } t(X_1, \ldots, X_n) \in Tr$

$Tr = \{\varepsilon, t(\varepsilon), t(\varepsilon, \varepsilon), \ldots, t(t(\varepsilon)), \ldots, t(\varepsilon, t(t(\varepsilon), \varepsilon), t(\varepsilon, \varepsilon, \varepsilon)), \ldots\}$

Structural Induction

Let us consider a set S inductively defined by a set $C = \{c_1, \dots, c_n\}$ of constructors of arity $\{a_1, \dots, a_n\}$ with

- $I = \{c_i(\,) \mid a_i = 0\}$
- R_i : if $X_1, \dots, X_{a_i} \in S$ then $c_i(X_1, \dots, X_{a_i}) \in S$

Principle of Structural Induction

To prove that $P(x)$ holds for every x of a structurally defined set S, it is sufficient to prove that

$$P(s_1), \dots, P(s_k) \implies P(c_k(s_1, \dots, s_k)) \qquad \text{if}$$

- for every constructor $c_k \in C$ and
- for every $s_1, \dots, s_k \in S$, where k is the arity of c_k

The base case is the one dealing with constructors of arity 0, i.e. with constants

Structural Induction – exercise

Prove that $sum(\ell) \leq max(\ell) * len(\ell)$, for every $\ell \in Lists(\mathbb{N})$

where

- $sum(\ell)$ is the sum of all elements in list ℓ
- $max(\ell)$ is the greatest element in ℓ (with $max([\,]) = 0$)
- $len(\ell)$ is the number of elements in ℓ

A refresher on induction

The induction principle is very useful, as you all probably know. Let's refresh it.

- Proof method

To show that a property, say P, holds of every natural number n (i.e., to prove P(n) for all n) it suffices to show that
  - P(0) is true &
  - for all k, P(k) implies P(n+1)

  Example: for all n, sum(n) = n(n+1)/2 where sum(k) = 1 + ... + k
    - sum(0) = 0 = 0(0+1)/2
    - for all k, if sum(k) = k(k+1)/2 then

sum(k+1) = sum(k) + (k+1)	by definition
= k(k+1)/2 + (k+1)	by inductive hypothesis
= (k(k+1) + 2(k + 1)) / 2	by arithmetic laws
= (k + 1)(k+2)/2	by distributivity of multiplication over sum on natural numbers

- Definitional mechanism

To define a set S inductively using a finite number of constructors f1,....,fn each with a finite arity on a set of 'basic elements'

- fix a set I of basic elements (you can think of the elements in I as constructors of arity 0)	basis
- if e1,...,ek are in S and f is a constructor of arity k then f(e1,...,ek) is an element of S	induction
- nothing else can be an element of S	closure

- Example: I ={0} and s(_) is a constructor of arity 1, then the inductively defined set S = {0, s(0), s(s(0)), ...} is isomorphic to natural numbers

(Indeed basis / induction / and closure boil down to the axioms of Peano).

An exercise in axiomatic semantics

m1: map f [] = []
m2: map f a:as = f(a):(map f as)

Example: double x = x+x => map double [1,2,3] = [2,4,6]

i1: inverse [] = []
i2: inverse a:as = (inverse as) ++ [a]

Example: inverse [1,2,3] = [3,2,1]

Exercise 1
Give an inductive definition of the set of lists of natural numbers.

Prove that for all functions f and all lists as, inverse (map f as) = map f (inverse as)

inverse (map f []) = inverse [] by m1
= [] by i1

map f (inverse []) = map f [] by i1
= [] by m1

inverse (map f a:as) = inverse (f(a):(map f as)) by m2
= (inverse (map f as)) ++ [f(a)]) by i2
= (map f (inverse as)) ++ [f(a)] by inductive hypothesis
= map f ((inverse as) ++ [a]) by lemma1: (map f as) ++ (map f bs) = map f (as ++ bs)
= map f (inverse as) ++ (inverse [a])) by lemma2: if len(as) = 1 then inverse as = as
= map f (inverse a: as) by lemma3: (inverse as) ++ (inverse bs) = inverse (bs ++ as)

Exercise 2
Prove lemmas 1, 2, and 3 above.