

Existence of unrecognizable languages

Counting

- **Definition:** A set S is countable if there exists a function ϕ mapping \mathbb{N} onto S (recall: a function $\phi : A \mapsto B$ is “onto” if for every $b \in B$ there exists $a \in A$ such that $\phi(a) = b$. An onto function is also called a “surjection”).
- **Example:** \mathbb{Z} is countable. Define $\phi(i) = (-1)^i \lceil i/2 \rceil$.

$$\begin{aligned}\phi(0) &= 0 \\ \phi(1) &= -1 \\ \phi(2) &= 1 \\ \phi(3) &= -2 \\ \phi(4) &= 2 \\ &\vdots\end{aligned}$$

- **Theorem [Cantor]:** \mathbb{R} is not countable.
- **Proof:** the technique is called “diagonalization”. Assume for a contradiction that \mathbb{R} is countable, i.e. there is a function ϕ mapping \mathbb{N} onto \mathbb{R} . For $i, j \in \mathbb{N}$ let $\phi(i)_j$ be the j -th digit after the decimal point in the decimal representation of $\phi(i)$ (if $\phi(i)$ has a terminating decimal representation then “pad” it with an infinite number of zeroes). We will define a number $R \in \mathbb{R}$ but for all i , $R \neq \phi(i)$, contradicting the assumption that ϕ is onto. Define R to be the number whose decimal representation is $0.R_0R_1R_2R_3\cdots$, where

$$R_i = \begin{cases} 1, & \text{if } \phi(i)_i \neq 1 \\ 2, & \text{otherwise} \end{cases}$$

Then $R \in \mathbb{R}$, since it has a decimal representation. But for all i , $\phi(i) \neq R$ since the i -th digit of $\phi(i)$ after the decimal place differs from the i -th digit of R .

- Why is this called diagonalization? Consider the following table:

$\phi(0)_0$	$\phi(0)_1$	$\phi(0)_2$	$\phi(0)_3$	\cdots
$\phi(1)_0$	$\phi(1)_1$	$\phi(1)_2$	$\phi(1)_3$	\cdots
$\phi(2)_0$	$\phi(2)_1$	$\phi(2)_2$	$\phi(2)_3$	\cdots
$\phi(3)_0$	$\phi(3)_1$	$\phi(3)_2$	$\phi(3)_3$	\cdots
\vdots	\vdots	\vdots	\vdots	\ddots

we are defining R so the i -th digit in R differs from the i -th digit on the diagonal of the table.

- **Theorem:** The set of recognizable languages is countable.
- **Proof:** For each recognizable language L there exists at least one TM M with $L(M) = L$. Let's pick one such TM and call it M_L . Every TM M_L has a binary representation $\langle M_L \rangle$. Let $N_L \in \mathbb{N}$ be the number whose binary representation is $\langle M_L \rangle$. Since for every TM M , $\langle M \rangle$ starts with a 1 it follows that $N_L \neq N_{L'}$ if $L \neq L'$. Consider the following function ϕ mapping \mathbb{N} to recognizable languages:

$$\phi(i) = \begin{cases} L, & \text{if } i = N_L \text{ for some recognizable language } L \\ \emptyset, & \text{otherwise} \end{cases}$$

For each recognizable language L , $\phi(N_L) = L$, so ϕ is onto.

- **Theorem:** The set of all languages is not countable.
- **Proof:** (by diagonalization) Assume, for contradiction, that the set of all languages is countable. Then there exists a function ϕ mapping \mathbb{N} onto the set of all languages. Let's define $L_i = \phi(i)$ for $i \in \mathbb{N}$. Let s_0, s_1, s_2, \dots be an enumeration of Σ^* . We will now define a language $L \subseteq \Sigma^*$ such that for all i , $L \neq L_i$, contradicting the assumption that ϕ is onto. The language L is defined by the following rule:

$$s_i \in L \iff s_i \notin L_i$$

For all $i \in \mathbb{N}$, $L \neq L_i$, so we have our contradiction.

- A good way to visualize this is by the following table:

	s_0	s_1	s_2	s_3	\dots
L_0	1	0	0	0	\dots
L_1	1	0	1	1	\dots
L_2	0	0	0	0	\dots
L_3	1	1	1	1	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\ddots

The entry at (L_i, s_j) is 1 if $s_j \in L_i$, and 0 otherwise. The language L is constructed by "flipping" the entries on the diagonal.

- **Theorem:** There exist unrecognizable languages.
- **Proof:** Suppose, for contradiction, that all languages are recognizable. Since the set of recognizable languages is countable, this implies that the set of all languages is countable, which contradicts the previous theorem.
- What is this theorem saying? There exist problems that cannot be solved by any algorithm (in fact, the situation is worse: the vast majority of problems cannot be solved by any algorithm).

- Notice that we didn't really use any features of Turing machines, except that they can be represented by finite strings. Even if you don't believe the Church-Turing thesis, as long as your definition of algorithm is such that every algorithm has a finite description, you will be able to prove the same theorem.
- The property of having a finite description is really inherent in the concept of "algorithm": most people would agree that an algorithm should be able to be communicated by one person to another in English (or another language), in some finite (though possibly very large) amount of time.

A specific unrecognizable language

- We know that there are unrecognizable languages, but we don't have any examples of such a language.
- We'll use diagonalization to come up with an example. Consider the following table:

	$\langle M_0 \rangle$	$\langle M_1 \rangle$	$\langle M_2 \rangle$	\dots
M_0	1	0	0	\dots
M_1	0	0	0	\dots
M_2	1	1	1	\dots
\vdots	\vdots	\vdots	\vdots	\ddots

The entry $(M_i, \langle M_j \rangle)$ is 1 if M_i accepts $\langle M_j \rangle$, and it is zero otherwise. If we obtain a language by "flipping" the entries on the diagonal, then that language differs from $L(M_i)$ for each i . That is, the language should contain the string $\langle M_i \rangle$ iff M_i does not accept $\langle M_i \rangle$.

- **Definition:** $\text{DIAG} = \{\langle M \rangle \mid M \text{ does not accept } \langle M \rangle\}$
- **Theorem:** DIAG is unrecognizable.
- **Proof:** Suppose, for contradiction, that there exists a Turing machine M with $L(M) = \text{DIAG}$. Consider whether $\langle M \rangle \in \text{DIAG}$.

$$\begin{aligned} \langle M \rangle \in \text{DIAG} &\implies \langle M \rangle \in L(M) && (\text{since } L(M) = \text{DIAG}) \\ &\implies M \text{ accepts } \langle M \rangle && (\text{def'n of } L(M)) \\ &\implies \langle M \rangle \notin \text{DIAG} \end{aligned}$$

$$\begin{aligned} \langle M \rangle \notin \text{DIAG} &\implies \langle M \rangle \notin L(M) && (\text{since } L(M) = \text{DIAG}) \\ &\implies M \text{ does not accept } \langle M \rangle && (\text{def'n of } L(M)) \\ &\implies \langle M \rangle \in \text{DIAG} \end{aligned}$$

So we have $\langle M \rangle \in \text{DIAG} \iff \langle M \rangle \notin \text{DIAG}$, which is a contradiction.