

Proof of a Property of *

In class last Thursday (3rd April, 2008) we defined the formal language of Regular Expressions, and then gave the terms of the language meaning as regular languages. To recap, we defined a meaning function $\mathcal{M}[\]$ that maps regular expressions over an alphabet A to regular languages as follows.

$$\mathcal{M}[\Lambda] =_{\text{def}} \Lambda \quad (1)$$

$$\mathcal{M}[\emptyset] =_{\text{def}} \emptyset \quad (2)$$

$$\forall a \in A. \mathcal{M}[a] =_{\text{def}} \{a\} \quad (3)$$

$$\forall R, S \in \text{RE}. \mathcal{M}[R + S] =_{\text{def}} \mathcal{M}[R] \cup \mathcal{M}[S] \quad (4)$$

$$\forall R, S \in \text{RE}. \mathcal{M}[RS] =_{\text{def}} \mathcal{M}[R] \cdot \mathcal{M}[S] \quad (5)$$

$$\forall R \in \text{RE}. \mathcal{M}[R^*] =_{\text{def}} \mathcal{M}[R]^* \quad (6)$$

Note that this is an inductive definition of a function. Rules 1–3 are the base cases, and rules 4–6 are the induction rules. There is one rule for each clause in the definition of Regular Expressions.

Then we proved the commutative property of $+$ (Lecture 2 Slide 9) by appealing to this definition. Next we tried to prove the first part of property 11.1.7 from Hein (p. 638):

$$(R + S)^* = (R^* + S^*)^*$$

Theorem 1 (A property of Regular Expressions)

$$(R + S)^* = (R^* + S^*)^*$$

Proof

$$\begin{aligned}\mathcal{M}[(R + S)^*] &= \mathcal{M}[(R + S)]^* && \text{(definition of } \mathcal{M} \text{ (6))} \\ &= (\mathcal{M}[R] \cup \mathcal{M}[S])^* && \text{(definition of } \mathcal{M} \text{ (4))} \\ &= (\mathcal{M}[R]^* \cup \mathcal{M}[S]^*)^* && \text{(property of } * \text{ (Hein property 1.16 d (p. 45))} \\ &= (\mathcal{M}[R^*] \cup \mathcal{M}[S^*])^* && \text{(definition of } \mathcal{M} \text{ (6))} \\ &= (\mathcal{M}[R^* + S^*])^* && \text{(definition of } \mathcal{M} \text{ (4))} \\ &= \mathcal{M}[(R^* + S^*)^*] && \text{(definition of } \mathcal{M} \text{ (6))}\end{aligned}$$

Q.E.D.

In other words, the theorem says that the required property of Regular Expressions follows from the corresponding property of the closure operation $*$:

$$(L^* \cup M^*)^* = (L \cup M)^*$$

This may seem like cheating, since Hein does not actually prove property 1.16 d. So, to make sure that we are on firm ground, let's prove this property.

Theorem 2 (Hein's Closure Property 1.16 d)

$$(L^* \cup M^*)^* = (L \cup M)^*$$

Proof

To prove the required equality, we prove the two inequalities

$$(L^* \cup M^*)^* \subseteq (L \cup M)^* \quad (7)$$

$$(L^* \cup M^*)^* \supseteq (L \cup M)^* \quad (8)$$

This suffices to prove our result, because \subseteq is antisymmetric.

Proof of equation 7

$$R \subseteq R \cup S \quad (\text{property of } \cup) \quad (9)$$

$$R^* \subseteq (R \cup S)^* \quad (\text{definition of } ^*) \quad (10)$$

$$S^* \subseteq (R \cup S)^* \quad (\text{line 10, interchanging } R \text{ and } S) \quad (11)$$

$$R^* \cup S^* \subseteq (R \cup S)^* \quad (\text{union of lines 10 and 11}) \quad (12)$$

$$(R^* \cup S^*)^* \subseteq ((R \cup S)^*)^* \quad (\text{apply } ^* \text{ to line 12}) \quad (13)$$

$$(R^* \cup S^*)^* \subseteq (R \cup S)^* \quad (L^* = (L^*)^*, \text{ Hein property 1.16 c}) \quad (14)$$

Proof of equation 8

$$L \subseteq L^* \quad (\text{definition of } ^*) \quad (15)$$

$$M \subseteq M^* \quad (\text{definition of } ^*) \quad (16)$$

$$L \cup M \subseteq L^* \cup M^* \quad (\text{union of equations 15 and 16}) \quad (17)$$

$$(L \cup M)^* \subseteq (L^* \cup M^*)^* \quad (\text{apply } ^* \text{ to line 17}) \quad (18)$$

Combining 7 and 8, we have our result.

Q.E.D.

Why did I do that?

- Example of a proof
- Handout on web site

Review of Entrance Exam

\mathbb{N} and its cardinality

- $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$
- How can we define \mathbb{N} without “...” ?

By induction

1. $0 \in \mathbb{N}$
2. if $x \in \mathbb{N}$, then $x+1 \in \mathbb{N}$
3. these are the only elements of \mathbb{N}

Cardinality of Sets

Cardinality of Sets

- How can we decide if two sets are of the same size?

Cardinality of Sets

- How can we decide if two sets are of the same size?
- Set up a *bijection* between the elements of the sets

Cardinality of Sets

- How can we decide if two sets are of the same size?
- Set up a *bijection* between the elements of the sets
- Is there a bijection between \mathbb{N} and \mathbb{N}_{even} ?

Cardinality of Sets

- How can we decide if two sets are of the same size?
- Set up a *bijection* between the elements of the sets
 - Is there a bijection between \mathbb{N} and \mathbb{N}_{even} ?
 - You bet!

Cardinality of Sets

- How can we decide if two sets are of the same size?
- Set up a *bijection* between the elements of the sets
 - Is there a bijection between \mathbb{N} and \mathbb{N}_{even} ?
 - You bet!
 - Any subset of a countable set is countable

Countability

- What is a countable set?
- Is \mathbb{N} a countable set?
- What about \mathbb{Q} ?

Countability of \mathbb{Q}

	1	2	3	4	5	6	7	8	...
1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{8}$...
2	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$	$\frac{2}{6}$	$\frac{2}{7}$	$\frac{2}{8}$...
3	$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{3}{6}$	$\frac{3}{7}$	$\frac{3}{8}$...
4	$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$	$\frac{4}{6}$	$\frac{4}{7}$	$\frac{4}{8}$...
5	$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$	$\frac{5}{6}$	$\frac{5}{7}$	$\frac{5}{8}$...
6	$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{3}$	$\frac{6}{4}$	$\frac{6}{5}$	$\frac{6}{6}$	$\frac{6}{7}$	$\frac{6}{8}$...
7	$\frac{7}{1}$	$\frac{7}{2}$	$\frac{7}{3}$	$\frac{7}{4}$	$\frac{7}{5}$	$\frac{7}{6}$	$\frac{7}{7}$	$\frac{7}{8}$...
8	$\frac{8}{1}$	$\frac{8}{2}$	$\frac{8}{3}$	$\frac{8}{4}$	$\frac{8}{5}$	$\frac{8}{6}$	$\frac{8}{7}$	$\frac{8}{8}$...
⋮	⋮								...

- is countable because we can line up its elements in order and count them
- Why do we do it in this wierd zig-zag fashion?

Uncountability of \mathbb{R}

To Prove: *The set of real numbers $\{x \in \mathbb{R} \mid 0 < x < 1\}$, is uncountable.*

Proof by contradiction: Suppose that the set is uncountable. Then we can claim to make an enumeration of all of them, and that it looks something like this:

1. 0.38602563708....
2. 0.57350762050....
3. 0.99356753207....
4. 0.25763200456....
5. 0.00005320562....
6. 0.99035638567....
7. 0.55522730567....
8.
9.
- 10.

Now we claim to have listed every decimal between 0 and 1. But you can always give me a decimal which is not in my table! Do it like this:

1. Take the first digit = 7 (not 3); Decimal = 0.7.....
2. Take the second digit = 3 (not 7); Decimal = 0.73.....
3. Take the third digit = 7 (not 3); Decimal = 0.737.....
4. Take the fourth digit = 7 (not 6); Decimal = 0.7377.....
5. Take the fifth digit = 3 (not 5); Decimal = 0.73773.....
6. Take the sixth = 3 (not 6); Decimal = 0.737733.....
7. 0.737733?.....
8. 0.737733xx.....
9.
- 10.

1.	0.38602563708....
2.	0.57350762050....
3.	0.99356753207....
4.	0.25763200456....
5.	0.00005320562....
6.	0.99035638567....
7.	0.55522730567....
8.
9.
10.	

The rule is: make sure that the k^{th} digit of the new decimal is not equal to the k^{th} digit of the k^{th} number in my original list. (We avoid using 9 and 0.)

Compete the Argument

- If the author of the enumeration says: the number that you wrote is already in my list, at position 153, you can say:
- No! My number differs from that in the 153rd decimal digit.
- So, the number you wrote in not in the list.
- Therefore, the list was not a complete enumeration of all the real numbers.
- But we can repeat this argument for *any* supposed enumeration
- So there is *no effective enumeration* of \mathbb{R}