Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-09-18

Plan for Today

- Semantics of Boolean Expressions (ctd.)
- **Validity** — this is a **semantic** concept
- Equivalence
  - Meaning of equivalence chains
- Starting Propositional Calculus (LADM Chapter 3)
  - **Theorems** — this is a **syntactic** concept
  - Equivalence axioms and theorems
  - Surprising uses of "Symmetry of ≡"

Necessary and Sufficient Conditions

(Textbook p. 36)

$\boxed{\text{To stay dry, it's } \textbf{neccessary} \text{ to wear a raincoat.}}$ $=$ $\boxed{\text{You will stay dry } \textbf{only if} \text{ you wear a raincoat.}}$

$= \left(\boxed{\text{You will stay dry.}} \Rightarrow \boxed{\text{You wear a raincoat.}} \right)$

$\boxed{\text{To stay dry, it's } \textbf{sufficient} \text{ to wear a raincoat.}}$ $=$ $\boxed{\text{You will stay dry } \textbf{if} \text{ you wear a raincoat.}}$

$= \left(\boxed{\text{You will stay dry.}} \Leftarrow \boxed{\text{You wear a raincoat.}} \right)$

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:

$$t \wedge (s \Rightarrow t)$$

Evaluation of Boolean Expressions Using Truth Tables

p	q	$\neg p$	$q \wedge \neg p$	$p \vee (q \wedge \neg p)$
F	F	T	F	F
F	T	T	T	T
T	F	F	F	T
T	T	F	F	T

- Identify variables
- Identify subexpressions
- Enumerate possible states (of the variables)
- Evaluate (sub-)expressions in all states

Alternative Presentation of Truth Tables

p	q	p	$\Rightarrow$	$(q$	$\wedge$	$\neg p)$
F	F		T		F	T
F	T		T		T	T
T	F		F		F	F
T	T		F		F	F

- Identify variables
- Identify subexpressions — **in doubt, add parentheses!**
- Enumerate possible states (of the variables)
- Evaluate (sub-)expressions in all states
  writing the result below the operator forming the subexpression
- (Proof tables are useful for confirming Boolean laws — you want to be confident doing them.)

Transforming "even if" — Truth Table

Args. t	s	t	
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: $t \wedge (s \Rightarrow t)$

t	s	t	$\wedge$	$(s$	$\Rightarrow$	$t)$
F	F		F		T	
F	T		F		F	
T	F		T		T	
T	T		T		T	

The truth table shows: $t \wedge (s \Rightarrow t)$ is **logically equivalent** to t.

We actually can already **prove** the equivalence $t \wedge (s \Rightarrow t) \;\equiv\; t$:

$$\begin{array}{ll} & t \wedge (s \Rightarrow t) \\ \equiv & \langle \text{Definition of } \Rightarrow \rangle \\ & t \wedge (\neg s \vee t) \\ \equiv & \langle \text{Absorption} \rangle \\ & t \end{array}$$

Truth Table for Associativity of Equivalence

p	q	r	$p \equiv q$	$q \equiv r$	$p \equiv (q \equiv r)$	$(p \equiv q) \equiv r$	$(p \equiv (q \equiv r)) = ((p \equiv q) \equiv r)$
F	F	F	T	T	F	F	T
F	F	T	T	F	T	T	T
F	T	F	F	F	T	T	T
F	T	T	F	T	F	F	T
T	F	F	F	T	T	T	T
T	F	T	F	F	F	F	T
T	T	F	T	F	F	F	T
T	T	T	T	T	T	T	T

$\big(p \equiv (q \equiv r)\big) = \big((p \equiv q) \equiv r\big)$ is true in every state:

- it is **valid**
- that is, $\equiv$ **is associative**

Validity and Satisfiability

- A boolean expression is **satisfied** in state s iff it evaluates to *true* in state s.
- A boolean expression is **valid** iff it is satisfied in every state.
- A valid boolean expression is called a **tautology**.
- A boolean expression is **satisfiable** iff there is a state in which it is satisfied.
- A boolean expression is called a **contradiction** iff it evaluates to *false* in every state.
- Two boolean expressions are called a **logically equivalent** iff they evaluate to the same truth value in every state.

These definitions rely on states / truth tables: **Semantic concepts**

What Does $p \equiv q \equiv r$ Mean?

We know that $\equiv$ is associative:

$$\boxed{(p \equiv q \equiv r) \quad = \quad ((p \equiv q) \equiv r) \quad = \quad (p \equiv (q \equiv r))}$$

We also know:

p	q	r	$p \equiv q \equiv r$
F	F	F	F
F	F	T	T
F	T	F	T
F	T	T	F
T	F	F	T
T	F	T	F
T	T	F	F
T	T	T	T

"One or three of p, q, and r are *true*."

LADM Theory of Integers — Trichotomy

(15.44) **Trichotomy:** $(a < b \quad \equiv \quad a = b \quad \equiv \quad a > b) \ \wedge$
$\neg(a < b \quad \wedge \quad a = b \quad \wedge \quad a > b)$

$p \equiv q \equiv r$ means:

"One or three of p, q, and r are *true*."

So, Trichotomy says:

"One or three of $a < b$, $a = b$, and $a > b$ are *true*,
but not all three."

"Exactly one of $a < b$, $a = b$, and $a > b$ is *true*."

LADM Exercise 2.6

Translate the following English statements into Boolean expressions.

1. None or both of p and q is *true*.
2. Exactly one of p and q is *true*.
3. Zero, two, or four of p, q, r, and s are *true*.
4. One or three of p, q, r, and s are *true*.

Among $p_1, \ldots, p_{2 \cdot k}$, an even number are *true*.

Equality Properties

Equivalence $\equiv$ can only used with Boolean values

$\Longrightarrow$ In "$p \equiv q$", both p and q must be Boolean values

Equality $=$ can be used "at" arbitrary types

$\Longrightarrow$ In "$a = b$", you only know that a and b have the same type

$\Longrightarrow$ If p and q are Boolean values, then $(p = q) \; = \; (p \equiv q)$

or, equivalently, $(p = q) \; \equiv \; (p \equiv q)$

$\Longrightarrow$ Equivalence is equality of Boolean values

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

(1.3) **Axiom, Symmetry of =:** $(a = b) \quad = \quad (b = a)$

(1.4) **Inference rule, Transitivity of =:** $\dfrac{X = Y \qquad Y = Z}{X = Z}$

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

Theorems

A theorem is

- **either** an **axiom**
- **or** the **conclusion of an inference rule** where the premises are theorems
- **or** a Boolean expression **proved** (using the inference rules) **equal** to an axiom or a previously proved **theorem**. ("— This is . . . ")

  Such proofs will be presented in the **calculational style**.

Propositional Calculus

- **Calculus**: method of reasoning by calculation with symbols
- **Propositional Calculus**: calculating
  - with Boolean expressions
  - containing propositional variables
- **The Textbook's Propositional Calculus**: **Equational Logic E**
  - a set of **axioms** defining operator properties
  - **four inference rules**:
    - (1.5) **Leibniz:** $\dfrac{X = Y}{E[z := X] = E[z := Y]}$ — We can apply equalities inside expressions.
    - (1.4) **Transitivity:** $\dfrac{X = Y \qquad Y = Z}{X = Z}$ — We can chain equalities.
    - (1.1) **Substitution:** $\dfrac{E}{E[x := R]}$ — We can can use substitution instances of theorems.
    - **Equipollence:** $\dfrac{X = Y \qquad X}{Y}$ — — This is ...

Calculational Proof Format

$$
\begin{array}{ll}
 & E_0 \\
= & \langle \text{ Explanation of why } E_0 = E_1 \rangle \\
 & E_1 \\
= & \langle \text{ Explanation of why } E_1 = E_2 \text{ — with comment } \rangle \\
 & E_2 \\
= & \langle \text{ Explanation of why } E_2 = E_3 \rangle \\
 & E_3
\end{array}
$$

Because the **calculational presentation** is **conjunctional**, this reads as:

$$E_0 = E_1 \qquad \wedge \qquad E_1 = E_2 \qquad \wedge \qquad E_2 = E_3$$

Because $=$ is **transitive**, this justifies:

$$E_0 = E_3$$

Theorems — Remember!

A **theorem** is

- **either** an **axiom**
- **or** the **conclusion of an inference rule** where the premises are theorems
- **or** a Boolean expression **proved** (using the inference rules) **equal** to an axiom or a previously proved **theorem**. ("— This is ...")

  Such proofs will be presented in the **calculational style**.

Note:

- **The theorem definition does not use evaluation/validity**
- But:
  - All theorems in **E** are valid
  - All valid Boolean expressions are theorems in **E**
- **Important:**
  - **We will prove theorems without using validity!**
  - This trains an **essential mathematical skill!**

Equivalence Axioms

(3.1) **Axiom, Associativity of** $\equiv$ **:** $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$ **:** $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

Example theorem — shown differently in the textbook:

Proving $p \equiv p \equiv q \equiv q$**:**

$$
\begin{aligned}
& p \equiv p \equiv q \equiv q \\
= \quad & \langle \text{(3.2) Symmetry of } \equiv \text{, with } p, q := p, q \equiv q \rangle \\
& p \equiv q \equiv q \equiv p \quad \text{— This is (3.2) Symmetry of } \equiv
\end{aligned}
$$

Equivalence Axioms

(3.1) **Axiom, Associativity of** $\equiv$ **:** $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$ **:** $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

Example theorem — shown differently in the textbook:

Proving $p \equiv p \equiv q \equiv q$**:**

$$
\begin{aligned}
& p \equiv (p \equiv (q \equiv q)) \\
\equiv \quad & \langle \text{(3.2) Symmetry of } \equiv \text{, with } p, q := p, (q \equiv q) \rangle \\
& p \equiv ((q \equiv q) \equiv p) \quad \text{— This is (3.2) Symmetry of } \equiv
\end{aligned}
$$

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."?

Explanation: $A_H \equiv \boxed{A \text{ is a knight}}$

Axiom schema "Knighthood": $\boxed{A \text{ says "}X\text{"}} \equiv A_H \equiv X$

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

4. A says "We are of the same type."?

$$
\begin{aligned}
& \boxed{A \text{ says "}A_H \equiv B_H\text{"}} \\
\equiv \; & \langle \text{"Knighthood"} \rangle \\
& A_H \equiv (A_H \equiv B_H) \\
\equiv \; & \langle \text{(3.3) Associativity of } \equiv \rangle \\
& A_H \equiv A_H \equiv B_H \\
\equiv \; & \langle \text{(3.2) Symmetry of } \equiv\text{: } p \equiv q \equiv q \equiv p \rangle \\
& B_H
\end{aligned}
$$

Equivalence Axioms

(3.1) **Axiom, Associativity of** $\equiv$**:** $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$**:** $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

(3.3) **Axiom, Identity of** $\equiv$**:** $\boxed{true \equiv q \equiv q}$

Can be used as:

- $(true \equiv q) = q$
- $true = (q \equiv q)$

Equivalence Axioms, and Theorem (3.4)

(3.1) **Axiom, Associativity of** $\equiv$**:** $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$**:** $\boxed{p \equiv q \equiv q \equiv p}$

(3.3) **Axiom, Identity of** $\equiv$**:** $\boxed{true \equiv q \equiv q}$

Can be used as: $true = (q \equiv q)$

The least interesting theorem:

Proving (3.4) *true***:**

$$
\begin{aligned}
& true \\
= \; & \langle \text{Identity of } \equiv \text{ (3.3), with } q := true \rangle \\
& true \equiv true \\
= \; & \langle \text{Identity of } \equiv \text{ (3.3), with } q := q \rangle \\
& true \equiv q \equiv q \quad \text{— This is Identity of } \equiv \text{ (3.3)}
\end{aligned}
$$

Equivalence Axioms and Theorems

(3.1) **Axiom, Associativity of $\equiv$:** $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of $\equiv$:** $\boxed{p \equiv q \equiv q \equiv p}$

(3.3) **Axiom, Identity of $\equiv$:** $\boxed{\mathit{true} \equiv q \equiv q}$

Theorems and Metatheorems:

(3.4) true

(3.5) **Reflexivity of $\equiv$:** $p \equiv p$

(3.6) **Proof Method**: To prove that $P \equiv Q$ is a theorem, transform P to Q or Q to P using Leibniz.

(3.7) **Metatheorem**: Any two theorems are equivalent.

Negation Axioms and Theorems

(3.8) **Axiom, Definition of** ***false*:** $\boxed{\mathit{false} \equiv \neg \mathit{true}}$

(3.9) **Axiom, Commutativity of $\neg$ with $\equiv$:** $\boxed{\neg(p \equiv q) \equiv \neg p \equiv q}$

(LADM: "Distributivity of $\neg$ over $\equiv$")

Can be used as:

- $\neg(p \equiv q) \quad = \quad (\neg p \equiv q)$
- $(\neg(p \equiv q) \equiv \neg p) \quad = \quad q$

(3.10) **Axiom, Definition of $\not\equiv$:** $\boxed{(p \not\equiv q) \equiv \neg(p \equiv q)}$

Theorems:

(3.11) $\neg p \equiv q \equiv p \equiv \neg q$ | $(\neg p \equiv \neg q) \equiv (p \equiv q)$

(3.12) **Double negation:** $\neg\neg p \equiv p$

(3.13) **Negation of** ***false*:** $\neg \mathit{false} \equiv \mathit{true}$

(3.14) $(p \not\equiv q) \ \equiv \ \neg p \equiv q$

(3.15) $\neg p \equiv p \equiv \mathit{false}$

Inequivalence Theorems

(3.16) **Symmetry of $\not\equiv$:** $(p \not\equiv q) \equiv (q \not\equiv p)$

(3.17) **Associativity of $\not\equiv$:** $((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$

(3.18) **Mutual associativity:** $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$

(3.19) **Mutual interchangeability:** $p \not\equiv q \equiv r \quad \equiv \quad p \equiv q \not\equiv r$

Note: Mutual associativity is not (yet...) automated!

(But omission of parentheses is implemented, similar to

- $k - m + n$
- $k + m - n$
- $k - m - n$

— None of these has $m - n$ as subexpression!

— But the second one is equal to $\quad k + (m - n) \quad \ldots)$

(3.23) Heuristic of Definition Elimination

To prove a theorem concerning an operator $\circ$ that is defined in terms of another, say $\bullet$, expand the definition of $\circ$ to arrive at a formula that contains $\bullet$; exploit properties of $\bullet$ to manipulate the formula, and then (possibly) reintroduce $\circ$ using its definition.

Textbook, p. 48

"Unfold-Fold strategy"

Inequivalence Theorems: Symmetry

(3.16) **Symmetry of $\not\equiv$:** $(p \not\equiv q) \equiv (q \not\equiv p)$

Proving (3.16) **Symmetry of $\not\equiv$:**

$$
\begin{array}{ll}
 & p \not\equiv q \\
= & \langle \text{(3.10) Definition of } \not\equiv \rangle \quad \text{— **Unfold**} \\
 & \neg(p \equiv q) \\
= & \langle \text{(3.2) Symmetry of } \equiv \rangle \\
 & \neg(q \equiv p) \\
= & \langle \text{(3.10) Definition of } \not\equiv \rangle \quad \text{— **Fold**} \\
 & q \not\equiv p
\end{array}
$$