

## Logical Propositions and Sets



# Logical Propositions and Sets



NOT

 $A^{C} = \{x \mid x \notin A\} = \{x \mid \neg (x \in A)\}$ 



Complement





 $x \in A \Rightarrow x \in B$  $A^C \bigcup B$ CNR Italy - ISTM



### **Propositional Calculus**



Two proposition are "equal" if and only if they have the same truth table

$$(\neg p \lor q) = (p \Longrightarrow q)$$





# Propositions and Classical Logic

lf <b>p</b> the <b>q</b>	$p \Rightarrow q$	${m  ho}$ sufficient condition for ${m q}$
if <b>q</b> then <b>p</b>	$q \Rightarrow p$	<b>p</b> necessary condition for <b>q</b>
<b>p</b> if and only if (iff) <b>q</b>	$p \Leftrightarrow q$	p necessary and sufficient condition for q: they are equivalent

The propositions p and q are **equivalent** if and only if each one imply the other

 $p \Rightarrow q \qquad \qquad q \Rightarrow p$ 

i.e. if and only if they satisfy the same "truth table" p=q

## Wiki: Boolean Algebra





# "Naive" Set Theory

Two sets are "equal" **if and only if** they contain the same elements, i.e., **if and only if** each one contains the other

 $(A = B) \Leftrightarrow (A \subset B) \land (B \subset A)$ 

 $x \in (A \cap B)^{c} \implies x \notin A \cap B$  $x \notin A \cap B \implies (x \notin A) \lor (x \notin B)$  $(x \notin A) \lor (x \notin B) \implies (x \in A^{c}) \lor (x \in B^{c})$  $(x \in A^{c}) \lor (x \in B^{c}) \implies x \in A^{c} \bigcup B^{c}$ 

 $(A\cap B)^C \subset A^c \cup B^c$ 

 $x \in A^{c} \cup B^{c} \Longrightarrow (x \in A^{c}) \lor (x \in B^{c})$  $(x \in A^{c}) \lor (x \in B^{c}) \Longrightarrow (x \notin A) \lor (x \notin B)$  $(x \notin A) \lor (x \notin B) \Longrightarrow x \notin A \cap B$  $x \notin A \cap B \Longrightarrow x \in (A \cap B)^{c}$ 

 $A^c \cup B^c \subset (A \cap B)^c$ 

 $(A \cap B)^c = A^c \cup B^c$ 



#### De Morgan's Laws

 $(A \cap B)^c = A^c \cup B^c \qquad (A \cup B)^c = A^c \cap B^c$ 

 $\neg (p \land q) = \neg p \lor \neg q \qquad \neg (p \lor q) = \neg p \land \neg q$ 

Isomorphic and Dual laws: they have the very same shape

Different concepts with the same shape, following the same rules, computed in the same way



#### How to use Sets

 $(a,b) = \{\{a\},\{a,b\}\}$ 

An **ordered couple** of elements of two sets A and B

$$A \times B = \{(a,b) \mid (a \in A) \land (b \in B)\}$$

The set of all ordered couples: the cartesian product of two sets A and B



A simple idea to build new sets from already existing sets



# **Binary Relations**

A binary relation R between the sets A and B is a subset of the cartesian product AxB.

The set A is defined *domain* and the set B codomain

 $R \subset A \times B$  $(a,b) \in R \ aRb$ 

If domain and codomain are the same set X, the  $R \subset X \times X$ binary relation may assume interesting properties:

reflexive $\forall x \in X : xRx$ symmetric $xRy \Rightarrow yRx$ antisymmetric $(xRy) \land (yRx) \Rightarrow x = y$ transitive $(xRy) \land (yRz) \Rightarrow xRz$ total $\forall x, y \in X : (xRy) \lor (yRx)$ 



# Order and Equivalence Relations

A binary relation *reflexive, antisymmetric* and *transitive* is called a *partial order*, and usually is denoted with the "less or equal" symbol.

If it is also total, is simply called an **order** relation or a **total order**.

If each non-empty subset of X as a "minimum" then is named a well order

A reflexive, symmetric and transitive binary relation is defined **equivalence relation** and is denoted with the symbol "~": it partitions the set X into a collection of disjoint subsets, called **equivalence classes**.

 $\forall x \in X : x \leq x$  $(x \le y) \land (y \le x) \Longrightarrow x = y$  $(x \le y) \land (y \le z) \Longrightarrow x \le z$  $\forall x, y \in X : (x \le y) \lor (y \le x)$  $Y \subset X, Y \neq \emptyset$  $\exists x \in Y : x \leq y, \forall y \in Y$  $[\mathbf{x}] = \{ \mathbf{y} \in \mathbf{X} \mid \mathbf{x} \sim \mathbf{y} \}$  $y \notin [x] \Rightarrow [x] \cap [y] = \emptyset$  $\bigcup [x] = X$ x∈X  $X / \sim$  quotient



## Equivalence and Order examples

The relation of "contained" between sets is a *partial order*: two sets may not be comparable

 $A \leq B \Leftrightarrow A \subset B$ 

A "chain" of a partially ordered set is any totally ordered subset

$$X_1 \subset X_2 \subset \ldots \subset X_n$$

The relation "same remainder", between two integers in  $\mathbb{Z}$ , divided by a given positive integer n, is an equivalence relation between relative integers

Inside the quotient  $\mathbb{Z}n=\mathbb{Z}/\sim$  may be defined the operations of sum and product [i]+[j]=[i+j]

 $[i] \times [j] = [i \times j]$ 

$$i \sim j \Leftrightarrow (i = q_i n + r) \land (j = q_j n + r)$$
  
 $Z_n = \{[0], [1], \dots, [n-1]\}$ 



#### Applications or correspondences

$$f \subset A \times B$$

Subset of the cartesian product: a correspondence between **domain A** and **codomain B** 

$$\forall a \in A \; \exists ! b \in B \colon (a, b) \in f$$

The unique element b=f(a) in B correspondent to an element in A, through f, is defined value of f in a

 $f: A \rightarrow B \quad (a,b) \in f \quad b = f(a)$ 

a *function* "is" its graph

$$f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$$
 injective application

 $\forall b \in B \exists a \in A \colon b = f(a)$ 

surjective application



#### Wiki: Correspondences



Injective and surjective



Non-injective and nonsurjective



Non-injective and surjective



Injective and surjective, bijective, one to one correspondence



# Cardinality



Two sets have the same **cardinality** if and only if there exists at least one bijection between them

An abstract general way to express the concept of *number* and an equivalence relation

A set A is defined *infinite* if and only if there exists at least one bijection between A and one of its proper subsets, a subset B of A, different from A



 $f: A \rightarrow B$  f bijection  $B \subset A \ A \neq B$ 

A set A is defined *finite* if and only if it is not infinite





### In class Exercise

**1**+100=**101 2**+99=**101 3**+98=**101** ... **50**+51=**101** 

thought **Carl Friedrich Gauss** (1777-1855) in 1786, at the age of nine

after Friedrich misbehaved, his teacher J.G. Büttner, gave him a task: add the integer numbers between 1 and 100

the young Gauss reputedly produced the correct answer  $1+2+3+...+100 = 50 \times 101 = (100 \times 101)/2 = 5.050$  within seconds, to the astonishment of his teacher and his assistant Martin Bartels

the young student, one of the greatest mathematician of the second millennium, applied the principle of *mathematical induction* 



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



### Mathematical Induction

We show a logical proposition p, related to integer numbers, is true for the first integer number **1** 

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

We assume the proposition p true for an arbitrary integer *n* 

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





We then proceed to prove the proposition p holds for the successor of n, n+1

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

The *principle of mathematical induction* then asserts the proposition p is true for all *natural integers*: it is a *principle*, it hasn't to be proved





# Peano's Integers: ℕ

The italian mathematician **Giuseppe Peano** (1858-1932) gave, at the end of XIX century, a theoretical set definition of natural integer numbers

The *naive set theory*, correspondences and mathematical induction are enough to achieve this bright result



The **natural integer numbers** are a non-empty set  $\mathbb{N}$ , containing at least the element **1**, for which there exists at least one correspondence  $s: \mathbb{N} \to \mathbb{N}$  satisfying the following properties:

- s is an injective correspondence  $s(n) = s(m) \Rightarrow n = m$
- ullet s never assumes the value  $oldsymbol{1}$ , for any element in  $\mathbb N$
- each subset J of N containing the element 1, which if it contains an element n then it contains s(n), it is coincident with the full set N

The function s is called **successor** function: s(n)=(n+1)n+1 it is not a sum, for now it is just a symbol



# Natural Integers Algebra

The successor function s is a bijective correspondence between  $\mathbb{N}$  and its proper subset  $\mathbb{N}$ -{**1**}: the natural integers set is *infinite*. It can be proved with the principle of mathematical induction.

Again, using the principle of mathematical induction and the successor function, it is easy to define the sum and product operations to make s(n) just the expected sum (n+1):

1+1=s(1) n+s(m) = s(n+m) n+(m+1) = (n+m)+11×1=1 n×s(m) = (n×m)+n n×(m+1) = (n×m)+n

In the same way it is possible to define the natural order relation we are naively using to compare natural integers.

We obtain a total order that is also a well order: each non-empty subset of  $\mathbb N$  has a minimum.



## Infinite, but well ordered

Actually  ${\mathbb N}$  is the smallest, in the sense of cardinality, infinite well ordered set.

In the natural order, each initial segment { i in  $\mathbb{N}|$  i <= n } = {1,2,...,n} is finite.

Instead of using Peano's Axioms we may think to define natural integers using this property: the natural integers  $\mathbb{N}$  are any **well ordered infinite** set where **all initial segments** are **finite**.

We would obtain a mathematical structure "isomorphic" with the Peano's Integers, beside the actual set we are using as a *model*.

The propositional calculus, the logic and the naive set theory are enough to build so much. And more.



### Beyond natural integers...

From ordered couples of Peano's integers a simple equivalence relation build the **ring** of **relative integers**  $\mathbb{Z}$ : the zero and the negative integer numbers are born

An analogous trick creates, from ordered couples of relative integers, fractions, the field of rational numbers  $\mathbb{Q}$ 

-9 -8 -7 -6 -5 -4 -3 -2 -1 () 1 2 3 4 5 6 7 8 9



### ... real and complex numbers

A more involved equivalence relation defines the field of **real numbers**  $\mathbb{R}$  from Cauchy sequences of rational numbers and the square root of 2 becomes the number 1.4142135... the **real line**, the **linear continuum** 

1,4	1,5	$\{x \in Q \mid x^2 < 2\}$
1,41	1,42	$\{\mathbf{x} \in \mathbf{O} \mid 2 < \mathbf{x}^2\}$
1,414	1,415	$\begin{bmatrix} \mathbf{x} \in \mathbf{Q} \mid 2 < \mathbf{x} \end{bmatrix}$
1,4142	1,4143	$\exists \mathbf{x} \in \mathbf{R} : \mathbf{x}^2 = 2$

A second degree polynomial equation, without any solution, defines the field of **complex numbers** C as ordered couples of real numbers, where all polynomial equations find a solution.

And complex numbers may be thought as a model for the plane  $\mathbb{R} \times \mathbb{R}$ 

 $\forall \varepsilon > 0 \exists n_{\varepsilon} : n, m > n_{\varepsilon} \Longrightarrow a_{n} - a_{m} | < \varepsilon$  $(a_n) \sim (b_n)$  $\forall \varepsilon > 0 \exists n_{\varepsilon} : n > n_{\varepsilon} \Longrightarrow a_n - b_n \mid < \varepsilon$  $(a,b) = a + ib, i^2 = -1$ (a+ib)+(c+id)=(a+c)+i(b+d)(a+ib)(c+id) = (ac-bd)+i(ad-bc) $z = a + ib = \rho e^{i\theta}$ 

 $i^2 = -1$ 

CNR Italy - ISTM

 $\exists z \in C : z^2 = -1$ 



#### And beyond numbers ...

As already observed from **René Descartes** (1596-1650), algebra and geometry are different models of the same mathematical structures.

The trigonometric functions, sine and cosine, describe the unit circle in the complex plane  $\mathbb{C}$ 



**Leonhard Euler** (1707-1783), proved a famous indentity containing all the important numbers of mathematics

![](_page_22_Picture_6.jpeg)

z = a + ib  $a \rightarrow x$   $\overline{z} = a - ib$ 

![](_page_22_Picture_8.jpeg)

![](_page_22_Figure_9.jpeg)

![](_page_22_Picture_10.jpeg)

CNR Italy - ISTM

 $e^{i\pi} + 1 = 0$ 

## ... the reality of Mathematics

The **dot product** between two vectors **a** and **b**, as ordered couples of real numbers:

 $\langle \mathbf{a} | \mathbf{b} \rangle = (a_1, a_2) \cdot (b_1, b_2) = a_1 b_1 + a_2 b_2$  $\langle \mathbf{a} | \mathbf{b} \rangle = \| \mathbf{a} \| \times \| \mathbf{b} \| \times \cos(\theta)$ 

Two vectors are **orthogonal** if and only if their scalar product is zero, i.e. the angle between them is 90 degree

an algebraic definition that may be easily generalized to vectors of complex numbers with an arbitrary number of dimensions Length of the vector  $\mathbf{a}$  $< \mathbf{a} | \mathbf{a} > = ||\mathbf{a}||^2$ 

![](_page_23_Figure_6.jpeg)

$$\mathbf{a} \cdot \mathbf{b} = <\mathbf{a} \mid \mathbf{b} >= 0$$

$$\langle \mathbf{z} | \mathbf{w} \rangle = (z_1, z_2, \dots, z_n) \cdot (w_1, w_2, \dots, w_n) = \sum_{i=1}^n z_i \overline{w_i}$$

![](_page_24_Picture_0.jpeg)

### Geometry and Algebra

In two dimensions, as in an arbitrary number of dimensions, orthogonality allows to define an **orthonormal basis**, a reference frame

And a *reference frame* allows to translate algebra in geometry and geometry in algebra

![](_page_24_Figure_4.jpeg)

 $<\mathbf{e}_{1} | \mathbf{e}_{1} >= \delta_{1,1} = 1$  $<\mathbf{e}_{2} | \mathbf{e}_{2} >= \delta_{2,2} = 1$  $<\mathbf{e}_{1} | \mathbf{e}_{2} >= \delta_{1,2} = 0$  $<\mathbf{e}_{2} | \mathbf{e}_{1} >= \delta_{2,1} = 0$ 

Hilbert Space, **David Hilbert**, (1862-1943)

![](_page_24_Picture_8.jpeg)

![](_page_25_Picture_0.jpeg)

## Infinite dimensions

A finite number of dimensions is not always enough to cope with reality, but mathematicians don't easily give up, they are able to use an *infinite* number of dimensions

They define the meaning of an *infinite sum* 

$$\langle \mathbf{e}_n | \mathbf{e}_m \rangle = \delta_{n,m} \quad n, m \in N$$

$$\mathbf{v} = \sum_{n=1}^{\infty} \langle \mathbf{v} | \mathbf{e}_n \rangle \langle \mathbf{e}_n \rangle$$

![](_page_25_Figure_6.jpeg)

and when integers are not enough, the **discrete** case, they define the meaning of a **continuous sum**:

$$< f \mid g >= \int f(x)\overline{g}(x)dx$$

$$<\mathbf{f} \mid \mathbf{g}> = \sum_{n=1}^{\infty} f_n \overline{g}_n$$

generalizing the meaning of dot product and thinking the *integral* as a continuous sum

# Up to the continuous, analysis

It is possible to travel through a unit circle with an arbitrary **frequency** 

$$e_{v}(t) = e^{i2\pi vt} = \cos(2\pi vt) + i\sin(2\pi vt)$$

 $\omega = 2\pi \upsilon \quad \upsilon = \frac{\omega}{2\pi}$ 

To each frequency corresponds a continuous vector, a unit circle traveled with a different speed in one or the opposite direction

$$\widehat{f}(\upsilon) = \langle f | e_{\upsilon} \rangle = \int f(t)\overline{e}_{\upsilon}(t)dt = \int f(t)e^{-i2\pi\upsilon t}dt$$

and for each vector and each regular function f(t) it is possible to compute the dot product, the projection over a **rotating unit circle** 

While trying to preserve the structure and the interpretation we defined the *Fourier Transform*, **Jean Baptiste Joseph Fourier** (1768-1830)

![](_page_26_Figure_8.jpeg)

![](_page_26_Picture_10.jpeg)

![](_page_27_Picture_0.jpeg)

### **Fourier Transform**

Unit circles, traveled with arbitrary frequencies, are an **orthonormal basis**, a *reference frame*, for regular functions

 $< e_{\upsilon} \mid e_{\xi} > = \delta_{\upsilon,\xi} \quad \upsilon, \xi \in \mathbb{R}$ 

We may write the vector f(t) as a continuous sum of all its projections on unit circles, traveled with arbitrary frequencies

$$f(t) = \int \langle f | e_{\upsilon} \rangle e_{\upsilon} d\upsilon = \int \hat{f}(\upsilon) e^{i2\pi \upsilon t} d\upsilon$$

it is not surprising **antitransforming** we get back the original function

the spectrum of the signal, the energy contained in the signal

![](_page_27_Figure_8.jpeg)

$$|\hat{f}(t)|^2 = \hat{f}(t)\bar{\hat{f}}(t)$$

## Spectrums ... from reality

7.5

ΕU

0.0

0.0

![](_page_28_Figure_1.jpeg)

Sine wave 50Hz

We can extract and transform spectrums to compress or filter signals

![](_page_28_Picture_4.jpeg)

2441.4062

Power Spectrum

Hz

![](_page_28_Figure_5.jpeg)

![](_page_28_Figure_6.jpeg)

# Real World and Digital World

Mathematical structures are powerful tools for the analysis of the reality: they can be used in many ways and in many fields to compute ... bits ... numbers, from analogical sources.

Because this is all and only what even the more modern and advanced computers are able to do: execute logical and arithmetical operations on string of bits, on integer numbers

0x41

![](_page_29_Figure_3.jpeg)

![](_page_29_Figure_4.jpeg)

Mathematics is a tool for creating models of the reality that our computers are able to process

0100 0001

'A'

65

+	00	01	x	00	01
00	00	01	00	00	00
01	01	10	01	00	01

Binary arithmetic: implemented using networks of logical gates, of transistors

![](_page_30_Picture_0.jpeg)

## The Numbers of The Net

In the last 5,000 days, roughly 15 years, we interconnected these networks of gates in one big Network, the Network of the Networks, the Internet.

And the numbers the Net are impressive:

- 1.2 billions of personal computers
- 2.7 billions of cell phones
- 1.3 billions of phones
- 27 millions of servers
- 80 millions of palms

Each device contains a large number of logical gates, of transistors: a 2004 Intel Pentium had 100 millions, a 2005 Intel Itanium over one billion.

The interaction between all these elementary networks is **The One Machine** we today call "**The Net**".

![](_page_30_Picture_11.jpeg)

![](_page_30_Figure_12.jpeg)

![](_page_31_Picture_0.jpeg)

## The One Machine

Into The Net over a billion of devices are interconnected: around 10^17 transistors, a number with 17 zeros, hundreds of millions of billions of logical gates.

The human brain is a network of over 100 billions of neurons. Even if neurons are not directly comparable with transistors, this is **six order of magnitude** less than the number of elementary units of The Net, 10^11 against 10^17

The One Machine uses around 5% of the electric energy globally produced over the planet Earth.

The size of The Net doubles at a fast rate: probably even faster than Moore's Law.

170 quadrillion	Transistors	
55 trillion	Links	
2 megahertz	Email	
31 kilohertz	Text messages	
162 kilohertz	Instant messages	
14 kilohertz	Search	
246 exabyte	Storage	
9 exabyte	RAM	
7 terabytes/second	Bandwidth	
800 billion kwh/year	Power consumption	

![](_page_31_Figure_7.jpeg)

Moore's Law: double every two years an empirical exponential law

# The next 5,000 days

Today The Net complexity may be compared with the human brain complexity.

In the next 5,000 days, 15 years, in a period between 2025 and 2040, its complexity may *explode*.

It is difficult to forecast its evolution, but, one day, it may become complex as thousands, millions or even billions of human brains.

![](_page_32_Picture_4.jpeg)

And we shouldn't forget the human brains already interacting with The One Machine, billions of *clicks* every day.

Kevin Kelly Wired

http://www.kk.org/thetechnium/archives/2007/11/dimensions\_of\_t.php

http://www.youtube.com/watch?v=J132shgliuY