Types

Types

A type t is a set of values.

Types

A type t is a set of values.

Some Basic Types

Name	Symbol	Type (set of values)
integer	$\mathbb{Z}$	integers: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
nat	$\mathbb{N}$	natural numbers: $0, 1, 2, \ldots$
positive	$\mathbb{Z}^+$	positive integers: $1, 2, 3, \ldots$
negative	$\mathbb{Z}^-$	negative integers: $-1, -2, -3, \ldots$
rational	$\mathbb{Q}$	rational numbers: i/j for i, j integers, $j \neq 0$
reals	$\mathbb{R}$	real numbers
positive reals	$\mathbb{R}^+$	positive real numbers
bool	$\mathbb{B}$	booleans: $true, false$

Annotated expressions

Every expression E has a type t.

Annotated expressions

Every expression E has a type t.

Expressions can be annotated with their types.

Annotated expressions

Every expression E has a type t.

Expressions can be annotated with their types.

Expression	Annotated expression
$a+b$	$a:\mathbb{Z}+b:\mathbb{Z}$
$a+b$	$a:\mathbb{R}+b:\mathbb{R}$
x^n	$((x:\mathbb{R})^{n:\mathbb{Z}}):\mathbb{R}$

Functions

A function has one or more parameters, and returns a value.

Functions

A function has one or more parameters, and returns a value.

Example

odd(n) is a function with one parameter that returns $true$ if integer n is odd.

odd(6) returns $false$.

Functions

A function has one or more parameters, and returns a value.

Example

odd(n) is a function with one parameter that returns $true$ if integer n is odd.

odd(6) returns $false$.

Functions with one parameter can be written without parentheses with a period.

Example

odd(n) can be written odd.n

Functions

A function has one or more parameters, and returns a value.

Example

odd(n) is a function with one parameter that returns $true$ if integer n is odd.
odd(6) returns $false$.

Functions with one parameter can be written without parentheses with a period.

Example

odd(n) can be written odd.n

Example

max(n, m) is a function with two parameters that returns the larger of n and m.
max(13, 7) returns 13.

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \to r$ written

$f : t_1 \times t_2 \times t_3 \to r$

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \to r$ written

$f : t_1 \times t_2 \times t_3 \to r$

Example

$\max(n, m)$ where n and m are integers has type

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \to r$ written

$f : t_1 \times t_2 \times t_3 \to r$

Example

$\max(n, m)$ where n and m are integers has type $\quad \max\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \to r$ written

$$f : t_1 \times t_2 \times t_3 \to r$$

Example

$\max(n, m)$ where n and m are integers has type $\max\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Example

odd(n) has type

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \rightarrow r$ written

$f : t_1 \times t_2 \times t_3 \rightarrow r$

Example

max(n, m) where n and m are integers has type max: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$.

Example

odd(n) has type odd: $\mathbb{Z} \rightarrow \mathbb{B}$.

A Logical Approach to Discrete Math

If $f(p_1, p_2, p_3)$ is a function with three parameters, and

p_1 has has type t_1

p_2 has has type t_2

p_3 has has type t_3

the function f returns type r

then function f has type $t_1 \times t_2 \times t_3 \to r$ written

$$f : t_1 \times t_2 \times t_3 \to r$$

<u>Example</u>

max(n, m) where n and m are integers has type max: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

<u>Example</u>

odd(n) has type odd: $\mathbb{Z} \to \mathbb{B}$.

<u>Example</u>

odd(n, m) is type incorrect.

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

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

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.

(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 $(\star x, y \mid R : P)$.

(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.

A Logical Approach to Discrete Math

(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.

(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

$$(+i \mid 0 \leq i < 4 : i \cdot 8) \quad =$$

$$(\cdot i \mid 0 \leq i < 3 : i + (i + 1)) \quad =$$

$$(\wedge i \mid 0 \leq i < 2 : i \cdot d \neq 6) \quad \equiv$$

$$(\vee i \mid 0 \leq i < 21 : b[i] = 0) \quad \equiv$$

A Logical Approach to Discrete Math

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

A Logical Approach to Discrete Math

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

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

A Logical Approach to Discrete Math

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

A Logical Approach to Discrete Math

$(+x \mid R : P)$	as	$(\Sigma x \mid R : P)$
$(\cdot x \mid R : P)$	as	$(\Pi x \mid R : P)$
$(\vee x \mid R : P)$	as	$(\exists x \mid R : P)$
$(\wedge x \mid R : P)$	as	$(\forall x \mid R : P)$

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

(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 $occurs(`v', `e')$ 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.

A Logical Approach to Discrete Math

(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

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

A Logical Approach to Discrete Math

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

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

$$(+x \mid 1 \le x \le 2 : y)[y := y + z] \quad =$$

$$(+i \mid 0 \le i < n : b[i] = n)[n := m] \quad =$$

$$(+y \mid 0 \le y < n : b[y] = n)[n := y] \quad =$$

$$(+y \mid 0 \le y < n : b[y] = n)[y := m] \quad =$$

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

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

$$(+x \mid 1 \leq x \leq 2 : y)[y := y + z] \quad = \quad (+x \mid 1 \leq x \leq 2 : y + z)$$

$$(+i \mid 0 \leq i < n : b[i] = n)[n := m] \quad =$$

$$(+y \mid 0 \leq y < n : b[y] = n)[n := y] \quad =$$

$$(+y \mid 0 \leq y < n : b[y] = n)[y := m] \quad =$$

A Logical Approach to Discrete Math

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

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

$$(+x \mid 1 \leq x \leq 2 : y)[y := y + z] \;=\; (+x \mid 1 \leq x \leq 2 : y + z)$$

$$(+i \mid 0 \leq i < n : b[i] = n)[n := m] \;=\; (+i \mid 0 \leq i < m : b[i] = m)$$

$$(+y \mid 0 \leq y < n : b[y] = n)[n := y] \;=$$

$$(+y \mid 0 \leq y < n : b[y] = n)[y := m] \;=$$

A Logical Approach to Discrete Math

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

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

$$(+x \mid 1 \leq x \leq 2 : y)[y := y + z] \;=\; (+x \mid 1 \leq x \leq 2 : y + z)$$

$$(+i \mid 0 \leq i < n : b[i] = n)[n := m] \;=\; (+i \mid 0 \leq i < m : b[i] = m)$$

$$(+y \mid 0 \leq y < n : b[y] = n)[n := y] \;=\; (+j \mid 0 \leq j < y : b[j] = y)$$

$$(+y \mid 0 \leq y < n : b[y] = n)[y := m] \;=$$

A Logical Approach to Discrete Math

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

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

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

A Logical Approach to Discrete Math

(8.12) **Leibniz:**

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

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

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 $+$.

$(+i \mid 2 \leq i < 5 : i^2) =$

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

true is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

true is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

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.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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 $+$.

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

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

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

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

$true$ is the identity of $\wedge$.

Suppose b is an array of integers.

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

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

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

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

A Logical Approach to Discrete Math

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.

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

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

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

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

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(`x', `E')$,

$(\star x \mid x = E : P) = P[x := E]$

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

Suppose b is an array of integers.

$(\vee i \mid i = 3 : b[i] < x) \; =$

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

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

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

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(`x', `E')$,

$$(\star x \mid x = E : P) = P[x := E]$$

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

Suppose b is an array of integers.

$$(\vee i \mid i = 3 : b[i] < x) \; =$$

(8.14) **Axiom, One-point rule:** Provided $\neg occurs(‘x’, ‘E’)$,
$(\star x \mid x = E : P) = P[x := E]$

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

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

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

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

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,

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

$$(+i \mid 1 \leq i < 4 : 2i) + (+i \mid 1 \leq i < 4 : 5i^2)$$

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

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

$$(+i \mid 1 \leq i < 4 : 2i) + (+i \mid 1 \leq i < 4 : 5i^2)$$

$=$ ⟨Expand quantifications⟩

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

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

$$(+i \mid 1 \leq i < 4 : 2i) + (+i \mid 1 \leq i < 4 : 5i^2)$$

$= \quad \langle$Expand quantifications$\rangle$

$$(2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3) + (5 \cdot 1^2 + 5 \cdot 2^2 + 5 \cdot 3^2)$$

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

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

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

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

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

A Logical Approach to Discrete Math

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

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

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

A Logical Approach to Discrete Math

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

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

$$(+i \mid R \vee S : i^2)$$

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

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

$(+i \mid R \vee S : i^2)$
$=$ ⟨Definition of R and S⟩

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

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

$$
\begin{array}{ll}
& (+i \mid R \vee S : i^2) \\
= & \langle \text{Definition of } R \text{ and } S \rangle \\
& (+i \mid 0 \leq i < 3\ \vee\ 6 \leq i < 9 : i^2)
\end{array}
$$

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

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

$(+i \mid R \vee S : i^2)$
$=$ ⟨Definition of R and S⟩
$(+i \mid 0 \leq i < 3\ \vee\ 6 \leq i < 9 : i^2)$
$=$ ⟨Expand quantification⟩

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

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

$(+i \mid R \vee S : i^2)$
$=$ ⟨Definition of R and S⟩
$(+i \mid 0 \leq i < 3 \ \vee\ 6 \leq i < 9 : i^2)$
$=$ ⟨Expand quantification⟩
$0^2 + 1^2 + 2^2 + 6^2 + 7^2 + 8^2$

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

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

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

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

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

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

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

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

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

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

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

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

A Logical Approach to Discrete Math

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

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

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

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

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

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

(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.

$R:\ 1 \leq i < 5$
$S:\ 3 \leq i < 7$

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

$$(+i \mid R \vee S : i^2) + (+i \mid R \wedge S : i^2)$$

(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.

$R: \; 1 \leq i < 5$
$S: \; 3 \leq i < 7$

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

$$(+i \mid R \vee S : i^2) + (+i \mid R \wedge S : i^2)$$
$=$ ⟨Definition of R and S⟩

(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.

$R:\ 1 \leq i < 5$
$S:\ 3 \leq i < 7$

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

$$\begin{array}{ll} & (+i \mid R \vee S : i^2) + (+i \mid R \wedge S : i^2) \\ = & \langle \text{Definition of } R \text{ and } S \rangle \\ & (+i \mid 1 \leq i < 7 : i^2) + (+i \mid 3 \leq i < 5 : i^2) \end{array}$$

(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.

$R:\ 1 \leq i < 5$
$S:\ 3 \leq i < 7$

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

$$(+i \mid R \vee S : i^2) + (+i \mid R \wedge S : i^2)$$

$=$ ⟨Definition of R and S⟩

$$(+i \mid 1 \leq i < 7 : i^2) + (+i \mid 3 \leq i < 5 : i^2)$$

$=$ ⟨Expand quantifications⟩

(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.

$R :\ 1 \leq i < 5$
$S :\ 3 \leq i < 7$

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

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

(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.

$R :\ 1 \leq i < 5$
$S :\ 3 \leq i < 7$

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

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

(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.

$R:\ 1 \leq i < 5$
$S:\ 3 \leq i < 7$

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

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

A Logical Approach to Discrete Math

(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.

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

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

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

(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.

$R:\ 1 \leq i < 5$
$S:\ 3 \leq i < 7$

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

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

(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.

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

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

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

(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.

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

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

(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.

$R :\ 0 \leq i < 2$

$S :\ 1 \leq i < 3$

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

$$(\wedge i \mid R : x < b[i]) \ \wedge \ (\wedge i \mid S : x < b[i])$$

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

$(\wedge i \mid R : x < b[i])\ \wedge\ (\wedge i \mid S : x < b[i])$

$=$ ⟨Definition of R and S⟩

(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.

$R :\ 0 \leq i < 2$

$S :\ 1 \leq i < 3$

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

$$
\begin{array}{ll}
 & (\wedge i \mid R : x < b[i]) \ \wedge \ (\wedge i \mid S : x < b[i]) \\
= & \langle \text{Definition of } R \text{ and } S \rangle \\
 & (\wedge i \mid 0 \leq i < 2 : x < b[i]) \ \wedge \ (\wedge i \mid 1 \leq i < 3 : x < b[i])
\end{array}
$$

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

$(\wedge i \mid R : x < b[i]) \ \wedge \ (\wedge i \mid S : x < b[i])$

$=$ ⟨Definition of R and S⟩

$(\wedge i \mid 0 \leq i < 2 : x < b[i]) \ \wedge \ (\wedge i \mid 1 \leq i < 3 : x < b[i])$

$=$ ⟨Expand quantifications⟩

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

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

(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.

$R:\ 0 \le i < 2$

$S:\ 1 \le i < 3$

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

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

(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.

$R:\ 0 \le i < 2$

$S:\ 1 \le i < 3$

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

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

(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.

$R:\ 0 \le i < 2$

$S:\ 1 \le i < 3$

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

$(\wedge i \mid R : x < b[i]) \ \wedge\ (\wedge i \mid S : x < b[i])$

$=$ ⟨Definition of R and S⟩

$(\wedge i \mid 0 \le i < 2 : x < b[i]) \ \wedge\ (\wedge i \mid 1 \le i < 3 : x < b[i])$

$=$ ⟨Expand quantifications⟩

$x < b[0] \ \wedge\ x < b[1] \ \wedge\ x < b[1] \ \wedge\ x < b[2]$

$=$ ⟨(3.38) $p \wedge p \equiv p$⟩

$x < b[0] \ \wedge\ x < b[1] \ \wedge\ x < b[2]$

$=$ ⟨Quantify⟩

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

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

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

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

(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.

$R:\ 0 \leq i < 2$

$S:\ 1 \leq i < 3$

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

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

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

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

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

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

$$(+x \mid R : (+y \mid Q : 6 \cdot x \cdot y))$$

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

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

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

$$
\begin{array}{ll}
 & (+x \mid R : (+y \mid Q : 6 \cdot x \cdot y)) \\
= & \langle \text{Expand inner quantification} \rangle
\end{array}
$$

(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 $\neg occurs(\text{`}x\text{'}, \text{`}8 \leq y < 10\text{'})$

$$\begin{array}{ll} & (+x \mid R : (+y \mid Q : 6 \cdot x \cdot y)) \\ = & \langle \text{Expand inner quantification} \rangle \\ & (+x \mid R : 6 \cdot x \cdot 8 + 6 \cdot x \cdot 9) \end{array}$$

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

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

Note that $\neg occurs(`y', `1 \le x < 4')$ and $\neg occurs(`x', `8 \le y < 10')$

$$
\begin{array}{ll}
 & (+x \mid R : (+y \mid Q : 6 \cdot x \cdot y)) \\
= & \langle \text{Expand inner quantification} \rangle \\
 & (+x \mid R : 6 \cdot x \cdot 8 + 6 \cdot x \cdot 9) \\
= & \langle \text{Expand quantification} \rangle
\end{array}
$$

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

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

Note that $\neg occurs(`y', `1 \le x < 4')$ and $\neg occurs(`x', `8 \le y < 10')$

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

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

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

Note that $\neg occurs(`y', `1 \le x < 4')$ and $\neg occurs(`x', `8 \le y < 10')$

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

(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 $\neg occurs(\text{`}x\text{'}, \text{`}8 \leq y < 10\text{'})$

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

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

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

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

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

(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 $\neg occurs(\text{`}x\text{'}, \text{`}8 \leq y < 10\text{'})$

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

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

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

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

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

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

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

Note that $\neg occurs(`y', `1 \le x < 4')$ and $\neg occurs(`x', `8 \le y < 10')$

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

Inverse functions

Inverse functions

Example

Inverse functions

Example

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

Inverse functions

Example

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

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

Inverse functions

Example

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

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

$$y = x^2$$

Inverse functions

Example

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

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

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

Inverse functions

Example

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

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

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

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

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

$f(f^{-1}(y)) =$

Inverse functions

Example

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

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

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

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

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

Inverse functions

Example

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

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

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

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

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

Inverse functions

Example

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

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

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

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

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

Inverse functions

Example

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

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

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

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

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

$f^{-1}(f(x)) =$

Inverse functions

Example

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

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

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

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

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

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

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

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

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

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

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

Inverse functions

Example

Definition of inverse function

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

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

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

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

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

Inverse functions

Example

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

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

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

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

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:

Prove (8.22) Change of dummy:

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

Prove (8.22) Change of dummy:

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

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

Prove (8.22) Change of dummy:

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

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

Proof:

Prove (8.22) Change of dummy:

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

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

Proof:

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

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:

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

$=$ ⟨(8.14) One-point rule in body⟩

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:

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

$= \quad \langle (8.14) \text{ One-point rule in body} \rangle$

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

Prove (8.22) Change of dummy:

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

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

Proof:

$$
\begin{array}{ll}
 & (\star y \mid R[x := f.y] : P[x := f.y]) \\
= & \langle \text{(8.14) One-point rule in body} \rangle \\
 & (\star y \mid R[x := f.y] : (\star x \mid x = f.y : P)) \\
= & \langle \text{(8.20) Nesting, because } x \text{ cannot be in } R[x := f.y] \rangle
\end{array}
$$

Prove (8.22) Change of dummy:

Provided $\neg occurs(`y', `R,P')$, 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 $R[x := f.y]\rangle$

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

Prove (8.22) Change of dummy:

Provided $\neg occurs(`y', `R,P')$, 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$

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

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

Prove (8.22) Change of dummy:

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

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

Proof:

$$
\begin{array}{ll}
& (\star y \mid R[x := f.y] : P[x := f.y]) \\
= & \langle \text{(8.14) One-point rule in body} \rangle \\
& (\star y \mid R[x := f.y] : (\star x \mid x = f.y : P)) \\
= & \langle \text{(8.20) Nesting, because } x \text{ cannot be in } R[x := f.y] \rangle \\
& (\star x, y \mid R[x := f.y] \wedge x = f.y : P) \\
= & \langle \text{(3.84a) Substitution} \rangle \\
& (\star x, y \mid R[x := x] \wedge x = f.y : P)
\end{array}
$$

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

$$
\begin{array}{ll}
 & (\star x, y \mid R[x := x] \wedge x = f.y : P) \\
= & \langle \text{Property of textual substitution } R[x := x] = R \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & (\star x, y \mid R[x := x] \land x = f.y : P) \\
= & \langle \text{Property of textual substitution } R[x := x] = R \rangle \\
 & (\star x, y \mid R \land x = f.y : P)
\end{array}
$$

A Logical Approach to Discrete Math

$$
\begin{array}{ll}
 & (\star x, y \mid R[x := x] \ \wedge \ x = f.y : P) \\
= & \langle \text{Property of textual substitution } R[x := x] = R \rangle \\
 & (\star x, y \mid R \ \wedge \ x = f.y : P) \\
= & \langle \text{Definition of inverse, } x = f.y \ \equiv \ y = f^{-1}.x \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & (\star x, y \mid R[x := x] \wedge x = f.y : P) \\
= & \langle \text{Property of textual substitution } R[x := x] = R \rangle \\
 & (\star x, y \mid R \wedge x = f.y : P) \\
= & \langle \text{Definition of inverse}, x = f.y \;\equiv\; y = f^{-1}.x \rangle \\
 & (\star x, y \mid R \wedge y = f^{-1}.x : P)
\end{array}
$$

A Logical Approach to Discrete Math

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

$= \quad \langle$Property of textual substitution $R[x := x] = R\rangle$

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

$= \quad \langle$Definition of inverse, $x = f.y \equiv y = f^{-1}.x\rangle$

$$(\star x, y \mid R \wedge y = f^{-1}.x : P)$$

$= \quad \langle$(8.20) Nesting, legal because $\neg occurs(`y', `R')\rangle$

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

A Logical Approach to Discrete Math

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

A Logical Approach to Discrete Math

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

A Logical Approach to Discrete Math

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

A Logical Approach to Discrete Math

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

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

<u>(8.22) Example</u>

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R,P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

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

<u>(8.22) Example</u>

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

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

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R,P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

$$(+i \mid 2 \leq i < 5 : i^2)$$

$= \quad \langle (8.22) \text{ with } i = f.j = j + 2 \rangle$

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

<u>(8.22) Example</u>

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

$$
\begin{aligned}
& (+i \mid 2 \leq i < 5 : i^2) \\
= \quad & \langle (8.22) \text{ with } i = f.j = j + 2 \rangle \\
& (+j \mid (2 \leq i < 5)[i := j+2] : (i^2)[i := j+2])
\end{aligned}
$$

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R, P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

$$
\begin{aligned}
& (+i \mid 2 \leq i < 5 : i^2) \\
= \quad & \langle \text{(8.22) with } i = f.j = j + 2 \rangle \\
& (+j \mid (2 \leq i < 5)[i := j + 2] : (i^2)[i := j + 2]) \\
= \quad & \langle \text{Textual substitution} \rangle
\end{aligned}
$$

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R,P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

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

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R,P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

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

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

<u>(8.22) Example</u>

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

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

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R, P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

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

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

(8.22) **Change of dummy:** Provided $\neg occurs(`y', `R,P')$, 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: $(+i \mid 2 \leq i < 5 : i^2) = 2^2 + 3^2 + 4^2$

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

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

However, the expansion is the same.

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

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

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

However, the expansion is the same.

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

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

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

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

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

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

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

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

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

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

Proof

(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

$(\star i \mid 0 \le i < n+1 : P)$

(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

$(\star i \mid 0 \le i < n+1 : P)$

$= \quad \langle \text{Math}, \quad 0 \le i < n+1 \ \equiv\ 0 \le i < n \ \vee\ i = n \rangle$

(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

$$(\star i \mid 0 \le i < n+1 : P)$$

$= \quad \langle \text{Math}, \quad 0 \le i < n+1 \ \equiv \ 0 \le i < n \ \vee \ i = n \rangle$

$$(\star i \mid 0 \le i < n \ \vee \ i = n : P)$$

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

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

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

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

Proof

$$
\begin{aligned}
& (\star i \mid 0 \leq i < n+1 : P) \\
= \quad & \langle \text{Math}, \quad 0 \leq i < n+1 \ \equiv \ 0 \leq i < n \ \vee \ i = n \rangle \\
& (\star i \mid 0 \leq i < n \ \vee \ i = n : P) \\
= \quad & \langle \text{(8.16) Range split} \rangle
\end{aligned}
$$

(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

$$
\begin{array}{ll}
 & (\star i \mid 0 \le i < n+1 : P) \\
= & \langle \text{Math}, \quad 0 \le i < n+1 \ \equiv\ 0 \le i < n \ \vee\ i = n \rangle \\
 & (\star i \mid 0 \le i < n \ \vee\ i = n : P) \\
= & \langle (8.16) \text{ Range split} \rangle \\
 & (\star i \mid 0 \le i < n : P) \star (\star i \mid i = n : P)
\end{array}
$$

(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

$(\star i \mid 0 \le i < n+1 : P)$

$=$ $\langle$Math, $0 \le i < n+1 \ \equiv\ 0 \le i < n \ \vee\ i = n\rangle$

$(\star i \mid 0 \le i < n \ \vee\ i = n : P)$

$=$ $\langle$(8.16) Range split$\rangle$

$(\star i \mid 0 \le i < n : P) \star (\star i \mid i = n : P)$

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

(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

$(\star i \mid 0 \le i < n+1 : P)$

$=$ ⟨Math, $0 \le i < n+1 \;\equiv\; 0 \le i < n \;\vee\; i = n$⟩

$(\star i \mid 0 \le i < n \;\vee\; i = n : P)$

$=$ ⟨(8.16) Range split⟩

$(\star i \mid 0 \le i < n : P) \star (\star i \mid i = n : P)$

$=$ ⟨(8.14) One-point rule⟩

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

Split off the last term

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

Split off the last term

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

Examples

Split off the last term

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

Examples

$(\Sigma i \mid 0 \leq i < n+1 : b[i])$

Split off the last term

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

Examples

$(\Sigma i \mid 0 \leq i < n+1 : b[i])$

$=$ $\langle$(8.23a)$\rangle$

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

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

Split off the last term

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

Examples

$$(\Sigma i \mid 0 \leq i < n+1 : b[i])$$
$$= \quad \langle (8.23a) \rangle$$
$$(\Sigma i \mid 0 \leq i < n : b[i]) + b[n]$$

$$(\Sigma i \mid 0 \leq i < n : b[i])$$

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

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

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

Split off the last term

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

Examples

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

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

Split off the last term

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

Examples

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

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

Examples

Split off the last term

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

Examples

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

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

Examples

$$(\forall i \mid 0 \leq i \leq n+1 : b[i] = 0)$$

Split off the last term

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

Examples

$$(\Sigma i \mid 0 \leq i < n+1 : b[i])$$
$$= \quad \langle (8.23a) \rangle$$
$$(\Sigma i \mid 0 \leq i < n : b[i]) + b[n]$$

$$(\Sigma i \mid 0 \leq i < n : b[i])$$
$$= \quad \langle (8.23a) \rangle$$
$$(\Sigma i \mid 0 \leq i < n-1 : b[i]) + b[n-1]$$

Examples

$$(\forall i \mid 0 \leq i \leq n+1 : b[i] = 0)$$
$$= \quad \langle (8.23a) \rangle$$

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

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

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

Examples

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

Split off the last term

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

Examples

$(\Sigma i \mid 0 \leq i < n+1 : b[i])$

$=$ $\langle (8.23a) \rangle$

$(\Sigma i \mid 0 \leq i < n : b[i]) + b[n]$

$(\Sigma i \mid 0 \leq i < n : b[i])$

$=$ $\langle (8.23a) \rangle$

$(\Sigma i \mid 0 \leq i < n-1 : b[i]) + b[n-1]$

Examples

$(\forall i \mid 0 \leq i \leq n+1 : b[i] = 0)$

$=$ $\langle (8.23a) \rangle$

$(\forall i \mid 0 \leq i \leq n : b[i] = 0) \wedge b[n+1] = 0$

$(\forall i \mid 0 \leq i \leq n : b[i] = 0)$

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

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

$=$ ⟨(8.23a)⟩

$(\Sigma i \mid 0 \le i < n : b[i]) + b[n]$

$(\Sigma i \mid 0 \le i < n : b[i])$

$=$ ⟨(8.23a)⟩

$(\Sigma i \mid 0 \le i < n-1 : b[i]) + b[n-1]$

Examples

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

$=$ ⟨(8.23a)⟩

$(\forall i \mid 0 \le i \le n : b[i] = 0) \wedge b[n+1] = 0$

$(\forall i \mid 0 \le i \le n : b[i] = 0)$

$=$ ⟨(8.23a)⟩

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

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

$= \quad \langle (8.23a) \rangle$

$(\Sigma i \mid 0 \le i < n : b[i]) + b[n]$

$(\Sigma i \mid 0 \le i < n : b[i])$

$= \quad \langle (8.23a) \rangle$

$(\Sigma i \mid 0 \le i < n-1 : b[i]) + b[n-1]$

Examples

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

$= \quad \langle (8.23a) \rangle$

$(\forall i \mid 0 \le i \le n : b[i] = 0) \wedge b[n+1] = 0$

$(\forall i \mid 0 \le i \le n : b[i] = 0)$

$= \quad \langle (8.23a) \rangle$

$(\forall i \mid 0 \le i < n : b[i] = 0) \wedge b[n] = 0$

Split off the first term

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

Split off the first term

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

Examples

Split off the first term

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

<u>Examples</u>

$(\Pi i \mid 0 \leq i < n+1 : b[i])$

Split off the first term

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

Examples

$(\Pi i \mid 0 \leq i < n+1 : b[i])$

$=$ $\langle$(8.23b)$\rangle$

Split off the first term

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

Examples

$(\Pi i \mid 0 \leq i < n+1 : b[i])$

$=$ $\langle$(8.23b)$\rangle$

$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$

Split off the first term

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

Examples

$$(\Pi i \mid 0 \leq i < n+1 : b[i])$$
$$= \quad \langle (8.23b) \rangle$$
$$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$$

$$(\Pi i \mid 1 \leq i < n+1 : b[i])$$

Split off the first term

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

Examples

$$(\Pi i \mid 0 \leq i < n+1 : b[i])$$
$= \quad \langle(8.23b)\rangle$
$$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$$

$$(\Pi i \mid 1 \leq i < n+1 : b[i])$$
$= \quad \langle(8.23b)\rangle$

Split off the first term

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

Examples

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

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

Split off the first term

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

Examples

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

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

Examples

Split off the first term

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

Examples

$(\Pi i \mid 0 \leq i < n+1 : b[i])$

$= \quad \langle (8.23b) \rangle$

$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$

$(\Pi i \mid 1 \leq i < n+1 : b[i])$

$= \quad \langle (8.23b) \rangle$

$b[1] \cdot (\Pi i \mid 1 < i < n+1 : b[i])$

Examples

$(\exists i \mid 0 < i < n : b[i] = 0)$

Split off the first term

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

Examples

$(\Pi i \mid 0 \leq i < n+1 : b[i])$

$=$ ⟨(8.23b)⟩

$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$

$(\Pi i \mid 1 \leq i < n+1 : b[i])$

$=$ ⟨(8.23b)⟩

$b[1] \cdot (\Pi i \mid 1 < i < n+1 : b[i])$

Examples

$(\exists i \mid 0 < i < n : b[i] = 0)$

$=$ ⟨(8.23b)⟩

Split off the first term

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

<u>Examples</u>

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

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

<u>Examples</u>

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

Split off the first term

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

<u>Examples</u>

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

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

<u>Examples</u>

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

$$(\exists i \mid 1 < i < n : b[i] = 0)$$

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

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

$=$ $\langle(8.23b)\rangle$

$b[0] \cdot (\Pi i \mid 0 < i < n+1 : b[i])$

$(\Pi i \mid 1 \le i < n+1 : b[i])$

$=$ $\langle(8.23b)\rangle$

$b[1] \cdot (\Pi i \mid 1 < i < n+1 : b[i])$

Examples

$(\exists i \mid 0 < i < n : b[i] = 0)$

$=$ $\langle(8.23b)\rangle$

$b[1] = 0 \vee (\exists i \mid 1 < i < n : b[i] = 0)$

$(\exists i \mid 1 < i < n : b[i] = 0)$

$=$ $\langle(8.23b)\rangle$

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

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

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

Examples

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

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

(a) $2 \leq i \leq 15$

(b) $2 \leq i < 16$

(c) $1 < i \leq 15$

(d) $1 < i < 16$