Discrete Mathematics, Class Notes

Eugen J. Ionascu © *Draft dated August 18, 2016*

Contents

List of Figures

List of Tables

Preface

These notes are mostly intended to bring a personal take on some of the topics taught today in a Discrete Mathematics courses. We used at the beginning the classic textbook of K. Rosen [1].

Chapter 1

Propositional logic

> Any new concept must be described as a special case of a more general concept: " a square is a quadrilateral (general concept) with four congruent sides and one right angle (special case)". Aristotle (Criterion of hierarchy)

1.1 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.

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

$\boxed{\mathbf{q}}$: For $x = 2$ and $y = 3$, we have $(x + y)^2 = x^2 + y^2$.

$\boxed{\mathbf{r}}$: For $x = 4$ and $y = 3$, we have $\sqrt{x^2 + y^2} = x + y$.

$\boxed{\mathbf{s}}$: For $x = 3$, the two fractions $\dfrac{2+x}{4+x}$, $\dfrac{1+x}{2+x}$ are equivalent.

t: $1 + 2 + 3 + ... + 63 = 2016$.

u: $2016 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5$

v: $2016 = 3^3 + 4^3 + 5^3 + 6^3 + 7^3 + 8^3 + 9^3$

$\boxed{\mathbf{w}}$: A chess board without two of the opposite corners can be covered with 2×1 dominoes pieces.

x: In the decimals of π there is an appearance of 2016, in other words one can write

$$\pi = 3.\underbrace{1415.....}_{n-decimals}2016....$$

y: Given two real number, we have

$$4a^4 + b^4 = [a^2 + (a+b)^2][a^2 + (a-b)^2]. \text{ (Sophie Germain's Identity)}$$

†**z**: There are exactly six sentences in this list that are true.

One can check that p, t, u, v, x and y are true and q, r, s and w are false. Check if z is true or false.

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

Examples: $\neg p$: 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. With the examples above for proposition t and u, we can write

$$t \wedge u: \quad 2016 = 1 + 2 + 3 + ... + 63 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5.$$

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.

Example: In this example let us assume that x and y are positive real numbers such that $x + y = 10$. We then consider the statements p: "$x \geq 5$" and q: "$y \geq 5$". Then $p \vee q$ is the statement $x \geq 5$ or $y \geq 5$. We will see that $p \vee q$ is true.

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.

Example: In this example let us assume that x is a whole number, i.e. 0, 1, 2, ... etc. We then consider the statements p: "$x/2$ is a whole number" and q: "$(x+1)/2$ is a whole number". Then $p \oplus q$ is the statement "exactly one of the two numbers $x/2$, $(x+1)/2$ is a whole number". We will see that $p \oplus q$ is true.

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 $|x| \leq 2$". Let us state a few of the most famous theorems in mathematics.

Examples: Pythagorean Theorem: *If a, b are the lengths of the legs of a right triangle and c is the length of its hypothenuse, then $a^2 + b^2 = c^2$.*

Fundamental Theorem of Algebra: *If $P(z)$ is a polynomial with complex coefficients of degree at least one, then $P(\zeta) = 0$ for at least one complex number ζ.*

Lagrange's Four-Square Theorem: *If x is a whole number, then there exist four whole numbers a, b, c and d such that $x = a^2 + b^2 + c^2 + d^2$*

When two compound proposition have the same truth values, we called them **logically equivalent** and we write $p \equiv q$. For instance, it is obvious that $p \equiv \neg(\neg p)$ for every proposition p. The **converse** of $p \to q$ is the implication $q \to p$.

In general, the converse of a theorem is not necessarily true. Let's take an example from Calculus: "Given a differentiable function, then it is continuous. " The converse is not true since $f(x) = |x|$ is continuous but not differentiable.

The **contrapositive** of $p \to q$ is the implication $\neg q \to \neg p$. The **inverse** of $p \to q$ is the implication $\neg p \to \neg q$.

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 instance, 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:**

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

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

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r). \tag{1.1}$$

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

An important observation at this point is the fact that the Truth Tables can be replaced by usual calculations with $0'$ and $1'$ in the following way. If p and q are thought as valued functions with two real number values, 1 for T and 0 for F then the tables above can be transformed as follows:

p	q	$\neg p := 1 - p$	$p \wedge q := pq$	$p \vee q := p + q - pq$	$p \oplus q$	$p \to q$
1	1	0	1	1	0	1
1	0	0	0	1	1	0
0	1	1	0	1	1	1
0	0	1	0	0	0	1

Problem 1: *What are some equivalent formulae for $p \oplus q$ and $p \to q$?*

Problem 2: *Prove (1.1) using this equivalent way instead of Truth Table.*

1.2 Predicates and Quantifiers

Criterion of existence: "Also required by Aristotle, this criterion demands proof that at least one instance of the newly defined concept exists."

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 $\exists$.

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

Fixed Point Theorem: $\forall$ $f : [a, b] \to [a, b]$ *continuous function,* $\exists$ $x \in [a, b]$ *such that* $f(x) = x$.

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

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

The order for nested quantifiers makes a big difference in defining the concepts in mathematics or stating a theorem.

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

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

With a moment of thought, this is saying that every function f is bounded which makes the definition useless.

Example 2: Use nested quantifiers to write the definition of a convergent sequence.

Given a real-valued sequence $\{x_n\}_{n\geq 1}$*, we say that it is* **convergent to the limit** ℓ*, if*

$\forall \epsilon > 0$, $\exists\ n \in \mathbb{N}$, $\forall \in m \geq n\ (\ |x_m - \ell| \leq \epsilon)$.

Example 3: 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*

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

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*

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

1.3 Introduction to proofs

By an **argument** we understand a sequence of conditional statements,

$$p_1 \to p_2, p_2 \to p_3, ..., p_{n-1} \to p_n. \tag{1.2}$$

An argument is **valid** if having the **premise** p_1 true, it follows that all the conditionals statements in that argument are true and finally, as a result, the **conclusion** p_n, must be true.

A **direct proof** of a conditional statement $p \to qn$ (as in (1.2) is a valid argument (as in (1.2) that starts with $p_1 = p$ and ends with $p_n = q$.

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.

Definition 2. Given a real number x, by $\lfloor x \rfloor$, we understand the greatest integer k such that $k \leq x$.

Examples of direct and indirect proofs

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

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1. \tag{1.3}$$

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 1.3.1. (Division Algorithm) *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 a 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, since q is an integer by definition and as result r is, all we need to show is that $r \in \{0, 1, 2, ..., n-1\}$ or $0 \leq r < n$. Because we have proved in (1.3) 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 $nq \leq k < nq + n$ and after subtracting nq, we get $0 \leq r < n$, which is exactly what we wanted. ■

We are going to prove the uniqueness stated in Theorem 1.3.2 latter. If $r = 0$ in Theorem 1.3.2, we say that k is a **multiple** of n, or n **divides** k, or k is **divisible** by n. and as notations we use $n|k$ or $k \vdots n$.

Another classical example is the following statement:

Theorem 1.3.2. *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 1.3.2 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 1.3.3. *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 1.3.2 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 1.3.2 is shown.

1.3.1 Proofs by Induction

The Principle of Mathematical Induction (PMI) is used to show that some proposition $P(n)$ is true for every $n \in \mathbb{N}$. This principle states that if $P(1)$ is true (**Basis Step**) and for every $n \in \mathbb{N}$ we have "$P(n)$ implies $P(n+1)$" true (the **Inductive Step:**), then $P(k)$ is true for all $k \in \mathbb{N}$.

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

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

Figure 1.1: $1+3+5+...+(2n-1)=n^2$

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,

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

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

$$1+3+5+...+(2k-1)=k^2 \tag{1.4}$$

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

In Figure 1.1, we see a "**proof without words**" of the identity (1.4).

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

A variation of this mathematical induction method is the so called the **strong induction**, which is logically equivalent to the regular induction. The only difference is that in the Inductive Step we get to assume more, i.e. we need to show that for every $n \in \mathbb{N}$ we have "($P(1)$, $P(2)$, ..., $P(n)$) implies $P(n+1)$" true.

Let us show the following important theorem known as *Bézout*'s Lemma.

Lemma 1.3.4. *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 $d \geq$ is a common divisor of m and n, since $mx + ny = 1$ if follows that d must divide $mx + ny = 1$. Then, this forces $d = 1$, or $gcd(m,n) = 1$.

(**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.

Hence, by SPMI we conclude that our lemma is true for every m and 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

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geq (\prod_{i=1}^{n} a_i)^{1/n}. \tag{1.5}$$

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 (1.5) true for every n non-negative numbers.

More Problems to practice induction:

Problem 5. *Prove that for all $n \geq 4$, we have $n! > 2^n$.*

Problem 6. *Prove that for any integer $n \geq 1$, $2^{2n} - 1$* is divisible by 3.

Problem 7. *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 8. *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 9. *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 10. *Show that for every $n \in \mathbb{N}$, there exist a number of n digits containing only the digits 2 and 3.*

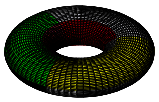

Figure 1.2: Toroidal chess board.

1.4 Conjectures and their role in mathematics

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 1.3.3, 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 a^b is a transcendental number."

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 1.2).

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.

Some more examples of open conjectures in mathematics.

Erdos-Straus Conjecture: *For all $n \in \mathbb{N}$, $n \geq 2$, there exists a, b and c in $\mathbb{N}$ such*

that

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

P vs NP: *If a problem whose solution can be checked in polynomial time, can be actually solved in polynomial time.*

More information about the $1,000,000 conjectures can be found at http://www.claymath.org/

Chapter 2

Sets, Functions, Sequences and Sums

2.1 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 $A = \{n \in \mathbb{N} | 5 \text{ } \textit{divides} \text{ } 2^n - 1\}$ and $B = \{n \in \mathbb{N} | n =$

$4k, k \in \mathbb{Z}\}$, then $A = B$.

2.2 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 $U \setminus A$.

2.3 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) for every $S \subset U$, $\chi_S^2 = \chi_S$

b) $\chi_A = \chi_B$ iff $A = B$

c) $A \subset B$ iff $\chi_A \leq \chi_B$

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

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

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

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

h) $\chi_{A\Delta B} = (\chi_A - \chi_B)^2$

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:*

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

Proof. Using the properties b) and h) we need to check that

$$((\chi_A - \chi_B)^2 - \chi_C)^2 = (\chi_A - (\chi_B - \chi_C)^2)^2. \tag{2.1}$$

To prove (2.1), first we use the difference of squares formula $a^2 - b^2 = (a-b)(a+b)$ and the property $(\chi_X)^2 = \chi_X$ for every set X. Then (2.1) is equivalent to

$$(\chi_A - \chi_B - \chi_C)^2(\chi_A - \chi_B + \chi_C)^2 = (\chi_A - \chi_B + \chi_C)^2(\chi_A + \chi_B - \chi_C)^2. \tag{2.2}$$

We observe that two of the factors are the same but the other two are not formally identical. In order to prove the identity (2.2) we see that it is enough to show that $\chi_A - \chi_B + \chi_C \neq 0$ implies $(\chi_A - \chi_B - \chi_C)^2 = (\chi_A + \chi_B - \chi_C)^2$. The last equality is the same as $\chi_B(\chi_A - \chi_C) = 0$. If $\chi_B(x)$ is not 0, then $\chi_A(x) - \chi_B(x) + \chi_C(x) = \chi_A(x) - 1 + \chi_C(x) \neq 0$. This relation can happen only if $\chi_A(x)$ and $\chi_C(x)$ are both zero or both 1. This shows that $\chi_A(x) - \chi_C(x) = 0$. Hence, $\chi_B(\chi_A - \chi_C) = 0$ if $\chi_A - \chi_B + \chi_C \neq 0$. Therefore, we have (2.2) and so (2.1) is correct. ■

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 $|A| = |B|$.

2.4 Linear Recurrent Sequences

First let us start with sequences that are given by a recurrence relation of degree one

$$x_{n+1} = ax_n + b_n, n \geq 1, \tag{2.3}$$

where a is a constant and b_n is known sequence; the first term of the sequence is x_1 which is also known. First if $a = 1$ then the general solution of (2.4) is simply $\boxed{x_{n+1} = x_1 + \sum_{k=1}^{n} b_k}$ which can be checked by induction, or one can arrive to this by using the method of telescoping sums. If $\{b_n\} = 0$ the recurrence is called homogeneous.

In what follows we will first deal with the case of a constant sequence $\{b_n\} = \{b\}$.

If $a \neq 1$ then we can make a substitution $y_n = x_n - \alpha$, where α is chosen in such a way that the recurrence for y_n becomes $y_n = ay_{n-1}$. This implies that $x_n - \alpha = ax_{n-1} - a\alpha$ or $(1-a)\alpha = b$. Hence $\boxed{\alpha = \frac{b}{1-a}}$. Solving for y_n, we get $y_n = a^{n-1}y_1$ which can be checked by induction or by the same telescoping principle in the product version.

Going back to x_n, this implies $x_n = \alpha + a^{n-1}(x_1 - \alpha)$ or

$$x_n = \frac{b + a^{n-1}[x_1(1-a) - b]}{1-a}.$$

We observe that the solution is of the form $C_1 a^n + C_2$. So, we can try to solve for such constants to determine the sequence.

Example 1: If the recurrence relation is $x_n = \frac{1+x_{n-1}}{2}$ with $x_1 = 0$ then the general term given by the above formula is $x_n = 1 - \frac{1}{2^{n-1}}$.

Example 2: Let us look at a non-homogeneous case: $x_{n+1} = 2x_n + n$, with $x_1 = 0$. We observe that we can add both sides $n+2$ and obtain $x_{n+1} + n + 2 = 2(x_n + n + 1)$, so if we introduce $y_n = x_n + n + 1$, then we have $y_{n+1} = 2y_n$. Since $y_1 = 2$, we see that $y_n = 2^n$, which gives $x_n = 2^n - n - 1$. So, the idea is to make a substitution and reduce it again to the homogeneous case.

Problem 9: *Find a simple formula for the recurrent sequence* $x_{n+1} = 2x_n + n^2$ *where* $x_1 = 0$.

Problem 10: *Prove by induction that the sequence in Problem 9 has the formula* $x_n = 3(2^n) - n^2 - 2n - 3$, $n \geq 1$.

For sequences that are given by a recurrence relation of degree two, let us start with the homogeneous case:

$$x_n = ax_{n-1} + bx_{n-2}, n \geq 3, \tag{2.4}$$

where a and b are constants and the first terms of the sequence x_2 and x_1 are also known. In this case we first solve the characteristic equation $t^2 - at - b = 0$ and suppose we get two different solutions t_1 and t_2. Then we set $x_n = At_1^{n-1} + Bt_2^{n-1}$ and determine A and B from the initial conditions, i.e. solve the system

$$\begin{cases} A + B = x_1 \\ \\ At_1 + Bt_2 = x_2. \end{cases}$$

In the case that the solutions are the same, $t_1 = t_2 = t$, then we set $x_n = (A + nB)t^{n-1}$ and solve for A and B from the initial conditions. In this situation the system becomes

$$\begin{cases} A + B = x_1 \\ \\ (A + 2B)t = x_2. \end{cases}$$

Then one can check by induction that the solutions found are indeed solving the problems.

Example 3: If we take the Fibonacci sequence, defined as usual by $F_n = F_{n-1}+F_{n-2}$ with $F_1 = F_2 = 1$, then the characteristic equation is $t^2 - t - 1 = 0$ with distinct solutions $t_1 = \frac{1+\sqrt{5}}{2}$ (the golden ratio) and $t_2 = \frac{1-\sqrt{5}}{2}$. Let us observe that $t_1 + t_2 = 1$ and $t_1 t_2 = -1$. Hence we need to solve the system

$$\begin{cases} A + B = 1 \\ \\ At_1 + Bt_2 = 1. \end{cases}$$

We observe that $B = 1 - A$ and so the second equation becomes $A(t_1 - t_2) = 1 - t_2 = t_1$ which implies $A = \frac{1}{\sqrt{5}}t_1$. Similarly, we derive $B = -\frac{1}{\sqrt{5}}t_2$. This gives an explicit formula for the Fibonacci sequence, which is called the Binet's formula

$$\boxed{F_n = \frac{1}{\sqrt{5}}(t_1^n - t_2^n)}, \text{ where } t_1 = \frac{1+\sqrt{5}}{2} \text{ and } t_2 = \frac{1-\sqrt{5}}{2}.$$

We observe that we could arrive at his formula easier if we set $F_0 = 0$, and checked the formula for $n = 0$ and $n = 1$.

A lot of the properties of the Fibonacci sequences can be shown by using Binet's formula.

Problem 11: *Show that for every $n \geq 1$, $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.*

Proof. We calculate first the product

$$F_{n-1}F_{n+1} = \frac{1}{5}(t_1^{2n} + t_2^{2n} - t_1^{n-1}t_2^{n+1} - t_1^{n+1}t_2^{n-1}).$$

Using the fact that $t_1 t_2 = -1$, we obtain that

$$F_{n-1}F_{n+1} - F_n^2 = \frac{1}{5}[2(-1)^n + (-1)^n(t_1^2 + t_2^2)].$$

Since $t_1^2+t_2^2 = (t_1+t_2)^2-2t_1t_2 = 1-2(-1) = 3$, we see that $F_{n-1}F_{n+1}-F_n^2 = (-1)^n$. ■

Problem 12: *Show that $F_{n-1}^2 + F_n^2 = F_{2n-1}$.*

Problem 13: Show that $F_n^3 + F_{n+1}^3 - F_{n-1}^3 = F_{3n}$.

Example 4: Suppose we want to solve the second order linear recurrence $x_n = 4x_{n-1} - 4x_{n-2}$ with $x_1 = 4$ and $x_2 = 10$. The characteristic equation is $t^2 - 4t + 4 = 0$ or $(t-2)^2 = 0$. Hence we have equal solutions $t_1 = t_2 = 2$. Then we need to solve the system

$$\begin{cases} A + B = 4 \\ \\ (A + 2B)2 = 10. \end{cases}$$

The second equation is equivalent to $A + 2B = 5$ and then $B = 5 - (A + B) = 5 - 4 = 1$. Therefore $A = 3$. This implies the sequence is given by the formula $x_n = (3 + n)2^{n-1}$.

In a similar manner one can treat higher order linear recurrences.

Problem 14: *Solve the recurrence* $x_n + 2x_{n-1} + x_{n-2} = 0$ *given that* $x_1 = 5$ *and* $x_2 = 8$.

Problem 15: *Solve the recurrence* $x_n - x_{n-1} - x_{n-2} + x_{n-3} = 0$ *(*$n \geq 4$*) given that* $x_1 = -6$, $x_2 = 1$, *and* $x_3 = -12$.

Problem 16: *Solve the recurrence* $x_{n+1} = x_n + x_{n-1} + n$ *given that* $x_1 = -2$ *and* $x_2 = -3$.

Chapter 3

Counting and Elements of Discrete Probability

3.1 Probability concepts

An **experiment** is a procedure that has one of finitely many outcomes. The **sample space** of an experiment is the set of all possible outcomes. An **event** is a subset of the sample space. The following definition goes back to Laplace (Pierre-Simon,1749-1827) :

Definition: Given a finite nonempty sample space (of equally likely outcomes), and E a subset of S (an event), then the **probability** of E is $P(E) = \frac{|E|}{|S|}$. In other words, the probability of an event is the number of outcomes that are favorable, divided by the total number of possible outcomes.

Example 1: What is the probability of rolling two dice (perfectly identical and with every of their faces likely possible to show up) the sum of the numbers facing up to be equal to 7?

Example 2: What is the probability of rolling three dice, (all as above) the sum of the numbers facing up to be equal to 7?

Example 3: What is the probability of rolling three dice, (all as above) the sum of the numbers facing up to be equal to 7?

Example 4: What is more likely, to throw a sum of 8 with two dice or three dice ?

Theorem 1: *The probability of the event $\overline{E}$, the complementary event of E, is* $P(\overline{E}) = 1 - P(E)$.

Example 4: What is probability that rolling two dice, the sum of their faces showing up is less or equal than 10 ?

Example 5: Choosing a natural number less or equal to 100, what is the probability that it contains no 9 digits ?

Theorem 2: *Given two events A and B of the sample space S, the probability of the event $A \cup B$ is*

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Example 6: Choosing a natural number less than or equal to 100, what is the probability that is divisible by 2 or by 3 ?

Example 7: Choosing a natural number less than or equal to 1000, what is the probability that is divisible by 3 or by 5 ?

Definition: Two events A and B are called **independent** if $P(A \cap B) = P(A)P(B)$.

Problem 1: Show that if A and B are independent events then so are $\overline{A}$ and $\overline{B}$.

Problem 2: Consider A to be the event that a randomly generated bit string of length four begins with a 1 and B is the event that this string contains an even number of 1's. Show that if A and B are independent events.

Problem 3: Choosing a natural number less than or equal to 100, what is the probability that is divisible by 2, by 3 or by 5 ?

Definition: The **sure event** is $E = S$ and the **impossible event** is $E = \emptyset$.

Problem 4: Prove that in a class of 26 students the probability that at least six of the students are having the same grade (only from the list {A,B,C,D,F}) is 1.

Problem 5: In a class of 25 students, what is the probability that at least six of the students are having the same grade (only from the list {A,B,C,D,F}) ?

Problem 6: In a class of n students $2 \leq n \leq 6$, what is the probability that at least two of the students are assigned the same grade ?

Theorem 3: [**Generalized Pigeonhole Principle**] *If N objects are placed into k boxes, then there is at least one box containing at least $\lceil \frac{N}{k} \rceil$ objects.*

Chapter 4

Relations and Graphs

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

Example: Let us define $\mathcal{D}$ 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.

4.1.1 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 since a divides a for every $a \in \mathbb{N}$. 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 have 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 $a = b$. Or, in other words, if for some $a \neq b$ we have $(a, b) \in R$ then $(b, a) \in R$.*

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 used quite frequently, the (mod n) relation on 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 $k \equiv \ell$ (mod n). This relation is clearly symmetric since if $k \equiv \ell$ (mod n) then $\ell \equiv k$ (mod 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 ($\mathcal{D}$, $\mathcal{O}$ and $\equiv (mod\ n)$).

Problem: 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).

4.1.2 Combining Relations

Since relations are subsets, any two relations can be combined in the way two subsets can be combined: union, intersection, difference or specific difference, etc. One special case of combining relations which is not a clear set operation, is the generalization of the usual composition of functions.

Definition: *Given a relation R from A to B and a relation S from B to C, then the* **composite** *of 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 4.1.1. *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 $n \in \mathbb{N}$.

4.2 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 4.2.1. The Handshaking Theorem *Let $G = (V, E, h_G)$ be an undirected graph $m = |E|$ edges. Then*

$$2m = \sum_{v \in V} deg(v). \tag{4.1}$$

Corollary 4.2.2. *An undirected graph has an even number of vertices with an odd degree.*

Definition: *A* **tree** *is an undirected graph in which any two vertices are connected by exactly one path. In other words, any connected graph without simple cycles is a tree. A forest is a disjoint union of trees.*

Definition: *A* **Boolean function** *(or switching function) is a function of the form $f : B^k \to B$, where $B = \{0, 1\}$ is a Boolean domain and k is a non-negative integer called the* **arity** *of the function.*

Bibliography

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