LMSE 1

Logische Methoden des Software Engineerings
Vertiefungsmodul 1

Prof. Dr. Jakob Rehof

M.Sc. Andrej Dudenhefner

Lehrstuhl XIV, Software Engineering

Diese Vorlesung

- Konsistenz und Normalisierung
- Kripke Modelle und Heyting Algebren

- Lesen:
  - LCHI 2.3, 2.4 (optional), 2.5, 2.6

- Übungen:
  - Folie 8 und 17

Consistency from normalization

By CHI!

4.3.1. Proposition. $\not\vdash \bot$.

Proof. Assume that $\vdash \bot$. Then $\vdash M : \bot$ for some $M \in \Lambda_\Pi$. By the weak normalization theorem and the subject reduction theorem there is then an $N \in \mathrm{NF}_\beta$ such that $\vdash N : \bot$.

Now, λ-terms in normal form have form $x\, N_1 \ldots N_m$ (where $N_1, \ldots, N_n$ are normal-forms) and $\lambda x{:}\sigma\, .\, N'$ (where N' is in normal form). We cannot have N of the first form (then $x \in \mathrm{FV}(N)$, but since $\vdash N : \bot$, $\mathrm{FV}(N) = \{\}$). We also cannot have N of the second form (then $\bot = \sigma \to \tau$ for some σ, τ which is patently false). □

Form of normal deductions!

Semantik der intuitionistischen Logik

- Für die klassische Logik haben wir die Boolsche Semantik der Wahrheit und Gültigkeit, die mit der Beweisbarkeit übereinstimmt (Gesundheit und Vollständigkeit)

- Die Frage meldet sich natürlich, ob es nicht eine ähnliche semantische Charakterisierung der Beweisbarkeit in der intuitionistsichen Logik gibt?

- Wir werden sehen, dass die Antwort ist: „ja und nein“ ☺

Semantik der intuitionistischen Logik

Menu:

- Wir repetieren zuerst die bekannte Warheitssemantik der klassichen Logik
- Wir erkennen, dass diese ein Spezialfall einer algebraischen Charakterisierung durch Boolsche Algebren ist
- Wir sehen dann, dass eine ähnliche Charakterisierung für die intuitionistische Logik möglich ist (also „ja“). Aber die Strukturen, die wir dafür brauchen, sind andere. Wir kriegen insbesondere *keine „Wahrheitstabellen“,* und insofern ist die Semantik der i.L. komplizierter als die Semantik der k.L. (also „nein“)
- Wir betrachten zwei alternative (und äquivalente) semantische Modelle: Kripke Modelle und Heyting Algebren

Wahrheitssemantik der klassischen Logik

2.3.1. DEFINITION. Let $\mathbb{B} = \{0, 1\}$.

(i) A *valuation in* $\mathbb{B}$ is a map $v : PV \to \mathbb{B}$; such a map will also be called a 0-1 *valuation.*

(ii) Given a 0-1 valuation v, define the map $[\![\bullet]\!]_v : \Phi \to \mathbb{B}$ by:

$$\begin{array}{lcll} [\![p]\!]_v & = & v(p), & \text{for } p \in PV; \\ [\![\bot]\!]_v & = & 0; & \\ [\![\varphi \vee \psi]\!]_v & = & \max\{[\![\varphi]\!]_v, [\![\psi]\!]_v\}; & \\ [\![\varphi \wedge \psi]\!]_v & = & \min\{[\![\varphi]\!]_v, [\![\psi]\!]_v\}; & \\ [\![\varphi \to \psi]\!]_v & = & \max\{1 - [\![\varphi]\!]_v, [\![\psi]\!]_v\}. & \end{array}$$

We also write $v(\varphi)$ for $[\![\varphi]\!]_v$.

(iii) A formula $\varphi \in \Phi$ is a *tautology* if $v(\varphi) = 1$ for all valuations in $\mathbb{B}$.

Mengentheoretische Semantik der klassischen Logik

2.3.2. DEFINITION. A *field of sets (over X)* is a nonempty family $\mathcal{R}$ of subsets of X, closed under unions, intersections and complement (to X).

It follows immediately that $\{\}, X \in \mathcal{R}$, for each field of sets $\mathcal{R}$ over X. Examples of fields of sets are:

(i) $P(X)$;

(ii) $\{\{\}, X\}$;

(iii) $\{A \subseteq X : A \text{ finite or } -A \text{ finite}\}$ ($-A$ is the complement of A).

Mengentheoretische Semantik der klassischen Logik

2.3.3. DEFINITION. Let $\mathcal{R}$ be a field of sets over X.

(i) A *valuation in* $\mathcal{R}$ is a map $v : PV \to \mathcal{R}$.

(ii) Given a valuation v in $\mathcal{R}$, define the map $[\![\bullet]\!]_v : \Phi \to X$ by:

$$
\begin{array}{lcll}
[\![p]\!]_v & = & v(p) & \text{for } p \in PV \\
[\![\bot]\!]_v & = & \{\} & \\
[\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \cup [\![\psi]\!]_v & \\
[\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \cap [\![\psi]\!]_v & \\
[\![\varphi \to \psi]\!]_v & = & (X - [\![\varphi]\!]_v) \cup [\![\psi]\!]_v &
\end{array}
$$

We also write $v(\varphi)$ for $[\![\varphi]\!]_v$.

Mengentheoretische Semantik der klassischen Logik

2.3.4. PROPOSITION. *The above two approaches to semantics are equivalent, i.e., the following conditions are equivalent for each field of subsets $\mathcal{R}$ over a nonempty set X:*

1. *φ is a tautology;*
2. *$v(\varphi) = X$, for all valuations v in $\mathcal{R}$.*

PROOF. (1) $\Rightarrow$ (2): Suppose that $v(\varphi) \neq X$. There is an element $a \in X$ such that $a \notin v(\varphi)$. Define a 0-1 valuation w so that $w(p) = 1$ iff $a \in v(p)$. Prove by induction that for all formulas ψ

$$w(\psi) = 1 \quad \text{iff} \quad a \in v(\psi).$$

Then $w(\varphi) \neq 1$.

(2) $\Rightarrow$ (1): A 0-1 valuation can be seen as a valuation in $\mathcal{R}$ that assigns only X and $\{\}$ to propositional variables. $\square$

Boolsche Algebra

2.3.5. DEFINITION. A *Boolean algebra* is an algebraic system of the form $\mathcal{B} = \langle B, \cup, \cap, -, 0, 1 \rangle$, where:

- $\cup, \cap$ are associative and commutative;
- $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$ and $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$;
- $a \cup 0 = a$ and $a \cap 1 = a$;
- $-a \cup a = 1$ and $-a \cap a = 0$.

The relation $\leq$ defined by $a \leq b$ iff $a \cup b = b$ is a partial order[1] in every Boolean algebra, and the operations $\cap, \cup$ are the *glb* and *lub* operations w.r.t. this order.

Semantik für intuitionistische Logik?

- *Wir können nicht die Wahrheitssemsemantik oder die Boolsche Semantik auf die intuitionistische Logik übertragen. Es gibt keine endliche Warhheitssemantik (siehe Folie 9).*

Intuitionistic logic is not finite-valued: There is no single finite Heyting algebra $\mathcal{H}$ such that $\vdash \varphi$ is equivalent to $\mathcal{H} \models \varphi$. Indeed, consider the formula $\bigvee\{p_i \leftrightarrow p_j : i, j = 0, \ldots, n \text{ and } i \neq j\}$. (Here the symbol $\bigvee$ abbreviates the disjunction of all members of the set.) This formula is not valid in general (Exercise 2.7.10), although it is valid in all Heyting algebras of cardinality at most n.

Kripke model (sec. 2.5)

2.5.1. DEFINITION. A *Kripke model* is defined as a tuple of the form $\mathcal{C} = \langle C, \leq, \Vdash \rangle$, where C is a non-empty set, $\leq$ is a partial order in C and $\Vdash$ is a binary relation between elements of C (called *states* or *possible worlds*) and propositional variables, that satisfies the following monotonicity condition:

$$\text{If } c \leq c' \text{ and } c \Vdash p \text{ then } c' \Vdash p.$$

Monotonicity

Kripke model

2.5.2. DEFINITION. If $\mathcal{C} = \langle C, \leq, \Vdash \rangle$ is a Kripke model, then

- $c \Vdash \varphi \vee \psi$ iff $c \Vdash \varphi$ or $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi$ iff $c \Vdash \varphi$ and $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi$ iff $c' \Vdash \psi$, for all c' such that $c \leq c'$ and $c' \Vdash \varphi$;
- $c \Vdash \bot$ never happens.

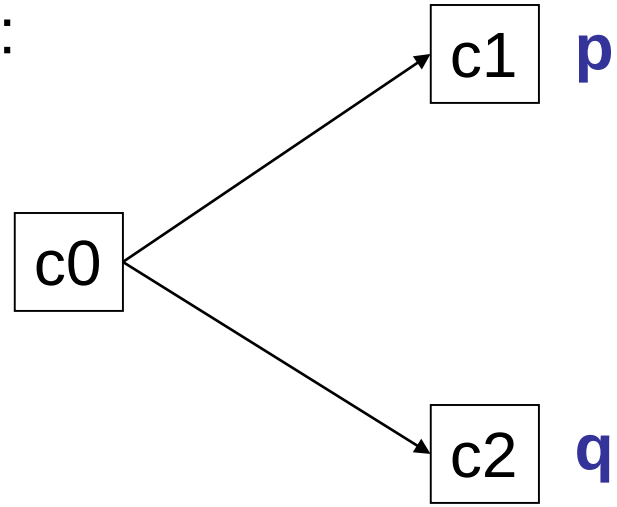
We use $\mathcal{C} \Vdash \varphi$ to mean that $c \Vdash \varphi$, for all $c \in \mathcal{C}$.

Implied rule for negation:

- $c \Vdash \neg\varphi$ iff $c' \nVdash \varphi$, for all $c' \geq c$.

Example

Kripke model:



In this Kripke model we have:

- c0 ||- **- - (p v q)**
- c0 ||- **(p→q)→q**
- *not* c0 ||- **(p v q)**

Übung I

- **Übung:** Beweisen Sie anhand des Kripke Modells auf Folie 25, dass c0 ||- (p -> q) -> q gilt.

- **Übung:** Beweisen Sie, dass die Formel (p -> q) -> q nicht intuitionistisch gültig ist

- **Übung:** Beweisen Sie die Monotonieeigenschaft:

$$\text{If } c \leq c' \text{ and } c \Vdash \varphi \text{ then } c' \Vdash \varphi.$$

Kripke model

Soundness and completeness of Kripe semantics:

2.5.6. THEOREM. *The sequent* $\Gamma \vdash \varphi$ *is provable iff for all Kripke models* $\mathcal{C}$, *the condition* $\mathcal{C} \Vdash \Gamma$ *implies* $\mathcal{C} \Vdash \varphi$.

Proof: By turning every Heyting algebra
into a Kripke model, using prime filter construction.

Disjunction property

2.5.7. PROPOSITION. *If* $\vdash \varphi \vee \psi$ *then either* $\vdash \varphi$ *or* $\vdash \psi$.

PROOF. Assume $\nvdash \varphi$ and $\nvdash \psi$. There are Kripke models $\mathcal{C}_1 = \langle C_1, \leq_1, \Vdash_1 \rangle$ and $\mathcal{C}_2 = \langle C_2, \leq_2, \Vdash_2 \rangle$ and states $c_1 \in C_1$ and $c_2 \in C_2$, such that $c_1 \nVdash \varphi$ and $c_2 \nVdash \psi$. Without loss of generality we can assume that c_1 and c_2 are least elements of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and that $C_1 \cap C_2 = \{\}$. Let $\mathcal{C} = \langle C_1 \cup C_2 \cup \{c_0\}, \leq, \Vdash \rangle$, where $c_0 \notin C_1 \cup C_2$, the order is the union of $\leq_1$ and $\leq_2$ extended by c_0 taken as the least element, and $\Vdash$ is the union of $\Vdash_1$ and $\Vdash_2$. That is,

$$c_0 \nVdash p,$$

for all variables p. It is easy to see that this is a Kripke model. In addition we have $\mathcal{C}, c_1 \Vdash \vartheta$ iff $\mathcal{C}_1, c_1 \Vdash \vartheta$, for all formulas ϑ, and a similar property holds for c_2.

Now suppose that $\vdash \varphi \vee \psi$. By soundness, we have $c_0 \Vdash \varphi \vee \psi$, and thus either $c_0 \Vdash \varphi$ or $c_0 \Vdash \psi$, by definition of $\Vdash$. Then either $c_1 \Vdash \varphi$ or $c_2 \Vdash \psi$, because of monotonicity. □

Implicational fragment

2.6.1. THEOREM. *The implicational fragment of intuitionistic propositional calculus is complete with respect to Kripke models, i.e.,* $\Gamma \vdash \varphi$ *is provable iff for all Kripke models* $\mathcal{C}$*, the condition* $\mathcal{C} \Vdash \Gamma$ *implies* $\mathcal{C} \Vdash \varphi$.

Note that this requires a proof (right-to-left implication)!

Conservativity over the implicational fragment:

2.6.2. THEOREM. *Let* φ *be an implicational formula, and let* Γ *be a set of implicational formulas. If* $\Gamma \vdash \varphi$ *can be derived in the intuitionistic propositional calculus then it can be derived in the implicational fragment.*

Heyting algebra

- *Wir können nicht die Wahrheitssemsemantik oder die Boolsche Semantik auf die intuitionistische Logik übertragen. Es gibt keine endliche Warhheitssemantik (siehe Folie 9).*

The best we can assert about $-a$ is that it is *the greatest element such that* $-a \cap a = 0$, and we can call it a *pseudo-complement*. Since negation is a special kind of implication, the above calls for a generalization. An element c is called a *relative pseudo-complement* of a with respect to b, iff c is the greatest element such that $a \cap c \leq b$. The relative pseudo-complement, if it exists, is denoted $a \Rightarrow b$.

Heyting algebra

2.4.1. DEFINITION. A *Heyting algebra* is an algebraic system of the form $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$, that satisfies the following conditions:

- $\cup, \cap$ are associative and commutative;
- $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$ and $(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$;
- $a \cup 0 = a$ and $a \cap 1 = a$;
- $a \cup a = a$;
- $a \cap c \leq b$ is equivalent to $c \leq a \Rightarrow b$ (where $a \leq b$ stands for $a \cup b = b$);
- $-a = a \Rightarrow 0$.

2.4.4. DEFINITION. Let $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ be a Heyting algebra.

(i) A *valuation* v in a $\mathcal{H}$ is a map $v : PV \to H$.

(ii) Given a valuation v in $\mathcal{H}$, define the map $[\![\bullet]\!]_v : \Phi \to H$ by:

$$\begin{array}{lcll} [\![p]\!]_v & = & v(p) & \text{for } p \in PV \\ [\![\bot]\!]_v & = & 0 & \\ [\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \cup [\![\psi]\!]_v & \\ [\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \cap [\![\psi]\!]_v & \\ [\![\varphi \to \psi]\!]_v & = & [\![\varphi]\!]_v \Rightarrow [\![\psi]\!]_v & \end{array}$$

As usual, we write $v(\varphi)$ for $[\![\varphi]\!]_v$.

2.4.5. NOTATION. Let $\mathcal{H} = \langle H, \cup, \cap, \Rightarrow, -, 0, 1\rangle$ be a Heyting algebra. We write:

- $\mathcal{H}, v \models \varphi$, whenever $v(\varphi) = 1$;
- $\mathcal{H} \models \varphi$, whenever $\mathcal{H}, v \models \varphi$, for all v;
- $\mathcal{H}, v \models \Gamma$, whenever $\mathcal{H}, v \models \varphi$, for all $\varphi \in \Gamma$;
- $\mathcal{H} \models \Gamma$, whenever $\mathcal{H}, v \models \Gamma$, for all v;
- $\models \varphi$, whenever $\mathcal{H}, v \models \varphi$, for all H, v;
- $\Gamma \models \varphi$, whenever $\mathcal{H}, v \models \Gamma$ implies $\mathcal{H}, v \models \varphi$, for all H and v.

2.4.6. THEOREM (Soundness and Completeness). *The following conditions are equivalent*

1. $\Gamma \vdash \varphi$;
2. $\Gamma \models \varphi$.

2.4.2. Definition.

- The symbol $\varrho(a, b)$ denotes the distance between points $a, b \in \mathbb{R}^2$;
- A subset A of $\mathbb{R}^2$ is *open* iff for every $a \in A$ there is an $r > 0$ with $\{b \in \mathbb{R}^2 : \varrho(a, b) < r\} \subseteq A$;
- If A is a subset of $\mathbb{R}^2$ then $\mathrm{Int}(A)$ denotes the *interior* of A, i.e., the union of all open subsets of A.

2.4.3. Proposition. *Let* $\mathcal{H} = \langle \mathcal{O}(\mathbb{R}^2), \cup, \cap, \Rightarrow, \sim, 0, 1 \rangle$, *where*

- $\mathcal{O}(\mathbb{R}^2)$ *is the family of all open subsets of* $\mathbb{R}^2$;
- *the operations* $\cap$, $\cup$ *are set-theoretic;*
- $A \Rightarrow B := \mathrm{Int}(-A \cup B)$, *for arbitrary open sets* A *and* B;
- $0 = \{\}$ *and* $1 = \mathbb{R}^2$.
- $\sim A = \mathrm{Int}(-A)$, *where* $-$ *is the set-theoretic complement.*

Then $\mathcal{H}$ *is a Heyting algebra.*

2.4.11. THEOREM. *Let $\mathcal{H}$ be the algebra of all open subsets of*

- *the set $\mathbb{R}$ of reals, or*
- *the set $\mathbb{Q}$ of rationals, or*
- *any Cartesian product of the above, in particular $\mathbb{R}^2$.*

Then $\mathcal{H} \models \varphi$ iff φ is valid.

Übung II

2.4.7. EXAMPLE. To see that Peirce's law $((p \to q) \to p) \to p$ is not intuitionistically valid, consider the algebra of open subsets of $\mathbb{R}^2$. Take $v(p)$ to be the whole space without one point, and $v(q) = \{\}$. (Note that $a \Rightarrow b = 1$ in a Heyting algebra iff $a \leq b$.)

- **Übung:** Beweisen Sie mittels einer Heyting Algebra, dass Pierce‘s Formel nicht intuitionistisch gültig ist.

- **Übung:** Beweisen Sie mittelse einer Heyting Algebra, dass p v –p nicht intuitionistisch gültig ist.