Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-09-24

CalcCheck-checked Mystery Steps

```
Calculation:
    p ∧ p
  ≡⟨ “Golden rule” ⟩
    p ∨ p
```

?

How can the Golden rule have been applied here?

```
Calculation:
    true ≡ p ≡ ¬ p
  ≡⟨ (3.15) `¬ p ≡ p ≡ false` ⟩
    false
```

?

```
Calculation:
    p ≡ ¬ q ≡ p ∨ q
  ≡⟨ (3.32) ⟩
    ¬ p ∨ ¬ q
```

?

Plan for Today

- Natural Numbers and **Induction** (ctd.)
- **Textbook Chapter 3: Propositional Calculus**
  - CalcCheck-checked mystery steps
  - Implication

Natural Numbers — Rigorous Definition

- The set of all **natural numbers** is written $\mathbb{N}$.
- Zero "0" is a natural number.
- If n is a natural number, then its successor "suc n" is a natural number, too.
- Nothing else is a natural number.
- Two natural numbers are equal **if and only if** they are constructed in the same way.

  Example: suc suc suc 0 $\neq$ suc suc suc suc 0

This is an inductive definition.

(Like the definition of expressions. . .)

Every inductive definition gives rise to an induction principle

— a way to prove statements about the inductively defined elements

Natural Numbers — Induction Proofs

Induction principle for the natural numbers:

- if $P[m := 0]$ — If P holds for 0
- and if we can obtain $P[m := \text{suc } m]$ from P, — and whenever P holds for m, it also holds for suc m,
- then P holds. — then P holds for all natural numbers.

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

Theorem: P

Proof:

By induction on $m : \mathbb{N}$**:**

Base case:

Proof for $P[m := 0]$

Induction step:

Proof for $P[m := \text{suc } m]$

using **Induction hypothesis** P

$$\frac{P[m := 0] \qquad \begin{array}{c} \ulcorner P \urcorner \\ \vdots \\ P[m := \text{suc } m] \end{array}}{P}$$

Factorial — Inductive Definition

The factorial operator "_!" on $\mathbb{N}$ can be defined as follows:

- The factorial of a natural number is a natural number again: $\_! : \mathbb{N} \to \mathbb{N}$
- $0\,! = 1$
- For every $n : \mathbb{N}$, we have: $(\text{suc } n)\,! = (\text{suc } n) \cdot (n\,!)$

```
Declaration: _! : ℕ → ℕ
Axiom “Definition of ! for 0”:       0 !        =  1
Axiom “Definition of ! for `suc`”:   (suc n) !  =  (suc n) · n !
```

_! is an inductively-defined function.

Why does this define _! for all possible arguments?

Because:

- _! takes **one** argument of type $\mathbb{N}$
- That argument is **always** either 0, or suc k; for some **smaller** $k : \mathbb{N}$
- Both cases are covered by the definition.
- The second clause "builds up" the domain of definition of _! from smaller to larger n.

Natural Number Addition — Inductive Definition

Addition on $\mathbb{N}$ can be defined as follows:

- The (infix) **addition operator** "+", when applied to two natural numbers, produces again a natural number:
  $\_+\_ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$
- For every $q : \mathbb{N}$, we have:
  - $0 + q = q$
  - For every $n : \mathbb{N}$ we have: $(\mathsf{suc}\ n) + q = \mathsf{suc}\ (n + q)$

```
Axiom “Definition of + for 0”:             0 + n = n
Axiom “Definition of + for `suc`”:  (suc m) + n = suc (m + n)
```

$\_+\_$ is an inductively-defined function.

Why does this define $\_+\_$ for all possible arguments?

Because:

- $\_+\_$ takes **two** arguments of type $\mathbb{N}$
- **Each of these arguments** is **always** either 0, or $\mathsf{suc}\ k$ for some **smaller** $k : \mathbb{N}$
- The second argument is in both clauses the variable q — all cases covered.
- For the first argument, each clause covers one case.
- The second clause "builds up" the domain of definition of $\_+\_$ from smaller to larger m.

Even Natural Numbers — Inductive Definition

- The predicates even and odd are declared as Boolean-valued **functions**:

```
Declaration: even, odd : ℕ → 𝔹
```

- Function application of function f to argument a is written as **juxtaposition**: $f\ a$
- Function application associates to the left: $f\ a\ b = (f\ a)\ b$
- The definition provided in Homework 5 is by **mutual recursion**:

```
Axiom “Zero is even”:     even 0
Axiom “Odd is not even”:  odd n ≡ ¬ (even n)
Axiom “Even successor”:   even (suc n) ≡ odd n
```

- This is clearly equivalent to an inductive definition for even that is independent from the definition of odd

```
Axiom “Zero is even”:              even 0
Axiom “Even successor (direct)”:   even (suc n) ≡ ¬ (even n)
Axiom “Odd is not even”:           odd n ≡ ¬ (even n)
```

even is an inductively-defined function.

Why does this define even for all possible arguments?

Because:

- even takes **one** argument of type $\mathbb{N}$

Proving "Even double"

```
Theorem “Even double”: even (n + n)
Proof:
  By induction on `n : ℕ`:
    Base case:
        even (0 + 0)
      ≡⟨ ? ⟩
        ?
    Induction step:
        even (suc n + suc n)
      ≡⟨ ? ⟩
        ?
```

An **induction proof** looks as follows:

Theorem: P
Proof:
By induction on $m : \mathbb{N}$**:**
Base case:
Proof for $P[m := 0]$
Induction step:
Proof for $P[m := \mathsf{suc}\ m]$
using **Induction hypothesis** P

$$\frac{P[m := 0] \qquad \begin{array}{c} \ulcorner P \urcorner \\ \vdots \\ P[m := \mathsf{suc}\ m] \end{array}}{P}$$

Proving “Even double”

```
Theorem “Even double”: even (n + n)
Proof:
  By induction on `n : ℕ`:
    Base case:
        even (0 + 0)
      ≡⟨ “Definition of + for 0” ⟩
        even 0
      ≡⟨ “Zero is even” ⟩
        true
    Induction step:
        even (suc n + suc n)
      ≡⟨ “Definition of + for `suc`” ⟩
        even (suc (n + suc n))
      ≡⟨ “Even successor” ⟩
        odd (n + suc n)
      ≡⟨ “Adding the successor” ⟩
        odd (suc (n + n))
      ≡⟨ “Odd successor” ⟩
        even (n + n)
      ≡⟨ Induction hypothesis ⟩
        true
```

Proving “Even double” — Using “— This is . . . ”

```
Theorem “Even double”: even (n + n)
Proof:
  By induction on `n : ℕ`:
    Base case:
        even (0 + 0)
      ≡⟨ “Definition of + for 0” ⟩
        even 0            — This is “Zero is even”
    Induction step:
        even (suc n + suc n)
      ≡⟨ “Definition of + for `suc`” ⟩
        even (suc (n + suc n))
      ≡⟨ “Even successor” ⟩
        odd (n + suc n)
      ≡⟨ “Adding the successor” ⟩
        odd (suc (n + n))
      ≡⟨ “Odd successor” ⟩
        even (n + n)      — This is induction hypothesis
```

Proving “Even double” — With Explicit Details

```
Theorem “Even double”: even (n + n)
Proof:
  By induction on `n : ℕ`:
    Base case `even (0 + 0)`:
        even (0 + 0)
      ≡⟨ “Definition of + for 0” ⟩
        even 0            — This is “Zero is even”
    Induction step `even (suc n + suc n)`:
        even (suc n + suc n)
      ≡⟨ “Definition of + for `suc`” ⟩
        even (suc (n + suc n))
      ≡⟨ “Even successor” ⟩
        odd (n + suc n)
      ≡⟨ “Adding the successor” ⟩
        odd (suc (n + n))
      ≡⟨ “Odd successor” ⟩
        even (n + n)
      — This is induction hypothesis `even (n + n)`
```

Defining Subtraction Inductively

```
Axiom “Subtraction from zero”:                         0 -       n  =  0
Axiom “Subtraction of zero from successor”:      (suc m) -       0  =  suc m
Axiom “Subtraction of successor from successor”: (suc m) - (suc n)  =  m - n
```

Why does this define _−_ for all possible arguments?

Because:

- _−_ takes **two** arguments of type $\mathbb{N}$
- **Each of these arguments** is **always** either 0, or suc k for some **smaller** $k : \mathbb{N}$
- Of the four possible combinations, two are covered by “Subtraction from zero”
- The remaining two clauses cover one of the remaining cases each.
- The third clause “builds up” the domain of definition of _−_ from smaller to larger m and n.

Defining Subtraction Inductively Using Three Clauses

```
Axiom “Subtraction from zero”:                         0 -       n  =  0
Axiom “Subtraction of zero from successor”:      (suc m) -       0  =  suc m
Axiom “Subtraction of successor from successor”: (suc m) - (suc n)  =  m - n
```

$\Longrightarrow$ **Some properties of subtraction need nested induction proofs!**

$\Longrightarrow$ **Inside nested induction steps, used induction hypotheses <u>must</u> be made explicit!**

How?

$$
\begin{array}{ll}
 & p \wedge p \\
= & \langle \text{(3.35) Golden rule } p \wedge q \equiv p \equiv q \equiv p \vee q \rangle \\
 & p \vee p \\
= & \langle \text{(3.26) Idempotency of } \vee \rangle \\
 & p
\end{array}
$$

?

How can the Golden rule have been applied here?

(3.35) **Axiom, Golden rule**: $\boxed{p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q}$

Can be used as:

- $p \wedge q \quad = \quad (p \equiv q \quad \equiv \quad p \vee q)$ — **Definition of $\wedge$**
- $(p \wedge q \quad \equiv \quad p \equiv q) \quad = \quad (p \vee q)$
- $(p \wedge q \quad \equiv \quad p) \quad = \quad (q \quad \equiv \quad p \vee q)$
- $(p \equiv q) \quad = \quad (p \wedge q \quad \equiv \quad p \vee q)$

Three Steps!

$$
\begin{array}{ll}
& p \wedge p \\
= & \langle \text{(3.35) \textbf{Golden rule}} \quad (p \wedge q) = (p \equiv q \equiv p \vee q) \rangle \\
& p \equiv p \equiv p \vee p \\
= & \langle \text{Adding parentheses} \rangle \\
& p \equiv (p \equiv p \vee p) \\
= & \langle \text{(3.35) \textbf{Golden rule}} \quad (p \wedge q \equiv p) = (q \equiv p \vee q) \rangle \\
& p \equiv (p \equiv p \wedge p) \\
= & \langle \text{Removing parentheses} \rangle \\
& p \equiv p \equiv p \wedge p \\
= & \langle \text{(3.35) \textbf{Golden rule}} \quad (p \wedge q \equiv p \equiv q) = (p \vee q) \rangle \\
& p \vee p \\
= & \langle \text{(3.26) Idempotency of } \vee \rangle \\
& p
\end{array}
$$

(3.35) **Axiom, Golden rule:** $\boxed{p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q}$

What Equivalences/Equalities are in the Golden Rule?

$p \wedge q \quad \equiv \quad p \equiv q$ **is not a consequence of (3.35) Golden rule!**

$p \wedge q \quad \equiv \quad p \vee q$ **is not a consequence of (3.35) Golden rule!**

Equality versus Equivalence

The operators $=$ (as Boolean operator) and $\equiv$

- have the **same meaning** (represent the same function),
- but **are used with different notational conventions:**
  - different precedences ($\equiv$ has lowest)
  - different **chaining behaviour**:
    - $\equiv$ is associative: $\boxed{(p \equiv q \equiv r) \quad = \quad ((p \equiv q) \equiv r) \quad = \quad (p \equiv (q \equiv r))}$
    - $=$ is **conjunctional**: $\boxed{(p = q = r) \quad = \quad ((p = q) \quad \wedge \quad (q = r))}$

(3.35) **Axiom, Golden rule:** $\boxed{p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q}$

What Equivalences/Equalities are in the Golden Rule?

$p \wedge q \quad \equiv \quad p \equiv q$ **is not a consequence of (3.35) Golden rule!**

$p \wedge q \quad \equiv \quad p \vee q$ **is not a consequence of (3.35) Golden rule!**

Equality versus Equivalence — in other words

- Writing $p = q = r$ is the same as writing $(p = q) \wedge (q = r)$
- Writing $p \equiv q \equiv r$ is the same as writing $p \equiv (q \equiv r)$
  and the same as writing $(p \equiv q) \equiv r$
- Writing $p \equiv q \equiv r$ can also be seen to be
  the same as writing $p = (q = r)$
  and the same as writing $(p = q) = r$

  — **but only for Boolean expression** p, q, r

CalcCheck-checked Mystery Steps

```
Calculation:
    true ≡ p ≡ ¬ p
  ≡⟨ (3.15) `¬ p ≡ p ≡ false` ⟩
    false
```

?

```
Calculation:
    p ≡ ¬ q ≡ p ∨ q
  ≡⟨ (3.32) ⟩
    ¬ p ∨ ¬ q
```

?

- **If you don't understand it, don't submit it!**
  (Understand the precise way in which the rule has been applied!)
- **If you encounter such "mystery steps", report!**
  (E.g. in Avenue discussions)
- When reporting such cases or asking questions about CalcCheck,

include (plain UTF8) text, not images!

Implication

(3.57) **Axiom, Definition of Implication**: $\boxed{p \Rightarrow q \ \equiv\ p \vee q \ \equiv\ q}$

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

Rewriting Implication:

(3.59) (Alternative) **Definition of Implication**: $p \Rightarrow q \ \equiv\ \neg p \vee q$

(3.60) (Dual) **Definition of Implication**: $p \Rightarrow q \ \equiv\ p \wedge q \ \equiv\ p$

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

All Propositional Axioms of the Equational Logic E

1. **(3.1) Axiom, Associativity of** $\equiv$
2. **(3.2) Axiom, Symmetry of** $\equiv$
3. **(3.3) Axiom, Identity of** $\equiv$
4. **(3.8) Axiom, Definition of** *false*
5. **(3.9) Axiom, Commutativity of** $\neg$ **with** $\equiv$
6. **(3.10) Axiom, Definition of** $\not\equiv$
7. **(3.24) Axiom, Symmetry of** $\vee$
8. **(3.25) Axiom, Associativity of** $\vee$
9. **(3.26) Axiom, Idempotency of** $\vee$
10. **(3.27) Axiom, Distributivity of** $\vee$ **over** $\equiv$
11. **(3.28) Axiom, Excluded Middle**
12. **(3.35) Axiom, Golden rule**
13. **(3.57) Axiom, Definition of Implication**
14. **(3.58) Axiom, Definition of Consequence**

The “Golden Rule” and Implication

(3.35) **Axiom, Golden rule**: $\boxed{p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q}$

Can be used as:

- $p \wedge q \quad = \quad (p \equiv q \quad \equiv \quad p \vee q)$
- $(p \equiv q) \quad = \quad (p \wedge q \quad \equiv \quad p \vee q)$
- …
- $(p \wedge q \quad \equiv \quad p) \qquad \equiv \qquad (q \quad \equiv \quad p \vee q)$

(3.57) **Axiom, Definition of Implication**: $p \Rightarrow q \ \equiv \ p \vee q \ \equiv \ q$

(3.60) (Dual) **Definition of Implication**: $p \Rightarrow q \ \equiv \ p \wedge q \ \equiv \ p$

Implication as Order on Propositions

“$p \Rightarrow q$” can be read “p is stronger-than-or-equivalent-to q”

— similar to “$x \leq y$” as “x is less-or-equal y”
— similar to “$x \geq y$” as “x is greater-or-equal y”

“$p \Rightarrow q$” can be read “p is at least as strong as q”

— similar to “$x \leq y$” as “x is at most y”
— similar to “$x \geq y$” as “x is at least y”

(3.57) **Axiom, Definition of** $\Rightarrow$ from disjunction: $p \Rightarrow q \ \equiv \ p \vee q \ \equiv \ q$

— defines the order from maximum: $p \Rightarrow q \ \equiv \ ((p \vee q) \ = \ q)$

— analogous to: $x \leq y \ \equiv \ ((x \uparrow y) \ = \ y)$
— analogous to: $k \mid n \ \equiv \ ((\mathsf{lcm}(k, n) \ = \ n)$

(3.60) (Dual) **Definition of** $\Rightarrow$ from conjunction: $p \Rightarrow q \ \equiv \ p \wedge q \ \equiv \ p$

— defines the order from minimum: $p \Rightarrow q \ \equiv \ ((p \wedge q) \ = \ p)$

— analogous to: $x \leq y \ \equiv \ ((x \downarrow y) \ = \ y)$

Weakening/Strengthening Theorems

“$p \Rightarrow q$” can be read “p is stronger-than-or-equivalent-to q”

“$p \Rightarrow q$” can be read “p is at least as strong as q”

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

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

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

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

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

Implication Theorems 2

(3.62) $p \Rightarrow (q \equiv r) \quad \equiv \quad p \wedge q \quad \equiv \quad p \wedge r$

(3.63) **Distributivity of $\Rightarrow$ over $\equiv$:**

$$p \Rightarrow (q \equiv r) \quad \equiv \quad p \Rightarrow q \quad \equiv \quad p \Rightarrow r$$

(3.64) **Self-distributivity of $\Rightarrow$:**

$$p \Rightarrow (q \Rightarrow r) \quad \equiv \quad (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$$

(3.65) **Shunting:** $\quad p \wedge q \Rightarrow r \quad \equiv \quad p \Rightarrow (q \Rightarrow r)$

Some Property Names

Let $\odot$ and $\oplus$ be binary operators and $\square$ be a constant.

*($\odot$ and $\oplus$ and $\square$ are **metavariables** for operators.)*

- "**$\odot$ is symmetric**": $x \odot y = y \odot x$
- "**$\odot$ is associative**": $(x \odot y) \odot z = x \odot (y \odot z)$
- "**$\odot$ is mutually associative with $\oplus$** (from the left)":

$$(x \odot y) \oplus z = x \odot (y \oplus z)$$

For example:

- $+$ **is** mutually associative with $-$:

$$(x + y) - z = x + (y - z)$$

- $-$ **is not** mutually associative with $+$:

$$(5 - 2) + 3 \neq 5 - (2 + 3)$$

Some Property Names (ctd.)

Let $\odot$ and $\oplus$ be binary operators and $\square$ be a constant.

*($\odot$ and $\oplus$ and $\square$ are **metavariables** for operators.)*

- "**$\odot$ is symmetric**": $x \odot y = y \odot x$
- "**$\odot$ is associative**": $(x \odot y) \odot z = x \odot (y \odot z)$
- "**$\odot$ is mutually associative with $\oplus$** (from the left)":

$$(x \odot y) \oplus z = x \odot (y \oplus z)$$

- "**$\odot$ is idempotent**": $x \odot x = x$
- "**$\square$ is a unit/identity of $\odot$**": $\square \odot x = x$ and $x \odot \square = x$
- "**$\square$ is a zero of $\odot$**": $\square \odot x = \square$ and $x \odot \square = \square$
- "**$\odot$ distributes over $\oplus$ from the left**":

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$

- "**$\odot$ distributes over $\oplus$ from the right**":

$$(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$$

- "**$\odot$ distributes over $\oplus$**":

$\odot$ distributes over $\oplus$ from the left **and**
$\odot$ distributes over $\oplus$ from the right