KTH ROYAL INSTITUTE
OF TECHNOLOGY

Review
Proof Writing and Structure

Lars Kroll ⟨lkroll@kth.se⟩

Overview

Introduction

- What is a proof?

Direct Proof

- Propositions without a Hypothesis
- Propositions with one or more Hypotheses
- The tactic of “division into cases”

Indirect Proof

- Proof by Contrapositive
- Proof by Contradiction
- Conclusions with Alternatives

Other Methods

- Evaluating the Truth of a Proposition
- Proof by Mathematical Induction
- Proof by Structural Induction

Introduction

What is a proof?

A proof is sufficient evidence or a sufficient argument for the truth of a proposition.

- The purpose of a proof is to *convince* an audience of the veracity of a proposition.
- Proofs are most common in philosophy, law, and mathematics (and related disciplines).
- We only consider mathematical proofs here.
- Mathematical propositions are usually expressed in (mostly first-order) logic and some natural language.

Introduction

What is a proof?

- Most proofs done by humans (not machines) assume a particular context from their audience.
- For example: $\forall_x x = x$ assumes that you know what $=$ means in this context and that it's defined for whatever x is.
- Context is typically a particular theory (e.g., set theory), its definitions, axioms, and previously proven theorems.
- Notation can also be considered context sometimes, though it's good to be explicit if possible.

Introduction

Types of proofs

P: For every x, if $H(x)$, then $C(x)$
P: $\forall_x \; H(x) \Rightarrow C(x)$

- This is the most common structure for a mathematical proposition P.
- H is the *hypothesis*
- C is the *conclusion*
- If we prove P as it's written, we call that *direct proof*.
- Sometimes we prove a logically equivalent statement instead. That is called an *indirect proof*.
- Sometimes propositions must be shown recursively, which is called *induction*.

Direct Proof

Propositions without a Hypothesis

General Structure: $\forall_x\ C(x)$
Example: For all sets A and B, $A \subseteq A \cup B$.

- Setup: Let A, B be sets.
- Rewrite the conclusion (using the definition of $\subseteq$): $\forall_{x \in A}\ x \in (A \cup B)$
- Rewrite again (using the definition of $\cup$): $\forall_{x \in A}\ x \in A \vee x \in B$. $\square$

Let A, B *be sets. Let* $a \in A$. *It follows trivially that* $a \in A \vee a \in B$, *which is equivalent to* $a \in A \cup B$. $\square$

Direct Proof

Propositions with one or more Hypotheses

General Structure: $\forall_x H(x) \Rightarrow C(x)$
Example: For all sets X, Y, Z*, if* $X \subseteq Y$*,*
then $X \cap Z \subseteq Y \cap Z$*.*

- Setup: Let X, Y, Z be sets.
- Use H as an assumption:
  Let X, Y be such that $X \subseteq Y$.
- Rewrite the hypothesis (using the definition of $\subseteq$):
  $\forall_{x \in X}\ x \in Y$
- Rewrite the conclusion (using the definition of $\subseteq$):
  $\forall_{z \in X \cap Z}\ z \in Y \cap Z$

Direct Proof

Propositions with one or more Hypotheses

For all sets X, Y, Z, if $X \subseteq Y$, then $X \cap Z \subseteq Y \cap Z$.

- Setup: Let X, Y, Z be sets, such that $X \subseteq Y$.
- Definition of $\subseteq$ on the hypothesis:
  $\forall_{x \in X}\ x \in Y$
- Definition of $\subseteq$ on the conclusion:
  $\forall_{x \in X \cap Z}\ x \in Y \cap Z$
- If $x \in X \cap Z$ the definition of $\cap$ implies $x \in X \wedge x \in Z$.
- Since $x \in Y$ (assumption), the definition of $\cap$ also implies $x \in Y \cap Z$. $\square$

Direct Proof

The tactic of "division into cases"

Example[1] *: For all sets A and B,*
$(A \cap B) \cup (A \cap \bar{B}) \subseteq A$.

[1] $\bar{B}$ is the set of all items not in B (but in some universal set U with $B \subseteq U$)

Direct Proof

The tactic of "division into cases"

Example: For all sets A and B, $(A \cap B) \cup (A \cap \bar{B}) \subseteq A$.

- Setup: Let A, B be sets.
- Rewrite conclusion (definition of $\subseteq$): $\forall_x \; x \in (A \cap B) \cup (A \cap \bar{B}) \Rightarrow x \in A$
- Let $x \in (A \cap B) \cup (A \cap \bar{B})$, rewrite with definition of $\cup$: $x \in (A \cap B) \vee x \in (A \cap \bar{B})$
- Show that it holds for either side of the $\vee$:
  - **Case 1** : Assume $x \in (A \cap B)$, then, by definition of $\cap$, $x \in A$
  - **Case 2** : Assume $x \in (A \cap \bar{B})$, then, by definition of $\cap$, $x \in A$ $\square$

Indirect Proof

- Sometimes a direct proof approach is difficult or impossible.
- It might be easier to prove a logically equivalent proposition instead.
- We can use one (or more) of the following logical equivalences (for any logical formulae p, q, r):

$$\neg q \to \neg p \iff p \to q \tag{1}$$

$$\neg p \to (q \wedge \neg q) \iff p \tag{2}$$

$$(p \wedge \neg q) \to r \iff p \to (q \vee r) \tag{3}$$

Indirect Proof

Proof by Contrapositive

Example: For every function $f : A \to B$ with $A, B \subseteq \mathbb{R}$, if f is strictly increasing, then f is injective (one-to-one).

- Setup: Let f be as above, and strictly increasing (i.e. $\forall_{x_1, x_2 \in A}\ x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$).
- Direct approach: Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. We'd need to to show that $x_1 = x_2$.
- Now we are stuck, because we can't use our "strictly increasing" assumption on $f(x_1), f(x_2)$.

Indirect Proof

Proof by Contrapositive

Example: For every function $f : A \to B$ with $A, B \subseteq \mathbb{R}$, if f is strictly increasing, then f is injective (one-to-one).

- Setup: Let f be as above, and strictly increasing.
- Indirect approach (assume the contrapositive (1)):
  Let $x_1 \neq x_2 \in A$
  Now we need to to show that $f(x_1) \neq f(x_2)$.
- Since $(\mathbb{R}, <)$ is a *strict total order*, it must be that $x_1 < x_2 \vee x_2 < x_1$.
- Assume (WLOG) $x_1 < x_2$, then, since f is strictly increasing, $f(x_1) < f(x_2)$ and thus $f(x_1) \neq f(x_2)$. $\square$

Indirect Proof

Proof by Contradiction

Example: For all sets A and B, if $A \subseteq B$, then $A \cap \bar{B} = \emptyset$.

- Setup: Let A, B be sets. Assume $A \subseteq B$.
- Direct approach – show mutual inclusion: $A \cap \bar{B} \subseteq \emptyset \wedge \emptyset \subseteq A \cap \bar{B}$
- $\emptyset \subseteq A \cap \bar{B}$ is trivially true.
- But how would we show $A \cap \bar{B} \subseteq \emptyset$? $x \in \emptyset$ is not an assumption we can make.
- Stuck again...

Indirect Proof

Proof by Contradiction

Example: For all sets A and B, if $A \subseteq B$, then $A \cap \bar{B} = \emptyset$.

- Setup: Let A, B be sets. Assume $A \subseteq B$.
- Indirect approach: Assume $A \cap \bar{B} \neq \emptyset$.
  Try to show that $A \cap \bar{B} \neq \emptyset$ leads to a contradiction (2) with $A \subseteq B$.
- Let $x \in A \cap \bar{B}$. Then $x \in A \wedge x \in \bar{B}$.
- By our hypothesis $x \in A$ implies $x \in B$.
- Thus $x \in B \wedge x \in \bar{B}$ ↯ $\square$

Indirect Proof

Conclusions with Alternatives

General Structure: $\forall_x H(x) \Rightarrow C_1(x) \vee C_2(x)$
Example: $\forall_{x,y\in\mathbb{R}}\ x \cdot y = 0 \Rightarrow x = 0 \vee y = 0.$

- Setup: Let $x, y \in \mathbb{R}$. Assume $x \cdot y = 0$.
- Direct Approach: Well...which of the two cases should we try to prove now?
- We are stuck...

Indirect Proof

Conclusions with Alternatives

General Structure: $\forall_x H(x) \Rightarrow C_1(x) \vee C_2(x)$
Example: $\forall_{x,y\in\mathbb{R}}\ x \cdot y = 0 \Rightarrow x = 0 \vee y = 0.$

- Setup: Let $x, y \in \mathbb{R}$. Assume $x \cdot y = 0$.
- Indirect Approach: Assume $x \neq 0$.
  Now try to show $y = 0$ and use (3).
- Since $x \neq 0$, the inverse $\frac{1}{x}$ must exist. Thus...

$$\begin{aligned} x \cdot y = 0 &\iff \frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0 \\ &\iff y = 0 \end{aligned}$$

$\square$

Other Methods

Evaluating the Truth of a Proposition

General Structure: For P of the form $\forall_x H(x) \Rightarrow C(x)$, is P true or false?

- Can try a direct or indirect proof of P.
  - If we succeed P is true.
  - If we fail, does that mean P is false? ...
- To disprove P we need to find a counter-example.
- That is a single instance of $\neg P$.

Other Methods

Evaluating the Truth of a Proposition

Example: For all sets X, Y, Z, if $X \cap Z \subseteq Y \cap Z$, then $X \subseteq Y$.

- Setup: Let X, Y, Z be sets.
- Negation of the proposition: There exist sets X, Y, Z such that, $X \cap Z \subseteq Y \cap Z$ and $\exists_{x \in X}\ x \notin Y$.
- Assume $X \cap Z \subseteq Y \cap Z$, and let $x \in X$.
- We'd need to know $x \in Z$ to use the assumption to make progress.
- Now the proof is stuck, but we got a hint of how to construct a counter-example: $x \notin X \cap Z$.

Other Methods

Evaluating the Truth of a Proposition

Counter-Example: There exist sets X, Y, Z such that, $X \cap Z \subseteq Y \cap Z$ and $\exists_{x \in X}\ x \notin Y$.

- Setup: Let $X = \{1, 4\}$, $Y = \{2, 4\}, Z = \{3, 4\}$.
- Then $X \cap Z = \{4\} = Y \cap Z$. ($=$ is a special case of $\subseteq$.)
- But $1 \in X$, yet $1 \notin Y$ $\square$

Other Methods

Proof by Mathematical Induction

General Structure: $\forall_{n\in\mathbb{N}} P(n)$
Example: $\forall_{n\in\mathbb{N}} \; \sum_{k=1}^{n} k = \frac{n\cdot(n+1)}{2}$

- Setup: Let $n \in \mathbb{N}$.
- Base case: Let $n = 1$, then $\sum_{k=1}^{1} k = 1 = \frac{1\cdot(1+1)}{2}$
- Induction Hypothesis: Assume that $\sum_{k=1}^{n} k = \frac{n\cdot(n+1)}{2}$.
- Try to show that:

$$\sum_{k=1}^{n+1} k = \frac{(n+1)\cdot(n+1+1)}{2}$$

Other Methods

Proof by Mathematical Induction

- Try to show that: $\sum_{k=1}^{n+1} k = \frac{(n+1)\cdot(n+2)}{2}$

$$
\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + n + 1 \\
&= \frac{n \cdot (n+1)}{2} + n + 1 && \text{by induction hypothesis} \\
&= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} \\
&= \frac{(n+1) \cdot (n+2)}{2} && \square
\end{aligned}
$$

Other Methods

Proof by Structural Induction

Example: For all lists L_1, L_2 over some set E,
$\mathtt{length}(L_1 +\!+ L_2) = \mathtt{length}(L_1) + \mathtt{length}(L_2)$

Definitions:
A *list* L over an element set E is either empty [] or of the form $h :: T$, where $h \in E$ and T is a list over E.

$$\mathtt{length}([]) = 0 \tag{4}$$
$$\mathtt{length}(h :: T) = 1 + \mathtt{length}(T) \tag{5}$$
$$[] +\!+ L = L \tag{6}$$
$$(h :: T) +\!+ L = h :: (T +\!+ L) \tag{7}$$

Other Methods

Proof by Structural Induction

Example: For all lists L_1, L_2 over some set E,
$\mathsf{length}(L_1 \mathbin{++} L_2) = \mathsf{length}(L_1) + \mathsf{length}(L_2)$

- Setup: Let L_1, L_2 be lists over E.
- Case []: Assume $L_1 = []$. Then

$$
\begin{aligned}
\mathsf{length}(L_1 \mathbin{++} L_2) &= \mathsf{length}([] \mathbin{++} L_2) \\
&= \mathsf{length}(L_2) && \text{by (6)} \\
&= 0 + \mathsf{length}(L_2) \\
&= \mathsf{length}([]) + \mathsf{length}(L_2) && \text{by (4)} \\
&= \mathsf{length}(L_1) + \mathsf{length}(L_2)
\end{aligned}
$$

Other Methods

Proof by Structural Induction

Example: For all lists L_1, L_2 over some set E,
$\text{length}(L_1 +\!\!+ L_2) = \text{length}(L_1) + \text{length}(L_2)$

- Induction Hypothesis (IH): Let T be a list and assume $\text{length}(T +\!\!+ L_2) = \text{length}(T) + \text{length}(L_2)$.
- Case $h :: T$: Assume $L_1 = h :: T \neq []$ for some $h \in E$.

$$
\begin{aligned}
\text{length}(L_1 +\!\!+ L_2) &= \text{length}((h :: T) +\!\!+ L_2) \\
&= \text{length}(h :: (T +\!\!+ L_2)) && \text{by (7)} \\
&= 1 + \text{length}(T +\!\!+ L_2) && \text{by (5)} \\
&= 1 + \text{length}(T) + \text{length}(L_2) && \text{by (IH)} \\
&= \text{length}(h :: T) + \text{length}(L_2) && \text{by (5)} \quad \square
\end{aligned}
$$

References

Loosely based on
A Guide to Proof-Writing
by *Ron Morash, University of Michigan–Dearborn*.