Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-09-27

Plan for Today

- **Textbook Chapter 3: Propositional Calculus**
  - Implication
  - Leibniz's Rule as an Axiom

CalcCheck-checked Mystery Steps

$$\begin{array}{ll} & p \equiv \neg q \equiv p \vee q \\ = & \langle \text{(3.32)}\ p \vee q \ \equiv\ p \vee \neg q \ \equiv\ p \rangle \\ & \neg p \vee \neg q \end{array}$$

?

$$\begin{array}{ll} & false \Rightarrow p \Rightarrow q \\ = & \langle \text{(3.75) } \textit{ex falso quodlibet} \ \ false \Rightarrow p \rangle \\ & false \quad \Rightarrow q \end{array}$$

?

$$\begin{array}{ll} & p \vee (q \equiv r) \equiv p \equiv p \equiv q \equiv r \equiv p \\ = & \langle \text{(3.35) Golden rule } \ p \wedge q \equiv p \equiv q \equiv p \vee q \rangle \\ & p \wedge (q \equiv r) \end{array}$$

?

$$\begin{array}{ll} & true \equiv p \equiv \neg p \\ = & \langle \text{(3.15)} \ \neg p \equiv p \equiv false \rangle \\ & false \end{array}$$

?

Some Important Implication Theorems

Args.		$\Rightarrow$	
F	F	T	If the moon is green, then $2 + 2 = 7$.
F	T	T	If the moon is green, then $1 + 1 = 2$.
T	F	F	If $1 + 1 = 2$, then the moon is green.
T	T	T	If $1 + 1 = 2$, then the sun is a star.

(3.71) **Reflexivity of $\Rightarrow$:** $p \Rightarrow p \quad \equiv \quad true$

(3.72) **Right-zero of $\Rightarrow$:** $p \Rightarrow true \quad \equiv \quad true$

(3.73) **Left-identity of $\Rightarrow$:** $true \Rightarrow p \quad \equiv \quad p$

(3.74) **Definition of $\neg$ from $\Rightarrow$:** $p \Rightarrow false \quad \equiv \quad \neg p$

(3.15) **Definition of $\neg$ from $\equiv$:** $\neg p \quad \equiv \quad p \equiv false$

(3.75) ***ex falso quodlibet:*** $false \Rightarrow p \quad \equiv \quad true$

(3.65) **Shunting:** $p \wedge q \ \Rightarrow \ r \quad \equiv \quad p \Rightarrow (q \Rightarrow r)$

(3.77) **Modus ponens:** $p \ \wedge \ (p \Rightarrow q) \quad \Rightarrow \quad q$

Do not be discouraged by the number of theorems. You do not have to memorize them all. It will suffice to become familiar with them and how they are organized, so you can find the ones you need when developing a proof, The more practice you have using the theorems, the more they will become your formal friends, who serve you in your mathematical work.

LADM p. 42

Implication

(3.57) **Axiom, Definition of Implication**: $\boxed{p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q}$

(3.58) **Axiom, Definition of Consequence**: $\boxed{p \Leftarrow q \quad\equiv\quad q \Rightarrow p}$

Rewriting Implication:

(3.59) (Alternative) **Definition of Implication**: $p \Rightarrow q \;\equiv\; \neg p \vee q$

(3.60) (Dual) **Definition of Implication**: $p \Rightarrow q \;\equiv\; p \wedge q \;\equiv\; p$

(3.61) **Contrapositive**: $p \Rightarrow q \quad\equiv\quad \neg q \Rightarrow \neg p$

The "Golden Rule" and Implication

(3.35) **Axiom, Golden rule**: $\boxed{p \wedge q \quad\equiv\quad p \equiv q \quad\equiv\quad p \vee q}$

Can be used as:

- $p \wedge q \quad = \quad (p \equiv q \quad\equiv\quad p \vee q)$
- $(p \equiv q) \quad = \quad (p \wedge q \quad\equiv\quad p \vee q)$
- ...
- $(p \wedge q \quad\equiv\quad p) \qquad\equiv\qquad (q \quad\equiv\quad p \vee q)$

(3.57) **Axiom, Definition of Implication**: $p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q$

(3.60) (Dual) **Definition of Implication**: $p \Rightarrow q \;\equiv\; p \wedge q \;\equiv\; p$

Weakening/Strengthening Theorems

"$p \Rightarrow q$" can be read "p is stronger-than-or-equivalent-to q"

"$p \Rightarrow q$" can be read "p is at least as strong as q"

(3.76a) $p \qquad \Rightarrow p \vee q$

(3.76b) $p \wedge q \qquad \Rightarrow p$

(3.76c) $p \wedge q \qquad \Rightarrow p \vee q$

(3.76d) $p \vee (q \wedge r) \qquad \Rightarrow p \vee q$

(3.76e) $p \wedge q \qquad \Rightarrow p \wedge (q \vee r)$

Implication Theorems 2

(3.62) $p \Rightarrow (q \equiv r) \quad \equiv \quad p \wedge q \quad \equiv \quad p \wedge r$

(3.63) **Distributivity of $\Rightarrow$ over $\equiv$:**

$$p \Rightarrow (q \equiv r) \quad \equiv \quad p \Rightarrow q \quad \equiv \quad p \Rightarrow r$$

(3.64) **Self-distributivity of $\Rightarrow$:**

$$p \Rightarrow (q \Rightarrow r) \quad \equiv \quad (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$$

(3.65) **Shunting:** $\quad p \wedge q \Rightarrow r \quad \equiv \quad p \Rightarrow (q \Rightarrow r)$

Some Property Names

Let $\odot$ and $\oplus$ be binary operators and $\square$ be a constant.

*($\odot$ and $\oplus$ and $\square$ are **metavariables** for operators.)*

- "**$\odot$ is symmetric**": $\quad x \odot y \;=\; y \odot x$
- "**$\odot$ is associative**": $\quad (x \odot y) \odot z \;=\; x \odot (y \odot z)$
- "**$\odot$ is mutually associative with $\oplus$** (from the left)":

$$(x \odot y) \oplus z \;=\; x \odot (y \oplus z)$$

For example:

- $+$ **is** mutually associative with $-$: $\quad (x + y) - z \;=\; x + (y - z)$
- $-$ **is not** mutually associative with $+$: $\quad (5 - 2) + 3 \neq 5 - (2 + 3)$

Some Property Names (ctd.)

Let $\odot$ and $\oplus$ be binary operators and $\square$ be a constant.

*($\odot$ and $\oplus$ and $\square$ are **metavariables** for operators.)*

- "**$\odot$ is symmetric**": $x \odot y \;=\; y \odot x$
- "**$\odot$ is associative**": $(x \odot y) \odot z \;=\; x \odot (y \odot z)$
- "**$\odot$ is mutually associative with $\oplus$** (from the left)":
$$(x \odot y) \oplus z \;=\; x \odot (y \oplus z)$$
- "**$\odot$ is idempotent**": $x \odot x \;=\; x$
- "**$\square$ is a unit/identity of $\odot$**": $\square \odot x \;=\; x$ and $x \odot \square \;=\; x$
- "**$\square$ is a zero of $\odot$**": $\square \odot x \;=\; \square$ and $x \odot \square \;=\; \square$
- "**$\odot$ distributes to the right over $\oplus$**":
$$x \odot (y \oplus z) \;=\; (x \odot y) \oplus (x \odot z)$$
- "**$\odot$ distributes to the left over $\oplus$**":
$$(y \oplus z) \odot x \;=\; (y \odot x) \oplus (z \odot x)$$
- "**$\odot$ distributes over $\oplus$**":

$\odot$ distributes to the right over $\oplus$ **and**
$\odot$ distributes to the left over $\oplus$

Implication Theorems 3

(3.66)	$p \wedge (p \Rightarrow q) \;\equiv\; p \wedge q$	$\langle \ldots \quad p \wedge q \equiv p \rangle$
(3.67)	$p \wedge (q \Rightarrow p) \;\equiv\; p$	$\langle \ldots \quad p \wedge q \equiv p \rangle$
(3.68)	$p \vee (p \Rightarrow q) \;\equiv\; true$	$\langle \ldots \quad \neg p \vee q \rangle$
(3.69)	$p \vee (q \Rightarrow p) \;\equiv\; q \Rightarrow p$	$\langle \ldots \quad p \vee q \equiv q \rangle$
(3.70)	$p \vee q \;\Rightarrow\; p \wedge q \;\equiv\; p \equiv q$	$\langle \ldots$ Golden Rule $\ldots \rangle$

Implication Theorems 4

(3.71)	**Reflexivity of $\Rightarrow$:**	$p \Rightarrow p \;\equiv\; true$
(3.72)	**Right-zero of $\Rightarrow$:**	$p \Rightarrow true \;\equiv\; true$
(3.73)	**Left-identity of $\Rightarrow$:**	$true \Rightarrow p \;\equiv\; p$
(3.74)	**Definition of $\neg$ from $\Rightarrow$:**	$p \Rightarrow false \;\equiv\; \neg p$
(3.75)	***ex falso quodlibet:***	$false \Rightarrow p \;\equiv\; true$

Implication Theorems 5

(3.77) **Modus ponens:** $p \wedge (p \Rightarrow q) \Rightarrow q$

(3.78) **Case analysis:** $(p \Rightarrow r) \wedge (q \Rightarrow r) \;\equiv\; (p \vee q \Rightarrow r)$

(3.79) **Case analysis:** $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \;\equiv\; r$

Implication Theorems 6

(3.80) **Mutual implication:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; p \equiv q$

(3.80b) **Reflexivity wrt. Equivalence:** $(p \equiv q) \Rightarrow (p \Rightarrow q)$

(3.81) **Antisymmetry:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\Rightarrow\; (p \equiv q)$

(3.82a) **Transitivity:** $(p \Rightarrow q) \wedge (q \Rightarrow r) \;\Rightarrow\; (p \Rightarrow r)$

(3.82b) **Transitivity:** $(p \equiv q) \wedge (q \Rightarrow r) \;\Rightarrow\; (p \Rightarrow r)$

(3.82c) **Transitivity:** $(p \Rightarrow q) \wedge (q \equiv r) \;\Rightarrow\; (p \Rightarrow r)$

One View of Relations

- Let T_1 and T_2 be two types.
- A function of type $T_1 \to T_2 \to \mathbb{B}$ can be considered as *one view of* a **relation from T_1 to T_2**
  - We will see a different view of relations later …
  - … and **the** way to switch between these views.
  - With such a way of switching, the two views “are the same” in colloquial mathematics
  - Therefore we will occasionally just use the term “relation” also for functions of types $T_1 \to T_2 \to \mathbb{B}$
- A function of type $T \to T \to \mathbb{B}$ may then be called **a relation on T**.
- We have seen:

$$\begin{aligned}
_=_ &: T \to T \to \mathbb{B}\\
_=_ &: \mathbb{Z} \to \mathbb{Z} \to \mathbb{B}\\
_=_ &: \mathbb{N} \to \mathbb{N} \to \mathbb{B}\\
\leq &: \mathbb{N} \to \mathbb{N} \to \mathbb{B}\\
\equiv &: \mathbb{B} \to \mathbb{B} \to \mathbb{B}\\
\Rightarrow &: \mathbb{B} \to \mathbb{B} \to \mathbb{B}
\end{aligned}$$

Order Relations

- Let T be a type.
- A relation $\_\leq\_$ on T is called:
  - **reflexive** iff $x \leq x$ is a theorem
  - **transitive** iff $x \leq y \Rightarrow y \leq z \Rightarrow x \leq z$ is a theorem
  - **antisymmetric** iff $x \leq y \Rightarrow y \leq x \Rightarrow x = y$ is a theorem
  - an **order** (or **ordering**) iff it is reflexive, transitive, and antisymmetric
- Orders you are familiar with:

$$\begin{array}{lcl} \_=\_ & : & T \to T \to \mathbb{B} \\ \_\leq\_ & : & \mathbb{Z} \to \mathbb{Z} \to \mathbb{B} \\ \_\geq\_ & : & \mathbb{Z} \to \mathbb{Z} \to \mathbb{B} \\ \_\leq\_ & : & \mathbb{N} \to \mathbb{N} \to \mathbb{B} \\ \_\geq\_ & : & \mathbb{N} \to \mathbb{N} \to \mathbb{B} \\ \_|\_ & : & \mathbb{N} \to \mathbb{N} \to \mathbb{B} \\ \_\equiv\_ & : & \mathbb{B} \to \mathbb{B} \to \mathbb{B} \\ \_\Rightarrow\_ & : & \mathbb{B} \to \mathbb{B} \to \mathbb{B} \\ \_\subseteq\_ & : & set(T) \to set(T) \to \mathbb{B} \end{array}$$

Implication as Order on Propositions

"$p \Rightarrow q$" can be read "p is stronger-than-or-equivalent-to q"

— similar to "$x \leq y$" as "x is less-or-equal y"
— similar to "$x \geq y$" as "x is greater-or-equal y"

"$p \Rightarrow q$" can be read "p is at least as strong as q" — similar to "$x \leq y$" as "x is at most y"
— similar to "$x \geq y$" as "x is at least y"

(3.57) **Axiom, Definition of** $\Rightarrow$ from disjunction: $p \Rightarrow q \;\equiv\; p \vee q \;\equiv\; q$

— defines the order from maximum: $p \Rightarrow q \;\equiv\; ((p \vee q) \;=\; q)$
— analogous to: $x \leq y \;\equiv\; ((x \uparrow y) \;=\; y)$
— analogous to: $k \mid n \;\equiv\; ((\mathsf{lcm}(k,n) \;=\; n)$

(3.60) (Dual) **Definition of** $\Rightarrow$ from conjunction: $p \Rightarrow q \;\equiv\; p \wedge q \;\equiv\; p$

— defines the order from minimum: $p \Rightarrow q \;\equiv\; ((p \wedge q) \;=\; p)$
— analogous to: $x \leq y \;\equiv\; ((x \downarrow y) \;=\; x)$
— analogous to: $k \mid n \;\equiv\; ((\mathsf{gcd}(k,n) \;=\; k)$

Leibniz's Rule as an Axiom

Recall the **inference rule** (scheme):

(1.5) **Leibniz:** $$\frac{X = Y}{E[z := X] = E[z := Y]}$$

Axiom scheme (E can be any expression, and z any variable):

(3.83) **Axiom, Leibniz:** $(e = f) \Rightarrow (E[z := e] = E[z := f])$

What is the difference?

- Given a theorem $X = Y$ and an expression E,
  the inference rule (1.5) **produces** a new theorem $E[z := X] = E[z := Y]$
- (3.83) **is** a theorem
- $((e = f) \Rightarrow (E[z := e] = E[z := f])) \quad = \quad true$

  Can be used **deep inside nested expressions**

  — making use of **local assumptions**

Leibniz's Rule as an Axiom — Examples

Recall the **inference rule** (scheme):

(1.5) **Leibniz:** $$\frac{X = Y}{E[z := X] = E[z := Y]}$$

Axiom scheme (E can be any expression, and z any variable):

(3.83) **Axiom, Leibniz:** $(e = f) \Rightarrow (E[z := e] = E[z := f])$

Examples

- $n = k + 1 \Rightarrow n \cdot (k - 1) = (k + 1) \cdot (k - 1)$
- $n = k + 1 \Rightarrow (z \cdot (k - 1))[z := n] = (z \cdot (k - 1))[z := k + 1]$
- $$\begin{aligned} & (n = k + 1 \Rightarrow n \cdot (k - 1) = k^2 - 1) = true \\ \Rightarrow \quad & (n > 5 \Rightarrow (n = k + 1 \Rightarrow n \cdot (k - 1) = k^2 - 1)) \\ & = (n > 5 \Rightarrow true) \end{aligned}$$

Leibniz's Rule Axiom, and Further Replacement Rules

Axiom scheme (E can be any expression; $z, e, f : t$ can be of **any type** t):

(3.83) **Axiom, Leibniz:** $(e = f) \Rightarrow (E[z := e] = E[z := f])$

— Axiom (3.83) is rarely useful directly!

— Allmost all applications are via derived **"Replacement"** theorems

Replacement rules: (P can be any expression **of type** $\mathbb{B}$)

(3.84a) **"Replacement":** $(e = f) \wedge P[z := e] \quad \equiv \quad (e = f) \wedge P[z := f]$

(3.84b) **"Replacement":** $(e = f) \Rightarrow P[z := e] \quad \equiv \quad (e = f) \Rightarrow P[z := f]$

(3.84c) **"Replacement":** $q \wedge (e = f) \Rightarrow P[z := e] \equiv q \wedge (e = f) \Rightarrow P[z := f]$

Using a Replacement (LADM: "Substitution") Rule

Replacement rule: (P can be any expression **of type** $\mathbb{B}$)

(3.84a) **"Replacement":** $(e = f) \wedge P[z := e] \quad \equiv \quad (e = f) \wedge P[z := f]$

Textbook-style application:

$$\begin{aligned} & k = n + 1 \quad \wedge \quad k \cdot (n - 1) = n^2 - 1 \\ = \quad & \langle \text{(3.84a) \textbf{"Replacement"}} \rangle \\ & k = n + 1 \quad \wedge \quad (n + 1) \cdot (n - 1) = n^2 - 1 \end{aligned}$$

Not so fast! — CalcCheck cannot do second-order matching (yet):

$$\begin{aligned} & k = n + 1 \quad \wedge \quad k \cdot (n - 1) = n \cdot n - 1 \\ = \quad & \langle \text{Substitution} \rangle \\ & k = n + 1 \quad \wedge \quad (z \cdot (n - 1) = n \cdot n - 1)[z := k] \\ = \quad & \langle \text{(3.84a) \textbf{"Replacement"}} \rangle \\ & k = n + 1 \quad \wedge \quad (z \cdot (n - 1) = n \cdot n - 1)[z := n + 1] \\ = \quad & \langle \text{Substitution} \rangle \\ & k = n + 1 \quad \wedge \quad (n + 1) \cdot (n - 1) = n \cdot n - 1 \end{aligned}$$