Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2017-09-17

Raymond Smullyan posed many puzzles about an island that has two kinds of inhabitants:

- **knights**, who always tell the truth, and
- **knaves**, who always lie.

You encounter two people A and B.
What are A and B if

1. A says "We are both knaves."?
2. A says "At least one of us is a knave."?
3. A says "If I am a knight, then so is B."?
4. A says "We are of the same type."?
5. A says "B is a knight" and
   B says "The two of us are opposite types."?

Plan for Today

- A Theorem of the Integers — brief outlook using LADM Chapter 15
- Boolean Expressions — picking up pieces of LADM Chapter 2

Proving Zero of Multiplication

(1.2) **Axiom, Reflexivity of =:** $a = a$

(15.3) **Axiom, Additive identity:** $a + 0 = a$

(15.5) **Axiom, Distributivity:** $a \cdot (b + c) = a \cdot b + a \cdot c$

(15.8) **Cancellation of +:** $a + b = a + c \quad \equiv \quad b = c$

Proving (15.9) $a \cdot 0 = 0$**:**

$$
\begin{array}{ll}
& a \cdot 0 = 0 \\
\equiv & \langle \text{Cancellation of + (15.8), with } a, b, c := a \cdot d,\ a \cdot 0,\ 0 \rangle \\
& a \cdot d + a \cdot 0 = a \cdot d + 0 \\
\equiv & \langle \text{Distributivity of } \cdot \text{ over + (15.5)} \rangle \\
& a \cdot (d + 0) = a \cdot d + 0 \\
\equiv & \langle \text{Identity of + (15.3), twice} \rangle \\
& a \cdot d = a \cdot d \quad \text{— This is Reflexivity of = (1.2)}
\end{array}
$$

Proving Zero of Multiplication

(1.2) **Axiom, Reflexivity of =:** $a = a$

(15.3) **Axiom, Additive identity:** $a + 0 = a$

(15.5) **Axiom, Distributivity:** $a \cdot (b + c) = a \cdot b + a \cdot c$

(15.8) **Cancellation of +:** $a + b = a + c \quad \equiv \quad b = c$

Proving (15.9) $a \cdot 0 = 0$**:**

$$
\begin{array}{ll}
& a \cdot 0 = 0 \\
\equiv & \langle \text{Cancellation of + (15.8), with } a, b, c := a \cdot 42,\ a \cdot 0,\ 0 \rangle \\
& a \cdot 42 + a \cdot 0 = a \cdot 42 + 0 \\
\equiv & \langle \text{Distributivity of } \cdot \text{ over + (15.5)} \rangle \\
& a \cdot (42 + 0) = a \cdot 42 + 0 \\
\equiv & \langle \text{Identity of + (15.3), twice} \rangle \\
& a \cdot 42 = a \cdot 42 \quad \text{— This is “Reflexivity of =” (1.2)}
\end{array}
$$

LADM Theory of Integers — (15.20)

(15.5) **Distributivity** $a \cdot (b + c) = a \cdot b + a \cdot c$	(15.3) **Identity of +** $0 + a = a$	(15.4) **Identity of ·** $1 \cdot a = a$
(15.8) **Cancellation of +** $a + b = a + c \ \equiv\ b = c$	(15.13) **Unary minus** $a + (-a) = 0$	(15.14) **Subtraction** $a - b = a + (-b)$

(15.20) $-a = -1 \cdot a$ **— Prove this here!**

Truth Values and Equivalence — Remember

Boolean constants/values: *false*, *true*

The set/type of Boolean values: $\mathbb{B}$

Equality of boolean values is also called **equivalence** and written $\equiv$

$p \equiv q$	can be read as:	p is equivalent to q
	or:	p exactly when q
	or:	p if-and-only-if q
	or:	p iff q

In many current notebooks, the following is added as as an axiom:

(15.8) **Cancellation of +:** $a + b = a + c \quad \equiv \quad b = c$

Remember: Equivalence is just equality of truth values!

— but written with a different symbol

— with different notational conventions

Existential Quantification Examples

$(\exists\, k : \mathbb{N} \bullet k > 9999)$

- "There exists a natural number k such that $k > 9999$ (holds)"
- "For some natural number k, we have $k > 9999$"
- "Some natural number is greater than 9999"

$(\exists\, x : \mathbb{R} \mid x > 0 \bullet x \cdot x = x + 1)$

- "There exists a real number x with $x > 0$ such that $x \cdot x = x + 1$ (holds)"
- "For some positive real number x, we have $x \cdot x = x + 1$"

$(\exists\, r, s : \mathbb{Q} \mid r < s < r + 1/1000 \bullet r < \pi < s)$

- "There exist rational numbers r and s with $r < s < r + 1/1000$ such that $r < \pi < s$ (holds)"
- "For some rational numbers r and s with $r < s$ and $s - r < 1/1000$, we have $r < \pi < s$"
- "π can be enclosed within rational bounds that are less than 1/1000 apart"

Universal Quantification Examples

$(\forall\, k : \mathbb{N} \bullet 2 \cdot k \geq k)$

- "For all natural numbers k, we have $2 \cdot k \geq k$"

$(\forall\, x, y : \mathbb{R} \bullet x \cdot y = y \cdot x)$

- "For all real numbers x and y, we have $x \cdot y = y \cdot x$"
- "Multiplication of real numbers is symmetric (commutative)"

$(\forall\, x : \mathbb{R} \mid x > 5 \bullet x \cdot x > 10)$

- "For all real numbers x with $x > 5$, we have $x \cdot x > 10$"
- "The square of a real number greater than 5 is greater than 10."

$(\forall\, m, n : \mathbb{N} \mid m \neq n \bullet m \cdot m \neq n \cdot n)$

- "For all natural numbers m and n with $m \neq n$, we have $m \cdot m \neq n \cdot n$"
- "Different natural numbers have different squares."

Combined Quantification Examples

- "Every integer has an additive inverse."
- "For every integer k, there exists an integer n such that $k + n = 0$ (holds)."

$$(\forall k : \mathbb{Z} \bullet (\exists\, n : \mathbb{Z} \bullet k + n = 0\,)\,)$$

- "There is a least natural number."
- "There exists a natural number b such that every natural number n is at least b".
- "There exists a natural number b such that for every natural number n, we have $b \leq n$".

$$(\exists b : \mathbb{N} \bullet (\forall n : \mathbb{N} \bullet b \leq n))$$

Combined Quantification Examples (ctd.)

- "There is a least integer."
- "There exists an integer b such that every integer n is at least b".
- "There exists an integer b such that for every integer n, we have $b \leq n$".

$$(\exists b : \mathbb{Z} \bullet (\forall n : \mathbb{Z} \bullet b \leq n))$$

- "π can be enclosed within rational bounds that are less than any ε apart"
- "For every positive real number ε, there are rational numbers r and s with $r < s < r + \varepsilon$, such that $r < \pi < s$"

$$(\forall \varepsilon : \mathbb{R} \mid 0 < \varepsilon$$
$$\bullet (\exists\, r, s : \mathbb{Q} \mid r < s < r + \varepsilon \bullet r < \pi < s))$$

Truth Values and Equivalence — Remember

Boolean constants/values: *false*, *true*

The set/type of Boolean values: $\mathbb{B}$

Equality of boolean values is also called **equivalence** and written $\equiv$

$p \equiv q$	can be read as:	p is equivalent to q
	or:	p exactly when q
	or:	p if-and-only-if q
	or:	p iff q

For now, treat the following as an axiom:

(15.8) **Cancellation of +:** $a + b = a + c \quad \equiv \quad b = c$

Remember: Equivalence is just equality of truth values!

— but written with a different symbol

— with different notational conventions

Boolean Expressions

- Boolean constants: *false*, *true*
- **Proposition symbols** p, q — **variables of type** $\mathbb{B}$
- Applications of Boolean-valued operators to expressions of their argument types:
  Number types $\mathbb{N}$, $\mathbb{Z}$:
  - $1 = 2$
  - $42 \leq 56$
  - $a + b = a + c$

  String: `"Hello" ≼ "Hello World!"`
  Set: $\{1,2,3\} \cap \{2,3,4\} = \{2,3\}$
  $\mathbb{B}$:
  - $(a + b = a + c) \equiv (b = c)$
  - $(a \leq b) \Rightarrow (c - b \leq c - a)$
  - $\boxed{\text{The inscription on the gold casket is true}} \not\equiv \boxed{\text{The portrait is in the gold casket}}$
  - $G \not\equiv gc$
  - $(p \wedge q) \Rightarrow p$

Truth Values & Unary Boolean Operators

Boolean constants/values: *false*, *true*

Unary Boolean operators:

Arg.	Result (one column per operator)				
		id	$\neg$		
false	*false*	*false*	*true*	*true*	$\neg$*false* = *true*
true	*false*	*true*	*false*	*true*	$\neg$*true* = *false*

This table shows all four possible functions that map one Boolean argument to a Boolean result.

Unary Boolean Operators — f_1

Unary Boolean operators:

Arg.	Result (one column per operator)				
	f_1	*id*	$\neg$	f_4	
false	*false*	*false*	*true*	*true*	$f_1(\mathit{false}) = \mathit{false}$
true	*false*	*true*	*false*	*true*	$f_1(\mathit{true}) = \mathit{false}$

Unary Boolean Operators — *id*

Unary Boolean operators:

Arg.	Result (one column per operator)				
	f_1	*id*	$\neg$	f_4	
false	*false*	*false*	*true*	*true*	$id(false) = false$
true	*false*	*true*	*false*	*true*	$id(true) = true$

Unary Boolean Operators — f_4

Unary Boolean operators:

Arg.	Result (one column per operator)				
	f_1	*id*	$\neg$	f_4	
false	*false*	*false*	*true*	*true*	$f_4(false) = true$
true	*false*	*true*	*false*	*true*	$f_4(true) = true$

How Many Binary Boolean Operators Are There?

- How many arguments does a binary Boolean operator take?
- How many different argument value ($\mathbb{B}$) combinations are there?
- How many ways are there to map all argument value combinations to $\mathbb{B}$?

Args.		Result (one column per operator)															
			$\wedge$	$\not\Rightarrow$		$\not\Leftarrow$		$\not\equiv$ $\neq$	$\vee$	nor	$\equiv$ $=$		$\Leftarrow$		$\Rightarrow$	nand	
F	F	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T
F	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
T	F	F	F	T	T	F	F	T	T	F	F	T	T	F	F	T	T
T	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T

Binary Boolean Operators

Args.		Result (one column per operator)															
			$\wedge$	$\not\Rightarrow$		$\not\Leftarrow$		$\not\equiv$ $\neq$	$\vee$	nor	$\equiv$ $=$		$\Leftarrow$		$\Rightarrow$	nand	
F	F	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T
F	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
T	F	F	F	T	T	F	F	T	T	F	F	T	T	F	F	T	T
T	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T

For example:

$$\begin{array}{lclcl} \textit{true} & \wedge & \textit{false} & = & \textit{false} \\ \textit{true} & \not\equiv & \textit{false} & = & \textit{true} \\ \textit{false} & \Leftarrow & \textit{true} & = & \textit{false} \end{array}$$

Names of Binary Boolean Operators & their Arguments

			$\wedge$					$\not\equiv$ $\neq$	$\vee$	nor	$\equiv$ $=$		$\Leftarrow$		$\Rightarrow$	nand	
F	F	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T
F	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
T	F	F	F	T	T	F	F	T	T	F	F	T	T	F	F	T	T
T	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T

- $b = c$ reads "b equals c" — conventional **equality**
- $b \neq c$ reads "b differs from c" — conventional **inequality**
- $b \vee c$ reads "b or c" — **disjunction**; b and c are **disjuncts**
- $b \wedge c$ reads "b and c" — **conjunction**; b and c are **conjuncts**
- $b \Rightarrow c$ reads "b implies c" or "if b then c" — **implication**; b is the **antecedent**; c is the **consequent**
- $b \Leftarrow c$ reads "b follows from c" or "b if c" — **consequence**; b is the **consequent**; c is the **antecedent**

Table of Precedences

- $[x := e]$ (textual substitution) **(highest precedence)**
- $.$ (function application)
- unary prefix operators $+$, $-$, $\neg$, $\#$, $\sim$, $\mathcal{P}$
- $**$
- $\cdot$ $/$ $\div$ **mod** **gcd**
- $+$ $-$ $\cup$ $\cap$ $\times$ $\circ$ $\bullet$
- $\downarrow$ $\uparrow$
- $\#$
- $\triangleleft$ $\triangleright$ $\hat{}$
- $=$ $\neq$ $<$ $>$ $\in$ $\subset$ $\subseteq$ $\supset$ $\supseteq$ $|$ (conjunctional)
- $\vee$ $\wedge$
- $\Rightarrow$ $\not\Rightarrow$ $\Leftarrow$ $\not\Leftarrow$
- $\equiv$ $\not\equiv$ **(lowest precedence)**

All non-associative binary infix operators associate to the left, except $**$, $\triangleleft$, $\Rightarrow$, $\rightarrow$, which associate to the right.

Modeling English Propositions — Recipe

- Transform into shape with clear subpropositions
- Introduce Boolean variables to denote subpropositions
- Replace these subpropositions by their corresponding Boolean variables
- Translate the result into a Boolean expression, using (no perfect translation rules are possible!) **for example**:

and, but	becomes	$\wedge$
or	becomes	$\vee$
not	becomes	$\neg$
it is not the case that	becomes	$\neg$
if p then q	becomes	$p \Rightarrow q$

Binary Boolean Operators: "but"

Args.		$\wedge$	
F	F	F	The moon is green, but $2 + 2 = 7$.
F	T	F	The moon is green, but $1 + 1 = 2$.
T	F	F	$1 + 1 = 2$, but the moon is green.
T	T	T	$1 + 1 = 2$, but the sun is a star.

Binary Boolean Operators: "if"

Args.		$\Leftarrow$	
F	F	T	The moon is green if $2 + 2 = 7$.
F	T	F	The moon is green if $1 + 1 = 2$.
T	F	T	$1 + 1 = 2$ if the moon is green.
T	T	T	$1 + 1 = 2$ if the sun is a star.

See also textbook p. 36:

To stay dry, it's **sufficient** to wear a raincoat. = You will stay dry **if** you wear a raincoat.

= (You will stay dry. $\Leftarrow$ You wear a raincoat.)

"p if q." = "If q then p."

Binary Boolean Operators: "only if"

Args.			
		$\Rightarrow$	
F	F	T	The moon is green only if $2 + 2 = 7$.
F	T	T	The moon is green only if the sun is a star.
T	F	F	The sun is a star only if the moon is green.
T	T	T	$1 + 1 = 2$ only if the sun is a star.

See also textbook p. 36:

To stay dry, it's **neccessary** to wear a raincoat. = You will stay dry **only if** you wear a raincoat.

= (You will stay dry. $\Rightarrow$ You wear a raincoat.)

"p only if q." = "If p then q."

Necessary and Sufficient Conditions

(Textbook p. 36)

To stay dry, it's **neccessary** to wear a raincoat. = You will stay dry **only if** you wear a raincoat.

= (You will stay dry. $\Rightarrow$ You wear a raincoat.)

To stay dry, it's **sufficient** to wear a raincoat. = You will stay dry **if** you wear a raincoat.

= (You will stay dry. $\Leftarrow$ You wear a raincoat.)

Binary Boolean Operators: "even if"

Args.			
p	q	p	
F	F	F	The moon is green, even if $2 + 2 = 7$.
F	T	F	The moon is green, even if $1 + 1 = 2$.
T	F	T	$1 + 1 = 2$, even if the moon is green.
T	T	T	$1 + 1 = 2$, even if the sun is a star.

Transforming "even if"

Args.		
p	q	p	
F	F	F	The moon is green, even if $2+2=7$.
F	T	F	The moon is green, even if $1+1=2$.
T	F	T	$1+1=2$, even if the moon is green.
T	T	T	$1+1=2$, even if the sun is a star.

$1+1=2$, and, if the sun is a star, we still have $1+1=2$.

Declarations:

$t \; := \; 1+1=2$

$s \; := \;$ The sun is a star

Formalisation:

$t \wedge (s \Rightarrow t)$