# Discrete Mathematics: Lecture 17

## Part III. Mathematical Logic

logically equivalent, rule of replacement, tautological implications, argument

Xuming He
Associate Professor

School of Information Science and Technology
ShanghaiTech University

Spring Semester, 2025

Notes by Prof. Liangfeng Zhang

# Truth Table & Types of WFFs (Review)

**DEFINITION:** Let $F$ be a WFF of $p_1, \dots, p_n$, $n$ propositional variables

- A **truth assignment** (真值指派) for $F$ is a map $\alpha: \{p_1, \dots, p_n\} \to \{\mathbf{T}, \mathbf{F}\}$.
  - There are $2^n$ different truth assignments.

**Tautology**(重言式): a WFF whose truth value is **T** for all truth assignment

**Contradiction**(矛盾式): a WFF whose truth value is **F** for all truth assignment

**Contingency**( 可能式): neither tautology nor contradiction

**Satisfiable**(可满足的):a WFF is satisfiable if it is true for at least one truth assignment

**Rule of Substitution**: (代入规则) Let $B$ be a formula obtained from a tautology $A$ by substituting a propositional variable in $A$ with an arbitrary formula. Then $B$ must be a tautology.

# Logically Equivalent (Review)

**DEFINITION:** Let $A$ and $B$ be WFFs in propositional variables $p_1, \ldots, p_n$.

- $A$ and $B$ are **logically equivalent** (等值) if they always have the same truth value for every truth assignment (of $p_1, \ldots, p_n$)
  - Notation: $A \equiv B$

**THEOREM:** $A \equiv B$ if and only if $A \leftrightarrow B$ is a tautology.

**THEOREM:** $A \equiv A$; If $A \equiv B$, then $B \equiv A$; If $A \equiv B, B \equiv C$, then $A \equiv C$

**QUESTION:** How to prove $A \equiv B$?

# Proving $A \equiv B$ (Review)

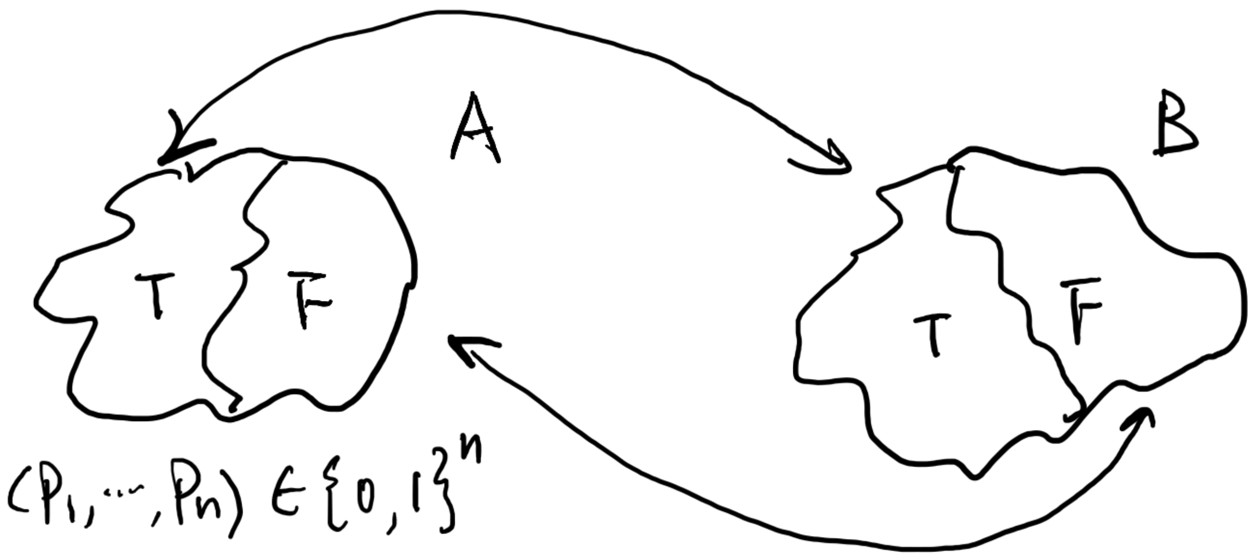
**Method 1**: Show that $A, B$ have the same truth table.

**Method 2: Rule of Replacement:** (替换规则) Replacing a sub-formula in a formula $F$ with a logically equivalent sub-formula gives a formula logically equivalent o the formula $F$.

# Logically Equivalent

**THEOREM:** Let $A^{-1}(\mathbf{T})$ be the set of truth assignments such that $A$ is true. Then $A \equiv B$ if and only if $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$.

- $A \equiv B$ if and only if $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$



# Proving $A \equiv B$

**EXAMPLE**: $P \wedge Q \equiv Q \wedge P$ **//commutative law**

- <u>Idea: Show that $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$.</u>
- $A = P \wedge Q; B = Q \wedge P$
  - $A = \mathbf{T}$ if and only if $(P, Q) = (\mathbf{T}, \mathbf{T})$
    - $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$
  - $B = \mathbf{T}$ if and only if $(Q, P) = (\mathbf{T}, \mathbf{T})$
    - $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$
- $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$
- $A \equiv B$

**REMARK**: $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ can be shown similarly.

- **Associative law**

# Proving $A \equiv B$

**EXAMPLE**: $P \vee Q \equiv Q \vee P$ **//commutative law**

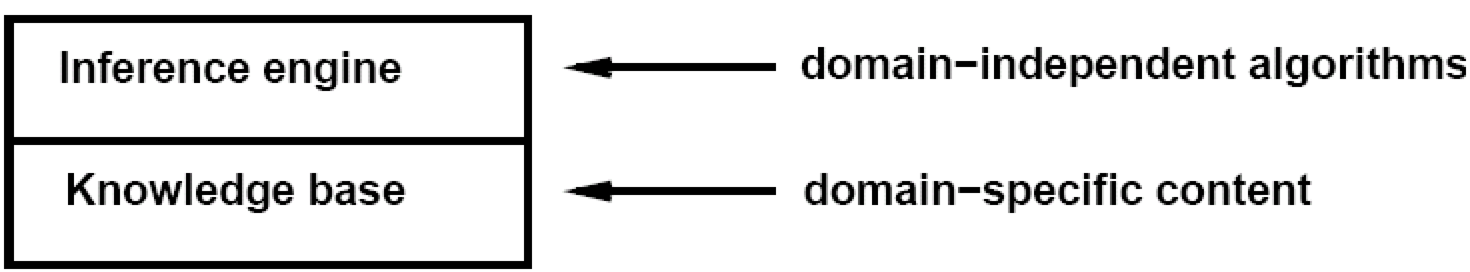
- Idea: Show that $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$.
- $A = P \vee Q$; $B = Q \vee P$
    - $A = \mathbf{F}$ if and only if $(P, Q) = (\mathbf{F}, \mathbf{F})$
        - $A^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{F})\}$
    - $B = \mathbf{F}$ if and only if $(Q, P) = (\mathbf{F}, \mathbf{F})$
        - $B^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{F})\}$
- $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$
- $A \equiv B$

**REMARK**: $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ can be shown similarly.

- **Associative law**

# Logic-based Inference (Review)

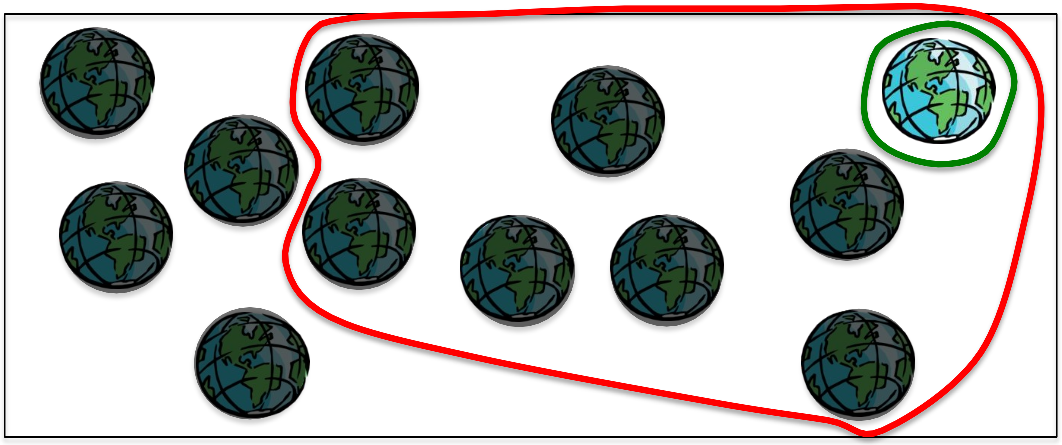
- Logic (Knowledge-Based) Inference
  - Knowledge base
    - set of sentences in a formal language to represent knowledge about the "world"
  - Inference engine
    - answers any answerable question following the knowledge base



# Tautological Implications

**DEFINITION:** Let $A$ and $B$ be WFFs in propositional variables $p_1, \ldots, p_n$.

- $A$ **tautologically implies** (重言蕴涵) $B$ if every truth assignment that causes $A$ to be true causes $B$ to be true.
  - Notation: $A \Rightarrow B$, called a **tautological implication**
  - $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T}); B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$



# Tautological Implications

**DEFINITION:** Let $A$ and $B$ be WFFs in propositional variables $p_1, \ldots, p_n$.

- $A$ **tautologically implies** (重言蕴涵) $B$ if every truth assignment that causes $A$ to be true causes $B$ to be true.
  - Notation: $A \Rightarrow B$, called a **tautological implication**
  - $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$; $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$

**THEOREM:** $A \Rightarrow B$ iff $A \rightarrow B$ is a tautology.

- $A \Rightarrow B$ iff $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$ iff $A \rightarrow B$ is a tautology

**THEOREM:** $A \Rightarrow B$ iff $A \land \neg B$ is a contradiction.

- $A \rightarrow B \equiv \neg A \lor B \equiv \neg(A \land \neg B)$

**Proving $\boldsymbol{A} \Rightarrow \boldsymbol{B}$:** (1) $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$; (2) $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$; (3) $A \rightarrow B$ is a tautology; (4) $A \land \neg B$ is a contradiction

# Proving $A \Rightarrow B$

**EXAMPLE**: Show the tautological implication "$p \wedge (p \to q) \Rightarrow q$".

- Let $A = p \wedge (p \to q)$; $B = q$. Need to show that "$A \Rightarrow B$"
- $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T})\}$; $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}), (\mathbf{F}, \mathbf{T})\}$: $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$.

| $p$ | $q$ | $p \to q$ | $A$ | $B$ |
|---|---|---|---|---|
| **T** | **T** | **T** | **<u>T</u>** | **<u>T</u>** |
| **T** | **F** | **F** | **F** | **F** |
| **F** | **T** | **T** | **F** | **T** |
| **F** | **F** | **T** | **F** | **F** |

- $$\begin{aligned} A \to B &\equiv \neg\big(p \wedge (p \to q)\big) \vee q \\ &\equiv \big(\neg p \vee \neg(p \to q)\big) \vee q \\ &\equiv (\neg p \vee q) \vee \neg(p \to q) \\ &\equiv (p \to q) \vee \neg(p \to q) \\ &\equiv \mathbf{T} \end{aligned}$$
- $$\begin{aligned} A \wedge \neg B &\equiv \big(p \wedge (p \to q)\big) \wedge \neg q \\ &\equiv (\neg q \wedge p) \wedge (p \to q) \\ &\equiv \neg(p \to q) \wedge (p \to q) \\ &\equiv \mathbf{F} \end{aligned}$$

# Tautological Implications

| Name | Tautological Implication | NO. |
|---|---|---|
| Conjunction(合取) | $(P) \wedge (Q) \Rightarrow P \wedge Q$ | 1 |
| Simplification(化简) | $P \wedge Q \Rightarrow P$ | 2 |
| Addition(附加) | $P \Rightarrow P \vee Q$ | 3 |
| Modus ponens(假言推理) | $P \wedge (P \to Q) \Rightarrow Q$ | 4 |
| Modus tollens(拒取) | $\neg Q \wedge (P \to Q) \Rightarrow \neg P$ | 5 |
| Disjunctive syllogism(析取三段论) | $\neg P \wedge (P \vee Q) \Rightarrow Q$ | 6 |
| Hypothetical syllogism(假言三段论) | $(P \to Q) \wedge (Q \to R) \Rightarrow (P \to R)$ | 7 |
| Resolution (归结) | $(P \vee Q) \wedge (\neg P \vee R) \Rightarrow Q \vee R$ | 8 |

# Proofs for 5 and 6

**EXAMPLE:** $\neg Q \land (P \to Q) \Rightarrow \neg P$

- $A = \neg Q \land (P \to Q), B = \neg P.$
- $A \to B \equiv \neg\big(\neg Q \land (P \to Q)\big) \lor \neg P$

$$\equiv \big(Q \lor \neg(P \to Q)\big) \lor \neg P$$

$$\equiv (\neg P \lor Q) \lor \neg(P \to Q)$$

$$\equiv \mathbf{T}$$

**EXAMPLE:** $\neg P \land (P \lor Q) \Rightarrow Q$

- $A = \neg P \land (P \lor Q), B = Q.$
- $A \to B \equiv \neg\big(\neg P \land (P \lor Q)\big) \lor Q$

$$\equiv \big(P \lor \neg(P \lor Q)\big) \lor Q$$

$$\equiv (\neg(P \lor Q) \lor P) \lor Q$$

$$\equiv \neg(P \lor Q) \lor (P \lor Q)$$

$$\equiv \mathbf{T}$$

# Proofs for 7 and 8

**EXAMPLE**: $(P \to Q) \land (Q \to R) \Rightarrow P \to R$

- $A = (P \to Q) \land (Q \to R);\ B = (P \to R).$
- $A \land \neg B \equiv (\neg P \lor Q) \land (\neg Q \lor R) \land (P \land \neg R)$

$$\equiv \big((\neg P \lor Q) \land P\big) \land \big((\neg Q \lor R) \land \neg R\big)$$
$$\equiv \big((\neg P \land P) \lor (Q \land P)\big) \land \big((\neg Q \land \neg R) \lor (R \land \neg R)\big)$$
$$\equiv (Q \land P) \land (\neg Q \land \neg R)$$
$$\equiv \mathbf{F}$$

**EXAMPLE**: $(P \lor Q) \land (\neg P \lor R) \Rightarrow Q \lor R$

- $A = (P \lor Q) \land (\neg P \lor R); B = (Q \lor R).$
- $A \land \neg B \equiv (P \lor Q) \land (\neg P \lor R) \land (\neg Q \land \neg R)$

$$\equiv \big((P \lor Q) \land \neg Q\big) \land ((\neg P \lor R) \land \neg R)$$
$$\equiv (P \land \neg Q) \land (\neg P \land \neg R)$$
$$\equiv \mathbf{F}$$

# More Examples

**EXAMPLE:** $(P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \Rightarrow (P \leftrightarrow R)$

- $A = (P \leftrightarrow Q) \wedge (Q \leftrightarrow R); B = (P \leftrightarrow R).$
- $A = \mathbf{T}$ iff $(P \leftrightarrow Q) = \mathbf{T}$ and $(Q \leftrightarrow R) = \mathbf{T}$ iff $P = Q$ and $Q = R$
  - $A^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{T}), (\mathbf{F}, \mathbf{F}, \mathbf{F})\}$
- $B = \mathbf{T}$ iff $P = R$
  - $B^{-1}(\mathbf{T}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{T}), (\mathbf{T}, \mathbf{F}, \mathbf{T}), (\mathbf{F}, \mathbf{T}, \mathbf{F}), (\mathbf{F}, \mathbf{F}, \mathbf{F})\}$
- $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$

**EXAMPLE:** $(Q \rightarrow R) \Rightarrow ((P \vee Q) \rightarrow (P \vee R))$

- $A = Q \rightarrow R; B = ((P \vee Q) \rightarrow (P \vee R)).$
- $A = \mathbf{F}$ iff $(Q, R) = (\mathbf{T}, \mathbf{F})$
  - $A^{-1}(\mathbf{F}) = \{(\mathbf{T}, \mathbf{T}, \mathbf{F}), (\mathbf{F}, \mathbf{T}, \mathbf{F})\}$
- $B = \mathbf{F}$ iff $(P \vee Q, P \vee R) = (\mathbf{T}, \mathbf{F})$ iff $(P, Q) \neq (\mathbf{F}, \mathbf{F})$ and $(P, R) = (\mathbf{F}, \mathbf{F})$
  - $B^{-1}(\mathbf{F}) = \{(\mathbf{F}, \mathbf{T}, \mathbf{F})\}$
- $A^{-1}(\mathbf{F}) \supseteq B^{-1}(\mathbf{F})$

# More Examples

**EXAMPLE**: $(P \to R) \land (Q \to S) \land (P \lor Q) \Rightarrow R \lor S$

- $A = (P \to R) \land (Q \to S) \land (P \lor Q); B = R \lor S$
- $A \land \neg B \equiv (P \to R) \land (Q \to S) \land (P \lor Q) \land \neg(R \lor S)$

$$
\begin{aligned}
&\equiv (\neg P \lor R) \land (\neg Q \lor S) \land (P \lor Q) \land (\neg R \land \neg S) \\
&\equiv ((\neg P \lor R) \land \neg R)) \land ((\neg Q \lor S) \land \neg S) \land (P \lor Q) \\
&\equiv ((\neg P \land \neg R) \lor (R \land \neg R)) \land ((\neg Q \land \neg S) \lor (S \land \neg S)) \land (P \lor Q) \\
&\equiv ((\neg P \land \neg R) \lor \mathbf{F}) \land ((\neg Q \land \neg S) \lor \mathbf{F}) \land (P \lor Q) \\
&\equiv (\neg P \land \neg R) \land (\neg Q \land \neg S) \land (P \lor Q) \\
&\equiv \neg R \land (\neg Q \land \neg S) \land (\neg P \land (P \lor Q)) \\
&\equiv \neg R \land (\neg Q \land \neg S) \land ((\neg P \land P) \lor (\neg P \land Q)) \\
&\equiv \neg R \land (\neg Q \land \neg S) \land (\mathbf{F} \lor (\neg P \land Q)) \\
&\equiv \neg R \land (\neg Q \land \neg S) \land (\neg P \land Q) \\
&\equiv \neg R \land \neg S \land \neg P \land (\neg Q \land Q) \\
&\equiv \neg R \land \neg S \land \neg P \land \mathbf{F} \\
&\equiv \mathbf{F}
\end{aligned}
$$

# Argument

**DEFINITION**: An **argument** (论证) is a sequence of propositions

- **Conclusion**(结论): the final proposition
- **Premises**(假设)**:** all the other propositions
- **Valid**(有效): the truth of premises implies that of the conclusion
- **Proof** (证明): a valid argument that establishes the truth of a conclusion

**EXAMPLE:** a valid argument, a proof

- If $\{2^{-n}\}$ is convergent, then $\{2^{-n}\}$ has a convergent subsequence.
- $\{2^{-n}\}$ is convergent.
- $\{2^{-n}\}$ has a convergent subsequence.

# Argument Form

**DEFINITION:** An **argument form**(论证形式) is a sequence of formulas.

- Replacing propositions in an argument with propositional variables
- **Valid**(有效)**:** no matter which propositions are substituted for the propositional variables, the truth of conclusion follows from the truth of premises

**EXAMPLE:** a valid argument form and an invalid argument form

$p \rightarrow q$

$p$

$q$

valid

$p$: $\{(-1)^n\}$ is convergent.

$q$: $\{(-1)^n\}$ has a convergent subsequence.

$p \rightarrow q$: If $\{(-1)^n\}$ is convergent, then $\{(-1)^n\}$ has a convergent subsequence.

$p \rightarrow q$

$\neg p$

$\neg q$

invalid

$\neg p$: $\{(-1)^n\}$ is not convergent.

$\neg q$: $\{(-1)^n\}$ does not have a convergent subsequence.

The truth of $\neg p$ and $p \rightarrow q$ does not imply that of $\neg q$

# Rules of inference

- **Rules of inference**(推理规则): relatively simple valid argument forms from tautological implications

| Name | Tautological Implication |
|---|---|
| Conjunction(合取) | $(P) \wedge (Q) \Rightarrow P \wedge Q$ |
| Simplification(化简) | $P \wedge Q \Rightarrow P$ |
| Addition(附加) | $P \Rightarrow P \vee Q$ |
| Modus ponens(假言推理) | $P \wedge (P \rightarrow Q) \Rightarrow Q$ |
| Modus tollens(拒取) | $\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P$ |
| Disjunctive syllogism(析取三段论) | $\neg P \wedge (P \vee Q) \Rightarrow Q$ |
| Hypothetical syllogism(假言三段论) | $(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow (P \rightarrow R)$ |
| Resolution (归结) | $(P \vee Q) \wedge (\neg P \vee R) \Rightarrow Q \vee R$ |

| *Rule of Inference* | *Tautology* |
|---|---|
| $p$<br>$p \rightarrow q$<br>$\therefore q$ | $(p \wedge (p \rightarrow q)) \rightarrow q$ |
| $\neg q$<br>$p \rightarrow q$<br>$\therefore \neg p$ | $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ |
| $p \rightarrow q$<br>$q \rightarrow r$<br>$\therefore p \rightarrow r$ | $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ |
| $p \vee q$<br>$\neg p$<br>$\therefore q$ | $((p \vee q) \wedge \neg p) \rightarrow q$ |
| $p$<br>$\therefore p \vee q$ | $p \rightarrow (p \vee q)$ |
| $p \wedge q$<br>$\therefore p$ | $(p \wedge q) \rightarrow p$ |
| $p$<br>$q$<br>$\therefore p \wedge q$ | $((p) \wedge (q)) \rightarrow (p \wedge q)$ |
| $p \vee q$<br>$\neg p \vee r$<br>$\therefore q \vee r$ | $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$ |

# Building Arguments

**QUESTION:** Given the premises $P_1, \dots, P_n$, show a conclusion $Q$, that is, show that $P_1 \wedge \cdots \wedge P_n \Rightarrow Q$.

| Name | Operations |
| ---: | --- |
| Premise | Introduce the given formulas $P_1, \dots, P_n$ in the process of constructing proofs. |
| Conclusion | Quote the intermediate formula that have been deducted. |
| Rule of replacement | Replace a formula with a logically equivalent formula. |
| Rules of Inference | Deduct a new formula with a tautological implication. |
| Rule of substitution | Deduct a formula from a tautology. |

# Building Arguments

**EXAMPLE**: Show that the premises 1, 2, 3, and 4 lead to conclusion 5.

1. "It is not sunny this afternoon and it is colder than yesterday,"
2. "We will go swimming only if it is sunny,"
3. "If we do not go swimming, then we will take a canoe trip,"
4. "If we take a canoe trip, then we will be home by sunset"
5. "We will be home by sunset."

- **Translating the premises and the conclusion into formulas. Let**
  - $p$: "It is sunny this afternoon"
  - $q$: "It is colder than yesterday"
  - $r$: "We will go swimming"
  - $s$: "We will take a canoe trip"
  - $t$: "We will be home by sunset"
    - The premises are $\neg p \wedge q, r \rightarrow p, \neg r \rightarrow s$, and $s \rightarrow t$.
    - The conclusion is $t$.
- **Question: ?**$(\neg p \wedge q) \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge ( s \rightarrow t) \Rightarrow t$
  - Can be proven with truth table. 32 rows!

# Building Arguments

**EXAMPLE**: Show that the premises 1, 2, 3, and 4 lead to conclusion 5.

1. "It is not sunny this afternoon and it is colder than yesterday,"
2. "We will go swimming only if it is sunny,"
3. "If we do not go swimming, then we will take a canoe trip,"
4. "If we take a canoe trip, then we will be home by sunset"
5. "We will be home by sunset."

- **Show that** $(\neg p \land q) \land (r \to p) \land (\neg r \to s) \land (s \to t) \Rightarrow t$

| | | |
|---|---|---|
| (1) | $\neg p \land q$ | Premise |
| (2) | $\neg p$ | Simplification using (1) |
| (3) | $r \to p$ | Premise |
| (4) | $\neg r$ | Modus tollens using (2) and (3) |
| (5) | $\neg r \to s$ | Premise |
| (6) | $s$ | Modus ponens using (4) and (5) |
| (7) | $s \to t$ | Premise |
| (8) | $t$ | Modus ponens using (6) and (7) |

# Building Arguments

**EXAMPLE**: Show that $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S) \Rightarrow S \vee R$

| | | |
|---|---|---|
| (1) | $P \vee Q$ | Premise |
| (2) | $\neg P \rightarrow Q$ | Rule of replacement applied to (1) |
| (3) | $Q \rightarrow S$ | Premise |
| (4) | $\neg P \rightarrow S$ | Hypothetical syllogism applied to (2) and (3) |
| (5) | $\neg S \rightarrow P$ | Rule of replacement applied to (4) |
| (6) | $P \rightarrow R$ | Premise |
| (7) | $\neg S \rightarrow R$ | Hypothetical syllogism applied to (5) and (6) |
| (8) | $S \vee R$ | Rule of replacement applied to (7) |