Basic mathematics as prerequisites for TLA+

Dr. Tianxiang Lu

March 20, 2015

1 Introduction

This lecture/note introducing the basic knowledge of mathematical reasoning. After this course, you will be able to understand the principle of modeling data in TLA+.

1.1 Warm up

You have two ropes. Each takes exactly 60 minutes to burn. They are made of different material so even though they take the same amount of time to burn, they burn at separate rates. In addition, each rope burns inconsistently. How do you measure out exactly 45 minutes? (Try to use your brain instead of google to solve this, in case you have not heard about the solution)

2 Numbers

2.1 Natural Numbers

The **natural numbers** $\mathbb{N}$ are all the numbers for counting things, i.e.,[1]

$$0, 1, 2, 3, \ldots$$

2.2 Integers

The **integers** $\mathbb{Z}$ are the positive and negative counting numbers, i.e.,

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Definition 1 (Dichotomy of Parity)**.** A number is **even** if it can be evenly divided by 2, i.e.,

$$\ldots, -4, -2, 0, 2, 4, \ldots$$

A number is **odd** if it is not even.

2.3 Rational Numbers

The **rational numbers** $\mathbb{Q}$ are the fractions, i.e.,

$$\frac{a}{b}$$

where a and b are integers, and b is nonzero.

2.4 Real Numbers

The **real numbers**$\mathbb{R}$ are all the decimals. This includes rational and **irrational** numbers, e.g., π, e, $\ln(2)$, $\sqrt[3]{2}$.

[1] In our lecture and in standard TLA+ context, 0 is a natural number.

3 Inequalities

3.1 Function

Definition 2. A **function** is an assignment, which assigns every value on its domain to exactly one value in its image. These are normally (although do not need to be given) by a rule, or explicit assignment.

Example 1. An example of a real-valued function is $f(x)$ given by the rule

$$f(x) := x^2$$

This function takes in a real value, and then squares it.

A non-example of a real-value function is

$$f(x)^2 := x$$

Some functions you might be familiar with are

- Polynomials: $f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$
- Trig function: $\sin(x), \cos(x), \tan(x)$.
- Exponential functions: $f(x) := a^x$

4 Propositional logic

A **proposition** is a statement or sentence that can be either true or false. A **propositional variable** is a variable having the value either true (T) or false (F), which we also call **boolean** values. The table below summarizes the main tools for symbolic logic:

Logic Statement	Symbolic Notation
NOT(p)	$\neg p$ (equivalently $\overline{p}$)
p AND q	$p \wedge q$
p OR q	$p \vee q$
IF p THEN q	$p \to q$
p IF AND ONLY IF q	$p \equiv q$

We can show that two statements, such as $\neg(p \vee q)$ and $\neg p \wedge \neg q$, are equivalent by evaluating a truth table and showing that every row has the same outcome. If there are n propositional variables, a truth table will have 2^n rows and so this process can become tedious quickly.

We can instead do algebraic manipulation of statements using these rules:

- Commutativity and associativity of AND and OR:

$$\begin{aligned} p \wedge q &\equiv q \wedge p && \text{(similar for OR)} \\ (p \vee q) \vee r &\equiv p \vee q \vee r \equiv p \vee (q \vee r) && \text{(similar for AND)} \end{aligned}$$

- Identity and zero for AND and OR:

$$\begin{aligned} \mathrm{T} \wedge p &\equiv p & \qquad \mathrm{F} \wedge p &\equiv \mathrm{F} \\ \mathrm{F} \vee p &\equiv p & \qquad \mathrm{T} \vee p &\equiv \mathrm{T} \end{aligned}$$

- Distributivity of AND over OR:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

- DeMorgan's law for distributing NOT over AND or OR:

$$\begin{aligned} \neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q \end{aligned}$$

5 A bit first-order logic

A **predicate** is a statement that contains 1 or more variables and becomes a proposition when the variable is replaced with an object. For example, we can form predicates $P(x)$ and $W(x)$ to mean "x is a philosopher" and "x is wise" respectively.

An assertion that a predicate is *sometimes* true is called an **existential quantification**, which uses the "exists" notation. Examples include
$(\exists x \in \mathbb{R})\ x^2 + 1 = 7$ or $(\exists x)\ P(x) \wedge W(x)$ or "There are PhD students currently enrolled in the TLA+ lecture."

An assertion that a predicate is *always* true is called a **universal quantification**, which uses the "for-all" notation. Examples include
$(\forall x \in \mathbb{R})\ x^2 + 1 \geq 0$ or $(\forall x)\ P(x) \rightarrow W(x)$ or "Every student in TLA+ lecture is intelligent."

The domain of discourse refers to the set of objects over which the variables x, y, etc can range. It is important to specify the domain because, as an example, the statement $(\exists x)\ x^2 = 2$ is true if the domain is the real numbers, $\mathbb{R}$, but is false if the domain is the natural numbers, $\mathbb{N}$. If no domain is explicitly given, then we assume that the statements exist in the universal domain of all objects.

The order of quantifiers matters if there is more than one variable involved. Notice that the statement:
$(\forall x \in \mathbb{N})\ (\exists a, b, c, d \in \mathbb{N})\ x = a^2 + b^2 + c^2 + d^2$ is true since any positive integer can be written as the sum of four squares, but the statement:
$(\exists a, b, c, d \in \mathbb{N})\ (\forall x \in \mathbb{N})\ x = a^2 + b^2 + c^2 + d^2$ is false since it is certainly not the case that every positive integer is the sum of *the same* four square numbers.

6 Sets

Set theory is a branch of mathematics that has its origins in the late 19th century. The "Father of Set Theory" was Georg Cantor.

6.1 A Definition

In **naïve set theory**, a set is simply a collection of objects, without formalizing exactly what we can do with these collections. Naïve set theory fails to be a sound system that we want to work in, which led to greater rigor. The contemporary system of set theory is called **ZFC**, which stands for **Z**ermelo-**F**raenkel Set Theory with **C**hoice.

6.2 Membership

The characteristic function of a set is used to ask the yes/no question: is x a member of A? In fact we have the following principle:

Definition 3 (Principle of Extensionality)**.** Two sets A and B are the same if they have exactly the same members.

If A is a set and x is some object, asking the question "Is x a member of A?" is denoted:

$$x \in A$$

This is an **atom**, having a boolean value (either true or false), and it's truth can be checked independently from all other claims. Note that

$$\{1, 1\} = \{1\}$$

and

$$\{1, 2\} = \{2, 1\}$$

6.3 The Empty Set

A set that has absolutely no items in it is called the **empty set**, written $\emptyset$. We have

$$\forall x \,.\, \neg(x \in \emptyset)$$

6.4 Subset

A is a **subset** of B, if every member of A a member of B

$$A \subseteq B \equiv \forall x \mathbf{.} x \in A \to x \in B$$

6.5 Equality

Two sets are equal if they are subset of each other.

$$(x \subseteq A) \land (x \subseteq B) \equiv \forall x \mathbf{.} x \in A \leftrightarrow x \in B$$

7 Operations on Sets

If we have two sets, we have several operations we can perform on them.

7.1 Unions

Given two collections of objects, we can perform a **union**, which joins the sets together. So, the union of A and B is just the things that is in A and the things that are in B. We write

$$A \cup B$$

as the union of A and B (in LaTeX, this symbol is \cup).

Another way to define an operation is to say exactly what the answer to $x \in A \cup B$ is, given you know the answers that A and B give. In this case, the definition looks like

$$\forall x \mathbf{.} x \in A \cup B \equiv (x \in A \lor x \in B)$$

Example 2. The union of $\{2, 4, 74\}$ and $\{4, 7, 12\}$ is

$$\{2, 4, 7, 12, 74\}$$

7.2 Intersections

Given two collection of objects, we can perform a **intersection**, which meets the sets. The intersection of A and B is the things that are in both A and B. We write this

$$A \cap B$$

(in LaTeX, this symbol is \cap)

Speaking logically, the definition looks like

$$\forall x \mathbf{.} x \in A \cap B \longleftrightarrow (x \in A \land x \in B)$$

Example 3. The intersection of $\{2, 4, 74\}$ and $\{4, 7, 12\}$ is

$$\{4\}$$

The intersection of $\{2, 4, 6\}$ and $\{1, 3, 5\}$ is

$$\emptyset$$

7.3 Relative Complements

Due to the lack of formal definition of universe, the definition of complement of a set is vague. Therefore, we introduce **relative complement** or **set difference**. The set difference$A \setminus B$ [2], which we say A take away B or A minus B, is the things which are in A but not in B.

$$\forall x \,.\, (x \in A \setminus B) \equiv ((x \in A) \wedge (x \notin B))$$

7.4 Powersets

We learn a new way to make a set out of another set. This is another way to form sets which is simply conjectured by the rules of set theory.

Definition 4. The **powerset** of a set A, denoted $\wp(A)$, is the set of all subsets of A.

Example 4. Let $A = \{1, 2, 3\}$. Then

$$\wp(A) = \{\, \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\} \,\}$$

Theorem 1. *For any set A, we have $\wp(A) \neq \emptyset$.*

Proof. To show $\wp(A) \neq \emptyset$, we need only show that $\wp(A)$ has a member. In other words, we need to show that A has a subset. Well, as stated, $\emptyset \subseteq X$ for any set X, therefore $\emptyset \subseteq A$. So $\emptyset \in \wp(A)$, so $\wp(A)$ is nonempty. □

Theorem 2.

$$\wp(A \cap B) = \wp(A) \cap \wp(B)$$

Proof. ($\subseteq$) Take $X \in \wp(A \cap B)$. Then $X \subseteq A \cap B$. As $X \subseteq A \cap B$ we know ever member of X is in A, so $X \subseteq A$; similar ever member of X is in B so $X \subseteq B$. Therefore $X \in \wp(A)$ and $X \in \wp(B)$, so $X \in \wp(A) \cap \wp(B)$.

($\supseteq$) Take $X \in \wp(A) \cap \wp(B)$. Then $X \in \wp(A)$ and $X \in \wp(B)$. Thus $X \subseteq A$ and $X \subseteq B$. We want to show that $X \in \wp(A \cap B)$, ie. $X \subseteq A \cap B$. So, take $x \in X$ arbitrary. As $X \subseteq A$ we know $x \in A$, and similar as $X \subseteq B$ we know $x \in B$. Therefore, $x \in A \cap B$, which is what we wanted. □

7.5 Cartesian Product

Definition 5. The **Cartesian Product** or sets A and B, denoted $A \times B$ (spoken as A cross B) is the set of ordered pairs, where the first coordinate comes from A and the second from B. That is, if $x \in A$ and $y \in B$ then

$$(x, y) \in A \times B$$

Example 5.

$$[3] \times [2] = \{\, (1,1), (2,1), (3,1), (1,2), (2,2), (3,2) \,\}$$

Therefore the notation for the Cartesian Plane is $\mathbb{R} \times \mathbb{R}$.

Remark 1. Ordered pairs can be compared; $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Definition 6. Equivalence relations are meant to capture the properties of equality on sets. $\sim$ is an equivalence relation on a set A if and only if it is

- Reflexive: $\forall a \in A \,.\, a \sim a$.
- Symmetric: $\forall a, b \in A \,.\, (a \sim b) \to (b \sim a)$.
- Transitive: $\forall a, b, c \in A \,.\, ((a \sim b) \wedge (b \sim c)) \to (a \sim c)$.

[2] In LaTeX, this is \setminus

7.6 Properties of Function

- A domain: the function only allows inputs from this set, and gaurentees for each input there will be only one, unique output. In the above, the domain is A.
- A codomain: the function promises that all outputs will lie here. In the above, the codomain is B.
- The image: these are the values of the function that that function will actually hit in the codomain.

There's some very basic properties of the image and preimage that we will not prove, but you should check:

Theorem 3. *If $f : A \to B$ then*

1. $f[A] \neq \emptyset$.
2. $f^{-1}[B] \neq \emptyset$.

A very useful property of the pre-image is the following

Theorem 4. *If $f : A \to B$ and $X, Y \subseteq B$ then*

$$f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y]$$

Proof. ($\subseteq$) Take an $x \in f^{-1}[X \cap Y]$. Then we know there is some $y \in X \cap Y$ such that $f(x) = y$. As $y \in X \cap Y$, we know it is in X and Y. Thus $x \in f^{-1}[X]$ and $x \in f^{-1}[Y]$ as there is some element of X, namely y, that x hits, and similarly for y.

($\supseteq$) Take $x \in f^{-1}[X] \cap f^{-1}[Y]$. Then $x \in f^{-1}[X]$ and $x \in f^{-1}[Y]$. So we know there is some $y \in X$ such that $f(x) = y$ and some $z \in Y$ such that $f(x) = z$. But, as f is a function, $z = y$, so $y \in X \cap Y$. Therefore, as $f(x) = y$ we know $x \in f^{-1}[X \cap Y]$ □

Theorem 5. *If $f : A \to B$ and $X, Y \subseteq B$ then*

$$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y]$$

7.7 Injections

Definition 7. $f : A \to B$ is **injective** iff

$$\forall x, y \in A \,.\, x \neq y \to f(x) \neq f(y)$$

or, alternatively, by looking at the contrapositive

$$\forall x, y \in A \,.\, f(x) = f(y) \to x = y$$

7.8 Surjection

Definition 8. A function $f : A \to B$ is **surjective** or **onto** iff

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

7.9 Composition

Definition 9. If $f : A \to B$ and $g : C \to D$ and $B \subseteq C$ then the g **composed with** f is

$$g \circ f : A \to D$$

And this is defined by

$$(g \circ f)(x) = g(f(x))$$