南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

# CS201 DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

# Important Logical Equivalences

- *Identity laws*
  - $p \wedge T \equiv p$
  - $p \vee F \equiv p$
- *Domination laws*
  - $p \vee T \equiv T$
  - $p \wedge F \equiv F$
- *Idempotent laws*
  - $p \vee p \equiv p$
  - $p \wedge p \equiv p$

# Important Logical Equivalences

- *Double negation laws*
  - $\neg(\neg p) \equiv p$

- *Commutative laws*
  - $p \lor q \equiv q \lor p$
  - $p \land q \equiv q \land p$

- *Associative laws*
  - $(p \lor q) \lor r \equiv p \lor (q \lor r)$
  - $(p \land q) \land r \equiv p \land (q \land r)$

# Important Logical Equivalences

- *Distributive laws*
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- *De Morgan's laws*
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
- *Others*
  - $p \vee (p \wedge q) \equiv p$
  - $p \wedge (p \vee q) \equiv p$

    *Absorption laws*
  - $p \vee \neg p \equiv T$
  - $p \wedge \neg p \equiv F$

    *Negation laws*
  - $p \rightarrow q \equiv \neg p \vee q$

    *Useful law*

# Using Logical Equivalences

- Equivalences can be used in proofs. A proposition or its part can be transformed using equivalences.

# Using Logical Equivalences

- Equivalences can be used in proofs. A proposition or its part can be transformed using equivalences.

- **Example**: Show that $\neg(p \oplus q)$ is equivalent to $p \leftrightarrow q$.

# Using Logical Equivalences

- Equivalences can be used in proofs. A proposition or its part can be transformed using equivalences.

- **Example**: Show that $\neg(p \oplus q)$ is equivalent to $p \leftrightarrow q$.

  **Proof**:
$$
\begin{aligned}
\neg(p \oplus q) &\equiv \neg((p \wedge \neg q) \vee (\neg p \wedge q)) && \text{Definition} \\
&\equiv \neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q) && \text{De Morgan's} \\
&\equiv (\neg p \vee \neg\neg q) \wedge (\neg\neg p \vee \neg q) && \text{De Morgan's} \\
&\equiv (\neg p \vee q) \wedge (p \vee \neg q) && \text{Double Negation} \\
&\equiv (p \rightarrow q) \wedge (q \rightarrow p) && \text{Useful} \\
&\equiv p \leftrightarrow q && \text{Definition}
\end{aligned}
$$

# Negation of Quantifiers

- Sentence: Nothing is perfect.
  - translation: $\neg\exists x\ \mathit{Perfect}(x)$

# Negation of Quantifiers

- Sentence: Nothing is perfect.
  - ◇ translation: $\neg\exists x\ Perfect(x)$
  - ◇ translation: $\forall x\ \neg Perfect(x)$ (Everything is imperfect.)

# Negation of Quantifiers

- Sentence: Nothing is perfect.
  - ◇ translation: $\neg\exists x\ \mathit{Perfect}(x)$
  - ◇ translation: $\forall x\ \neg\mathit{Perfect}(x)$
    (Everything is imperfect.)

**Conclusion**: $\neg\exists x\ P(x)$ is equivalent to $\forall x\ \neg P(x)$

# Negation of Quantifiers

- Sentence: Not all horses are white.
  - translation: $\neg\forall x\ (Horse(x) \rightarrow White(x))$

# Negation of Quantifiers

- Sentence: Not all horses are white.
  - ◇ translation: $\neg\forall x\ (Horse(x) \rightarrow White(x))$
  - ◇ translation: $\exists x\ (Horse(x) \wedge \neg White(x))$
    (There is a horse that is not white.)

# Negation of Quantifiers

- Sentence: Not all horses are white.
  - ◇ translation: $\neg\forall x\ (Horse(x) \rightarrow White(x))$
  - ◇ translation: $\exists x\ (Horse(x) \wedge \neg White(x))$
    (There is a horse that is not white.)
  - ◇ logically equivalent to
    $\exists x\ \neg(Horse(x) \rightarrow White(x))$

# Negation of Quantifiers

- Sentence: Not all horses are white.
  - ◇ translation: $\neg\forall x\ (Horse(x) \rightarrow White(x))$
  - ◇ translation: $\exists x\ (Horse(x) \wedge \neg White(x))$
    (There is a horse that is not white.)
  - ◇ logically equivalent to
    $\exists x\ \neg(Horse(x) \rightarrow White(x))$

**Conclusion**: $\neg\forall x\ P(x)$ is equivalent to $\exists x\ \neg P(x)$

# Negation of Quantified Statements

- a.k.a. De Morgan laws for quantifiers

| Negation | Equivalent Statement | When Is Negation True? | When False? |
|---|---|---|---|
| $\neg \exists x\ P(x)$ | $\forall x\ \neg P(x)$ | For every $x$, $P(x)$ is false. | There is an $x$ for which $P(x)$ is true. |
| $\neg \forall x\ P(x)$ | $\exists x\ \neg P(x)$ | There is an $x$ for which $P(x)$ is false. | $P(x)$ is true for every $x$. |

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

  **Example 1**: "Every real number has its corresponding negative."

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

**Example 1**: "Every real number has its corresponding negative."

- ◇ a real number is denoted by $x$ and its negative as $y$
- ◇ a predicate $P(x, y)$ denotes "$x + y = 0$"

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

  **Example 1**: "Every real number has its corresponding negative."

  - a real number is denoted by $x$ and its negative as $y$
  - a predicate $P(x, y)$ denotes "$x + y = 0$"

  $\forall x \exists y \; P(x, y)$

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

  **Example 2**: "There is a person who loves everybody."

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

  **Example 2**: "There is a person who loves everybody."

  - variables $x$ and $y$ denote people
  - a predicate $L(x, y)$ denotes "$x$ loves $y$"

# Nested Quantifiers

- More than one quantifier may be necessary to capture the meaning of a statement in the predicate logic.

**Example 2**: "There is a person who loves everybody."

◇ variables $x$ and $y$ denote people

◇ a predicate $L(x, y)$ denotes "$x$ loves $y$"

$$\exists x \forall y \; L(x, y)$$

# Order of Quantifiers

- The order of nested quantifiers matters if quantifiers are of different type.

# Order of Quantifiers

- The order of nested quantifiers matters if quantifiers are of different type.

  **Example**: $\forall x \exists y\ L(x, y) \neq \exists y \forall x\ L(x, y)$

  - $L(x, y)$ denotes "$x$ loves $y$"

# Order of Quantifiers

- The order of nested quantifiers matters if quantifiers are of different type.

**Example**: $\forall x \exists y\ L(x, y) \not\equiv \exists y \forall x\ L(x, y)$

◇ $L(x, y)$ denotes "$x$ loves $y$"

◇ $\forall x \exists y\ L(x, y)$: Everybody loves somebody.

◇ $\exists y \forall x\ L(x, y)$: There is someone who is loved by everyone.

# Order of Quantifiers

- The order of nested quantifiers does no matter if quantifiers are of the same type.

# Order of Quantifiers

- The order of nested quantifiers does no matter if quantifiers are of the same type.

  **Example**: $\forall x \forall y\ (Parent(x, y) \rightarrow Child(y, x))$

  - ◇ For all $x$ and $y$, if $x$ is a parent of $y$ then $y$ is a child of $x$

# Order of Quantifiers

- The order of nested quantifiers does no matter if quantifiers are of the same type.

**Example**: $\forall x \forall y\ (Parent(x, y) \rightarrow Child(y, x))$

- ◇ For all $x$ and $y$, if $x$ is a parent of $y$ then $y$ is a child of $x$

- ◇ $\forall x \forall y\ (Parent(x, y) \rightarrow Child(y, x))$
- ◇ $\forall y \forall x\ (Parent(x, y) \rightarrow Child(y, x))$

# Translation Exercise

- Suppose that variables $x, y$ denote people, and $L(x, y)$ denotes $x$ loves $y$.

**Translate**:

- Everybody loves Raymond.
- Everybody loves somebody.
- There is somebody whom everybody loves.
- There is somebody whom Raymond doesn't love.
- There is somebody whom no one loves.

# Translation Exercise

- Suppose that variables $x, y$ denote people, and $L(x, y)$ denotes $x$ loves $y$.

**Translate**:

- Everybody loves Raymond. $\forall x\ L(x, Raymond)$
- Everybody loves somebody. $\forall x \exists y\ L(x, y)$
- There is somebody whom everybody loves.
  $\exists y \forall x\ L(x, y)$
- There is somebody whom Raymond doesn't love.
  $\exists y\ \neg L(Raymond, y)$
- There is somebody whom no one loves.
  $\exists y \forall x\ \neg L(x, y)$

# Translation Exercise

- Suppose that variables $x, y$ denote people, and $L(x, y)$ denotes $x$ loves $y$.

  **Translate**:

  - Everybody loves Raymond. $\forall x\ L(x, Raymond)$
  - Everybody loves somebody. $\forall x \exists y\ L(x, y)$
  - There is somebody whom everybody loves.
    $\exists y \forall x\ L(x, y)$
  - There is somebody whom Raymond doesn't love.
    $\exists y\ \neg L(Raymond, y)$
  - There is somebody whom no one loves.
    $\exists y \forall x\ \neg L(x, y)$

  - There is exactly one person whom everybody loves.

# Translation Exercise

- Suppose that variables $x, y$ denote people, and $L(x, y)$ denotes $x$ loves $y$.

  **Translate**:

  - Everybody loves Raymond. $\forall x\ L(x, Raymond)$
  - Everybody loves somebody. $\forall x \exists y\ L(x, y)$
  - There is somebody whom everybody loves.
    $\exists y \forall x\ L(x, y)$
  - There is somebody whom Raymond doesn't love.
    $\exists y\ \neg L(Raymond, y)$
  - There is somebody whom no one loves.
    $\exists y \forall x\ \neg L(x, y)$
  - There is exactly one person whom everybody loves.
    $\exists y(\forall x L(x, y) \wedge \forall z(\forall x L(x, z) \to z = y))$

# Quantifications of Two Variables

| Statement | When True? | When False |
|---|---|---|
| $\forall x \forall y P(x,y)$ <br> $\forall y \forall x P(x,y)$ | $P(x,y)$ is true for every pair $x,y$. | There is a pair $x$, $y$ for which $P(x,y)$ is false. |
| $\forall x \exists y P(x,y)$ | For every $x$ there is a $y$ for which $P(x,y)$ is true. | There is an x such that $P(x,y)$ is false for every $y$. |
| $\exists x \forall y P(x,y)$ | There is an $x$ for which $P(x,y)$ is true for every $y$. | For every $x$ there is a y for which $P(x,y)$ is false. |
| $\exists x \exists y P(x,y)$ <br> $\exists y \exists x P(x,y)$ | There is a pair $x$, $y$ for which $P(x,y)$ is true. | $P(x,y)$ is false for every pair $x,y$ |

# Negating Nested Quantifiers

- Sentence: for every real number $x$, there exists a real number $y$ such that $xy = 1$.

# Negating Nested Quantifiers

- Sentence: for every real number $x$, there exists a real number $y$ such that $xy = 1$.
    - $\forall x \exists y\ (xy = 1)$

# Negating Nested Quantifiers

- Sentence: for every real number $x$, there exists a real number $y$ such that $xy = 1$.

  ◇ $\forall x \exists y\ (xy = 1)$

$$
\begin{aligned}
& \neg \forall x \exists y\ (xy = 1) \\
\equiv\ & \exists x \neg \exists y\ (xy = 1) \\
\equiv\ & \exists x \forall y\ \neg (xy = 1) \\
\equiv\ & \exists x \forall y\ (xy \neq 1)
\end{aligned}
$$

# Theorems and Proofs

- An *axiom* or *postulate* is a statement or proposition which is regarded as being established, accepted, or self-evidently true.

# Theorems and Proofs

- An *axiom* or *postulate* is a statement or proposition which is regarded as being established, accepted, or self-evidently true.

  **Example**:

  ◇ A straight line segment can be drawn joining any two points.

# Theorems and Proofs

- An *axiom* or *postulate* is a statement or proposition which is regarded as being established, accepted, or self-evidently true.

  **Example**:

  ◇ A straight line segment can be drawn joining any two points.

- A *theorem* is a statement that can be proved to be true.

# Theorems and Proofs

- An *axiom* or *postulate* is a statement or proposition which is regarded as being established, accepted, or self-evidently true.

  **Example**:

  ◇ A straight line segment can be drawn joining any two points.

- A *theorem* is a statement that can be proved to be true.

  **Example**:

  ◇ There are infinitely many prime numbers.

# Theorems and Proofs

- An *axiom* or *postulate* is a statement or proposition which is regarded as being established, accepted, or self-evidently true.

  **Example**:

  ◇ A straight line segment can be drawn joining any two points.

- A *theorem* is a statement that can be proved to be true.

  **Example**:

  ◇ There are infinitely many prime numbers.

- A *lemma* is a statement that can be proved to be true, and is used in proving a theorem or proposition.

# Theorems and Proofs

Journal of Combinatorial Theory, Series A 131 (2015) 61–70

ELSEVIER

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Journal of Combinatorial Theory

Difference balanced functions and their generalized difference sets

CrossMark

Alexander Pott [a], Qi Wang [b,1]

[a] *Institute of Algebra and Geometry, Faculty of Mathematics, Otto-von-Guericke University Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany*

[b] *Department of Electrical and Electronic Engineering, South University of Science and Technology of China, Nanshan Shenzhen 518055, Guangdong, China*

# Theorems and Proofs

Journal of Combinatorial Theory, Series A 131 (2015) 61–70

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta


**Lemma 3.1.** *(See [16].) For $q = p$ prime, every difference balanced function $f$ from $\mathbb{F}_{p^n}^*$ to $\mathbb{F}_p$ must be balanced, or an affine shift of a balanced function.*

**Remark 3.2.** Without loss of generality, we may always assume that a difference balanced function $f$ from $\mathbb{F}_{p^n}^*$ to $\mathbb{F}_p$ is balanced (otherwise, replace $f$ by $f - b$ for a suitable $b \in \mathbb{F}_p^*$).

By Lemma 3.1, $(1, t)$ is a multiplier of $D$ implies that $D^{(1,t)} = (a_t, 0)D$ for some $a_t \in \mathbb{F}_{p^n}^*$ by the balance property. Then the equivalence relation in Theorem 2.2 could be formulated as follows for $q = p$ prime.

**Corollary 3.3.** *Suppose that $D := \{(x, f(x)) : x \in \mathbb{F}_{p^n}^*\} \subseteq G = (\mathbb{F}_{p^n}^*, \cdot) \times (\mathbb{F}_p, +)$, where $f : \mathbb{F}_{p^n}^* \to \mathbb{F}_p$ is difference balanced. Then $(1, t)$ is a multiplier of $D$ for every $t \in \mathbb{F}_p^*$ if and only if $f$ is a $d$-homogeneous function for some $d$ with $\gcd(d, p-1) = 1$.*

# Theorems and Proofs

Journal of Combinatorial Theory, Series A 131 (2015) 61–70

**Theorem 3.5.** *Let $D = \{(x, f(x)) : x \in \mathbb{F}_{p^n}^*\}$ be a difference set satisfying (2.1) in the group $G = N_2 \times N_1$, where $N_2 = (\mathbb{F}_{p^n}^*, \cdot)$, $N_1 = (\mathbb{F}_p, +)$ and $p$ is a prime. Then $(1, t)$ is a multiplier of $D$ for every $t \in \mathbb{F}_p^*$.*

**Proof.** We may assume that $f$ is balanced, see Remark 3.2: Note that the difference sets defined by $f$ and by affine shifts $f - b$ admit the same multipliers. Let $w = (p^n - 1)p$, let $\zeta_p$ be a complex $p$-th root of unity, and $\zeta_{p^n-1}$ be a complex $(p^n - 1)$-st root of unity. In the ring $\mathbb{Z}[\zeta_p, \zeta_{p^n-1}]$, the prime ideal $(p)$ decomposes as $(p) = (\pi_1 \dots \pi_v)^{\phi(p)}$, where the $\pi_i$'s are distinct prime ideals and $v = \phi(p^n - 1)/n$ (see [12]). If $\chi$ is a character of $N_2 \times N_1$ and $1 \le t \le p - 1$, then

$$\chi\big((x, y)^{(1,t)}\big) = \chi(x, ty) \equiv \chi(x, y) \pmod{p},$$

since the ring automorphism induced by $\zeta_p \mapsto \zeta_p^t$ and $\zeta_{p^n-1} \mapsto \zeta_{p^n-1}$ fixes the ideals $\pi_i$ (see [12], again). Therefore by (2.2), we have

$$\chi\big(D^{(1,t)}\big)\chi\big(D^{(-1)}\big) \equiv \chi(D)\chi\big(D^{(-1)}\big) \equiv 0 \pmod{p^n}$$

# Theorems and Proofs

- To show the truth value of such a statement following from other statements, we need to provide a correct supporting argument (*proof*)

# Theorems and Proofs

- To show the truth value of such a statement following from other statements, we need to provide a correct supporting argument (*proof*)

- Important questions:
  - ◇ Why is the argument correct?
  - ◇ How to construct a correct argument?

# Theorems and Proofs

- Typically, a theorem looks like this:

$$\underbrace{(p_1 \wedge p_2 \wedge \ldots \wedge p_n)}_{\text{premises}} \rightarrow \underbrace{q}_{\text{conclusion}}$$

# Theorems and Proofs

- Typically, a theorem looks like this:

$$\underbrace{(p_1 \wedge p_2 \wedge \ldots \wedge p_n)}_{\text{premises}} \to \underbrace{q}_{\text{conclusion}}$$

**Example**: (Fermat's little theorem)

◇ If $p$ is a prime and $a$ is an integer not divisible by $p$, then $a^{p-1} \equiv 1 \pmod{p}$.

# Formal Proofs

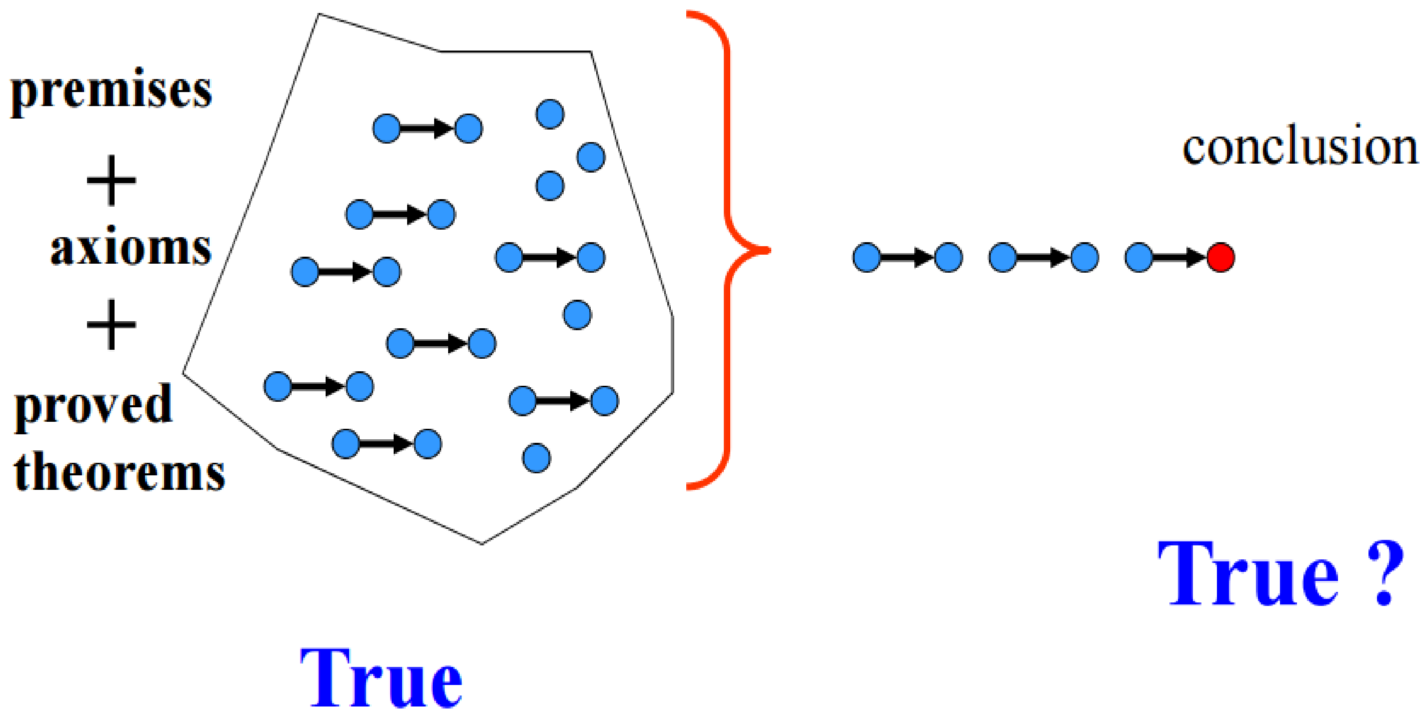
- A *proof* provides an argument supporting the validity of the statement, and may use premises, axioms, lemmas, results of other theorems, etc.

- In *formal proofs*, steps follow logically from the set of premises, axioms, lemmas, and other theorems.

# Formal Proofs

- A *proof* provides an argument supporting the validity of the statement, and may use premises, axioms, lemmas, results of other theorems, etc.

- In *formal proofs*, steps follow logically from the set of premises, axioms, lemmas, and other theorems.



# Using Logical Equivalence Rules

- (Proofs based on logical equivalences): A proposition can be transformed using a sequence of equivalence rewrites until some conclusion can be reached.

# Using Logical Equivalence Rules

- (Proofs based on logical equivalences): A proposition can be transformed using a sequence of equivalence rewrites until some conclusion can be reached.

**Example**: Show that $(p \wedge q) \to p$ is a tautology.

**Proof**: 

| | |
|---|---|
| $(p \wedge q) \to p \equiv \neg(p \wedge q) \vee p$ | Useful |
| $\equiv (\neg p \vee \neg q) \vee p$ | De Morgan's |
| $\equiv (\neg q \vee \neg p) \vee p$ | Commutative |
| $\equiv \neg q \vee (\neg p \vee p)$ | Associative |
| $\equiv \neg q \vee T$ | Negation |
| $\equiv T$ | Domination |

# Rules of Inference for Propositional Logic

- Allow us to infer new true statements from existing true statements.
- Represent logically valid inference patterns

# Rules of Inference for Propositional Logic

- Allow us to infer new true statements from existing true statements.
- Represent logically valid inference patterns
- **modus ponens** (*law of detachment*) 肯定前件式

$$\begin{array}{l} p \rightarrow q \\ p \\ \hline \therefore q \end{array}$$

corresponding tautology:
$(p \wedge (p \rightarrow q)) \rightarrow q$

# Rules of Inference for Propositional Logic

- Allow us to infer new true statements from existing true statements.
- Represent logically valid inference patterns
- **modus ponens** (*law of detachment*) 肯定前件式

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

corresponding tautology:
$(p \wedge (p \to q)) \to q$

**Example**:

$p$ – "It is raining."
$q$ – "I will study discrete math."

$p \to q$ – "If it is raining, then I will study discrete math."
$p$ – "It is raining."

$q$ – "Therefore, I will study discrete math."

# Rules of Inference for Propositional Logic

- **modus tollens** 否定后件式

$$\begin{array}{c} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

corresponding tautology:
$(\neg q \wedge (p \to q)) \to \neg p$

- **hypothetical syllogism** 假言三段论

$$\begin{array}{c} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

corresponding tautology:
$((p \to q) \wedge (q \to r)) \to (p \to r)$

# Rules of Inference for Propositional Logic

- **disjunctive syllogism** 选言三段论

$$\begin{array}{l} p \lor q \\ \neg p \\ \hline \therefore q \end{array}$$

corresponding tautology:
$(\neg p \land (p \lor q)) \to q$

- **Addition**

$$\begin{array}{l} p \\ \hline \therefore p \lor q \end{array}$$

corresponding tautology:
$p \to (p \lor q)$

- **Simplification**

$$\begin{array}{l} p \land q \\ \hline \therefore q \end{array}$$

corresponding tautology:
$(p \land q) \to p$

# Rules of Inference for Propositional Logic

## Conjunction

$$\begin{array}{l} p \\ q \\ \hline \therefore p \land q \end{array}$$

corresponding tautology:
$((p) \land (q)) \to (p \land q)$

## Resolution

$$\begin{array}{l} \neg p \lor r \\ p \lor q \\ \hline \therefore q \lor r \end{array}$$

corresponding tautology:
$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$

# Applying Rules of Inference for Propositional Logic

- "It is not sunny this afternoon and it is colder than yesterday."

  "We will go swimming only if it is sunny."

  "If we do not go swimming then we will take a canoe trip."

  "If we take a canoe trip, then we will be home by sunset."

  Show that all these lead to a conclusion:
  - We will be home by sunset.

# Applying Rules of Inference for Propositional Logic

- "It is not sunny this afternoon and it is colder than yesterday."

  "We will go swimming only if it is sunny."

  "If we do not go swimming then we will take a canoe trip."

  "If we take a canoe trip, then we will be home by sunset."

  Show that all these lead to a conclusion:
  - ◇ We will be home by sunset.

  $p$ – 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.

# Applying Rules of Inference for Propositional Logic

- "It is not sunny this afternoon and it is colder than yesterday."
  $\neg p \wedge q$

  "We will go swimming only if it is sunny."
  $r \rightarrow p$

  "If we do not go swimming then we will take a canoe trip."
  $\neg r \rightarrow s$

  "If we take a canoe trip, then we will be home by sunset."
  $s \rightarrow t$

  Show that all these lead to a conclusion:
  - We will be home by sunset. $t$

$p$ – 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.

# Applying Rules of Inference for Propositional Logic

- Translation:
  - ◇ premises: $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
  - ◇ conclusion: $t$

# Applying Rules of Inference for Propositional Logic

- Translation:
  - premises: $\neg p \land q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
  - conclusion: $t$

**Proof**:

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

# Rules of Inference for Quantified Statements

- **Universal Instantiation** (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

- **Universal Generalization** (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

- **Existential Instantiation** (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

- **Existential Generalization** (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

# Applying Rules of Inference for Quantified Statements

- "A student in this class has not read the book."

  "Everyone in this class passed the first exam."

  Show that all these lead to a conclusion:
  - Someone who passed the first exam has not read the book.

# Applying Rules of Inference for Quantified Statements

- "A student in this class has not read the book."

  "Everyone in this class passed the first exam."

  Show that all these lead to a conclusion:
  - Someone who passed the first exam has not read the book.

$C(x)$ – $x$ is in this class.
$B(x)$ – $x$ has read the book.
$P(x)$ – $x$ passed the first exam.

# Applying Rules of Inference for Quantified Statements

- "A student in this class has not read the book."

  $\exists x(C(x) \land \neg B(x))$

  "Everyone in this class passed the first exam."

  $\forall x(C(x) \to P(x))$

  Show that all these lead to a conclusion:

  - Someone who passed the first exam has not read the book.

  $\exists x(P(x) \land \neg B(x))$

$C(x)$ – $x$ is in this class.
$B(x)$ – $x$ has read the book.
$P(x)$ – $x$ passed the first exam.

# Applying Rules of Inference for Quantified Statements

- Translation:
  - ◇ premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \rightarrow P(x))$
  - ◇ conclusion: $\exists x(P(x) \wedge \neg B(x))$

# Applying Rules of Inference for Quantified Statements

- Translation:
  - premises: $\exists x(C(x) \wedge \neg B(x))$, $\forall x(C(x) \rightarrow P(x))$
  - conclusion: $\exists x(P(x) \wedge \neg B(x))$

**Proof**:

| Step | Reason |
|---|---|
| 1. $\exists x(C(x) \wedge \neg B(x))$ | Premise |
| 2. $C(a) \wedge \neg B(a)$ | EI from (1) |
| 3. $C(a)$ | Simplification from (2) |
| 4. $\forall x(C(x) \rightarrow P(x))$ | Premise |
| 5. $C(a) \rightarrow P(a)$ | UI from (4) |
| 6. $P(a)$ | MP from (3) and (5) |
| 7. $\neg B(a)$ | Simplification from (2) |
| 8. $P(a) \wedge \neg B(a)$ | Conj from (6) and (7) |
| 9. $\exists x(P(x) \wedge \neg B(x))$ | EG from (8) |

# Informal Proofs

- Proving theorems in practice:

  ◇ The steps of the proofs are not expressed in any formal language of logic.

  ◇ One must always watch the *consistency* of the argument made, logic and its rules can often help us to decide the soundness of the argument.

# Informal Proofs

- Proving theorems in practice:

  ◇ The steps of the proofs are not expressed in any formal language of logic.

  ◇ One must always watch the *consistency* of the argument made, logic and its rules can often help us to decide the soundness of the argument.

- We use (*informal*) proofs to illustrate different methods of proving theorems.

# Methods of Proving Theorems

- Basic methods to prove theorems:
  - *direct proof*
    - $p \rightarrow q$ is proved by showing that if $p$ is true then $q$ follows
  - *proof by contrapositive*
    - show the contrapositive $\neg q \rightarrow \neg p$
  - *proof by contradiction*
    - show that $(p \wedge \neg q)$ contradicts the assumptions
  - *proof by cases*
    - give proofs for all possible cases
  - *proof of equivalence*
    - $p \leftrightarrow q$ is replaced with $(p \rightarrow q) \wedge (q \rightarrow p)$

# Direct Proof

- $p \to q$ is proved by showing that if $p$ is true then $q$ follows

# Direct Proof

- $p \rightarrow q$ is proved by showing that if $p$ is true then $q$ follows

**Example**: Prove that "if $n$ is odd, then $n^2$ is odd"

# Direct Proof

- $p \to q$ is proved by showing that if $p$ is true then $q$ follows

**Example**: Prove that "if $n$ is odd, then $n^2$ is odd"

**Proof**:

Assume that (the hypothesis is true, i.e., $n$ is odd)
$n = 2k + 1$ where $k$ is an integer.
Then

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$

Therefore, $n^2$ is odd.

# Proof by Contrapositive

- $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$

# Proof by Contrapositive

- $p \rightarrow q$ is proved by showing the contrapositive $\neg q \rightarrow \neg p$

**Example**: Prove that "if $3n + 2$ is odd, then $n$ is odd"

# Proof by Contrapositive

- $p \to q$ is proved by showing the contrapositive $\neg q \to \neg p$

**Example**: Prove that "if $3n + 2$ is odd, then $n$ is odd"

**Proof**:

Assume that $n$ is even, i.e., $n = 2k$, where $k$ is an integer. Then

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$.

Therefore, $3n + 2$ is even.

# Proof by Contradiction

- Assume that $p$ is true but $q$ is false ($p \wedge \neg q$). Then show a contradiction to $p$, or $\neg q$, or other settled results.

# Proof by Contradiction

- Assume that $p$ is true but $q$ is false ($p \wedge \neg q$). Then show a contradiction to $p$, or $\neg q$, or other settled results.

  **Example**: Prove that "if $3n + 2$ is odd, then $n$ is odd"

# Proof by Contradiction

- Assume that $p$ is true but $q$ is false ($p \wedge \neg q$). Then show a contradiction to $p$, or $\neg q$, or other settled results.

**Example**: Prove that "if $3n+2$ is odd, then $n$ is odd"

**Proof**:

Assume that $3n+2$ is odd and $n$ is even, i.e., $n = 2k$, where $k$ is an integer. Then

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$.

Thus, $3n+2$ is even. This is a contradiction to the assumption that $3n+2$ is odd. Therefore, $n$ is odd.

# Proof by Cases

- We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$. Why?

# Proof by Cases

- We want to show $(p_1 \lor p_2 \lor \ldots \lor p_n) \to q$. This is equivalent to $(p_1 \to q) \land (p_2 \to q) \land \ldots \land (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \lor p_2 \lor \ldots \lor p_n) \to q \\
\equiv\ & \neg(p_1 \lor p_2 \lor \ldots \lor p_n) \lor q \\
\equiv\ & (\neg p_1 \land \neg p_2 \land \ldots \land \neg p_n) \lor q \\
\equiv\ & (\neg p_1 \lor q) \land (\neg p_2 \lor q) \land \ldots \land (\neg p_n \lor q) \\
\equiv\ & (p_1 \to q) \land (p_2 \to q) \land \ldots \land (p_n \to q)
\end{aligned}
$$

# Proof by Cases

- We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\
\equiv\ & \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \\
\equiv\ & (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \\
\equiv\ & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \\
\equiv\ & (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)
\end{aligned}
$$

**Example**: Prove that "$|x||y| = |xy|$ for real numbers $x, y$"

# Proof by Cases

- We want to show $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$. This is equivalent to $(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)$. Why?

$$
\begin{aligned}
& (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\
\equiv\ & \neg(p_1 \vee p_2 \vee \ldots \vee p_n) \vee q \\
\equiv\ & (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_n) \vee q \\
\equiv\ & (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \ldots \wedge (\neg p_n \vee q) \\
\equiv\ & (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)
\end{aligned}
$$

**Example**: Prove that "$|x||y| = |xy|$ for real numbers $x, y$"

**Proof**: Four cases:

- $\diamond$ $x \geq 0,\ \ y \geq 0$
- $\diamond$ $x \geq 0,\ \ y < 0$
- $\diamond$ $x < 0,\ \ y \geq 0$
- $\diamond$ $x < 0,\ \ y < 0$

# Proof of Equivalences

- To prove "$p \leftrightarrow q$", show $(p \rightarrow q) \wedge (q \rightarrow p)$.

# Proof of Equivalences

- To prove "$p \leftrightarrow q$", show $(p \rightarrow q) \wedge (q \rightarrow p)$.

**Example**: Prove that "An integer $n$ is odd if and only if $n^2$ is odd"

# Proof of Equivalences

- To prove "$p \leftrightarrow q$", show $(p \to q) \land (q \to p)$.

**Example**: Prove that "An integer $n$ is odd if and only if $n^2$ is odd"

**Proof**:

- ◇ proof of $p \to q$: direct proof
- ◇ proof of $q \to p$: proof by contrapositive

# Vacuous Proof

- To prove $p \to q$, suppose that $p$ (the hypothesis) is always false, then $p \to q$ is always true.

# Vacuous Proof

- To prove $p \to q$, suppose that $p$ (the hypothesis) is always false, then $p \to q$ is always true.

**Example**: $P(n)$ – "if $n > 1$ then $n^2 > n$". Show that $P(0)$

# Vacuous Proof

- To prove $p \rightarrow q$, suppose that $p$ (the hypothesis) is always false, then $p \rightarrow q$ is always true.

**Example**: $P(n)$ – "if $n > 1$ then $n^2 > n$". Show that $P(0)$

**Proof**: Since the premise $0 > 1$ is always false. Thus $P(0)$ is true.

# Trivial Proof

- To prove $p \rightarrow q$, suppose that $q$ (the conclusion) is always true, then $p \rightarrow q$ is always true.

# Trivial Proof

- To prove $p \rightarrow q$, suppose that $q$ (the conclusion) is always true, then $p \rightarrow q$ is always true.

**Example**: $P(n)$ – "if $a \geq b$ then $a^n \geq b^n$". Show that $P(0)$

# Trivial Proof

- To prove $p \to q$, suppose that $q$ (the conclusion) is always true, then $p \to q$ is always true.

**Example**: $P(n)$ – "if $a \geq b$ then $a^n \geq b^n$". Show that $P(0)$

**Proof**: Since the conclusion $a^0 \geq b^0$ is always true. Thus $P(0)$ is true.

# Proofs with Quantifiers

- **Universally quantified statements**
  - ◇ prove the property holds for all examples
    - – proof by cases to divide the proof into different parts
  - ◇ counterexamples
    - – disprove universal statements

## Proofs with Quantifiers

- **Existence proof**
  - ◇ constructive
    - – find a specific example to show the statement holds
  - ◇ nonconstructive
    - – proof by contradiction

# Proof Exercises

- Prove that "$\sqrt{2}$ is *irrational*". (*rational numbers* are those of the form $\frac{m}{n}$, where $m, n$ are integers.)

# Proof Exercises

- Prove that "$\sqrt{2}$ is *irrational*". (*rational numbers* are those of the form $\frac{m}{n}$, where $m, n$ are integers.)

**Proof**:

Suppose that $\sqrt{2}$ is rational. Then there exist two integers $m$ and $n$ such that $\gcd(m, n) = 1$ and $\sqrt{2} = m/n$. We have then $m^2 = 2n^2$. It then follows that $m$ is even. Let $m = 2k$ for some integer $k$. It then follows that $n^2 = 2k^2$. Hence, $n$ is also even. This means $\gcd(m, n)$ must have a factor 2, which contradicts to the assumption that $\gcd(m, n) = 1$.

# Proof Exercises

- Prove that "There are infinitely many prime numbers ".

# Proof Exercises

- Prove that "There are infinitely many prime numbers".

**Proof**:

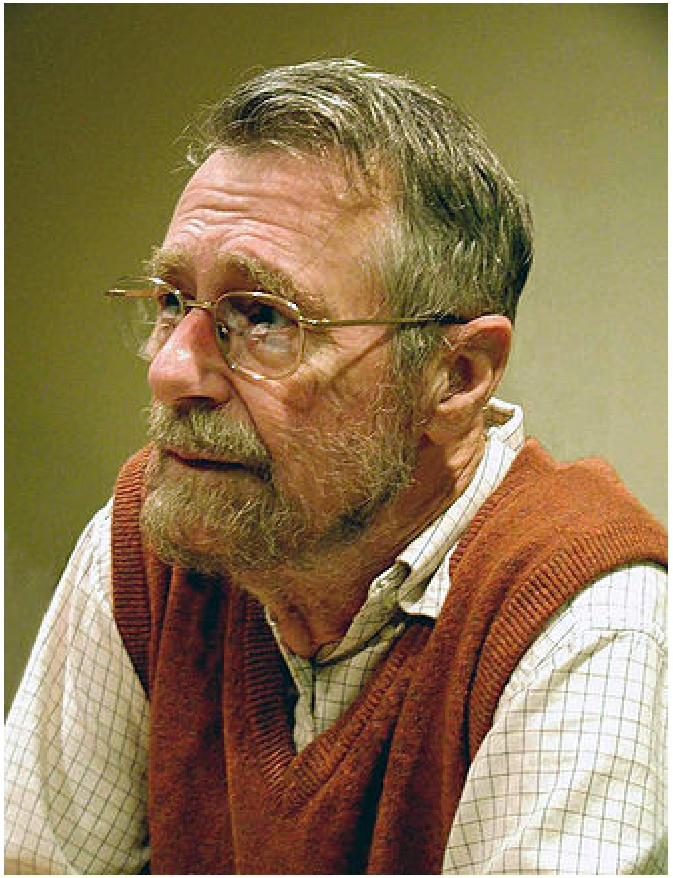
Suppose that there are only a finite number of primes. Then some prime number $p$ is the largest of all the prime numbers, and we can list the prime numbers in ascending order:

$2, 3, 5, 7, 11, \ldots, p.$

Let $n = (2 \times 3 \times 5 \times \cdots \times p) + 1$. Then $n > 1$, and $n$ cannot be divided by any prime number in the list above. This means that $n$ is also a prime. Clearly, $n$ is larger than all the primes in the list above. This is contrary to the assumption that all primes are in the list.

# Words from Dijkstra

Edsger W. Dijkstra
(1930–2002)



–"... mathematical logic is and must be the basis for software design. ... mathematical analysis of designs and specifications have become central activities in computer science research..."

# Next Lecture

- sets, functions ...