Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-23

Plan for Today

- **Textbook Chapters 8:** General Quantification
  - … using metavariable $\star$ for operators
  - Theorems that work for all quantification operators
- **Textbook Chapters 9:** Predicate Logic
  - **Universal and Existential Quantification**

Quantification Examples

$$
\begin{array}{ll}
 & (\sum i \mid 0 \leq i < 4 \bullet i \cdot 8) \\
= & \langle \text{Quantification expansion, substitution} \rangle \\
 & 0 \cdot 8 + 1 \cdot 8 + 2 \cdot 8 + 3 \cdot 8
\end{array}
$$

$$
\begin{array}{ll}
 & (\prod i \mid 0 \leq i < 3 \bullet i + (i + 1)) \\
= & \langle \text{Quantification expansion, substitution} \rangle \\
 & (0 + 1) \cdot (1 + 2) \cdot (2 + 3)
\end{array}
$$

$$
\begin{array}{ll}
 & (\forall i \mid 1 \leq i < 3 \bullet i \cdot d \neq 6) \\
= & \langle \text{Quantification expansion, substitution} \rangle \\
 & 1 \cdot d \neq 6 \wedge 2 \cdot d \neq 6
\end{array}
$$

$$
\begin{array}{ll}
 & (\exists i \mid 0 \leq i < 21 \bullet b.i = 0) \\
= & \langle \text{Quantification expansion, substitution} \rangle \\
 & b.0 = 0 \vee b.1 = 0 \vee \boxed{\ldots} \vee b.20 = 0
\end{array}
$$

General Quantification

It works not only for $+$, $\wedge$, $\vee$ ...

Let a type T and an operator $\star : T \times T \to T$ be given.
If for an appropriate $u : T$ we have:

- **Symmetry:** $b \star c = c \star b$
- **Associativity:** $(b \star c) \star d = b \star (c \star d)$
- **Identity** u**:** $u \star b = b = b \star u$

we may use $\star$ as quantification operator:

$$(\star\, x : T_1, y : T_2 \mid R \bullet P)$$

- $R : \mathbb{B}$ is the **range** of the quantification
- $P : T$ is the **body** of the quantification
- P and R may refer to the **quantified variables** x and y
- The type of the whole quantification expression is T.

General Quantification: Instances

Let a type T and an operator $\star : T \times T \to T$ be given.
If for an appropriate $u : T$ we have:

- **Symmetry:** $b \star c = c \star b$
- **Associativity:** $(b \star c) \star d = b \star (c \star d)$
- **Identity** u**:** $u \star b = b = b \star u$

we may use $\star$ as quantification operator: $(\star\, x : T_1, y : T_2 \mid R \bullet P)$

- $\vee : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ is symmetric (3.24), associative (3.25) and has *false* as identity (3.30):

$$(\vee\, k : \mathbb{N} \mid k > 0 \bullet k \cdot k < k + 1)$$
$$(\exists\, k : \mathbb{N} \mid k > 0 \bullet k \cdot k < k + 1)$$

- $\wedge : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ is symmetric (3.36), associative (3.27) and has *true* as identity (3.39):

$$(\ \wedge\, k : \mathbb{N} \mid k > 2 \bullet \mathit{prime}\ k \Rightarrow \neg \mathit{prime}(k + 1)\ )$$
$$(\ \forall\, k : \mathbb{N} \mid k > 2 \bullet \mathit{prime}\ k \Rightarrow \neg \mathit{prime}(k + 1)\ )$$

Quantification Examples — Notation

$$\begin{aligned} & (+\, i \mid 0 \le i < 4 \bullet i \cdot 8) \\ = \ & \langle \text{ switching to conventional “quantifier” } \rangle \\ & (\textstyle\sum i \mid 0 \le i < 4 \bullet i \cdot 8) \end{aligned}$$

$$\begin{aligned} & (\cdot\, i \mid 0 \le i < 3 \bullet i + (i + 1)) \\ = \ & \langle \text{ switching to conventional “quantifier” } \rangle \\ & (\textstyle\prod i \mid 0 \le i < 3 \bullet i + (i + 1)) \end{aligned}$$

$$\begin{aligned} & (\wedge\, i \mid 1 \le i < 3 \bullet i \cdot d \ne 6) \\ = \ & \langle \text{ switching to conventional “quantifier” } \rangle \\ & (\forall\, i \mid 1 \le i < 3 \bullet i \cdot d \ne 6) \end{aligned}$$

$$\begin{aligned} & (\vee\, i \mid 0 \le i < 21 \bullet b\ i = 0) \\ = \ & \langle \text{ switching to conventional “quantifier” } \rangle \\ & (\exists\, i \mid 0 \le i < 21 \bullet b\ i = 0) \end{aligned}$$

Trivial Range Axioms

(8.13) **Axiom, Empty Range** (where u is the identity of $\star$):

$$
\begin{aligned}
(\star\, x \mid false \bullet P) &= u \\
(\forall\, x \mid false \bullet P) &= true \\
(\exists\, x \mid false \bullet P) &= false \\
(\sum\, x \mid false \bullet P) &= 0
\end{aligned}
$$

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

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

Distributivity

(8.15) **Axiom,** (Quantification) **Distributivity:**

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

provided each quantification is defined.

$$
\begin{aligned}
& (\sum\, i : \mathbb{N} \mid i < n \bullet f\, i) + (\sum\, i : \mathbb{N} \mid i < n \bullet g\, i) \\
= \; & \langle \text{ Quantification Distributivity (8.15) } \rangle \\
& (\sum\, i : \mathbb{N} \mid i < n \bullet f.i + g.i)
\end{aligned}
$$

Note: Some quantifications are not defined, e.g.: $(\sum n : \mathbb{N} \bullet n)$

Note that quantifications over $\wedge$ or $\vee$ are always defined:

$$(\forall\, x \mid R \bullet P) \wedge (\forall\, x \mid R \bullet Q) = (\forall\, x \mid R \bullet P \wedge Q)$$

$$(\exists\, x \mid R \bullet P) \vee (\exists\, x \mid R \bullet Q) = (\exists\, x \mid R \bullet P \vee Q)$$

Disjoint Range Split

(8.16) **Axiom, Range Split:**

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

provided $R \wedge S = false$ and each quantification is defined.

$$(\Sigma\, x \mid R \vee S \bullet P) = (\Sigma\, x \mid R \bullet P) + (\Sigma\, x \mid S \bullet P)$$

provided $R \wedge S = false$ and each sum is defined.

$$(\forall\, x \mid R \vee S \bullet P) = (\forall\, x \mid R \bullet P) \wedge (\forall\, x \mid S \bullet P)$$

provided $R \wedge S = false$.

$$(\exists\, x \mid R \vee S \bullet P) = (\exists\, x \mid R \bullet P) \vee (\exists\, x \mid S \bullet P)$$

provided $R \wedge S = false$.

Range Split "Axioms"

(8.16) **Axiom, Range Split:**

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

provided $R \wedge S = \mathit{false}$ and each quantification is defined.

(8.17) **Axiom, Range Split:**

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

provided each quantification is defined.

(8.18) **Axiom, Range Split for idempotent $\star$:**

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

provided each quantification is defined.

Range Split for Idempotent Operators

(8.18) **Axiom, Range Split for idempotent $\star$:**

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

provided each quantification is defined.

$$(\forall\, x \mid R \vee S \bullet P) = (\forall\, x \mid R \bullet P) \wedge (\forall\, x \mid S \bullet P)$$

$$(\exists\, x \mid R \vee S \bullet P) = (\exists\, x \mid R \bullet P) \vee (\exists\, x \mid S \bullet P)$$

Manipulating Ranges

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

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

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

- Typical use: Verification of loops
- Generalisation: $\mathbb{N} \longrightarrow \mathbb{Z}$, $\quad 0 \longrightarrow m : \mathbb{Z}$ (with $m \le n$)

The following work both with $m, n, i : \mathbb{N}$ and with $m, n, i : \mathbb{Z}$:

Theorem: Split off term from top:

$$m \le n \Rightarrow (\star\, i \mid m \le i < n+1 \bullet P) = (\star\, i \mid m \le i < n \bullet P) \star P[i := n]$$

Theorem: Split off term from bottom:

$$m \le n \Rightarrow (\star\, i \mid m \le i < n+1 \bullet P) = P[i := m] \star (\star\, i \mid m+1 \le i < n+1 \bullet P)$$

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 $\forall$, 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 \`$x : \mathbb{N}$\`:

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

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 \`$x < 2$\`:

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

$\exists$-Introduction

$$
\begin{array}{ll}
 & P[x := E] \\
= & \langle \text{ (8.14) One-point rule } \rangle \\
 & (\exists\, x \mid x = E \bullet P) \\
\Rightarrow & \langle \text{ (9.25) Range weakening for } \exists \rangle \\
 & (\exists\, x \mid \mathit{true} \lor x = E \bullet P) \\
= & \langle \text{ (3.29) Zero of } \lor \rangle \\
 & (\exists\, x \mid \mathit{true} \bullet P) \\
= & \langle\, \mathit{true} \text{ range in quantification } \rangle \\
 & (\exists\, x \bullet P)
\end{array}
$$

This proves:

(9.28) **$\exists$-Introduction:** $P[x := E] \quad \Rightarrow \quad (\exists\, x \bullet P)$

An expression E with $P[x := E]$ is called a "**witness**" of $(\exists\, x \bullet P)$.