Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-22

Plan for Today

- **Textbook Chapters 8 and 9: Quantification and Predicate Logic**
  - **Variable Binding:** Interplay between Substitution and Quantification
  - **Universal and Existential Quantification**

General Shape of Universal and Existential Quantifications

$$(\forall\, x : t_1; y, z : t_2 \mid R \bullet P)$$

$$(\exists\, x : t_1; y, z : t_2 \mid R \bullet P)$$

- Any number of **variables** x, y, z can be quantified over
- The quantified variables may have **type annotations** (which act as **type declarations**)
- $R : \mathbb{B}$ is the **range** of the quantification
- $P : \mathbb{B}$ is the **body** of the quantification
- Both R and P may refer to the **quantified variables** x, y, z
- The type of the whole quantification expression is $\mathbb{B}$.
- The range defaults to *true*: $(\forall\, x \bullet P) \quad = \quad (\forall\, x \mid true \bullet P)$
  $(\exists\, x \bullet P) \quad = \quad (\exists\, x \mid true \bullet P)$

  ("syntactic sugar", covered by reflexivity of $\equiv$)

Bound / Free Variable Occurrences

(8.7) $(\forall\, i \bullet x \cdot i = 0)$ LADM example expression

Is this true or false? In which states?

We have: $(\forall\, i \bullet x \cdot i = 0) \quad \equiv \quad x = 0$

The value of (8.7) in a state depends only on x, not on i!

Renaming quantified variables does not change the meaning:

$$(\forall\, i \bullet x \cdot i = 0) \quad \equiv \quad (\forall\, j \bullet x \cdot j = 0)$$

- **Occurrences** of quantified variables inside the quantified expression are **bound**
- **Variable occurences** in an expression where they are not bound are **free**

$$i > 0 \vee (\forall\, i \mid 0 \le i \bullet x \cdot i = 0)$$

- The variable declarations after the quantification operator may be called **binding occurrences**.

Textual Substitution Revisited

Let E and R be expressions and let x be a variable. **Original definition:**

> We write: $E[x := R]$ or E^x_R
> to denote an expression that is the same as E but with all occurrences of x replaced by (R).

This was for expressions E built from **constants, variables, operator applications** only!

In presence of **variable binders**, such as $\sum$, $\prod$, $\forall$, $\exists$ and substitution,

- only **free** occurrences of x can be replaced
- **and** we need to avoid **"capture of free variables"**:

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

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

LADM Chapter 8:

"$\star$ is a **metavariable** for operators $\_+\_$, $\_\cdot\_$, $\_\wedge\_$, $\_\vee\_$ (resp. $\sum$, $\prod$, $\forall$, $\exists$)

(8.11) is part of the Substitution keyword in CalcCheck.

Read LADM Chapter 8!

Substitution Examples

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

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

- $(\sum\, x \mid 1 \le x \le 2 \bullet y)[y := y + z]$
  $=$ ⟨ substitution ⟩
  $(\sum\, x \mid 1 \le x \le 2 \bullet y + z)$

- $(\sum\, x \mid 1 \le x \le 2 \bullet y)[y := y + x]$
  $=$ ⟨ (8.21) Variable renaming ⟩
  $(\sum\, z \mid 1 \le z \le 2 \bullet y)[y := y + x]$
  $=$ ⟨ substitution ⟩
  $(\sum\, z \mid 1 \le z \le 2 \bullet y + x)$

Renaming of Bound Variables

(8.21) **Axiom, Dummy renaming** (α-conversion):

$$(\star\, x \mid R \bullet P) \quad = \quad (\star\, y \mid R[x := y] \bullet P[x := y])$$

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

$(\sum i \mid 0 \le i < k \bullet n^i)$

$=$ ⟨ Dummy renaming (8.21), $\neg occurs(`j', `0 \le i < k,\ n^i')$ ⟩

$(\sum j \mid 0 \le j < k \bullet n^j)$

$(\sum i \mid 0 \le i < k \bullet n^i)$

? ⟨ Dummy renaming (8.21)⟩ ×

$(\sum k \mid 0 \le k < k \bullet n^k)$

In CalcCheck, renaming of bound variables is part of "Reflexivity of =",
but can also be mentioned explicitly.

Substitution Examples (ctd.)

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

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

- $(\sum x \mid 1 \le x \le 2 \bullet y)[x := y + x]$
  $=$ ⟨ (8.21) Variable renaming ⟩
  $(\sum z \mid 1 \le z \le 2 \bullet y)[x := y + x]$
  $=$ ⟨ Substitution ⟩
  $(\sum z \mid 1 \le z \le 2 \bullet y)$
  $=$ ⟨ (8.21) Variable renaming ⟩
  $(\sum x \mid 1 \le x \le 2 \bullet y)$

(8.11f) Provided $\neg occurs(`x', `E')$,

$$E[x := F] \quad = \quad E$$

Leibniz Rules for Quantification

Try to use $x + x = 2 \cdot x$ to obtain:

$$(\sum x \mid 0 \le x < 9 \bullet x + x) = (\sum x \mid 0 \le x < 9 \bullet 2 \cdot x)$$

Not possible with (1.5)! — $E[z := X] = E[z := Y]$ **renames x!**

(8.12) **Leibniz** $\dfrac{P = Q}{(\star\, x \mid E[z := P] \bullet S) = (\star\, x \mid E[z := Q] \bullet S)}$

(8.12) **Leibniz** $\dfrac{R \Rightarrow P = Q}{(\star\, x \mid R \bullet E[z := P]) = (\star\, x \mid R \bullet E[z := Q])}$

(These **inference rules** will also be used **implicitly**.)

Important: $P = Q$ needs to be a **theorem**!

These rules are **not** available for local **Assumptions**!

(Because x may occur in P, Q.)

Variable Binding Rearrangements

(8.19) **Axiom, Interchange of dummies:**

$$(\star\, x \mid R \bullet (\star\, y \mid S \bullet P)) \quad = \quad (\star\, y \mid S \bullet (\star\, x \mid R \bullet P))$$

provided $\neg occurs('y', 'R')$ and $\neg occurs('x', 'S')$, and each quantification is defined.

(8.20) **Axiom, Nesting:**

$$(\star\, x, y \mid R \wedge S \bullet P) \quad = \quad (\star\, x \mid R \bullet (\star\, y \mid S \bullet P))$$

provided $\neg occurs('y', 'R')$.

(8.21) **Axiom, Dummy renaming** (α-conversion):

$$(\star\, x \mid R \bullet P) \quad = \quad (\star\, y \mid R[x := y] \bullet P[x := y])$$

provided $\neg occurs('y', 'R, P')$.

***Substitution* (8.11) *prevents capture of* y *by binders in* R *or* P**

Permutation of Bound Variables

Apparently not provable for general quantification from the quantification axioms in the textbook:

(8.20a) **Dummy List Permutation:**

$$(\star\, x, y \mid R \bullet P) \quad = \quad (\star\, y, x \mid R \bullet P)$$

(without side conditions restricting variable occurrences!)

However, the following are easily provable from (8.19) — **Exercise:**

(8.20a$\forall$) **Dummy List Permutation for $\forall$:**

$$(\forall\, x, y \mid R \bullet P) \quad = \quad (\forall\, y, x \mid R \bullet P)$$

(8.20a$\exists$) **Dummy List Permutation for $\exists$:**

$$(\exists\, x, y \mid R \bullet P) \quad = \quad (\exists\, y, x \mid R \bullet P)$$

Instantiation for $\forall$

$$
\begin{array}{ll}
& P[x := E] \\
\equiv & \langle \text{(8.14) One-point rule} \rangle \\
& (\forall\, x \mid x = E \bullet P) \\
\Leftarrow & \langle \text{(9.10) Range weakening for } \forall \rangle \\
& (\forall\, x \mid true \vee x = E \bullet P) \\
\equiv & \langle \text{(3.29) Zero of } \vee \rangle \\
& (\forall\, x \mid true \bullet P) \\
\equiv & \langle\, true \text{ range in quantification} \rangle \\
& (\forall\, x \bullet P)
\end{array}
$$

This proves:

(9.13) **Instantiation:** $(\forall\, x \bullet P) \quad \Rightarrow \quad P[x := E]$

The one-point rule is **"sharper"** than Instantiation.

Using sharper rules often means fewer dead ends...

A sharp version obtained via (3.60): $(\forall\, x \bullet P) \quad \equiv \quad (\forall\, x \bullet P) \wedge P[x := E]$

Using Instantiation for $\forall$

(9.13) **Instantiation:** $(\forall\, x \bullet P) \quad \Rightarrow \quad P[x := E]$

A sharp version of Instantiation obtained via (3.60): $(\forall\, x \bullet P) \equiv (\forall\, x \bullet P) \wedge P[x := E]$

Proving $(\forall\, x \bullet x+1 > x) \quad \Rightarrow \quad y+2 > y$**:**

$$
\begin{array}{ll}
& (\forall\, x \bullet x+1 > x) \\
= & \langle \text{ Instantiation (9.13) with (3.60) } \rangle \\
& (\forall\, x \bullet x+1 > x) \quad \wedge \quad y+1 > y \\
\Rightarrow & \langle \text{ Left-Monotonicity of } \wedge \text{ (4.3) with Instantiation (9.13) } \rangle \\
& (y+1)+1 > y+1 \quad \wedge \quad y+1 > y \\
\Rightarrow & \langle \text{ Transitivity of } > \text{ (15.41) } \rangle \\
& y+1+1 > y \\
= & \langle\, 1+1 = 2 \,\rangle \\
& y+2 > y
\end{array}
$$

Recall: `with` ...

$$
\begin{array}{ll}
& \neg\,(a \cdot b = a \cdot 0) \\
\equiv & \langle \text{ “Cancellation of ·” with Assumption `}a \neq 0\text{` } \rangle \\
& \neg\,(b = 0)
\end{array}
$$

In a hint of shape “*HintItem1* `with` *HintItem2* `and` *HintItem3*”:

- If *HintItem1* refers to a theorem of shape $p \Rightarrow q$,
- then *HintItem2* and *HintItem3* are used to prove p
- and q is used in the surrounding proof.

Here:

- *HintItem1* is “Cancellation of ·”: $z \neq 0 \Rightarrow (z \cdot x = z \cdot y \quad \equiv \quad x = y)$
- *HintItem2* is “Assumption $a \neq 0$”
- The surrounding proof uses: $a \cdot b = a \cdot 0 \quad \equiv \quad b = 0$

Monotonicity `with` ...

$$
\begin{array}{ll}
& (\forall\, x \bullet x+1 > x) \quad \wedge \quad y+1 > y \\
\Rightarrow & \langle \text{ Left-Monotonicity of } \wedge \text{ (4.3) with Instantiation (9.13) } \rangle \\
& (y+1)+1 > y+1 \quad \wedge \quad y+1 > y
\end{array}
$$

In a hint of shape “*HintItem1* `with` *HintItem2* `and` *HintItem3*”:

- If *HintItem1* refers to a theorem of shape $p \Rightarrow q$,
- then *HintItem2* and *HintItem3* are used to prove p
- and q is used in the surrounding proof.

Here:

- *HintItem1* is “Left-Monotonicity of $\wedge$”: $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$
- *HintItem2* is “Instantiation”: $\begin{array}{ll} & (\forall\, x \bullet x+1 > x) \\ \Rightarrow & (y+1)+1 > y+1 \end{array}$
- The surrounding proof uses: $\begin{array}{ll} & (\forall\, x \bullet x+1 > x) \quad \wedge \quad y+1 > y \\ \Rightarrow & (y+1)+1 > y+1 \quad \wedge \quad y+1 > y \end{array}$

Using Instantiation for ∀

(9.13) **Instantiation:** $(\forall x \bullet P) \quad \Rightarrow \quad P[x := E]$

A sharp version of Instantiation obtained via (3.60): $(\forall x \bullet P) \;\equiv\; (\forall x \bullet P) \land P[x := E]$

```
Theorem: (∀ x : ℕ • x < x + 1) ⇒ y < y + 2
Proof:
    ∀ x : ℕ • x < x + 1
  ≡⟨ “Instantiation” with (3.60) ⟩
    (∀ x : ℕ • x < x + 1) ∧ (x < x + 1)[x ≔ y]
  ≡⟨ Substitution ⟩
    (∀ x : ℕ • x < x + 1) ∧ y < y + 1
  ⇒⟨ “Monotonicity of ∧” with “Instantiation” ⟩
    (x < x + 1)[x ≔ y + 1] ∧ y < y + 1
  ≡⟨ Substitution ⟩
    y + 1 < (y + 1) + 1  ∧  y < y + 1
  ⇒⟨ “Transitivity of <” with “Shunting” ⟩
    y < y + 1 + 1
  ≡⟨ Evaluation ⟩
    y < y + 2
```

Theorems and Universal Quantification

(9.16) **Metatheorem**: P is a theorem iff $(\forall x \bullet P)$ is a theorem.

LHS ⇒ RHS: Assume P is a theorem, then $P \equiv \mathit{true}$ by (3.7).

$$
\begin{array}{ll}
 & (\forall x \bullet P) \\
\equiv & \langle \text{ Leibniz (8.12) with } P = \mathit{true} \rangle \\
 & (\forall x \bullet \mathit{true}) \\
\equiv & \langle \text{ (9.8) } \quad (\forall x \bullet \mathit{true}) \equiv \mathit{true} \rangle \\
 & \mathit{true}
\end{array}
$$

RHS ⇒ LHS:

$$
\begin{array}{ll}
 & (\forall x \bullet P) \\
\Rightarrow & \langle \text{ (9.13) Instantiation } \rangle \\
 & P[x := x] \\
\equiv & \langle \text{ Substitution } \rangle \\
 & P
\end{array}
$$

Implicit Universal Quantification in Theorems

(9.16) **Metatheorem**: P is a theorem iff $(\forall x \bullet P)$ is a theorem.

Proof method: To prove $(\forall x \mid R \bullet P)$,
we prove P for arbitrary x in range R.

That is:

- Assume R to prove P (and assume nothing else that mentions x)
- This proves $R \Rightarrow P$
- Then, by (9.16), $(\forall x \bullet R \Rightarrow P)$ is a theorem.
- With (9.2) Trading for ∀, this is transformed into $(\forall x \mid R \bullet P)$.

In CalcCheck:

Proving $(\forall v : \mathbb{N} \bullet P)$:	**For any ‘$v : \mathbb{N}$‘:** *Proof for P*
Proving $(\forall v : \mathbb{N} \mid R \bullet P)$:	**For any ‘$v : \mathbb{N}$‘ satisfying ‘R‘:** *Proof for P using* **Assumption** R

Using "**For any**" for "Proof by Generalisation"

In CalcCheck:

- Proving $(\forall v : \mathbb{N} \bullet P)$:

For any '$v : \mathbb{N}$'**:**
Proof for P

Proving $\forall x : \mathbb{N} \bullet x < x + 1$**:**

For any \`$x : \mathbb{N}$\`:

$$
\begin{aligned}
& x < x + 1 \\
\equiv\ & \langle \text{Identity of } + \rangle \\
& x + 0 < x + 1 \\
\equiv\ & \langle \text{Cancellation of } + \rangle \\
& 0 < 1 \\
\equiv\ & \langle \text{Fact `}1 = \mathsf{suc}\ 0\text{`} \rangle \\
& 0 < \mathsf{suc}\ 0 \\
\equiv\ & \langle \text{Zero is less than successor} \rangle \\
& \mathit{true}
\end{aligned}
$$

Using "**For any … satisfying**" for "Proof by Generalisation"

In CalcCheck:

- Proving $(\forall v : \mathbb{N} \mid R \bullet P)$:

For any '$v : \mathbb{N}$' **satisfying** 'R'**:**
Proof for P using **Assumption** *R*

Proving $\forall x : \mathbb{N} \mid x < 2 \bullet x < 3$ **:**

For any \`$x : \mathbb{N}$\` satisfying \`$x < 2$\`:

$$
\begin{aligned}
& x \\
<\ & \langle \text{Assumption `}x < 2\text{`} \rangle \\
& 2 \\
\equiv\ & \langle \text{Fact `}2 < 3\text{`} \rangle \\
& 3
\end{aligned}
$$