# Mathematics for Computer Science

### Prof.dr.hab. Viorel Bostan

Technical University of Moldova viorel.bostan@adm.utm.md

Lecture 1. Part 2



### Last Lecture Outline



- Naive Set Theory;
- Functions (bijections, injections, surjections);
- Cardinal number of a set;
- Mapping Rule:

### Theorem (Mapping Rule)

If X and Y are sets then:

- **1**  $f: X \to Y$  is surjection ( denoted by X surj Y), if and only if  $|X| \ge |Y|$ .
- **2**  $f: X \to Y$  is injection (denoted by X inj Y), if and only if  $|X| \leq |Y|$ .
- **3**  $f: X \to Y$  is bijection (denoted by X bij Y), if and only if |X| = |Y|.
- Infinite sets;

### Last Lecture Outline



Countable sets (finite or infinite)

#### Definition

A set X is called **infinitely countable** if and only if there is a bijection between  $\mathbb{N}$  and X.

$$\aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|.$$

■ Finite union of countable sets

If 
$$|A_1| = |A_2| = |A_3| = \aleph_0$$
, then  $|A_1 \cup A_2 \cup A_3| = \aleph_0$ .

Union of countable sets

If 
$$|A_i| = \aleph_0$$
, then  $\left| \bigcup_{i=1}^{\infty} A_i \right| = |A_1 \cup A_2 \cup \cdots \cup A_n \cup \ldots| = \aleph_0$ .

Cartesian product of countable sets

$$\aleph_0 = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Q} \times \mathbb{Q}| = |\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}|.$$



How about cardinality of  $|\mathbb{R}|$ ?



How about cardinality of  $|\mathbb{R}|$ ?

Obviously, 
$$|(0,1)| = |[0,1]| = |\{0,1\} \cup (0,1)|$$
.



How about cardinality of  $|\mathbb{R}|$ ?

Obviously,  $|(0,1)| = |[0,1]| = |\{0,1\} \cup (0,1)|$ .

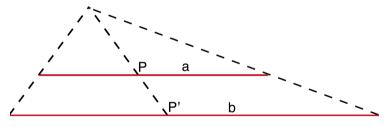
How about, e.g., |[2,7]| and |[1,23]|?



How about cardinality of  $|\mathbb{R}|$ ?

Obviously,  $|(0,1)| = |[0,1]| = |\{0,1\} \cup (0,1)|$ .

How about, e.g., |[2,7]| and |[1,23]|?

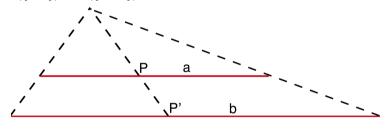




How about cardinality of  $|\mathbb{R}|$ ?

Obviously, 
$$|(0,1)| = |[0,1]| = |\{0,1\} \cup (0,1)|$$
.

How about, e.g., |[2,7]| and |[1,23]|?



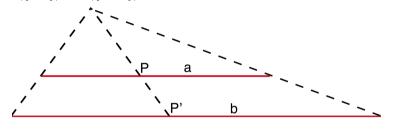
Clearly, there is a bijection between points in both intervals.



How about cardinality of  $|\mathbb{R}|$ ?

Obviously, 
$$|(0,1)| = |[0,1]| = |\{0,1\} \cup (0,1)|$$
.

How about, e.g., |[2,7]| and |[1,23]|?



Clearly, there is a bijection between points in both intervals.

$$|[a,b]| = |[c,d]|$$
 for any  $a,b,c,d \in \mathbb{R}$ .

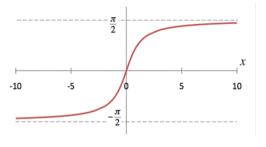


How about  $|\mathbb{R}| = |(-\infty, +\infty)|$  and  $|(0, +\infty)|$  or |(0, 1)|?



How about  $|\mathbb{R}| = |(-\infty, +\infty)|$  and  $|(0, +\infty)|$  or |(0, 1)|?

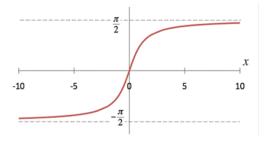
Consider function  $f: \mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$  defined by  $f(x) = \arctan x$ .





How about  $|\mathbb{R}| = |(-\infty, +\infty)|$  and  $|(0, +\infty)|$  or |(0, 1)|?

Consider function  $f: \mathbb{R} \to (-\frac{\pi}{2}, \frac{\pi}{2})$  defined by  $f(x) = \arctan x$ .



It is a bijection, and therefore,

$$|\mathbb{R}| = \left| \left( -\frac{\pi}{2}, \frac{\pi}{2} \right) \right| = |(0, 1)|$$



### Proposition

If 
$$|X| = n$$
, then  $|2^X| = 2^n$ .

#### Notation

The collection of all *n*-bit sequences will be denoted by  $\{0,1\}^n$ .

The collection of all finite-bit sequences will be denoted by  $\{0,1\}^*$ .

The collection of all infinit-bit sequences will be denoted by  $\{0,1\}^\omega$ .



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .

#### Notation

The collection of all *n*-bit sequences will be denoted by  $\{0,1\}^n$ . The collection of all finite-bit sequences will be denoted by  $\{0,1\}^*$ . The collection of all infinit-bit sequences will be denoted by  $\{0,1\}^\omega$ .

### Example



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .

### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ :



### Proposition

If 
$$|X| = n$$
, then  $|2^X| = 2^n$ .

### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ : Let  $x_1, x_2, \ldots x_n \in X$ .



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .

#### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ : Let  $x_1, x_2, \ldots x_n \in X$ . Then, a subset of X maps to the sequence  $(b_1, b_2, \ldots, b_n)$ , where  $b_i = 1$  if and only if  $x_i \in$  that subset.



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .

#### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ : Let  $x_1, x_2, \ldots x_n \in X$ . Then, a subset of X maps to the sequence  $(b_1, b_2, \ldots, b_n)$ , where  $b_i = 1$  if and only if  $x_i \in$  that subset.

For example, if n = 10, then the subset  $\{x_3, x_4, x_8, x_{10}\}$  maps to a 10-bit sequence as follows



### Proposition

If 
$$|X| = n$$
, then  $|2^X| = 2^n$ .

#### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ : Let  $x_1, x_2, \ldots x_n \in X$ . Then, a subset of X maps to the sequence  $(b_1, b_2, \ldots, b_n)$ , where  $b_i = 1$  if and only if  $x_i \in$  that subset.

For example, if n = 10, then the subset  $\{x_3, x_4, x_8, x_{10}\}$  maps to a 10-bit sequence as follows



### Proposition

If 
$$|X| = n$$
, then  $|2^X| = 2^n$ .

#### Proof.

Let X be a set and |X| = n. There is a natural bijection from power set  $2^X$  to  $\{0,1\}^n$ : Let  $x_1, x_2, \ldots x_n \in X$ . Then, a subset of X maps to the sequence  $(b_1, b_2, \ldots, b_n)$ , where  $b_i = 1$  if and only if  $x_i \in$  that subset.

For example, if n = 10, then the subset  $\{x_3, x_4, x_8, x_{10}\}$  maps to a 10-bit sequence as follows

and vice versa, sequence (1011101010) corresponds to the subset  $\{x_1, x_3, x_4, x_5, x_7, x_9\}$ . Clearly, this is a bijection.



### Proposition

If 
$$|X| = n$$
, then  $|2^X| = 2^n$ .

#### Proof Contd.

Since,

$$2^X$$
 bij  $\{0,1\}^n$ ,

it follows that

$$\left|2^X\right| = \left|\{0,1\}^n\right|$$



### Proposition

If |X| = n, then  $|2^X| = 2^n$ .

#### Proof Contd.

Since,

 $2^X$  bij  $\{0,1\}^n$ ,

it follows that

$$\left|2^X\right| = \left|\{0,1\}^n\right|$$

Show that

$$\left|\{0,1\}^n\right|=2^n$$

and we are done.



### Cantor's discovery

Not all infinite sets are the same size!



### Cantor's discovery

Not all infinite sets are the same size!

### Theorem (Cantor)

For any set X,

$$|X| < |2^X|$$
.



### Cantor's discovery

Not all infinite sets are the same size!

### Theorem (Cantor)

For any set X,

$$|X| < |2^X|$$
.

Let's prove a particular case of this theorem:

#### Theorem

$$|\mathbb{N}| < |2^{\mathbb{N}}|.$$

In other words, the set of all subsets of natural numbers is uncountable.



#### Proof.

Establish a natural bijection between all subsets of  $\mathbb{N}$  and  $\{0,1\}^{\omega}$  (infinite-bit sequences).

$$\left|2^{\mathbb{N}}\right| = \left|\{0,1\}^{\omega}\right|.$$

Then, we will prove that

$$\aleph_0 < \left| \{0,1\}^{\omega} \right|.$$

Proof by contradiction.



#### Proof.

Establish a natural bijection between all subsets of  $\mathbb{N}$  and  $\{0,1\}^{\omega}$  (infinite-bit sequences).

$$\left|2^{\mathbb{N}}\right| = \left|\{0,1\}^{\omega}\right|.$$

Then, we will prove that

$$\aleph_0 < \left| \{0,1\}^{\omega} \right|.$$

### Proof by contradiction.

Suppose that  $\{0,1\}^{\omega}$  is a countable set. It means that its elements can be listed:

$$s_1, s_2, s_3, s_4, s_5, s_6, s_7, \dots$$



### Proof Contd.

```
0 0
                                    0
s_3 =
s_4 =
s_5 =
s_6 =
                             0
s_7 =
s_8 =
s_9 =
s_{10} =
```



### Proof Contd.

```
0
                                  0 0
                                  0
 s_3 =
 s_4 =
 s_5 =
 s_6 =
 s_7 =
 s_8 =
 s_9 =
s_{10} =
                        1 0
                               0 0
x =
```



### Proof Contd.

```
0
 s_1 =
                                   0
 s_3 =
 s_4 =
 s_5 =
 s_6 =
 s_8 =
 s_9 =
 s_{10} =
                          1 0
                                 0 0
x =
```

Is x listed above?



### Proof Contd.

```
0
 s_1 =
                                  0
 s_3 =
 s_4 =
 s_5 =
 s_6 =
 s_8 =
 s_9 =
s_{10} =
                        1 0
                               0 0
x =
```

Is x listed above? **NO**.



### Proof Contd.

```
0 0 0 0 0
                             1 \quad 1 \quad 0 \quad 0 \quad 1 \quad \cdots
 s_3 =
 s_4 =
 s_5 =
 s_6 =
 s_7 =
 s_8 =
 s_9 =
s_{10} =
            1 1 0 1 1 0 0 0 0 1 ...
x =
```

Is x listed above? **NO**. Means that  $x \notin \{0, 1\}^{\omega}$ .



### Proof Contd.

```
0 0 0 0 0 ...
                        1 \ 1 \ 0 \ 0 \ 1 \ \cdots
 s_3 =
 s_4 =
 s_5 =
 s_6 =
 s_7 =
 s_8 =
 s_9 =
s_{10} =
          1 1 0 1 1 0 0 0 0 1 ...
x =
```

Is x listed above? **NO**. Means that  $x \notin \{0,1\}^{\omega}$ . Contradiction!



### Proof Contd.

Thus, initial supposition that we can list (count) all elements of  $\{0,1\}^{\omega}$  is **wrong**.



#### Proof Contd.

Thus, initial supposition that we can list (count) all elements of  $\{0,1\}^{\omega}$  is **wrong**.

Therefore,  $\{0,1\}^{\omega}$  is uncountable, which means

$$\left|\{0,1\}^{\omega}\right|>\aleph_0.$$

We have proved that

$$|\mathbb{N}| < |2^{\mathbb{N}}|.$$

#### Definition

Procedure used in the above proof is called **Cantor's diagonal argument**.



Corollary

The set of real numbers  ${\mathbb R}$  is uncountable.



Corollary

The set of real numbers  $\mathbb{R}$  is uncountable.

Actually, let's prove

Corollary

The set of real numbers  ${\mathbb R}$  from interval (0,1) is uncountable.



### Corollary

The set of real numbers  $\mathbb{R}$  is uncountable.

Actually, let's prove

## Corollary

The set of real numbers  $\mathbb R$  from interval (0,1) is uncountable.

#### Proof.

Proof by contradiction and using Cantor's diagonal argument.



### Corollary

The set of real numbers  $\mathbb{R}$  is uncountable.

Actually, let's prove

### Corollary

The set of real numbers  $\mathbb{R}$  from interval (0,1) is uncountable.

#### Proof.

Proof by contradiction and using Cantor's diagonal argument.

Suppose that the set (0,1) is countable. Consider real numbers from (0,1), written in binary decimal form. Since (0,1) is countable, we can list all numbers from (0,1) in a sequence:



#### Proof Contd.

```
0. 0 0
      0 1
0. 1 0 0 0
            0
0. 0 0 0 0
```



### Proof Contd.

```
0 0 0 0 0
    0. 0 0 0
     0. 0 0
     0. 1 0 0 0
                  0
\alpha_{10} =
     0. 0 0 0 0
\alpha = 0. 1 1 0 1 1 0 0 0 1 \cdots
```



#### Proof Contd.

```
0. 1 0 0 0
                     0
\alpha_{10} = 0. 0 0 0 0
\alpha = 0. 1 1 0 1 1 0 0 0 1 \cdots
```

Is real number  $\alpha \in (0,1)$  listed above?



#### Proof Contd.

```
0 1 1 0
     0. 1 0 0 0
                 0
\alpha_{10} = 0. 0 0 0 0
\alpha = 0.1101100001.
```

Is real number  $\alpha \in (0,1)$  listed above? **NO**.



#### Proof Contd.

```
\alpha_1 = 0. \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots
\alpha_2 = 0. \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ \cdots
\alpha_6 = 0. 0 0 0 1
\alpha_7 = 0. 1 0 0 0
                       0 0
\alpha_9 = 0. 1 1 0 1 1
\alpha_{10} = 0. 0 0 0 0
                        0 1 1 1 0 0 ...
\alpha = 0. 1 1 0 1 1 0 0 0 1 \cdots
```

Is real number  $\alpha \in (0,1)$  listed above? **NO**. Means that  $\alpha \notin (0,1)$ .



#### Proof Contd.

```
\alpha_1 = 0. \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ \cdots
\alpha_2 = 0. \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ \cdots
\alpha_6 = 0. 0 0 0 1
\alpha_7 = 0. 1 0 0 0
                        0 0
\alpha_{10} = 0. 0 0 0 0
\alpha = 0. 1 1 0 1 1 0 0 0 1 \cdots
```

Is real number  $\alpha \in (0,1)$  listed above? **NO**. Means that  $\alpha \notin (0,1)$ . **Contradiction!** 



### Definition

The cardinal number of set  $\mathbb R$  is called **continuum**:  $|\mathbb R|=c$ .



### Definition

The cardinal number of set  $\mathbb{R}$  is called **continuum**:  $|\mathbb{R}| = c$ .

## Corollary

$$\aleph_0 < c$$
.



#### Definition

The cardinal number of set  $\mathbb{R}$  is called **continuum**:  $|\mathbb{R}| = c$ .

Corollary

$$\aleph_0 < c$$
.

**Proposition** 

$$\left| \mathbb{N} \right| < \left| 2^{\mathbb{N}} \right| < \left| 2^{2^{\mathbb{N}}} \right| < \dots$$
  
 $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$ 

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$$



#### Definition

The cardinal number of set  $\mathbb{R}$  is called **continuum**:  $|\mathbb{R}| = c$ .

### Corollary

$$\aleph_0 < c$$
.

### **Proposition**

$$\left| \mathbb{N} \right| < \left| 2^{\mathbb{N}} \right| < \left| 2^{2^{\mathbb{N}}} \right| < \dots$$
  
 $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$ 

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$$

#### Remark

It follows from Sroder-Bernstein Theorem that:

$$2^{\aleph_0}=c.$$

## Continuum hypothesis



So far, we know that

$$\aleph_0 < c$$
.

G. Cantor in 1878 formulated the question whether there is no set whose cardinality is strictly between that of the integers and the real numbers. D. Hilbert in his set of biggest problems of mathematics called it the 1st problem.

# Continuum hypothesis



So far, we know that

$$\aleph_0 < c$$
.

G. Cantor in 1878 formulated the question whether there is no set whose cardinality is strictly between that of the integers and the real numbers. D. Hilbert in his set of biggest problems of mathematics called it the 1st problem.

It is known as:

Continuum Hypothesis (CH)

$$c=2^{\aleph_0}\stackrel{?}{=}\aleph_1$$

Kurt Godel advanced in the solution of Hilbert's 1st problem, and Paul Cohen showed in 1963 that CH cannot be proven from ZFC axioms, in other words, CH is independent of ZFC. For his work, P. Cohen was awarded the Fields Medal (1966).