Proofs by contradiction

For every proposition p, p is equivalent to the conditional proposition

$$true \to p,$$

whose contrapositive is

$$\neg p \to false.$$

X	Y	X → Y	˥Y	˥Y→X
T	T	T	F	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

A proof of p by contradiction means

1. assuming that p is false and
2. deriving a contradiction (i.e., deriving false statement).

Proofs by contradiction

Example of a proposition with proof by contradiction:

There is no smallest positive real number (SPRN).

Proof by contradiction:

- Suppose that x is SPRN.

- Then $x>0$ because it is given that *x* is positive.

- But if we take $0<\frac{1}{2}<1$, and multiply by *x* we obtain $0<\frac{1}{2}x<x$.

- $\frac{1}{2}x$ is smaller than x, so this is a contradiction to the assumption

- Hence, there is no SPRN

Claim. *Let L_1 and L_2 be subsets of $\{a, b\}^*$. Prove that if $L_1 \subseteq L_2$, then $L_1^* \subseteq L_2^*$.*

- We will prove this claim by contradiction.
- The claim says: if $L_1 \subseteq L_2$, then $L_1^* \subseteq L_2^*$, i.e., given the condition $L_1 \subseteq L_2$, we need to prove that all elements of L_1^* are also elements of L_2^*.
- A contradiction to it is when we assume that there exist something that contradicts the statement, and then we'll show that this is not true.
- Contradiction: let's assume that $\exists x \in L_1^*$ such that $x \notin L_2^*$.

This is what we will prove by induction, i.e., all three induction steps will be contradictions.

Claim. *Let L_1 and L_2 be subsets of $\{a, b\}^*$. Prove that if $L_1 \subseteq L_2$, then $L_1^* \subseteq L_2^*$.*

Proof sketch. Let's assume that $\exists x \in L_1^*$ such that $x \notin L_2^*$.

By definition of L_1^*, x is a concatenation of k strings

$$x_i \in L_1,\ 0 \leq i \leq k-1,\ \text{i.e.,}$$

$$x = x_0 x_1 \dots x_{k-1} \text{ or } x = \Lambda.$$

We prove the statement by induction on k, always showing the contradiction.

- Basis step:
  - $k = 0 \Rightarrow x = \Lambda$ - the claim is correct because $\Lambda \in L_2^*$ by the definition of $*$;
  - $k = 1 \Rightarrow x = x_0 \neq \Lambda$ then $x \in L_1 \Rightarrow x \in L_2 \Rightarrow x \in L_2^*$.

Claim. *Let L_1 and L_2 be subsets of $\{a, b\}^*$. Prove that if $L_1 \subseteq L_2$, then $L_1^* \subseteq L_2^*$.*

Proof sketch (cont).

- Hypothesis: The claim is correct for $k-1$ strings (i.e., the contradiction is wrong).
- Induction step:
  - $x = x_0 x_1 \cdots x_{k-2} x_{k-1}$ then $x = y x_{k-1}$, where y is a concatenation of $k-1$ strings,
  - By induction hypothesis $y \in L_2^*$.
  - However, $x_{k-1} \in L_1$ and since $L_1 \subseteq L_2$ then $x_{k-1} \in L_2$.
  - Then, $x \in L_2^*$ because $x = y x_{k-1}$, where $y \in L_2^*$ and $x_{k-1} \in L_2$.

$\square$

Claim. *Let L_1 and L_2 be subsets of $\{a, b\}^*$. Prove that*

$$L_1^* \cup L_2^* \subseteq (L_1 \cup L_2)^*.$$

Proof sketch.

$$\begin{aligned} L_1 \subseteq L_1 \cup L_2 \ \Rightarrow & \quad L_1^* \subseteq (L_1 \cup L_2)^* \\ L_2 \subseteq L_1 \cup L_2 \ \Rightarrow & \quad L_2^* \subseteq (L_1 \cup L_2)^* \\ \Rightarrow & \quad L_1^* \cup L_2^* \subseteq (L_1 \cup L_2)^*. \end{aligned}$$

Recursive definitions

- A recursive definition of a set begins with a *basis statement* that specifies one or more elements in the set. The *recursive part* of the definition involves one or more operations that can be applied to elements already known to be in the set, so as to produce new elements of the set.

Example: let $AnBn$ be the language over $\Sigma = \{a, b\}$ defined as $AnBn = \{a^n b^n \mid n \in \mathbb{N}\}$. Its recursive definition is

1. $\Lambda \in AnBn$
2. For every $x \in AnBn$, $axb \in AnBn$.

Example: recursive definition of PAL over $\Sigma = \{a, b\}$

1. $\Lambda, a, b \in PAL$
2. For every $x \in PAL$, $axa \in PAL$ and $bxb \in PAL$.

Recursive definitions of functions

Example 1: factorial function $n! = n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 1$

$$f(0) = 1; \text{ for every } n \in \mathbb{N}, \; f(n+1) = (n+1) \cdot f(n)$$

Different notation

$$f(n) = \begin{cases} 1 & n = 0 \\ nf(n-1) & \text{otherwise} \end{cases}$$

Example 2

The function $f(n) = 2n + 1$ for natural numbers n can be defined recursively

$$f(0) = 1; \text{ for every } n \in \mathbb{N}, \; f(n+1) = f(n) + 2$$