Logic and the theory of computation

theory of computation part, 3rd lecture

Cardinality

definition

An important property of finite sets is their size. ($\Rightarrow$ *natural numbers*). Goal: find a generalization for infinite sets. One such generalization is **cardinality** *(G. Cantor, 1845-1918)*.

Cardinality of sets

- Sets A and B have the same cardinality, if there's a bijection between them. Notation: $|A| = |B|$.
- The cardinality of A is greater or equal to the cardinality of B if there's an injective mapping from B to A. Notation: $|A| \geq |B|$.
- The cardinality of A is greater than the cardinality of B if there is an injective mapping from B to A, but there is no bijection between them. Notation: $|A| > |B|$.

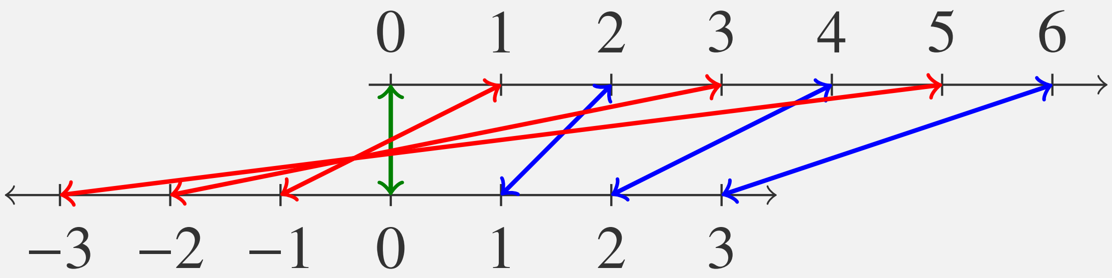
Cantor-Bernstein Theorem

If $|A| \leq |B|$ and $|A| \geq |B|$, then $|A| = |B|$.

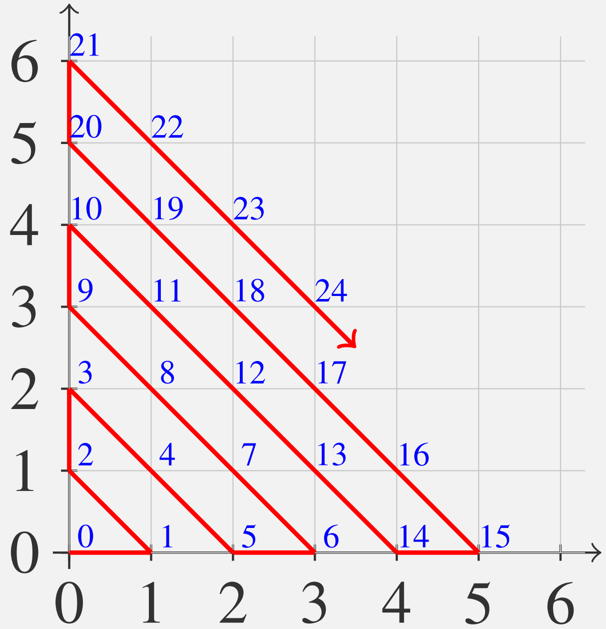
Cardinality

Examples

1st example: $|\mathbb{N}| = |\mathbb{Z}|$.



2nd example: $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.



Cardinality

Further examples

3rd example: $|\mathbb{N}| = |\mathbb{Q}|$.
Proof:
$\mathbb{N} \subset \mathbb{Q}$, so $|\mathbb{N}| \leq |\mathbb{Q}|$.
$\mathbb{Q}^+ := \{\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+$, and the fraction can not be simplified$\}$.
$\mathbb{Q}^- := \{-\frac{p}{q} \mid p \in \mathbb{N}^+, q \in \mathbb{N}^+$, and the fraction can not be simplified$\}$.
$|\mathbb{Q}^+| = |\mathbb{Q}^-|$.
$\frac{p}{q} \in \mathbb{Q}^+ \mapsto (p, q) \in \mathbb{N} \times \mathbb{N}$ injective, so $|\mathbb{Q}^+| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.
Let $\mathbb{Q}^+ = \{a_1, a_2 \ldots, \}$, $\mathbb{Q}^- = \{b_1, b_2 \ldots, \}$, so $\mathbb{Q} = \{0, a_1, b_1, a_2, b_2, \ldots\}$

Countably infinite cardinality

The cardinality of $\mathbb{N}$ is called **countably infinite**. A set is **countable** either if it is finite or countably infinite.

Cardinality

Continuum cardinality

Theorem

Union of countable countable sets is countable.

Are there other cardinalities?

Yes, $|\mathbb{R}| > |\mathbb{N}|$.

Continuum cardinality

The cardinality of $\mathbb{R}$is called **continuum**.

4th example: $|\mathbb{R}| = |(0, 1)|$.

$\operatorname{tg}(\pi(x - \frac{1}{2}))\big|_{(0,1)} : (0, 1) \to \mathbb{R}$ is a bijection between $(0, 1)$ and $\mathbb{R}$.

Remark: $|\mathbb{R}| = |(a, b)| = |[c, d]|$ and $|\mathbb{R}| = |\mathbb{R}^n|$.

Cardinality

Words and languages

5th example : $|\{0,1\}^*| = |\mathbb{N}|$.

Shortlex ordering is a bijection:
ε,0,1,00,01,10,11,000,001,010,011,100,101,110,111,0000,. . .

6th example
$$\left|\{L \mid L \subseteq \{0,1\}^*\}\right| = \left|\{(b_1, \ldots, b_i, \ldots) \mid b_i \in \{0,1\},\ i \in \mathbb{N}\}\right|$$

Natural bijection:
Order the binary words according to shortlex.
We can associate for an arbitrary language a 0-1 sequence of length countably infinite. Let the ith bit be 1 if ith word is a an element of the lnguage, 0 otherwise.
(the *characterestic sequence* of the language).

Let the RHS be denoted by $\{0,1\}^{\mathbb{N}}$.

Cardinality

Words and languages

7th example $|\{0, 1\}^{\mathbb{N}}| = |[0, 1)|$.

Proof (sketch):

We can associate for any $x \in [0, 1)$ an infinte binary sequence, namely (one of) the sequence after "0." in the binary representation of x. This an injective mapping, so $|[0, 1)| \leq |\{0, 1\}^{\mathbb{N}}|$.

For a $\mathbf{z} \in \{0, 1\}^{\mathbb{N}}$ replace all occurences of a 1 by a 2, write "0." before the sequence and see the result as a ternary representation of a number from $[0, 1)$. This mapping is an injective one, so $|\{0, 1\}^{\mathbb{N}}| \leq |[0, 1)|$.

According to the theorem of Cantor and Bernstein $|\{0, 1\}^{\mathbb{N}}| = |[0, 1)|$.

Cardinality

Cantor's diagonal method

Claim: $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$

Proof:

$|\{0,1\}^{\mathbb{N}}| \geq |\mathbb{N}|$:

$H_0 := \{(1, 0, 0, 0, \ldots), (0, 1, 0, 0, \ldots), (0, 0, 1, 0, \ldots), \ldots\}$

$H_0 \subset \{0,1\}^{\mathbb{N}}$, and $|H_0| = |\mathbb{N}|$.

So we need: $|\{0,1\}^{\mathbb{N}}| \neq |\mathbb{N}|$.

Cardinality

Cantors's diagonal method

Claim: $|\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$

Suppose, that $|\{0,1\}^{\mathbb{N}}| = |\mathbb{N}|$. This means there's a bijection between $\{0,1\}^{\mathbb{N}}$ and $\mathbb{N}$, so $\{0,1\}^{\mathbb{N}} = \{u_i \mid i \in \mathbb{N}\} = \{u_1, u_2, \ldots\}$ is an enumaration of $\{0,1\}^{\mathbb{N}}$.
Let $u_i = (u_{i,1}, u_{i,2}, \ldots, u_{i,j}, \ldots)$, where $u_{i,j} \in \{0,1\}$ holds for all $i, j \in \mathbb{N}$.
Consider the countably infinite sequence $u = \{\overline{u_{1,1}}, \overline{u_{2,2}}, \ldots, \overline{u_{i,i}}, \ldots)$, i.e., $u \in \{0,1\}^{\mathbb{N}}$, where $\overline{b} = 0$, if $b = 1$ and $\overline{b} = 1$, if $b = 0$.

Since all countably infinite 0-1 sequences are enumerated there is a $k \in \mathbb{N}$, such that $u = u_k$.

The kth bit of u k equals $u_{k,k}$ since this was a notation for its kth bit.
Otherwise it is $\overline{u_{k,k}}$ by the definition of u.
But this is impossible, so our assumption $|\{0,1\}^{\mathbb{N}}| = |\mathbb{N}|$ was false.

1st corollary

Continuum is a greater cardinality than countably infinite.

Cardinality

Cantor's diagonal method

2nd corollary

There are more languages than words over the alphabet $\{0, 1\}$.

Remark $\{L \mid L \subseteq \{0,1\}^*\} = \mathcal{P}(\{0,1\}^*)$. Is it true that $|\mathcal{P}(H)| > |H|$ always holds?

Theorem

$|\mathcal{P}(H)| > |H|$ holds for all sets H.

Proof: $|\mathcal{P}(H)| \geq |H|$, since $\{\{h\} \mid h \in H\} \subseteq \mathcal{P}(H)$.

$|\mathcal{P}(H)| \neq |H|$: by Cantor's diagonal method
Assume $f : \mathcal{P}(H) \leftrightarrow H$ is a bijection. Let us define a set $A \subseteq H$:
$\forall x \in H : \quad x :\in A \;\Leftrightarrow\; x \notin f^{-1}(x)$

Is it true that $f(A) \in A$? If yes, $f(A) \notin A$, if not $f(A) \in A$, so $f(A)$ is neither in A nor outside A which is a contradiction. So our initial assumption was false.

Solving computational problems by TM's

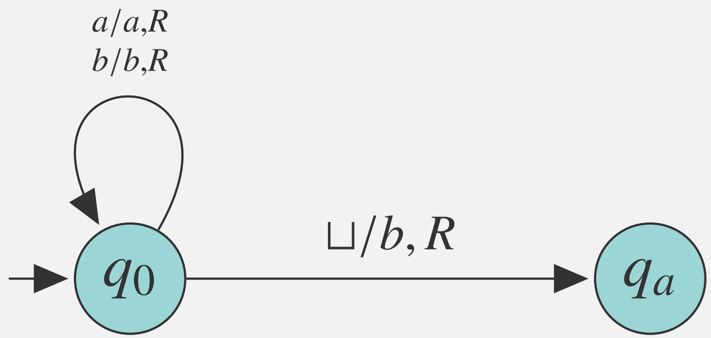
We can use TM's for solving computation problems, too.

TM for computational problems

We say that a TM $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_a, (q_r)\rangle$ computes the function $f : \Sigma^* \to \Delta^*$ if for all inputs $u \in \Sigma^*$ it halts, and $f(u) \in \Delta^*$ can be read on its last tape.

Remark: for computing tasks we do not need to distinguish q_a and q_r, one halting state would have been enough.

Example: $f(u) = ub \quad (u \in \{a, b\}^*)$.



Problems as formal languages

If a problem has countable possible inputs we can code them over a finite alphabet.
How large should be the size of the alphabet? For an alphabet of size d we need words of length $log_d n$ to code the first n words. Since $log_d n = \Theta(log_{d'} n)$ for $d, d' \geq 2$ the size of the alphabet does not really count.
But! Do not use unary codes.! See: representing natural numbers by drawing sticks.

For an input I let $\langle I \rangle$ denote the code of I.

Decision problems:
$L = \{\langle I \rangle \,|\, I$ is a "yes" istance of the problem$\}$. Can L be decided by a TM?

Function problems (includes decision problems):
Is there a TM computing the function f, i.e., computing the function $\langle I \rangle \mapsto \langle f(I) \rangle$ for all possible inputs I.

Coding TM's

We may assume, that $\Sigma = \{0, 1\}$. Any set of inputs can be efficiently coded of Σ.
The **code** of a TM M (notation $\langle M \rangle$) is the following:
Let $M = (Q, \{0, 1\}, \Gamma, \delta, q_0, q_a, q_r)$, where

- $Q = \{p_1, \ldots, p_k\},\ \Gamma = \{X_1, \ldots, X_m\},\ D_1 = R,\ D_2 = S, D_3 = L$
- $k \geq 3,\ p_1 = q_0,\ p_{k-1} = q_a,\ p_k = q_r,$
- $m \geq 3,\ X_1 = 0,\ X_2 = 1,\ X_3 = \sqcup.$
- the code for a transition $\delta(p_i, X_j) = (p_r, X_s, D_t)$ is $0^i 10^j 10^r 10^s 10^t$.
- $\langle M \rangle$ is the concatenation of the codes of the transitions separated by 11's.

Observation: $\langle M \rangle$ always starts and ens with 0 and doies not contaion consecutive three 1's.

$\langle M, w \rangle := \langle M \rangle 111 w$

Existance of a non-Turing-recognisable language

Notation: for all $i \geq 1$,

- Let w_i denote the ith elemnt of $\{0, 1\}^*$ according to the shortlex ordering.
- Let M_i denote the TM defined by w_i (if w_i is not a code of a TM then let M_i be a TM accepting nothing)

Theorem

There exists a non-Turing-recognisable language.

Proof: Two different languages can not be recognised by the same TM. The cardinality of TM's is countably infinite (the above coding is an injection into a countable set $\{0, 1\}^*$). On the other hand, the number of languages over $\{0, 1\}$ has cardinality continuum.

So actually the "majority" of the languages are unrecognisable by a TM. Is there a specific unrecognizable language? Yes, $L_{\text{diag}} = \{\langle M \rangle \mid \langle M \rangle \notin L(M)\}$.

L_{diag} Turing-unrecognisable

Theorem

$L_{\text{diag}} \notin RE$.

With Cantor's diagonal method:

Proof: Consider the following bit table T of size $\mathbb{N}$ in both dimension.

$T(i, j) := 1 \;\Leftrightarrow\; w_j \in L(M_i)\ (i, j \geq 1)$.

Let $\mathbf{z}$ be the diagonal of T. Then $\mathbf{z}$ is string of countably infinite bits.

$\bar{\mathbf{z}}$ is the bitwise complement of $\mathbf{z}$. Then:

- for all $i \geq 1$ the ith row of T is characteristic sequence of $L(M_i)$.
- $\bar{\mathbf{z}}$ is the characteristic sequence of L_{diag}
- for all $L \in RE$ its characteristic sequence appears as a row of T
- $\bar{\mathbf{z}}$ is different from all rows of T
- so L_{diag} is different from all languages from RE

The universal TM

recognisability

Universal language: $L_u = \{\langle M, w\rangle \mid w \in L(M)\}$.

Theorem

$L_u \in RE$

Proof: We construct a "universal" 4-tape TM U which can simulate all TM's on each possible input.

1st tape: read only tape, U can always read $\langle M, w\rangle$ here.

2nd tape: the current content of M's tape (coded as above)

3rd tape: the current state of M (coded as above)

4th tape: work tape

The universal TM

recognisability

Universal language: $L_u = \{\langle M, w\rangle \mid w \in L(M)\}$.

Theorem

$L_u \in RE$

sketch of the construction of U:

- Checks whether the input is of type $\langle M, w\rangle$. If not, it rejects the input.
- if yes, it copies w to its second tape, the code of q_0 to its 3rd tape
- Simulates a step of M:
  – Reads the current tape symbol on M's tape from its second tape
  – Reads the current state of M from its 3rd tape
  – Simulates a step of M (uses the 4th tape if neccessary)
  according to the description of M (can be read on tape 1).
- If M goes to its accepting/rejecting state, so does U.

The universal TM

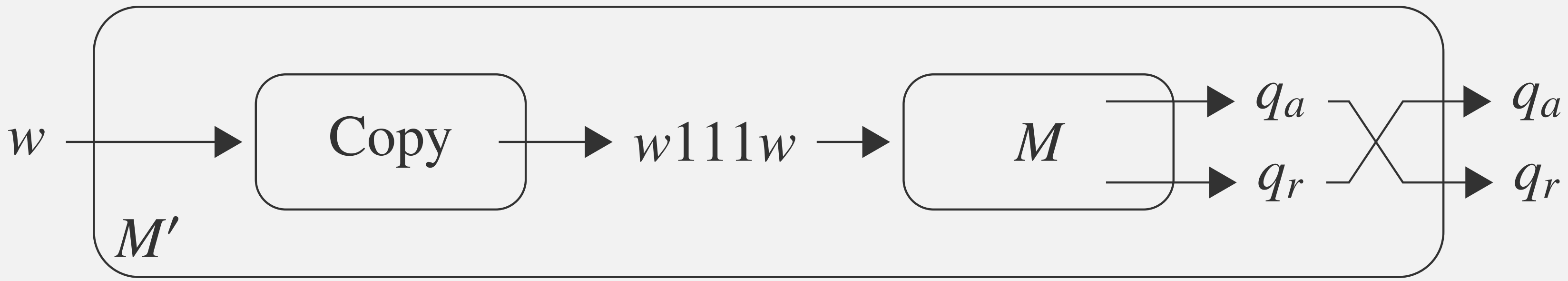
undecidability

Remark: if M does not halt on w, then so does U for $\langle M, w\rangle$, so U does not decide L_u.

Theorem

$L_u \notin R$.

Proof: Suppose on the contrary that there exists a TM M deciding L_u. Using M we construct a TM M' recognising L_{diag}.



$w \in L(M') \ \Leftrightarrow w111w \notin L(M) \Leftrightarrow$ the TM coded by w does not accept $w \Leftrightarrow \ w \in L_{\text{diag}}$.

So $L(M') = L_{\text{diag}}$, contradiction.

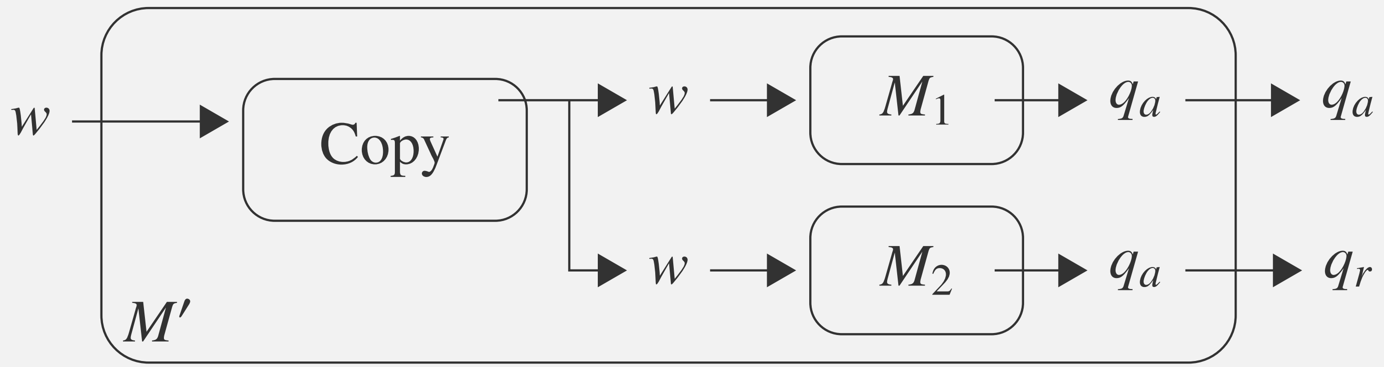
Properties of R and RE

Notation: For $L \subseteq \Sigma^*$, let $\bar{L} = \{u \in \Sigma^* \mid u \notin L\}$.

Theorem

If L and $\bar{L} \in RE$, then $L \in R$.

Proof: Let M_1 and M_2 be TM's recognising L and $\bar{L}$ respectively.
We construct a 2-tape TM M':



M' copies w to its second tape, then simulates M_1 and M_2 by switching between simulations step by step until one of them reaches its q_a.
So M' recognises L, but also halts on every input, so $L \in R$.

Properties of R and RE

Corollary

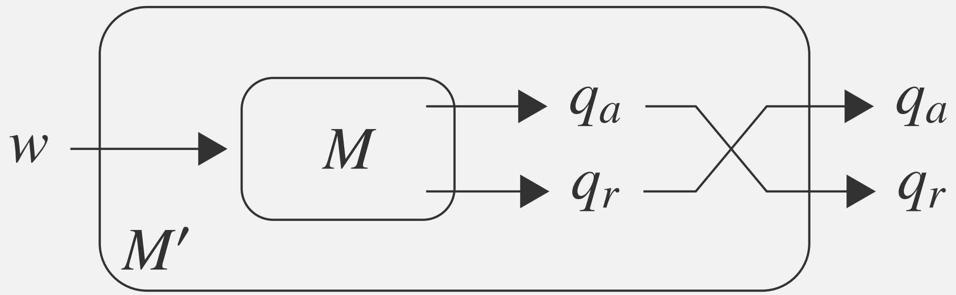
RE is not closed for the complement operation

Proof:
Let $L \in RE \setminus R$ (one such language is L_u) Then $\bar{L} \notin RE$, otherwise $\bar{L} \in RE$ but then $L \in R$ would follow, contradiction .

Theorem

R is closed for the complement operation.

Proof: Let $L \in R$ be a TM deciding M. Then M' decides $\bar{L}$:



Reduction

Computable function

$f : \Sigma^* \to \Delta^*$ is **computable**, if there is a TM which computes it. [see TM's for computing functions]

Reduction

$L_1 \subseteq \Sigma^*$ is **reducible** to $L_2 \subseteq \Delta^*$ if there is a computable function $f : \Sigma^* \to \Delta^*$ such that $w \in L_1 \Leftrightarrow f(w) \in L_2$. Notation: $L_1 \leq L_2$

(Emil Post, 1944, many-one reducibility)

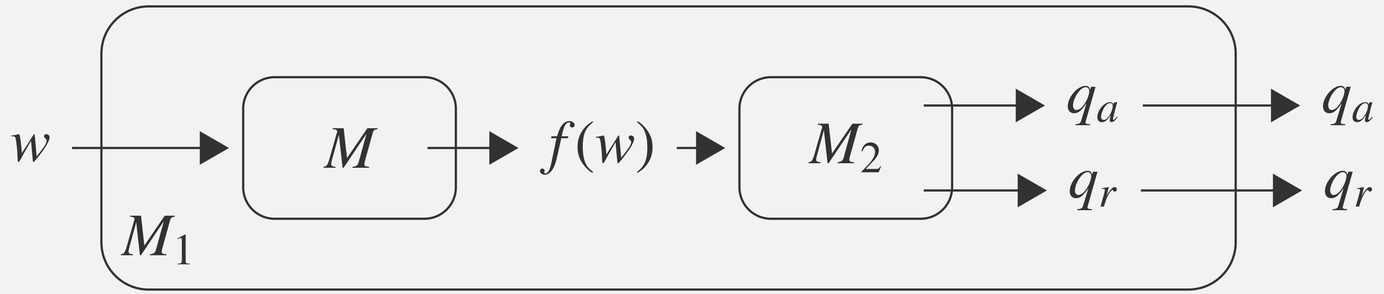
Theorem

- If $L_1 \leq L_2$ and $L_1 \notin RE$, then $L_2 \notin RE$.
- If $L_1 \leq L_2$ and $L_1 \notin R$, then $L_2 \notin R$.

Reduction

Proof:

Let $L_2 \in RE$ ($\in R$) and $L_1 \leq L_2$. Let M_2 be a TM recognising (deciding) L_2. Furthermore let M be the TM computing the reduction. Construction of M_1:



If M_2 recognises L_2 then M_1 recognises L_1 as well. If it decides L_2, then so does M_1 with L_1.

Corollary

- If $L_1 \leq L_2$ and $L_2 \in RE$, then $L_1 \in RE$.
- If $L_1 \leq L_2$ and $L_2 \in R$, then $L_1 \in R$.

The halting problem of TM's

Halting problem:
$L_h = \{\langle M, w\rangle \mid M \text{ halts on input } w\}$.
Observation: $L_u \subseteq L_h$
Is it true? $A \subseteq B$, and A is undecidable. Is B undecidable as well? No.

Theorem

$L_h \notin R$.

Proof: It is enough to show that $L_u \leq L_h$.
For an arbitrary TM M let M' be the following. M' does the following for an arbitrary input u:

1. it runs M on u
2. if M goes to q_a, M' does the same for its q_a, as well
3. if M goes to q_r, let M' go to an infite cycle

The halting problem of TM's

Proof: (cont'd.)
Can be proved that

- $f : \langle M, w\rangle \to \langle M', w\rangle$ is a computable function
- for an arbitrary (TM,input) pair (M, w):
  $\langle M, w\rangle \in L_u \Leftrightarrow M$ accepts $w \Leftrightarrow M'$ halts on $w \Leftrightarrow \langle M', w\rangle \in L_h$

So the construction of M' gives a reduction of L_u to L_h. So $L_h \notin R$.
Remark: At reductions we usually focus on the image of the interesting objects.
E.g., in the previous proof we were focusing on words that are codes of a TM. To complete the function f for all words of $\{0, 1\}^*$:

$$f(x) = \begin{cases} \langle M', w\rangle & \text{if } x = \langle M, w\rangle \text{ for some TM } M \text{ and word } w, \\ \varepsilon & \text{otherwise.} \end{cases}$$

$(x \in \{0, 1\}^*)$

The halting problem of TM's

Theorem

$L_h \in RE$.

Proof: It's enough to show that $L_h \leq L_u$. For a TM M let M' be the following TM: M' works on an input u as follows:

1. it runs M on u
2. if M goes to q_a, M' does the same for its q_a, as well
3. if M goes to q_r, let M' go to its q_a.

Can be proved that

- $f : \langle M \rangle \to \langle M' \rangle$ is a computable function
- for an arbitrary (TM,input) pair (M, w): $\langle M, w \rangle \in L_h \Leftrightarrow M$ halts on $w \Leftrightarrow M'$ accepts $w \Leftrightarrow \langle M', w \rangle \in L_u$

So the construction of M' is a reduction of L_h to L_u. We are done due to the previous theorems.