Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-09-11

Ladies or Tigers — The Second Case

Raymond Smullyan provides, in **The Lady or the Tiger?**, the following context for a number of puzzles to follow:

> [...] the king explained to the prisoner that each of the two rooms contained either a lady or a tiger, but it *could* be that there were tigers in both rooms, or ladies in both rooms, or then again, maybe one room contained a lady and the other room a tiger.

In the **second case**, the following signs are on the doors of the rooms:

1	2
At least one of these rooms contains a lady	A tiger is in the other room

We are told that the signs are either both true or both false.

Plan for Today

- **Anatomy of calculation: Substitution**
  - **Substitution as such:** Replaces variables with expressions in expressions, e.g.,

$$\begin{array}{ll} & (x + 2 \cdot y)[x, y := 3 \cdot y, x + 5] \\ = & \langle \text{Substitution} \rangle \\ & 3 \cdot y + 2 \cdot (x + 5) \end{array}$$

  - **Inference rule Substitution:** Justifies applying instances of theorems:

$$\begin{array}{ll} & 2 \cdot y \ + \ -(2 \cdot y) \\ = & \langle \text{“Unary minus”}\ a + -a = 0 \text{ with ‘}a := 2 \cdot y\text{’} \rangle \\ & 0 \end{array}$$

  - **Inference rule Leibniz:** Justifies applying (instances of) **equational** theorems deeper inside expressions:

$$\begin{array}{ll} & 2 \cdot x + 3 \cdot (y \ - \ 5 \cdot (4 \cdot x + 7)) \\ = & \langle \text{“Subtraction”}\ a - b = a + -b \text{ with ‘}a, b := y, 5 \cdot (4 \cdot x + 7)\text{’} \rangle \\ & 2 \cdot x + 3 \cdot (y \ + \ -(5 \cdot (4 \cdot x + 7))) \end{array}$$

Calculational Proofs of Theorems — (15.17) $-(-a) = a$

(15.3) **Identity of +** $0 + a = a$	(15.13) **Unary minus** $a + (-a) = 0$

Theorem (15.17) “Self-inverse of unary minus”: $-(-a) = a$
Proof:

$$
\begin{aligned}
& -(-a) \\
= \; & \langle \text{ Identity of + (15.3) } \rangle \\
& 0 + -(-a) \\
= \; & \langle \text{ Unary minus (15.13) } \rangle \\
& a + (-a) + -(-a) \\
= \; & \langle \text{ Unary minus (15.13) } \rangle \\
& a + 0 \\
= \; & \langle \text{ Identity of + (15.3) } \rangle \\
& a
\end{aligned}
$$

Details of Applying Theorems — (15.17) with Explicit Substitutions

(15.3) **Identity of +** $0 + a = a$	(15.13) **Unary minus** $a + (-a) = 0$

Theorem (15.17): $-(-a) = a$
Proof:

$$
\begin{aligned}
& -(-a) \\
= \; & \langle \text{ Identity of + (15.3) with } a := -(-a) \rangle \\
& 0 + -(-a) \\
= \; & \langle \text{ Unary minus (15.13) with } a := a \rangle \\
& a + (-a) + -(-a) \\
= \; & \langle \text{ Unary minus (15.13) with } a := -a \rangle \\
& a + 0 \\
= \; & \langle \text{ Identity of + (15.3) with } a := a \rangle \\
& a
\end{aligned}
$$

See Textbook p. 15 top.

Specifying Substitutions for Theorem Application in CalcCheck

```
Theorem (15.19) “Distributivity of unary minus over +”:
    -(a + b) = (- a) + (- b)
Proof:
    - (a + b)
  =⟨ (15.20) with `a ≔ a + b` ⟩
    - 1 · (a + b)
  =⟨ “Distributivity of · over +” with `a, b, c ≔ - 1, a, b` ⟩
    - 1 · a + - 1 · b
  =⟨ (15.20) with `a ≔ a` ⟩
    - a  + - 1 · b
  =⟨ (15.20) with `a ≔ b` ⟩
    - a + - b
```

- Backquotes enclose math embedded in English. (MarkDown convention)
- Substitution notation as in LADM: *variables* := *expressions*
- The variable list has the same length as the expression list.
- No variable occurs twice in the variable list.
- CalcCheck$_{\text{Web}}$ notebooks “with rigid matching” **require** all theorem variables to be substituted.
- (“rigid matching”: You specify a theorem that needs to match without substitution)

Automatic Application of Associativity and Symmetry Laws

(15.1) **Axiom, Associativity:** $(a + b) + c = a + (b + c)$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(15.2) **Axiom, Symmetry:** $a + b = b + a$
$a \cdot b = b \cdot a$

- You have been trained to reason "up to symmetry and associativity"
- Making symmetry and associativity steps explicit is
  - **always allowed**
  - sometimes **very useful for readability**
- CalcCheck allows selective activation of symmetry and associativity laws
  $\Longrightarrow$ "Exercise … / Assignment …: […] **without automatic associativity and symmetry**"

(15.17) with Explicit Associativity and Symmetry Steps

(15.3) **Identity of +** $0 + a = a$	(15.13) **Unary minus** $a + (-a) = 0$

Proving (15.17) $-(-a) = a$**:**

$$
\begin{array}{ll}
 & -(-a) \\
= & \langle \text{Identity of } + \text{ (15.3)} \rangle \\
 & 0 + -(-a) \\
= & \langle \text{Unary minus (15.13)} \rangle \\
 & (a + (-a)) + -(-a) \\
= & \langle \text{Associativity of } + \text{ (15.1)} \rangle \\
 & a + ((-a) + -(-a)) \\
= & \langle \text{Unary minus (15.13)} \rangle \\
 & a + 0 \\
= & \langle \text{Symmetry of } + \text{ (15.2)} \rangle \\
 & 0 + a \\
= & \langle \text{Identity of } + \text{ (15.3)} \rangle \\
 & a
\end{array}
$$

Opportunity for Practice: Equational Theory of Integers — Axioms and Theorems

(15.1) **Associativity** $(a + b) + c = a + (b + c)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(15.2) **Symmetry** $a + b = b + a$ $a \cdot b = b \cdot a$	(15.3) **Identity of +** $0 + a = a$ $a + 0 = a$
(15.5) **Distributivity** $a \cdot (b + c) = a \cdot b + a \cdot c$ $(b + c) \cdot a = b \cdot a + c \cdot a$	(15.4) **Identity of ·** $1 \cdot a = a$ $a \cdot 1 = a$	(15.13) **Unary minus** $a + (-a) = 0$ (15.14) **Subtraction** $a - b = a + (-b)$

(15.17) $-(-a) = a$
(15.18) $-0 = 0$
(15.20) $-a = -1 \cdot a$
(15.19) $-(a + b) = -a + -b$
(15.21) $(-a) \cdot b = a \cdot (-b)$
(15.22) $a \cdot (-b) = -(a \cdot b)$
(15.23) $(-a) \cdot (-b) = a \cdot b$
(15.24) $a - 0 = a$
(15.25) $(a - b) + (c - d) = (a + c) - (b + d)$
(15.25a) $a + (b - c) = (a + b) - c$

Textual Substitution

Let E and R be expressions and let x be a variable. We write:

$$E[x := R] \qquad \text{or} \qquad E^x_R$$

to denote an expression that is the same as E but with all occurrences of x replaced by (R).

Example 1:

$$\begin{aligned} & (0+a)[a := -(-a)] \\ = & \quad \langle \text{ Applying substitution } \rangle \\ & (0+(-(-a))) \\ = & \quad \langle \text{ Removing (some) unnecessary parentheses } \rangle \\ & 0+-(-a) \end{aligned}$$

Textual Substitution

Let E and R be expressions and let x be a variable. We write:

$$E[x := R] \qquad \text{or} \qquad E^x_R$$

to denote an expression that is the same as E but with all occurrences of x replaced by (R).

Example 2:

$$\begin{aligned} & (x+y)[x := z+2] \\ = & \quad \langle \text{ Applying substitution } \rangle \\ & ((z+2)+y) \\ = & \quad \langle \text{ Removing unnecessary parentheses } \rangle \\ & z+2+y \end{aligned}$$

Textual Substitution

Let E and R be expressions and let x be a variable. We write:

$$E[x := R] \qquad \text{or} \qquad E^x_R$$

to denote an expression that is the same as E but with all occurrences of x replaced by (R).

Example 3:

$$\begin{aligned} & (x \cdot y)[x := z+2] \\ = & \quad \langle \text{ Applying substitution } \rangle \\ & ((z+2) \cdot y) \\ = & \quad \langle \text{ Removing unnecessary parentheses } \rangle \\ & (z+2) \cdot y \end{aligned}$$

Textual Substitution

Let E and R be expressions and let x be a variable. We write:

$$E[x := R] \qquad \text{or} \qquad E^x_R$$

to denote an expression that is the same as E but with all occurrences of x replaced by (R).

Example 4:

$$\begin{array}{cl} & x + y[x := z + 2] \\ = & \langle \text{ adding parentheses for clarity } \rangle \\ & x + (y[x := z + 2]) \\ = & \langle \text{ Applying substitution } \rangle \\ & x + (y) \\ = & \langle \text{ Removing unnecessary parentheses } \rangle \\ & x + y \end{array}$$

Textual Substitution

Let E and R be expressions and let x be a variable. We write:

$$E[x := R] \qquad \text{or} \qquad E^x_R$$

to denote an expression that is the same as E but with all occurrences of x replaced by (R).

Examples:

Expression	Result	Unnecessary parentheses removed
$x[x := z + 2]$	$(z + 2)$	$z + 2$
$(x + y)[x := z + 2]$	$((z + 2) + y)$	$z + 2 + y$
$(x \cdot y)[x := z + 2]$	$((z + 2) \cdot y)$	$(z + 2) \cdot y$
$x + y[x := z + 2]$	$x + y$	$x + y$

Note: Substitution $[x := R]$ is a **highest precedence** postfix operator

Sequential Substitution

$$\begin{array}{cl} & (x + y)[x := y - 3][y := z + 2] \\ = & \langle \text{ adding parentheses for clarity } \rangle \\ & ((x + y)[x := y - 3])[y := z + 2] \\ = & \langle \text{ performing inner substitution } \rangle \\ & (((y - 3) + y))[y := z + 2] \\ = & \langle \text{ performing outer substitution } \rangle \\ & ((((z + 2) - 3) + (z + 2))) \\ = & \langle \text{ removing unnecessary parentheses } \rangle \\ & z + 2 - 3 + z + 2 \end{array}$$

Simultaneous Textual Substitution

If R is a **list** $R_1, \ldots, R_n$ of expressions
and x is a **list** $x_1, \ldots, x_n$ of **distinct variables**, we write:

$$E[x := R]$$

to denote the **simultaneous** replacement of the variables of x
by the corresponding expressions of R,
each expression being enclosed in parentheses.

Example:

$$\begin{array}{cl} & (x+y)[x,y := y-3, z+2] \\ = & \langle \text{ performing substitution } \rangle \\ & ((y-3)+(z+2)) \\ = & \langle \text{ removing unnecessary parentheses } \rangle \\ & y-3+z+2 \end{array}$$

Simultaneous Textual Substitution

If R is a **list** $R_1, \ldots, R_n$ of expressions
and x is a **list** $x_1, \ldots, x_n$ of **distinct** variables, we write:

$$E[x := R]$$

to denote the **simultaneous** replacement of the variables of x
by the corresponding expressions of R,
each expression being enclosed in parentheses.

Examples:

Expression	Result	Unnecessary parentheses removed
$x[x,y := y-3, z+2]$	$(y-3)$	$y-3$
$(y+x)[x,y := y-3, z+2]$	$((z+2)+(y-3))$	$z+2+y-3$
$(x+y)[x,y := y-3, z+2]$	$((y-3)+(z+2))$	$y-3+z+2$
$x+y[x,y := y-3, z+2]$	$x+(z+2)$	$x+z+2$

Simultaneous Substitution:

$$\begin{array}{cl} & (x+y)[x,y := y-3, z+2] \\ = & \langle \text{ performing substitution } \rangle \\ & ((y-3)+(z+2)) \\ = & \langle \text{ Reflexivity of } = \text{ — removing unnecessary parentheses } \rangle \\ & y-3+z+2 \end{array}$$

Sequential Substitution:

$$\begin{array}{cl} & (x+y)[x := y-3][y := z+2] \\ = & \langle \text{ adding parentheses for clarity } \rangle \\ & ((x+y)[x := y-3])[y := z+2] \\ = & \langle \text{ performing inner substitution } \rangle \\ & (((y-3)+y))[y := z+2] \\ = & \langle \text{ performing outer substitution } \rangle \\ & ((((z+2)-3)+(z+2))) \\ = & \langle \text{ removing unnecessary parentheses } \rangle \\ & z+2-3+z+2 \end{array}$$

Inference Rule: Substitution

(1.1) **Substitution:** $\dfrac{E}{E[x := R]}$

Example:

If $a + 0 = a$ is a theorem, $\boxed{\text{"Identity of +"}}$

then $3 \cdot b + 0 = 3 \cdot b$ is also a theorem. $\boxed{\text{"Identity of +" with '}a := 3 \cdot b\text{'}}$

$$\frac{a + 0 = a}{(a + 0 = a)[a := 3 \cdot b]} \qquad \frac{a + 0 = a}{3 \cdot b + 0 = 3 \cdot b}$$

Example:

$$\frac{z \geq x \uparrow y \quad \equiv \quad z \geq x \quad \wedge \quad z \geq y}{x + y \geq x \uparrow y \quad \equiv \quad x + y \geq x \quad \wedge \quad x + y \geq y}$$

What is an Inference Rule?

$$\frac{\text{premise}_1 \qquad \ldots \qquad \text{premise}_n}{\text{conclusion}}$$

- **If all the premises are theorems, then the conclusion is a theorem.**
- A thereom is a "proved truth"
- The premises are also called hypotheses.
- The conclusion and each premise all have to be Boolean
- **Axioms** are inference rules with zero premises

Logical Definition of Equality

Two **axioms** (i.e., postulated as theorems):

- (1.2) **Reflexivity of =:** $x = x$
- (1.3) **Symmetry of =:** $(x = y) = (y = x)$

Two **inference rule schemes**:

- (1.4) **Transitivity of =:** $\dfrac{X = Y \qquad Y = Z}{X = Z}$
- (1.5) **Leibniz:** $\dfrac{X = Y}{E[z := X] = E[z := Y]}$

— the rule of "replacing equals for equals"