Proofs

A proof is a formal demonstration that a statement is true in a certain context (called premises)

The demonstration is syntactic and can be mechanically verified.

A proof consists of a sequence of formlas with the premises occurring first.

Each subsequent line must be a valid <u>inference</u> from preceding formulas.

A valid inference is justified by an <u>inference</u> <u>rule</u>. The set of inference rules define a <u>proof system</u>.

The final formula is the <u>conclusion</u>.

Notation

"There is a proof with premises Γ and conclusion φ"

$$\Gamma \vdash \varphi$$

turnstyle

A proof system defines

$\vdash$

Natural Deduction Proof System

- provides a direct proof starting from premises a leads to a conclusion
- allows for indirect proofs starting from assumptions (wffs without a justification)
- let's first look at some notation

Inference rule notation:

$$\frac{\alpha_1 \ \alpha_2 \ \cdots \ \alpha_n}{\beta}$$

← these appear previously in proof

← this can be inferred (written as next line in proof

Proof notation:

	justification
1. formula	Premise
2. formula	Premise
3. formula β	Inference rule used: lines used for $\alpha_1 \dots \alpha_n$
$\vdots$	Inference rule used: lines used for $\alpha_1 \dots \alpha_n$
n-1. formula β	Inference rule used: lines used for $\alpha_1 \dots \alpha_n$
n. formula β	Inference rule used:

conclusion

Initial inference rule

Reflexivity : $\dfrac{\alpha}{\alpha}$ (basically, a formula already in the proof can be rewritten in the proof — important for subproofs)

Although this first example may suggest that inference is like equivalence, it is not. It is only in one direction.

Inference Rules

$$\frac{\alpha \quad \beta}{\alpha \wedge \beta} \qquad \wedge\text{-Introduction}$$

$$\frac{(\alpha \wedge \beta)}{\alpha} \qquad \wedge\text{-Elimination}$$

$$\frac{\alpha}{\alpha \vee \beta} \qquad \vee\text{-Introduction}$$

$$\frac{(\alpha \vee \beta) \quad \neg\alpha}{\beta} \qquad \vee\text{-Elimination}$$

(continued)

$$\frac{(\alpha \to \beta) \quad \alpha}{\beta}$$

$\to$-Elimination (modus ponens)

$$\frac{\boxed{\begin{array}{l}\alpha \\ \vdots \\ \beta\end{array}}}{(\alpha \to \beta)}$$

$\to$-Introduction

$$\boxed{\begin{array}{l}\alpha \\ \vdots \\ \beta\end{array}}$$

This is the notation for a <u>subproof</u>.

α is an <u>assumption</u> (or <u>hypothesis</u>)

<u>Note</u>: No line inside a box can be used outside of that box.

(further continuation)

The box can be closed after any line in the subproof, so β can be any line.

α can be any wff

<u>Every</u> subproof must be closed.

Subproofs can include subproofs.

Logically equivalent formulas

- a logically equivalent formula can always be added to the proof

e.g. $(\alpha \wedge \beta) \equiv (\beta \wedge \alpha)$

Examples

$$\{p, q\} \vdash p$$

premise

conclusion

1. p Premise
2. q Premise
3. p Reflexivity: 1

Another example

$$\{(p \wedge q)\} \vdash (q \wedge p)$$

1. $(p \wedge q)$ Premise
2. $(q \wedge p)$ Equivalence

$$\{(p \wedge q), r\} \vdash (p \wedge r)$$

1. $(p \wedge q)$ Premise
2. r Premise
3. p $\wedge$-Elimination: 1
4. $(p \wedge r)$ $\wedge$-Introduction: 3,2

Alternative proofs

$\wedge$- Elimination : $\dfrac{\alpha \wedge \beta}{\alpha}$ or $\dfrac{\alpha \wedge \beta}{\beta}$

$\{(p \wedge q), r\} \vdash (q \wedge r)$

1.	$(p \wedge q)$	Premise
2.	r	Premise
3.	q	$\wedge$-Elimination : 1
4	$(q \wedge r)$	$\wedge$-Introduction : 3,2

1.	$(p \wedge q)$	Premise
2.	r	Premise
3.	$(q \wedge p)$	Equivalence : 1
4.	q	$\wedge$-Elimination : 3
5.	$(q \wedge r)$	$\wedge$-Introduction : 4,2

$\to$-Introduction Example

$$\{(p \to q), (q \to r)\} \vdash p \to r$$

1.	$(p \to q)$	Premise
2.	$(q \to r)$	Premise
3.	p	Assumption
4.	q	$\to$-Elimination: 1,3
5.	r	$\to$-Elimination: 2,4
6.	$(p \to r)$	$\to$-Introduction: 3–5

More Inference Rules

$$\frac{\alpha}{\alpha \vee \beta} \quad \vee\text{-Introduction} \qquad \left[\text{could add also}: \frac{\alpha}{\beta \vee \alpha}\right]$$

$$\frac{\alpha_1 \vee \alpha_2 \qquad \boxed{\begin{array}{c}\alpha_1 \\ \vdots \\ \beta\end{array}} \qquad \boxed{\begin{array}{c}\alpha_2 \\ \vdots \\ \beta\end{array}}}{\beta} \quad \vee\text{-Elimination} \quad \text{"proof by cases"}$$

Show: $\{(p \vee q)\} \vdash ((p \to q) \vee (q \to p))$

1.	$(p \vee q)$	Premise
2.	p	Assumption
3.	q	Assumption
4.	p	Reflexivity: 2
5.	$(q \to p)$	$\to$-Introduction: 3–4
6.	$((p \to q) \vee (q \to p))$	$\vee$-Introduction: 5
7.	q	Assumption
8.	p	Assumption
9.	q	Reflexivity: 7
10.	$(p \to q)$	$\to$-Introduction: 8–9
11.	$((p \to q) \vee (q \to p))$	$\vee$-Introduction: 10
12.	$((p \to q) \vee (q \to p)$	$\vee$-Elimination: 1, 2–6, 7–11

Proof by contradiction

$\Gamma \vdash \alpha$ $\qquad\qquad$ $\Gamma = \{\gamma_1, \dots, \gamma_n\}$

1.	γ_1	Premise
2.	γ_2	Premise
$\vdots$		$\vdots$
n.	γ_n	Premise
n+1.	$\boxed{\neg\alpha}$	Assumption
$\vdots$		
n+k.	$\bot$	justification
n+k+1.	$\neg\alpha \to \bot$	$\to$-Introduction : n+1 – n+k
n+k+2.	$\neg\bot \to \alpha$	Equivalence : n+k+1 (contrapositive)
n+k+3.	$\neg\neg\bot \vee \alpha$	Equivalence : n+k+2 ($\alpha \to \beta \equiv \neg\alpha \vee \beta$)
n+k+4.	$\bot \vee \alpha$	Equivalence : n+k+3 (double negation)
n+k+5.	α	Equivalence : n+k+4 (absorption)

subproof that leads to $\bot$ after assuming $\neg\alpha$

Deduction Theorem

If $\Gamma, \alpha \vdash \beta$ then $\Gamma \vdash (\alpha \to \beta)$

[We will accept this as true — would need structural induction to prove it.]

Converse of the Deduction Theorem

If $\Gamma \vdash (\alpha \to \beta)$ then $\Gamma, \alpha \vdash \beta$

1. α Premise
2. $\left.\begin{array}{l} \\ \\ \end{array}\right\}$ proof of $(\alpha \to \beta)$

⋮

n.

n+1. β $\to$-Elimination: 1, n

Soundness

If $\Gamma \vdash \alpha$ then $\Gamma \vDash \alpha$

Completeness

If $\Gamma \vDash \alpha$ then $\Gamma \vdash \alpha$

Natural deduction is sound and complete.

(Proof ...)