Chapter 1

Logics

Course "Model checking"

Volker Stolz, Martin Steffen

Autumn 2019

Section

Algebraic and first-order signatures

Chapter 1 “Logics”
Course “Model checking”
Volker Stolz, Martin Steffen
Autumn 2019

Intro

Signature

- fixes the "syntactic playground"
- selection of se
  - *functional* and
  - *relational*

  symbols, together with "arity" or sort-information

Sorts

- Sort
  - name of a domain (like `Nat`)
  - restricted form of type
- single-sorted vs. multi-sorted case
- single-sorted
  - one sort only
  - "degenerated"
  - *arity* = number of arguments (also for relations)

Terms

- given: signature Σ
- set of variables X (with typical elements $x, y', \ldots$)

$$
\begin{array}{rcll}
t & ::= & x & \text{variable} \\
& | & f(t_1, \ldots, t_n) & f \text{ of arity } n
\end{array}
\tag{1}
$$

- $T_\Sigma(X)$
- terms without variables (from $T_\Sigma(\emptyset)$ or short T_Σ): *ground* terms

Substutition

- Substitution = *replacement*, namely of variables by terms
- notation $t[s/x]$

First-order signature (with relations)

- add relational symbols to Σ
- typical elements P, Q
- relation symbols with fixed arity n-ary predicates or relations)
- standard binary symbol: $\doteq$ (equality)

Section

First-order logic

Syntax
Semantics
Proof theory

Chapter 1 “Logics”
Course “Model checking”
Volker Stolz, Martin Steffen
Autumn 2019

Syntax

- given: first order signature Σ

$$
\begin{array}{rcll}
\varphi & ::= & P(t, \ldots, t) \mid \top \mid \bot & \text{atomic formula} \\
& \mid & \varphi \wedge \varphi \mid \neg\varphi \mid \varphi \rightarrow \varphi \mid \ldots & \text{formulas} \\
& \mid & \forall x.\varphi \mid \exists x.\varphi &
\end{array}
$$

First-order structures and models

- given Σ
- assume single-sorted case

first-order model

model M

$$M = (A, I)$$

- A some domain/set
- interpretation I, respecting arity
  - $[\![f]\!]^I : A^n \to A$
  - $[\![P]\!]^I : A^n$

- cf. first-order structure

Giving meaning to variables

Variable assignment

- given Σ and model

$$\sigma : X \to A$$

- other names: *valuation*, *state*

(E)valuation of terms

- σ "straightforwardly extended/lifted to terms"
- how would one define that (or write it down, or implement)?

Free and bound occurrences of variables

- quantifiers *bind* variables
- *scope*
- other binding, scoping mechanisms
- variables can *occur* free or not (= *bound*) in a formula
- careful with substitution
- how could one define it?

Substitution

- basically:
  - generalize substitution from terms to formulas
  - careful about binders especially don't let substitution lead to variables being "captured" by binders

Example

$$\varphi = \exists x.x + 1 \doteq y \qquad \theta = [y/x]$$

Satisfaction

Definition ($\models$)

$M, \sigma \models \varphi$

- Σ fixed
- in model M and with variable assignment σ formula φ is true (holds
- M and σ satisfy φ
- minority terminology: M, σ model \$$\varphi$

Exercises

- substitutions and variable assignments: similar/different?
- there are infinitely many primes
- there is a person with at least 2 neighbors (or exactly)
- every even number can be written as the sum of 2 primes

Proof theory

- how to infer, derive, deduce formulas (from others)
- mechanical process
- soundness and completeness
- *proof* = deduction (sequence or tree of steps)
- theorem
  - syntactic: derivable formula
  - semantical a formula which holds (in a given model)
- (fo)-theory: set of formulas which are
  - derivable
  - true (in a given model)
- soundness and completeness

Deductions and proof systems

A proof system for a given logic consists of

- axioms (or *axiom schemata*), which are formulae assumed to be true, and
- inference rules, of approx. the form

$$\frac{\varphi_1 \quad \cdots \quad \varphi_n}{\psi}$$

- $\varphi_1, \ldots, \varphi_n$ are premises and ψ conclusion.

A simple form of derivation

Derivation of φ

Sequence of formulae, where each formula is

- an axiom or
- can be obtained by applying an inference rule to formulae earlier in the sequence.

- $\vdash \varphi$
- more general: set of formulas Γ

$$\Gamma \vdash \varphi$$

- proof $=$ derivation
- theorem: derivable formula ($=$ last formula in a proof)

Proof systems and proofs: remarks

- "definitions" from the previous slides: not very formal

in general: a proof system: a "mechanical" (= formal and constructive) way of conclusions from axioms (= "given" formulas), and other already proven formulas

- Many different "representations" of how to draw conclusions exists, the one sketched on the previous slide
  - works with "sequences"
  - corresponds to the historically oldest "style" of proof systems ("Hilbert-style"), some would say outdated ...
  - otherwise, in that naive form: impractical (but sound & complete).
  - nowadays, better ways and more suitable for computer support of representation exists (especially using trees). For instance natural deduction style system

A proof system for prop. logic

Observation

We can axiomatize a subset of *propositional logic* as follows.

$$\varphi \to (\psi \to \varphi) \tag{Ax1}$$

$$(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi)) \tag{Ax2}$$

$$((\varphi \to \bot) \to \bot) \to \varphi \tag{DN}$$

$$\frac{\varphi \quad \varphi \to \psi}{\psi} \tag{MP}$$

A proof system

Example

$p \to p$ is a theorem of PPL:

$(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$	Ax_2	(1)
$p \to ((p \to p) \to p)$	Ax_1	(2)
$(p \to (p \to p)) \to (p \to p)$	MP on (1) and (2)	(3)
$p \to (p \to p)$	Ax_1	(4)
$p \to p$	MP on (3) and (4)	(5)

Section

Modal logics

Chapter 1 “Logics”
Course “Model checking”
Volker Stolz, Martin Steffen
Autumn 2019

Introduction

- Modal logic: logic of *"necessity"* and *"possibility"*, in that originally the intended meaning of the *modal* operators $\Box$ and $\Diamond$ was
  - $\Box\varphi$: φ is necessarily true.
  - $\Diamond\varphi$: φ is possibly true.
- Depending on what we intend to capture: we can interpret $\Box\varphi$ differently.

temporal φ will always hold.
doxastic I believe φ.
epistemic I know φ.
intuitionistic φ is provable.
deontic It ought to be the case that φ.

We will restrict here the modal operators to $\Box$ and $\Diamond$ (and mostly work with a temporal "mind-set".

Kripke structures

Definition (Kripke frame and Kripke model)

- A Kripke frame is a structure (W, R) where
  - W is a non-empty set of *worlds*, and
  - $R \subseteq W \times W$ is called the *accessibility relation* between worlds.

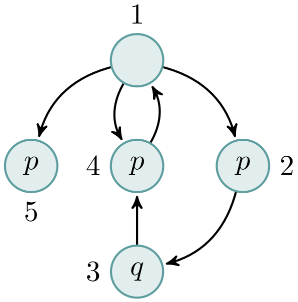
Kripke structures

Definition (Kripke frame and Kripke model)

- A Kripke frame is a structure (W, R) where
  - W is a non-empty set of *worlds*, and
  - $R \subseteq W \times W$ is called the *accessibility relation* between worlds.
- A Kripke model M is a structure (W, R, V) where
  - (W, R) is a frame, and
  - V a function of type $V : W \to (P \to \mathbb{B})$ (called valuation).

isomorphically: $V : W \to 2^P$

Illustration



Example (Kripke model)

Let $P = \{p, q\}$. Then let $M = (W, R, V)$ be the Kripke model such that

- $W = \{w_1, w_2, w_3, w_4, w_5\}$
- $R = \{(w_1, w_5), (w_1, w_4), (w_4, w_1), \dots\}$
- $V = [w_1 \mapsto \emptyset, w_2 \mapsto \{p\}, w_3 \mapsto \{q\}, \dots]$

Satisfaction

Definition (Satisfaction)

A modal formula φ is true in the world w of a model V, written $V, w \models \varphi$, if:

$V, w \models p$	iff	$V(w)(p) = \top$
$V, w \models \neg\varphi$	iff	$V, w \not\models \varphi$
$V, w \models \varphi_1 \vee \varphi_2$	iff	$V, w \models \varphi_1$ or $V, w \models \varphi_2$
$V, w \models \Box\varphi$	iff	$V, w' \models \varphi$, for all w' such that wRw'
$V, w \models \Diamond\varphi$	iff	$V, w' \models \varphi$, for some w' such that wRw'

“Box” and “diamond”

- modal operators $\Box$ and $\Diamond$
- often pronounced “nessecarily” and “possibly”
- mental picture: depends on “kind” of logic (temporal, epistemic, deontic . . .) and (related to that) the form of accessibilty relation R:
- formal definition: see previous slide

Different kinds of relations

R a *binary relation* on a set, say W, i.e., $R \subseteq W$

- reflexive
- transitive
- (right) Euclidian
- total
- order relation
- ....

Valid in frame/for a set of frames

If $(W, R, V), s \models \varphi$ for all s and V, we write

$$(W, R) \models \varphi$$

Example (Samples)

- $(W, R) \models \Box\varphi \rightarrow \varphi$ iff R is reflexive.
- $(W, R) \models \Box\varphi \rightarrow \Diamond\varphi$ iff R is total.
- $(W, R) \models \Box\varphi \rightarrow \Box\Box\varphi$ iff R is transitive.
- $(W, R) \models \neg\Box\varphi \rightarrow \Box\neg\Box\varphi$ iff R is Euclidean.

Some Exercises

Prove the double implications from the slide before!

Base line axiomatic system ("K")

$$\frac{\varphi \text{ is a propositional tautology}}{\varphi}\ \mathrm{PL}$$

$$\frac{}{\Box(\varphi_1 \to \varphi_2) \to (\Box\varphi_1 \to \Box\varphi_2)}\ \mathrm{K}$$

$$\frac{\varphi \to \psi \qquad \varphi}{\psi}\ \mathrm{MP}$$

$$\frac{\varphi}{\Box\varphi}\ \mathrm{G}$$

Sample axioms for different accessibility relations

$$\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi) \tag{K}$$

$$\Box\varphi \to \Diamond\varphi \tag{D}$$

$$\Box\varphi \to \varphi \tag{T}$$

$$\Box\varphi \to \Box\Box\varphi \tag{4}$$

$$\neg\Box\varphi \to \Box\neg\Box\varphi \tag{5}$$

$$\Box(\Box\varphi \to \psi) \to \Box(\Box\psi \to \varphi) \tag{3}$$

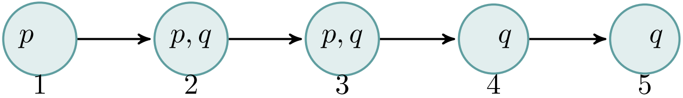
$$\Box(\Box(\varphi \to \Box\varphi) \to \varphi) \to (\Diamond\Box\varphi \to \varphi)) \tag{Dum}$$

Different “flavors” of modal logic

Logic	Axioms	Interpretation	Properties of R
D	K D	deontic	total
T	K T		reflexive
K45	K 4 5	doxastic	transitive/euclidean
S4	K T 4		reflexive/transitive
S5	K T 5	epistemic	reflexive/euclidean
			reflexive/symmetric/transitive
			equivalence relation

Some exercises

Consider the frame (W, R) with $W = \{1, 2, 3, 4, 5\}$ and $(i, i+1) \in R$

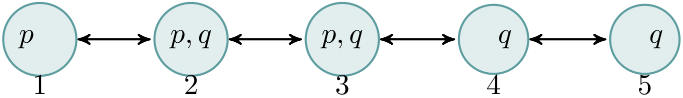


- $M, 1 \models \Diamond\Box p$
- $M, 1 \models \Diamond\Box p \rightarrow p$
- $M, 3 \models \Diamond(q \wedge \neg p) \wedge \Box(q \wedge \neg p)$
- $M, 1 \models q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q)))$
- $M \models \Box q$

Exercises (2): bidirectional frames

Bidirectional frame

A frame (W, R) is bidirectional iff $R = R_F + R_P$ s.t. $\forall w, w'(wR_Fw' \leftrightarrow w'R_Pw)$.



Consider $M = (W, R, V)$ from before. Which of the following statements are correct in M and why?

1. $M, 1 \models \Diamond\Box p$
2. $M, 1 \models \Diamond\Box p \rightarrow p$
3. $M, 3 \models \Diamond(q \wedge \neg p) \wedge \Box(q \wedge \neg p)$
4. $M, 1 \models q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q)))$
5. $M \models \Box q$
6. $M \models \Box q \rightarrow \Diamond\Diamond p$

Exercises (3): validities

Which of the following are *valid* in modal logic. For those that are not, argue why and find a class of frames on which they become valid.

1. $\Box\bot$
2. $\Diamond p \rightarrow \Box p$
3. $p \rightarrow \Box\Diamond p$
4. $\Diamond\Box p \rightarrow \Box\Diamond p$

Section

References

Chapter 1 “Logics”
Course “Model checking”
Volker Stolz, Martin Steffen
Autumn 2019

References I

Bibliography

[1] Bowen, J. P. and Hinchey, M. G. (2005). Ten commandments revisited: a ten-year perspective on the industrial application of formal methods. In *FMICS '05: Proceedings of the 10th international workshop on Formal methods for industrial critical systems*, pages 8–16, New York, NY, USA. ACM Press.

[2] Peled, D. (2001). *Software Reliability Methods*. Springer Verlag.