

Chapter 1: Mathematical Background

This chapter consists of the material on set theory, induction, inductive definitions and recursion that will be required in later chapters.

Copyright © 2003–8 Alley Stoughton

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

The \LaTeX source of these slides, the associated book, and the distribution of the Forlan toolset are available on the WWW at <http://people.cis.ksu.edu/~stough/forlan/>.

1

1.1: Basic Set Theory

In this section, we will cover the material on sets, relations, functions and data structures that will be needed in what follows. Much of this material should be at least partly familiar.

1.1.1: Sets of Numbers

We write:

- \mathbb{N} for the set $\{0, 1, \dots\}$ of all natural numbers;
- \mathbb{Z} for the set $\{\dots, -1, 0, 1, \dots\}$ of all integers;
- \mathbb{R} for the set of all real numbers.

2

1.1.2: Relationships between Sets

Sets A and B are equal ($A = B$) iff (if and only if) they have the same elements, i.e., for all x , $x \in A$ iff $x \in B$.

Suppose A and B are sets. We say that:

- A is a *subset* of B ($A \subseteq B$) iff, for all $x \in A$, $x \in B$;
- A is a *proper subset* of B ($A \subsetneq B$) iff $A \subseteq B$ but $A \neq B$.

For example, $\emptyset \subsetneq \mathbb{N}$, $\mathbb{N} \subseteq \mathbb{N}$ and $\mathbb{N} \subsetneq \mathbb{Z}$.

We also have the notions of superset ($A \supseteq B$) and proper superset ($A \supsetneq B$).

3

1.1.3: Set Formation

We will make extensive use of the $\{\dots | \dots\}$ notation for forming sets. Let's consider two representative examples of its use.

Let

$$A = \{n \mid n \in \mathbb{N} \text{ and } n^2 \geq 20\} = \{n \in \mathbb{N} \mid n^2 \geq 20\}.$$

Then, for all n ,

$$n \in A \quad \text{iff} \quad n \in \mathbb{N} \text{ and } n^2 \geq 20.$$

Is $5 \in A$? Yes— $5 \in \mathbb{N}$ and $5^2 \geq 20$.

Is $5.5 \in A$? No— $5.5 \notin \mathbb{N}$.

Is $4 \in A$? No— $4^2 \not\geq 20$.

4

1.1.3: Set Formation (Cont.)

Let

$$B = \{n^3 + m^2 \mid n, m \in \mathbb{N} \text{ and } n, m \geq 1\}.$$

Then, for all l ,

$$l \in B \text{ iff } l = n^3 + m^2, \text{ for some } n, m \text{ such that } n, m \in \mathbb{N} \text{ and } n, m \geq 1$$

$$\text{iff } l = n^3 + m^2, \text{ for some } n, m \in \mathbb{N} \text{ such that } n, m \geq 1.$$

Is $9 \in B$? To answer “yes”, we must show

$$9 = n^3 + m^2 \text{ and } n, m \in \mathbb{N} \text{ and } n, m \geq 1,$$

for some values of n, m . Yes— $9 = 2^3 + 1^2$ and $2, 1 \in \mathbb{N}$ and $2, 1 \geq 1$.

5

1.1.3: Set Formation (Cont.)

Given $n, m \in \mathbb{Z}$, we write $[n : m]$ for $\{l \in \mathbb{Z} \mid l \geq n \text{ and } l \leq m\}$.

Thus $[n : m]$ is all of the integers that are at least n and no more than m .

For example, $[-2 : 1]$ is $\{-2, -1, 0, 1\}$ and $[3 : 2]$ is \emptyset .

6

1.1.4: Operations on Sets

Recall the following operations on sets A and B :

$$\begin{aligned}A \cup B &= \{x \mid x \in A \text{ or } x \in B\} && \text{(union)} \\A \cap B &= \{x \mid x \in A \text{ and } x \in B\} && \text{(intersection)} \\A - B &= \{x \in A \mid x \notin B\} && \text{(difference)} \\A \times B &= \{(x, y) \mid x \in A \text{ and } y \in B\} && \text{(product)} \\\mathcal{P}A &= \{X \mid X \subseteq A\} && \text{(power set).}\end{aligned}$$

$A - B$ is formed by removing the elements of B from A , if necessary.

For example, $\{0, 1, 2\} - \{1, 4\} = \{0, 2\}$.

$A \times B$ consists of all ordered pairs (x, y) , where x comes from A and y comes from B . For example,

$\{0, 1\} \times \{1, 2\} = \{(0, 1), (0, 2), (1, 1), (1, 2)\}$. We can also write

$A \times B \times C$, etc.

Finally, $\mathcal{P}A$ consists of all of the subsets of A . For example,

$\mathcal{P}\{0, 1\} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

7

(1.1.4) Generalized Union and Intersection

If X is a set of sets, then the *generalized union* of X ($\bigcup X$) is

$$\{a \mid a \in A, \text{ for some } A \in X\}.$$

For example

$$\bigcup\{\{0, 1\}, \{1, 2\}, \{2, 3\}\} = \{0, 1, 2, 3\} = \{0, 1\} \cup \{1, 2\} \cup \{2, 3\},$$

$$\bigcup \emptyset = \emptyset.$$

If X is a *nonempty* set of sets, then the *generalized intersection* of X ($\bigcap X$) is

$$\{a \mid a \in A, \text{ for all } A \in X\}.$$

For example

$$\bigcap\{\{0, 1\}, \{1, 2\}, \{2, 3\}\} = \emptyset = \{0, 1\} \cap \{1, 2\} \cap \{2, 3\}.$$

8

1.1.5: Relations and Functions

A *relation* R is a set of ordered pairs. The *domain* of a relation R ($\mathbf{domain} R$) is $\{x \mid (x, y) \in R, \text{ for some } y\}$, and the *range* of R ($\mathbf{range} R$) is $\{y \mid (x, y) \in R, \text{ for some } x\}$. We say that R is a *relation from* a set X to a set Y iff $\mathbf{domain} R \subseteq X$ and $\mathbf{range} R \subseteq Y$, and that R is a *relation on* a set A iff $\mathbf{domain} R \cup \mathbf{range} R \subseteq A$. We often write $x R y$ for $(x, y) \in R$.

Consider the relation

$$R = \{(0, 1), (1, 2), (0, 2)\}.$$

Then, $\mathbf{domain} R = \{0, 1\}$, $\mathbf{range} R = \{1, 2\}$, R is a relation from $\{0, 1\}$ to $\{1, 2\}$, and R is a relation on $\{0, 1, 2\}$.

9

(1.1.5) Properties of Relations

A relation R is:

- *reflexive on* a set A iff, for all $x \in A$, $(x, x) \in R$;
- *transitive* iff, for all x, y, z , if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$;
- *symmetric* iff, for all x, y , if $(x, y) \in R$, then $(y, x) \in R$;
- a *function* iff, for all x, y, z , if $(x, y) \in R$ and $(x, z) \in R$, then $y = z$.

Is $R = \{(0, 1), (1, 2), (0, 2)\}$ reflexive on $\{0, 1, 2\}$? No— $(0, 0) \notin R$.

Is R transitive? Yes; since $(0, 1), (1, 2) \in R$, $(0, 2) \in R$ required.

Is R symmetric? No— $(0, 1) \in R$, but $(1, 0) \notin R$.

Is R a function? No— $(0, 1) \in R$ and $(0, 2) \in R$.

(1.1.5) More on Functions

The relation

$$f = \{(0, 1), (1, 2), (2, 0)\}$$

is a function.

If f is a function and $x \in \mathbf{domain} f$, we write $f x$ for the *application* of f to x , i.e., the unique y such that $(x, y) \in f$. We say that f is a *function from* a set X to a set Y iff f is a function, $\mathbf{domain} f = X$ and $\mathbf{range} f \subseteq Y$. We write $X \rightarrow Y$ for the set of all functions from X to Y .

For the f defined above, we have that $f 0 = 1$, $f 1 = 2$, $f 2 = 0$, f is a function from $\{0, 1, 2\}$ to $\{0, 1, 2\}$, and $f \in \{0, 1, 2\} \rightarrow \{0, 1, 2\}$.

11

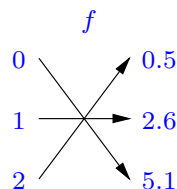
(1.1.5) Bijections

A *bijection* f from a set X to a set Y is a function from X to Y such that, for all $y \in Y$, there is a unique $x \in X$ such that $(x, y) \in f$.

For example,

$$f = \{(0, 5.1), (1, 2.6), (2, 0.5)\}$$

is a bijection from $\{0, 1, 2\}$ to $\{0.5, 2.6, 5.1\}$. We can visualize f as a one-to-one correspondence between these sets:



12

1.1.6: Set Cardinality

We say that a set X has the *same size* as a set Y ($X \cong Y$) iff there is a bijection from X to Y . It's not hard to show that for all sets X, Y, Z :

- $X \cong X$;
- If $X \cong Y \cong Z$, then $X \cong Z$;
- If $X \cong Y$, then $Y \cong X$.

13

(1.1.6) Finite and Infinite Sets

A set X is *finite* iff $X \cong [1 : n]$, for some $n \in \mathbb{N}$; otherwise X is *infinite*.

A set X is *countably infinite* iff $X \cong \mathbb{N}$.

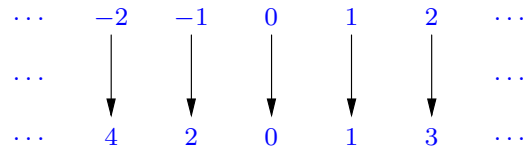
A set X is *countable* iff X is either finite or countably infinite; otherwise X is *uncountable*.

Every set X has a *size* or *cardinality* ($|X|$) and we have that, for all sets X and Y , $|X| = |Y|$ iff $X \cong Y$. The sizes of finite sets are natural numbers.

14

(1.1.6) Set Size Examples

- The sets \emptyset and $\{0.5, 2.6, 5.1\}$ are finite, and are thus also countable;
- The sets \mathbb{N} , \mathbb{Z} , \mathbb{R} and $\mathcal{P}\mathbb{N}$ are infinite;
- The set \mathbb{N} is countably infinite, and is thus countable;
- The set \mathbb{Z} is countably infinite, and is thus countable, because of the existence of the following bijection:



- The sets \mathbb{R} and $\mathcal{P}\mathbb{N}$ are uncountable.

15

1.1.7: Data Structures Booleans

$\mathbf{Bool} = \{\mathbf{true}, \mathbf{false}\}$.

We have the usual negation (**not**), conjunction (**and**) and disjunction (**or**) operations on booleans.

16

(1.1.7) Options

Option $X = \{\text{none}\} \cup \{\text{some } x \mid x \in X\}$.

For example, **Option Bool** = $\{\text{none}, \text{some true}, \text{some false}\}$.

We could define a function $f \in \mathbb{N} \times \mathbb{N} \rightarrow \mathbf{Option\ Bool}$ by:

$$f(n, m) = \begin{cases} \text{none}, & \text{if } m = 0, \\ \text{some true} & \text{if } m \neq 0 \text{ and } n = ml \text{ for some } l \in \mathbb{N}, \\ \text{some false} & \text{if } m \neq 0 \text{ and } n \neq ml \text{ for all } l \in \mathbb{N}. \end{cases}$$

17

(1.1.7) Lists

A *list* is a function with domain $[1 : n]$, for some $n \in \mathbb{N}$.

For example \emptyset is a list, as it is a function with domain $\emptyset = [1 : 0]$.

And $\{(1, 3), (2, 5), (3, 7)\}$ is a list, as it is a function with domain $[1 : 3]$.

We abbreviate a list $\{(1, x_1), (2, x_2), \dots, (n, x_n)\}$ to $[x_1, x_2, \dots, x_n]$.

Thus \emptyset and $\{(1, 3), (2, 5), (3, 7)\}$ are abbreviated to $[]$ and $[3, 5, 7]$.

$|\cdot|$ doubles as list *length*.

$f @ g$ is list concatenation. E.g., $[2, 3, 4] @ [5, 6] = [2, 3, 4, 5, 6]$.

Concatenation is associative $(f @ g) @ h = f @ (g @ h)$ and has $[]$ as its identity ($[] @ f = f = f @ []$).

List X is all X -lists, i.e., all lists whose elements come from X .

18