# CS 361: Lecture 2 Handout

Shikha Singh

## 1 Proof by Construction

**Theorem 1.** *The set of integers $\mathbb{Z}$ is countable.*

*Proof.* To prove that $\mathbb{Z}$ is countable, we need to show that there exists a function $f(x) : \mathbb{Z} \to \mathbb{N}$ that is a bijection. We constructed the following function $f : \mathbb{Z} \to \mathbb{N}$ in class.

$$f(x) = \begin{cases} 2x & \text{if } x > 0 \\ -2x + 1 & \text{if } x \leq 0 \end{cases}$$

We convinced ourselves that this function is bijective in class using a combination of "laser vision", "pattern matching", and "proof by picture". While that is great for intuition, we need to also learn how to prove it formally using math. We do that now.

To prove that $f(x)$ is a bijection, we need to show that $f(x)$ is one-one and onto.

**One-one:** To prove that $f(x)$ is one-one, we need to show that if $f(x_1) = f(x_2)$ then $x_1 = x_2$. We have several cases depending on whether $x_1$ and $x_2$ are positive or not.

*Case 1.* $x_1 > 0$ and $x_2 > 0$ then if

$$\begin{aligned} f(x_1) &= f(x_2) \\ 2x_1 &= 2x_2 \\ x_1 &= x_2 \end{aligned}$$

*Case 2.* $x_1 \leq 0$ and $x_2 \leq 0$ then if

$$\begin{aligned} f(x_1) &= f(x_2) \\ -2x_1 + 1 &= -2x_2 + 1 \\ x_1 &= x_2 \end{aligned}$$

*Case 3.* $x_1 > 0$ and $x_2 \leq 0$ then if

$$\begin{aligned} f(x_1) &= f(x_2) \\ 2x_1 &= -2x_2 + 1 \\ x_1 + x_2 &= 1/2 \end{aligned}$$

This case can never happen because $x_1$ and $x_2$ are integers and their sum cannot be a fraction. Thus in this case, the "if" part is false, so we do not need to prove the "then" part. The same happens when we try out the fourth case where $x_1 \leq 0$ and $x_2 > 0$, we find out that we can never have a case that $f(x_1) = f(x_2)$ for any $x_1$ and $x_2$ in this case.

**Onto:** To prove that $f(x)$ is onto, we have to prove that for every $y \in \mathbb{N}$, there is an $x \in \mathbb{Z}$ such that $f(x) = y$. We pick an arbitrary natural number $y$ and divide this into two cases.

*Case 1.* $y$ is an even natural number. Then $y = 2k$ for some natural number $k$ (this is the definition of an even number). Then $x = k$ is a positive integer that maps to $y$, that is, $f(x) = 2k = y$.

*Case 2.* $y$ is an odd natural number. Then $y = 2k + 1$ for some natural number $k$ (this is the definition of an odd number). Then $x = -k$ is a negative integer that maps to $y$, that is, $f(x) = (-2)(-k) + 1 = 2k + 1 = y$.

Since $f(x)$ is one-one and onto, it is a bijection. □

## 2 Proof by Induction

Even though we did not cover this in class, here is an example of a proof by induction.

**Theorem 2.** *A set of $n$ elements has $\frac{n(n-1)}{2}$ subsets of size 2.*

In other words, we want to prove that if we have $n$ elements, we can make $n(n-1)/2$ pairs using these elements. We prove this by induction on the size of the set.

*Proof. Base case.* For a set of size $n = 1$, we can make $n(n-1)/2 = 0$ pairs which proves the base case.

*Induction hypothesis.* Assume that for any set of size $n = k$, we can make $\frac{n(n-1)}{2} = \frac{k(k-1)}{2}$ pairs using its elements.

*Inductive step.* Consider a set of size $n = k + 1$. We need to show that we can make $\frac{n(n-1)}{2} = \frac{(k+1)k}{2}$ pairs using its elements using the hypothesis.

There are two ways of selecting pairs from $k+1$ elements: either we select all pairs from the first $k$ elements or we select one element from the first $k$ elements and pair it with the $(k+1)$th element. From the inductive hypothesis, we know that we can make $\frac{k(k-1)}{2}$ pairs out of the first $k$ elements. And there are only $k$ ways to pair one element from the first $k$ elements with the $(k+1)$th element. Thus overall, we can make $\frac{k(k-1)}{2} + k = \frac{k(k+1)}{2}$ pairs from the $k+1$ elements which concludes the proof. □ □

## 3 Proof by Contradiction: Cantor's Diagonalization

**Theorem 3.** *The power set $\mathcal{P}(\mathbb{N})$ of natural numbers $\mathbb{N}$ is not countable.*

*Proof.* When you have to prove a negative statement, such as this or in general prove that a statement $X$ is false, it may be helpful to think about proof by contradiction first. In proof by contradiction, you start by assuming that the statement $X$ is true and find an absurdity or a "contradiction", which is a conclusion that violates one of your primary assumptions.

Here, let us assume that the power set $\mathcal{P}(\mathbb{N})$ is countable. If $\mathcal{P}(\mathbb{N})$ is countable, then by definition, there must exists a function $f : \mathcal{P}(\mathbb{N}) \rightarrow \mathbb{N}$ that is a bijection. This means that each subset $S \in \mathcal{P}(\mathbb{N})$ can be mapped to a natural number $j \in \mathbb{N}$, that is, $f(S) = j$ or in other words, this means that the subsets of $\mathbb{N}$ can be enumerated as a list $(S_{f(S)})_{S \in \mathcal{P}(\mathbb{N})} = S_1, S_2, S_3, \ldots$, so that every subset is $S_j$ for some $j \in \mathbb{N}$.

Consider the set $D = \{i \in \mathbb{N} \mid i \in S_i\}$. This set can be pictorially represented as the diagonal (blue cells) in the following table where a "Y" in a cell $(S_i, j)$ means that element $j$ is included in set $S_i$ and a "N" in that call means that element $j$ is not included in set $S_i$.

| $S_i$ \ $j$ | 1 | 2 | 3 | 4 | 5 | ... |
|---|---|---|---|---|---|---|
| $S_1$ | Y | N | N | Y | N | ... |
| $S_2$ | N | N | Y | N | N | ... |
| $S_3$ | Y | N | Y | N | Y | ... |
| $S_4$ | N | N | N | N | N | ... |
| $S_5$ | N | N | Y | Y | Y | ... |
| ... | ... | ... | ... | ... | ... | ... |
| $S_k$ | N | Y | N | N | N | ... |

Let set $\bar{D} = \mathbb{N} - D = \{i \in \mathbb{N} \mid i \notin S_i\}$. This set is essentially formed by flipping the Ys and Ns in the diagonal. This set $\bar{D}$ is a subset of $\mathbb{N}$ so it must be equal to a set $S_k = \bar{D}$ for some natural number $k$. But this leads to the following contradictory statements.

1. If $k \notin \bar{D}$, then $k \in D$ and thus $k \in S_k = \bar{D}$.
2. If $k \in \bar{D}$, then $k \notin D$, thus $k \notin S_k = \bar{D}$.

Thus, we have our contradiction as $k$ can either be in set $\bar{D}$ or not in set $\bar{D}$. Thus, our assumption that $\mathcal{P}(\mathbb{N})$ is countable is false, that is, $\mathcal{P}(\mathbb{N})$ is not countable.

□

This contradiction technique is called **diagonalization** and we will see more examples of it when we study undecidability.