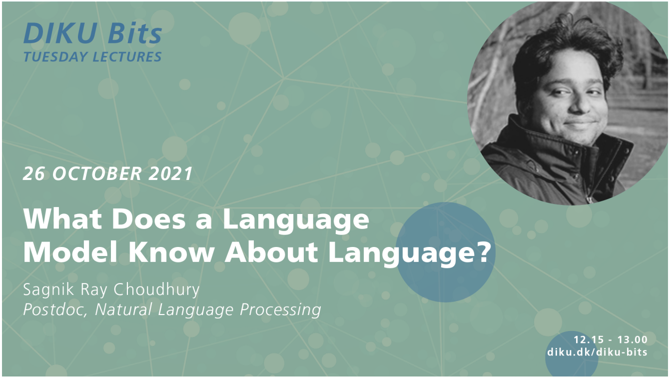
DMA: Proof Techniques

Laura Mančinska
Institut for Matematiske Fag

Organization



Reading: Before,Tuesday's lecture read up on the asymptotic notation in weekly notes and CLRS.

Proofs

KBR: “Construction of proofs is an art and must be learned in part from observation and experience.”

A proof is a series of statements, each of which follows logically from what has gone before.

- It starts with things we are assuming to be true.
- It ends with the thing we are trying to prove.

Task: Prove that for any $n \in \mathbb{Z}$, the number $n + (n + 2)$ is even.

Proof. Assume that $n \in \mathbb{Z}$.
Then $n + (n + 2) = 2n + 2 = 2(n + 1)$. By definition, a number is even, if it is an integer multiple of 2. Observe that $n + 1$ is an integer.
Therefore, $n + (n + 2)$ is even.

How to think up a proof

- Understand what is given (start) and what we need to prove (end)
    - Write down the relevant definitions.
- Try to manipulate both the beginning and the end to make them look like one another.
- Take big unjustified steps and work on justifying them afterwards.
- Try using one of the common *proof strategies*

Strategies for proving specific types of statements

- Proving an implication $p \Rightarrow q$
  - by a direct proof
  - by proving the contrapositive
- Proving a biconditional statement $p \Leftrightarrow q$
- Proof by contradiction

Proving an implication

$$p \Rightarrow q$$

Proving an implication: Direct proof

Task: Prove that $p \Rightarrow q$.

Proof template

- Assume p holds.
- Use relevant definitions and previously proven statements to argue that q must hold.

Proving an implication: Direct proof (example)

Task: Prove that if $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.

By definition:

$x \in \mathbb{Z}$ is even if we can write it as $x = 2n$ for some $n \in \mathbb{Z}$.
$x \in \mathbb{Z}$ is odd if we can write it as $x = 2n + 1$ for some $n \in \mathbb{Z}$.

Proof. Assume that x and y are odd integers.
So we can write them as $x = 2n + 1$ and $y = 2m + 1$ for some $n, m \in \mathbb{Z}$.
Then $x + y = (2n + 1) + (2m + 1) = 2(n + m + 1)$.
Hence, $x + y$ is even. $\square$

Proving an implication: via contrapositive

Task: Prove that $p \Rightarrow q$.

Recall: $(p \Rightarrow q) \equiv ((\sim q) \Rightarrow (\sim p))$

If it rains, then I take my umbrella $\equiv$ If I don't take my umbrella then it is not raining.

Proof template

- Write: "We prove the contrapositive:" and then state the contrapositive.
- Prove the contrapositive, $(\sim q) \Rightarrow (\sim p)$, by a direct proof:
  - Assume $\sim q$ holds.
  - Use relevant definitions and previously proven statements to argue that $\sim p$ must hold.

Proving an implication: via contrapositive (example)

Task: Let $a, b, n \in \mathbb{Z}$. Prove that if $n \nmid (ab)$, then $n \nmid a$ and $n \nmid b$.

By definition: $d \mid k$ if $k = cd$ for some $c \in \mathbb{Z}$.

Implication: $n \nmid (ab) \;\Rightarrow\; (n \nmid a \text{ and } n \nmid b)$
Contrapositive: $(n \mid a \text{ or } n \mid b) \;\Rightarrow\; n \mid (ab)$

Proof. We prove the contrapositive: If $n \mid a$ or $n \mid b$, then $n \mid (ab)$.
Assume that $n \mid a$ or $n \mid b$. Let us analyze the cases when $n \mid a$ and when $n \mid b$ separately.

(finish on the board)

Proving a biconditional

$$p \Leftrightarrow q$$

Proving a biconditional

Task: Prove that $p \Leftrightarrow q$.

Recall: $(p \Leftrightarrow q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Proof template

- Write: "We prove p implies q and vice versa".
- Write: "First we show $p \Rightarrow q$": prove the implication.
- Write: "Now we show $q \Rightarrow p$": prove the implication.

Note: A different proof technique can be used for each implication.

Proving a biconditional (example)

Task: Let $a \in \mathbb{Z}$. Prove that a is even if and only if a^2 is even.

By definition:

$b \in \mathbb{Z}$ is even if $b = 2k$ for some $k \in \mathbb{Z}$.

$b \in \mathbb{Z}$ is odd if $b = 2k + 1$ for some $k \in \mathbb{Z}$.

Proof. We prove that if a is even then a^2 is even and vice versa.

We first show that if a is even then a^2 is even.

Assume that a is even. Then $a = 2k$ for some $k \in \mathbb{Z}$. Hence, $a^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which shows that a^2 is even.

(other direction on the board)

Proof by contradiction

Proof by contradiction

Task: Prove that q holds.

Note: $q \equiv (\sim q \Rightarrow \underbrace{(p \wedge (\sim p))}_{\text{absurdity}})$ (check!)

Proof template

- Write: "We use proof by contradiction."
- Assume $\sim q$ holds.
- Deduce something known to be false (a contradiction).
- Write: "We have reached a contradiction. Hence, q holds."

Proof by contradiction (example)

Task: Prove that $\sqrt{2}$ is an irrational number.

Definitions:

- $\sqrt{2}$ is a number such that $(\sqrt{2})^2 = 2$.
- We say that $x \in \mathbb{R}$ is rational if we can express it as $\frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Otherwise, we say that x is irrational.

Proof. We use proof by contradiction.
Assume that $\sqrt{2}$ is rational. So by definition, this means that $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$.

(finish on the board)