

Logical Foundations of CS – CS5303

Sets and Functions

These notes were written using *Mathématiques pour l'Informatique*, by André Arnold and Irène Guessarian.

1 Sets

Let us review some notations about sets.

Let us consider that E is a set, and e is an element.

- $e \in E$ means that e is an element of E , e is in set E
- $e \notin E$ means that e does not belong to E , e is “outside” E
- the empty set is denoted \emptyset

Let us consider two sets A and B .

- $A \subseteq B$ means that A is a subset of B : this means that A is included in B , i.e., all elements of A are also elements of B
- the negation of the above is noted $A \not\subseteq B$, and means that A is not included in B : it **does not mean** that B is included in A
- Note: $A = B$ iff ($A \subseteq B$ and $B \subseteq A$)
- if $A \subseteq B$ but $A \neq B$, we can note it as follows: $A \subsetneq B$
- $\mathcal{P}(E)$ denotes the set of subsets of E : in particular, $A \subseteq E$ iff $A \in \mathcal{P}(E)$; and $\emptyset \in \mathcal{P}(E)$, $E \in \mathcal{P}(E)$

The cartesian product of two sets E and F is the set of all couples made of one element of E and one element of F :

$$E \times F = \{(x, y) \mid x \in E, y \in F\}$$

More generally,

$$E_1 \times \cdots \times E_n = \{(x_1, \dots, x_n) \mid \forall 1 \leq i \leq n, x_i \in E_i\}$$

In the following, we suppose that we work in a general set (universe) E , and we consider two subsets of E , namely A and B .

- $A \cap B = \{e \in E \mid e \in A \wedge e \in B\}$
- $A \cup B = \{e \in E \mid e \in A \vee e \in B\}$
- $A \setminus B = \{e \in E \mid e \in A \wedge e \notin B\}$
- $\overline{A} = \{e \in E \mid e \notin A\}$
- $A \Delta B = (A \setminus B) \cup (B \setminus A)$
- A and B are disjoint iff $A \cap B = \emptyset$

Let us consider a family $(A_i)_{i \in I}$ of subsets of E :

- $\bigcup_{i \in I} A_i = \{e \in E \mid \exists i \in I, e \in A_i\}$
- $\bigcap_{i \in I} A_i = \{e \in E \mid \forall i \in I, e \in A_i\}$
- $\bigcup_{i \in \emptyset} A_i = \emptyset$
- $\bigcap_{i \in \emptyset} A_i = E$

A family $(A_i)_{i \in I}$ of subsets of E is a partition of E iff:

- $A_i \neq \emptyset, \forall i \in I$
- $A_i \cap A_j = \emptyset, \forall i \neq j \in I$
- $E = \bigcup_{i \in I} A_i$

Exercise 1 Verify the following statements:

- $\overline{\overline{E}} = \emptyset$ and $\overline{\emptyset} = E$
- $A \cap \emptyset = \emptyset, A \cup E = E, A \Delta E = \overline{A}$
- $A \cap A = A \cup A = A \cup \emptyset = A \Delta \emptyset = A \cap E = A$
- $A \setminus B = A \cap \overline{B}$
- $A \setminus A = A \Delta A = \emptyset$

The DeMorgan's laws that you know in logic also hold here:

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

Also note that \cup and \cap are distributive.

2 Functions

An application f from a set E to a set F is a procedure allowing to associate to each element of E a **unique** element $f(x)$ of F .

- Domain of f : $Dom(f) = \{x \in E \mid \exists y \in F, y = f(x)\}$
- Image of f : $Im(f) = \{y \in F \mid \exists x \in E, y = f(x)\}$
- Image by f of a subset X of E : $f(X) = \{y \in F \mid \exists x \in X, y = f(x)\}$
- For all subsets Y of F , $f^{-1}(Y) = \{x \in E \mid \exists y \in Y, y = f(x)\}$
- $Dom(f) = f^{-1}(F)$ and $Im(f) = f(E)$

Examples:

- the identity application of E : $id_E : E \rightarrow E$ is defined by $id_E(x) = x, \forall x \in E$.
- the characteristic function of a subset A of E is the function: $\xi_A : E \rightarrow \{0, 1\}$ such that: $\xi_A(e) = 1$ if $e \in A$, 0 otherwise

Injective, surjective, bijective:

- f is injective iff: $\forall x_1, x_2 \in E, f(x_1) = f(x_2) \rightarrow x_1 = x_2$
- f is surjective iff: $\forall y \in F, \exists x \in E, y = f(x)$
- f is bijective iff f is injective and surjective (determine the corresponding formal definition)

Composition: Let $f : E \rightarrow F$ and $g : F \rightarrow G$ be two applications. The composition of f and g is the application $g \circ f : E \rightarrow G$, defined by $g \circ f(x) = g(f(x))$. Note: \circ is associative.

Example: Consider $f : E \rightarrow F$. Then $f \circ id_E = id_F \circ f = f$.

Let $f : E \rightarrow F$ and $g : F \rightarrow G$ be two applications. Then,

- f and g injective $\rightarrow g \circ f$ injective
- f and g surjective $\rightarrow g \circ f$ surjective
- f and g bijective $\rightarrow g \circ f$ bijective

Prove the above statements.

3 Cardinality

3.1 Finite sets

For all integer n , let us note $[n]$ the set $\{1, \dots, n\}$ of all integers between 1 and n . If $n < m$ then there is no possible injective function between $[m]$ and $[n]$.

Therefore two integers n and m are equal iff there exists a bijective function between $[n]$ and $[m]$.

A set E is finite if there exists $n \in \mathbb{N}$ and a bijective function $f : E \rightarrow [n]$. n is then called the cardinal of E , and denoted by $|E|$.

Let E and F be two finite sets, and $f : E \rightarrow F$ an application:

- f injective $\rightarrow \forall y \in F, |f^{-1}(\{y\})| \leq 1$
- f surjective $\rightarrow \forall y \in F, |f^{-1}(\{y\})| \geq 1$
- f bijective $\rightarrow \forall y \in F, |f^{-1}(\{y\})| = 1$

If in addition, $|E| = |F|$ then:

$$f \text{ injective} \leftrightarrow f \text{ surjective} \leftrightarrow f \text{ bijective}$$

However, in case E is infinite, the above statement does not hold. For instance, $f : \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(n) = 2n$ is injective but not surjective.

Let E and F be two finite sets.

1. If E and F are disjoint, then $|E \cup F| = |E| + |F|$
2. If $(A_i)_{i \in [n]}$ is a partition of E then $|E| = |A_1| + \dots + |A_n|$
3. $|E \times F| = |E| \times |F|$
4. $|F^E| = |F|^{|E|}$ where F^E denotes the set of all applications from E to F
5. $|\mathcal{P}(E)| = 2^{|E|}$

Prove these properties.

Example: Let n be the number of possible words coded in 16 bits. Each word is a sequence of 0s and 1s of length 16, and can be considered as an application: $[16] \rightarrow \{0, 1\}$. Therefore, $n = 2^{16} = 65536$.

3.2 Countable sets

The notion of cardinality can be extended to infinite sets, such that the following properties can be verified by any two sets E and F .

- $|E| \leq |F| \leftrightarrow$ there exists an injection from E to F
- $|E| \geq |F| \leftrightarrow$ there exists a surjection from E to F
- $|E| = |F| \leftrightarrow$ there exists a bijection from E to F

Deduce from the above that if there exist both an injection and a surjection, then there exists a bijection.

Countability:

- A set E is countable if there exists a bijection from E to \mathbb{N} (or reversely).
- ω denotes the cardinal of \mathbb{N}
- a union $\bigcup_{i \in I} A_i$ is countable if I is countable
- Countable sets satisfy the following properties:
 - all subsets of a countable set is either finite or countable
 - all cartesian product of countable sets is countable
 - all countable union of countable sets is countable

Show that $\mathbb{N} \times \mathbb{N}$ is countable.

4 Operations and relations

An operation over a set E is an application $\Psi : E^n \rightarrow E$. n is called the arity of Ψ , and denoted $a(\Psi)$. We say that Ψ is a n -ary operation. In the following we mostly review binary operations, i.e., operations of arity 2 ($n = 2$).

4.1 Binary operations

A binary operation $*$ over a set E is an application: $E \times E \rightarrow E$. The image of a couple (x, y) is denoted $x * y$. In addition, there are the following properties:

- $*$ is associative iff $\forall a, b, c \in E, a * (b * c) = (a * b) * c$
- $*$ is commutative iff $\forall a, b \in E, a * b = b * a$
- $*$ has a neutral element e iff $\forall a \in E, a * e = e * a = a$

Semi-group, monoid:

- A set E with an associative operation $*$ is a semi-group.
- A semi-group E whose operation has a neutral element is a monoid.
- A semi-group E whose operation is commutative is a commutative semi-group.

Examples:

- \mathbb{N} with the addition and the neutral element 0, is a commutative monoid.
- \mathbb{N} with the multiplication and the neutral element 1, is a commutative monoid.
- $\mathcal{P}(E)$ with the union (or the intersection) is a commutative monoid.
- the set of square matrices with real coefficients is a monoid for the multiplication of matrices, but it is not commutative.

Group:

- A monoid E with the operation $*$ is a group if all element in E has an inverse, i.e., $\forall a \in E, \exists b \in E$ such that $a * b = b * a = e$ where e is the neutral element for $*$.
- If in addition $*$ is commutative, E is a commutative group.

Examples:

- $(\mathbb{Z}, +)$ is a commutative set
- The set of square matrices with an inverse is a group for $*$, but not commutative

4.2 Relations

A relation over a set E is a subset \mathcal{R} of $E \times E$.

Examples:

- Let $E = \mathbb{N}$, the following sets are relations:
 - $\{(n, m) \mid n \leq m\}$
 - $\{(n, m) \mid n \leq m \leq 2n\}$
 - $\{(n, m) \mid n \leq m \text{ and } \exists k : n^2 + m^2 = k^2\}$
- Over $E = \mathcal{P}(A)$, inclusion is a relation.

4.3 Set operations over relations

Since a relation is a set, then we can define unions, intersections, etc. on them:

- $\overline{\mathcal{R}}$: $(e, e') \in \overline{\mathcal{R}} \leftrightarrow (e, e') \notin \mathcal{R}$
- $\mathcal{R}_1 \cup \mathcal{R}_2$: $(e, e') \in \mathcal{R}_1 \cup \mathcal{R}_2 \leftrightarrow (e, e') \in \mathcal{R}_1 \vee (e, e') \in \mathcal{R}_2$
- $\mathcal{R}_1 \cap \mathcal{R}_2$: $(e, e') \in \mathcal{R}_1 \cap \mathcal{R}_2 \leftrightarrow (e, e') \in \mathcal{R}_1 \wedge (e, e') \in \mathcal{R}_2$

Similarly, we can also define:

- the empty relation, \emptyset_E : $\forall e, e' \in E, (e, e') \notin \emptyset_E$
- the full relation, \prod_E : $\forall e, e' \in E, (e, e') \in \prod_E$
- the identity relation, Id_E : $\forall e, e' \in E, (e, e') \in Id_E \leftrightarrow e = e'$

And then:

- $\mathcal{R}_1 \subseteq \mathcal{R}_2$ iff $\forall e, e' \in E, (e, e') \in \mathcal{R}_1 \rightarrow (e, e') \in \mathcal{R}_2$

4.4 Other operations over relations

- inverse relation \mathcal{R}^{-1} : $e\mathcal{R}^{-1}e' \leftrightarrow e'\mathcal{R}e$
- product of relations $\mathcal{R}_1.\mathcal{R}_2$: $e(\mathcal{R}_1.\mathcal{R}_2)e' \leftrightarrow \exists e'', e\mathcal{R}_1e'' \wedge e''\mathcal{R}_2e'$
The product of relations is associative. Its neutral element is Id_E .
- $\mathcal{R}^* = Id_E \cup \mathcal{R} \cup (\mathcal{R}.\mathcal{R}) \cup \dots = \bigcup_{i \geq 0} \mathcal{R}^i$ with $\mathcal{R}^0 = Id_E$
- $\mathcal{R}^{i+j} = \mathcal{R}^i.\mathcal{R}^j$

4.5 Some properties of binary relations

A relation \mathcal{R} is:

- **reflexive**: if $\forall e \in E, e\mathcal{R}e$
- **irreflexive**: if $\forall e, e' \in E, e\mathcal{R}e' \Rightarrow e \neq e'$
- **symmetric**: if $\forall e, e' \in E, e\mathcal{R}e' \Rightarrow e'\mathcal{R}e$
- **anti-symmetric**: if $\forall e, e' \in E, e\mathcal{R}e'$ and $e'\mathcal{R}e \Rightarrow e' = e$
- **transitive**: if $\forall e, e', e'' \in E, e\mathcal{R}e'$ and $e'\mathcal{R}e'' \Rightarrow e\mathcal{R}e''$

4.6 Equivalence relations

An equivalence relation is a relation that is reflexive, symmetric and transitive.

Let \mathcal{R} be an equivalence relation over E , and let $e \in E$. The set defined by $\{e' \in E \mid e\mathcal{R}e'\}$ is usually denoted by $[e]_{\mathcal{R}}$, and is called the equivalence class of e .

Example:

- The identity relation over E , denoted Id_E , is an equivalence relation.
- Let n be an integer ≥ 2 . The relation over \mathbb{Z} defined by: “the remainder of x/n is equal to the remainder of y/n ” is an equivalence relation. It is denoted as $x \equiv y[n]$, or $x = y \pmod n$.

Properties:

1. The intersection $\mathcal{R} \cap \mathcal{R}'$ of two equivalence relations, is an equivalence relation.
2. Let \mathcal{R} be a relation. Then $(\mathcal{R} \cup \mathcal{R}^{-1})$ is an equivalence relation, and it is the smallest equivalence relation containing \mathcal{R} .
3. Let \mathcal{R} be an equivalence relation. Then:
 - (a) $\forall e \in E, e \in [e]_{\mathcal{R}}$
 - (b) $\forall e, e' \in E, e\mathcal{R}e' \Rightarrow [e]_{\mathcal{R}} = [e']_{\mathcal{R}}$
 - (c) if $[e]_{\mathcal{R}} \cap [e']_{\mathcal{R}} \neq \emptyset$ then $[e]_{\mathcal{R}} = [e']_{\mathcal{R}}$
 - (d) As a result of the above, the set $\{[e]_{\mathcal{R}} \mid e \in E\}$ of subsets of E is a partition of E .

4.7 Congruence

An equivalence relation \mathcal{R} over a set E with an operation $*$ is a congruence if it is compatible with $*$, i.e.,

$$\forall e, e', d, d' \in E, (e\mathcal{R}e' \text{ and } d\mathcal{R}d') \Rightarrow (e * d)\mathcal{R}(e' * d')$$

Example: Let $n \geq 2$. The relation over \mathbb{Z} defined by $x \equiv y[n]$ is a congruence for $+$ and $*$.