Diagonalization

The Halting Problem

In this lecture we present the notion of a ***cardinality*** of a set and prove some unintuitive properties of infinite sets. The proofs use a common mathematical technique known as ***Diagonalization***, which was first used by the Jewish German mathematician Cantor.

Cardinality

Cantor dealt with questions like:

How many **natural numbers** are there? Infinity!

How many **real numbers** are there? Infinity!

Does the **amount of natural numbers equal to** the **amount of real numbers?**

How is the size of infinite sets measured?

Cardinality

Cantor’s answer to these question was the notion of ***Cardinality***.

The ***cardinality*** of a set is a property marking its size.

Two sets have the same cardinality if there is a ***correspondence*** between their elements.

Intuitive Notion of Correspondence

At this point of the lecture, think about a correspondence between sets A and B as 2 lists: A list of A's elements and in parallel a list of B's elements. These 2 lists are juxtaposed so that each element of A corresponds to a unique element of B.

Example

$A = \{1,2,3,4\}$ $\quad$ $B = \{2,4,6,8\}$

$$\begin{array}{ccccc} A & 1 & 2 & 3 & 4 \\ B & 2 & 4 & 6 & 8 \end{array}$$

Clearly, the **cardinality** of A is equal to the **cardinality** of B.

How about the cardinality of infinite sets?

Example

How about the cardinality of infinite sets?

Is the cardinality of ***natural numbers*** larger than the cardinality of ***even natural numbers***?

Intuitively, the cardinality of any set **should be larger** that the cardinality of any of its **proper subsets**. Alas, our intuition of sets is driven by our daily experience with ***finite sets***.

Example

So let us try to create a correspondence between the ***natural numbers*** the ***even natural numbers***?

$$N = \{1,2,3,4,\ldots,n,\ldots\}$$
$$EN = \{2,4,6,8,\ldots,2n,\ldots\}$$

N	1	2	3	...	n	...
EN	2	4	6	...	$2n$	...

Indeed $f(n) = 2n$ ***defines*** the wanted correspondence between the 2 sets.

Example

$$N = \{1,2,3,4,\ldots,n,\ldots\}$$

$$EN = \{2,4,6,8,\ldots,2n,\ldots\}$$

N	1	2	3	$\ldots$	n	$\ldots$
EN	2	4	6	$\ldots$	$2n$	$\ldots$

So the ***cardinality*** of N is ***equal to*** the ***cardinality*** of EN.

Countable Sets

This last example suggests the notion of ***Countable Sets***:

A set A is ***countable*** if it is either ***finite*** or its cardinality is equal to the cardinality of N.

A cool way of looking at countable sets is: "A set is countable if a list of its elements can be created".

Countable Sets

"A set is countable if a list of its elements can be created".

Note: This list does not have to be finite, but for each natural number i, one should be able to specify the i-th element on the list.

For example, for the set EN the i-th element on the list is $2i$.

Countable Sets

We just proved that EN, the set of even natural numbers is countable. What about the set of ***rational numbers***?

Is the set Q of rational numbers ***countable***?

Can its elements be ***listed***?

The set of Rationals is Countable

Theorem

The set of ***rational numbers*** is countable.

Proof

In order to prove this theorem we have to show how a complete list of the rational numbers can be formed.

The set of Rationals is Countable

Recall that each natural number is defined by a pair of natural numbers.

One way to look at the Rationals is by listing them in an infinite Rectangle.

1/1	1/2	1/3	1/4	1/5	………
2/1	2/2	2/3	2/4	2/5	………
3/1	3/2	3/3	3/4	3/5	………
4/1	4/2	4/3	4/4	4/5	………
5/1	5/2	5/3	5/4	5/5	………

…………………………………………………

The set of Rationals is Countable

How can we form a list including all these numbers?

If we first list

The first row –

We will never

reach the second.

$$
\begin{array}{cccccc}
1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \cdots\cdots \\
2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \cdots\cdots \\
3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots\cdots \\
4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \cdots\cdots \\
5/1 & 5/2 & 5/3 & 5/4 & 5/5 & \cdots\cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}
$$

The set of Rationals is Countable

1/1	1/2	1/3	1/4	1/5
2/1	2/2	2/3	2/4	2/5
3/1	3/2	3/3	3/4	3/5
4/1	4/2	4/3	4/4	4/5
5/1	5/2	5/3	5/4	5/5

One way to do it is to start from the upper left corner,

and continue in this fashion

The set of Rationals is Countable

Note that some rational numbers appear more than once. For example: all numbers on the main diagonal are equal to 1, so this list is not final.

In order to compute the actual place of a given rational, we need to erase all duplicates, but this is a technicality…

So perhaps all sets are countable

Can you think of any infinite set whose elements cannot be listed in one after the other?

Well, there are many:

Theorem

The set of infinite binary sequences is not countable.

Uncountable Sets

Assume that there exists a list of all binary sequences. Such a list may look like this:

1	0	1	1	0	………
1	1	0	0	1	………
0	0	0	0	1	………
1	1	1	0	1	………
1	0	0	0	1	………

…………………………………………

Uncountable Sets

But can you be sure that all sequences are in this list?

In fact, There exist infinitely many sequences that are not on the list:

1	0	1	1	0	………
1	1	0	0	1	………
0	0	0	0	1	………
1	1	1	0	1	………
1	0	0	0	1	………

……………………………………

Uncountable Sets

Consider for example S=0,0,1,1,0,… . The sequence S is formed so that

$S[1] \neq$ 1st elt. Of 1st seq.

$S[2] \neq$ 2nd elt. Of 2nd seq.

$S[3] \neq$ 3rd elt. Of 3rd seq.

And so on …

$$
\begin{array}{cccccc}
1 & 0 & 1 & 1 & 0 & \cdots\cdots \\
1 & 1 & 0 & 0 & 1 & \cdots\cdots \\
0 & 0 & 0 & 0 & 1 & \cdots\cdots \\
1 & 1 & 1 & 0 & 1 & \cdots\cdots \\
1 & 0 & 0 & 0 & 1 & \cdots\cdots \\
\end{array}
$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Uncountable Sets

Define $S[i] = 1 - S_i[i]$. Obviously, for every $i \in N$, the i-th element of $S, S[i]$ differs from the i-th element of the i-th sequence in the list, that is: The **element on the diagonal**.

Can the sequence S appear on the list?

Uncountable Sets

S_1	1	0	1	1	0	...	...
S_2	1	1	0	0	1	...	...
S_3	0	0	0	0	1	...	...
S_4	1	1	1	0	1	...	...
S_5	1	0	0	0	1	...	...
...	...	...	...	...	...	...	...
S	0	0	1	1	0	...	?

Assume there exists an index j such that $S = S_j$

In this case,

$$S_j[j] = S[j]$$

But by definition:

$$S[j] \neq S_j[j]$$

Contradiction!!

Uncountable Sets

For obvious reasons, this technique is called ***Diagonalization***.

We just used Diagonalization to prove that the set of infinite binary sequences is uncountable.

Can a similar proof for the set of **real numbers**?

Turing Unrecognizable Languages

Corollary

Some Languages are not Turing-recognizable.

Proof

For any (finite) alphabet, Σ , the set of (finite) strings Σ^*, is countable. A list of all elements in Σ^* is obtained by first listing strings of length 1, then 2, …, then n…

Proof (cont.)

The set of all TM-s is also countable because every TM, M, can be described by its encoding $\langle M \rangle$, which is a string over Σ. So the set of TM-s corresponds to a subset of Σ^*.

Note: Here we use the (unproven but correct) fact that the cardinality of a set is always not greater then the cardinality of any of its supersets.

Proof (cont.)

Since each TM recognizes exactly a single language, a list of all TM-s can be used as a list of all recognizable languages.

If we show that the set of languages over Σ is **uncountable**, we can deduce that at least a single language is not on the list, that is: ***it is not recognized by any TM***.

Proof (cont.)

We have already seen that the set of infinite binary sequences is uncountable. Now we form a correspondence between the set of languages over Σ and the set of infinite binary sequences to show that the set of languages is uncountable.

Proof (cont.)

Let L be the set of all languages over alphabet Σ. Let B be the set of all infinite binary sequences. We show that L is uncountable by giving a correspondence with B, thus showing that the two sets are the same side.

We have already seen that the set Σ^* is countable. Let Σ^*={s_1, s_2, s_3, …}. Each language A $\in$L has a unique **characteristic sequence** in B:

ith bit is 1 if $s_i \in$ A and 0 otherwise.

Proof (cont.)

The function f: $L \rightarrow B$, where f(A) equals the characteristic sequence of A, is one-to-one and onto. Hence, it is a correspondence.

Therefore, as B is uncountable, L is uncountable as well.