Logic and Formal Systems — Syllabus

- ★ Propositional logic (natural deduction, semantics, soundness and completeness).
- ★ Predicate logic (natural deduction, semantics, undecidability).
- ★ Logic programming and the language Prolog.
- ★ Temporal logics (LTL, CTL, CTL^*).
- ★ Model checking and the verifier SMV.
- ★ Program verification (Floyd-Hoare logic).
- ★ Modal logic and agents.
- ★ Binary decision diagrams

Motivation for studying Logic: To acquire the ability to model real-life situations in a way that would allow us to reason about them formally.

Example 1: If the train arrives late and there are no taxis at the station, then John is late for his meeting. John is not late for his meeting. The train did arrive late. ***Therefore***, there were taxis at the station.

Example 2: If it is raining and Jane does not have her umbrella with her, then she will get wet. Jane is not wet. It is raining. ***Therefore***, Jane has her umbrella with her.

Can we verify the validity of these arguments formally?

- We need to turn the English sentences into formulas (***modeling***).
- Then, we can apply mathematical reasoning to formulas

Encoding:

	Example 1	Example 2
p	the train is late	it is raining
q	there are taxis at the station	Jane has her umbrella with her
r	John is late for his meeting	Jane gets wet

Pattern:

If p and not q, then r. Not r. p. Therefore q.

We shall study ***reasoning patterns***.

Declarative Sentences

Declarative sentences (we can consider whether they're true or not):

- The sum of the numbers 3 and 5 equals 8.
- Jane reacted violently to Jack's accusations.
- Every even natural number is the sum of two prime numbers.
- All Martians like peperoni on their pizza.

Non-declarative sentences (can't tell whether they're true or not):

- Could you please pass the salt.
- Ready, steady, go.
- May fortune come your way.

We want to turn declarative sentences into formulas and create a formalism to manipulate such formulas.

Turning English Phrases into Formulas

Atomic sentences:

- p: I won the lottery last week.
- q: I purchased a lottery ticket.
- r: I won last week's sweepstakes.

Connectives:

- $\neg$: **negation** —$\neg p$: I did not win the lottery.
- $\vee$: **disjunction** —$p \vee r$: I won the lottery last week or I won the last week's sweepstakes.
- $\wedge$: **conjunction** —$p \wedge r$: I won the lottery and the sweepstakes last week.
- $\rightarrow$: **implication** —$p \rightarrow q$: If I won the lottery last week, then I purchased a lottery ticket.

Composite formulas: $(p \wedge q) \rightarrow ((\neg r) \vee q)$; connective priority, $\neg$, $\wedge$, $\vee$, $\rightarrow$. By this convention, we can remove the brackets: $p \wedge q \rightarrow \neg r \vee q$.

Natural Deduction

- Collection of ***proof rules***, which allow to infer new formulas from existing formulas.

- Given the formulas $\Phi_1, \ldots, \Phi_n$, we intend to infer a conclusion Ψ. We denote this by

$$\Phi_1, \ldots, \Phi_n \vdash \Psi$$

  This construct is called a ***sequent***.

- Example:

$$p \wedge \neg q \rightarrow r, \neg r, p \vdash q$$

- There is no "perfect" set of proof rules. You can create your own (you can even invent your own logic). Such exercise resembles computer programming.

Natural Deduction Rules — Conjunction

$$\frac{\Phi \quad \Psi}{\Phi \wedge \Psi} \; \wedge\mathrm{i}$$

and-introduction

$$\frac{\Phi \wedge \Psi}{\Phi} \; \wedge\mathrm{e1} \qquad \frac{\Phi \wedge \Psi}{\Psi} \; \wedge\mathrm{e2}$$

and-elimination

Example: Prove $p \wedge q, r \vdash q \wedge r$

1	$p \wedge q$	premise
2	r	premise
3	q	$\wedge$e2 1
4	$q \wedge r$	$\wedge$i 3,2

Alternate way to write the proof:

$$\dfrac{\dfrac{p \wedge q}{q}\ \wedge\mathrm{e2} \qquad r}{q \wedge r}\ \wedge\mathrm{i}$$

Natural Deduction Rules — Double Negation and Implication Elimination

$$\frac{\neg\neg\Phi}{\Phi}\ \neg\neg e$$

double negation elimination

$$\frac{\Phi}{\neg\neg\Phi}\ \neg\neg i$$

double negation introduction

$$\frac{\Phi \quad \Phi \to \Psi}{\Psi}\ \to e$$

implication elimination

Example: $p, \neg\neg(q \wedge r) \vdash \neg\neg p \wedge r$

1	p	premise
2	$\neg\neg(q \wedge r)$	premise
3	$\neg\neg p$	$\neg\neg$i 1
4	$q \wedge r$	$\neg\neg$e 2
5	r	$\wedge$e2 4
6	$\neg\neg q \wedge r$	$\wedge$i 3,5

Justification:

$$\frac{p\text{: It rained} \qquad p \to q\text{: If it rained, the street is wet}}{q\text{: The street is wet}}$$

Example: $p, p \to q, p \to (q \to r) \vdash r$

1	$p \to (q \to r)$	premise
2	$p \to q$	premise
3	p	premise
4	$q \to r$	$\to$e 1,3
5	q	$\to$e 2,3
6	r	$\to$e 4,5

Natural Deduction Rules — Implication Introduction

$$\frac{\boxed{\begin{array}{c}\Phi \\ \vdots \\ \Psi\end{array}}}{\Phi \to \Psi} \; \to \mathrm{i}$$

In order to prove $\Phi \to \Psi$, we make the temporary assumption of Φ, and then prove Ψ. The scope of the assumption is indicated by the box.

Example: $p \wedge q \to r \vdash p \to (q \to r)$

1	$p \wedge q \to r$	premise
2	p	assumption
3	q	assumption
4	$p \wedge q$	$\to$i 2,3
5	r	$\to$e 1,4
6	$q \to r$	$\to$i 3-5
7	$p \to (q \to r)$	$\to$i 2-6

Remark: We may transform any proof of

$$\Phi_1, \ldots, \Phi_n \vdash \Psi$$

into a proof of

$$\vdash \Phi_1 \to (\Phi_2 \to (\cdots (\Phi_n \to \Psi) \cdots))$$

Implication Introduction Examples

Example: $p \to (q \to r) \vdash p \wedge q \to r$

1	$p \to (q \to r)$	premise
2	$\boxed{p \wedge q}$	assumption
3	p	$\wedge$e1 2
4	q	$\wedge$e2 2
5	$q \to r$	$\to$e 1,3
6	r	$\to$e 4,5
7	$p \wedge q \to r$	$\to$i 2–6

Example: $p \to q \vdash p \wedge r \to q \wedge r$

1	$p \to q$	premise
2	$p \wedge r$	assumption
3	p	$\wedge$e1 2
4	r	$\wedge$e2 2
5	q	$\to$e 1,3
6	$q \wedge r$	$\wedge$i 4,5
7	$p \wedge r \to q \wedge r$	$\to$i 2–6

Natural Deduction Rules — Disjunction

$$\frac{\Phi}{\Phi \vee \Psi}\ \vee\mathrm{i1} \qquad \frac{\Psi}{\Phi \vee \Psi}\ \vee\mathrm{i2}$$

$$\frac{\Phi \wedge \Psi \qquad \boxed{\begin{array}{c}\Phi\\ \vdots\\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\Psi\\ \vdots\\ \chi\end{array}}}{\chi}\ \vee\mathrm{e}$$

Example: $p \vee q \vdash q \vee p$

1	$p \vee q$	premise
2	p	assumption
3	$q \vee p$	$\vee$i2 2
4	q	assumption
5	$q \vee p$	$\vee$i1 4
6	$q \vee p$	$\vee$e 1,2-3,4-5

Example: $q \to r \vdash p \vee q \to p \vee r$

1	$q \to r$	premise
2	$p \vee q$	assumption
3	p	assumption
4	$p \vee r$	$\vee$i1 3
5	q	assumption
6	r	$\to$e 1,5
7	$p \vee r$	$\vee$i2 6
8	$p \vee r$	$\vee$e 2,3-4,5-7
9	$p \vee q \to p \vee r$	$\to$i 2-8

Contradictions: formulas of the form $\Phi \wedge \neg\Phi$, $\neg\Phi \wedge \Phi$ —all such formulas shall be denoted by $\perp$ (bottom).

$$\frac{\perp}{\Phi}\ \perp\mathrm{e} \qquad\qquad \frac{\Phi \quad \neg\Phi}{\perp}\ \neg\mathrm{e}$$

Example: $p \to q, p \to \neg q \vdash \neg p$

1	$p \to q$	premise
2	$p \to \neg q$	premise
3	p	assumption
4	q	$\to$e 1,3
5	$\neg q$	$\to$e 2,3
6	$\perp$	$\neg$e 4,5
7	$\neg p$	$\neg$i 3-6

Example: $\neg p \vee q \vdash p \to q$

1	$\neg p \vee q$	premise
2	$\neg p$	$\vee$e2
3	p	assumption
4	$\perp$	$\neg$e 3,2
5	q	$\perp$e4
6	$p \to q$	$\to$i 3-5
7	q	premise
8	p	assumption
9	q	copy 7
10	$p \to q$	$\to$i 9-10
11	$p \to q$	$\vee$e 1,2-6,7-10

Natural Deduction — Derived Rules

$$\frac{\Phi \to \Psi \quad \neg\Psi}{\neg\Phi}\ \text{MT}$$

1	$\Phi \to \Psi$	premise
2	$\neg\Psi$	premise
3	Φ	assumption
4	Ψ	$\to$e 1,3
5	$\bot$	$\neg$e 4,2
6	$\neg\Phi$	$\neg$i 3-5

Justification: If I am Chinese, then I am Asian. I am not Asian. Therefore, I'm not Chinese.

$$\frac{\Phi}{\neg\neg\Phi}\ \neg\neg\text{i}$$

1	Φ	premise
2	$\neg\Phi$	assumption
3	$\bot$	$\neg$e 1,2
4	$\neg\neg\Phi$	$\neg$i 2-3

$$\frac{\boxed{\begin{array}{c}\neg\Psi \\ \vdots \\ \bot\end{array}}}{\Phi}\ \text{RAA (Reductio ad Absurdum)}$$

1	$\neg\Phi \to \bot$	given
2	$\neg\Phi$	assumption
3	$\bot$	$\to$e 1,2
4	$\neg\neg\Phi$	$\neg$i 2-3
5	Φ	$\neg\neg$e 4

Natural Deduction Summary

Basic rules:

	Introd.	Elim.
$\wedge$	$\dfrac{\Phi \quad \Psi}{\Phi \wedge \Psi}\ \wedge\mathrm{i}$	$\dfrac{\Phi \quad \Psi}{\Phi}\ \wedge\mathrm{e1}$ $\quad$ $\dfrac{\Phi \quad \Psi}{\Psi}\ \wedge\mathrm{e2}$
$\vee$	$\dfrac{\Phi}{\Phi \vee \Psi}\ \vee\mathrm{i1}$ $\quad$ $\dfrac{\Psi}{\Phi \vee \Psi}\ \vee\mathrm{i2}$	$\dfrac{\Phi \vee \Psi \quad \boxed{\begin{array}{c}\Phi\\ \vdots\\ \chi\end{array}} \quad \boxed{\begin{array}{c}\Psi\\ \vdots\\ \chi\end{array}}}{\chi}\ \vee\mathrm{e}$
$\to$	$\dfrac{\boxed{\begin{array}{c}\Phi\\ \vdots\\ \Psi\end{array}}}{\Phi \to \Psi}\ \to\mathrm{i}$	$\dfrac{\Phi \quad \Phi \to \Psi}{\Psi}\ \to\mathrm{e}$
$\neg$	$\dfrac{\boxed{\begin{array}{c}\Phi\\ \vdots\\ \bot\end{array}}}{\neg\Phi}\ \neg\mathrm{i}$	$\dfrac{\neg\neg\Phi}{\Phi}\ \neg\neg\mathrm{e}$

Basic rules (cont'd):

	Introd.	Elim.
$\bot$	no rule	$\dfrac{\bot}{\Phi}\ \bot\mathrm{e}$
$\neg\neg$	derived	$\dfrac{\neg\neg\Phi}{\Phi}\ \neg\neg\mathrm{e}$

Useful derived rules:

$$\dfrac{\Phi \to \Psi \quad \neg\Psi}{\neg\Phi}\ \mathrm{MT} \qquad \dfrac{\Phi}{\neg\neg\Phi}\ \neg\neg\mathrm{i}$$

$$\dfrac{\boxed{\begin{array}{c}\neg\Psi\\ \vdots\\ \bot\end{array}}}{\Phi}\ \mathrm{RAA} \qquad \dfrac{}{\Phi \vee \neg\Phi}\ \mathrm{LEM}$$

Definition: We say that two formulas Ψ and Φ are ***provably equivalent*** iff both $\Phi \vdash \Psi$ and $\Psi \vdash \Phi$. We denote this by $\Psi \dashv\vdash \Phi$.

Remark: We could define $\Psi \dashv\vdash \Phi$ to mean that $\vdash (\Phi \to \Psi) \land (\Psi \to \Phi)$ holds.

Interesting proof

Statement: There exist irrational numbers a and b such that a^b is rational.

Proof: Choose $b = \sqrt{2}$. We have two cases.

b^b *is rational.* Then choose $a = b$ and the statement is proven.

b^b *is irrational.* Then choose $a = b^b = (\sqrt{2})^{\sqrt{2}}$. We have

$$a^b = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2 \quad \text{—rational.}$$

Proofs are in fact proof schemas.

$p \to q, p \vdash q$

1	$p \to q$	premise
2	p	premise
3	q	$\to$e 1,2

$r \vee \neg s \to s \to r, r \vee \neg s \vdash s \to r$

1	$r \vee \neg s \to s \to r$	premise
2	$r \vee \neg s$	premise
3	$s \to r$	$\to$e 1,2

$p \leadsto r \vee \neg s$
$q \leadsto s \to r$

- We can build complicated formulas using our rules.
- What exactly are the formulas? We need to define a formal language.

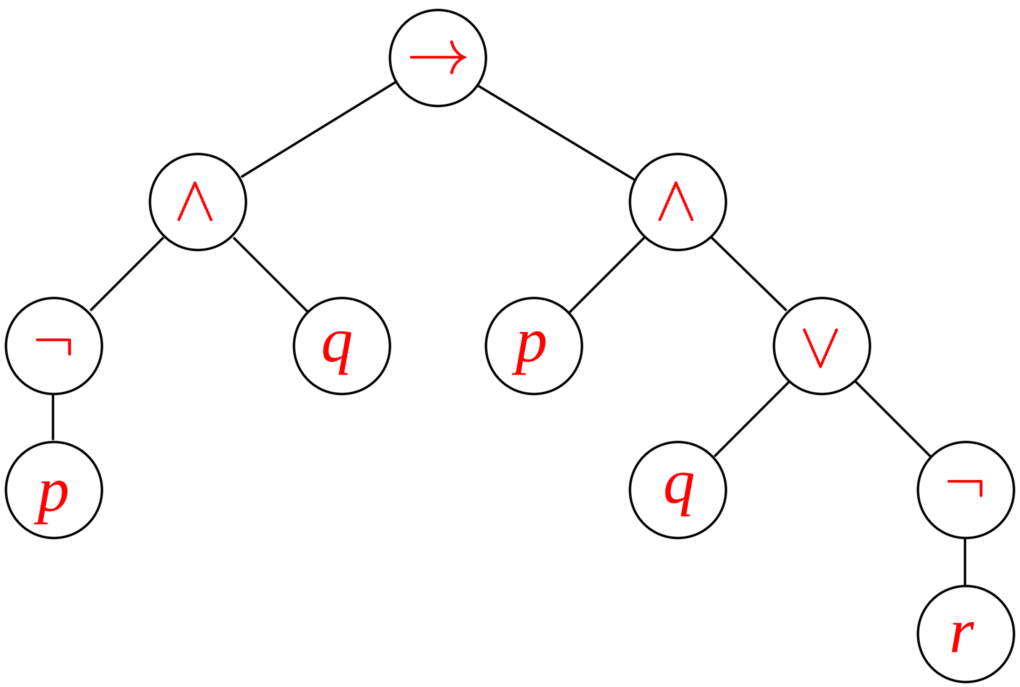
Definition:

atoms: propositional symbols p, q, p_1, p_2, . . .
an atom is a ***well-formed formula (wff)***
if Φ and Ψ are formulas, then so are $(\neg\Phi)$, $(\Phi \wedge \Psi)$, $(\Phi \wedge \Psi)$,$(\Phi \to \Psi)$.

BNF form: $\Phi ::= p \,|\, (\neg\Phi) \,|\, (\Phi \wedge \Phi) \,|\, (\Phi \vee \Phi) \,|\, (\Phi \to \Phi)$

Syntax Trees

Well-formed formula: $$(\underbrace{((\neg p) \wedge q)}_{\substack{\text{subformula}\\ \text{corresponding to the}\\ \text{left subtree}}} \rightarrow (p \wedge (q \vee (\neg r))))$$



All subformulas:

p

q

r

$(\neg p)$

$((\neg p) \wedge q)$

$(\neg r)$

$(q \vee (\neg r))$

$(p \wedge (q \vee (\neg r)))$

$(((\neg p) \wedge q) \rightarrow (p \wedge (q \vee (\neg r))))$

The semantics of propositional logic is a mapping

$$\text{Interpretation} : \text{WFF} \mapsto \{T, F\}$$

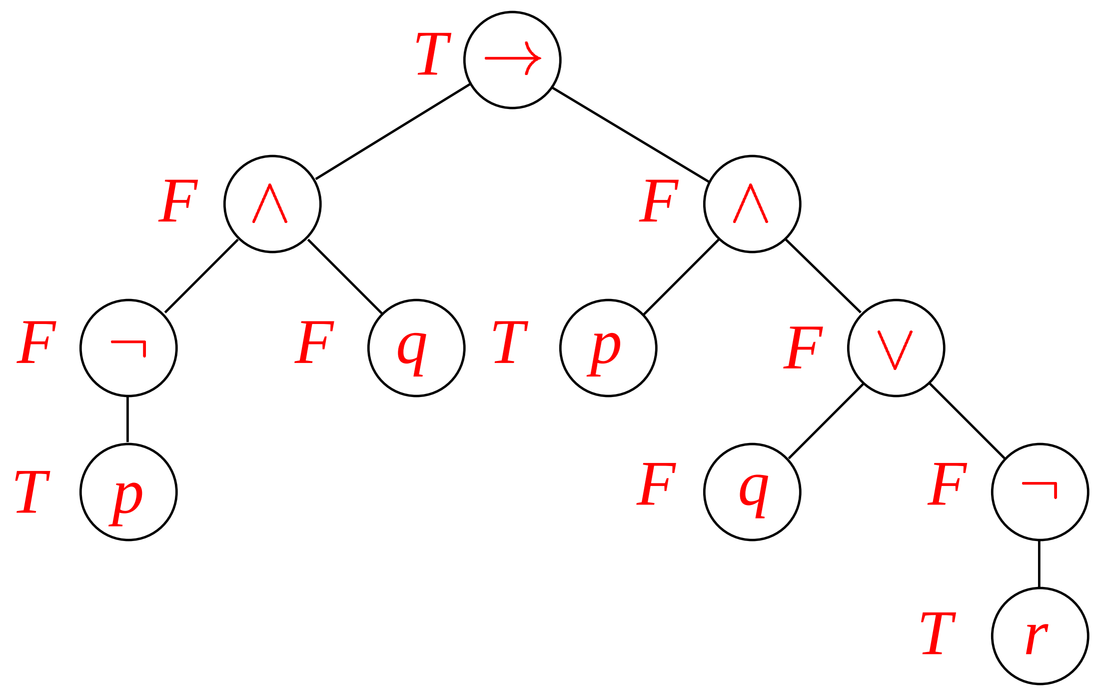
where T stands for ***true*** and F stands for ***false***. The semantics has to be consitent w.r.t. the connectives $\neg$, $\wedge$, $\vee$, and $\rightarrow$. This consitency is specified by the following ***truth table***.

Φ	Ψ	$\neg\Psi$	$\Phi \wedge \Psi$	$\Phi \vee \Psi$	$\Phi \rightarrow \Psi$	$\top$	$\bot$
F	F	T	F	F	T	T	F
F	T	F	F	T	T		
T	F		F	T	F		
T	T		T	T	T		

Truth tables are means of exploring all possible interpretations for a given formula.

Truth Table Example

p	q	r	$p \wedge q \rightarrow p \wedge (q \vee \neg r)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T



Given a sequent $\Phi_1, \Phi_2, \ldots, \Phi_n \vdash \Psi$ (which we don't know whether it is valid), we denote by

$$\Phi_1, \Phi_2, \ldots, \Phi_n \models \Psi$$

a new kind of sequent, which is valid if for every semantics S such that $S(\Phi_i) = T$, $i = 1, \ldots, n$, we also have that $S(\Psi) = T$. The $\models$ relation is called ***semantic entailment***.

Example: $p, q \models p \wedge (q \vee \neg r)$

How do we prove that $1+2+\cdots+n = \frac{n\cdot(n+1)}{2}$? **Answer:** Mathematical induction.

(Base case) We prove the statement for $n = 1$. Indeed, $1 = \frac{1\cdot 2}{2}$.

(Induction case) We assume that the statement is true for some general value of n, and we show that it implies the statement for $n+1$. In other words, we prove that

$$1+2+\cdots+n = \frac{n\cdot(n+1)}{2} \to 1+2+\cdots+n+(n+1) = \frac{(n+1)\cdot(n+2)}{2}$$

Indeed

$$1+2+\cdots+n+(n+1) = \frac{n\cdot(n+1)}{2}+(n+1) = \frac{(n+1)\cdot(n+2)}{2}$$

General Mathematical Induction Principle

Given a statement $\eta(n)$ that depends on a natural number n, and whose validity we want to prove for all possible values of n, we proceed in the following two steps:

- ***Base case:*** prove that $\eta(1)$ holds.
- ***Induction case:*** prove that $\eta(n) \to \eta(n+1)$, for all natural numbers n. When proving such a statement, we call $\eta(n)$ the ***induction hypothesis***.
- These two conditions prove $\eta(n)$ for all n.

Course of Values Induction

Given a statement $\eta(n)$ that depends on a natural number n, and whose validity we want to prove for all possible values of n, we proceed in the following two steps:

- ***Base case:*** prove that $\eta(1)$ holds.
- ***Induction case:*** prove that $\eta(1) \wedge \eta(2) \wedge \cdots \wedge \eta(n) \rightarrow \eta(n+1)$, for all natural numbers n. When proving such a statement, we call $\eta(1) \wedge \eta(2) \wedge \cdots \wedge \eta(n)$ the ***induction hypothesis***.
- These two conditions prove $\eta(n)$ for all n.

Course of Values Induction Example

Definition: Given a well-formed formula Φ, we define its height to be 1 plus the length of its largest path of its parse tree.

Theorem: For every well-formed propositional logic formula, the number of left brackets is equal to the number of right brackets.

Proof: Denote by $\eta(n)$ the statement "all formulas Φ of height n have the same number of left and right brackets."

> ***Base case:*** $n = 1$. $\eta(1)$ applies to all propositional formulas p, q, $\ldots$ and obvioulsy holds.
>
> ***Induction case:*** $n > 1$. Then the root of the parse tree of Φ is one of the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$. We assume that it is $\rightarrow$ (the other cases are proved in a similar manner.) Then $\Phi = \Phi_1 \rightarrow \Phi_2$ for some wffs Φ_1 and Φ_2, whose heights are strictly smaller than n. Using the induction hypothesis, the number of left and right brackets is equal for both Φ_1 and Φ_2. Φ adds only two brackets, one $'('$ and one $')'$. Therefore, the statement is correct.

When we define a logic (or any type of calculus), we want to show that it is useful.

- ***Soundness:*** Formulas that we derive using the calculus reflect a “real” truth.
- ***Completeness:*** Every formula corresponding to a “real” truth can be inferred using the rules of the calculus.

In the case of propositional logic, given the wffs Φ_1, Φ_2, $\ldots$, Φ_n, and Ψ, we have

- ***Soundness:*** if $\Phi_1, \ldots, \Phi_n \vdash \Psi$ holds, then $\Phi_1, \ldots, \Phi_n \models \Psi$ holds.
- ***Completeness:*** if $\Phi_1, \ldots, \Phi_n \models \Psi$ holds, then $\Phi_1, \ldots, \Phi_n \vdash \Psi$ holds.