Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-25

Plan for Today

- **Predicate Logic** (Textbook Chapter 9)
  - Properties of Universal and Existential Quantification
  - "Sentences"
- **Sequences** (Textbook Chapter 13)
  - Inductive view from empty sequence (ϵ) and "cons" ($\triangleleft$)

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

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

Using ∃-Introduction for "Proof by Example"

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

$$
\begin{array}{ll}
& (\exists\, x : \mathbb{N} \bullet x \cdot x < x + x) \\
\Leftarrow & \langle\ \exists\text{-Introduction}\ \rangle \\
& (x \cdot x < x + x)[x := 1] \\
\equiv & \langle\ \text{Substitution}\ \rangle \\
& 1 \cdot 1 < 1 + 1 \\
\equiv & \langle\ \text{Evaluation}\ \rangle \\
& \mathit{true}
\end{array}
$$

Using ∃-Introduction for "Proof by Counter-Example"

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

$$
\begin{array}{ll}
& \neg(\forall\, x : \mathbb{N} \bullet x + x < x \cdot x) \\
\equiv & \langle\ \text{Generalised De Morgan}\ \rangle \\
& (\exists\, x : \mathbb{N} \bullet \neg(x + x < x \cdot x)) \\
\Leftarrow & \langle\ \exists\text{-Introduction}\ \rangle \\
& (\neg(x + x < x \cdot x))[x := 2] \\
\equiv & \langle\ \text{Substitution}\ \rangle \\
& \neg(2 + 2 < 2 \cdot 2) \\
\equiv & \langle\ \text{Fact `}2 + 2 < 2 \cdot 2 \equiv \mathit{false}\text{`}\ \rangle \\
& \neg \mathit{false} \\
\equiv & \langle\ \text{Negation of } \mathit{false}\ \rangle \\
& \mathit{true}
\end{array}
$$

Sentences

Definition: A sentence is a Boolean expression without free variables.

- Expressions without free variables are also called "closed":
  A sentence is a closed Boolean expression.
- The value of an expression only depends on its free variables.
- The value of a closed expression does not depend on the state.
- A closed Boolean expression, or sentence,
  - either always evaluates to *true*
  - or always evaluates to *false*
- A closed Boolean expression, or sentence,
  - is either valid
  - or a contradiction
- For a closed Boolean expression, or sentence, ϕ
  - either ϕ is valid
  - or $\neg\phi$ is valid
- For a closed Boolean expression, or sentence, ϕ,
  only one of ϕ and $\neg\phi$ can have a proof!

2018 Midterm 2

- For a closed Boolean expression, or sentence, ϕ,
  only one of ϕ and $\neg\phi$ can have a proof!

Prove one of the following two theorem statements — **only one is valid.** (Should be easy in less than ten steps.)

```
Theorem “M2-3A-1-yes”: (∃ x : ℤ • ∀ y : ℤ • (x - 2) · y + 1 = x - 1)

Theorem “M2-3A-1-no”: ¬ (∃ x : ℤ • ∀ y : ℤ • (x - 2) · y + 1 = x - 1)
```

Monotonicity With Respect To ⇒

(4.2) Left-Monotonicity of ∨:	$(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$
(4.3) Left-Monotonicity of ∧:	$(p \Rightarrow q) \Rightarrow p \wedge r \Rightarrow q \wedge r$
Antitonicity of ¬:	$(p \Rightarrow q) \Rightarrow \neg q \Rightarrow \neg p$
Left-Antitonicity of ⇒:	$(p \Rightarrow q) \Rightarrow (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
Right-Monotonicity of ⇒:	$(p \Rightarrow q) \Rightarrow (r \Rightarrow p) \Rightarrow (r \Rightarrow q)$
Guarded Right-Monotonicity of ⇒:	$(r \Rightarrow (p \Rightarrow q)) \Rightarrow (r \Rightarrow p) \Rightarrow (r \Rightarrow q)$

Weakening/Strengthening for ∀ and ∃ — “Cheap Antitonicity/Monotonicity”

(9.10) **Range** weakening/**strengthening for ∀:**	$(\forall x \mid Q \vee R \bullet P) \Rightarrow (\forall x \mid Q \bullet P)$
(9.11) **Body weakening**/strengthening **for ∀:**	$(\forall x \mid R \bullet P \wedge Q) \Rightarrow (\forall x \mid R \bullet P)$
(9.25) **Range weakening**/strengthening **for ∃:**	$(\exists x \mid R \bullet P) \Rightarrow (\exists x \mid Q \vee R \bullet P)$
(9.26) **Body weakening**/strengthening **for ∃:**	$(\exists x \mid R \bullet P) \Rightarrow (\exists x \mid R \bullet P \vee Q)$

Monotonicity for ∀

(9.12) **Monotonicity of ∀:**

$$(\forall x \mid R \bullet P_1 \Rightarrow P_2) \Rightarrow \big((\forall x \mid R \bullet P_1) \Rightarrow (\forall x \mid R \bullet P_2)\big)$$

(9.12a) **Range-Antitonicity of ∀:**

$$(\forall x \bullet R_2 \Rightarrow R_1) \Rightarrow \big((\forall x \mid R_1 \bullet P) \Rightarrow (\forall x \mid R_2 \bullet P)\big)$$

$(\forall x \bullet R_2 \Rightarrow R_1)$

$\Rightarrow$ ⟨ (9.12) with shunted (3.82a) Transitivity of $\Rightarrow$ ⟩

$(\forall x \bullet (R_1 \Rightarrow P) \Rightarrow (R_2 \Rightarrow P))$

$\Rightarrow$ ⟨ (9.12) Monotonicity of ∀ ⟩

$(\forall x \bullet R_1 \Rightarrow P) \Rightarrow (\forall x \bullet R_2 \Rightarrow P)$

$=$ ⟨ (9.2) Trading for ∀ ⟩

$(\forall x \mid R_1 \bullet P) \Rightarrow (\forall x \mid R_2 \bullet P)$

Monotonicity for ∃

(9.27) (Body) **Monotonicity of ∃:**

$$(\forall x \mid R \bullet P_1 \Rightarrow P_2) \Rightarrow \big((\exists x \mid R \bullet P_1) \Rightarrow (\exists x \mid R \bullet P_2)\big)$$

(9.27a) **Range-Monotonicity of ∃:**

$$(\forall x \bullet R_1 \Rightarrow R_2) \Rightarrow \big((\exists x \mid R_1 \bullet P) \Rightarrow (\exists x \mid R_2 \bullet P)\big)$$

Witnesses

(9.30v) **Metatheorem Witness**: If $\neg occurs(`x', `Q')$, then:

$(\exists x \mid R \bullet P) \Rightarrow Q$ is a theorem iff $(R \wedge P) \Rightarrow Q$ is a theorem

---

Theorem "Witness": $(\exists x \mid R \bullet P) \Rightarrow Q \quad \equiv \quad (\forall x \bullet R \wedge P \Rightarrow Q)$ prov. $\neg occurs(`x', `Q')$

Proof:

$(\exists x \mid R \bullet P) \Rightarrow Q$

$=$ ⟨ (9.19) Trading for ∃ ⟩

$(\exists x \bullet R \wedge P) \Rightarrow Q$

$=$ ⟨ (3.59) $p \Rightarrow q \equiv \neg p \vee q$, (9.18b) Gen. De Morgan ⟩

$(\forall x \bullet \neg(R \wedge P)) \vee Q$

$=$ ⟨ (9.5) Distributivity of ∨ over ∀ — $\neg occurs(`x', `Q')$ ⟩

$(\forall x \bullet \neg(R \wedge P) \vee Q)$

$=$ ⟨ (3.59) $p \Rightarrow q \equiv \neg p \vee q$ ⟩

$(\forall x \bullet R \wedge P \Rightarrow Q)$

The last line is, by (9.16) Univeral quantification in theorems, a theorem iff $(R \wedge P) \Rightarrow Q$ is.

Witnesses (ctd.)

(9.30v) **Metatheorem Witness**: If $\neg occurs(`x', `Q')$, then:

$(\exists\, x \mid R \bullet P) \Rightarrow Q$ is a theorem iff $(R \wedge P) \Rightarrow Q$ is a theorem

(9.30) **Metatheorem Witness**: If $\neg occurs(`\hat{x}', `P, Q, R')$, then:

$$\begin{array}{ll} (\exists\, x \mid R \bullet P) \Rightarrow Q & \text{is a theorem iff} \\ (R \wedge P)[x := \hat{x}] \Rightarrow Q & \text{is a theorem.} \end{array}$$

Witnesses: Using Existential Assumptions/Theorems

(9.30) **Metatheorem Witness**: If $\neg occurs(`\hat{x}', `P, Q, R')$, then:

$$\begin{array}{ll} (\exists\, x \mid R \bullet P) \Rightarrow Q & \text{is a theorem iff} \\ (R \wedge P)[x := \hat{x}] \Rightarrow Q & \text{is a theorem.} \end{array}$$

Prove: $a + b = a + c \Rightarrow b = c$, using:

(9.31) $(\exists\, x : \mathbb{Z} \bullet x + a = 0)$

(9.30) turns this into $(x + a = 0)[x := \alpha]$, so we use $\alpha + a = 0$.

$$\begin{array}{ll} & a + b = a + c \\ \Rightarrow & \langle \text{ Leibniz, with Deduction Theorem (4.4) } \rangle \\ & \alpha + a + b = \alpha + a + c \\ = & \langle \text{ Assumption } \alpha + a = 0 \ \rangle \\ & 0 + b = 0 + c \\ = & \langle \text{ Additive identity (15.3) } \rangle \\ & b = c \end{array}$$

Predicate Logic Laws You Really Need To Know

(9.2) **Trading for ∀:** $(\forall\, x \mid R \bullet P) \equiv (\forall\, x \bullet R \Rightarrow P)$

(9.4a) **Trading for** ∀: $(\forall\, x \mid Q \wedge R \bullet P) \equiv (\forall\, x \mid Q \bullet R \Rightarrow P)$

(9.19) **Trading for ∃:** $(\exists\, x \mid R \bullet P) \equiv (\exists\, x \bullet R \wedge P)$

(9.20) **Trading for** ∃: $(\exists\, x \mid Q \wedge R \bullet P) \equiv (\exists\, x \mid Q \bullet R \wedge P)$

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

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

(9.17) **Generalised De Morgan**: $(\exists\, x \mid R \bullet P) \equiv \neg(\forall\, x \mid R \bullet \neg P)$

(8.13) **Empty Range**: $(\forall\, x \mid \mathit{false} \bullet P) = \mathit{true}$

$(\exists\, x \mid \mathit{false} \bullet P) = \mathit{false}$

(8.14) **One-point Rule:** Provided $\neg occurs(`x', `E')$, $(\forall x \mid x = E \bullet P) \equiv P[x := E]$

$(\exists x \mid x = E \bullet P) \equiv P[x := E]$

. . . and correctly handle substitution, Leibniz, renaming of bound variables, and monotonicity/antitonicity . . .

Sequences

- We may write $\langle 33, 22, 11\rangle$ for the sequence that has
  - "33" as its first element,
  - "22" as its second element,
  - "11" as its third element, and
  - no further elements.

  (Notation "$\langle\ldots\rangle$" for sequences is not supported by CalcCheck.)
- Sequence matters: $\langle 33, 22, 11\rangle$ and $\langle 11, 22, 33\rangle$ are different!
- Multiplicity matters: $\langle 33, 22, 11\rangle$ and $\langle 33, 22, 22, 11\rangle$ are different!
- We consider the type Seq A of sequences with elements of type A as generated inductively by the following two constructors:

ϵ	:	Seq A	`\eps`	empty sequence
$\triangleleft$	:	$A \to$ Seq $A \to$ Seq A	`\cons`	"cons"

  $\triangleleft$ associates to the right.
- Therefore:

$$\begin{aligned}\langle 33, 22, 11\rangle &= 33 \triangleleft \langle 22, 11\rangle \\ &= 33 \triangleleft 22 \triangleleft \langle 11\rangle \\ &= 33 \triangleleft 22 \triangleleft 11 \triangleleft \epsilon\end{aligned}$$

Concatenation

```
Axiom (13.17) “Left-identity of ⌢”
              “Definition of ⌢ for ϵ”:          ϵ ⌢ ys = ys
Axiom (13.18) “Mutual associativity of ◃ with ⌢”
              “Definition of ⌢ for ◃”:          (x ◃ xs) ⌢ ys = x ◃ (xs ⌢ ys)
```

Sequences — Induction Principle

- The set of all **sequences over type A** is written Seq A.
- The <u>empty sequence</u> "ϵ" is a sequence over type A.
- If x is an element of A and xs is a sequence over type A, then "$x \triangleleft xs$" (pronounced: "x <u>cons</u> xs") is a sequence over type A, too.
- Two sequences are equal **<u>iff</u>** they are constructed the same way from ϵ and $\triangleleft$.

Induction principle for sequences:

- if $P(\epsilon)$ — If P holds for ϵ
- and if $P(xs)$ implies $P(x \triangleleft xs)$ for all $x : A$,
  and whenever P holds for xs, it also holds for any $x \triangleleft xs$,
- then for all xs : Seq A we have $P(xs)$. — then P holds for all sequences over A.

Sequences — Induction Proofs

Induction principle for sequences:

- if $P(\epsilon)$ — $\boxed{\text{If } P \text{ holds for } \epsilon}$
- and if $P(xs)$ implies $P(x \lhd xs)$ **for all** $x : A$,
  $\boxed{\text{and whenever } P \text{ holds for } xs\text{, it also holds for any } x \lhd xs}$,
- then for all $xs : \mathsf{Seq}\ A$ we have $P(xs)$. $\boxed{\text{then } P \text{ holds for all sequences over } A.}$

An **induction proof** using this looks as follows:

Theorem: P

Proof:

By induction on $xs : \mathsf{Seq}\ A$**:**

Base case:

Proof for $P[xs := \epsilon]$

Induction step:

Proof for $(\forall x : A \bullet P[xs := x \lhd xs])$

using **Induction hypothesis** P

(13.7) Tail is different: $x \lhd xs \neq xs$

(13.7) Tail is different: $\forall\ xs : \mathsf{Seq}\ A \bullet \forall\ x : A \bullet x \lhd xs \neq xs$