Foundations, Class Notes

Eugen J. Ionascu

Contents

List of Figures

List of Tables

Preface

I have been teaching the Foundations lately from the classic textbook "Problem-solving and proofs" by John P. D'Angelo and Douglas B. West. Most of the ideas presented here follow this text. Some other problems are taken from various places or from the questions that were posed by the students in class.

Chapter 1

Some classical facts and basic tools

> Even fairly good students, when they have obtained the solution of the problem and written down neatly the argument, shut their books and look for something else. Doing so, they miss an important and instructive phase of the work. ... A good teacher should understand and impress on his students the view that no problem whatever is completely exhausted.
>
> George Pólya

1.1 Formulae and identities

There are important identities that are used quite often in the mathematical proofs. Let us just start with a few that are most common:

$$(a \pm b)^2 = a^2 \pm 2ab + b^2 \quad \text{binomial formula} \tag{1.1}$$

$$a^2 - b^2 = (a - b)(a + b) \quad \text{difference of squares formula} \tag{1.2}$$

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2) \text{ difference of cubes formula} \tag{1.3}$$

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2) \text{ sum of cubes formula.} \tag{1.4}$$

An identity less known is the sum of three cubes formula

$$a^3+b^3+c^3=3abc+(a+b+c)(a^2+b^2+c^2-ab-bc-ca). \tag{1.5}$$

Some important summations to prove latter by induction.

$$\sum_{k=0}^{n} r^k = 1+r+\cdots+r^n = \frac{r^{n+1}-1}{r-1},\ r\neq 1,$$

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}, \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4},$$

$$\sum_{k=0}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

$$\sum_{k=0}^{n} kx^{k-1} = \frac{1-(n+1)x^n+nx^{n+1}}{(1-x)^2}, (x\neq 1).$$

Theorem 1.1.1. (Binomial Formula in General) *For a and b real numbers, and $n\in\mathbb{N}$, we have*

$$(a+b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + ...$$

The formula for the quadratic equation below is known also as the half-quadratic formula: "If $a\neq 0$ and $b^2\geq ac$ the equation $ax^2+2bx+c=0$ has as solutions

$$x_{1,2} = \frac{-b\pm\sqrt{b^2-ac}}{a}."$$

Indeed, we start with $ax^2+2bx+c=0$ and proceed equivalently by completing the square:

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

or

$$\left(x+\frac{b}{a}\right)^2 = \frac{b^2-ac}{a^2}. \tag{1.6}$$

Because we are talking about real valued zeros and $b^2 - ac \geq 0$ the number $\sqrt{b^2 - ac}$ exists and then (1.6) becomes

$$x + \frac{b}{a} = \pm\frac{\sqrt{b^2 - ac}}{a}.$$

This is basically the formula we wanted to prove.

Exercise 1: Check the trinomial formula:

$$(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz.$$

1.1.1 Transformations of Proportions

Given four positive real numbers a, b, c and d satisfying $\frac{a}{b} = \frac{c}{d}$ then

(i) $\frac{a\pm b}{b} = \frac{c\pm d}{d}$ and for arbitrary m, n we also have $\frac{ma+nb}{b} = \frac{mc+nd}{d}$

(ii) $\frac{a}{b+a} = \frac{c}{d+c}$

(iii) $\frac{a}{b} = \frac{c}{d} = \frac{a+c}{b+d}$

(iv) $a = \frac{bc}{d}$, $b = \frac{ad}{c}$, $c = \frac{ad}{b}$ and $d = \frac{bc}{a}$

(v) $ad = bc$, $\frac{a}{c} = \frac{b}{d}$, $\frac{d}{b} = \frac{c}{a}$ and $\frac{b}{a} = \frac{d}{c}$

(vi) $\frac{a-b}{a+b} = \frac{c-d}{c+d}$ and for $m, n > 0$ we also have $\frac{ma-nb}{ma+nb} = \frac{mc-nd}{mc+nd}$

As an application solve the system of equations

$$\begin{cases} 2x + 3y = 5 \\ \\ \frac{x}{y} = \frac{2}{7}. \end{cases}$$

We observe that $\frac{x}{y} = \frac{2}{7}$ implies $\frac{2x+3y}{y} = \frac{2(2)+3(7)}{7}$ and so $y = \frac{7}{5}$ and then $x = \frac{2}{5}$.

1.2 Some Classical Inequalities

"One of the first and foremost duties of the teacher is not to give his students the impression that mathematical problems have little connection with each other, and no connection at all with anything else. We have a natural opportunity to investigate the connections of a problem when looking back at its solution." George Pólya

1.2.1 Arithmetic-Geometric Mean Inequality

Given two positive real numbers a and b, their **arithmetic mean** is $\frac{a+b}{2}$, their **harmonic mean** is $\frac{2}{\frac{1}{a}+\frac{1}{b}} = \frac{2ab}{a+b}$ and their geometric mean is equal to $\sqrt{ab}$.

Let us first show that

$$\frac{2}{\frac{1}{a}+\frac{1}{b}} \underset{(ii)}{\leq} \sqrt{ab} \underset{(i)}{\leq} \frac{a+b}{2} \text{ AGM-inequality for two numbers.} \tag{1.7}$$

We see that the second inequality in (1.7) is equivalent to

$$\sqrt{ab} \leq \frac{a+b}{2} \Leftrightarrow 2\sqrt{ab} \leq a+b \Leftrightarrow a+b-2\sqrt{ab} \geq 0 \Leftrightarrow$$
$$(\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \geq 0 \Leftrightarrow (\sqrt{a}-\sqrt{b})^2 \geq 0$$

This last inequality is true, since one can easily show that $x^2 \geq 0$, for all $x \in \mathbb{R}$.

Next, in order to prove (ii) in (1.7) we observe that

$$\frac{2}{\frac{1}{a}+\frac{1}{b}} \leq \sqrt{ab} \Leftrightarrow \frac{\frac{1}{a}+\frac{1}{b}}{2} \geq \frac{1}{\sqrt{ab}} = \sqrt{\frac{1}{a}\cdot\frac{1}{b}}.$$

This last inequality follows from (i) applied to $1/a$ and $1/b$ instead of a and b.

The next step in the attempt of generalizing (1.7) to more than two numbers, is an idea due to Cauchy (Augustin-Louis Cauchy 21 August 1789 – 23 May 1857) and that consists in jumping to four positive real numbers a, b, c, and d:

$$\frac{4}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}} \underset{(ii)}{\leq} \sqrt[4]{abcd} \underset{(i)}{\leq} \frac{a+b+c+d}{4} \text{ AGM- for 4 numbers.} \tag{1.8}$$

Using (i) in (1.7), we have $\frac{a+b}{2} \geq \sqrt{ab}$ and $\frac{c+d}{2} \geq \sqrt{cd}$. Adding these two inequalities together gives us

$$\frac{a+b+c+d}{2} \geq \sqrt{ab}+\sqrt{cd} \quad \Big| \div 2$$
$$\Leftrightarrow \frac{a+b+c+d}{4} \geq \frac{\sqrt{ab}+\sqrt{cd}}{2} \underset{(1.7)(i)\ again}{\geq} \sqrt{\sqrt{ab}\sqrt{cd}} = \sqrt[4]{abcd}.$$

From the transitivity of the order (1.8)(i) follows. To show (1.8)(ii), we proceed as before and observe that (1.8)(ii) can be written as

$$\frac{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{d}}{4} \geq \sqrt[4]{\frac{1}{a}\cdot\frac{1}{b}\cdot\frac{1}{c}\cdot\frac{1}{d}},$$

which is true by (1.8)(i).

This brings us back to three numbers for the AGM inequality. The idea is to take $d=\frac{a+b+c}{3}$ in (1.8)(i). This gives us,

$$\frac{a+b+c+\frac{a+b+c}{3}}{4} \geq \sqrt[4]{abc(\frac{a+b+c}{3})} \Leftrightarrow \frac{\frac{4a+4b+4c}{3}}{4} \geq \sqrt[4]{abc(\frac{a+b+c}{3})} \Leftrightarrow$$

$$\Leftrightarrow (\frac{a+b+c}{3})^4 \geq abc(\frac{a+b+c}{3}) \Leftrightarrow (\frac{a+b+c}{3})^3 \geq abc.$$

Clearly, the last inequality implies AGM-inequality for three numbers. Encouraged by this, we may wonder if this technique works for more numbers. Let us recall some standard notation $\sum_{i=1}^{n} x_i = x_1+x_2+x_3+\ldots+x_n$ and $\prod_{i=1}^{n} x_i = x_1\cdot x_2\cdot x_3\ldots\cdot x_n$. With this in mind, let us move to eight numbers now, so let us consider x_1, x_2, ..., and x_8 positive real numbers.

$$\frac{\sum_{i=1}^{8} x_i}{8} \geq \left(\prod_{i=1}^{8} x_i\right)^{\frac{1}{8}}. \tag{1.9}$$

As we did earlier, we can use (1.8)(i) and write $\frac{\sum_{i=1}^{4} x_i}{4} \geq \left(\prod_{i=1}^{4} x_i\right)^{\frac{1}{4}}$ and $\frac{\sum_{i=5}^{8} x_i}{4} \geq \left(\prod_{i=5}^{8} x_i\right)^{\frac{1}{4}}$. Adding these together gives

$$\frac{\sum_{i=1}^{8} x_i}{8} \geq \frac{\left(\prod_{i=1}^{4} x_i\right)^{\frac{1}{4}}+\left(\prod_{i=5}^{8} x_i\right)^{\frac{1}{4}}}{2} \geq \sqrt{\left(\prod_{i=1}^{4} x_i\right)^{\frac{1}{4}}\left(\prod_{i=5}^{8} x_i\right)^{\frac{1}{4}}} = \left(\prod_{i=1}^{8} x_i\right)^{\frac{1}{8}}$$

Next we let in (1.9), $x_1=a_1$, $x_2=a_2$, $x_3=a_3$, $x_4=a_4$, $x_5=a_5$, $x_6=\frac{a_1+a_2+a_3+a_4+a_5}{5}=x_7=x_8=S$:

$$\frac{a_1+a_2+a_3+a_4+a_5+3S}{8}=\frac{5S+3S}{8}\geq (a_1a_2a_3a_4a_5S^3)^{\frac{1}{8}}\Rightarrow S\geq (a_1a_2a_3a_4a_5S^3)^{\frac{1}{8}}\Rightarrow$$

$$S^8\geq a_1a_2a_3a_4a_5S^3\Rightarrow S\geq (a_1a_2a_3a_4a_5)^{\frac{1}{5}}$$

We leave this to the reader, to obtain the AGM for six numbers. Let us give another proof for the AGM for three numbers

$$\frac{a+b+c}{3}\geq \sqrt[3]{abc} \tag{1.10}$$

using the identity (1.4).

Lets us show first that $\forall x,y,z\in\mathbb{R}$, $x^2+y^2+z^2-xy-xz-yz\geq 0$. We begin by multiplying by 2

$$x^2+y^2+z^2-xy-xz-yz\geq 0\Leftrightarrow 2x^2+2y^2+2z^2-2xy-2xz-2yz\geq 0.$$

Grouping the terms in such a way to complete three squares, we obtain equivalently

$$(x-y)^2+(x-z)^2+(y-z)^2\geq 0$$

which is true since the sum of non-negative numbers is also non-negative. We observe that equality happens only if $x=y=z$. From (1.4), we conclude that if x, y and z are non-negative then $x^3+y^3+z^3-3xyz\geq$. Letting $x=\sqrt[3]{a}, y=\sqrt[3]{b}, andc=\sqrt[3]{c}$ with $a,b,c>0$, we see that $a+b+c-3\sqrt[3]{abc}\geq 0$ and so (1.10) follows.

Applications of AGM Inequality:

1) $a,b,c>0$

$\frac{a}{b}+\frac{b}{c}+\frac{c}{a}\geq 3$

or

$x,y,z>0$

$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}\geq 3 \Big| 3$

Start by dividing by 3 to get,

$\frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3}\geq 1$

Substituting this into $\frac{a+b+c}{3} \geq \sqrt[3]{abc} \implies$
$\implies \frac{\frac{x}{y}+\frac{y}{z}+\frac{z}{x}}{3} \geq \sqrt[3]{\frac{x}{y}\frac{y}{z}\frac{z}{x}} = 1$

This is a straightforward application of AGM Inequality.

2) $x, y, z > 0$
$\frac{x}{y} + \frac{y}{x} \geq 2 \implies \frac{\frac{x}{y}+\frac{y}{x}}{2} \geq 1$

3) $(x+y+z)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}) \geq 9 \Leftrightarrow$

$\Leftrightarrow 1+\frac{x}{y}+\frac{x}{z}+\frac{y}{x}+1+\frac{y}{z}+\frac{z}{x}+\frac{z}{y}+1 \geq 9 \quad \Big| \; 6$

Removing the ones from the LHS and dividing by 6 gives us,

$\implies \frac{\frac{x}{y}+\frac{x}{z}+\frac{y}{x}+\frac{y}{z}+\frac{z}{x}+\frac{z}{y}}{6} \geq 1$

Or a different way is to say,

$\frac{x+y+z}{3}\frac{(\frac{1}{x}+\frac{1}{y}+\frac{1}{z})}{3} \geq \sqrt[3]{xyz}\sqrt[3]{\frac{1}{xyz}} = 1$

4) $(x+y+z)^2 \leq 3(x^2+y^2+z^2) \Leftrightarrow$

Using the trinomial formula on the LHS give us,

$\Leftrightarrow x^2+y^2+z^2+2xy+2xz+2yz \leq 3x^2+3y^2+3z^2 \Leftrightarrow$
$\Leftrightarrow 2x^2+2y^2+2z^2-2xy-2yz-2xy \geq 0 \Leftrightarrow$
$\Leftrightarrow (x-y)^2+(y-z)^2+(x-z)^2 \geq 0$

"=" $\implies$ x=y=z

Next, we move on to the triangle inequality,

(1.11) $$\forall x, y \in \mathbb{R},\ |x+y| \leq |x|+|y|,\ \triangle$$

As an application of the triangle inequality, we want to show that $\forall a, b \in \mathbb{R}$,

$$||a| - |b|| \leq |a - b|.$$

Case I: ($|b| \geq |a|$) The inequality becomes
($\triangle$)$\Leftrightarrow |b| - |a| \leq |a - b| \Leftrightarrow |b| \leq |a - b| + |a|$
Let $x = a - b, y = -a$ in the Triangle Inequality:
And now we make a quick observation that $|x| = |-x|$ to get,
$|x + y| \leq |x| + |y|$ or $|-b| \leq |a - b| + |-a|$, which implies
$\Leftrightarrow |b| - |a| \leq |a - b| \Leftrightarrow |b| \leq |a - b| + |a|$
Case II ($|b| < |a|$) This can be done in a similar way.

1.2.2 Cauchy-Schwartz Inequality

Given a_1, a_2,..., a_n,b_1, b_2,..., b_n real numbers then

$$(a_1^2 + a_2^2 + ... + a_n^2)(b_1^2 + b_2^2 + ... + b_n)^2 \geq (a_1b_1 + a_2b_2 + ... + a_nb_n)^2. \tag{1.12}$$

Chapter 2

Proofs

> Even fairly good students, when they have obtained the solution of the problem and written down neatly the argument, shut their books and look for something else. Doing so, they miss an important and instructive phase of the work. ... A good teacher should understand and impress on his students the view that no problem whatever is completely exhausted.
>
> George Pólya

2.1 Induction Proofs

In general the PMI (principle of mathematical induction) is stated in the following way:

Theorem 2.1.1. *For $n \in \mathbb{N}$, we let $P(n)$ be some statement. If the implications (i) and (ii) below are satisfied, then $P(n)$ is true for every $n \in \mathbb{N}$.*

(i) **Basis Step:** *$P(1)$ is true*

(ii) **Induction Step:** *Given $n \in \mathbb{N}$, then $P(n) \Rightarrow P(n+1)$.*

Let us look at some example. First, we want to show that for every $k \in \mathbb{N}$:

$$P(k): \ 1 + 3 + 5 + ... + (2k+1) = (k+1)^2$$

Proof. We proceed by induction on n. **Basis Step:** To show that $P(1)$ is true we observe that we need to check that $1 + 3 = 2^2$ which is clearly true. To show the **Inductive Step:** we assume that $P(n)$ is true. In other words,

$$1 + 3 + 5 + ... + (2n+1) = (n+1)^2.$$

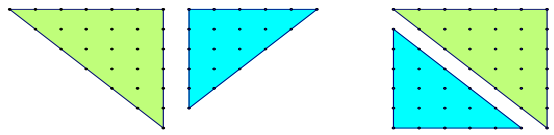

Figure 2.1: $1 + 3 + 5 + ... + (2n - 1) = n^2$

In order to show that "$P(n)$ implies $P(n+1)$" true, we need to prove $P(n+1)$ true from the above equality. We add both sides $(2n + 3)$, which is the next odd number in line. Hence we have

$$1+3+5+...+(2n+1)+(2n+3) = (n+1)^2+(2n+3) = n^2+2n+1+2n+3 = n^2+4n+4 \Rightarrow$$

$$1 + 3 + 5 + ... + (2n + 1) + (2(n + 1) + 1) = (n + 2)^2 = [(n + 1) + 1]^2.$$

But this last equality is precisely $P(n + 1)$. Therefore by the PMI we have

$$1 + 3 + 5 + ... + (2k - 1) = k^2 \tag{2.1}$$

for every $k \in \mathbb{N}$ (for $k = 1$ can be check it is correct too). ■

In Figure 2.1, we see a "**proof without words**" of the identity (2.1).

Problem 4: Show by induction that $1^2 + 2^2 + ... + n^2 = n(n + 1)(2n + 1)/6$ for every $n \in \mathbb{N}$.

Some less standard application of the induction principle is the following proof of AGM-inequality. We need to show that given a_1, a_2, ...,a_n non-negative numbers we have

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geq (\prod_{i=1}^{n} a_i)^{1/n}. \tag{2.2}$$

Let us observe that we can assume that the numbers are strictly positive. Without loss of generality, we may assume that $\prod_{i=1}^{n} a_i = 1$. Indeed, if the product is not equal to one but say P, we can reduce to this situation by substitution $b_i = a_i/P^{1/n}$, $i = 1, 2, ..., n$.

For the Basis Step, we need to prove that $(1/2)(a + b) \geq 1$ if $ab = 1$. This is as usual true since we can write $(1/2)(a + b) \geq 1$ as $(\sqrt{a} - \sqrt{b})^2 \geq 0$. For the Induction Step, we assume that for n positive numbers $\{a_i\}$ whose product is 1, we have $a_1 + a_2 + ... + a_n \geq n$. We need to show that given $n + 1$ positive numbers b_j, whose product is 1, then $b_1 + b_2 + ... + b_n + b_{n+1} \geq n + 1$.

We know that $b_1 b_2 ... b_n b_{n+1} = 1$. We notice that not all these numbers can be greater than 1. Otherwise the product is strictly greater than one. Hence, there exists $b_i \leq 1$. Similarly, not all the $b's$ can be less than 1. hence, there exists b_j $(i \neq j)$ such that $b_j \geq 1$. Without loss of generality, we may assume that i and j are 1 and 2. By the induction hypothesis, $b_1 b_2 + b_3 + ... + b_{n+1} \geq n$. Now, let us observe that $b_1 + b_2 \geq b_1 b_2 + 1$ is equivalent to $0 \geq (b_1 - 1)(b_2 - 1)$ (true by our assumption on b_1 and b_2). Therefore,

$$b_1 + b_2 + b_3 + ... + b_{n+1} \geq b_1 b_2 + 1 + b_3 + ... + b_{n+1} \geq n + 1,$$

which finishes the Induction Step. Hence by PMI, we must have (2.2) true for every n non-negative numbers.

Problem 1: *Find a similar argument by reducing the AGM to the case* $a_1 + a_2 + \cdots + a_n = n$*, i.e., proving by induction that if*

$$[a_i \geq 0, i = 1, 2, ..., n, a_1 + a_2 + \cdots + a_n = n] \Rightarrow \left(\prod_{i=1}^{n} a_i\right) \leq 1.$$

Problem 2: *Prove Bernoulli's inequality: for* $n \in \mathbb{N}$*, and* $a > -1$*, we have*

$$(1 + a)^n \geq 1 + na.$$

Problem 3: *Use AGM to prove Bernoulli's inequality.*

Problem 4: *Show that for every* $n \in \mathbb{N}$, $2^{3^n} + 1$ *is divisible by* 3^{n+1}.

Problem 5: *Every road in Sikinia is one-way. Every pair of cities is connected by exactly one direct road. Show that there exists a city which can be reached from every other city either directly or via at most one other city.*

Problem 6: *If one square of a* $2^n \times 2^n$ *chessboard is removed, then the remaining board can be covered by* $L - trominoes$.

Problem 7: *Given* n *circles in the plane, they divide the plane into regions. Show that one can color these regions with two colors, so that no regions with common boundary line are colored the same way. (Such a coloring is called a proper coloring).*

Problem 8: *All numbers of the form* 1007, 10017, 100117, ..., *are divisible by* 53.

Problem 9: *Prove that the cardinality of the set of all functions* $f : \{1, 2, ..., n\} \to \{0, 1\}$ *is* 2^n.

Problem 10: *Prove that the cardinality of the set of all one-to-one functions* $f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ *is* $n!$.

Problem 11: *Prove that* 57 *divides* $7^{n+2} + 8^{2n+1}$ *for every* $n \geq 0$.

Problem 12: *If* F_n *is the Fibonacci sequence show that* $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$, *for all* $m, n \in \mathbb{N}$.

2.1.1 Strong Mathematical Induction

The strong mathematical induction (PSMI) is stated in the following way:

Theorem 2.1.2. *For* $n \in \mathbb{N}$, *we let* $P(n)$ *be some statement. If the implications (i) and (ii) below are satisfied, then* $P(n)$ *is true for every* $n \in \mathbb{N}$.

(i) **Basis Step:** $P(1)$ *is true*

(ii) **Induction Step:** *Given* $n \in \mathbb{N}$, *then* $[P(1), P(2), ..., P(n)] \Rightarrow P(n + 1)$.

The two principles are equivalent and they are equivalent to the Well-Ordering Principle (Proposition 3.30 in [2]). The Well-Ordering Principle is stating that "Every non-empty set of natural numbers has a least element."

Two of the most important applications of SMI is the following theorems: *Bézout*'s Lemma and the Fundamental Theorem of Arithmetic (or the Unique Factorization Theorem or the Unique-Prime-Factorization Theorem). First let us start

with the *Bézout*'s Lemma.

Lemma 2.1.3. *Given two natural numbers m and n, then $gcd(m,n) = 1$ if and only if there exists integers x and y such that $mx + ny = 1$.*

Proof. (**Sufficiency:** $\Leftarrow$) Let us use a direct argument here. If $d \geq 1$ is a common divisor of m and n, since $1 = mx+ny$ it follows that d must divide $mx+ny$ or in other words d divides 1. Then, this forces $d = 1$, and so $gcd(m,n) = 1$.

(**Necessity:** $\Rightarrow$) We proceed by Strong Induction on $k = max(m,n)$. For the Basis Step let us say $k = 1$. Then, $m = n = 1$. We can pick $x = 2$ and $y = -1$ to satisfy the relation $mx + ny = 1$. For the Inductive Step, we fix $k \geq 1$ and assume that for every two given natural numbers m and n with $max(m,n) \leq k$ and $gcd(m,n) = 1$, we can find integers x and y such that $mx + ny = 1$. Let us take two natural number A and B such that $k + 1 = max(A,B)$ and $gcd(A,B) = 1$. First, we observe that A cannot be equal to B because in this case $A = B = k + 1$ and so $gcd(A,B) = k + 1 \geq 2$ ($k \geq 1$) leads us into a contradiction. Without loss of generality we may assume that $1 \leq A < B = k + 1$. This shows that $B = k + 1 \leq k + A$ which implies $b := B - A \leq k$ and $a := A \leq k$. Also, we observe that $\gcd(a,b) = 1$. Indeed, if $d \geq 1$ divides a and b, it must divide $b + a = (B - A) + A = B$ and so d must be 1 by the hypothesis that $gdc(A,B) = 1$.

Then we can use the Induction Hypothesis to find integer x' and y' such that $ax' + b'y = 1$ or $Ax' + (B - A)y' = 1$. This can be written as $A(x' - y') + By' = 1$ and so the conclusion we wanted follows.

Therefore, by SPMI we conclude that our lemma is true for every m and n. ■

Definition: A natural number $p > 1$ is a **prime** number if $p = ab$ for some $a, b \in \mathbb{N}$ implies $a = 1$ or $b = 1$.

This is saying that a prime cannot have any proper divisors, i.e. other than 1 and itself.

Corollary 2.1.4. *(of 2.1.3) Given a, b, c natural numbers and p a prime, we have:*

(i) If a divides bc and $\gcd(a,b) = 1$, then a divides c.

(ii) If p divides ab then p divides a or p divides b.

Proof. (i) By our Lemma we have $ax + by = 1$ for some integers x and y. Then, multiplying this by c we get $acx + bcy = c$. By hypothesis $bc = az$ for some integer z. Therefore $c = acx + bcy = acx + az = a(cx + zy)$ which shows that a divides c.

(ii) If p is a prime number, then $d = \gcd(p,a)$ is either 1 or p. If $d = p$ then p divides a and we are done. If $d = 1$, then by (i) we must have p dividing b. ■

With this preparation the proof of the following theorem is obvious and left to the reader.

Theorem 2.1.5. *Every natural number $n \in \mathbb{N}$, $n \geq 2$, is either a prime number or it can be written as a product of primes. The writing is unique up to the order of factors.*

Here is an example from the "The 70th William Lowell Putnam Mathematical Competition held on Saturday, December 5, 2009" : *Show that every positive rational number can be written as a quotient of products of factorials of (not necessarily distinct) primes. For example,*

$$\frac{10}{9} = \frac{2! \cdot 5!}{3! \cdot 3! \cdot 3!}.$$

Skecth of proof: We are going to use Strong Induction on $k = max(m, n)$ and show that m/n (in reduced form) has the required property. The **Basis Step** is $1 = 2!/2!$. To go from k to $k+1$ we look at the decompositions of m and n (such that $max(m, n) = k + 1$) in their prime factors. according to Theorem 2.1.5. If $k+1 = p$ is a prime then $k+1 = \frac{p!}{(p-1)!} = \frac{p!}{k!}$ and for all of the other factors involved we apply the induction hypothesis. If $k + 1$ is not a prime we just us the induction hypothesis on every factor of the factorizations involved.

One other example from "The 66th William Lowell Putnam Mathematical Competition held on Saturday, December 3, 2005" is: *Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$, where r and s are nonnegative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$.)*

Problem 13. *Prove that for all $n \geq 4$, we have $n! > 2^n$.*

Problem 14. *Prove that for any integer $n \geq 1$, $2^{2n} - 1$* is divisible by 3.

Problem 15. *Let a and b be two distinct integers, and n any positive integer. Prove that $a^n - b^n$ is divisible by $a - b$.*

Problem 16. *The Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13,...$ is defined as a sequence whose two first terms are $F_0 = 0$ and $F_1 = 1$ and each subsequent term is the sum of the two previous ones: $F_n = F_{n-1} + F_{n-2}$ (for $n \geq 2$). Prove that $F_n < 2^n$ for every $n \geq 0$.*

Problem 17. *Prove the identity for all positive integers n:*

$$\frac{1}{n+1}+\frac{1}{n+2}+\cdots+\frac{1}{2n}=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{2n-1}-\frac{1}{2n}.$$

Problem 18. *Show that for every $n \in \ltimes$, there exist a number of n digits containing only the digits 2 and 3.*

2.2 Direct and indirect proofs

A **direct proof** *of a conditional statement $p \to q$ is a valid argument that starts with p and ends with q.* **Definition 2.** *Given a real number x, by $\lfloor x \rfloor$, we understand the greatest integer k such that $k \leq x$.*

Let us show that for every real number x, we have

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1. \tag{2.3}$$

Let us say that $\lfloor x \rfloor = k$. We want to show that $k \leq x < k+1$. By definition, we must have $k \leq x$. By way of contradiction, let us assume that $x < k+1$ is not true. In other words $k+1 \leq x$. Since $k+1$ is an integer less than or equal to x, by definition of k as being the greatest with this property, we must have $k \geq k+1$. But this leads to the contradiction $0 \geq 1$. ■

More general, we have the following theorem which is usually referred to as the Division Algorithm.

Theorem 2.2.1. *Given an nonzero positive integer n (natural number, $n \in \mathbb{N}$) and an integer k, then there exists two (unique) integers q and r, $r \in \{0, 1, 2, ..., n-1\}$, such that $k = nq + r$.*

The number q is called **quotient** *and the number r is called the* **remainder**. *Let us use a direct proof of this theorem. Assume that the hypothesis is true. In other words we have an integer k and positive natural number n. To prove the conclusion we need to show the existence of q and r satisfying the required conditions. We define $q = \lfloor \frac{k}{n} \rfloor$ (greatest integer function defined earlier) and $r = k - nq$. We observe that $x = \frac{k}{n}$ is a well defined real number since n is not zero. Next, all we need to show is that $r \in \{0, 1, 2, ..., n-1\}$ or $0 \leq r < n$. Because we have proved in (2.3) that*

$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, we have $\lfloor \frac{k}{n} \rfloor \leq \frac{k}{n} < \lfloor \frac{k}{n} \rfloor + 1$. This can be written as $q \leq \frac{k}{n} < q+1$ or $0 \leq r < n$, which is exactly what we wanted. ■

An **indirect proof** *of a conditional statement $p \to q$, is either by contraposition by showing directly that $\neg q \to \neg p$ (using the fact that the contrapositive statement is logically equivalent to the original statement), or by* **contradiction** *by showing that if the conclusion q is not true then one can derive a contradiction (a statement of the form $r \wedge \neg r$).*

Definition 1. *An integer $k \in \mathbb{Z}$ is called* **even** *if $k = 2m$ for some integer m. An integer $k \in \mathbb{Z}$ is called* **odd** *if $k = 2m + 1$ for some integer m.*

We are going to prove the uniqueness stated in Theorem 2.2.2 latter. If $r = 0$ in Theorem 2.2.2, we say that k is a **multiple** *of n, or n* **divides** *k, or k is* **divisible** *by n.*

Another classical example is the following statement:

Theorem 2.2.2. *Given an integer k, then k^2 is either a multiple of 4 or a multiple of 8 plus one.*

Proof. Having an integer k, it is either even or odd. First, let us assume that k is even, i.e. $k = 2m$ for some integer m. Then $k^2 = 4m^2$ and so k^2 is a multiple of 4. So, the conclusion of our statement is true in this situation.

If k is odd, we have $k = 2m + 1$ for some integer m. This implies $k^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1$. To finish the proof, we observe that it is enough to prove that $m(m + 1)$ is even. This is clearly true if m is even and if m is odd then $m + 1$ is even. ■

In the previous proof we actually used an analysis by cases: k odd or k even. This is what usually is called a **proof by cases**.

Problem 1 Use a proof by cases to show that given an integer k, then $k(k+1)(k+2)$ is divisible by 3.

Problem 2 Use a proof by cases to show that given an integer k which is a multiple of 4 plus 3, then there are no integers x and y such that $k = x^2 + y^2$.

Definition 3 *A real number x is called rational if there exists two integers k and ℓ, with $\ell in \mathbb{N}$, such that $x = \frac{k}{\ell}$. A number which is not rational is called* **irrational**.

Problem 3 Prove by contradiction that $\sqrt{2}$ is irrational.

The proof of Theorem 2.2.2 is also called an existence proof (we showed the existence of q and r). The existence proofs can be **constructive** *or* **nonconstructive**. *The constructive proofs are providing an explicit algorithm or formula of how*

to obtain the objects from the given ones in a finite number of steps. The nonconstructive proofs show the existence without giving any clear method of how to obtain the objects claimed in the existence from some given data. One interesting example here is to prove the following theorem.

Theorem 2.2.3. *Prove that there exists a and b irrational numbers so that a^b is rational.*

Proof. Let us consider the number $x = \sqrt{2}^{\sqrt{2}}$. We know that $\sqrt{2}$ is irrational. We have two possibilities. Either x is rational, in which case the conclusion of our statement is true by taking $a = b = \sqrt{2}$. Or, x is irrational, in which case we observe that $x^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$ a rational and so the conclusion of our statement is true by taking $a = x$ and $b = \sqrt{2}$. ■

Let us observe that b is explicit in the proof but a is not. In fact, a is either $\sqrt{2}$ or $\sqrt{2}^{\sqrt{2}}$.

We end this section by showing the **uniqueness** *claimed in Theorem 2.2.2 by using an argument by way of contradiction. Suppose that we have two distinct writings, $k = nq_1 + r_1$ and $k = nq_2 + r_2$ with $r_1, r_2 \in \{0, 1, 2, ..., n-1\}$. We may assume, without loss of generality, that $q_1 \neq q_2$. Indeed, if $q_1 = q_2$ then $r_1 = k - nq_1 = k - nq_2 = r_2$ and so we have the same writing, but we assumed these writings were distinct. Since $|q_1 - q_2|$ is a positive integer, it must by at least 1. Then $n(q_1 - q_2) = r_2 - r_1$ which implies $|r_2 - r_1| = n|q_1 - q_2| \geq n(1) = n$. Suppose, without loss of generality, that $r_1 \geq r_2$. Then $n \leq r_2 - r_1 \leq r_2 < n$, which leads to the contradiction $n < n$. It remains that the two writings must be the same and the uniqueness in Theorem 2.2.2 is shown.*

2.3 Conjectures

In mathematics a **conjecture** *is a conditional statement which is believed to be true but no proof of it is known. In the previous example, Theorem 2.2.3, it is actually known that $\sqrt{2}^{\sqrt{2}}$ is irrational and even more it is transcendental. A real number x is called* **algebraic** *if is the solution of an equation of the form $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$ where a_i are integers. A real number which is not algebraic is called* **transcendental**. *David Hilbert (1862-1943), a German mathematician, has conjectured 23 problems at the beginning of the last century. One of these conjectures asked whether or not a^b is trancendental if a is algebraic not 0 or 1 and b is irrational algebraic. The problem was solved in 1935: Gelfond - Schneider theorem "If a and b are algebraic numbers with $a \notin \{0, 1\}$ and b irrational, then any value of ab is a transcendental number."*

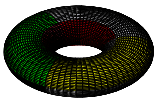

Figure 2.2: Toroidal chess board.

There are very many conjectures in mathematics. One less famous conjecture which may be of an interest to some of you is the so called half-domination problem in the toroidal kings graph. Suppose we have a chess board $m \times n$ *in which* m *is a multiple of* 5*. Think of the board as glued together in the the following way: the top and bottom sides and also the vertical sides without changing the orientation. We obtain what is called a toroidal chess board (see Figure 2.2). The conjecture asks to prove that one cannot place more than* $3mn/5$ *kings on this board so that each king attacks no more than* 4 *other kings.*

Chapter 3

Sets, Functions, Sequences and Sums

"A mathematician who can only generalise is like a monkey who can only climb up a tree, and a mathematician who can only specialise is like a monkey who can only climb down a tree. In fact neither the up monkey nor the down monkey is a viable creature. A real monkey must find food and escape his enemies and so must be able to incessantly climb up and down. A real mathematician must be able to generalise and specialise." Quoted in D MacHale, Comic Sections (Dublin 1993) George Pólya

3.1 Sets

Definition: *A* **set** *is an unordered collection of objects, called* **elements** *or* **members** *of the set. An element a of the set A is written as $a \in A$.*

The main sets of numbers are defined as usual $\mathbb{N} = \{1, 2, 3, ...\}$ (natural numbers), $\mathbb{Z} = \{... - 5, -4, -3, -2, -1, 0, 1, 2, ...\}$ (integers), $\mathbb{Q} = \{a/b | a \in \mathbb{Z}, b \in \mathbb{N}\}$ (rationals), $\mathbb{R}$ (all real numbers), and $\mathbb{C}$ (complex numbers).

The set $\{1, 2, 3, ..., n\}$ is usually denoted by $[n]$.

Definition: *The* **power set** *of a set A is the set of all subsets of A and it is denoted by $\mathcal{P}(A)$.*

Example: *If A is $\{a, b\}$ then $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.*

Definition: *An* **ordered n-tuple** *is a list $(a_1, a_2, ...a_n)$.*

Definition: *Let A and B be sets. The Cartesian product of A and B, denoted by*

$A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

Definition: *A set A is a* **subset** *of set B is every element in A is an element of B (notation $A \subset B$).*

Proposition Two sets A and B are equal, iff $A \subset B$ and $B \subset A$.

Problem 1: *Prove that if $A = \{x \in \mathbb{R} | x - x^2 < 0\}$ and $B = \{x \in \mathbb{R} | 0 < x < 1\} = (0, 1)$, then $A = B$.*

Problem 2: *Prove that if $A = \{n \in \mathbb{N} | 5$ divides $2^n - 1\}$ and $B = \{n \in \mathbb{N} | n = 4k, k \in \mathbb{Z}\}$, then $A = B$.*

3.2 Set Operations

Definition: *Given two sets A and B the* **union** *of these two sets is denoted by $A \cup B$ and it consists of the elements in A or the elements of B. The* **intersection** *of these sets is denoted by $A \cap B$ and it consists of those elements in A and in B. Two sets are said to be disjoint if $A \cap B = \emptyset$. The* **difference** *of A and B (in this order) is denoted by $A \setminus B$ and it consists of the elements in A which are not in B.*

Example: *If $A = \{1, 3, 5, 7\}$ and $B = \{2, 3, 4, 5\}$, then $A \cup B = \{1, 2, 3, 4, 5, 7\}$, $A \cap B = \{3, 5\}$ and $A \setminus B = \{1, 7\}$.*

The Principle of Inclusion-Exclusion gives the number of elements in a union of sets. If a set A is finite, we denote the number of elements by $|A|$ (called also the cardinality of A):

$$|A \cup B| = |A| + |B| - |A \cap B| \ (2 \ sets),$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \ (3 \ sets).$$

If a set U contains all the elements of the sets we are interested in, it is usually called the universe that is understood in the concept of **complement** *of a set A which is simply $U \setminus A$.*

3.3 Functions

Definition: *A* **function** *(or* **map***) f defined on A (domain) with values in B (target) is a way of assigning to every element in A one and only one element in*

B. If $a \in A$ is arbitrary (usually called input) and $b \in B$ is assigned to a, we write $b = f(a)$ (b is called output). We usually write $f : A \to B$. Every function must have all these three characteristics, the domain, the target and the rule which is the way the assignment goes.

Example: *Let's take the ceiling function c defined on all real numbers x to be the smallest integer k greater than or equal to x. So, we can say that $x : \mathbb{R} \to \mathbb{Z}$ and $c(x) = k$ where $k - 1 < x \leq k$. The usual notation for c is actually $c(x) = \lceil x \rceil$.*

Definition: *A function is said to be* **one-to-one** *or* **injective** *if for different inputs we obtain different outputs.*

Example: *The function called* **absolute value** *with domain and target $\mathbb{R}$ defined by the rule*

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0, \end{cases}$$

is not injective since for different inputs 1 and -1 we have $|1| = |-1| = 1$.

Problem 3: *Show that $f : \mathbb{R} \to \mathbb{R}$ given by the rule $f(x) = 2x - |x|$ is injective.*

Definition: *A function is said to be* **onto** *or* **surjective** *if every element in the target is the output of some input. A function which is a surjection and an injection at the same time is called a* **bijection** *or is said to be* **bijective**.

Example: *Consider the function $f : \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{1\}$ defined by the rule $f(x) = \frac{x+1}{x-1}$. This is a surjection since if we take an element in the target y, there exists and element in the domain x, (check that $x = f(y)$) such that $f(x) = y$.*

Problem 4: *Prove that the function $f : [n] \to [n]$ given by the rule $f(x) = n + 1 - x$ is a bijection (surjection and injection).*

Problem 5: *Consider the set $A := \{0, 1, 2, ..., n-1\}$ the usual set of remainders when dividing a number by $n \in \mathbb{N}$. Define the function $f(x) = r$ where $2x = nq + r$ given by the Division algorithm (q and r are unique). Show that f is a bijection iff n is odd.*

Problem 6: *Use a proof by cases, show that $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.*

Definition: *The* **factorial** *function $F : \mathbb{N} \cup \{0\} \to \mathbb{Z}$ is defined by the rule, $F(0) = 0! = 1$, $F(1) = 1$ and $F(n) = \underbrace{n(n-1)\cdots(2)(1)}_{n \text{ factors}}$ for every $n \geq 2$.*

Example: *Example* $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$,....

Definition: *Given $f : A \to B$ and $g : B \to C$ then we can consider the* **composition** *of these two functions, denoted by $g \circ f : A \to C$ defined by the rule $(g \circ f)(x) = g(f(x))$ for every $x \in A$.*

Definition: *A function $f : A \to B$ has an* **inverse**, *denoted by $f^{-1} : B \to A$ if $f \circ f^{-1}$ and $f^{-1} \circ f$ are the identity functions.*

Theorem *A function has an inverse iff it is one-to-one and onto.*

Let S be a subset of an universal set U. The **characteristic function** χ_S *of S is the function $\chi : U \to \{0, 1\}$ such that $\chi_S(x) = 1$ if $x \in S$ and $\chi_S(x) = 1$ if $x \notin S$. Let A and B be sets in U. Show that a) $\chi_A = \chi_B$ iff $A = B$*

b) $\chi_{\overline{A}} = 1 - \chi_A$

c) $\chi_{A \cap B} = \chi_A \chi_B$

d) $\chi_{A \cup B} = \chi_A + \chi_B - \chi_A \chi_B$

e) $\chi_{A \setminus B} = \chi_A - \chi_A \chi_B$

Problem 7: *Use the technique of the characteristic function to prove the set identity $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

Problem 8: *Use the technique of the characteristic function to prove that the symmetric difference is an associative operation:*

$$(A \Delta B) \Delta C = A \Delta (B \Delta C).$$

Important identities, to show by induction:

$$\sum_{k=0}^{n} r^k = 1 + r + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}, \ r \neq 1,$$

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}, \sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4},$$

$$\sum_{k=0}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

Definition: *We say that two sets have the same* **cardinality** *(or the same number of elements) if there exists a bijection from A to B.*

Theorem I: *If A is finite and $f : A \to A$ is one-to-one, then f is also onto.*

Theorem II: *If A is finite and $f : A \to A$ is onto then f is also one-to-one.*

SCHRÖDER-BERNSTEIN THEOREM *If $f : A \to B$ and $g : B \to A$ are two one-to one maps, then $|A| = |B|$.*

Chapter 4

Propositional logic

"When introduced at the wrong time or place, good logic may be the worst enemy of good teaching. The American Mathematical Monthly 100 (3)."
George Pólya

4.1 Simple logical operators

A **proposition** *is a declarative sentence that can be determined to be either true or false, but not both. We use letters like p, q, r etc. for propositional variables.*

Example: p: For $x = 7$ *and* $y = 8$*, we have* $(x + y)^2 = x^2 + 2xy + y^2$*.*

q: For $x = 2$ *and* $y = 3$*, we have* $(x + y)^2 = x^2 + y^2$*.*

We see that p is true and q is false.

The **negation** *of a proposition p, denoted by* $\neg p$ *is the statement "It is not the case that p."*

Example: $\neg p$*: For* $x = 7$ *and* $y = 8$*, we have* $(x + y)^2 \neq x^2 + 2xy + y^2$*.*

$\neg q$*: For* $x = 2$ *and* $y = 3$*, we have* $(x + y)^2 \neq x^2 + y^2$*.*

Logical operators which are used to form new propositions from two or more existing propositions are called **connectives***. Given p and q two propositions, we have the* **conjunction** *of these, denoted by* $p \wedge q$*, which is the proposition "p and q". The conjunction* $p \wedge q$ *is true if both p and q are true and false otherwise.*

Given p and q two propositions, we have the **disjunction** *of these, denoted by* $p \vee q$*, which is the proposition "p or q". The disjunction* $p \vee q$ *is false if both p and q are false and true otherwise.*

Given p and q two propositions, we have the **exclusive or** *of these, denoted by $p \oplus q$, which is the proposition "p or q, both not both". The exclusive or $p \oplus q$ is true if exactly one of p and q is true, and false otherwise.*

The Truth Table for all of these connectives defined so far is given in the table below.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	F	T	T	F
T	F	F	F	T	T
F	T	T	F	T	T
F	F	T	F	F	F

Given p and q two propositions, we have the **conditional statement**, *denoted by $p \to q$, which is the proposition "if p, then q". The implication $p \to q$ is false if p is true and q is false, and true otherwise. p is usually called* **hypothesis** *and q is called* **conclusion**.

The Truth table above can be completed to

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$
T	T	F	T	T	F	T
T	F	F	F	T	T	F
F	T	T	F	T	T	T
F	F	T	F	F	F	T

The "implication" is used in mathematics especially in the statement of theorems and one may encounter various ways to express it: "p implies q" or "q follows from p", "if p, q", "p is sufficient for q" or "p is a sufficient condition for q" or "a sufficient condition for q is p" , "q if p", "q is necessary for p" or "a necessary condition for p is q", and "q unless $\neg p$".

The last formulation is less used, but let us observe that the Truth values of $p \to q$ and $q \vee \neg p$ are the same:

p	q	$\neg p$	$q \vee \neg p$	$p \to q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

To give an example, let us write the implication "If $|x| > 2$ then $x^2 > 4$." in the form "q unless $\neg p$": "We have $x^2 > 4$ unless $|x| \leq 2$".

When two compound proposition have the same truth values, we called them **equivalent**. *The* **converse** *of $p \to q$ is the implication $q \to p$. The* **contrapositive** *of $p \to q$ is the implication $\neg q \to \neg p$. The* **inverse** *of $p \to q$ is the implication $\neg p \to \neg q$.*

Compound propositions p and q with the same truth values are called **logically equivalent** *and we write $p \equiv q$.*

The important observation here is that an implication and its contrapositive are logically equivalent statements. Indeed, the Truth table given below confirms this

p	q	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Let us look at some examples. It is clear that the Pythagorean Theorem,

"If a right triangle has legs a and b and hypothenuse c, then $a^2 + b^2 = c^2$"

can be reformulated as its contrapositive:

"If in a triangles the biggest side, say c, does not satisfy $c^2 = a^2 + b^2$, then the triangle is not a right triangle".

Given p and q two propositions, we have the **biconditional statement**, *denoted by $p \leftrightarrow q$, which is the proposition "p if and only if q". The equivalence $p \leftrightarrow q$ is true if p and q have the same truth values, and false otherwise. This connective is the most important in mathematics. Most of the important theorems in mathematics are biconditional statements.*

In geometry for instance, almost every true statement can be turned into a biconditional statement (characterization). For onstance, the formulation of the Pythagorean Theorem as a biconditional statement is

"Given a triangle whose sides are a, b and c with $a \leq b \leq c$, the triangle is a right triangle if and only if $a^2 + b^2 = c^2$."

Other common formulations for $p \leftrightarrow q$ are "p is necessary and sufficient for q", "p iff q" and "if p then q, and conversely".

Applications of propositional logic are found in translating English sentences, system specifications, boolean searches (web page searching), logic puzzles, logic circuits, etc.

Definition: *A compound proposition whose truth values are all T (true) is called a* **tautology**. *A compound proposition whose truth values are all F (false) is called a* **contradiction**. *A compound proposition which is neither a tautology nor a contradiction is called a* **contingency**.

Examples: $p \vee \neg p$ is a tautology and $p \wedge \neg p$ is a contradiction for every proposition p. Taking two logically equivalent compound propositions p and q, the biconditional statement $p \leftrightarrow q$ becomes a tautology. The most famous of logically equivalent

compound propositions are given by the **De Morgan Laws:**

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \textit{and} \quad \neg(p \vee q) \equiv \neg p \wedge \neg q.$$

Another example of logically equivalent compound propositions which involves three propositional variables is the distributive law of conjunction with respect to disjunction:

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

Definition: *A compound proposition for which there exists a T value in its Truth table is called* **satisfiable**.

Problem: *Write an algorithm to solve a given* 4×4 *Sudoku puzzle.*

It is interesting that Integer Linear Programming can be used to solve the classical Sudoku puzzles with the idea of assigning Boolean variables $x(i, j, k)$ *having value of* 1 *if in the cell* (i, j) *there is a* k *in the feasible solution (which is unique), and* 0 *otherwise.*

4.2 Predicates and Quantifiers

If a proposition p *depends on a certain number of variables* x_1, x_2, ... *then we call it a* **propositional function** $P(x_1, x_2, ...)$.

The universal quantifier as a symbol is $\forall$ *and the existential quantifier is* $\exists$.

Example: $\forall$ x *and* y *real numbers, we have* $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.

The negation of $\forall x P(x)$ *is* $\exists x \neg P(x)$.

The negation of $\exists x P(x)$ *is* $\forall x \neg P(x)$.

Nested quantifiers make a difference in mathematics.

Example 1: *Let us look into this by defining the concept of a bounded real valued function. Suppose* f *is a function defined on* $\mathbb{R}$ *and with values in* $\mathbb{R}$. *We say that* f *is bounded if*

$$\exists M \geq 0, \forall\ x \in \mathbb{R}\ (|f(x)| \leq M).$$

If we change the order of the quantifiers we obtain

$$\forall\ x, \in \mathbb{R} \exists M \geq 0,\ (|f(x)| \leq M).$$

This is saying that every function f is bounded which makes the definition useless.

Example 2: *Use nested quantifiers to write the definition of the limit of a function.*

Given a real-valued function f defined on a domain $D = (a, b) \setminus \{x_0\}$, we say that f has limit L at x_0 if

$\forall \epsilon > 0, \exists\ \delta > 0\ (\ 0 < |x - x_0| < \delta \rightarrow |f(x) - L| \leq \epsilon)$.

The negation of this definition is what we usually encounter when a function doesn't have a limit at a point.

So, f does not have L as its limit at x_0 if

$\exists \epsilon > 0, \forall\ \delta > 0\ (\ 0 < |x - x_0| < \delta \wedge |f(x) - L| > \epsilon)$.

Chapter 5

Relations and Graphs

5.1 Relations

Definition: *Given two sets A an B, a* **relation** *from A to B is just a subset of $A \times B$. A relation on a set A is a relation from A to A.*

If $R \subset A \times B$ then for an element (a, b) in R, we say that a is in the relation R with b.

Example: *Let us defined $\mathcal{D}$ as the divisibility relation on $\mathbb{N}$: $(a, b) \in \mathcal{D}$ if and only if a divides b. For instance, $(5, 10) \in \mathcal{D}$ but $(3, 4) \notin \mathcal{D}$.*

Observation: *Every function f defined on A and with values in B is an example of a relation by setting $(a, b) \in R_f$ if and only if $b = f(a)$. Some textbooks define the concept of function in terms of the concept of relation by saying that every two pairs $(a, b), (a, b') \in R_f$ implies $b = b'$. So, in general a relation is not a function. For example, the divisibility relation on $\mathbb{N}$ is not a functions since $(2, 4)$ and $(2, 6)$ are in $\mathcal{D}$.*

Given a finite set A with n elements we have 2^{n^2} possible relations on A (the number of subsets of $A \times A$). Of these only n^n are functions, and only $n!$ are bijections.

5.1.1 Properties of Relations

Definition: *We say that a relation R on a set A is* **reflexive** *if $(a, a) \in R$ for every $a \in A$.*

The divisibility relation $\mathcal{D}$, defined earlier, is reflexive. Let us define the relation of usual order $\mathcal{O}$ on the real numbers: two real numbers x, and y are in this

relation, $(x, y) \in \mathcal{O}$, if and only if $x \leq y$. This relation is also reflexive since for every real number x, we can say that $x \leq x$.

Definition: *We say that a relation R on a set A is* **symmetric** *if $(a, b) \in R$ implies $(b, a) \in R$. A relation R on a set A is* **anti-symmetric** *if $(a, b) \in R$ and $(b, a) \in R$ implies $a = b$.*

The relation of order defined earlier, $\mathcal{O}$ is not symmetric but antisymmetric. The same is true for $\mathcal{D}$. Let us define a new relation which is going to be very much used in what follows, the (mod n) relation of integers for some fixed natural number n: two integers k and ℓ are in this relation, if $k - \ell$ is divisible by n. We write usually this by $k \equiv \ell \pmod{n}$. This relation is clearly symmetric since if $k \equiv \ell \pmod{n}$ then $\ell \equiv k \pmod{n}$.

Definition: *We say that a relation R on a set A is* **transitive** *if $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$.*

All relations defined earlier are transitive.

Problem 1: *How many reflexive/symmetric/antisymmetric exist on a finite set with n elements ?*

The similar problem for transitive relations is open (not even a conjecture) but some results are known, for instance, there are $3,994$ transitive relations on a set with 4 elements (see the number A006905 in the The On-Line Encyclopedia of Integer Sequences).

Definition: *A relation which is reflexive, symmetric and transitive is called an* **equivalence relation**. *For an equivalence relation R on a set A, the set of all elements $y \in A$ which are in relation with a given x is called the* **equivalence class of** *x and it is sometime denoted by $\overline{x}$.*

Problem 2: *Show that the relation $\equiv \pmod{n}$ on the set of integers is an equivalence relation.*

The set of equivalence classes for the relation $\equiv \pmod{n}$ is usually denoted by $\mathbb{Z}_n$.

Let us define two operations on $\mathbb{Z}_n$, denoted $+$ and $\cdot$ by

$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{and} \quad \overline{x} \cdot \overline{x} = \overline{x \cdot y},$$

for every x, $y \in \mathbb{Z}$.

Problem 3: *Show that the operations defined above are well defined (do not depend of the representatives chosen of a class).*

Problem 4: *Show that $\mathbb{Z}_n$ with these operations forms a commutative ring with*

unity.

Proposition 5.1.1. *If p is a prime, then $\mathbb{Z}_p$ is a field.*

Proof. We need to show that every non-zero class $\overline{x}$ has an inverse. The fact that $\overline{x} \neq \overline{0}$ means x is not divisible by p, or $gcd(x,p) = 1$. By Bezout's lemma there exists y and z such that $xy + pz = 1$ or $\overline{x} \cdot \overline{x} = \overline{1}$. ■

Problem 5: *If p is a prime, and $\overline{a}$ is a non-zero class, then $f : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by $f(\overline{x}) = \overline{a} \cdot \overline{x}$, is a bijection.*

Theorem 5.1.2. *(Fermat's Little Theorem) If p is a prime, and $\overline{a}$ is a non-zero class in $\mathbb{Z}_p$, then $\overline{a}^{p-1} = \overline{1}$ or equivalently, for every integer a not divisible by prime p then $a^{p-1} - 1$ is divisible by p.*

Proof. Exercise

5.1.2 Combining Relations

Since relations are subsets, any two relations can be combined in a way two subsets can be combined: union, intersection, and difference. One special case here is that the usual composition of functions can be generalized for relations.

Definition: *Given a relation R from A to B and a relation S from B to C, then the* **composite** *or R and S is the relation denoted by $S \circ R$ from A to C defined by $(a,c) \in S \circ R$ if and only if there exists an element $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$.*

Given a relation R on a set A we can iterate this composition, so R^n is the composite relation $\underbrace{R \circ R \circ ....R}_{n-times}$.

Theorem 5.1.3. *A relation on A is transitive if and only if $R^n \subset R$ for every $n \in \mathbb{N}$.*

Problem: *Show that if R is symmetric then R^n is symmetric for every $n \in \mathbb{N}$.*

5.2 Graphs

Definition: *A* **graph** *is a triple $G = (V, E, h_G)$ where V is a nonempty set whose elements are called vertices, E a set whose elements are called edges and $h_G : E \to V^2$ (directed graph) or $h_G : E \to \mathcal{P}(V)_2$ (undirected graph). For $e \in E$ and $h_G(e) =$*

uv we say that u and v are the **endpoints** *(or u and v are adjacent, if e is irrelevant) of e and e is* **incident** *to u and v. If u = v, we say e is a* **loop**.

In the case h_G is injective, we say G is a **simple graph** *(it doesn't allow multiple edges), and in this case we write $e = uv$ instead of $h_g(e) = uv$. If h_G is not injective, we have what are usually called* **multigraph** *and we have the concept of multiplicity of an edge e: cardinality of $h_G^{-1}(h_G(e))$.*

The set V can be infinite or finite, in which case we say the graph is a **infinite graph** *or an* **finite graph**. *For examples of concrete models of graphs see 10.1 in our textbook.*

Definition: *Given a undirected graph $G = (V, E, h_G)$, for a vertex $v \in V$ we denote by $N(v)$ the set of all vertices $u \in V$ which are adjacent to v. The set $N(v)$ is called the* **neighborhood** *of v. The cardinality of $h_G^{-1}(\{vu | u \in N(v)\})$ is usually called the degree of the vertex v - the loops are counted twice and it is denoted by $deg(v)$*

A undirected graph whose every vertex has the same degree is called a **regular** *graph.*

Theorem 5.2.1. The Handshaking Theorem *Let $G = (V, E, h_G)$ be an undirected graph $m = |E|$ edges. Then*

$$2m = \sum_{v \in V} deg(v). \tag{5.1}$$

Corollary 5.2.2. *An undirected graph has an even number of vertices with an odd degree.*

Bibliography

[1] Arthur Engel, Problem-Solving Strategies, Springer 1998

[2] John P. D'Angelo and Douglas. B. West, Problem-solving and proofs, Prentice Hall, 2nd Edition, 1997

[3] David S. Gunderson, Hanbook of Mathematical Induction, CRC Press, 7th Edition, 2010

[4] Kenneth H. Rosen, Discrete Mathematics and Its Applications, McGraw Hill, 7th Edition, 2012