CS208: Mathematical Foundations of CS **Fall 2018**

Lecture 18: September 19

Lecturer: Samar *Scribes: Deepshikha Rana,Navya Varakantham*

18.1 Power sets are strictly bigger

Theorem 1 *For any set A,the power set pow(A) is strictly larger than A*

Proof: To show that A is strictly smaller than pow(A), we have to show that if g is a function from A to pow(A), then g is not a surjection.

A is strictly smaller than pow(A) iff NOT(A surjection pow(A)). This means if there is a relation g from A to pow(A),then g can't be surjective. So, g can be partial function or total function. Since any partial function with nonempty codomain can be extended to a total function with the same range,so let us assume that g is a total function.

To show that g is not a surjection, well simply find a subset $Ag \subseteq A$ that is not in the range of g. For any element $a \in A$, to look at the set $g(a) \subseteq A$ and ask whether or not a happens to be in g(a). First, define

$$\text{Ag} ::= \{a \in A \mid a \notin g(a)\}$$

Ag is a subset of A, that means $Ag \in pow(A)$. But for every element $a \in A$, Ag differs from its image g(a).

To explain the above statement, suppose to the contrary that Ag is in the range of g, that means, there must be some element a_0 in A such that Ag = g(a_0). Now by definition of Ag,

$$a \in g(a_0) \text{ iff } a \in Ag \text{ iff } a \notin g(a)$$

for all a/inA. Let a = a_0 which yields the contradiction

$$a_0 \in g(a_0) \text{ iff } a_0 \notin g(a_0)$$

So g is not a surjection, because there is an element in the power set of A, specifi- cally the set Ag , that is not in the range of g.

This concludes the proof.

■

Exercise:

Prove that there exists a bijection, $\mathbb{N} \longrightarrow \mathbb{N}^n$.

Hint: For any a $\in \mathbb{N}$ it can be uniquely decomposed into x and y as,

$$\text{a} = \frac{(x+y+1)\times(x+y)}{2} + \text{y}$$

18.1.1 Some Representations

Infinite bit sequences : $[0,1]^w$

Countable bit sequences : $[0,1]^*$

For a given set A,

All countable sequences : A^w

Infinite sequences : A^*

18.1.2 pow($\mathbb{N}$)s uncountable

Lemma 1 *pow($\mathbb{N}$) is uncountable.*

$\mathbb{N}$ is strictly smaller than pow($\mathbb{N}$)

C is countable iff $\mathbb{N}$ surj C(proved already in previous lecture) If C is uncountable

$$\text{NOT}(\mathbb{N} \text{ surj C) iff } \mathbb{N} \text{ strict C.}$$

We know that $\mathbb{N}$ strict pow($\mathbb{N}$).Therefore,

$$\text{pow}(\mathbb{N}) \text{ is uncountable.}$$

This completes the proof.

The bijection between subsets of an n-element set and the length n bit-strings $[0,1]^n$ carries over to a bijection between subsets of a countably infinite set and the infinite bit-strings, $[0,1]^w$. That is, pow(N) bij $[0,1]^w$. This immediately implies

$$[0,1]^w \text{ is uncountable.}$$

Corollary 1.1 *(a) If U is an uncountable set and A surj U , then A is uncountable.*

(b) If C is a countable set and C surj A, then A is countable.

Corollary 1.2 *The set $\mathbb{R}$ of real numbers is uncountable.*

To prove this, think about the infinite decimal expansion of a real number:

$$\sqrt[2]{2} = 1.4142...,$$

$$6 = 6.000...,$$

$$1/10 = 0.1000...,$$

$$4\tfrac{1}{99} = 4.010101...,$$

Lets map any real number r to the infinite bit string b(r) equal to the sequence of bits in the decimal expansion of r, starting at the decimal point. If the decimal expansion of r contains a digit other than 0 or 1, then leave b(r) as undefined.

For example,

$$\text{b}(\sqrt[2]{2}) = \text{undefined},$$

$$\text{b}(6) = 000...,$$

$$\text{b}(1/10) = 1000...,$$

$$\text{b}(4\tfrac{1}{99}) = 010101...$$

Now b is a function from real numbers to infinite bit strings. It is not a total function, but it clearly is a surjection. This shows that

$$\mathbb{R} \text{ surj } [0,1]^w$$

and the uncountability of the reals.

18.1.3 Larger Infinities

There are lots of different sizes of infinite sets. For example, starting with the infinite set N of non-negative integers, we can build the infinite sequence of sets

$$\mathbb{N} \text{ strict pow}(\mathbb{N}) \text{ strict pow}(\text{pow}(\mathbb{N})) \text{ strict pow}(\text{pow}(\text{pow}(\mathbb{N}))) \text{ strict ...}$$

Each of these sets is strictly bigger than all the pre- ceding ones. The union of all the sets in the sequence is strictly bigger than each set in the sequence.

$$\text{U} = \bigcup pow^n(\mathbb{N})$$

There exists $\mathbb{R}$ surj pow(U).

18.2 Diagonal Argument

Suppose there is a bijection between $\mathbb{N}$ and $[0,1]^w$. If such a relation existed, we would be able to display it as a list of the infinite bit strings in some countable order or another. Once wed found a viable way to organize this list, any given string in $[0,1]^w$ would appear in a finite number of steps, just as any integer you can name will show up a finite number of steps from 0. This hypothetical list would look something like the one below, extending to infinity both vertically and horizontally.

$$\boxed{\begin{array}{l} A_0 = 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0 \ldots \\ A_1 = 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1 \ldots \\ A_2 = 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1 \ldots \\ A_3 = 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1 \ldots \\ A_4 = \ldots .\ 0 \ldots \ldots \\ A_5 = \ldots \ldots 1 \ldots \ldots \end{array}}$$

we can form a sequence D consisting of the bits on the diagonal.

D = 1 1 1 0 0 1 . . .

Then, we can form another sequence by switching the 1s and 0s along the diagonal. Call this sequence C :

C = 0 0 0 1 1 0 . . . (complement of D)

Now if the nth term of A_n is 1 then the nth term of C is 0, and vice versa, which guarantees that C differs from A_n. In other words, C has at least one bit different from every sequence on our list. So C is an element of $[0, 1]^w$ that does not appear in our listour list cant be complete!

This diagonal sequence C corresponds to the set $\{a \in A \mid a \notin g(a)\}$. Both are defined in terms of a countable subset of the uncountable infinity in a way that excludes them from that subset, thereby proving that no countable subset can be as big as the uncountable set.

References

[LLM13] E. LEHMAN, F. T. LEIGHTON ANDA. R. MEYER, Mathematics for Computer Science, 2013, pp.13, 16, 24.