Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-29

Plan for Today

- **Predicate Logic** (Textbook Chapter 9)
  - Usage Examples
- **Sequences** (Textbook Chapter 13)
  - Inductive view from empty sequence (ϵ) and "cons" ($\triangleleft$)

LADM Theory of Integers — Ordering Properties

(15.41) **Transitivity:**

$$\begin{array}{ll}(a) & a < b \;\wedge\; b < c \;\Rightarrow\; a < c\\ (b) & a \leq b \;\wedge\; b < c \;\Rightarrow\; a < c\\ (c) & a < b \;\wedge\; b \leq c \;\Rightarrow\; a < c\\ (d) & a \leq b \;\wedge\; b \leq c \;\Rightarrow\; a \leq c\end{array}$$

(15.42) **Monotonicity of +:** $a < b \;\equiv\; a + d < b + d$

(15.43) **Monotonicity of $\cdot$:** $0 < d \;\Rightarrow\; (a < b \;\equiv\; a \cdot d < b \cdot d)$

(15.44) **Trichotomy:** $(a < b \;\equiv\; a = b \;\equiv\; a > b) \;\wedge$ $\neg(a < b \;\wedge\; a = b \;\wedge\; a > b)$

(15.45) **Antisymmetry of $\leq$:** $a \leq b \;\wedge\; a \geq b \;\equiv\; a = b$

(15.46) **Reflexivity of $\leq$:** $a \leq a$

(15.47) $a = b \;\equiv\; (\forall z \bullet z \leq a \;\equiv\; z \leq b)$

Indirect Equality

(15.47) $a = b \;\equiv\; (\forall z \bullet z \leq a \;\equiv\; z \leq b)$

Witnesses

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

$$(\exists x \mid R \bullet P) \Rightarrow Q \text{ is a theorem} \qquad \text{iff} \qquad (R \land P) \Rightarrow Q \text{ is a theorem}$$

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

Proof:

$$
\begin{aligned}
& (\exists x \mid R \bullet P) \Rightarrow Q \\
= & \langle \text{(9.19) Trading for } \exists \rangle \\
& (\exists x \bullet R \land P) \Rightarrow Q \\
= & \langle \text{(3.59) } p \Rightarrow q \equiv \neg p \lor q, \text{ (9.18b) Gen. De Morgan} \rangle \\
& (\forall x \bullet \neg(R \land P)) \lor Q \\
= & \langle \text{(9.5) Distributivity of } \lor \text{ over } \forall \text{ — } \neg occurs(`x', `Q') \rangle \\
& (\forall x \bullet \neg(R \land P) \lor Q) \\
= & \langle \text{(3.59) } p \Rightarrow q \equiv \neg p \lor q \rangle \\
& (\forall x \bullet R \land P \Rightarrow Q)
\end{aligned}
$$

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

LADM Theory of Integers — Axioms

(15.1) **Axiom, Associativity:** $(a+b)+c = a+(b+c)$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(15.2) **Axiom, Symmetry:** $a+b = b+a$

$a \cdot b = b \cdot a$

(15.3) **Axiom, Additive identity:** $0+a = a$

(15.4) **Axiom, Multiplicative identity:** $1 \cdot a = a$

(15.5) **Axiom, Distributivity:** $a \cdot (b+c) = a \cdot b + a \cdot c$

(15.6) **Axiom, Additive Inverse:** $(\exists x \bullet x+a = 0)$

(15.7) **Ax., Cancellation of $\cdot$:** $c \neq 0 \Rightarrow (c \cdot a = c \cdot b \equiv a = b)$

(15.8) **Cancellation of $+$:** $a+b = a+c \quad \equiv \quad b = c$

(15.10b) **Unique mult. identity:** $a \neq 0 \Rightarrow (a \cdot z = a \equiv z = 1)$

(15.12) **Unique additive inverse:** $x+a = 0 \land y+a = 0 \Rightarrow x = y$

```
Theorem (15.8) “Cancellation of +”: a + b = a + c  ≡  b = c
Proof:
  Using “Mutual implication”:
    Subproof for `b = c  ⇒  a + b = a + c`:
      Assuming `b = c`:
          a + b
        =⟨ Assumption `b = c` ⟩
          a + c
    Subproof for `a + b = a + c  ⇒  b = c`:
          a + b = a + c  ⇒  b = c
        ≡⟨ “Left-identity of ⇒”, “Additive inverse” with `a = a` ⟩
          (∃ x : ℤ • x + a = 0)  ⇒  a + b = a + c  ⇒  b = c
        ≡⟨ “Witness” ⟩
          ∀ x : ℤ • x + a = 0  ⇒  a + b = a + c  ⇒  b = c
      Proof for this:
        For any `x : ℤ`:
          Assuming `x + a = 0`, `a + b = a + c`:
              b
            =⟨ “Identity of +” ⟩
              0 + b
            =⟨ Assumption `x + a = 0` ⟩
              x + a + b
            =⟨ Assumption `a + b = a + c` ⟩
              x + a + c
            =⟨ Assumption `x + a = 0` ⟩
              0 + c
            =⟨ “Identity of +” ⟩
              c
```

(15.6) **Additive Inverse:**

$(\exists x \bullet x+a = 0)$

(15.8) **Cancellation of $+$:**

$a+b = a+c \quad \equiv \quad b = c$

```
Theorem (15.8) “Cancellation of +”: a + b = a + c  ≡  b = c
Proof:
  Using “Mutual implication”:
    Subproof for `b = c  ⇒  a + b = a + c`:
      Assuming `b = c`:
          a + b
        =⟨ Assumption `b = c` ⟩
          a + c
    Subproof for `a + b = a + c  ⇒  b = c`:
          a + b = a + c  ⇒  b = c
        ≡⟨ “Left-identity of ⇒”, “Additive inverse” with `a = a` ⟩
          (∃ x : ℤ • x + a = 0)  ⇒  a + b = a + c  ⇒  b = c
        ≡⟨ “Witness”, “Trading for ∀” ⟩
          ∀ x : ℤ ❙ x + a = 0  •  a + b = a + c  ⇒  b = c
      Proof for this:
        For any `x : ℤ` satisfying `x + a = 0`:
          Assuming `a + b = a + c`:
              b
            =⟨ “Identity of +” ⟩
              0 + b
            =⟨ Assumption `x + a = 0` ⟩
              x + a + b
            =⟨ Assumption `a + b = a + c` ⟩
              x + a + c
            =⟨ Assumption `x + a = 0` ⟩
              0 + c
            =⟨ “Identity of +” ⟩
              c
```

(15.6) **Additive Inverse:**
$(\exists x \bullet x + a = 0)$

(15.8) **Cancellation of +:**
$a + b = a + c \quad \equiv \quad b = c$

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:

$(\exists x \mid R \bullet P) \Rightarrow Q$ is a theorem iff
$(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem.

(Simplified) Inference Rules —- See LADM p. 133, “Using Z” ch. 2&3

$\dfrac{P \wedge Q}{P}$ $\wedge$-Elim$_1$ $\qquad \dfrac{P \wedge Q}{Q}$ $\wedge$-Elim$_2$ $\qquad \dfrac{\forall x \bullet P}{P[x := E]}$ Instantiation ($\forall$-Elim)

$\dfrac{P}{P \vee Q}$ $\vee$-Intro$_1$ $\qquad \dfrac{Q}{P \vee Q}$ $\vee$-Intro$_2$ $\qquad \dfrac{P[x := E]}{\exists x \bullet P}$ $\exists$-Intro

$\dfrac{P \qquad Q}{P \wedge Q}$ $\wedge$-Intro $\qquad \dfrac{P}{\forall x \bullet P}$ $\forall$-Intro (prov. x not free in assumptions)

$\dfrac{P \vee Q \qquad \begin{matrix} \ulcorner P \urcorner \\ \vdots \\ R \end{matrix} \qquad \begin{matrix} \ulcorner Q \urcorner \\ \vdots \\ R \end{matrix}}{R}$ $\vee$-Elim $\qquad \dfrac{(\exists x \bullet P) \qquad \begin{matrix} \ulcorner P \urcorner \\ \vdots \\ R \end{matrix}}{R}$ $\exists$-Elim (prov. x not free in R, assumptions)

Witnesses: Using Existential Assumptions/Theorems

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

$$(\exists x \mid R \bullet P) \Rightarrow Q \quad \text{is a theorem iff}$$
$$(R \wedge P)[x := \hat{x}] \Rightarrow Q \quad \text{is a theorem.}$$

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 $\alpha + a = 0$.

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

(15.6) **Additive Inverse:**
$(\exists x \bullet x + a = 0)$

(15.8) **Cancellation of +:**
$a + b = a + c \quad \equiv \quad b = c$

```
Theorem (15.8) “Cancellation of +”: a + b = a + c  ≡  b = c
Proof:
  Using “Mutual implication”:
    Subproof for `b = c  ⇒  a + b = a + c`:
      Assuming `b = c`:
          a + b
        =⟨ Assumption `b = c` ⟩
          a + c
    Subproof for `a + b = a + c  ⇒  b = c`:
          a + b = a + c  ⇒  b = c
        ≡⟨ “Left-identity of ⇒”, “Additive inverse” ⟩
          (∃ x : ℤ • x + a = 0)  ⇒  a + b = a + c  ⇒  b = c
      Proof for this:
        Assuming witness `x : ℤ` satisfying `x + a = 0`:
          Assuming `a + b = a + c`:
              b
            =⟨ “Identity of +” ⟩
              0 + b
            =⟨ Assumption `x + a = 0` ⟩
              x + a + b
            =⟨ Assumption `a + b = a + c` ⟩
              x + a + c
            =⟨ Assumption `x + a = 0` ⟩
              0 + c
            =⟨ “Identity of +” ⟩
              c
```

```
Theorem (15.8) “Cancellation of +”: a + b = a + c  ≡  b = c
Proof:
  Using “Mutual implication”:
    Subproof for `b = c  ⇒  a + b = a + c`:
      Assuming `b = c`:
          a + b
        =⟨ Assumption `b = c` ⟩
          a + c
    Subproof for `a + b = a + c  ⇒  b = c`:
      Assuming witness `x : ℤ` satisfying `x + a = 0`
          by “Additive inverse”:
        Assuming `a + b = a + c`:
            b
          =⟨ “Identity of +” ⟩
            0 + b
          =⟨ Assumption `x + a = 0` ⟩
            x + a + b
          =⟨ Assumption `a + b = a + c` ⟩
            x + a + c
          =⟨ Assumption `x + a = 0` ⟩
            0 + c
          =⟨ “Identity of +” ⟩
            c
```

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 ∀:** $(\forall x \mid Q \land R \bullet P) \equiv (\forall x \mid Q \bullet R \Rightarrow P)$

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

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

(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 $\neg \mathit{occurs}(`x', `E')$,
$$(\forall x \mid x = E \bullet P) \equiv P[x := E]$$
$$(\exists x \mid x = E \bullet P) \equiv P[x := E]$$

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

Sequences

- We may write $[33, 22, 11]$ 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 "[. . .]" for sequences is not supported by CalcCheck. LADM writes "$\langle \ldots \rangle$".)
- Sequence matters: $[33, 22, 11]$ and $[11, 22, 33]$ are different!
- Multiplicity matters: $[33, 22, 11]$ and $[33, 22, 22, 11]$ 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:
$$\begin{aligned}[33, 22, 11] &= 33 \triangleleft [22, 11] \\ &= 33 \triangleleft 22 \triangleleft [11] \\ &= 33 \triangleleft 22 \triangleleft 11 \triangleleft \epsilon\end{aligned}$$

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)
```

Membership

```
Axiom “Membership in ϵ”:  x ∈ ϵ        ≡ false
Axiom “Membership in ◃”:  x ∈ y ◃ ys  ≡  x = y ∨ x ∈ ys
```

Subsequences

```
Axiom (13.25) “Empty subsequence”: ϵ ⊆ ys
Axiom (13.26) “Subsequence” “Cons is not a subsequence of ϵ”: ¬ (x ◃ xs ⊆ ϵ)
Axiom (13.27) “Subsequence anchored at head”: x ◃ ys ⊆ x ◃ zs  ≡  ys ⊆ zs
Axiom (13.28) “Subsequence without head”: x ≠ y  ⇒  (x ◃ xs ⊆ y ◃ ys  ≡  x ◃ xs ⊆ ys)
```

Prefixes and Segments — “Contiguous Subsequences”

```
Axiom (13.36) “Empty prefix”:
    isprefix ϵ xs
Axiom (13.37) “Not Prefix” “Cons is not prefix of ϵ”:
    isprefix (x ◃ xs) ϵ ≡ false
Axiom (13.38) “Prefix” “Cons prefix”:
    isprefix (x ◃ xs) (y ◃ ys) = x = y ∧ isprefix xs ys


Axiom (13.39) “Segment” “Segment of ϵ”: isseg xs ϵ  ≡  xs = ϵ
Axiom (13.40) “Segment” “Segment of ◃”:
  isseg xs (y ◃ ys)  ≡  isprefix xs (y ◃ ys) ∨ isseg xs ys
```