CAB203 Discrete Structures

Lecture Notes

Jack Girard 2023

Contents

1 What is Mathematics?

1.1 What is Mathematics?

1.1.1 Abstraction

Abstraction can be used to simplify a problem by ignoring all the information that is not needed. They capture the relevant properties of a situation, and the relationships between them. Those properties can then be used to work out the solution.

- You have x apples
- You have y friends
- Are there enough apples for all your friends?

The usual abstraction for problems involving counting is *natural numbers* (non-negative integers). By abstracting away irrelevant properties such as size, shape, colour etc. the problem can be simplified to:

$$x \geq y?$$

Limitations of abstractions can include:

- Not enough information
- Too much information
- Incorrect information

1.1.2 Mathematical Theories

An abstraction without reference to a particular problem is called a *mathematical theory*, usually consisting of:

- Mathematical objects (numbers, operations, etc.)
- Axioms (statements about how objects relate to each other)

1.1.3 Axioms

Some examples of axioms for the natural numbers include:

1. 0 is a natural number
2. $x = x$
3. if $x = y$ then $y = x$
4. if $x = y$ and $y = z$ then $x = z$
5. if $x = w$ then w is a natural number
6. $S(x)$ is a natural number
7. if $S(x) = S(y)$ then $x = y$
8. $S(x) = 0$ is always false

Axioms can be combined to create new true statements. For example, axiom 6 in the list above states $S(x)$ is a natural number, so by combining it with itself it can be deduced that $S(S(x))$ is also a natural number.

Note

S refers to the *successor function* that increments a natural number.

$$S(x) = x + 1$$

1.1.4 Mathematical Objects

Mathematical objects are abstract objects that can correspond to concrete objects. They can only be defined in how they relate to other objects - this is done through axioms. Formally, objects are just symbols. They have no meaning, and are just names.

Relationships between objects are given by *propositions*. Propositions are statements that can be true or false. Axioms are propositions that assert to be true for objects in the mathematical theory.

1.1.5 Models

A mathematical theory can apply to a real situation if:

- Every object in the theory matches up to something in the real situation (at least hypothetically)
- All axioms in the theory remain true in the real situation

If this can be done, the real situation can be defined as a *model* for the theory.

Another instance of a model is a *mathematical model*. This type of model is an abstraction of a particular system to be studied and analysed in a mathematical way, and is the primary focus of this course when referring to "model".

1.1.6 Truth in Mathematics

Statements in mathematics are always relative to a particular mathematical theory. A statement may be true in one theory and false in another.

- For example, $ab = ba$ is true for real numbers, but not for matrices.

A true statement in a theory is irrelevant to a real situation, **unless** it is a model for that theory. The rules of logic guarantee that true statements in a theory are also true in every model of the theory.

Note

It is possible for every statement in a theory to be true **and** false. This is called an *inconsistent* theory and cannot have any models.

1.2 Modular Arithmetic

1.2.1 Mathematical Definitions

A mathematical definition creates a short name for some concept. This is purely for brevity and does not express new things. In definitions, italics are used to emphasise the words that are being defined.

1.2.2 "Divides"

A mathematical definition for "divides" is as follows:

Divides Definition

Let a, b be integers. If there is another integer c such that $ac = b$, then it can be said that a *divides* b, written as $a|b$. Equivalently, it can also be said that b is *divisible* by a.

This definition states all the following are true:

- $a|b$
- a divides b
- b is divisible by a
- There is some integer c such that $ac = b$

1.2.3 Modular Arithmetic and Equivalence

For any positive integer n, it can have arithmetic modulo n. Modular arithmetic replaces equality with *modular equivalence*. a mathematical definition for modular equivalence is as follows:

Modular Equivalence Definition

if $n|(a-b)$, then a and b are *equivalent modulo* n, written as

$$a \equiv b \pmod{n}$$

Modular equivalence carries similar properties to addition, subtraction, and multiplication. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$

1.2.4 Mod Operator

The mod operator is used to perform modular arithmetic. A mathematical definition for the operator is as follows:

Mod Operator Definition

$a \bmod n$ is the smallest non-negative b such that $a \equiv b \pmod{n}$

Equivalently, $a \bmod n$ is the remainder you get when you divide a by n. In most programming languages, the mod operator is denoted by %.

1.2.5 Example: Proving Lemma

Lemma

Let a and b be integers. If $a \bmod b = 0$, then $b|a$.

This lemma can be proven using previously stated definitions:

$$a \bmod b = 0 \text{ is the same as } a \equiv 0 \pmod{b}.$$
$$a \equiv 0 \pmod{b} \text{ is the same as } b|(a-0).$$
$$a - 0 = a \text{ therefore } b|a.$$

This example is often used in programming to determine divisibility, or test if a number is even.

1.3 Exponents and Logarithms

2 Data Representation