# Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-04

## Plan for Today

- **Command Correctness: Consequence Rules, Reversed Presentation**
- **Textbook Chapter 4: Relaxing the Proof Style**

  — nicer implication proofs

  - Proving implications **Assuming** the antecedent
  - Proving **By cases**
  - **Using** theorems as proof methods
    - Proof by Contrapositive
    - Proof by Mutual Implication

## Transitivity Rules for Calculational Command Correctness Reasoning

```
Primitive inference rule "Sequence":
    `P  ⇒[ C₁ ]  Q`,   `Q  ⇒[ C₂ ]  R`
  ⊢─────────────────────────────────────
      `P  ⇒[ C₁ ; C₂ ]  R`
```

Strengthening the precondition:

```
    `P₁ ⇒ P₂`,    `P₂ ⇒[ C ] Q`
 ⊢──────────────────────────────
         `P₁ ⇒[ C ] Q`
```

Weakening the postcondition:

```
    `P ⇒[ C ] Q₁`,    `Q₁ ⇒ Q₂`
 ⊢──────────────────────────────
         `P ⇒[ C ] Q₂`
```

$$\begin{array}{ll} & P \\ \Rrightarrow[\,C_1\,] & \langle \ \ldots \ \rangle \\ & Q \\ \Rightarrow & \langle \ \ldots \ \rangle \\ & Q' \\ \Rrightarrow[\,C_2\,] & \langle \ \ldots \ \rangle \\ & R \end{array}$$

- Activated as transitivity rules
- Therefore used implicitly in calculations, e.g., proving $P \Rrightarrow[\, C_1 \fatsemi C_2\,]\, R$ to the right
- No need to refer to these rules explicitly.

```
Fact: x = 5 ⇒⁅ (y := x + 1 ⨾ x := y + y) ⁆x = 12
Proof:
      x = 5
    ≡ ⟨ “Cancellation of +” ⟩
      x + 1 = 5 + 1
    ≡ ⟨ Fact `5 + 1 = 6` ⟩
      x + 1 = 6
    ≡ ⟨ Substitution ⟩
      (y = 6)[y ≔ x + 1]
    ⇒⁅ y := x + 1 ⁆ ⟨ “Assignment” ⟩
      y = 6
    ≡ ⟨ “Cancellation of ·” with Fact `2 ≠ 0` ⟩
      2 · y = 2 · 6
    ≡ ⟨ Evaluation ⟩
      (1 + 1) · y = 12
    ≡ ⟨ “Distributivity of · over +” ⟩
      1 · y + 1 · y = 12
    ≡ ⟨ “Identity of ·” ⟩
      y + y = 12
    ≡ ⟨ Substitution ⟩
      (x = 12)[x ≔ y + y]
    ⇒⁅ x := y + y ⁆ ⟨ “Assignment” ⟩
      x = 12
```

Using converse operator for backward presentation:

$\_[\_]\Leftarrow\_$

```
Fact: x = 5 ⇒⁅ (y := x + 1 ⨾ x := y + y) ⁆ x =12
Proof:
      x = 12
    ⁅ x := y + y ⁆⇐ ⟨ “Assignment” with Substituti
      y + y = 12
    ≡ ⟨ “Identity of ·” ⟩
      1 · y + 1 · y = 12
    ≡ ⟨ “Distributivity of · over +” ⟩
      (1 + 1) · y = 12
    ≡ ⟨ Evaluation ⟩
      2 · y = 2 · 6
    ≡ ⟨ “Cancellation of ·” with Fact `2 ≠0` ⟩
      y = 6
    ⁅ y := x + 1 ⁆⇐ ⟨ “Assignment” with Substituti
      x + 1 = 6
    ≡ ⟨ Fact `5 + 1 = 6` ⟩
      x + 1 = 5 + 1
    ≡ ⟨ “Cancellation of +” ⟩
      x = 5
```

## (4.3) Left-Monotonicity of ∧ (shorter proof)

(4.3) $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$

PROOF:

**Assume** $p \Rightarrow q$ (which is equivalent to $p \wedge q \equiv p$)

$$
\begin{array}{ll}
 & p \wedge r \\
= & \langle \text{Assumption } p \wedge q \equiv p \rangle \\
 & p \wedge q \wedge r \\
\Rightarrow & \langle \text{(3.76b) Weakening} \rangle \\
 & q \wedge r
\end{array}
$$

How to do “which is equivalent to” in CALCCHECK?

- Transform before assuming
- or transform the assumption when using it
- or “Assuming . . . and using with . . . ”

## Prove Lemma with Transformed Asumption

(4.3) $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$

PROOF:

**Assume** $p \Rightarrow q$ (which is equivalent to $p \wedge q \equiv p$)

$$
\begin{array}{ll}
 & p \wedge r \\
= & \langle \text{Assumption } p \wedge q \equiv p \rangle \\
 & p \wedge q \wedge r \\
\Rightarrow & \langle \text{(3.76b) Weakening} \rangle \\
 & q \wedge r
\end{array}
$$

```
Theorem “Lemma Left-monotonicity of ∧”: (p ∧ q ≡ p) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
  Assuming `p ∧ q ≡ p`:
      p ∧ r
    ≡⟨ Assumption `p ∧ q ≡ p` ⟩
      p ∧ q ∧ r
    ⇒⟨ “Weakening” (3.76b) ⟩
      q ∧ r
```

## Prove Lemma with Transformed Asumption (ctd.)

```
Theorem “Lemma Left-monotonicity of ∧”: (p ∧ q ≡ p) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
  Assuming `p ∧ q ≡ p`:
      p ∧ r
    ≡⟨ Assumption `p ∧ q ≡ p` ⟩
      p ∧ q ∧ r
    ⇒⟨ “Weakening” (3.76b) ⟩
      q ∧ r

Theorem (4.3) “Left-monotonicity of ∧”: (p ⇒ q) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
    p ⇒ q
  ≡⟨ “Definition of ⇒” (3.60) ⟩
    p ∧ q ≡ p
  ⇒⟨ “Lemma Left-monotonicity of ∧” ⟩
    p ∧ r ⇒ q ∧ r
```

## Transform, then Assume in Sub-Proof

```
Theorem (4.3) “Left-monotonicity of ∧”: (p ⇒ q) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
    p ⇒ q
  ≡⟨ “Definition of ⇒” (3.60) ⟩
    p ∧ q ≡ p
  ⇒⟨ Subproof for `(p ∧ q ≡ p) ⇒ (p ∧ r ⇒ q ∧ r)`:
      Assuming `p ∧ q ≡ p`:
          p ∧ r
        ≡⟨ Assumption `p ∧ q ≡ p` ⟩
          p ∧ q ∧ r
        ⇒⟨ “Weakening” (3.76b) ⟩
          q ∧ r
    ⟩
    p ∧ r ⇒ q ∧ r
```

## Transform Whole Theorem, and Assume in Sub-Proof

```
Theorem (4.3) “Left-monotonicity of ∧”: (p ⇒ q) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
    (p ⇒ q) ⇒ (p ∧ r ⇒ q ∧ r)
  ≡⟨ “Definition of ⇒” (3.60) ⟩
    (p ∧ q ≡ p) ⇒ (p ∧ r ⇒ q ∧ r)
  ≡⟨ Subproof for `(p ∧ q ≡ p) ⇒ (p ∧ r ⇒ q ∧ r)`:
      Assuming `p ∧ q ≡ p`:
          p ∧ r
        ≡⟨ Assumption `p ∧ q ≡ p` ⟩
          p ∧ q ∧ r
        ⇒⟨ “Weakening” (3.76b) ⟩
          q ∧ r
    ⟩
    true
```

## Transform Assumption When Used

(4.3) $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$

PROOF:

**Assume** $p \Rightarrow q$ (which is equivalent to $p \wedge q \equiv p$)

$$
\begin{array}{ll}
 & p \wedge r \\
= & \langle \text{ Assumption } p \wedge q \equiv p \rangle \\
 & p \wedge q \wedge r \\
\Rightarrow & \langle \text{ (3.76b) Weakening } \rangle \\
 & q \wedge r
\end{array}
$$

---

```
Theorem (4.3) “Left-monotonicity of ∧”: (p ⇒ q) ⇒ (p ∧ r ⇒ q ∧ r)
Proof:
  Assuming `p ⇒ q`:
      p ∧ r
    ≡⟨ Assumption `p ⇒ q` with “Definition of ⇒” (3.60) ⟩
      p ∧ q ∧ r
    ⇒⟨ “Weakening” ⟩
      q ∧ r
```

## Assuming . . . and using with . . .

(4.3) $(p \Rightarrow q) \Rightarrow ((p \wedge r) \Rightarrow (q \wedge r))$

PROOF:

**Assume** $p \Rightarrow q$ (which is equivalent to $p \wedge q \equiv p$)

$$
\begin{array}{ll}
 & p \wedge r \\
= & \langle \text{ Assumption } p \wedge q \equiv p \rangle \\
 & p \wedge q \wedge r \\
\Rightarrow & \langle \text{ (3.76b) Weakening } \rangle \\
 & q \wedge r
\end{array}
$$

---

```
Theorem (4.3) “Left-monotonicity of ∧” “Monotonicity of ∧”:
    (p ⇒ q) ⇒ ((p ∧ r) ⇒ (q ∧ r))
Proof:
  Assuming `p ⇒ q` and using with “Definition of ⇒” (3.60):
      p ∧ r
    ≡⟨ Assumption `p ⇒ q` ⟩
      p ∧ q ∧ r
    ⇒⟨ “Weakening” (3.76b) ⟩
      q ∧ r
```

## General Case Analysis

(4.6) $(p \vee q \vee r) \wedge (p \Rightarrow s) \wedge (q \Rightarrow s) \wedge (r \Rightarrow s) \Rightarrow s$

**Proof pattern for general case analysis:**

**Prove:** $S$

**By cases:** $P, Q, R$

(proof of $P \vee Q \vee R$ — omitted if obvious)

**Case** $P$ **:** ( proof of $P \Rightarrow S$ )

**Case** $Q$ **:** ( proof of $Q \Rightarrow S$ )

**Case** $R$ **:** ( proof of $R \Rightarrow S$ )

### Case Analysis Example: (4.2) $(p \Rightarrow q) \;\Rightarrow\; p \vee r \;\Rightarrow\; q \vee r$

**Assume** $p \Rightarrow q$
**Assume** $p \vee r$
**Prove:** $q \vee r$
**By Cases:** $p, r$ — $p \vee r$ holds by assumption
**Case** $p$ **:**

$$
\begin{array}{ll}
 & p \\
\Rightarrow & \langle \text{ Assumption } p \Rightarrow q \;\rangle \\
 & q \\
\Rightarrow & \langle \text{ Weakening (3.76a) } \rangle \\
 & q \vee r
\end{array}
$$

**Case** $r$ **:**

$$
\begin{array}{ll}
 & r \\
\Rightarrow & \langle \text{ Weakening (3.76a) } \rangle \\
 & q \vee r
\end{array}
$$

### Context for Examples: LADM Theory of Integers — Positivity and Ordering

(15.30) **Axiom, Addition in** pos: $\mathsf{pos}.a \wedge \mathsf{pos}.b \;\Rightarrow\; \mathsf{pos}(a+b)$

(15.31) **Axiom, Multiplication in** pos: $\mathsf{pos}.a \wedge \mathsf{pos}.b \;\Rightarrow\; \mathsf{pos}(a \cdot b)$

(15.32) **Axiom:** $\neg\mathsf{pos}.0$

(15.33) **Axiom:** $b \neq 0 \;\Rightarrow\; (\mathsf{pos}.b \;\equiv\; \neg\mathsf{pos}(-b))$

(15.34) $b \neq 0 \;\Rightarrow\; \mathsf{pos}(b \cdot b)$

(15.35) $\mathsf{pos}.a \;\Rightarrow\; (\mathsf{pos}.b \;\equiv\; \mathsf{pos}(a \cdot b))$

(15.36) **Axiom, Less:** $a < b \;\equiv\; \mathsf{pos}(b - a)$

(15.37) **Axiom, Greater:** $a > b \;\equiv\; \mathsf{pos}(a - b)$

(15.38) **Axiom, At most:** $a \leq b \;\equiv\; a < b \;\vee\; a = b$

(15.39) **Axiom, At least:** $a \geq b \;\equiv\; a > b \;\vee\; a = b$

(15.40) **Positive elements:** $\mathsf{pos}.b \;\equiv\; 0 < b$

### Case Analysis Example: "Positivity of Squares"

**Theorem (15.34) "Positivity of squares":** b ≠ 0 ⇒pos (b · b)
**Proof:**
  **Assuming** \`b ≠ 0\`**:**
    **By cases:** \`pos b\`, \`¬ pos b\`
      **Completeness:**
        **By** "LEM"
      **Case** \`pos b\`**:**
        **By** (15.31a) with Assumption \`pos b\`
      **Case** \`¬ pos b\`**:**
          true
        ≡⟨ Assumption \`¬ pos b\` ⟩
          ¬ pos b
        ≡⟨ (15.33b) with Assumption \`b ≠ 0\` ⟩
          pos (- b)
        ≡⟨ "Idempotency of ∧" ⟩
          pos (- b) ∧ pos (- b)
        ⇒⟨ "Positivity under ·" ⟩
          pos (- b · - b)

## Case Analysis with Calculation for "Completeness:"

**Theorem (15.34) "Positivity of squares":** b ≠ 0 ⇒pos (b · b)

**Proof:**

  **Assuming** \`b ≠ 0\`**:**

    **By cases:** \`pos b\`, \`¬ pos b\`

      **Completeness:**

          pos b ∨ ¬ pos b

        ≡⟨ "Excluded Middle" ⟩

          true

      **Case** \`pos b\`**:**

        **By** (15.31a) with Assumption \`pos b\`

      **Case** \`¬ pos b\`**:**

          true

        ≡⟨ Assumption \`¬ pos b\` ⟩

          ¬ pos b

        ≡⟨ (15.33b) with Assumption \`b ≠ 0\` ⟩

          pos (- b)

        ≡⟨ "Idempotency of ∧" ⟩

          pos (- b) ∧ pos (- b)

## Case Analysis with Calculation for "Completeness:" ...

    **By cases:** \`pos b\`, \`¬ pos b\`

      **Completeness:**

          pos b ∨ ¬ pos b

        ≡⟨ "Excluded Middle" ⟩

          true

      **Case** \`pos b\`**:**

        **By** (15.31a) with Assumption \`pos b\`

---

- After "**Completeness:**" goes a proof for the disjunction of all cases listed after "**By cases:**"
- This can be any kind of proof.
- Inside the "**Case** '$p$'**:**" block, you may use "**Assumption** '$p$'"

## Proof by Contrapositive

(3.61) **Contrapositive:** $p \Rightarrow q \quad \equiv \quad \neg q \Rightarrow \neg p$

(4.12) **Proof method:** Prove $P \Rightarrow Q$ by proving its contrapositive $\neg Q \Rightarrow \neg P$

---

**Proving** $x + y \geq 2 \quad \Rightarrow \quad x \geq 1 \vee y \geq 1$**:**

$$
\begin{array}{ll}
 & \neg(x \geq 1 \vee y \geq 1) \\
= & \langle \text{ De Morgan (3.47) } \rangle \\
 & \neg(x \geq 1) \ \wedge\ \neg(y \geq 1) \\
= & \langle \text{ Def. } \geq \text{ (15.39) with Trichotomy (15.44) } \rangle \\
 & x < 1 \ \wedge\ y < 1 \\
\Rightarrow & \langle \text{ Monotonicity of + (15.42) } \rangle \\
 & x + y < 1 + 1 \\
= & \langle \text{ Def. 2 } \rangle \\
 & x + y < 2 \\
= & \langle \text{ Def. } \geq \text{ (15.39) with Trichotomy (15.44) } \rangle \\
 & \neg(x + y \geq 2)
\end{array}
$$

## Proof by Contrapositive in CALCCHECK — `Using`

**Theorem "Example for use of Contrapositive":** $x + y \geq 2 \Rightarrow x \geq 1 \lor y \geq 1$
**Proof:**
  **Using** "Contrapositive"**:**
    **Subproof for** \`$\neg (x \geq 1 \lor y \geq 1) \Rightarrow \neg (x + y \geq 2)$\`**:**
      $\neg (x \geq 1 \lor y \geq 1)$
    $\equiv\langle$ "De Morgan" $\rangle$
      $\neg (x \geq 1) \land \neg (y \geq 1)$
    $\equiv\langle$ "Complement of <" with (3.14) $\rangle$
      $x < 1 \land y < 1$
    $\Rightarrow\langle$ "<-Monotonicity of +" $\rangle$
      $x + y < 1 + 1$
    $\equiv\langle$ Evaluation $\rangle$
      $x + y < 2$
    $\equiv\langle$ "Complement of <" with (3.14) $\rangle$
      $\neg (x + y \geq 2)$

- "**Using** *HintItem1*: *subproof1 subproof2*"
  is processed as "**By** *HintItem1* **with** *subproof1* **and** *subproof2*"
- If you get the subproof goals wrong, the `with` heuristic has no chance to succeed…

## Proof by Mutual Implication — `Using`

(3.80) **Mutual implication:** $(p \Rightarrow q) \land (q \Rightarrow p) \equiv p \equiv q$

```
Theorem (15.44A) "Trichotomy — A":
    a < b  ≡  a = b  ≡  a > b
Proof:
  Using "Mutual implication":
    Subproof for `a = b  ⇒  (a < b  ≡  a > b)`:
      Assuming `a = b`:
          a < b
        ≡⟨ "Converse of <", Assumption `a = b` ⟩
          a > b
    Subproof for `(a < b  ≡  a > b) ⇒ a = b`:
        a < b  ≡  a > b
      ≡⟨ "Definition of <", "Definition of >" ⟩
        pos (b - a) ≡ pos (a - b)
      ≡⟨ (15.17), (15.19), "Subtraction" ⟩
        pos (b - a) ≡ pos (- (b - a))
      ⇒⟨ (15.33c) ⟩
        b - a = 0
      ≡⟨ "Cancellation of +" ⟩
        b - a + a = 0 + a
      ≡⟨ "Identity of +", "Subtraction", "Unary minus" ⟩
        a = b
```

## Proof by Contradiction

(3.74) $p \Rightarrow \mathit{false} \quad \equiv \quad \neg p$

(4.9) **Proof by contradiction:** $\neg p \Rightarrow \mathit{false} \quad \equiv \quad p$

**"This proof method is overused"**

If you intuitively try to do a proof by contradiction:

- Formalise your proof
- This may already contain a direct proof!
- So check whether contradiction is still necessary
- …, or whether your proof can be transformed into one that does not use contradiction.