Logic & Set Theory Cheatsheet

3.AB PreIB Math

Adam Klepáč

Natural Numbers

Logic is the language of mathematics. It uses propositions to talk about sets.

Propositions are sentences which can be either true or false. For example

- 'Cats are black.' is a proposition;
- 'How are you?' is *not* a proposition;
- 'We will have colonised Mars by 2500.' is also a proposition.

As the third example suggests, we need not necessarily know whether a proposition is true or false – it remains a proposition anyway.

Whole numbers

Propositions can be joined together using logical conjunctions. They pretty much correspond to the conjunctions of natural language. Let us consider two propositions:

$p =$ 'It's raining outside.'
$q =$ 'I'll stay at home.'

($\wedge$) Logical and forms a proposition that is only true if both of its constituents are also true. In natural language, the proposition $p \wedge q$ can be expressed as

$p \wedge q =$ 'It's raining outside and I'll stay at home.'

($\vee$) Logical or forms a proposition that is true if at least one of its constituents is true. In natural language, the proposition $p \vee q$ can be expressed as

$p \vee q =$ 'It's raining outside or I'll stay at home.'

In mathematical logic, or is **not exclusive**! This means that $p \vee q$ is true even if both p and q are true.

($\neg$) Logical not isn't strictly speaking a conjunction but I include it anyway. It reverses the truth value of a proposition. For example, the proposition $\neg p$ can be read as

$\neg p =$ 'It's not raining outside.'

It follows that $\neg p$ is true exactly when p is false and vice versa.

($\Rightarrow$) Logical implication is a conjunction that makes the first proposition into an *assumption* or *premise* and the second one into a *conclusion*. The proposition $p \Rightarrow q$ is read in multiple ways, to list a few:

$p \Rightarrow q =$ 'If it's raining outside, then I'll stay at home.'
$p \Rightarrow q =$ 'It raining outside implies that I'll stay at home.'
$p \Rightarrow q =$ 'Assuming it's raining outside, I'll stay at home.'

The implication is tricky. It's true if both p and q are true and false if p is true but q is false. However, it is always true if p is false. That is because, in mathematical logic, whatever follows from a lie is automatically true.

($\Leftrightarrow$) Logical equivalence is true only if both propositions have the same truth value – they're both true or both false. In natural language, it is typically read like this:

$p \Leftrightarrow q =$ 'It's raining if and only if I stay at home.'

Equivalence is basically just a two-way implication. The proposition p is both a premise and a conclusion to q and q is both a premise and a conclusion to p. If it's raining outside, I stay at home and if I stay at home, then it's raining outside.

Rational numbers

Toto je o racionalnich cislech.

Divisibility

A conjunction of propositions being true or false based on whether its constituent propositions are true or false can be summarized using so-called truth table. It is basically just a table that lists all the possibilities of p and q being true or false and the resulting truth value of their conjunctions.

For the basic logical conjunctions from above, it can look like this (we represent true by 1 and false by 0):

p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	0
1	1	0	0	1	1	1	1

Prime decomposition

Sets are the 'stuff' that makes up the world of mathematics. Their basic characteristics and properties are described using logic.

Sets cannot be defined inside set theory but we interpret them as *groups of things*.

There's only one foundational *proposition* related to set theory – the proposition 'An object is an element of a set.' If we label the object in question x and the set A, this proposition is written as $x \in A$ (the symbol $\in$ is just the letter 'e' in 'element'). Combining these propositions using logical conjunctions allows for various set-theoretic constructions.

If a set A has, for example, exactly three elements – $\square$, $\triangle$ and $\bigcirc$, I can write it as a list of these three elements inside curly brackets $\{\}$. In this case,

$$A = \{\square, \triangle, \bigcirc\}.$$

A few warnings about sets:

- **Sets are not ordered**. There is nothing like a 'first', 'second' or 'last' element of a set. Either an object **is** inside a set or it **isn't**. Nothing else. For example, the three sets below are exactly the same, only written differently.

$$\{\square, \triangle, \bigcirc\} = \{\bigcirc, \triangle, \square\} = \{\triangle, \square, \bigcirc\}$$

- **Elements of sets have no frequency**. Again, an element either is inside a set or not. It cannot be twice in a set, for example. The three sets below are exactly the same.

$$\{\square, \triangle, \bigcirc\} = \{\square, \triangle, \bigcirc, \triangle, \bigcirc\} = \{\triangle, \square, \square, \triangle, \bigcirc, \triangle\}$$

Euler's algorithm

Using logical conjunctions, we form new sets from existing ones. Consider two sets – A and B.

($\cap$) I can form the set of all objects x that satisfy the proposition $x \in A \wedge x \in B$, that is all objects that lie in both A and B. This set is called the intersection of A and B and written $A \cap B$. For example,

$$\{\bigcirc, \triangle, \square\} \cap \{\times, \bigcirc, \square, \sim\} = \{\bigcirc, \square\}.$$

($\cup$) I can form the set of all objects that satisfy the proposition $x \in A \vee x \in B$, the set of all objects that lie in A or in B. It is called the union of A and B and denoted $A \cup B$. All elements of $A \cup B$ can be found *only* in A, *only* in B or in *both* A and B. For example,

$$\{\bigcirc, \triangle, \square\} \cup \{\times, \bigcirc, \square, \sim\} = \{\bigcirc, \triangle, \square, \times, \sim\}.$$

($\Rightarrow$) Implication is a little different from intersection and union. It describes a lot of different sets with one logical proposition. I ask: 'Which sets A satisfy the proposition $x \in A \Rightarrow x \in B$?' In other words, which sets A have all their elements contained in the set B? The answer is that A must be a subset of B and we denote that fact by $A \subseteq B$. The set A is only allowed to have elements which also lie in B but not necessarily all of them. All the subsets of $B = \{\triangle, \bigcirc\}$ are listed below.

$$\emptyset, \{\triangle\}, \{\bigcirc\}, \{\triangle, \bigcirc\},$$

where $\emptyset$ is the empty set, a set containing no elements.

($\Leftrightarrow$) Equivalence defines equality on sets. If sets A and B must satisfy the proposition $x \in A \Leftrightarrow x \in B$, then they must be equal because all the elements of A lie in B and all elements of B lie in A. That is, $A = B$.

Congruence

Now that we have defined the remainder after division we want to express the idea that two numbers (x and y) have the same remainder (r) after diving by some number m. Mathematically we write it as:

$$x \equiv y \pmod m.$$

In other words this means:

$$x = km + r \qquad \text{and} \qquad y = lm + r$$

for some numbers $l, k \in \mathbb{N}$. This way we can for example say that 13 and 25 are the same modulo 12, because they share the remainder 1 when divided by 12 (formally written as $13 \equiv 25 \pmod{12}$).

This idea might sound unintuitive and artificial yet it is all around us. If we for example take the regular old clock. Looking only at the clock and seeing both hands up tells me that it is either noon or midnight. This is because we use the 12 hours format which gives the time $\mod 12$.

Congruence is in sense very similar to normal equations (it is also equivalence try to prove it!). Similar to equations we can manipulate it. More specifically:

- $x + a \equiv y + a \pmod m$ - **adding** also works for subtracting so $a \in \mathbb{Z}$
- $xk \equiv yk \pmod{km}$ - **multiplying**
- $x^k \equiv y^k \pmod m$ - **exponentiation**

for any $k \in \mathbb{N}$.

An interesting thing to note about the equivalence classes created by some congruence $\mod m$ is that there will be m of them. This is because all the possible remainders after diving by m are numbers $1, \ldots, m$.

Similarly to system of equations we can have also systems of congruences.

Chineese remainder theorem

Imagine we have a system of linear congruences:

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\vdots \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

Where all the numbers are natural and $m_1, \ldots m_n$ are mutually coprime. The CRT tells us that there is unique solution x smaller then the product of all the numbers we divide by, $M = m_1 \cdot m_2 \ldots m_n$.

Each congruence limits the possible solutions radically. For example the congruence $x \equiv r \pmod m$ has solutions in the form: $km + r$ for any $k \in \mathbb{N}$. So if we write down all the solutions of each congruence up to M and then find the intersection, we have found x such that it satisfies all the congruences and thus is the solution to the whole system.

We can do this process also graphically. If we circle solutions to the individual congruences the number with n circles is the solution to the whole system.

If, for example, we have the linear congruences: $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, we can draw:

1	2	3	4	5	6	7	8
9	10	11	$\boxed{12}$	13	14	15	16
17	18	19	20	21	22	23	$\boxed{24}$
25	26	27	28	29	30	31	32

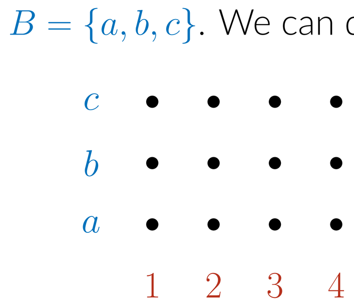
The box around 12 and 24 indicates on what intervals are we guaranteed to have a unique solution. This is because $M = m_1 \cdot m_2 = 3 \cdot 4 = 12$.

If we find the smallest solution x (the one smaller then M) then we have every other because they are all in the form of $x + kM$ for any $k \in \mathbb{N}$.

Drawing Products And Relations

One can draw the product $A \times B$ similarly to the way we draw Cartesian coordinates – by distributing the elements of A horizontally and those of B vertically. Each point in the resulting grid represents an element of $A \times B$.

Take, for example, $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. We can depict the set $A \times B$ like this:



Any relation $R \subseteq A \times B$ can now be easily drawn into the grid just by marking certain dots. For example, the relation $R = \{(1, c), (2, b), (2, a)\} \subseteq A \times B$ looks like this: