Proving statements

and some examples around us

Sukrit Gupta and Nitin Auluck

January 23, 2024

Outline

Acknowledgement and disclaimer

All mistakes (if any) are mine.
I have used several other sources which I have referred to in the appropriate places.

Section 1

Conditional statements around us

A recent debate

October 12, 2021: Hon'ble Prime Minister of India Mr. Narendra Modi interlinked the idea of human rights and duties. "Human rights should not be only about rights, but also duties," said the prime minister. "The two should be discussed together, not separately. Other than awareness of their rights, each individual must abide by their duties." [1]

In 1925, Mohandas Karamchand Gandhi said, "The true source of rights is duty. If we all discharge our duties, rights will not be far to seek." In his book Hind Swaraj, he wrote, "Real rights are a result of performance of duty ..."

[1] Source: The Print

Somewhat unjust (over)simplification

Propositions A and B: A: you perform your fundamental duties; B: you can exercise your fundamental rights.

If A, then B

If you perform your fundamental duties, then you can exercise your fundamental rights.

Section 2

Visualizing conditional statements

Conditional statements

- A proposition B is implicated by a proposition A when the following relationship holds: $A \rightarrow B$
- This states that, "if A, then B", or, "if Socrates is a man, then Socrates is human".
- In a conditional such as this, A is the antecedent, and B is the consequent. So we can interpret "all of A is in B" as (venn diagram):

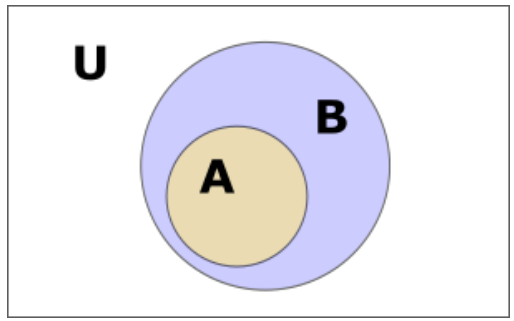

Figure: Venn Diagram for $A \rightarrow B$

Table: truth table for $A \rightarrow B$

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Let's go back to our conditional statement

If you perform your fundamental duties, then you can exercise your fundamental rights.

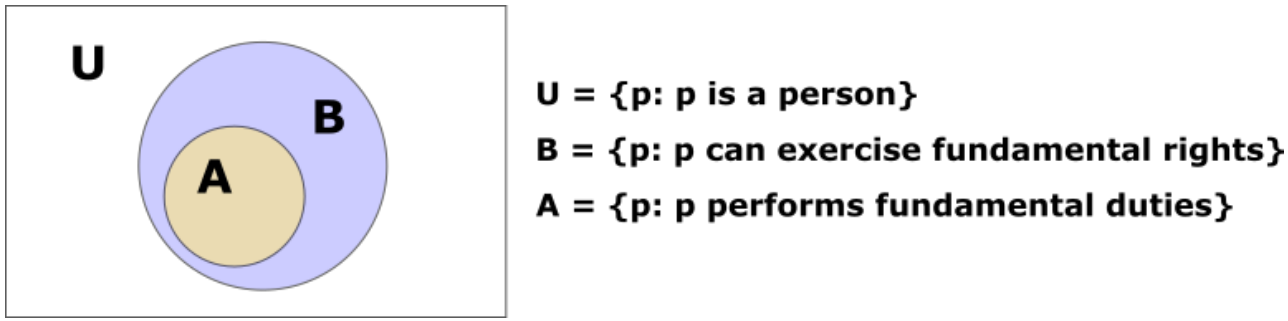

Figure: Venn Diagram for $A \rightarrow B$

It is important to understand the difference between:

1. If you perform your fundamental duties, then you can exercise your fundamental rights.
2. You can exercise your fundamental rights only if you perform your fundamental duties.

Let's see

Statement 2: If you are exercising your fundamental rights, then you have performed your fundamental duties.

Statement 2 means that if you're exercising your fundamental rights, then it is imperative that you must have performed your fundamental duties.

B: You're exercising your fundamental rights
A: You perform your fundamental duties
$B \rightarrow A$

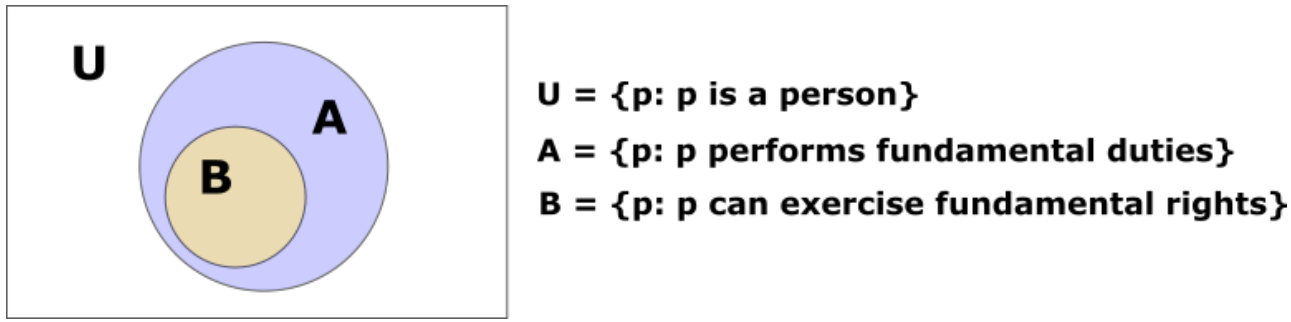

Figure: Venn Diagram for $B \rightarrow A$

Section 3

Contraposition and its implications

Contraposition

Contraposition refers to the inference of going from a conditional statement into its logically equivalent contrapositive, and an associated proof method known as proof by contraposition.

Conditional Statement: $A \rightarrow B$
The contrapositive of $A \rightarrow B$ is $\neg B \rightarrow \neg A$.
"If it is raining, then I wear my coat" $\Leftrightarrow$ "If I don't wear my coat, then it isn't raining."

Table: truth table

A	B	$A \rightarrow B$	$\neg B \rightarrow \neg A$
1	1	1	1
1	0	0	0
0	1	1	1
0	0	1	1

Contraposition

Let's look at the Venn diagram again:

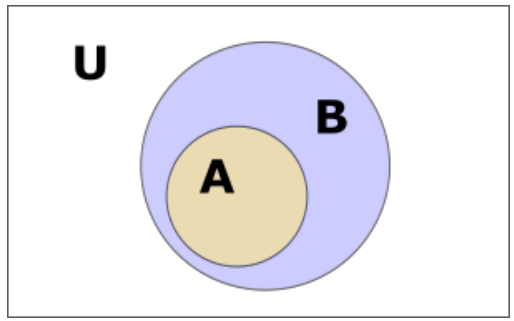

Figure: Venn Diagram for $A \rightarrow B$

Anything that is not within B cannot be within A, either. This can be expressed as:
$\neg B \rightarrow \neg A$
This is the contrapositive of the statement $A \rightarrow B$. Therefore, one can say that
$(A \rightarrow B) \Leftrightarrow (\neg B \rightarrow \neg A)$

Implications of contraposition on our little example

Statement 1: If you perform your fundamental duties, then you can exercise your fundamental rights.

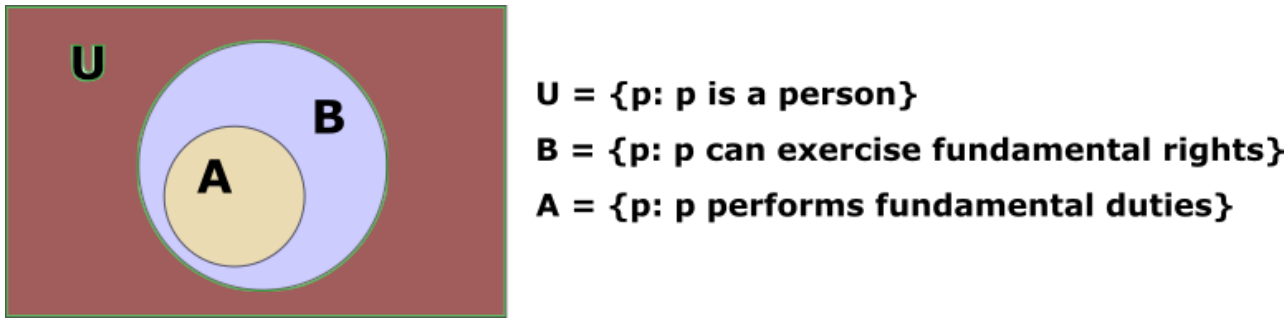

Figure: Venn Diagram for $\neg B \rightarrow \neg A$

So:

- Contrapositive of Statement 1: If you cannot exercise your fundamental rights, then *it is certain* that you have not performed your fundamental duties $\neg B \rightarrow \neg A$.
- If you have not performed fundamental duties $\neg A = 1$, you still can exercise your rights $(\neg B = 0, 0 \rightarrow 1 = 1)$.

Implications of contraposition on our little example

Statement 2: If you are exercising your fundamental rights, then you have performed your fundamental duties.

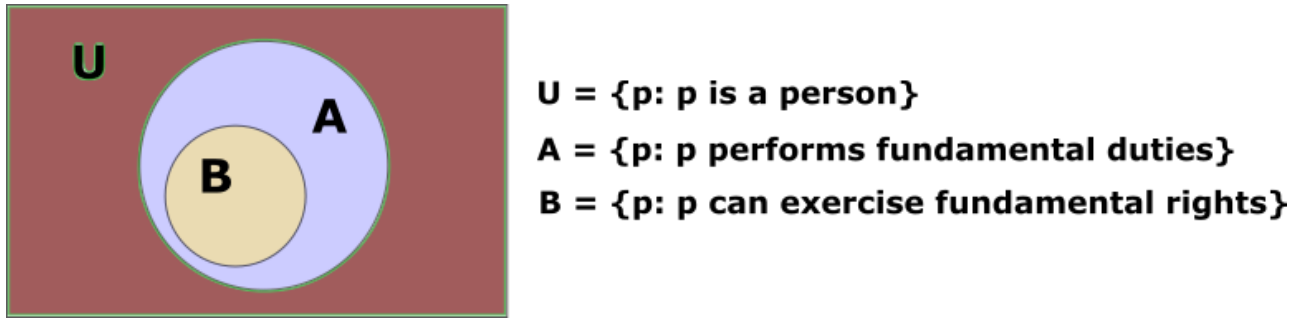

Figure: Venn Diagram for $\neg A \rightarrow \neg B$

So:

- Contrapositive of Statement 2: *If you did not perform your fundamental duties, then you cannot exercise your fundamental rights* $(\neg A \rightarrow \neg B)$.
- *Even if you have performed fundamental duties* $(\neg A = 0)$*, there is a chance that you may not be able to exercise your rights* $(\neg B = 1, 0 \rightarrow 1 = 1)$.
- Woah!

Section 4

Proofs

Direct Proof

- Often all that is required to prove something is a systematic explanation of what everything means. Direct proofs are especially useful when proving implications.
- The general format to prove $P \rightarrow Q$ is this:
  Assume P. Explain, explain, ... , explain. Therefore Q.
- Often we want to prove universal statements, perhaps of the form $\forall x(P(x) \rightarrow Q(x))$. We assume $P(x)$ is true and deduce $Q(x)$.
- But what about the x? We want this to work for all x. We accomplish this by fixing x to be an arbitrary element (of the sort we are interested in).

Example

Prove that $\forall n \in \mathbb{Z}$ if n is even, then n^2 is even

- If n is even, it can be represented in the form: $n = 2k$.
- If $n = 2k$, then $n^2 = 4k^2$.
- $n^2 = 2 \cdot (2k^2)$.
- $n^2 = 2k_2$.
- n^2 is also even.

Example

Prove that $\forall a, b, c \in \mathbb{Z}$ if a is divisible by b and b is divisible by c then a is divisible by c.

- If a is divisible by b, then $a = k_1 b$.
- If b is divisible by c, then $b = k_2 c$.
- If $a = k_1 b$ and $b = k_2 c$, then $a = k_1 k_2 c$.
- If $a = k_1 k_2 c$, then $a = k_3 c$.
- If $a = k_3 c$, then a is divisible by c.

Example

Prove that $\forall n \in \mathbb{Z}$, if n^2 is even, then n is even

- Let us add n^2 to n.
- $n^2 + n = n(n+1)$.
- $n(n+1)$ is always even. Given that n^2 is even.
- n is even.

Proof by Contraposition

- Recall that $(A \rightarrow B) \Leftrightarrow (\neg B \rightarrow \neg A)$.
- Sometimes there are statements that are hard to prove directly, but whose contrapositive can easily be proven directly.
- That's all. You do a direct proof of the contrapositive of the implication.
- Assume $\neg Q$. Explain, explain, ..., explain. Therefore $\neg P$.

Coming back to one of our questions ...

$\forall n \in \mathbb{Z}$: if n^2 is even, then n is even.

- What is the contrapositive of this statement?
- $\forall n \in \mathbb{Z}$: if n is odd, then n^2 is odd.
- Now prove the contrapositive.

Example: $\forall n \in \mathbb{P}$: if $n \neq 2$, then n is odd.

- $\mathbb{P}$ is the set of prime numbers.
- Contrapositive?
- $\forall n \in \mathbb{P}$: if n is even, then $n = 2$.

Proof by Contradiction

- Not all statements can be phrased as implications (the form $A \rightarrow B$).
- This is where we do a proof by contradiction.
- Let's see an example.

Example

Prove that there are no integers x and y such that $x^2 = 4y + 2$.

Process for a proof by contradiction

- The proposition to be proved, P, is assumed to be false. That is, $\neg P$ is true.
- Proceed as you would with a direct proof.
- It is then shown that $\neg P$ implies two mutually contradictory assertions, Q and $\neg Q$.
- Since Q and $\neg Q$ cannot both be true, the assumption that P is false must be wrong, so P must be true.

Coming back to the example

Prove that there are no integers x and y such that $x^2 = 4y + 2$.

- Let us assume that $x, y \in \mathbb{Z}$ exist.
- $x^2 = 2(2y + 1)$
- $2(2y + 1)$ is even. Then x^2 is even.
- Then x is even and of the form $x = 2k$.
- $4k^2 = 2(2y + 1) \rightarrow 2k^2 = 2y + 1$.
- $2y + 1$ is odd but $2k^2$ is even.
- Thus, the initial assumption is incorrect.

Example

Show that for any right triangle, the length of the hypotenuse is less than the sum of the lengths of the two remaining sides.

Show that $h < a + b$.

- Assume: $h \geq a + b$.
- $\rightarrow h^2 \geq (a + b)^2$.
- $\rightarrow h^2 \geq a^2 + b^2 + 2ab$.
- But $h^2 = a^2 + b^2$.
- $\rightarrow h^2 \geq h^2 + 2ab$.
- Since a and b cannot be zero, even the equality cannot hold.
- Thus, our assumption is false.

Example

Show that $\sqrt{2}$ is an irrational number.

- Assume: $\sqrt{2}$ is a rational number. Thus $\sqrt{2} = \frac{a}{b}$ such that a and b are co-prime.
- $2 = \frac{a^2}{b^2}$.
- $a^2 = 2b^2$.
- $2b^2$ is even. a^2 is even.
- a is even. So $a = 2k$.
- $2b^2 = 4k^2 \rightarrow b^2 = 2k^2$, b is also even.
- a and b are both even. So they are not co-prime.
- Wrong assumption.

Section 5

A famous proof in Computer Science

The Halting Problem: Background

- What does halting mean?
- Basically halting means terminating or stopping.
- Given a certain input I_0, will a program P_0:
  - accept it and halt after processing it;
  - reject it and halt; or
  - accept it and go into an infinite loop
- Now, with some effort you can compute whether some known program P_0 or P_1 or some arbitrary P_i will halt.
- But can you think of a *general* machine that can do it for any arbitrary program?
- Problem statement: **Does a machine** that can take
  - **any** random program, P_k; and
  - some corresponding input, I_k as inputs
- and predict whether the program P_k will halt for the given input I_k **exist**?

The Halting Problem: Checking if a Solution Exists

- Does a machine that can take any random program, P_k, and some corresponding input, I_k, as inputs and predict whether the program P_k will halt for the given input I_k exist?
- Christopher Strachey outlined a proof by contradiction that *the halting problem is not solvable*. The proof proceeds as follows:
- Suppose that there exists a *computable* function `halts(P)` that returns `True` if the input arbitrary Program P halts (for some Input I, assumed to be abstracted here) and returns `False`, otherwise.
- A computable function is a mathematical function that can be calculated by an algorithm, i.e. it can be computed by a computer in a finite amount of time.

The Halting Problem: Checking if a Solution Exists

- Now consider the following wrapper around `halts`:

```
1  def Q():
2      if halts(Q):
3          loop_forever()
4      else:
5          return True
```

- Notice that `Q` is also a program. So it can also be taken as an input to the `halts` program.
- `halts(Q)` must either return `True` or `False`, because `halts` was assumed to be computable.
- However, if `halts(Q)` returns `True`, then `Q` will call `loop_forever` and never halt, which is a contradiction.
- Conversely, if `halts(Q)` returns `False`, then `Q` will halt, because it will return True. This is also a contradiction.

The Halting Problem: Checking if a Solution Exists

```
def Q():
    if halts(Q):
        loop_forever()
    else:
        return True
```

- Overall, `Q` does the opposite of what `halts(Q)` predicted for `Q`. So `halts` does not return a truth value that is consistent with whether `Q` halts.
- Therefore, the initial assumption that `halts` is a computable function must be `False`.
- Do you see how this was proved using proof by contradiction?

The Halting Problem: Implications

- The Halting Problem has an extensive scope and plays a crucial role in understanding the limitations of computation.
- It sets the boundary for what computers can and cannot solve and has substantial implications for multiple areas of study.
- Offers key insights into the fundamental paradox of computer systems: even with perfect knowledge of a system's state and rules, it's impossible to predict its future with certainty.
- The above directly impacts program verification, an essential part of software development. Software testing involves not just finding bugs but also verifying the program's correctness.
- Yet, the Halting Problem shows that it is theoretically impossible to guarantee that a program behaves as expected for all inputs or even confirm whether it will halt.

What did we learn today?

1. Conditional statements around us
2. Visualizing conditional statements
3. Contraposition and its implications
4. Proofs
5. A famous proof in Computer Science

Thank you!