0. MATH RECAP

Mihai-Valentin DUMITRU
mihai.dumitru2201@upb.ro

October 2024

AA is not a mathematics course, but we will be studying fields such as *"Computability Theory"* and *"Complexity Theory"* which can be considered branches of mathematics.

In our approach, we shall employ mathematical formalism and rigor to reach results that are *provably true*.

As such, it's important to recap the relevant mathematical concepts that are studied in the high school curriculum.

This is a short review of various already-familiar mathematical concepts that we consider a prerequisite for AA .

1 Boolean logic

There are two *values* in boolean logic: FALSE and TRUE.

We can operate directly on this values, or on variables which can take any value out of the two.

1.1 Operators

Boolean operations can be characterized by tables. For an operation with n *operands*, the first n columns correspond to each of the operands (represented by variables) and list all the possible combinations of boolean values. The last column represents the value of the operation for that particular combination of operand values.

- **Negation**:

x	$\neg x$ (read: "not x")
FALSE	TRUE
TRUE	FALSE

- **Conjunction**:

x	y	$x \wedge y$ (read: "x and y")
FALSE	FALSE	FALSE
FALSE	TRUE	FALSE
TRUE	FALSE	FALSE
TRUE	TRUE	TRUE

- **Disjunction**:

x	y	$x \vee y$ (read: "x or y")
FALSE	FALSE	FALSE
FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	TRUE

- **Exclusive disjunction**:

x	y	$x \oplus y$ (read: "x xor y")
FALSE	FALSE	FALSE
FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	FALSE

2 Sets

A set is commonly denoted as a comma-separated list, surrounded by braces. For example, consider the set:

$$S = \{18, 3, 29\}$$

The order of the contained objects is unimportant and each element can appear only once. The following is the same set as S:

$$T = \{29, 18, 3\}$$

Definition 0.1. A *"set"* is an **unordered** collection of **unique** objects.

We call the objects in a set its "members" or "elements".

Sets don't have to contain numbers, here are some example:

$$S_1 = \{\text{“}alpha\text{”}, \text{“}beta\text{”}, \text{“}gamma\text{”}, \text{“}delta\text{”}\}$$
$$S_2 = \{\{1, 3\}, \{4, 81, 32, 2\}, \{66\}\}$$
$$S_3 = \{\square, \triangle\}$$

There's a special set with no elements, called *"the empty set"*, usually denoted by $\emptyset$.

2.1 Operators

For a set S and an object a we can use the following operators:

- $a \in S$ – a is a member of S
- $a \notin S$ – a is not a member of S

For two sets A and B we can use the following relations:

- $A = B$ if the sets contain exactly the same objects
- $A \neq B$ if the sets are not equal
- $A \subseteq B$ ("A is a **subset** of B") if all objects in A are also in B
- $A \subsetneq B$ ("A is a **proper subset** of B") if all objects in A are also in B, but $A \neq B$, i.e. B also contains some other elements

We can also build new sets from existing ones:

- $A \cup B$: the *union*, the set with all objects that are either members of A or of B
- $A \cap B$: the *intersection*, the set with all objects that are members of both A and of B
- $A \setminus B$: the *difference*, the set with all objects that are members of A, but not of B
- $\overline{A}$: the *complement*, the set with all objects that are not in A.

  The complement is usually expressed in relation to a large superset of A that is the set of all possible objects; usually this is implicit in context.

2.2 Finite and infinite sets

Sets can contain either a finite number of objects, or be infinite.

For finite sets, we can describe them by explicitly listing their members; for infinite sets, that is not an option, but we can either use a "..." notation:

$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$
$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$$

or a notation that specifies that the set contains all objects satisfying some *predicate* (more about them in section 5):

$$E = \{n \mid n \text{ is even } \}$$
$$L = \{x \mid x \geq 1000\}$$

2.3 Powersets

Definition 0.2. The *powerset* of a set A is the set consisting of all the subsets of A.

The definition might seem a bit confusing, but hopefully an example can remedy this:

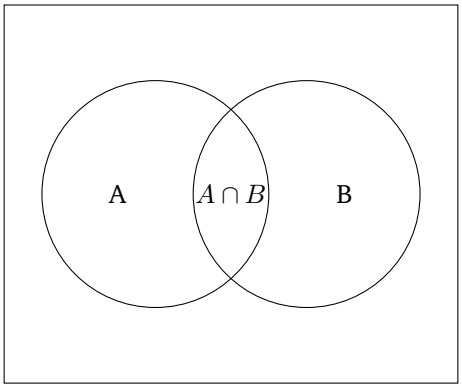
$$A = \{a, b, c\}$$
$$\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Note that the powerset is a set of sets.

The empty set is a member of any powerset because it is a subset of any set.

2.4 Set diagrams

Usually, it's helpful to visualize mathematical concepts. We can draw *set diagrams* to show how sets interact:

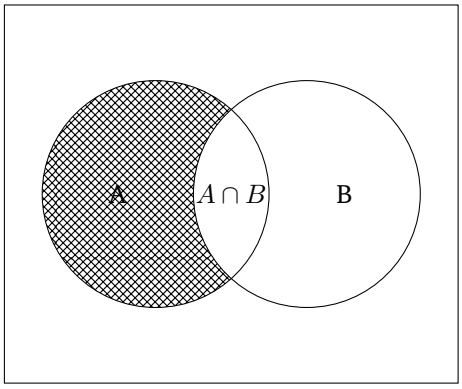


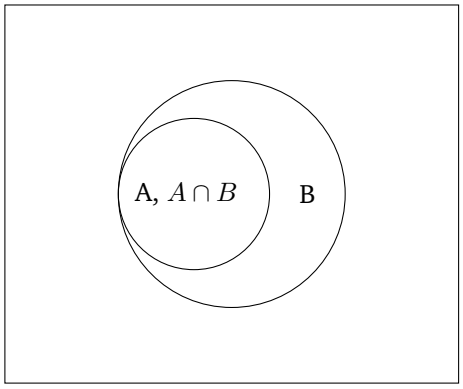
Here we can see several sets; for example:

- The circle on the left is set A
- The circle on the right is set B
- The region in the middle where the two circles overlap is their intersection: $A \cap B$
- The region outside both circles is the complement of their union: $\overline{A \cup B}$

However, two sets A and B may not intersect; or there might not be any part of A that is outside the intersection. We can illustrate this by either shading an area to show that it is empty, or simply not show it at all.

Below, you can see two ways of illustrating the case where $A \subsetneq B$:





3 Sequences

Sequences are denoted by a comma-separated list of items, surrounded by parentheses:

$$S = (16, 17, 18, 19, 20, 21)$$

Definition 0.3. A *sequence* is an ordered collection of objects.

Unlike sets, order matters. The sequence $S = (11, 34, 81)$ is different from $T = (34, 81, 11)$.

3.1 Tuples and infinite sequences

Like sets, sequences can be finite or infinite.

Definition 0.4. A *tuple* is a finite sequence. More precisely, a *k-tuple* is a finite sequence of k elements, for some $k \in \mathbb{N}$.
A *pair* is a 2-tuple.

We call $(13, 4)$ a pair. $(4, 6, 8)$ is a 3-tuple or a *triplet*. $(1, 2, 4, 8, 9, 0)$ is a 6-tuple.

3.2 Cartesian product of sets

Definition 0.5. For two sets A and B, their *Cartesian product* $A \times B$ is the set of all pairs (a, b), with $a \in A$ and $b \in B$.

Examples:

$$\{15, 16\} \times \{12, 141, 82\} = \{(15, 12), (15, 141), (15, 82), (16, 12), (16, 141), (16, 82)\}$$

4 Functions

Definition 0.6. A *function* is a mapping from the elements of a set A to those of a set B.

The notation expressing that "function f maps elements from A to elements of B" is:

$$f : A \to B$$

A is called *"the domain"*, while B is called *"the codomain"*. To denote the value of f for some particular object x, we write $f(x)$.

Functions always map **one** set to another, but for convenience, we can say a function *"takes k arguments"* when its argument is a k-tuple. In that case, the domain is the Cartesian product of some sets.

$$h : A \times B \to C$$

We will omit a couple of parentheses and always write $f(a, b)$ instead of $f((a, b))$.

The result of the function can also be a tuple, in which case the codomain is also a product of multiple sets:

$$j : \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$$

4.1 Representing functions

There are various ways to represent a function. For functions over finite domains, one option is to describe it explicitly, as a table with two columns:

Example:

$$f : \{1, 3, 23\} \to \{3, 7\}$$

x	f(x)
1	3
3	7
23	3

For functions over infinite domains, most often we shall use some mathematical formula:

$$g : \mathbb{N} \to \mathbb{N}$$
$$g(x) = 2x + 1$$

Here are some concrete mappings of g:

$g(0) = 1$

$g(1) = 3$

$g(2) = 5$

...

$g(17) = 35$

...

4.2 Injections, surjections and bijections

Definition 0.7. An *injection* is a function $f : D \to C$ such that $f(x) = f(y) \iff x = y$.

In other words, all values from the domain are mapped onto unique values from the codomain.

Alternatively, we can express this property with an adjective, by saying that f is *injective*.

Definition 0.8. A *surjection* is a function $f : D \to C$ such that $\forall y \in C, \exists x \in D, f(x) = y$.

In other words, for each value in the codomain, there is a value from the domain which maps onto it.

Alternatively, we can express this property with an adjective, by saying that f is *surjective*.

Definition 0.9. A *bijection* is a function that is both injective and surjective.

Alternatively, we can express this property with an adjective, by saying that f is *bijective*.

5 Predicates

Definition 0.10. A *predicate* is a function with a boolean codomain.

In other words, a function that looks like $p : A \to \{\texttt{FALSE}, \texttt{TRUE}\}$.

If $p(x) = \texttt{TRUE}$ we say that *"p holds for object x"* and we can shorten it to $p(x)$.

6 Relations

Definition 0.11. A *relation* over sets $S_1, S_2, ..., S_n$ is a subset of the cartesian product $S_1 \times S_2 \times ... \times S_n$.

In other words, a relation $R : S_1 \times S_2 \times ... \times S_n$ is a set of tuples $(x_1, x_2, ..., x_n)$, where $x_1 \in S_1, x_2 \in S_2, ..., x_n \in S_n$.

An example relation is "less-than", which establishes for a pair (a, b) of natural numbers if a is less than b:

$$\leq : \mathbb{N} \times \mathbb{N}$$

Because it involved exactly two sets, this is a *binary relation*.

6.1 Properties of binary relations

Binary relations whose domain is of the form $A \times A$ (same set, twice) will be especially important to us.

Here are some relevant properties that such a relation r over A can have:

- **reflexivity**: $\forall x \in A, r(x, x)$
- **transitivity**: $\forall x, y, z \in A, r(x, y) \wedge r(y, z) \Rightarrow r(x, z)$

7 Definitions and statements

Definition 0.12. A *definition* is a precise, usually formal, description of some mathematical object.

This definition itself is not formally expressed, but it's precise enough for our purposes. We've also seen other examples of definitions, such as Definition 2 and Definition 2.3.

Definition 0.13. A *statement* is a mathematical proposition about an object and its properties or relations to other objects.

An example statement is: $2 + 2 = 4$. We won't always write statements using formal notation; this is also a statement: "there exists a prime number larger than 10 and smaller than 20".

Note that something doesn't have to be *true* to be a statement; this is also a statement: $18 - 13 = 9$.

For some statements we can show that they hold; for others we can show that they don't.

8 Proofs and theorems

Definition 0.14. A *proof* is a convincing argument that a particular statement is true.

Generally, a proof is a chain of reasoning that starts from some premises which we already accept, and uses various methods to derive new statements, which can then further be used as premises for further statements and so on.

The "steps" used in the proof have to be small, clearly understandable leaps from one point to another.

For example, let's prove that:

$$\forall x \in \mathbb{N}, (4x + 3) \text{ is not a multiple of } 6.$$

Proof. A multiple of 6 must be even. (1)

$4x$ must be even, so $4x + 3$ must be odd. (2)

From (1) and (2) it follows that $4x + 3$ cannot be a non-zero multiple of 6.

Finally, $4x + 3$ is at least 3, so it cannot be 0. □

The level of detail needed in a proof is context-dependent. In a high-level math conversation, the original statement could be judged "obvious" and not given any further justification. In the context of *proof theory*, more statements would need justification (e.g. why is (1) true?).

Definition 0.15. A *theorem* is an interesting statement for which a proof is given.

Having provided a proof for it, we could consider the earlier statement a theorem; we could give it a easy-to-use name, such as $T1$ and refer to it as such in future proofs to keep them short.

9 Proof methods

9.1 Proof by construction

This is probably the most intuitive type of proof. We show that some object exists, by explicitly constructing it.

Let's try this example:

Theorem 0.1. For any complex number $x = a + bi$ other than 0, there exists exactly one complex number $y = c + di$, such that $xy = 1$

Proof. We start from: $xy = 1$ and rewrite it as $(a + bi)(c + di) = 1$.

That is, $ac + adi + bci - bd = 1$, or $(ac - bd) + (ad + bc)i = 1$.

From here, we obtain the following two equations (note that what we want is to express c and d in terms of a and b):

$$ac - bd = 1$$
$$ad + bc = 0$$

From the first equation, we can rewrite c:

$$c = \frac{1+bd}{a}$$

and substitute it in the second equation:

$$ad + \frac{b+b^2d}{a} = 0$$
$$\frac{a^2d+b+b^2d}{a} = 0$$
$$(a^2 + b^2)d + b = 0$$

So d is:

$$d = \frac{-b}{a^2+b^2}$$

(Note that the expression is valid, because the premise requires $x \neq 0$, so that means at least one of a or b is not 0, so the denominator is not 0).

Going back to c we find its value to be:

$$c = \frac{1+b\frac{-b}{a^2+b^2}}{a}$$
$$c = \frac{\frac{a^2+b^2-b^2}{a^2+b^2}}{a}$$
$$c = \frac{a^2}{a^2+b^2}\frac{1}{a}$$
$$c = \frac{a}{a^2+b^2}$$

So, there we have it, our unique number is:

$$y = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$$

□

9.2 Proof by contradiction

One other type of proof involves assuming a statement is false and showing that this assumption leads to a contradiction. This must mean that our original assumption was incorrect, so the original statement was true.

Theorem 0.2. $\sqrt{2}$ is irrational.

Proof. We *assume* the statement is false, i.e. $\sqrt{2}$ is rational.

That means that there exist two *coprime*[†] integers a and b, with $b > 0$, such that:

$$\sqrt{2} = \frac{a}{b}$$

We can then square both sides of the equation to obtain:

$$2 = \frac{a^2}{b^2}$$

Multiplying each side by b^2, we get:

$$2b^2 = a^2$$

Because a^2 is the result of multiplying something by 2, we know that a^2 is *even*. But that is only possible if a itself is even. (1)

As such, there exists a natural number c, such that $a = 2c$. Replacing it in the equation above, we get:

$$2b^2 = (2c)^2$$

$$2b^2 = 4c^2$$

We then divide both sides by two to obtain:

$$b^2 = 2c^2$$

Because b^2 is the result of multiplying something by 2, we know that b^2 is *even*. But that is only possible if b itself is even. (2)

From (1) and (2) we conclude that both a and b are even, which means their GCD is at least 2, but our initial assumption was that it is 1. Thus, we obtained a contradiction, so our assumption (that such a and b exist) is false.

$$2b^2 = a^2$$

□

[†]Their greatest common divisor is 1.

9.3 Proof by induction

Proofs by induction are helpful for infinite sets to prove that all elements have some property. An element having some property simply means that a predicate P holds for that element.

Each proof consists of two parts: the *base case* and the *induction step*, each of which can be a particular type of proof.

The base case shows that $P(0)$ is true[‡].

The induction step assumes that if P holds for a number (this is called *"the inductive hypothesis"*), it also holds for its successor; in other words, it proves that: $n \geq 0, P(i) \implies P(i+1)$.

These two proofs together help us prove a property for **all** numbers. The base case tells us that $P(0)$; then the induction step assures us that, if $P(0)$, then $P(1)$.

Let us prove the following property of natural numbers:

Theorem 0.3. $\forall n, 0 + 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$

Proof. **Base case:**

$$0 = \frac{0(0+1)}{2}.$$

Using basic properties of arithmetic, we can reduce this to $0 = 0$, which is true.

Induction step: here we assume the inductive hypothesis, that this statement is true for n:

$$0 + 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}.$$

We now set to prove, using arithmetic and the inductive hypothesis, that this property is true for $n + 1$:

$$0 + 1 + 2 + 3 + ... + n + (n + 1) = \frac{(n+1)((n+1)+1)}{2}.$$

We observe that the left-hand-side of this equation is the left-hand-side of the inductive hypothesis, plus the term $n + 1$, so we can substitute it with the right-hand-side of the inductive hypothesis and rewrite it as:

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

Which can be rewritten as:

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

$$\frac{n^2+n+2n+2}{2} = \frac{n^2+2n+n+2}{2}$$

$$\frac{n^2+3n+2}{2} = \frac{n^2+3n+2}{2}$$

□

[‡]More generally, it shows the predicate P holds for some n_0; for numbers smaller than n_0, the property might not hold, but these are just a finite subset of the natural numbers.

9.4 If-and-only-if proofs

We will often deal with statements of the form: $P \iff Q$ (read *"P if and only if Q"*), where P and Q are some other statements.

In order to prove this, we will prove two partial statements, namely $P \Rightarrow Q$ (*"Q if P"*) and $P \Leftarrow Q$ (*"P if Q"*).

The difficulty of the directions might not be the same and they might require different types of proof.

Theorem 0.4. $\forall a, b \in \mathbb{N}^*, gcd(a, b) = b \iff b \mid a$.

Proof. We have to prove two statements.

First, we prove $gcd(a, b) = b \Rightarrow b \mid a$.

By the definition of the *greatest common divisor*, $gcd(a, b) = b$ means b divides both a and b. So $b \mid a$.

We then prove: $b \mid a \Rightarrow gcd(a, b)$.

Then b is a divisor of both a and b. This means that $gcd(a, b) \geq b$. (1)

But $b > 0$ so all its divisors must be strictly smaller: $gcd(a, b) \leq b$. (2)

From (1) and (2), it follows that $gcd(a, b) = b$.

We have proved the implications in both directions and thus the equivalence.

□

9.5 The contrapositive

Sometimes we might have to prove a statement of the form $P \Rightarrow Q$ (for example, as one half of an if-and-only-if proof) that seems too hard to address.

We could instead try to prove *the contrapositive*; i.e. the statement: $\neg Q \Rightarrow \neg P$.

This approach is correct because the contrapositive is equivalent to the original statement (try to write the truth table for both).

Theorem 0.5. $\forall n \in \mathbb{N}, n^2$ even $\Rightarrow n$ even

Proof. We prove the contrapositive: n odd $\Rightarrow n^2$ odd .

For n to be odd, there must be some $k \in \mathbb{N}$ s.t. $n = 2k + 1$.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$.

This number is of the form $2k' + 1$ (with $k' = 2k^2 + 2k$), so it is odd.

□

10 References and further reading

This list of relevant mathematical topics to review for such a course was very much inspired by chapter 0 of Michael Sipser's *"Introduction to the Theory of Computation"* [1].

The rest of that textbook could serve as a useful resource for much of `AA` . Chapters 3-5 cover roughly the same subjects that we will study in the first part of the course (Computability Theory), while chapter 7 covers topics pertaining to Complexity Theory.

Chapters 1 and 2 are related to subjects that will be discussed next year at the `LFA` course.

Another good resource to get you started is the gigantic *"Mathematics for Computer Science"* [2][§]. You can read section I, chapters 1 through 5. This is, of course, optional, but if you read those chapters and solve all exercises presented, you'll surely have no problems with the math involved at `AA`.

[§] `https://courses.csail.mit.edu/6.042/spring18/mcs.pdf`

Bibliography

[1] Michael Sipser. *Introduction to the Theory of Computation, Third Edition*. CENGAGE Learning, 2012.

[2] Eric Lehman, F Thomson Leighton, and Albert R Meyer. *Mathematics for Computer Science*. 2018.