Deduction

Zhaoguo Wang

Adapted From:

教材《数理逻辑与集合论》1.6, 2.5, 2.7~2.10

Outline – This Lecture

- Deduction
- Dual Formula
- Polish Notation

Deduction

DEFINITION

A proof is an argument that demonstrates why a conclusion is true, subject to certain standards of truth, which is made up of a finite sequence of fixed indisputable steps.

DEFINITION

Proofs in natural language are informal proof.

Proofs in logic are formal proofs or deductions(推理).

Deduction

DEFINITION

A proof is an argument that demonstrates why a conclusion is true, subject to certain standards of truth, which is made up of a finite sequence of fixed indisputable steps.

Remember that an "informal" proof must still be convincing!

DEFINITION

Proofs in natural language are informal proof.

Proofs in logic are formal proofs or deductions(推理).

Deduction

facts assumed to be true for the purpose of the deduction

Axioms or Assumptions

Deduction $\left\{ \begin{array}{l} \text{Axioms or Assumptions} \\ \text{Inference rules} \end{array} \right.$

a group of rules for creating new facts from old

Inference rules

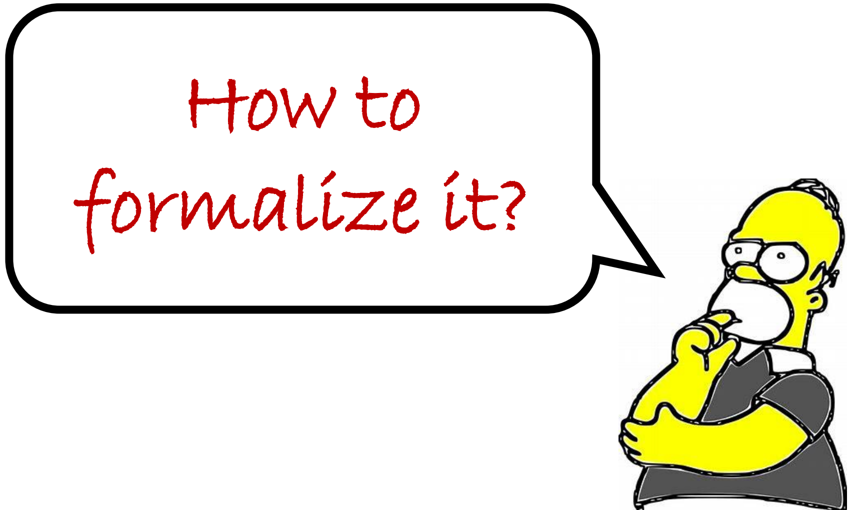
Deduction is a sequence of theorems obtained using a specific set of assumptions and rules of inference.

Deduction

DEFINITION

Formalize the deduction relation and we can get a deduction form (推理形式).

- If I am ill, I don’t go to school.
- I am ill.
- So I don’t go to school.



Deduction

DEFINITION

Formalize the deduction relation and we can get a deduction form(推理形式).

A I am ill.

B I don't go to school.

$A \to B$

If I am ill, I don't go to school.

$$A \wedge (A \to B) \to B$$

$$\begin{array}{rl} A \to B & assumption \\ A & assumption \\ \hline B & conclusion \end{array}$$

Deduction

$$A \wedge (A \rightarrow B) \rightarrow B$$

P Q

This is a correct deduction form iff it is a tautology.

DEFINITION

Given two formulas A and B, if B must be true when A is true, then A tautologically implies(重言蕴含) B. $A \Rightarrow B$

Deduction form is correct iff P tautologically implies Q.

It's not a connective.

Deduction

$$A \wedge (A \to B) \Rightarrow B$$

It can be proved by truth table, equivalence calculus and interpretation in natural language.

THEOREM

1) If $A \Longrightarrow B$, A is a tautology, then B is a tautology.

2) If $A \Longrightarrow B, B \Longrightarrow A$, then $A = B$.

3) If $A \Longrightarrow B, B \Longrightarrow C$, then $A \Longrightarrow C$.

4) If $A \Longrightarrow B, A \Longrightarrow C$, then $A \Longrightarrow B \wedge C$.

5) If $A \Longrightarrow C, B \Longrightarrow C$, then $A \vee B \Longrightarrow C$.

Deduction

There are many important tautology implication expressions.

They can be used as inference rules to produce new theorems.

$$\neg(P \to Q) \Rightarrow P$$

$$\neg(P \to Q) \Rightarrow \neg Q$$

$$P \wedge (P \to Q) \Rightarrow Q$$

hypothetical reasoning(假言推理/分离规则)

$$(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$$

Syllogism(三段论)

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

$(1) P$ $\qquad$ $introduce\ premise$

We can introduce assumptions/premise(前提引入规则) anytime in deduction process.

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

$(1) P$ *introduce premise*

$(2) P \to Q$ *introduce premise*

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

$(1) P$	*introduce premise*
$(2) P \to Q$	*introduce premise*
$(3) Q$	*Hypothetical reasoning on* (1)(2)

We can use hypothetical reasoning to produce new theorems(分离规则), which can be used as premise(结论引用规则).

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

$(1) P$ — *introduce premise*

$(2) P \to Q$ — *introduce premise*

$(3) Q$ — *Hypothetical reasoning on* $(1)(2)$

$(4) Q \to R$ — *introduce premise*

Deduction

We now introduce an example to explain deduction calculus.

Prove R when $P \to Q$, $Q \to R$ and P.

$$
\begin{aligned}
&(1)P && \textit{introduce premise} \\
&(2)P \to Q && \textit{introduce premise} \\
&(3)Q && \textit{Hypothetical reasoning on } (1)(2) \\
&(4)Q \to R && \textit{introduce premise} \\
&(5)R && \textit{Hypothetical reasoning on } (3)(4)
\end{aligned}
$$

Substitution rule

THEOREM

Substitution rule(代入规则):

For any propositional variable P that occurs in tautology A, replace each and every occurrence of P in A with another formula and get a new formula B. Then B is also a tautology.

$$P \vee \neg P \quad \xrightarrow{\frac{P}{(R \vee S)}} \quad (R \vee S) \vee \neg(R \vee S)$$

Replacement rule

THEOREM

Replacement rules(置换规则) are rules of replacing sub-formula in A and still have a wff B with the same truth-value; in other words, they are a list of logical equivalencies.

We have implicitly applied replacement rules in propositional equivalence calculus.

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

$(1) \neg R \lor P$ *introduce premise*

Deduction

Prove $(P \to (Q \to S)) \wedge (\neg R \vee P) \wedge Q \Rightarrow R \to S$.

$$(1) \neg R \vee P \qquad \textit{introduce premise}$$

$$(2) R \to P \qquad \textit{replacement rule}$$

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

$(1) \neg R \lor P$	*introduce premise*
$(2) R \to P$	*replacement rule*
$(3) R$	*introduce premise*

We can introduce R because $\boldsymbol{A \land B \Longrightarrow C}$ ***iff*** $\boldsymbol{A \Longrightarrow B \to C}$.(条件证明规则)

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

$(1) \neg R \lor P$ *introduce premise*

$(2) R \to P$ *replacement rule*

$(3) R$ *introduce premise*

$(4) P$ *Hypothetical reasoning on (2)(3)*

Deduction

Prove $(P \to (Q \to S)) \wedge (\neg R \vee P) \wedge Q \Rightarrow R \to S$.

$(1) \neg R \vee P$	*introduce premise*
$(2) R \to P$	*replacement rule*
$(3) R$	*introduce premise*
$(4) P$	*Hypothetical reasoning on* (2)(3)
$(5) P \to (Q \to S)$	*introduce premise*

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

$(1)\neg R \lor P$	*introduce premise*
$(2)R \to P$	*replacement rule*
$(3)R$	*introduce premise*
$(4)P$	*Hypothetical reasoning on* (2)(3)
$(5)P \to (Q \to S)$	*introduce premise*
$(6)Q \to S$	*Hypothetical reasoning on* (4)(5)

Deduction

Prove $(P \to (Q \to S)) \wedge (\neg R \vee P) \wedge Q \Rightarrow R \to S$.

$(1) \neg R \vee P$	*introduce premise*
$(2) R \to P$	*replacement rule*
$(3) R$	*introduce premise*
$(4) P$	*Hypothetical reasoning on* (2)(3)
$(5) P \to (Q \to S)$	*introduce premise*
$(6) Q \to S$	*Hypothetical reasoning on* (4)(5)
$(7) Q$	*introduce premise*

Deduction

Prove $(P \to (Q \to S)) \wedge (\neg R \vee P) \wedge Q \Rightarrow R \to S$.

$(1) \neg R \vee P$	*introduce premise*
$(2) R \to P$	*replacement rule*
$(3) R$	*introduce premise*
$(4) P$	*Hypothetical reasoning on* (2)(3)
$(5) P \to (Q \to S)$	*introduce premise*
$(6) Q \to S$	*Hypothetical reasoning on* (4)(5)
$(7) Q$	*introduce premise*
$(8) S$	*Hypothetical reasoning on* (6)(7)

Deduction

Prove $(P \to (Q \to S)) \land (\neg R \lor P) \land Q \Rightarrow R \to S$.

$(1) \neg R \lor P$	*introduce premise*
$(2) R \to P$	*replacement rule*
$(3) R$	*introduce premise*
$(4) P$	*Hypothetical reasoning on* (2)(3)
$(5) P \to (Q \to S)$	*introduce premise*
$(6) Q \to S$	*Hypothetical reasoning on* (4)(5)
$(7) Q$	*introduce premise*
$(8) S$	*Hypothetical reasoning on* (6)(7)
$(9) R \to S$	*deduction theorem*

条件证明规则

Resolution Reasoning(归结推理法)

Because $\boldsymbol{A} \Longrightarrow \boldsymbol{B}$ iff $\boldsymbol{A} \wedge \neg \boldsymbol{B}$ is a contradiction. We can prove $\boldsymbol{A} \wedge \neg \boldsymbol{B}$ is a contradiction.

Resolution Reasoning

DEFINITION

For formula $C_1 = L \vee C_1'$ and $C_2 = \neg L \vee C_2'$, $R(C_1, C_2) = C_1' \vee C_2'$ is a resolvent(归结式) of C_1 and C_2.

- To prove $\boldsymbol{A} \Longrightarrow \boldsymbol{B}$ $(\boldsymbol{P} \rightarrow \boldsymbol{Q}) \wedge \boldsymbol{P} \Longrightarrow \boldsymbol{Q}$
- Prove $\boldsymbol{A} \wedge \neg \boldsymbol{B}$ is a contradiction $(\boldsymbol{P} \rightarrow \boldsymbol{Q}) \wedge \boldsymbol{P} \wedge \neg \boldsymbol{Q}$
- Convert $\boldsymbol{A} \wedge \neg \boldsymbol{B}$ to CNF $\boldsymbol{A_1} \wedge \boldsymbol{A_2} \wedge \cdots \wedge \boldsymbol{A_n}$ $(\neg \boldsymbol{P} \vee \boldsymbol{Q}) \wedge \boldsymbol{P} \wedge \neg \boldsymbol{Q}$
- Repeatly produce resolvents from $\boldsymbol{A_i}$
- Find contradiction and proof ends

Resolution Reasoning

Prove that $(P \to Q) \land P \Rightarrow Q$.

Resolution Reasoning

Prove that $(P \to Q) \land P \Rightarrow Q$.

$$(P \to Q) \land P \land \neg Q = (\neg P \lor Q) \land P \land \neg Q$$

Resolution Reasoning

Prove that $(P \rightarrow Q) \wedge P \Rightarrow Q$.

$$(P \rightarrow Q) \wedge P \wedge \neg Q = (\neg P \vee Q) \wedge P \wedge \neg Q$$

$$S = \{\neg P \vee Q, P, \neg Q\}$$

Resolution Reasoning

Prove that $(P \to Q) \wedge P \Rightarrow Q$.

$$(P \to Q) \wedge P \wedge \neg Q = (\neg P \vee Q) \wedge P \wedge \neg Q$$

$$S = \{\neg P \vee Q, P, \neg Q\}$$

$(1) \neg P \vee Q$ *introduce premise*

Resolution Reasoning

Prove that $(P \to Q) \wedge P \Rightarrow Q$.

$$(P \to Q) \wedge P \wedge \neg Q = (\neg P \vee Q) \wedge P \wedge \neg Q$$

$$S = \{\neg P \vee Q, P, \neg Q\}$$

$(1) \neg P \vee Q$ *introduce premise*

$(2) P$ *introduce premise*

Resolution Reasoning

Prove that $(P \to Q) \wedge P \Rightarrow Q$.

$$(P \to Q) \wedge P \wedge \neg Q = (\neg P \vee Q) \wedge P \wedge \neg Q$$

$$S = \{\neg P \vee Q, P, \neg Q\}$$

$$\begin{aligned} &(1) \neg P \vee Q && \textit{introduce premise} \\ &(2) P && \textit{introduce premise} \\ &(3) Q && \textit{resolution of (1) and (2)} \end{aligned}$$

Resolution Reasoning

Prove that $(P \to Q) \land P \Rightarrow Q$.

$$(P \to Q) \land P \land \neg Q = (\neg P \lor Q) \land P \land \neg Q$$

$$S = \{\neg P \lor Q, P, \neg Q\}$$

$$
\begin{aligned}
&(1)\neg P \lor Q && \textit{introduce premise} \\
&(2)P && \textit{introduce premise} \\
&(3)Q && \textit{resolution of (1) and (2)} \\
&(4)\neg Q && \textit{introduce premise}
\end{aligned}
$$

Resolution Reasoning

Prove that $(P \rightarrow Q) \wedge P \Rightarrow Q$.

$$(P \rightarrow Q) \wedge P \wedge \neg Q = (\neg P \vee Q) \wedge P \wedge \neg Q$$

$$S = \{\neg P \vee Q, P, \neg Q\}$$

$(1) \neg P \vee Q$	*introduce premise*
$(2) P$	*introduce premise*
$(3) Q$	*resolution of (1) and (2)*
$(4) \neg Q$	*introduce premise*
$(5) \square$	*resolution of (3) and (4)*

Exercise

Prove $((P \to Q) \wedge (Q \to R)) \Rightarrow (P \to R)$

Exercise

Prove $((P \to Q) \wedge (Q \to R)) \Rightarrow (P \to R)$

证明 先将$(P\to Q)\wedge(Q\to R)\wedge\neg(P\to R)$

化成合取范式

$$(\neg P\vee Q)\wedge(\neg Q\vee R)\wedge P\wedge\neg R$$

建立子句集

$$S=\{\neg P\vee Q,\neg Q\vee R,P,\neg R\}$$

归结过程:

(1) $\neg P\vee Q$

(2) $\neg Q\vee R$

(3) P

(4) $\neg R$

(5) $\neg P\vee R$ (1) (2) 归结

(6) R (3) (5) 归结

(7) $\square$ (4) (6) 归结

Dual formula (对偶式)

Duality underlines the world

Dual formula

DEFINITION

Given a formula A, replace $\vee$, $\wedge$, T, F in A with $\wedge$, $\vee$, F, T and get A^*.

Then A and A^* are dual formulas(对偶式) with each other.

Dual formula

THEOREM

$$A = A(P_1, \dots, P_n), \quad A^- = A(\neg P_1, \dots, \neg P_n)$$

$$\neg(A^*) = (\neg A)^*, \quad \neg(A^-) = (\neg A)^-$$

$$(A^*)^* = A, \quad (A^-)^- = A$$

$$(\neg A) = A^{*-}$$

How to prove these theorems?

Dual formula

THEOREM

$$A = A(P_1, ..., P_n), \quad A^- = A(\neg P_1, ..., \neg P_n)$$

$$\neg(A^*) = (\neg A)^*, \quad \neg(A^-) = (\neg A)^-$$

$$(A^*)^* = A, \quad (A^-)^- = A$$

$$(\neg A) = A^{*-}$$

Recap: induction is a natural way to prove theorems about inductive-defined objects.

Dual formula

THEOREM

$$A = A(P_1, ..., P_n), \quad A^- = A(\neg P_1, ..., \neg P_n)$$

$$\neg(A^*) = (\neg A)^*, \quad \neg(A^-) = (\neg A)^-$$

$$(A^*)^* = A, \quad (A^-)^- = A$$

$$(\neg A) = A^{*-}$$

Proof is on p23 in the textbook.

Dual formula

THEOREM

1) If $A = B$, then $A^* = B^*$

2) If $A \longrightarrow B$ is a tautology, then $B^* \longrightarrow A^*$ is a tautology

3) A is a tautology iff A^- is a tautology

4) A is satisfiable iff A^- is satisfiable

5) $\neg A$ is a tautology iff A^* is a tautology

6) $\neg A$ is satisfiable iff A^* is satisfiable

Polish notation（波兰表达式）

- The previous wff is called infix notation（中缀表达式）
- There is a different notation called polish notation（波兰表达式）or prefix notation（前缀表达式）
- Polish notation can achieve higher performance than infix notation

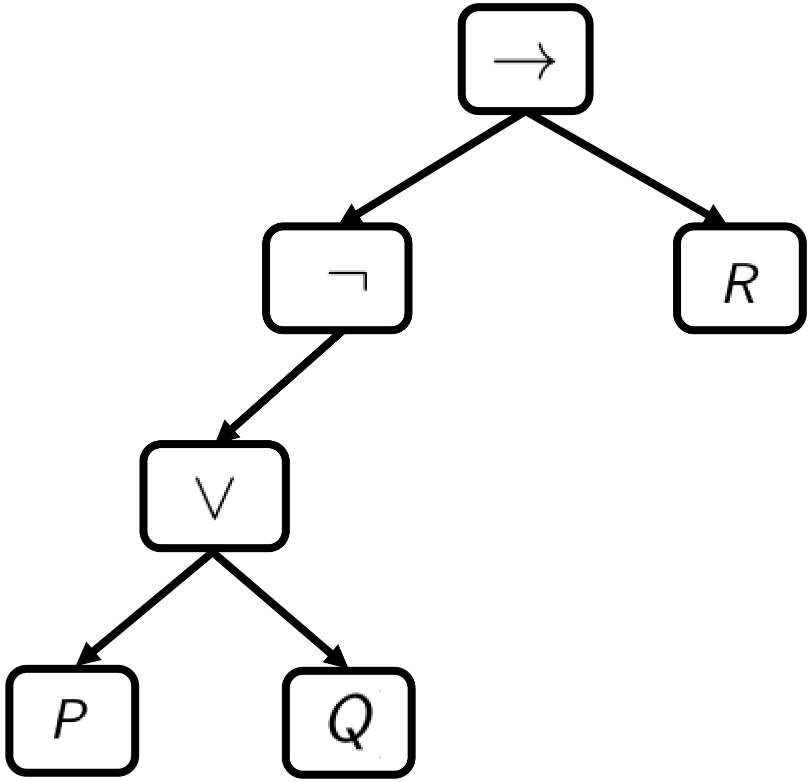
polish notation
in solver

```
(declare-const a Int)
(declare-fun f (Int Bool) Int)
(assert (> a 10))
(assert (< (f a true) 100))
(check-sat)
```

Polish notation

- We show here how to convert the infix notation to polish notation

$((\neg(P \vee Q)) \rightarrow R)$

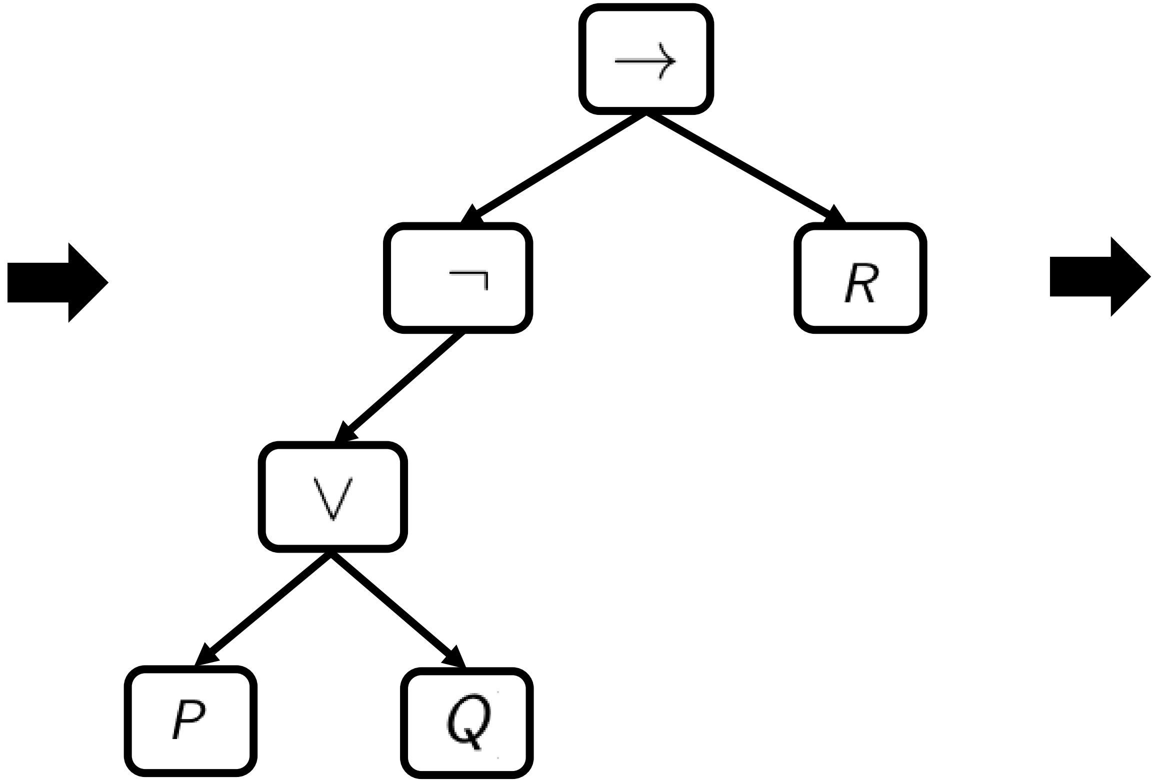


$\rightarrow \neg \vee PQR$

Reverse polish notation（逆波兰表达式）

- There is also a different notation called reverse polish notation（逆波兰表达式）or postfix notation（后缀表达式）

$((\neg(P \vee Q)) \to R)$



$PQ \vee \neg R \to$

Thanks & Questions