A Logical Approach to Discrete Math

Definition of an expression

- A constant (e.g. 231) or variable (e.g. x) is an expression.
- If E is an expression, then (E) is an expression.
- If $\circ$ is a unary prefix operator and E is an expression, then $\circ E$ is an expression, with operand E. For example, the negation symbol $-$ is used as a unary operator, so -5 is an expression.
- If $\star$ is a binary infix operator and D and E are expressions, then $D \star E$ is an expression, with operands D and E. For example, the symbols $+$ (for addition) and $\cdot$ (for multiplication or product) are binary operators, so $1+2$ and $(-5)\cdot(3+x)$ are expressions.

Table of Precedences

(a) $[x := e]$ (textual substitution) (highest precedence)
(b) . (function application)
(c) unary prefix operators: $+ \quad - \quad \neg \quad \# \quad \sim \quad \mathcal{P}$
(d) $**$
(e) $\cdot \quad / \quad \div$ **mod** **gcd**
(f) $+ \quad - \quad \cup \quad \cap \quad \times \quad \circ \quad \bullet$
(g) $\downarrow \quad \uparrow$
(h) $\#$
(i) $\triangleleft \quad \triangleright \quad \hat{}$
(j) $= \quad < \quad > \quad \in \quad \subset \quad \subseteq \quad \supset \quad \supseteq \quad |$ (conjunctional, see page 29)
(k) $\vee \quad \wedge$
(l) $\Rightarrow \quad \Leftarrow$
(m) $\equiv$

All nonassociative binary infix operators associate from left to right except $**$, $\triangleleft$, and $\Rightarrow$, which associate from right to left.

Definition of $/$: The operators on lines (j), (l), and (m) may have a slash $/$ through them to denote negation—e.g. $x \notin T$ is an abbreviation for $\neg(x \in T)$.

State

A state is a list of variables and their values.

Example

$(x, 5), (y, 6)$

An expression may be true in some states, but not in other states.

$2x+3y = 7$ is true in the state $(x, 5), (y, -1)$ but is not true in the state $(x, 1), (y, 2)$

A Logical Approach to Discrete Math

TABLE 1.1. EXAMPLES OF TEXTUAL SUBSTITUTION

Substitution for one variable

$35[x := 2] \;=\; 35$

$y[x := 2] \;=\; y$

$x[x := 2] \;=\; 2$

$(x \cdot x + y)[x := c + y] \;=\; (c + y) \cdot (c + y) + y$

$(x^2 + y^2 + x^3)[x := x + y] \;=\; (x + y)^2 + y^2 + (x + y)^3$

Substitution for several variables

$(x + y + y)[x, y := z, w] \;=\; z + w + w$

$(x + y + y)[x, y := 2 \cdot y, x \cdot z] \;=\; 2 \cdot y + x \cdot z + x \cdot z$

$(x + 2 \cdot y)[x, y := y, x] \;=\; y + 2 \cdot x$

$(x + 2 \cdot y \cdot z)[x, y, z := z, x, y] \;=\; z + 2 \cdot x \cdot y$

A property of textual substitution

Example

$$((a+b)\cdot c)[b:=x][x:=b]$$
$$= \quad \langle \text{t.s. and r.u.p} \rangle$$
$$((a+x)\cdot c)[x:=b]$$
$$= \quad \langle \text{t.s. and r.u.p} \rangle$$
$$(a+b)\cdot c$$

Same as original expression

Example

$$((a+b)\cdot x)[b:=x][x:=b]$$
$$= \quad \langle \text{t.s. and r.u.p} \rangle$$
$$((a+x)\cdot x)[x:=b]$$
$$= \quad \langle \text{t.s. and r.u.p} \rangle$$
$$(a+b)\cdot b$$

<u>Not</u> the same as original

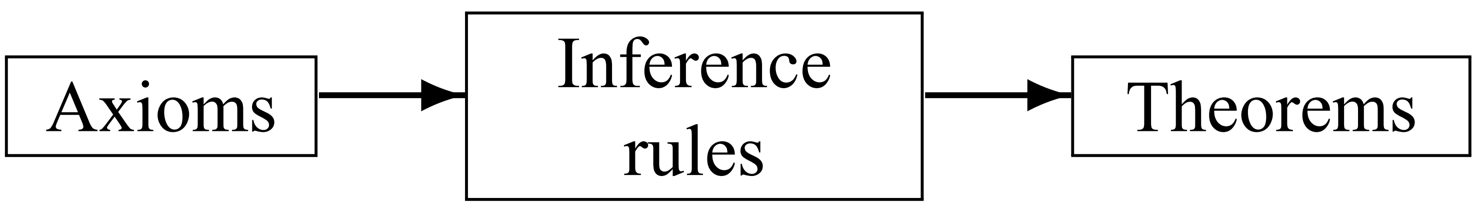
If $\neg \text{occurs}(`x', `E')$ then $E[y:=x][x:=y]=E$

Proofs

Analogy of computational system:

Given a program, and its input, the program produces the output.

Axiomatic logic systems



Given the inference rules, and some axioms, the logic system produces theorems.

Inference rules

An inference rule has a horizontal line.

The premise, or hypothesis,
assumed to be true in all states

The conclusion

Inference rules

There are four inference rules for logic proofs:

Substitution: $$\frac{E}{E[z := F]}$$

Leibniz: $$\frac{X = Y}{E[z := X] = E[z := Y]}$$

Equanimity: $$\frac{X, \quad X = Y}{Y}$$

Transitivity: $$\frac{X = Y, \quad Y = Z}{X = Z}$$

Assignment 2

Exercises

1.7 ... Fill in the missing parts and write down what expression E is.
(a)

$$\frac{x = x + 2}{4 \cdot x + y = \ ?}$$

1.8 ... For each of the expressions $E[z := X]$ and hints $X = Y$ below, write the resulting expression $E[z := Y]$.

	$E[z := X]$	hint $X = Y$
(a)	$x + y + w$	$x = b + c$

1.9 ... For each of the following pair of expressions $E[z := X]$ and $E[z := Y]$, identify a hint $X = Y$ that would show them to be equal and indicate what E is.

	$E[z := X]$	$E[z := Y]$
(a)	$(x + y) \cdot (x + y)$	$(x + y) \cdot (y + x)$

The four laws of equality

(1.2) **Reflexivity:** $x = x$

(1.3) **Symmetry** : $(x = y) = (y = x)$

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

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

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$a \cdot b \cdot a = a^2 \cdot b$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$\begin{array}{ll} & a \cdot b \cdot a = a^2 \cdot b \\ = & \langle (1) \text{ with } x, y := b, a, \text{ which is } b \cdot a = a \cdot b \rangle \end{array}$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$\begin{aligned} & a \cdot b \cdot a = a^2 \cdot b \\ = \quad & \langle (1) \text{ with } x, y := b, a, \text{ which is } b \cdot a = a \cdot b \rangle \\ & a \cdot a \cdot b = a^2 \cdot b \end{aligned}$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$
\begin{array}{ll}
& a \cdot b \cdot a = a^2 \cdot b \\
= & \langle (1) \text{ with } x, y := b, a \text{, which is } b \cdot a = a \cdot b \rangle \\
& a \cdot a \cdot b = a^2 \cdot b \\
= & \langle (2) \text{ with } x := a \text{, which is } a \cdot a = a^2 \rangle
\end{array}
$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$
\begin{array}{ll}
& a \cdot b \cdot a = a^2 \cdot b \\
= & \langle (1) \text{ with } x, y := b, a \text{, which is } b \cdot a = a \cdot b \rangle \\
& a \cdot a \cdot b = a^2 \cdot b \\
= & \langle (2) \text{ with } x := a \text{, which is } a \cdot a = a^2 \rangle \\
& a^2 \cdot b = a^2 \cdot b
\end{array}
$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$$a \cdot b \cdot a = a^2 \cdot b$$

Proof

$$\begin{array}{ll} & a \cdot b \cdot a = a^2 \cdot b \\ = & \langle (1) \text{ with } x, y := b, a, \text{ which is } b \cdot a = a \cdot b \rangle \\ & a \cdot a \cdot b = a^2 \cdot b \\ = & \langle (2) \text{ with } x := a, \text{ which is } a \cdot a = a^2 \rangle \\ & a^2 \cdot b = a^2 \cdot b \\ = & \langle (3) \text{ with } x := a^2 \cdot b, \text{ which is } a^2 \cdot b = a^2 \cdot b \rangle \end{array}$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$
\begin{array}{ll}
 & a \cdot b \cdot a = a^2 \cdot b \\
= & \langle (1) \text{ with } x, y := b, a \text{, which is } b \cdot a = a \cdot b \rangle \\
 & a \cdot a \cdot b = a^2 \cdot b \\
= & \langle (2) \text{ with } x := a \text{, which is } a \cdot a = a^2 \rangle \\
 & a^2 \cdot b = a^2 \cdot b \\
= & \langle (3) \text{ with } x := a^2 \cdot b \text{, which is } a^2 \cdot b = a^2 \cdot b \rangle \\
 & true \quad //
\end{array}
$$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$
\begin{aligned}
& a \cdot b \cdot a = a^2 \cdot b \\
= \quad & \langle (1) \text{ with } x, y := b, a, \text{ which is } b \cdot a = a \cdot b \rangle \\
& a \cdot a \cdot b = a^2 \cdot b \\
= \quad & \langle (2) \text{ with } x := a, \text{ which is } a \cdot a = a^2 \rangle \\
& a^2 \cdot b = a^2 \cdot b \\
= \quad & \langle (3) \text{ with } x := a^2 \cdot b, \text{ which is } a^2 \cdot b = a^2 \cdot b \rangle \\
& true \quad //
\end{aligned}
$$

Substitution: $\dfrac{E}{E[z := F]} \qquad \dfrac{x \cdot y = y \cdot x}{(x \cdot y = y \cdot x)[x, y := b, a]}$

Example proof

Assuming these axioms

(1) $x \cdot y = y \cdot x$

(2) $x \cdot x = x^2$

(3) $x = x$

prove that

$a \cdot b \cdot a = a^2 \cdot b$

Proof

$$
\begin{array}{ll}
 & \boxed{a \cdot b \cdot a = a^2 \cdot b} \\
= & \langle (1) \text{ with } x, y := b, a, \text{ which is } \boxed{b \cdot a = a \cdot b} \rangle \\
 & \boxed{a \cdot a \cdot b = a^2 \cdot b} \\
= & \langle (2) \text{ with } x := a, \text{ which is } a \cdot a = a^2 \rangle \\
 & a^2 \cdot b = a^2 \cdot b \\
= & \langle (3) \text{ with } x := a^2 \cdot b, \text{ which is } a^2 \cdot b = a^2 \cdot b \rangle \\
 & \mathit{true} \quad //
\end{array}
$$

Leibniz: $\dfrac{X = Y}{E[z := X] = E[z := Y]}$ $\qquad \dfrac{\boxed{b \cdot a = a \cdot b}}{\boxed{(a \cdot z = a^2 \cdot b)[z := b \cdot a]} = \boxed{(a \cdot z = a^2 \cdot b)[z := a \cdot b]}}$

General proof step

Leibniz:

$$\frac{X = Y}{E[z := X] = E[z := Y]}$$

Proof step:

$$\begin{array}{ll} & E[z := X] \\ = & \langle X = Y \rangle \\ & E[z := Y] \end{array}$$

The assignment statement

Uses the same symbol as textual substitution $:=$

The effect is to change the state.

Example

Initial state:	$(x,3),(y,2),(z,6)$
Assignment:	$y := z+1$
Final state:	$(x,3),(y,7),(z,6)$

The assignment statement

Notation

Operation	Formal methods	Java, C++
Equals	=	==
Assignment	:=	=

TABLE 1.2. EXAMPLES OF MULTIPLE ASSIGNMENTS

$x, y := y, x$	Swap x and y
$x, i := 0, 0$	Store 0 in x and i
$i, x := i + 1, x + i$	Add 1 to i and i to x
$x, i := x + i, i + 1$	Add 1 to i and i to x

The Hoare triple

Definition: An expression is valid if it is true in all states.

$$\{P\}\ S\ \{Q\}$$

Postcondition

Statement

Precondition

Interpretation: If the precondition is true, and you execute the statement, then the statement terminates, and the postcondition is guaranteed to be true.

The Hoare triple

$$\{P\}\ S\ \{Q\}$$

Examples

$\{x = 0\}\ x := x + 1\ \{x > 0\}$	valid
$\{x > 5\}\ x := x + 1\ \{x > 0\}$	valid
$\{x + 1 > 0\}\ x := x \cdot 2\ \{x > 0\}$	not valid
$\{x > -2\}\ x := x + 1\ \{x > 0\}$	not valid

The definition of assignment

$$\{R[x := E]\}\ x := E\ \{R\}$$

Assignment

Textual substitution

You calculate the precondition from the statement and the postcondition.

$$\{x+1>4\} \quad x := x+1 \quad \{x>4\}$$

$$\{x \cdot 6 > 0\} \quad y := 6 \quad \{x \cdot y > 0\}$$

$$\{x \cdot 2 = 10\} \quad x := x \cdot 2 \quad \{x = 10\}$$

$$\{y = 6\} \quad x := y \quad \{x = 6\}$$

$$\{y = 6\} \quad x := y \quad \{y = 6\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. Examples of Hoare Triples for Multiple Assignment

$$\{y > x\} \quad \underline{x, y := y, x} \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$\{y > x\} \quad x, y := y, x \quad \{x > y\}$

$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$
$x, i := x + i, i + 1$
$\{x = 1 + 2 + \cdots + (i - 1)\}$

$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$
$i, x := i + 1, x + i$
$\{x = 1 + 2 + \cdots + (i - 1)\}$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

A Logical Approach to Discrete Math

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (\underline{i} - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

TABLE 1.3. EXAMPLES OF HOARE TRIPLES FOR MULTIPLE ASSIGNMENT

$$\{y > x\} \quad x, y := y, x \quad \{x > y\}$$

$$\{x + i = 1 + 2 + \cdots + (\underline{i + 1} - 1)\}$$
$$x, i := x + i, i + 1$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$

$$\{x + i = 1 + 2 + \cdots + (i + 1 - 1)\}$$
$$i, x := i + 1, x + i$$
$$\{x = 1 + 2 + \cdots + (i - 1)\}$$