Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-10-02

Plan for Today

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

  — nicer implication proofs

  - Proving implications **Assuming** the antecedent
  - Transforming applied theorems using `with`
  - Resolving antecedents of used implications using `with`
  - Proving **By cases**
  - **Using** theorems as proof methods
    - Proof by Contrapositive
    - Proof by Mutual Implication

CalcCheck: Subproof Hint Items

You have used the following kinds of hint items:

- Theorem name references **"Identity of ≡"**
- Theorem number references **(3.32)**
- Certain key words and key phrases: Substitution, Evaluation, Induction hypothesis
- Fact \`*Expression*\`
- Composed hint items: "Identity of +" with \`*Substitution*\`

  "Monotonicity of +" with *HintItem*

A new kind of hint item:

Subproof for \`*Expression*\`: $\boxed{\text{Proof}}$

For example, Fact \`$3 = 2 + 1$\` is really syntactic sugar for a subproof using Evaluation:

```
Calculation:
    3 · x
  =⟨ Subproof for `3 = 2 + 1`:
      By evaluation
    ⟩
    (2 + 1) · x
```

Abbreviated Proofs for Implications

This:

$$\begin{array}{ll} & p \\ \equiv & \langle \text{ Why } \quad p \equiv q \ \rangle \\ & q \\ \Rightarrow & \langle \text{ Why } \quad q \Rightarrow r \ \rangle \\ & r \end{array}$$

proves: $\boxed{p \Rightarrow r}$

Because:

$$\begin{array}{ll} & (p = q) \wedge (q \Rightarrow r) \\ \Rightarrow & \langle \text{ (3.82b) Transitivity of } \Rightarrow \ \rangle \\ & p \Rightarrow r \end{array}$$

(4.1) — Creating the Proof "Bottom-up"

Proving (4.1) $p \Rightarrow (q \Rightarrow p)$**:**

$$\begin{array}{ll} & p \\ \Rightarrow & \langle \text{ (3.76a) Strenghtening } p \vee q \Leftarrow p \ \rangle \\ & \neg q \vee p \\ \equiv & \langle \text{ (3.59) Definition of implication } \rangle \\ & q \Rightarrow p \end{array}$$

We have:

Axiom (3.58) Consequence: $\boxed{p \Leftarrow q \quad \equiv \quad q \Rightarrow p}$

This means that the $\Leftarrow$ relation is the **converse** of the $\Rightarrow$ relation.

Theorem: The converse of a transitive relation is transitive again, and the converse of an order is an order again.

CalcCheck supports *activation* of such converse properties, enabling **reversed presentations following mathematical habits** of transitivity calculations such as the above.

(4.1)

Proving (4.1) $p \Rightarrow (q \Rightarrow p)$**:**

$$\begin{array}{ll} & q \Rightarrow p \\ \equiv & \langle \text{ (3.59) Definition of implication } \rangle \\ & \neg\, q \vee p \\ \Leftarrow & \langle \text{ (3.76a) Strenghtening } p \vee q \Leftarrow p \ \rangle \\ & p \end{array}$$

In CalcCheck, if the converse property is not activated, then $\Leftarrow$ is a separate operator requiring explicit conversion:

```
Theorem (4.1): p ⇒ (q ⇒ p)
Proof:
    q ⇒ p
  ≡⟨ “Definition of ⇒” (3.59) ⟩
    ¬ q ∨ p
  ⇐⟨ “Strengthening” (3.76a), “Definition of ⇐” ⟩
    p
```

(4.1) Implicitly Using "Consequence"

Axiom (3.58) Consequence: $\boxed{p \Leftarrow q \quad \equiv \quad q \Rightarrow p}$

Proving (4.1) $p \Rightarrow (q \Rightarrow p)$**:**

$$
\begin{array}{ll}
 & q \Rightarrow p \\
\equiv & \langle \text{(3.59) Definition of implication} \rangle \\
 & \neg q \vee p \\
\Leftarrow & \langle \text{(3.76a) Strenghtening } p \Rightarrow p \vee q \rangle \\
 & p
\end{array}
$$

Recall: Weakening/Strengthening Theorems

(3.76a) $p \Rightarrow p \vee q$

(3.76b) $p \wedge q \Rightarrow p$

(3.76c) $p \wedge q \Rightarrow p \vee q$

(3.76d) $p \vee (q \wedge r) \Rightarrow p \vee q$

(3.76e) $p \wedge q \Rightarrow p \wedge (q \vee r)$

(4.2) Left-Monotonicity of $\vee$

$$\boxed{(p \Rightarrow q) \ \Rightarrow \ (p \vee r \Rightarrow q \vee r)}$$

$$
\begin{array}{ll}
 & p \vee r \Rightarrow q \vee r \\
= & \langle \text{(3.57) } p \Rightarrow q \quad \equiv \quad p \vee q \quad \equiv \quad q \rangle \\
 & p \vee r \vee q \vee r \quad \equiv \quad q \vee r \\
= & \langle \text{(3.26) Idempotency of } \vee \rangle \\
 & p \vee q \vee r \quad \equiv \quad q \vee r \\
= & \langle \text{(3.27) Distributivity of } \vee \text{ over } \equiv \rangle \\
 & (p \vee q \quad \equiv \quad q) \vee r \\
= & \langle \text{(3.57) } p \Rightarrow q \quad \equiv \quad p \vee q \quad \equiv \quad q \rangle \\
 & (p \Rightarrow q) \vee r \\
\Leftarrow & \langle \text{(3.76a) Strenghtening } p \Rightarrow p \vee q \rangle \\
 & p \Rightarrow q
\end{array}
$$

(4.3) Left-Monotonicity of $\wedge$

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

$$
\begin{array}{ll}
 & p \wedge r \Rightarrow q \wedge r \\
= & \langle \text{(3.60) Definition of implication} \rangle \\
 & p \wedge r \wedge q \wedge r \equiv p \wedge r \\
= & \langle \text{(3.38) Idempotency of } \wedge \rangle \\
 & (p \wedge q) \wedge r \equiv p \wedge r \\
= & \langle \text{(3.49)} \rangle \\
 & ((p \wedge q) \equiv p) \wedge r \equiv r \\
= & \langle \text{(3.60) Definition of implication} \rangle \\
 & (p \Rightarrow q) \wedge r \equiv r \\
= & \langle \text{(3.60) Definition of implication} \rangle \\
 & r \Rightarrow (p \Rightarrow q) \\
\Leftarrow & \langle \text{(4.1) } p \Rightarrow (q \Rightarrow p) \rangle \\
 & p \Rightarrow q
\end{array}
$$

Proving Implications...

How to prove the following?

"=-Congruence of +": $b = c \quad \Rightarrow \quad a + b = a + c$

"We have been doing this via Leibniz (1.5)......"

- One of the "Replacement" theorems of the "Leibniz as Axiom" section can help.
- It may be nicer to turn this into a situation where the inference rule Leibniz (1.5) can be used again:

Assuming the Antecedent

```
Lemma "=-Congruence of +":  b = c  ⇒  a + b = a + c
Proof:
  Assuming `b = c`:
      a + b
    =⟨ Assumption `b = c` ⟩
      a + c
```

Assuming the Antecedent

To prove an implication $p \Rightarrow (q \diamond r)$
we can prove its conclusion $q \diamond r$ using p as **assumption**:

Assume p

$$
\begin{array}{ll}
 & q \\
\diamond & \langle \text{Assumption } p \rangle \\
 & r
\end{array}
$$

Justification:

(4.4) **(Extended) Deduction Theorem:** Suppose adding $P_1, \ldots, P_n$ as axioms to propositional logic **E**, **with the variables of the P_i considered to be constants**, allows Q to be proved.

Then $\quad P_1 \wedge \ldots \wedge P_n \Rightarrow Q \quad$ is a theorem.

That is:

Assumptions **cannot** be used with substitutions (with '$a, b := e, f$')
— just like induction hypotheses.

"Assuming the Antecedent" is not allowed in LADM Chapter 3!

Using Implication Theorems: Resolving the Antecedent via `with`

Theorem "Non-zero multiplication": $a \neq 0 \Rightarrow (b \neq 0 \Rightarrow a \cdot b \neq 0)$
Proof:
Assuming `$a \neq 0$` , `$b \neq 0$`:

$a \cdot b \neq 0$
$\equiv\langle$ "Definition of $\neq$" $\rangle$
$\neg (a \cdot b = 0)$
$\equiv\langle$ "Zero of $\cdot$" $\rangle$
$\neg (a \cdot b = a \cdot 0)$
$\equiv\langle$ "Cancellation of $\cdot$" with Assumption `$a \neq 0$` $\rangle$
$\neg (b = 0)$
$\equiv\langle$ "Definition of $\neq$", Assumption `$b \neq 0$` $\rangle$
true

- *HintItem1* `with` *HintItem2* `and` *HintItem3*, *HintItem4* parses as (*HintItem1* `with` (*HintItem2* `and` *HintItem3*)), *HintItem4*

`with` Moved Into Subproof

Theorem "Non-zero multiplication": $a \neq 0 \Rightarrow (b \neq 0 \Rightarrow a \cdot b \neq 0)$
Proof:
Assuming `$a \neq 0$` , `$b \neq 0$`:

$a \cdot b \neq 0$
$\equiv\langle$ "Definition of $\neq$" $\rangle$
$\neg (a \cdot b = 0)$
$\equiv\langle$ "Zero of $\cdot$" $\rangle$
$\neg (a \cdot b = a \cdot 0)$
$\equiv\langle$ Subproof for `$a \cdot b = a \cdot 0 \equiv b = 0$`:
By "Cancellation of $\cdot$" with Assumption `$a \neq 0$`
$\rangle$
$\neg (b = 0)$
$\equiv\langle$ "Definition of $\neq$", Assumption `$b \neq 0$` $\rangle$
true

`with` Moved Into Subproof . . .

$\neg (a \cdot b = a \cdot 0)$
$\equiv\langle$ Subproof for `$a \cdot b = a \cdot 0 \equiv b = 0$`:
By "Cancellation of $\cdot$" with Assumption `$a \neq 0$`
$\rangle$
$\neg (b = 0)$

- Theorem variable names in a subproof goal refer to theorem variables
- These variables cannot be differently instantiated
- The subproof can use theorem assumptions and induction hypotheses mentioning these variables.
- Subproof goals can be used like any other theorem/assumption in the enclosing hint (Here as equation used via the inference rule Leibniz.)
- 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.

with Calculated Away

Theorem "Non-zero multiplication": $a \neq 0 \Rightarrow (b \neq 0 \Rightarrow a \cdot b \neq 0)$
Proof:
Assuming `a ≠ 0` , `b ≠ 0`:

```
      a · b ≠ 0
    ≡⟨ "Definition of ≠" ⟩
      ¬ (a · b = 0)
    ≡⟨ "Zero of ·" ⟩
      ¬ (a · b = a · 0)
    ≡⟨ Subproof for `a · b = a · 0 ≡ b = 0`:
            a · b = a · 0 ≡ b = 0
          ≡⟨ "Left-identity of ⇒" ⟩
            true ⇒ (a · b = a · 0 ≡ b = 0)
          ≡⟨ Assumption `a ≠ 0` ⟩
            a ≠ 0 ⇒ (a · b = a · 0 ≡ b = 0)     — This is     "Cancellation of ·"
      ⟩
      ¬ (b = 0)
    ≡⟨ "Definition of ≠", Assumption `b ≠ 0` ⟩
      true
```

with Calculated Away . . .

```
      ¬ (a · b = a · 0)
    ≡⟨ "Cancellation of ·" with Assumption `a ≠0` ⟩
      ¬ (b = 0)
```

```
      ¬ (a · b = a · 0)
    ≡⟨ Subproof for `a · b = a · 0 ≡ b = 0`:
            a · b = a · 0 ≡ b = 0
          ≡⟨ "Left-identity of ⇒" ⟩
            true ⇒ (a · b = a · 0 ≡ b = 0)
          ≡⟨ Assumption `a ≠ 0` ⟩
            a ≠ 0 ⇒ (a · b = a · 0 ≡ b = 0)     — This is     "Cancellation of ·"
      ⟩
      ¬ (b = 0)
```

- In a hint of shape "*HintItem1* `with` *HintItem2* and *HintItem3*":

  If *HintItem1* refers to a theorem of shape $p \Rightarrow q$, or of shape $p \equiv q$

  then *HintItem2* and *HintItem3* are used to prove p

  and q is used in the surrounding proof.

(4.3) Left-Monotonicity of $\wedge$ (shorter proof)

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

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 . . . "