Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-08

Plan for Today

- **Textbook Chapter 4: Relaxing the Proof Style**

  — structured, more flexible proofs
  - ... with ...
  - **Using** theorems as proof methods
    - Proof by Contrapositive
    - Proof by Mutual Implication
- Briefly revisit the "Replacement" rules

Recall: `with` ...

$$\begin{array}{l} \quad \neg (a \cdot b = a \cdot 0) \\ \equiv \langle \text{"Cancellation of } \cdot \text{" with Assumption `} a \neq 0\text{`} \rangle \\ \quad \neg (b = 0) \end{array}$$

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

Monotonicity `with` ...

$$(\forall x \bullet x+1>x) \quad \wedge \quad y+1>y$$
$\Rightarrow$ ⟨ **Left-Monotonicity of $\wedge$ (4.3) with Instantiation (9.13)** $(\forall x \bullet P) \Rightarrow P[x := E]$ ⟩
$$(y+1)+1>y+1 \quad \wedge \quad y+1>y$$

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": $(\forall x \bullet x+1>x)$
  $\Rightarrow (y+1)+1>y+1$
- The surrounding proof uses: $(\forall x \bullet x+1>x) \quad \wedge \quad y+1>y$
  $\Rightarrow (y+1)+1>y+1 \quad \wedge \quad y+1>y$

`with` — Overview

CalcCheck currently knows three kinds of "`with`":

- For explicit substitutions: **"Identity of +"** with '$x := 2$'
- *ThmA* `with` *ThmB*
  - If *ThmB* gives rise to an equality/equivalence $L = R$:
    Rewrite *ThmA* with $L \mapsto R$ to *ThmA*$'$,
    and use *ThmA*$'$ for rewriting the goal.
- *ThmA* `with` *ThmB* and *ThmB*$_2$ ...
  - If *ThmA* gives rise to an implication $A_1 \Rightarrow A_2 \Rightarrow \ldots (L = R)$:
    Perform **conditional rewriting**, rigidly applying $L\sigma \mapsto R\sigma$
    if using *ThmB* and *ThmB*$_2$ ... to prove $A_1\sigma, A_2\sigma, \ldots$ succeeds

Using hi_1: sp_1 sp_2	is essentially syntactic sugar for:	By hi_1 with sp_1 and sp_2

`with`$_1$: Rewriting Theorems before Rewriting

ThmA `with` *ThmB*

- If *ThmB* gives rise to an equality/equivalence $L = R$:
  Rewrite *ThmA* with $L \mapsto R$
- E.g.: Assumption `$p \Rightarrow q$` with (3.60)

  The local theorem $p \Rightarrow q$ (resulting from the Assumption)
  rewrites via: $p \Rightarrow q \;\mapsto\; p \equiv p \wedge q$
  to: $p \quad \equiv \quad p \wedge q$
  which can be used as: $p \quad \mapsto \quad p \wedge q$

```
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
```

`with`$_2$: Conditional Rewriting

ThmA `with` *ThmB* and *ThmB*$_2$ ...

- If *ThmA* gives rise to an implication $A_1 \Rightarrow A_2 \Rightarrow \ldots (L = R)$:
  - Find substitution σ such that $L\sigma$ matches goal
  - Resolve $A_1\sigma, A_2\sigma, \ldots$ using *ThmB* and *ThmB*$_2$ ...
  - Rewrite goal applying $L\sigma \mapsto R\sigma$ rigidly.
- E.g.: "Cancellation of ·" with Assumption '$m + n \neq 0$'

  when trying to prove $(m+n)\cdot(n+2) = (m+n)\cdot 5\cdot k$:
  - "Cancellation of ·" is: $c \neq 0 \Rightarrow (c\cdot a = c\cdot b \equiv a = b)$
  - We try to use: $c\cdot a = c\cdot b \mapsto a = b$, so L is $c\cdot a = c\cdot b$
  - Matching L against goal produces $\sigma = [a, b, c := (n+2), (5\cdot k), (m+n)]$
  - $(c \neq 0)\sigma$ is $(m+n) \neq 0$ and can be proven by "Assumption '$m+n \neq 0$'"
  - The goal is rewritten to $(a = b)\sigma$, that is, $(n+2) = 5\cdot k$.

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 ≥ 2 ⇒ x ≥ 1 ∨ y ≥ 1
Proof:
  Using "Contrapositive"**:**
    Subproof for `¬ (x ≥ 1 ∨ y ≥ 1) ⇒ ¬ (x + y ≥2)`**:**

$$\begin{array}{ll}
 & \neg(x \geq 1 \vee y \geq 1) \\
\equiv & \langle \text{"De Morgan"} \rangle \\
 & \neg(x \geq 1) \wedge \neg(y \geq 1) \\
\equiv & \langle \text{"Complement of <" with (3.14)} \rangle \\
 & x < 1 \wedge y < 1 \\
\Rightarrow & \langle \text{"<-Monotonicity of +"} \rangle \\
 & x + y < 1 + 1 \\
\equiv & \langle \text{Evaluation} \rangle \\
 & x + y < 2 \\
\equiv & \langle \text{"Complement of <" with (3.14)} \rangle \\
 & \neg(x + y \geq 2)
\end{array}$$

- "**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:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; p \equiv q$

```
        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.

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

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

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

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

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

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

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

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

LADM Theory of Integers — Ordering Properties

(15.41) **Transitivity:**
$$(a)\quad a < b \;\wedge\; b < c \;\Rightarrow\; a < c$$
$$(b)\quad a \le b \;\wedge\; b < c \;\Rightarrow\; a < c$$
$$(c)\quad a < b \;\wedge\; b \le c \;\Rightarrow\; a < c$$
$$(d)\quad a \le b \;\wedge\; b \le c \;\Rightarrow\; a \le c$$

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

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

(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 ≤:** $a \le b \;\wedge\; a \ge b \;\equiv\; a = b$

(15.46) **Reflexivity of ≤:** $a \le a$

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)
        ≡⟨ (15.23) ⟩
          pos (b · b)

(15.30) $\mathrm{pos}.a \wedge \mathrm{pos}.b \Rightarrow \mathrm{pos}(a+b)$
(15.31) $\mathrm{pos}.a \wedge \mathrm{pos}.b \Rightarrow \mathrm{pos}(a \cdot b)$
(15.32) $\neg\mathrm{pos}.0$
(15.33) $b \ne 0 \Rightarrow (\mathrm{pos}.b \equiv \neg\mathrm{pos}(-b))$

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*’”

Some Replacements

$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \equiv (x > f\,5))$$
$$\equiv \langle \quad ? \quad \rangle$$
$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \equiv (y < g\,7))$$

$$((f\,5) = (g\,y)) \quad \wedge \quad ((f\,x \le g\,y) \equiv x > (f\,5))$$
$$\equiv \langle \quad ? \quad \rangle$$
$$((f\,5) = (g\,y)) \quad \wedge \quad ((f\,x \le g\,y) \equiv x > g\,y))$$

$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \Rightarrow p(x-1) \vee (x > f\,5))$$
$$\equiv \langle \quad ? \quad \rangle$$
$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \Rightarrow p(x-1) \vee (y < g\,7))$$

Replacements 1 & 2

$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \equiv (x > f\,5))$$
$$\equiv \langle\ (3.51)\ \textbf{“Replacement”}\ (p \equiv q) \wedge (r \equiv p) \ \equiv\ (p \equiv q) \wedge (r \equiv q)\ \rangle$$
$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \equiv (y < g\,7))$$

$$((f\,5) = (g\,y)) \quad \wedge \quad ((f\,x \le g\,y) \equiv x > (f\,5))$$
$$\equiv \langle\ \text{Substitution}\ \rangle$$
$$((f\,5) = (g\,y)) \quad \wedge \quad \underline{((f\,x \le g\,y) \equiv x > z)}[z := (f\,5)]$$
$$\equiv \left\langle \begin{array}{l} (3.84a)\ \textbf{“Replacement”} \\ \qquad (e = f) \wedge \underline{P}[z := e] \ \equiv\ (e = f) \wedge \underline{P}[z := f], \\ \text{Substitution} \end{array} \right\rangle$$
$$((f\,5) = (g\,y)) \quad \wedge \quad ((f\,x \le g\,y) \equiv x > g\,y))$$

Replacement 3

$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \Rightarrow p(x-1) \vee (x > f\,5))$$
$$\equiv \langle\ \text{Substitution}\ \rangle$$
$$((x > f\,5) \equiv (y < g\,7)) \wedge \underline{((f\,x \le g\,y) \Rightarrow p(x-1) \vee z)}[z := (x > f\,5)]$$
$$\equiv \left\langle \begin{array}{l} (3.84a)\ \textbf{“Replacement”} \\ \qquad (e = f) \wedge \underline{P}[z := e] \ \equiv\ (e = f) \wedge \underline{P}[z := f], \\ \textbf{“Definition of} \equiv\textbf{”}\ (p \equiv q) = (p = q), \text{Substitution} \end{array} \right\rangle$$
$$((x > f\,5) \equiv (y < g\,7)) \quad \wedge \quad ((f\,x \le g\,y) \Rightarrow p(x-1) \vee (y < g\,7))$$

Replacements 1–3 in CalcCheck

```
Calculation:
    ((x > f 5) ≡ (y < g 7)) ∧ ((f x ≤ g y) ≡ (x > f 5))
  ≡⟨ “Replacement” ⟩
    ((x > f 5) ≡ (y < g 7)) ∧ ((f x ≤ g y) ≡ (y < g 7))

Calculation:
    ((f 5) = (g y)) ∧ ((f x ≤ g y) ≡ (x > f 5))
  ≡⟨ Substitution ⟩
    ((f 5) = (g y)) ∧ ((f x ≤ g y) ≡ (x > z))[z ≔ f 5]
  ≡⟨ “Replacement”, Substitution ⟩
    ((f 5) = (g y)) ∧ ((f x ≤ g y) ≡ (x > g y))

Calculation:
    ((x > f 5) ≡ (y < g 7)) ∧ ((f x ≤ g y) ≡ (x > f 5))
  ≡⟨ Substitution ⟩
    ((x > f 5) ≡ (y < g 7)) ∧ ((f x ≤ g y) ≡ z)[z ≔ (x > f 5)]
  ≡⟨ “Replacement”, Substitution ⟩
    ((x > f 5) ≡ (y < g 7)) ∧ ((f x ≤ g y) ≡ (y < g 7))
```

Leibniz's Rule Axiom, and Further Replacement Rules

Axiom scheme (E can be any expression; z can be of any type):

(3.83) **Axiom, Leibniz:** $(e = f) \Rightarrow (E[z := e] = E[z := f])$

Replacement rules: (P can be any expression **of type** $\mathbb{B}$)

(3.84a) **“Replacement”:** $(e = f) \wedge P[z := e] \;\equiv\; (e = f) \wedge P[z := f]$

(3.84b) **“Replacement”:** $(e = f) \Rightarrow P[z := e] \;\equiv\; (e = f) \Rightarrow P[z := f]$

(3.84c) **“Replacement”:** $q \wedge (e = f) \Rightarrow P[z := e] \;\equiv\; q \wedge (e = f) \Rightarrow P[z := f]$

(Below, p and z are **of type** $\mathbb{B}$)

(3.85a) **Replace by** ***true*****:** $p \Rightarrow P[z := p] \;\equiv\; p \Rightarrow P[z := \mathit{true}]$

Replacing Variables by Boolean Constants

In each of the following, P can be any expression **of type** $\mathbb{B}$:

(3.85a) **Replace by** ***true*****:** $p \Rightarrow P[z := p] \;\equiv\; p \Rightarrow P[z := \mathit{true}]$

(3.85b) $q \wedge p \Rightarrow P[z := p] \;\equiv\; q \wedge p \Rightarrow P[z := \mathit{true}]$

(3.86a) **Replace by** ***false*****:** $P[z := p] \Rightarrow p \;\equiv\; P[z := \mathit{false}] \Rightarrow p$

(3.86b) $P[z := p] \Rightarrow p \vee q \;\equiv\; P[z := \mathit{false}] \Rightarrow p \vee q$

(3.87) **Replace by** ***true*****:** $p \wedge P[z := p] \;\equiv\; p \wedge P[z := \mathit{true}]$

(3.88) **Replace by** ***false*****:** $p \vee P[z := p] \;\equiv\; p \vee P[z := \mathit{false}]$

(3.89) **Shannon:**

$$P[z := p] \;\equiv\; (p \wedge P[z := \mathit{true}]) \vee (\neg p \wedge P[z := \mathit{false}])$$

Note: Using Shannon on all propositional variables in sequence is equivalent to producing a truth table.

> “Prove the following theorems (**without using Shannon or the proof method of case analysis by Shannon**), ...”