Discrete Mathematics

SyG

October 7, 2020

Chapter 1

Introduction

Propositional logic

Propositional logic (and mathematics, in general) studies propositions: **declarative sentences** (a sentence that declares a fact) that is either true or false, but not both.

Example 1.1. Propositions:

1. Toronto is the capital of Canada (false but a declarative sentence nonetheless)
2. 1+1=2
3. 2+2=3
4. 3 is a prime number

The following are not propositions:

Not declarative:

1. What time is it?
2. Read this carefully.

Neither true or false:

1. $x + 1 - 2$
2. $x + y - z$

We use letters to denote propositions: **p, q, r,** .... Now propositions (called compound propositions) are constructed by combining one or more propositions using logical operators.

Negation (NOT)

If p is a proposition, its negation is denoted by $\neg p$.

"It's not the case that p". "The negation of p".

Example 1.2. p: "My PC runs Linux"

$\neg p$: "It's not the case that my PC runs Linux" $\Rightarrow$ "My PC doesn't run Linux"

Example 1.3. p: $1 + 1 = 2$ $\neg$ p: $1 + 1 \neq 2$

$\Rightarrow$ $\neg p$ is true iff (if and only if) p is false.

Conjunction (AND)

Let p, q be two propositions $\Rightarrow p \wedge q$ "p and q".

$p \wedge q$ is true iff p and q are true.

Remark. Sometimes the word "but" is used instead of "and". For example: 2 is even but 3 is odd.

Disjunction (OR)

Let p, q be two propositions $\Rightarrow p \vee q$ "p or q".

$p \vee q$ is true iff p is true, q is true or both are.

This correspondos to the **inclusive or** in English.

Remark. The **exclusive or**, it is not possible to have both propositions. For example: soup or salad comes as an entrée, it most certainly means that the customer cannot have both soup or salad.

Conditional statement / Implication

Let p, q be two propositions $\Rightarrow p \to q$ "if p, then q".

Because of its essential role in mathematical reasoning, a variety of terminology is used to express $p \to q$:

- if p and then q
- if p, q $\to$ p implies q
- q if p $\to$ p only if q
- q when p
- if p, q

$p \to q$ is false when p (the hypothesis / antecedent) is true and q (the consequence / conclusion) is false; otherwise, it is true.

Useful way to understand its truth value: A pledge many politicians make when running for office: "If I'm elected, I will lower taxes". It is only when the politician is elected that does not lower taxes that it can be said he has broken his pledge.

Remark. Note that this definition is more general tthan the meaning attached to such statements in English: there needs to be no relationship between p and q: "If the Moon is made of cheese, then 2+3=4".

Biconditional statement / Bi-implication

$q \leftrightarrow q$. It's equivalent to $(p \to q) \wedge (q \to p)$.

It's True iff the truth values of p and q are the same.

The main advantage of logical language over natural ones is that it removes ambiguity.

Predicate logic or first-order logic

Statements such as: $x > 3$ or $x + 1 = y$ are often found in mathematical assertions. They are neither true or false (when the value of the variables are not specified) and have fall outside of the scope of propositional logic.

In "$x > 3$" there are two parts:

- the variable x.
- the predicate "is greater than 3".

By denoting the predicate with P, the statement can be represented as $P(x)$.

Example 1.4.
- If $P(x)$ is "$x > 3$" then P(4) is True, P(2) is False, P(y) is undefined.
- $Q(x, y)$ is "$x = y + 2$": $Q(3, 1)$ is True.

Quantifiers

In addition to assigning values to variables, there is another way to get truth values from predicate statements. For that, it is necessary to assume a domain or universe.

Universal quantification

$$P(x) \ \rightarrow \ \forall x, \ P(x) \ : \quad \text{P(x) for all values of x in the domain.}$$

$$\forall x, \ P(x) \text{ is true iff P(a) is true for all elements a in the universe}$$

Example 1.5.
1. $\forall x, \ x + 1 > x$ is true in $\mathbb{R}$ and $\mathbb{N}$.
2. $\forall x, \ x \geq 0$ is true in $\mathbb{N}$ but not in $\mathbb{R}$. Alternative, mathematical notation:
   - $\forall x \in \mathbb{N}, \ x \geq 0$
   - $\forall x \in \mathbb{R}, \ x \geq 0$
3. $U = \{0, \ 1, \ 2, \ 3\}, \ \forall x \in U, \ x^2 < 10$ is true.
4. $\forall x, \ \forall y, \quad x + y > x$ is true in $\mathbb{N}$, false in $\mathbb{R}$.
5. $\forall x, \ \forall y, \quad x \cdot y > x + y$ is false in $\mathbb{N}$ and in $\mathbb{R}$

Existencial quantification

$P(x) \ \rightarrow \ \exists x, \ P(x) \ :$ "There exists at least one element x in the domain such that P(x)".

$$\exists x, \ P(x) \text{ is true iff P(a) is true for some a in the universe}$$

Example 1.6. $\exists x, \ x < 0$ is true in $\mathbb{R}$ but not in $\mathbb{N}$.

Both quantifiers

Example 1.7. 1. $\forall x,\ \exists y:\ x+y=0$ is True in $\mathbb{R}$ and False in $\mathbb{N}$.

2. $\exists y,\ \forall x:\ x+y=0$ is False in $\mathbb{R}$ and True in $\mathbb{N}$.

Remark. The order of the quantifiers matters.

Remark. What if the universe is empty (there are no elements)?

$$\forall x,\ P(x) \text{ is trivially true}$$

$$\exists x,\ P(x) \text{ is false}$$

Proof techniques

Direct proofs

$p \to q$ can be proved by showing that if p is True then q must be also True.

Example 1.8. *If n is even then n^2 is even.* Assumming n is even, therefore $n = 2k,\ k \in \mathbb{N}$.

We then have $n^2 = 4k^2,\ k \in \mathbb{N}$. We can define $i = k^2$.

$\Rightarrow\ n^2 = 2 \cdot (2i)$. $\Rightarrow$ We define $2i = m$

$\therefore n^2 = 2 \cdot m$ is even. □

Proof by contraposition

To prove $p \to q$ is equivalent to showing its contrapositive: $\neg q \to \neg p$.

False iff $\neg q$ is True, $\neg p$ is False.

$\Leftrightarrow$ q is False, p is True.

$\Leftrightarrow$ p $\to$ q is False.

Example 1.9. *If $3n+2$ is odd, then n is odd.* We define p="If $3n+2$ is odd" and q="n is odd."

$\Rightarrow\ \neg q$="n is even". *** terminar

□

Vacuous and trivial proofs

$p \to q$ is True if the hypothesis is False.

$p \to q$ is True if so is q.

Example 1.10. If n^2 is odd then n is odd (contrapositive: start with a draft proof)

*** terminar

Proofs by contradiction

To show that q is True it is enough to show that $\neg p$ leads to a contradiction.

Example 1.11. *Out of 22 weekdays, at least 4 must fall on the same day of the week.* Let's first assume that the result is not True i.e. False.

If each day is repeated 3 times, we have 21 weekdays in the end. But as we have 22 weekdays, at least one of them is repeated 4 times. Therefore the hypothesis by contradiction is True.

□

Counterexample

To show that $\forall x,\ P(x)$ is False, we need to only find a value such that P(a) is False.

Example 1.12. *Every positive integer is the sum of three squares.*

$$6 = 1^2 + 2^2 + 1^2 \text{ but } 7 = 2^2 + 1^2 + 1^2 + 1^2 \text{ (it's four squares)}$$

□

We have the following Universe: Kingdom=99 cities. Roads join 2 cities and 3 roads go through every city.

As every road from and to a city, we need to avoid counting it twice, then:

$$\frac{99 \circ 3}{2}$$

, which isn't an integer, then it is impossible for it to exist.

Chapter 2

2: Numbers, induction and recursion

2.1 Principle of Mathematical Induction

The successor of $n \in \mathbb{N}$ is $s(n) = n + 1$.

The set $\mathbb{N}$ of natural numbers is generated by 0 and s.

$$\begin{aligned}\mathbb{N} =&\{0, 1, 2, 3, \ldots\}\\ &\{0, s(0), s(s(0)), s(s(s(0)), \ldots)\}\end{aligned}$$

Similarly, starting with $m \in \mathbb{N}$ and applying s, the set $\mathbb{N}_m$ of all natural numbers, from m upward, is generated:

$$\begin{aligned}\mathbb{N} =&\{m, m + 1, m + 2, \ldots\}\\ &\{m, s(m), s(s(m)), \ldots)\}\end{aligned}$$

Definition 2.1. Principle of mathematical induction

To prove that $P(n)$ is true for all numbers, we complete two steps:

- Basis step: we verify that $P(0)$ is true.
- Inductive step: assuming that $P(k)$ is true (inductive hypothesis), we use it to show that $P(k + 1)$ is true.

Example 2.2.

- $P(n) : \forall n \geq 0 : 2 + 4 + 6 + \ldots + 2n = n(n + 1)$.
- $Q(n) : \forall n \geq 0 : 1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.

Sometimes, the property $P(n)$ holds for all numbers, greater than or equal to w. In this case, we need to modify the basis step:

- Basis step: we verify that $P(w)$ is true.
- $\forall n \geq 1 : 1 + 3 + 5 + \ldots + (2n - 1) = \sum_{i=1}^{n}(2i - 1) = n^2$
- Exercise: $2^n < n!, \forall n \geq 4$.

Definition 2.3. Strong induction

To prove that $P(n)$ is true for all $n \in \mathbb{N}$, we complete two steps:

- Basis step: we verify that $P(0)$ is true.

- Inductive step: assuming that $P(0), P(1), \ldots$ and $P(k)$ are true, we show that $P(k+1)$ is true.
- $\forall n > 1$, n can be decomposed as the product of prime factors.

Sometimes it is also useful to modify the basis step in the strong induction:

- Basis step: we verify that $P(w)$ is true.

More exercises:

- $\forall n \geq 1 : 1 + a + a^2 + \ldots + a^n = \dfrac{a^{n+1} - 1}{a - 1}$.
- Every price ≥ 24 can be paid using notes of 5 and 6.

  $\forall n \geq 24, \exists p, q \geq 0 : n = 5p + 6q$

2.2 Recursive definitions

Definition 2.4. Let A be a set and $m \in \mathbb{N}$. A **sequence** (of elements from A indexed by $\mathbb{N}_m$) is a function:

$$f : \mathbb{N}_m \mapsto A$$

We write a_n for $f(n)$ and call a_n a term of the sequence.

A sequence can be defined via an explicit or a recursive definition.

Definition 2.5. Explicit definition: give a direct procedure to compute a_n.

- $f : \mathbb{N} \mapsto \mathbb{Q}$ with $f(n) = q_n = \dfrac{1}{2^n}$

  $\longrightarrow 1, \dfrac{1}{2}, \dfrac{1}{4}, \dfrac{1}{8}, \ldots$
- $g : \mathbb{N} \mapsto \mathbb{Z}$ with $g(n) = x_n$ defined by cases:

$$x_n = \begin{cases} i & \text{if } n \text{ is even }, n = 2i, i \geq 0 \\ j & \text{if } n \text{ is odd }, n = 2j - 1, j \geq 1 \end{cases}$$

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

Definition 2.6. Recursive definition: we use two steps:

- Basis step: specify the value of the sequence for the initial segment $a_m, a_{m+1}, \ldots, a_l$.
- Recursive step: give a rule for finding its value at $l < n$, from its values at smaller natural numbers.

Example 2.7. Fibonacci Sequence

$fib : \mathbb{N} \mapsto \mathbb{N}$

RS: $fib(0) = 0,\ fib(1) = 1.$
RS: $fib(n) = fib(n-2) + fib(n-1), \quad n > 1.$

*** pagina 5, el cuadro

Alternatively, we can compute the values of $fib(n)$ by "reduction".

$$\begin{aligned} fib(4) &= fib(3) + fib(2) \\ &= fib(2) + fib(1) + fib(1) + fib(0) \\ &= fib(1) + fib(0) + 1 + 1 + 0 \\ &= 1 + 0 + 1 + 1 + 0 \\ &= 3 \end{aligned}$$

Some calculations are repeated, as opposed to tabulation.

2.2.1 Summation and product

Summations and products can be defined recursively.

$\sum_{k=0}^{n} a_k = a_0 + a_1 + \ldots + a_n = F(n)$

- B.S: $\sum_{k=0}^{0} a_k = a_0$
- R.S: $\sum_{k=0}^{n+1} a_k = (\sum_{k=0}^{n} a_k) + a_{n+1}$

Similarly for products. Consider the factorial:

$n! = n \cdot (n-1) \ldots 3 \cdot 2 \cdot 1 = \prod_{k=1}^{n} k$

- B.S: $0! = 1$
- R.S: $(n+1)! = (n+1) \cdot n!$

Example 2.8.

- $\forall n \geq 3 : \sum_{i=0}^{n} fib(i)^2 = fib(n) \cdot fib(n+1)$??? properties about recursive sequences often require the strong principle of mathematical induction. Though not in this case.
- Let (a_n) be defined as:
  - B.S: $a_0 = 2,\ a_1 = 1$
  - R.S: $a_n = a_{n-1} + 2a_{n-2}$ for $n > 1$

  $forall n \geq 0 : a_n = 2^n + (-1)^n$ ASK TEACHER *** Prove $a_n = b_n$. (Strong induction)

2.2.2 Recursive functions with more than 1 argument

Recursive definitions can be used whenever a function has one argument ranging over $\mathbb{N}_m$. For example:

$f : \mathbb{N} \mapsto \mathbb{N}$

- B.S: $f(0, a) = a$
- R.S: $f(n, a) = f(n-1, n \cdot a), \quad n > 0$

Recursion over the first argument.

To compute the values of such function, use either tabulation or reduction:

$f(3, a) = f(2, 3 \cdot a) = f(1, 2 \cdot 3 \cdot a) = f(0, 1 \cdot 2 \cdot 3 \cdot a) = 1 \cdot 2 \cdot 3 \cdot a = 3! \cdot a$

It can be proved, by mathematical induction, that $f(n, a) = n! \cdot a$.

2.3 Divisibility

Let $a, b \in \mathbb{Z}$. We say that b **divides** a, or that a is a **multiple** of b, if there is an integer c such that $a = b \cdot c$. The notation b/a denotes that b divides a; we write $b \not| a$ when b does not divide a.

If b/a and c is unique, we write $c = \frac{b}{a}$. We call c the **quotient**.

Remark.
- $0/0$ but $\frac{0}{0}$ is undefined.
- If $b \neq 0$ then $\frac{0}{b} = 0$.

2.3.1 Integer division

Let $a, b \in \mathbb{Z}, b \neq 0$. If $b \not| a$, the (exact) quotient $displaystyle\frac{a}{b}$ does not exist, but an integer division between a (dividend) and b (divisor) can be performed to produce a quotient (q) and a remainder (r).

Theorem 2.9. ***Division algorithm***

Given $a \in \mathbb{Z}$ (dividend) and $b \in \mathbb{Z}$ (divisor), $b \neq 0, b > 0$, there are unique integers q and r such that

$$a = b \cdot q + r \text{ and } 0 \leq r < b$$

Proof. Uniqueness: Assume $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

- $a = bq_1 + r_1,\ 0 \leq r_1 < b$
- $a = bq_2 + r_2,\ 0 \leq r_2 < b$

Let us show that $q_1 = q_2$ and $r_1 = r_2$. If $q_1 \neq q_2$ then either $q_1 > q_2$ or $q_2 > q_1$. In case $q_1 > q_2$:

$a = bq_1 + r_1 = bq_2 + b(q_1 - q_2) + r_1$
$\Rightarrow a - bq_2 = b(q_1 - q_2) + r_1$ Contradicting the fact that $r_2 < b$. (Remember that
$\Rightarrow r_2 = b(q_1 - q_2) + r_1 \geq b + r_1 \geq b$
$q_1 \geq q_2, r_1 \geq 0$)

From $q_2 > q_1$ a similar contradiction is reached and hence $q_1 = q_2$. And then:

$$r_1 = a - bq_1 = a - bq_2 = r_2$$

□