Mathematical Foundations for Software Engineering

Course notes

Attila Matolcsy

25th August 2023 - Present

Contents

1 About

This document is Attila Matolcsy's own personal notes from the University of Gothenburg's Software Engineering and Management Bsc. Programme's Mathematical Foundations for SEM course.

These are all the notes from lessons, unprocessed.

WARNING

This document has typos in it, please use the main document that is cleaned up!

2 28^{th} August 2023

2.1 Introduction to the course

Lessons are not mandatory, nor the TA sessions. We join a TA group on Canvas, we are asked not to jump between them. The gropus should not have more than 8 persons / group.

Workload $\approx 200h$

Groups up to 3 are allowed but submissions must be on an individual basis.

FAQ is available on Canvas

You can send christian.berger@gu.se an email about problems that come up during class.

Course literature is available on Canvas, non of which is mandatory.

2.2 Logic

Logic = Meaning of mathematical statements $\wedge$ basis of reasoning

Applications = design of computing machines

0s & 1s.

Proofs = matheatical argument, essential for programs
= Security of systems

Theorem = Proven mathematical statements

Propositions = declerative statemnt that is either True or False

For e.g.:
- Stockholm is the capital of Sweden
- $4x5 = 20$
- $\pi \approx \frac{22}{7}$

Counter e.g.:
- attend my lectures
- $x + 1 = \pi$

Propositions are named by letters: p, q, r, s

field of propositional logic = the field that deals with propositionals

mathematical statements can be compined $\Rightarrow$ compoind propositions

Def1: $\neg p =$ not p

Def2: Conjuction: pq

p	q	$p \wedge q$	$\neg(A \wedge B)$
T	T	T	F
F	T	F	T
T	F	F	T
F	F	F	T

(From now on I will refer to Trues (Ts) as 1 and Falses (Fs) as 0)

Def 3: $\vee$ is logical or

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Def 4: exclusive or

p	q	$p \oplus q$	$\neg(p \oplus q)$
1	1	0	1
1	0	1	0
0	1	1	0
0	0	0	1

Def 5: implication / conditional statements

p	q	$p \Rightarrow q$	$\neg p \vee q$	$\neg p$
1	1	1	1	0
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Def 6: Biconditional statements, if and only if, iff

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Def 7: tantology: always true regardless of values of the propositions

Contardiction: always false regardless of values of the propositions

contingency: $\neg$ (tantology) $\wedge \neg$ (contradiction)

equivalents:

$$\begin{aligned} p \wedge 1 &\equiv p \\ p \vee 1 &\equiv 1 \\ p \wedge 0 &\equiv 0 \\ p \vee 0 &\equiv p \end{aligned}$$

$p \wedge q \equiv p$

p	q	$p \wedge q$
1	1	1
0	0	0

negation laws:

$p \vee \neg p \equiv 1$

p	$\neg p$	$p \vee \neg p$
1	0	1
0	1	1

$p \wedge \neg p \equiv 0$

p	$\neg p$	$p \wedge \neg p$
1	0	0
0	1	0

3 29th August 2023

3.1 Binary counting

...	p	q	r	s
x increases from right to left: 2^x This is what the binary number represents:	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
This is our binary number:	$0\,(F)$	$1\,(T)$	$0\,(F)$	$1\,(T)$
We need to sum this: $0 + 4 + 0 + 1 = 5$	$0 \cdot 8 = 0$	$1 \cdot 4 = 4$	$0 \cdot 2 = 0$	$1 \cdot 1 = 1$

3.2 Predicate Logic

Propositional logic: everything is atomic

Predicate logic: Formalism of propositional logic is extended and more complicated expressions are possible to be ued for formal inference.

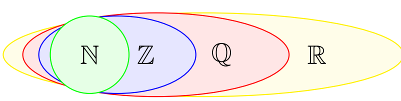
Predicate logic contains:

- all components from propositional logic
- terms (E.g.: Alice likes BOS [Underlined is a term])
- quantifiers:
  - something is always True
  - something is sometimes True
  - something is never True
- Predicate symbols: P, Q, R
- functions: f, g
- quantifiers: $\forall, \exists$
- identity: $=$

Example: "There is a smallest number."

Collection of al persons, ideas, symbols, data structures that affect the logical argument under consideration

Elements of the inverese of the discourse are called individuals



...

Order of args is important

unary predicate: "x is a cat" binary predicate: "y is mother of y"

unary predicates descripbe properties of object: $p(x) \Rightarrow$ x has property P

interpret as: of a predicate (P) in a set of objects (called A) is a set og those elements of A (AKA subset) that have property p:

$\{\alpha \in A \quad | \quad P(\alpha)\}$

$\{(\alpha, \beta) \in A \times A \quad | \quad Q(\alpha, \beta)\}$

Atomic formula

1. predicate name + arguments
2. an identity $t_1 = t_2$

Atomic formulas are statements that can be combined woth logical connectioves

$M(j,p) \to \neg M(p,j)$

If Jane is Paul's mother, then Paul is not Jame's mother.

If all arguments of a predicate are individual constants, the resulting formula must be T or F

Example:

	Bob	Jane	Alice	Paul
Bob	F	F	F	F
Jane	F	F	T	T
Alice	F	F	F	F
Paul	F	F	F	F

$M(a,b)$

Inly method that assigns truth values to all possible combinations of individuals is called assignment of the predicate

Universal quantifier: $\forall$

something is true for all infividuals

Existential quantifier: $\exists$

something is for at least one individual

$\forall \times A$ $\forall =$ for all
$\times$ is bound by the quantifier
A is the scope

Everone gets a break once in a while

$B(x) :=$ "x gets a break in a while"
$\forall \times B(x)$

Some people don't eat meat

$p(x) :=$ "x eats meat"
$\exists \times (\neg P(x))$

$\exists x (\forall y k (x,y))$

$\neg \exists x A(x) \equiv \forall x \neg A$