A Logical Approach to Discrete Math

8.1 Given are functions a, b, c, d, and e with types as follows.

$$a : A \to B$$
$$b : B \to C$$
$$c : C \to A$$
$$d : A \times C \to D$$
$$e : B \times B \to E$$

State whether each expression below is type correct. If not, explain why. Assume $u{:}A$, $w{:}B$, $x{:}C$, $y{:}D$, and $z{:}E$.

(a) $e(a.u, w)$
(b) $b.x$
(c) $e(a(c.x), a.u)$
(d) $a(c(b(a.y)))$
(e) $d(c.x, c.x)$

Abelian monoid

Symmetry: $b \star c = c \star b$

Associativity: $(b \star c) \star d = b \star (c \star d)$

Identity u**:** $u \star b = b = b \star u$

You can quantify an abelian monoid.

(8.6) $(\star x{:}t1, y{:}t2 \mid R : P)$

where:

- Variables x and y are distinct. They are called the *bound variables* or *dummies* of the quantification. There may be one or more dummies.
- $t1$ and $t2$ are the types of dummies x and y. If $t1$ and $t2$ are the same type, we may write $(\star x, y{:}t1 \mid R : P)$. In the interest of brevity, we usually omit the type when it is obvious from the context, writing simply $(\star x, y \mid R : P)$.
- R, a boolean expression, is the *range* of the quantification —values assumed by x and y satisfy R. R may refer to dummies x and y. If the range is omitted, as in $(\star x \mid : P)$, then the range *true* is meant.
- P, an expression, is the *body* of the quantification. P may refer to dummies x and y.
- The type of the result of the quantification is the type of P.

A Logical Approach to Discrete Math

$$
\begin{array}{rcl}
(+i \mid 0 \le i < 4 : i \cdot 8) & = & 0\cdot 8 \;+\; 1\cdot 8 \;+\; 2\cdot 8 \;+\; 3\cdot 8 \\
(\cdot i \mid 0 \le i < 3 : i + (i+1)) & = & (0+1)\cdot(1+2)\cdot(2+3) \\
(\wedge i \mid 0 \le i < 2 : i\cdot d \neq 6) & \equiv & 0\cdot d \neq 6 \;\wedge\; 1\cdot d \neq 6 \\
(\vee i \mid 0 \le i < 21 : b[i] = 0) & \equiv & b[0] = 0 \;\vee\; \cdots \;\vee\; b[20] = 0
\end{array}
$$

A Logical Approach to Discrete Math

$$
\begin{array}{lcl}
(+x \mid R : P) & \text{as} & (\Sigma\, x \mid R : P) \\
(\cdot x \mid R : P) & \text{as} & (\Pi\, x \mid R : P) \\
(\vee x \mid R : P) & \text{as} & (\exists x \mid R : P) \\
(\wedge x \mid R : P) & \text{as} & (\forall x \mid R : P)
\end{array}
$$

(8.9) **Definition.** The occurrence of i in the expression i is free.

Suppose an occurrence of i in expression E is free. Then that same occurrence of i is free in (E), in function application $f(\ldots, E, \ldots)$, and in $(\star x \mid E : F)$ and $(\star x \mid F : E)$ provided i is not one of the dummies in list x.

Define $occurs(\text{`}v\text{'}, \text{`}e\text{'})$ to mean that at least one variable in the list v of variables occurs free in at least one expression in expression list e.

(8.10) **Definition.** Let an occurrence of i be free in an expression E. That occurrence of i is *bound* (to dummy i) in the expression $(\star x \mid E : F)$ or $(\star x \mid F : E)$ if i is one of the dummies in list x.

Suppose an occurrence of i is bound in expression E. Then it is also bound (to the same dummy) in (E), $f(\ldots, E, \ldots)$, $(\star x \mid E : F)$ and $(\star x \mid F : E)$.

A Logical Approach to Discrete Math

$$i + j + (\Sigma\, i \mid 1 \leq i \leq 10 : b[i]^j) +$$
$$(\Sigma\, i \mid 1 \leq i \leq 10 : (\Sigma\, j \mid 1 \leq j \leq 10 : c[i, j]))$$

A Logical Approach to Discrete Math

(8.11) Provided $\neg occurs(\text{`}y\text{'}, \text{`}x, F\text{'})$,

$$(\star y \mid R : P)[x := F] \;=\; (\star y \mid R[x := F] : P[x := F]) \quad .$$

$$(+x \mid 1 \leq x \leq 2 : y)[y := y + z] \;=\; (+x \mid 1 \leq x \leq 2 : y + z)$$
$$(+i \mid 0 \leq i < n : b[i] = n)[n := m] \;=\; (+i \mid 0 \leq i < m : b[i] = m)$$
$$(+y \mid 0 \leq y < n : b[y] = n)[n := y] \;=\; (+j \mid 0 \leq j < y : b[j] = y)$$
$$(+y \mid 0 \leq y < n : b[y] = n)[y := m] \;=\; (+j \mid 0 \leq j < n : b[j] = n)$$

(8.12) **Leibniz:**

$$\frac{P = Q}{(\star x \mid E[z := P] : S) = (\star x \mid E[z := Q] : S)}$$

$$\frac{R \;\Rightarrow\; P = Q}{(\star x \mid R : E[z := P]) = (\star x \mid R : E[z := Q])}$$

For symmetric and associative binary operator $\star$ with identity u.

(8.13) **Axiom, Empty range:** $(\star x \mid false : P) = u$

0 is the identity of $+$.

$(+i \mid 2 \le i < 5 : i^2) = 2^2 + 3^2 + 4^2$

$(+i \mid 2 \le i < 4 : i^2) = 2^2 + 3^2$

$(+i \mid 2 \le i < 3 : i^2) = 2^2$

$(+i \mid 2 \le i < 2 : i^2) = (+i \mid false : i^2) = 0$

true is the identity of $\wedge$.

Suppose b is an array of integers.

$(\wedge i \mid 2 \le i < 5 : b[i] < x) = b[2] < x \wedge b[3] < x \wedge b[4] < x$

$(\wedge i \mid 2 \le i < 4 : b[i] < x) = b[2] < x \wedge b[3] < x$

$(\wedge i \mid 2 \le i < 3 : b[i] < x) = b[2] < x$

$(\wedge i \mid 2 \le i < 2 : b[i] < x) = (+x \mid false : b[i] < x) = true$

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}E\text{'})$,
$(\star x \mid x = E : P) = P[x := E]$

$(+i \mid i = 3 : i^2) \;=\; i^2\,[i := 3] \;=\; 3^2$

Suppose b is an array of integers.
$(\vee i \mid i = 3 : b[i] < x) \;=\; (b[i] < x)\,[i := 3] \;=\; b[3] < x$

(8.15) **Axiom, Distributivity:** Provided $P, Q : \mathbb{B}$ or R is finite,

$$(\star x \mid R : P) \star (\star x \mid R : Q) = (\star x \mid R : P \star Q)$$

$$\begin{aligned}
& (+i \mid 1 \leq i < 4 : 2i) + (+i \mid 1 \leq i < 4 : 5i^2) \\
= \quad & \langle \text{Expand quantifications} \rangle \\
& (2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3) + (5 \cdot 1^2 + 5 \cdot 2^2 + 5 \cdot 3^2) \\
= \quad & \langle \text{Symmetry and associativity of } + \rangle \\
& (2 \cdot 1 + 5 \cdot 1^2) + (2 \cdot 2 + 5 \cdot 2^2) + (2 \cdot 3 + 5 \cdot 3^2) \\
= \quad & \langle \text{Quantify} \rangle \\
& (+i \mid 1 \leq i < 4 : 2i + 5i^2)
\end{aligned}$$

(8.16) **Axiom, Range split:** Provided $R \wedge S \equiv false$ and $P : \mathbb{B}$ or R and S are finite,
$(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$

$R : \ 0 \le i < 3$
$S : \ 6 \le i < 9$
$R \vee S : \ 0 \le i < 3 \ \vee \ 6 \le i < 9$
$R \wedge S : \ false$

$$
\begin{array}{ll}
 & (+i \mid R \vee S : i^2) \\
= & \quad \langle \text{Definition of } R \text{ and } S \rangle \\
 & (+i \mid 0 \le i < 3 \ \vee \ 6 \le i < 9 : i^2) \\
= & \quad \langle \text{Expand quantification} \rangle \\
 & 0^2 + 1^2 + 2^2 + 6^2 + 7^2 + 8^2 \\
= & \quad \langle \text{Associativity of } + \rangle \\
 & (0^2 + 1^2 + 2^2) + (6^2 + 7^2 + 8^2) \\
= & \quad \langle \text{Quantify} \rangle \\
 & (+i \mid 0 \le i < 3 : i^2) + (+i \mid 6 \le i < 9 : i^2) \\
= & \quad \langle \text{Definition of } R \text{ and } S \rangle \\
 & (+i \mid R : i^2) + (+i \mid S : i^2)
\end{array}
$$

(8.17) **Axiom, Range split:** Provided $P : \mathbb{B}$ or R and S are finite,

$$(\star x \mid R \vee S : P) \star (\star x \mid R \wedge S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$$

Now, $R \wedge S$ is not required to be false.

$R :\ 1 \le i < 5$
$S :\ 3 \le i < 7$
$R \vee S :\ 1 \le i < 7$
$R \wedge S :\ 3 \le i < 5$

$$\begin{array}{ll} & (+i \mid R \vee S : i^2) + (+i \mid R \wedge S : i^2) \\ = & \quad \langle \text{Definition of } R \text{ and } S \rangle \\ & (+i \mid 1 \le i < 7 : i^2) + (+i \mid 3 \le i < 5 : i^2) \\ = & \quad \langle \text{Expand quantifications} \rangle \\ & (1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2) + (3^2 + 4^2) \\ = & \quad \langle \text{Symmetry and associativity of } + \rangle \\ & (1^2 + 2^2 + 3^2 + 4^2) + (3^2 + 4^2 + 5^2 + 6^2) \\ = & \quad \langle \text{Quantify} \rangle \\ & (+i \mid 1 \le i < 5 : i^2) + (+i \mid 4 \le i < 5 : i^2) \\ = & \quad \langle \text{Definition of } R \text{ and } S \rangle \\ & (+i \mid R : i^2) + (+i \mid S : i^2) \end{array}$$

(8.18) **Axiom, Range split for idempotent $\star$:** Provided $P : \mathbb{B}$ or R and S are finite,

$$(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$$

$\wedge$ is idempotent because $p \wedge p \equiv p$.

Suppose b is an array of integers.

$R :\ 0 \le i < 2$

$S :\ 1 \le i < 3$

$R \vee S :\ 0 \le i < 3$

$$
\begin{array}{ll}
 & (\wedge i \mid R : x < b[i]) \ \wedge \ (\wedge i \mid S : x < b[i]) \\
= & \quad \langle \text{Definition of } R \text{ and } S \rangle \\
 & (\wedge i \mid 0 \le i < 2 : x < b[i]) \ \wedge \ (\wedge i \mid 1 \le i < 3 : x < b[i]) \\
= & \quad \langle \text{Expand quantifications} \rangle \\
 & x < b[0] \ \wedge \ x < b[1] \ \wedge \ x < b[1] \ \wedge \ x < b[2] \\
= & \quad \langle (3.38)\ p \wedge p \equiv p \rangle \\
 & x < b[0] \ \wedge \ x < b[1] \ \wedge \ x < b[2] \\
= & \quad \langle \text{Quantify} \rangle \\
 & (\wedge i \mid 0 \le i < 3 : x < b[i]) \\
= & \quad \langle \text{Definition of } R \text{ and } S \rangle \\
 & (\wedge i \mid R \vee S : x < b[i])
\end{array}
$$

(8.19) **Axiom, Interchange of dummies:** Provided $\star$ is idempotent or R and Q are finite,
$\neg occurs(\text{`}y\text{'}, \text{`}R\text{'}), \neg occurs(\text{`}x\text{'}, \text{`}Q\text{'}),$
$(\star x \mid R : (\star y \mid Q : P)) = (\star y \mid Q : (\star x \mid R : P))$

$R: \ 1 \leq x < 4$
$Q: \ 8 \leq y < 10$
$P: \ 6 \cdot x \cdot y$

Note that $\neg occurs(\text{`}y\text{'}, \text{`}1 \leq x < 4\text{'})$ and $\neg occurs(\text{`}x\text{'}, \text{`}8 \leq y < 10\text{'})$

$$
\begin{array}{ll}
 & (+x \mid R : (+y \mid Q : 6 \cdot x \cdot y)) \\
= & \quad \langle \text{Expand inner quantification} \rangle \\
 & (+x \mid R : 6 \cdot x \cdot 8 + 6 \cdot x \cdot 9) \\
= & \quad \langle \text{Expand quantification} \rangle \\
 & (6 \cdot 1 \cdot 8 + 6 \cdot 1 \cdot 9) + (6 \cdot 2 \cdot 8 + 6 \cdot 2 \cdot 9) + (6 \cdot 3 \cdot 8 + 6 \cdot 3 \cdot 9) \\
= & \quad \langle \text{Symmetry and associativity of } + \rangle \\
 & (6 \cdot 1 \cdot 8 + 6 \cdot 2 \cdot 8 + 6 \cdot 3 \cdot 8) + (6 \cdot 1 \cdot 9 + 6 \cdot 2 \cdot 9 + 6 \cdot 3 \cdot 9) \\
= & \quad \langle \text{Quantify over } x \rangle \\
 & (+x \mid R : 6 \cdot x \cdot 8) + (+x \mid R : 6 \cdot x \cdot 9) \\
= & \quad \langle \text{Quantify over } y \rangle \\
 & (+y \mid Q : (+x \mid R : 6 \cdot x \cdot y))
\end{array}
$$

Inverse functions

Example

Suppose you have function: $f(x) = x^2$

Using the dot notation: $f.x = x^2$

$$
\begin{aligned}
& y = x^2 \\
= \quad & \langle \text{Solve for } x \rangle \\
& x = \sqrt{y}
\end{aligned}
$$

So $f^{-1}(y) = \sqrt{y}$

$$f(f^{-1}(y)) = f(\sqrt{y}) = (\sqrt{y})^2 = y$$
$$f^{-1}(f(x)) = f^{-1}(x^2) = \sqrt{x^2} = x$$

Definition of inverse function

$y = f.x \quad \equiv \quad x = f^{-1}.y$

Or, switching x and y

$x = f.y \quad \equiv \quad y = f^{-1}.x$

Prove (8.22) Change of dummy:

Provided $\neg occurs(\text{`}y\text{'}, \text{`}R, P\text{'})$, and f has an inverse,

$(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$

Proof:

$(\star y \mid R[x := f.y] : P[x := f.y])$

$=$ $\langle$(8.14) One-point rule in body$\rangle$

$(\star y \mid R[x := f.y] : (\star x \mid x = f.y : P))$

$=$ $\langle$(8.20) Nesting, because x cannot be in $R[x := f.y]\rangle$

$(\star x, y \mid R[x := f.y] \wedge x = f.y : P)$

$=$ $\langle$(3.84a) Substitution$\rangle$

$(\star x, y \mid R[x := x] \wedge x = f.y : P)$

$$
\begin{array}{ll}
 & (\star x, y \mid R[x := x] \ \wedge \ x = f.y : P) \\
= & \quad \langle \text{Property of textual substitution } R[x := x] = R \rangle \\
 & (\star x, y \mid R \ \wedge \ x = f.y : P) \\
= & \quad \langle \text{Definition of inverse, } x = f.y \ \equiv \ y = f^{-1}.x \rangle \\
 & (\star x, y \mid R \ \wedge \ y = f^{-1}.x : P) \\
= & \quad \langle \text{(8.20) Nesting, legal because } \neg \mathit{occurs}(\text{`}y\text{'}, \text{`}R\text{'}) \rangle \\
 & (\star x \mid R : (\star y \mid y = f^{-1}.x : P)) \\
= & \quad \langle \text{(8.14) One-point rule} \rangle \\
 & (\star x \mid R : P[y := f^{-1}.x]) \\
= & \quad \langle \text{Textual substitution because } \neg \mathit{occurs}(\text{`}y\text{'}, \text{`}P\text{'}) \rangle \\
 & (\star x \mid R : P) \quad //
\end{array}
$$

(8.22) **Change of dummy:** Provided $\neg occurs(\text{`}y\text{'}, \text{`}R, P\text{'})$, and f has an inverse,
$(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$

(8.22) Example

Suppose you have quantification: $(+i \mid 2 \le i < 5 : i^2) = 2^2 + 3^2 + 4^2$

$$
\begin{array}{ll}
 & (+i \mid 2 \le i < 5 : i^2) \\
= & \quad \langle \text{(8.22) with } i = f.j = j+2 \rangle \\
 & (+j \mid (2 \le i < 5)[i := j+2] : (i^2)[i := j+2]) \\
= & \quad \langle \text{Textual substitution} \rangle \\
 & (+j \mid 2 \le j+2 < 5 : (j+2)^2) \\
= & \quad \langle \text{Math} \rangle \\
 & (+j \mid 0 \le j < 3 : (j+2)^2)
\end{array}
$$

Both the range and the body are different from the original.

However, the expansion is the same.

$(+j \mid 0 \le j < 3 : (j+2)^2) = (0+2)^2 + (1+2)^2 + (2+2)^2$

(8.23) **Split off term:** For n: $\mathbb{N}$,

(a) $(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P[i := n]$

(b) $(\star i \mid 0 \le i < n+1 : P) = P[i := 0] \star (\star i \mid 0 < i < n+1 : P)$

Prove (8.23a) $(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P[i := n]$

Proof

$$
\begin{array}{ll}
 & (\star i \mid 0 \le i < n+1 : P) \\
= & \quad \langle \text{Math}, \quad 0 \le i < n+1 \;\equiv\; 0 \le i < n \;\vee\; i = n \rangle \\
 & (\star i \mid 0 \le i < n \;\vee\; i = n : P) \\
= & \quad \langle \text{(8.16) Range split} \rangle \\
 & (\star i \mid 0 \le i < n : P) \star (\star i \mid i = n : P) \\
= & \quad \langle \text{(8.14) One-point rule} \rangle \\
 & (\star i \mid 0 \le i < n : P) \star P[i := n] \quad //
\end{array}
$$

Split off the last term

(8.23a) $(\star i \mid 0 \le i < n+1 : P) = (\star i \mid 0 \le i < n : P) \star P[i := n]$

Examples

$$
\begin{array}{ll}
 & (\Sigma i \mid 0 \le i < n+1 : b[i]) \\
= & \quad \langle (8.23a) \rangle \\
 & (\Sigma i \mid 0 \le i < n : b[i]) + b[n]
\end{array}
$$

$$
\begin{array}{ll}
 & (\Sigma i \mid 0 \le i < n : b[i]) \\
= & \quad \langle (8.23a) \rangle \\
 & (\Sigma i \mid 0 \le i < n-1 : b[i]) + b[n-1]
\end{array}
$$

Examples

$$
\begin{array}{ll}
 & (\forall i \mid 0 \le i \le n+1 : b[i] = 0) \\
= & \quad \langle (8.23a) \rangle \\
 & (\forall i \mid 0 \le i \le n : b[i] = 0) \wedge b[n+1] = 0
\end{array}
$$

$$
\begin{array}{ll}
 & (\forall i \mid 0 \le i \le n : b[i] = 0) \\
= & \quad \langle (8.23a) \rangle \\
 & (\forall i \mid 0 \le i < n : b[i] = 0) \wedge b[n] = 0
\end{array}
$$

Split off the first term

(8.23b) $(\star i \mid 0 \le i < n+1 : P) = P[i := 0] \star (\star i \mid 0 < i < n+1 : P)$

Examples

$$
\begin{array}{ll}
 & (\Pi i \mid 0 \le i < n+1 : b[i]) \\
= & \quad \langle (8.23b) \rangle \\
 & b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])
\end{array}
$$

$$
\begin{array}{ll}
 & (\Pi i \mid 1 \le i < n+1 : b[i]) \\
= & \quad \langle (8.23b) \rangle \\
 & b[1] \cdot (\Pi i \mid 1 < i < n+1 : b[i])
\end{array}
$$

Examples

$$
\begin{array}{ll}
 & (\exists i \mid 0 < i < n : b[i] = 0) \\
= & \quad \langle (8.23b) \rangle \\
 & b[1] = 0 \vee (\exists i \mid 1 < i < n : b[i] = 0)
\end{array}
$$

$$
\begin{array}{ll}
 & (\exists i \mid 1 < i < n : b[i] = 0) \\
= & \quad \langle (8.23b) \rangle \\
 & b[2] = 0 \vee (\exists i \mid 2 < i < n : b[i] = 0)
\end{array}
$$

(a) $2 \leq i \leq 15$
(b) $2 \leq i < 16$
(c) $1 < i \leq 15$
(d) $1 < i < 16$