CSCI 2824 - CU Boulder, 2019 Summer

Lecture 12: Computability

20 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications, Rosens's Discrete Mathematics and its Applications, Bettina and Thomas Richmond's A Discrete Transition to Advanced Mathematics, and Andrew Altomare's notes.

1 In-class problems

Theorem 1.1. *Suppose the domain and co-domain of a function f are finite sets with the same cardinality. Then f is injective if and only if f is surjective.*

Proof. Let A and B be finite sets such that $|A| = |B| = n$ for arbitrary $n \in \mathbb{N}$. We will consider both directions of the biconditional.

f is injective therefore f is surjective. Let $C = f(A) = \{f(a_1), f(a_2), \ldots, f(a_n)\}$, the range of f over A. Thus $C \subseteq B$. Further, $|C| = n$ because $\forall i, j \in \mathbb{N}$ if $i \neq j$ then $f(a_i) \neq f(a_j)$. Therefore, $C = B$.

f is surjective therefore f is injective. Since f is surjective, the range $f(A)$ is also the co-domain B. If it were not injective, then there would exist distinct elements a_i and a_j such that $f(a_i) = f(a_j)$. Thus, $|f(A)| < |B|$ a contradiction. □

Theorem 1.2. *Suppose $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are injective functions. Then, $g \circ f$ is injective.*

Proof. Consider $p, q \in A$ such that $p = q$. Then, under f we find $f(p) = f(q)$ since f is injective. Further, since g is injective then $g(f(p)) = g(f(q))$ proving injectivity. □

Theorem 1.3. *Suppose $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are surjective functions. Then, $g \circ f$ is surjective.*

Proof. Consider $c \in C$. Since g is surjective, then there exists $b \in \boldsymbol{B}$ such that $g(b) = c$. And since f is surjective there exists $a \in A$ such that $f(a) = b$. Then, we chain them together and show that a maps to c under $g \circ f$ and therefore $g \circ f$ is surjective. □

Theorem 1.4. *Suppose $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are bijective functions. Then, $g \circ f$ is bijective.*

Proof. By Theorems 1.2 and 1.3, we see this directly. □

> **Exercise**
> What about the converse of Theorems 1.2, 1.3, and 1.4; are they true?

Theorem 1.5. *Let $f : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N}$ be defined $f(n) = \{kn | k \in \mathbb{N}\}$. Then, f is injective and is not surjective.*

Proof. Consider $n, n' \in \mathbb{N}$ such that $f(n) = f(n')$. Then, $\{1n, 2n, 3n, \ldots\} = \{1n', 2n', 3n', \ldots\}$. We only have to consider the first element when $k = 1$ to see that their minimums are the same and since we are only considering multiples therefore the other elements are also equivalent. Thus, $n = n'$.

It is not surjective because we can consider $\{1, 2\}$. It is finite and f always maps to infinite sets. $\square$

Theorem 1.6. *Let $g : \mathbb{N} \longrightarrow \mathbb{N}$ be defined $g(A) = \begin{cases} 1 & \textit{if } A = \emptyset \\ \min A & \textit{if } A \neq \emptyset \end{cases}$. Then, g is not injective and is surjective.*

Proof. Consider $A = \emptyset$ and $B = \{1\}$ then $g(A) = g(B)$ while $A \neq B$ so it's not injective.

To prove surjectivity consider $n \in \mathbb{N}$ then $g(\{n\}) = n$. $\square$

> **Exercise**
> For $n \in \mathbb{N}$ find $(g \circ f)(n)$ and for $A \in \mathcal{P}(\mathbb{N})$ find $(f \circ g)(A)$.

Theorem 1.7. $\mathbb{N} \times \mathbb{N}$ *is countable.*

$$
\begin{tikzcd}
(1,1) \arrow[r] & (1,2) \arrow[dl] & (1,3) \arrow[r] & (1,4) \arrow[dl] & \cdots \\
(2,1) \arrow[d] & (2,2) \arrow[ur] & (2,3) \arrow[dl] & (2,4) & \cdots \\
(3,1) \arrow[ur] & (3,2) \arrow[dl] & (3,3) & (3,4) & \cdots \\
(4,1) & (4,2) & (4,3) & (4,4) & \cdots
\end{tikzcd}
$$

The above figure shows our function. We can argue that it's injective and surjective easily. The same argument shows that $\mathbb{Q}$ is countable.

2 Computability

Exercise
Show that the set of all computer programs in a given computer language is countable.

This result is a consequence of the fact that any program in any language is a finite string of symbols in a finite alphabet. So given a computer language, let P be the set of all computer programs in the language. Either P is finite or P is infinite. If it's finite, then it's countable.

If it's infinite, we set up a binary code to translate the symbols of the alphabet into strings of 0s and 1s. For each program in P use this code. We then order the resulting strings by length and strings of the same length are ordered by their corresponding binary number. We then define a function $F : \mathbb{Z}^{+} \longrightarrow P$ such that $F(n)$ is the nth program in our list. This is a bijection and thus P is countably infinite.

Now, we want to show that there are non-computable functions.

Let T be the set of all functions from the positive integers to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Exercise
Show that T is uncountable.

Let S be the set of all real numbers between 0 and 1. An element of S can be represented as $0.a_1a_2a_3a_4\ldots$ Define a function F from S to a subset of T as: $F(0.a_1a_2a_3\ldots)$ is the function that sends n to a_n. Choose the co-domain of F to be exactly the subset of T that makes F surjective, i.e. the co-domain of F is the image of F. Now F is injective because for $F(x) = F(x')$ they must habe the same value for each positive integer and so the decimal digits of x and x' correspond. Thus, it's a bijection. So, T has an uncountable subset since T is uncountable.

Exercise
We're now ready to state that there noncomputable functions. Show that in any computer language there must be a function F form $\mathbb{Z}^{+}$ to $\{, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with the property that no computer program can be written in the language to take arbitrary values as input and output the corresponding function values.

The set of all programs in a language is countable. So any computer language there are not enough programs to compute every possible function. Thus, there are functions that are not computable.