Review I(Slides 11 - 62)

Logics &Sets & Induction

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

January 16, 2022

VE203 - Discrete Mathmatics

Set Operations

- union & intersection
- set difference
- symmetric difference
- power set
- cardinality
- cartesian product

Difference?

Venn Diagram v.s. Euler Diagram

Exercise

1. Let A, B, M be three sets and $A, B \subseteq M$. Show that
   1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   2. $A - (B \cup C) = (A - B) \cap (A - C)$
   3. $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

It's too boring! Let's just do the second one!

Predicates

A function $P : X \to \{\top, \bot\}$ is called a **predicate** on its domain X.

It is a declarative sentence involving variables, *i.e.*, a statement involving variables such that when the variables a substituted with appropriate individuals we obtain a **proposition**.

- **Predicate:** $P(x) : x > 1$;
- **Proposition:** $P(0) : 0 > 1$ (false); $P(2) : 2 > 1$ (true).

Logical Operations

Five operations you need to be vary familiar with:

$$\neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow$$

Strategy

- Change $p \rightarrow q$ to $\neg p \vee q$
- Truth Table
- Be careful! $\Leftrightarrow$ or $\leftrightarrow$?

Exercise

I admit this is boring but indeed you need to do it.

2. Prove that
   - $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$
   - $((P \vee Q) \wedge \neg Q) \to P$ is a tautology
   - $(A \to (B \to C)) \to (B \to (A \to C))$ is a tautology

Induction¿

A strange example shared by Horst. What's going wrong?

1.3.5. Example. Let us use mathematical induction to argue that every set of $n \geq 2$ lines in the plane, no two of which are parallel, meet in a common point.

The statement is true for $n = 2$, since two lines are not parallel if and only if they meet at some point. Since these are the only lines under considerations, this is the common meeting point of the lines.

We next assume that the statement is true for n lines, i.e., any n non-parallel lines meet in a common point. Let us now consider $n + 1$ lines, which we number 1 through $n + 1$. Take the set of lines 1 through n; by the induction hypothesis, they meet in a common point. The same is true of the lines $2, \dots, n + 1$. We will now show that these points must be identical.

Induction¿

A strange example shared by Horst. What's going wrong?

Assume that the points are distinct. Then all lines $2, \dots, n$ must be the same line, because any two points determine a line completely. Since we can choose our original lines in such a way that we consider distinct lines, we arrive at a contradiction. Therefore, the points must be identical, so all $n+1$ lines meet in a common point. This completes the induction proof.

Where is the mistake in the above "proof" of our (obviously false) supposition?

Exercise

3. Let a_n be the following expression with n nested radicals:

$$a_n = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2 + \sqrt{2}}}}$$

Please find the explict formula for a_n.

Solution

Note that a_n can be defined recursively like this: $a_1 = \sqrt{2}$, and $a_{n+1} = \sqrt{a_n + 2}$ for $n \geq 1$. We proceed by induction.

Hypothesis: $a_n = 2\cos\frac{\pi}{2^{n+1}}$

Base case: $a_1 = \sqrt{2}$, and $2 \cdot \cos\frac{\pi}{4} = 2 \cdot \frac{1}{\sqrt{2}} = \sqrt{2}$.

Inductive case: assuming the **IH** is true for n, then

$$
\begin{aligned}
a_{n+1} = \sqrt{2 + a_n} &= \sqrt{2 + 2\cos\frac{\pi}{2^{n+1}}} \\
&= \sqrt{2 + 2\cos\frac{2\pi}{2^{n+2}}} \\
&= \sqrt{2 + 2(2\cos^2\frac{\pi}{2^{n+2}} - 1)} \\
&= \sqrt{4\cos^2\frac{\pi}{2^{n+2}}} = 2\cos\frac{\pi}{2^{n+2}}
\end{aligned}
$$

By induction, we conclude that $a_n = 2\cos\frac{\pi}{2^{n+1}}$.

Structural Induction

Let B be a set and let $C_1, \ldots, C_n$ be construction rules. Let B be recursively defined to be the $\subseteq$-least set such that $B \subseteq A$ and A is closed under the rules $C_1, \ldots, C_n$. Let $P(x)$ be a property. If

1. for all $b \in B$, $P(b)$ holds
2. for all $a_1, \ldots, a_m$ and c and $1 \leq i \leq n$, if $P(a_1), \ldots, P(a_m)$ all hold and c is obtained from $a_1, \ldots, a_m$ by a single application of the rule C_i, then $P(c)$ holds

Then $P(x)$ holds for every element in A.

Exercise

Taken from Ve203 FA 2020 assignment 2:

4. Let $S \subset \mathbb{N}$ be defined by
   - $(0, 0) \in S$
   - $(a, b) \in S \Rightarrow (((a + 2, b + 3) \in S) \wedge ((a + 3, b + 2) \in S))$

Use structural induction to show that $(a, b) \in S$ implies $5 \mid (a + b)$. **(3 Marks)**

DNF & CNF

Definition:

- CNF: **product of sums** or an **AND of ORs**
- DNF: **sum of products** or an **OR of ANDS**

Examples:

- $(\neg p \vee q \vee r) \wedge (\neg q \vee \neg r) \wedge (r)$
- $(\neg p \wedge q \wedge r) \vee (\neg q \wedge \neg r)$

Question

What's the DNF/CNF for a tautology?

Exercise

5. Suppose that a truth table in **n** propositional variables is specified. Show that a compound proposition with this truth table can be written to a well-determined DNF.
(Take from Vv186 Assignment Exercise 1.4)

A	B	$f(A, B)$
T	T	T
T	F	F
F	T	T
F	F	F

$$f(A, B) = (A \wedge B) \vee (\neg A \wedge B)$$

Introduction to boolean algebra

If we regard $\vee$ as $+$, $\wedge$ as $\cdot$, then the equation

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

is just the distributivity law:

$$A \cdot (B + C) = (A \cdot B) + (A \cdot C)$$

Do It Yourself:

Check whether the axiom P1 – P9 for rational numbers also hold for such operations.

Properties

We denote $\neg A$ as $\overline{A}$. And, 1 means true ($\top$), 0 means false ($\bot$). We have the following:

- $A \cdot 1 = A$
- $A + 1 = 1$
- $A + \overline{A} = 1$
- $A \cdot \overline{A} = 0$
- $\overline{\overline{A}} = A$
- $\overline{A + B} = \overline{A} \cdot \overline{B}$
- $\overline{A \cdot B} = \overline{A} + \overline{B}$
- $A + AB = A$
- $\ldots$

A Truth Table

A	B	C	$F(A,B,C)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	T
F	F	F	F

Expression in DNF:

$$F = ABC + AB\overline{C} + \overline{A}BC + \overline{A}\,\overline{B}C$$

Ugly! How to simplify?

Gray Code

In the encoding of a set of binary numbers, if any two adjacent codes differ by **only one** binary digit, the encoding is called a gray code.

Interestingly, there's also only a **one-digit difference** between the largest and the smalleset number, namely **end to end**.

number	code	number	code
0	0000	8	1100
1	0001	9	1101
2	0011	10	1111
3	0010	11	1110
4	0110	12	1010
5	0111	13	1011
6	0101	14	1001
7	0100	15	1000

How to transfer?

Binary code -> Gray code (coding) :

From the rightmost bit, each bit XOR with the left, as the value of the corresponding gray code, the leftmost bit remains unchanged.

Gray code - > binary code (decoding) :

From the second digit on the left, each bit XOR with the decoded value of the left bit, as the decoded value of that bit, the leftmost bit remains unchanged.

Example

`https://vijos.org/p/1176`

Karnaugh Graph

A \ BC	00	01	11	10
00			1	1
01	1		1	1

Table: Karnaugh Graph of 3 variables

Expressions:

$$
\begin{aligned}
F &= \overline{A}BC + \overline{A}B\overline{C} + A\overline{B}\,\overline{C} + ABC + AB\overline{C} \\
&= A\overline{C} + B
\end{aligned}
$$

Exercise

5. Simplify the following expressions:

a) $wxyz + wxy\bar{z} + wx\bar{y}\,\bar{z} + w\bar{x}yz + w\bar{x}\,\bar{y}z + w\bar{x}\,\bar{y}\,\bar{z} + \bar{w}x\bar{y}z + \bar{w}\,\bar{x}yz + \bar{w}\,\bar{x}y\bar{z}$

b) $wx\bar{y}\,\bar{z} + w\bar{x}yz + w\bar{x}y\bar{z} + w\bar{x}\,\bar{y}\,\bar{z} + \bar{w}x\bar{y}\,\bar{z} + \bar{w}\,\bar{x}y\bar{z} + \bar{w}\,\bar{x}\,\bar{y}\,\bar{z}$

wx \ yz	00	01	11	10
00	1			1
01				
11				
10	1			1

Table: $x\bar{z} = wxyz + wx\bar{y}z + \bar{w}xyz + \bar{w}x\bar{y}z$

Answer: a) $wxyz + wx\bar{z} + w\bar{x}\,\bar{y} + \bar{w}\,\bar{x}y + \bar{w}x\bar{y}z$

b) $\bar{y}\,\bar{z} + w\bar{x}y + \bar{x}\,\bar{z}$

OR & AND in circuits

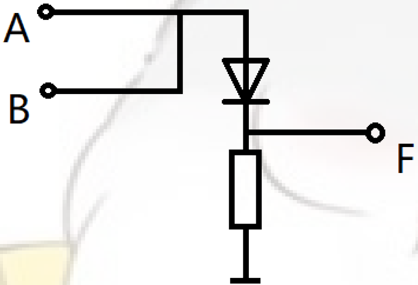

Figure: OR circuit

What about AND and NOT ?

Reference

- Pictures from Dr. Horst Hohberger.
- Exercises from 2020-Ve203 Assignment2.
- Exercises from 2021-Vv186 Assignment1.
- Exercises from 2019–Vv186 TA-Zhang Leyang.
- Contents from 2020 Fall Ve203 TA-Peng Chengjun.
- Exercises from 2021 Fall Ve203 TA-Zhao Jiayuan.
- Exercises from my 2021–Vv186 Mid1 RC.
- Kenneth, H.Rosen. Translated by Xu Liutong etc. *Discrete Mathematics amd Its Applications*, Eightth Edition, Chinese Abridgement. China Machine Press, 2019 print.