Discrete Mathematics with Applications I

COMPSCI&SFWRENG 2DM3

McMaster University, Fall 2019

Wolfram Kahl

2019-09-20

Plan for Today

- **Textbook Chapter 3: Propositional Calculus**

  > When reading this chapter, avoid the temptation to evaluate the boolean expressions being discussed. Simply derive theorems. The skill of manipulating formulas, without regard for their meaning, is extremely useful in all of mathematics, and studying this chapter will help you acquire this skill.
  >
  > LADM p. 42

  - (Inequivalence)
  - Disjunction
  - Conjunction

- **Inductive Definition of Natural Numbers, Induction Proofs**

Equivalence Axioms and Theorems

(3.1) **Axiom, Associativity of** $\equiv$: $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$: $\boxed{p \equiv q \equiv q \equiv p}$

(3.3) **Axiom, Identity of** $\equiv$: $\boxed{true \equiv q \equiv q}$

Theorems and Metatheorems:

(3.4) *true*

(3.5) **Reflexivity of** $\equiv$: $p \equiv p$

(3.6) **Proof Method**: To prove that $P \equiv Q$ is a theorem, transform P to Q or Q to P using Leibniz.

(3.7) **Metatheorem**: Any two theorems are equivalent.

Negation Axioms and Theorems

(3.8) **Axiom, Definition of** *false*: $\boxed{false \equiv \neg true}$

(3.9) **Axiom, Commutativity of $\neg$ with $\equiv$**: $\boxed{\neg(p \equiv q) \equiv \neg p \equiv q}$

(LADM: "Distributivity of $\neg$ over $\equiv$")
Can be used as:

- $\neg(p \equiv q) \quad = \quad (\neg p \equiv q)$
- $(\neg(p \equiv q) \equiv \neg p) \quad = \quad q$

(3.10) **Axiom, Definition of $\not\equiv$**: $\boxed{(p \not\equiv q) \equiv \neg(p \equiv q)}$

Theorems:

(3.11) $\neg p \equiv q \equiv p \equiv \neg q$ $\qquad$ $(\neg p \equiv \neg q) \equiv (p \equiv q)$

(3.12) **Double negation**: $\neg\neg p \equiv p$

(3.13) **Negation of** *false*: $\neg false \equiv true$

(3.14) $(p \not\equiv q) \equiv \neg p \equiv q$

(3.15) $\neg p \equiv p \equiv false$

Raymond Smullyan posed many puzzles about an island that has two kinds of inhabitants:

- **knights**, who always tell the truth, and
- **knaves**, who always lie.

You encounter two people A and B.
What are A and B if

1. A says "We are both knaves."?
2. A says "At least one of us is a knave."?
3. A says "If I am a knight, then so is B."?
4. **A says "We are of the same type."?**
5. A says "B is a knight" and
   B says "The two of us are opposite types."?

You encounter two people A and B. What are A and B if

4. A says "We are of the same type."?

Explanation: $A_V \equiv \boxed{A \text{ is a knave}}$

Axiom schema "Knavehood": $\boxed{A \text{ says } X} \quad \equiv \quad A_V \equiv \neg X$

$\boxed{A \text{ says } (A_V \equiv B_V)} \equiv A_V \equiv \neg(A_V \equiv B_V)$ — This is "Knavehood"

$\equiv$ ⟨ (3.9) $\neg(p \equiv q) \equiv \neg p \equiv q$ ⟩

$\boxed{A \text{ says } (A_V \equiv B_V)} \equiv A_V \equiv A_V \equiv \neg B_V$

$\equiv$ ⟨ (3.2) Symmetry of $\equiv$: $p \equiv q \equiv q \equiv p$ ⟩

$\boxed{A \text{ says } (A_V \equiv B_V)} \equiv \neg B_V$

Avoid Repetition in Proofs!

(3.22) **Principle:** Structure proofs to avoid repeating the same subexpression on many lines.

Textbook, p. 48

You encounter two people A and B. What are A and B if

1. A says "We are of the same type."?

Explanation: $A_V \equiv \boxed{A \text{ is a knave}}$

Axiom schema "Knavehood": $\boxed{A \text{ says } X} \quad \equiv \quad A_V \equiv \neg X$

$$
\begin{array}{ll}
 & \boxed{A \text{ says } (A_V \equiv B_V)} \\
\equiv & \langle \text{ "Knavehood" } \rangle \\
 & A_V \quad \equiv \quad \neg(A_V \equiv B_V) \\
\equiv & \langle \text{ (3.9) } \neg(p \equiv q) \ \equiv \ \neg p \equiv q \ \rangle \\
 & A_V \quad \equiv \quad A_V \quad \equiv \quad \neg B_V \\
\equiv & \langle \text{ (3.2) Symmetry of } \equiv\text{: } p \equiv q \equiv q \equiv p \ \rangle \\
 & \neg B_V
\end{array}
$$

Inequivalence Theorems

(3.16) **Symmetry of $\not\equiv$:** $(p \not\equiv q) \equiv (q \not\equiv p)$

(3.17) **Associativity of $\not\equiv$:** $((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$

(3.18) **Mutual associativity**: $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$

(3.19) **Mutual interchangeability**: $p \not\equiv q \equiv r \quad \equiv \quad p \equiv q \not\equiv r$

Note: Mutual associativity is not automated!

(But omission of parentheses is implemented, similar to

- $k - m + n$
- $k + m - n$
- $k - m - n$

— None of these has $m - n$ as subexpression!
— But the second one is equal to $k + (m - n)$ ...)

(3.23) Heuristic of Definition Elimination

To prove a theorem concerning an operator $\circ$ that is defined in terms of another, say $\bullet$, expand the definition of $\circ$ to arrive at a formula that contains $\bullet$; exploit properties of $\bullet$ to manipulate the formula, and then (possibly) reintroduce $\circ$ using its definition.

Textbook, p. 48

"Unfold-Fold strategy"

Inequivalence Theorems: Symmetry

(3.16) **Symmetry of $\not\equiv$:** $(p \not\equiv q) \equiv (q \not\equiv p)$

Proving (3.16) Symmetry of $\not\equiv$:

$p \not\equiv q$

$\equiv$ ⟨ (3.10) Definition of $\not\equiv$ ⟩ — **Unfold**

$\neg(p \equiv q)$

$\equiv$ ⟨ (3.2) Symmetry of $\equiv$ ⟩

$\neg(q \equiv p)$

$\equiv$ ⟨ (3.10) Definition of $\not\equiv$ ⟩ — **Fold**

$q \not\equiv p$

Disjunction Axioms

(3.24) **Axiom, Symmetry of $\vee$:** $\boxed{p \vee q \equiv q \vee p}$

(3.25) **Axiom, Associativity of $\vee$:** $\boxed{(p \vee q) \vee r \equiv p \vee (q \vee r)}$

(3.26) **Axiom, Idempotency of $\vee$:** $\boxed{p \vee p \equiv p}$

(3.27) **Axiom, Distributivity of $\vee$ over $\equiv$:** $\boxed{p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r}$

(3.28) **Axiom, Excluded Middle**: $\boxed{p \vee \neg p}$

The Law of the Excluded Middle (LEM)

Aristotle:

> . . . there cannot be an **intermediate** between contradictories, but of one subject we must either affirm or deny any one predicate. . .

Bertrand Russell in "The Problems of Philosophy":

> Three "Laws of Thought":
> 1. Law of identity: "Whatever is, is."
> 2. Law of noncontradiction: "Nothing can both be and not be."
> 3. Law of excluded middle: "Everything must either be or not be."
>
> These three laws are samples of self-evident logical principles. . .

(3.28) **Axiom, Excluded Middle**: $p \vee \neg p$

— this will often be used as: $p \vee \neg p \equiv true$

Disjunction Axioms and Theorems

(3.24)	**Axiom, Symmetry of** $\vee$:	$p \vee q \equiv q \vee p$
(3.25)	**Axiom, Associativity of** $\vee$:	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
(3.26)	**Axiom, Idempotency of** $\vee$:	$p \vee p \equiv p$
(3.27)	**Axiom, Distr. of** $\vee$ **over** $\equiv$:	$p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
(3.28)	**Axiom, Excluded Middle**:	$p \vee \neg p$

Theorems:

(3.29)	**Zero of** $\vee$:	$p \vee true \equiv true$
(3.30)	**Identity of** $\vee$:	$p \vee false \equiv p$
(3.31)	**Distrib. of** $\vee$ **over** $\vee$:	$p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
(3.32)	**(3.32)**	$p \vee q \equiv p \vee \neg q \equiv p$

Heuristics of Directing Calculations

(3.33) **Heuristic:** To prove $P \equiv Q$, transform the expression with the most structure (either P or Q) into the other.

Proving (3.29) $p \vee true \equiv true$**:**

$p \vee true$
$\equiv$ ⟨ Identity of $\equiv$ (3.3) ⟩
$p \vee (q \equiv q)$
$\equiv$ ⟨ Distr. of $\vee$ over $\equiv$ (3.27) ⟩
$p \vee q \equiv p \vee q$
$\equiv$ ⟨ Identity of $\equiv$ (3.3) ⟩
$true$

Proving (3.29) $p \vee true \equiv true$**:**

$true$
$\equiv$ ⟨ Identity of $\equiv$ (3.3) ⟩
$p \vee p \equiv p \vee p$
$\equiv$ ⟨ Distr. of $\vee$ over $\equiv$ (3.27) ⟩
$p \vee (p \equiv p)$
$\equiv$ ⟨ Identity of $\equiv$ (3.3) ⟩
$p \vee true$

?

(3.34) **Principle:** Structure proofs to minimize the number of rabbits pulled out of a hat — make each step seem obvious, based on the structure of the expression and the goal of the manipulation.

The Conjunction Axiom: The "Golden Rule"

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

Can be used as:

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

Theorems:

(3.36) **Symmetry of $\wedge$**: $p \wedge q \equiv q \wedge p$

(3.37) **Associativity of $\wedge$**: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

(3.38) **Idempotency of $\wedge$**: $p \wedge p \equiv p$

(3.39) **Identity of $\wedge$**: $p \wedge true \equiv p$

(3.40) **Zero of $\wedge$**: $p \wedge false \equiv false$

(3.41) **Distributivity of $\wedge$ over $\wedge$**: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$

(3.42) **Contradiction**: $p \wedge \neg p \equiv false$

Conjunction Theorems: Symmetry

(3.36) **Symmetry of $\wedge$**: $(p \wedge q) \equiv (q \wedge p)$

Proving (3.36) **Symmetry of $\wedge$:**

$p \wedge q$

$\equiv$ ⟨ (3.35) Definition of $\wedge$ (Golden rule) ⟩ — **Unfold**

$p \equiv q \equiv p \vee q$

$\equiv$ ⟨ (3.2) Symmetry of $\equiv$, (3.24) Symmetry of $\vee$ ⟩

$q \equiv p \equiv q \vee p$

$\equiv$ ⟨ (3.35) Definition of $\wedge$ (Golden rule) ⟩ — **Fold**

$q \wedge p$

Theorems Relating $\wedge$ and $\vee$

(3.43) **Absorption**: $p \wedge (p \vee q) \equiv p$
$p \vee (p \wedge q) \equiv p$

(3.44) **Absorption**: $p \wedge (\neg p \vee q) \equiv p \wedge q$
$p \vee (\neg p \wedge q) \equiv p \vee q$

(3.45) **Distributivity of $\vee$ over $\wedge$**: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(3.46) **Distributivity of $\wedge$ over $\vee$**: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(3.47) **De Morgan**: $\neg(p \wedge q) \equiv \neg p \vee \neg q$
$\neg(p \vee q) \equiv \neg p \wedge \neg q$

(3.21) Heuristic

Identify applicable theorems by matching the structure of expressions or subexpressions. The operators that appear in a boolean expression and the shape of its subexpressions can focus the choice of theorems to be used in manipulating it.

Obviously, the more theorems you know by heart and the more practice you have in pattern matching, the easier it will be to develop proofs.

Textbook, p. 47

What is a natural number?

How is the set $\mathbb{N}$ of all natural numbers defined?

(Without referring to the integers)

(From first principles...)

Natural Numbers — $\mathbb{N}$

- The set of all **natural numbers** is written $\mathbb{N}$.
- In Computing, zero "0" is a natural number.
- If n is a natural number, then its successor "suc n" is a natural number, too.
- We write
  - "1" for "suc 0"
  - "2" for "suc 1"
  - "3" for "suc 2"
  - "4" for "suc 3"
  - ...

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 Principle

- 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.

Induction principle for the natural numbers:

- if $P(0)$ — If P holds for 0
- and if $P(m)$ implies $P(\text{suc } m)$, — and whenever P holds for m, it also holds for suc m,
- then for all $m : \mathbb{N}$ we have $P(m)$. — then P holds for all natural numbers.

Natural Numbers — Induction Principle

- 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.

Induction principle for the natural numbers:

- if $P(0)$ — If P holds for 0
- and if $P(m)$ implies $P(\text{suc } m)$, — and whenever P holds for m, it also holds for suc m,
- then for all $m : \mathbb{N}$ we have $P(m)$. — then P holds for all natural numbers.

Natural Numbers — Induction Principle as Inference Rule

Induction principle for the natural numbers:

- if $P(0)$ — If P holds for 0
- and if $P(m)$ implies $P(\mathsf{suc}\ m)$, — and whenever P holds for m, it also holds for $\mathsf{suc}\ m$,
- then for all $m : \mathbb{N}$ we have $P(m)$. — then P holds for all natural numbers.

As **inference rule**:

Informally:

$$\frac{P(0) \qquad \begin{array}{c}\ulcorner P(m) \urcorner \\ \vdots \\ P(\mathsf{suc}\ m)\end{array}}{P(m)}$$

Formally:

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

Natural Numbers — Induction Proofs

Induction principle for the natural numbers:

- if $P[m := 0]$ — If P holds for 0
- and if we can obtain $P[m := \mathsf{suc}\ m]$ from P, — and whenever P holds for m, it also holds for $\mathsf{suc}\ m$,
- 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 $P[m := \mathsf{suc}\ m]$
using **Induction hypothesis** P

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

Factorial — Inductive 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 "$\mathsf{suc}\ n$" is a natural number, too.
- Nothing else is a natural number.
- Two natural numbers are only equal if constructed in the same way.

$\mathbb{N}$ is an inductively-defined set.

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:
  $$(\mathsf{suc}\ n)\,! = (\mathsf{suc}\ n) \cdot (n\,!)$$

_! is an inductively-defined function.

Proving properties about inductively-defined functions on $\mathbb{N}$ frequently requires use of the induction principle for $\mathbb{N}$.

Natural Number Addition — Inductive 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 only equal if constructed in the same way.

$\mathbb{N}$ is an inductively-defined set.

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: $(\mathsf{suc}\ n) + q = \mathsf{suc}\ (n + q)$

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

Proving properties about $\_+\_$ frequently requires use of the induction principle for $\mathbb{N}$.

Proving "Right-Identity of +"

Theorem "Right-identity of +": $m + 0 = m$

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 $P[m := \mathsf{suc}\ m]$
using **Induction hypothesis** P

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

Proving "Right-Identity of +"

```
Theorem "Right-identity of +": m + 0 = m
Proof:
  By induction on `m : ℕ`:
    Base case:
        0 + 0
      =⟨ "Definition of + for 0" ⟩
        0
    Induction step:
        suc m + 0
      =⟨ "Definition of + for `suc`" ⟩
        suc (m + 0)
      =⟨ Induction hypothesis ⟩
        suc m
```

Proving "Right-Identity of +" — Indentation!

```
Theorem "Right-identity of +": m + 0 = m
Proof:
␣␣By induction on `m : ℕ`:
␣␣␣␣Base case:
␣␣␣␣␣␣␣␣0 + 0
␣␣␣␣␣␣=⟨ "Definition of + for 0" ⟩
␣␣␣␣␣␣␣␣0
␣␣␣␣Induction step:
␣␣␣␣␣␣␣␣suc m + 0
␣␣␣␣␣␣=⟨ "Definition of + for `suc`" ⟩
␣␣␣␣␣␣␣␣suc (m + 0)
␣␣␣␣␣␣=⟨ Induction hypothesis ⟩
␣␣␣␣␣␣␣␣suc m
```

Proving "Right-Identity of +" — With Details

```
Theorem "Right-identity of +": m + 0 = m
Proof:
  By induction on `m : ℕ`:
    Base case `0 + 0 = 0`:
        0 + 0
      =⟨ "Definition of + for 0" ⟩
        0
    Induction step `suc m + 0 = suc m`:
        suc m + 0
      =⟨ "Definition of + for `suc`" ⟩
        suc (m + 0)
      =⟨ Induction hypothesis `m + 0 = m` ⟩
        suc m
```