E. Clarke & B.-H. Schlingloff: Model Checking Chapters 6,7 (p. 1689–1711)

Completeness & Decision Procedures

Petteri Kaski

Logic = syntax + semantics

▷ Syntax

\[ \text{ML} \overset{\text{def}}{=} \mathcal{P} \upharpoonright \bot \upharpoonright (\text{ML} \to \text{ML}) \upharpoonright (R)\text{ML} \]

▷ Semantics via Kripke models and frames:

- (Truth in a model) \( M \models \phi \) \( M = (U, I, w_0) \);
- (Validity in a frame) \( \mathcal{F} \models \phi \) \( \mathcal{F} = (U, I) \);
- (Universal validity) \( \models \phi \) \( \mathcal{F} \models \phi \) for all frames \( \mathcal{F} \).

“Completeness” and “Decision procedures”

▷ A logic is complete if it has a proof system that is both sound and complete.

▷ A proof system is a “syntactic” method for establishing semantic consequence, e.g.,

“if \( p \) and \( p \to q \) are true, then \( q \) must be true.”

In other words, \( q \) is a semantic consequence of \( \{p, (p \to q)\} \).

▷ A decision procedure is an algorithm that determines whether a sentence \( \phi \) is a semantic consequence of a set of sentences \( \Phi \).

▷ Not all complete logics are decidable, that is, have a decision procedure.

Global semantic consequence

▷ Let \( \mathcal{L} \) be a logic (e.g. ML, CTL, LTL) whose semantics are defined via Kripke models.

▷ Let \( \Phi \subseteq \mathcal{L} \) be a set of sentences and suppose \( \phi \in \mathcal{L} \) is a sentence.

▷ \( \phi \) is a (global) semantic consequence of \( \Phi \) if

\[ \mathcal{F} \models \Phi \text{ implies } \mathcal{F} \models \phi \text{ for every frame } \mathcal{F}. \]

We indicate this by writing \( \Phi \models \phi \) (or \( \models \phi \) if \( \Phi \) is empty).

▷ \( \{p, (p \to q)\} \models q \)

▷ \( \{p\} \models [R]p \)

▷ \( \{(p \to \Box^n q) : n \in \mathbb{N}\} \models (p \to \Box^* q) \)
Proof systems

▷ A proof system $P$ for a logic $L$ is a syntactic method for deciding semantic consequence.

▷ We write $\Phi \vdash \phi$ if we can prove $\phi$ from the premises $\Phi$ (using a proof system $P$).

▷ A proof system need not in general be connected with the semantics of the logic.

▷ A proof system is sound if $\Phi \vdash \phi$ implies $\Phi \models \phi$.
  “Everything provable from $\Phi$ is a semantic consequence of $\Phi$.”

▷ A proof system is complete if $\Phi \models \phi$ implies $\Phi \vdash \phi$.
  “Every semantic consequence of $\Phi$ has a proof from $\Phi$.”

Deductive proof systems

▷ A deductive proof system for a logic $L$ consists of a set of axioms and a set of deductive rules.

  * An axiom is simply a sentence $\phi \in L$.
  * A deductive rule is a pair $(\{\phi_1, \ldots, \phi_N\}, \psi)$, written
    $$\phi_1, \ldots, \phi_N \vdash \psi,$$
  where $\phi_1, \ldots, \phi_N \in L$ are the prerequisites and $\psi$ is the conclusion. (The number of prerequisites is always finite.)

Provability in deductive proof systems

▷ Fix any deductive proof system $P$ for $L$.

▷ A finite sequence $\phi_1, \ldots, \phi_N \in L$ is a derivation of $\phi \in L$ from the premises $\Phi \subseteq L$ if $\phi = \phi_N$ and, for every $i = 1, \ldots, N$,
  1. either $\phi_i$ is an axiom; or
  2. $\phi_i$ is a premise (i.e. $\phi_i \in \Phi$); or
  3. $\phi_i$ is the conclusion of a deductive rule $\psi_1, \ldots, \psi_M \vdash \phi_i$, and $\psi_1, \ldots, \psi_M$ appear earlier in the derivation.

▷ We say that $\phi$ is provable from $\Phi$ (notation $\Phi \vdash \phi$) if there exists a derivation of $\phi$ from $\Phi$.

Trivial examples of deductive proof systems

▷ Consider the multimodal logic $ML$.
  1. Take all sentences in $ML$ as axioms.
  2. Assume the axiom set is empty.

▷ Recall that
  * a proof system is sound if $\Phi \vdash \phi$ implies $\Phi \models \phi$.
  * a proof system is complete if $\Phi \models \phi$ implies $\Phi \vdash \phi$.

▷ Is either of the “trivial” proof systems above sound?

▷ What about complete?
A sound and complete proof system for ML

(T)  (Propositional tautologies)
(K)  ([R] (p → q) → ([R]p → [R]q))
(MP) p, (p → q) ⊢ q
(N)  p ⊢ [R]p

▷ (T) and (K) are axioms.
▷ (MP) and (N) are deductive rules.
▷ Arbitrary (but systematic) substitution of ML sentences in place of atomic propositions is allowed to occur.

Theorem. The deductive proof system for ML is sound.
Proof sketch.
▷ Let φ₁, ..., φₘ be a derivation of φₘ from the premises Φ.
▷ Let F = (U, I) be any frame for which F ⊨ Φ.
▷ Proceed by induction: if F ⊨ φⱼ for all j = 1, ..., i, conclude that F ⊨ φᵢ₊₁. Then F ⊨ φₘ holds eventually.
▷ Example: The (N) rule. Suppose that φᵢ₊₁ = [R]φⱼ, where j ≤ i. By induction hypothesis F ⊨ φⱼ. Fix any w ∈ U and consider any w' such that (w, w') ∈ I(R). Since F ⊨ φⱼ, we have (U, I, w') ⊨ φⱼ. So, (U, I, w) ⊨ [R]φⱼ because w' was arbitrary. Because w was arbitrary, F ⊨ [R]φⱼ.

Soundness

An example derivation

Let φ, ψ be arbitrary ML sentences and suppose Φ = {⟨φ → ψ⟩}. We derive ([R]φ → [R]ψ) as follows:
1. φ → ψ  (GP)
2. [R] (φ → ψ)  (1,N)
3. ([R] (φ → ψ) → ([R]φ → [R]ψ))  (K)
4. ([R]φ → [R]ψ)  (2,3,MP)

So, {⟨φ → ψ⟩} ⊨ ([R]φ → [R]ψ).

Completeness

Theorem. The deductive proof system for ML is complete.
Proof sketch.
▷ We prove the contrapositive claim Φ ∤ φ implies Φ ∤ φ.
▷ The aim is to construct a canonical frame F₀ = (U, I) that satisfies F₀ ⊨ Φ, but for which there exists a w ∈ U such that (U, I, w) ⊭ φ
▷ Then F₀ is the counterexample that demonstrates Φ ∤ φ.
▷ The construction is based on a syntactic notion of consistency with the premises Φ.
▷ A set Ψ ⊆ ML is consistent (with Φ) if there exists no finite subset {ψ₁, ..., ψₙ} ⊆ Ψ such that Φ ⊨ ¬(ψ₁ ∧ ... ∧ ψₙ).
A consistent set $\Psi$ is maximal if no proper extension $\Psi' \supset \Psi$ of $\Psi$ is consistent.

Lemma (Lindenbaum). Every consistent set $\Psi \subseteq \text{ML}$ can be extended to a maximal consistent set.

Lemma. Let $\Psi \subseteq \text{ML}$ be a maximal consistent set. Then $\Phi \subseteq \Psi$ and, for every $\psi \in \text{ML}$, either $\psi \in \Psi$ or $\neg \psi \in \Psi$, but not both.

Define

$U \overset{\text{def}}{=} \{\Psi \subseteq \text{ML} : \Psi \text{ is consistent and maximal}\},$

$I(R) \overset{\text{def}}{=} \{(\Psi_0, \Psi_1) \in U \times U : \Psi_0^{[R]} \subseteq \Psi_1\},$

$I(p) \overset{\text{def}}{=} \{\Psi \in U : p \in \Psi\},$

where $\Psi^{[R]} \overset{\text{def}}{=} \{\psi : [R]\psi \in \Psi\}.$

**Consequences of the completeness proof**

For any premise set $\Phi \subseteq \text{ML}$ there exists a canonical frame $F_\Phi = (U, I)$ that has the following property:

$\Phi \not\vdash \phi$ if and only if $\exists \Psi \in U$ such that $(U, I, \Psi) \not\models \phi.$

$\Rightarrow$ $\Phi \not\vdash \phi$ implies $\Phi \not\vdash \phi$ by the soundness theorem, so $\Psi$ exists.

$\Leftarrow$ Clear since $F_\Phi \models \Phi$ by construction.

So, it suffices to consider only the canonical frame $F_\Phi$ to determine whether $\Phi \vdash \phi$.

Unfortunately, the canonical frame is uncountably infinite, and the problem of determining whether $\Phi \vdash \phi$ for arbitrary $\Phi, \phi$ is undecidable.

For finite $\Phi$ the problem becomes decidable. (More on this later.)

**Lemma (Truth).** For every $\psi \in \text{ML}$ and every $\Psi \subseteq U$, we have $\psi \in \Psi$ if and only if $\Psi \models \psi$.

So, since $\Phi \subseteq \Psi$ for every $\Psi \in U$, we have $F_\Phi \models \Phi$.

Recall that we assume $\Phi \not\vdash \phi$.

So, $\{\neg \phi\}$ must be consistent. (Otherwise $\Phi \vdash \neg (\neg \phi)$, i.e., $\Phi \vdash \phi$.)

Let $\Psi_0 \in U$ be any maximal consistent extension of $\{\neg \phi\}$.

Then, since $\neg \phi \in \Psi_0$, we have $\phi \notin \Psi_0$.

Consequently $(U, I, \Psi_0) \not\models \phi$ and hence $F_\Phi \not\models \phi$.

**Monomodal logic with transitive closure.**

Syntax

$\text{ML}^+_1 \overset{\text{def}}{=} \mathcal{P} \mid \perp \mid (\text{ML}^+_1 \rightarrow \text{ML}^+_1) \mid \text{X} \text{ML}^+_1 \mid \text{F}^* \text{ML}^+_1$

Semantics via (restricted) Kripke models and frames.

$X \phi \overset{\text{def}}{=} (\mathcal{X}) \phi$, $F^* \phi \overset{\text{def}}{=} (\phi \lor (\mathcal{X}) \phi)$.

Restriction on models and frames:

$I(\mathcal{X}) = I(\mathcal{X})^+,$

where $I(\mathcal{X})^+$ denotes the transitive closure of $I(\mathcal{X})$.

Syntactic abbreviations:

$\mathcal{N} \phi \overset{\text{def}}{=} \neg X \neg \phi$, $G^* \phi \overset{\text{def}}{=} \neg F^* \neg \phi.$
A sound and (weakly) complete proof system for $\text{ML}^+_1$

(T) (Propositional tautologies)
(K) $(\mathfrak{N}(p \rightarrow q) \rightarrow (\mathfrak{N}p \rightarrow \mathfrak{N}q))$
(Rec) $G^*p \rightarrow (p \land \mathfrak{N}G^*p)$
(MP) $p, (p \rightarrow q) \vdash q$
(N) $p \vdash \mathfrak{N}p$
(Ind) $(p \rightarrow (q \land \mathfrak{N}p)) \vdash (p \rightarrow G^*q)$

▷ (T), (K) and (Rec) are axioms.
▷ (MP), (N) and (Ind) are deductive rules.
▷ Arbitrary (but systematic) substitution of $\text{ML}^+_1$ sentences in place of atomic propositions is allowed to occur.

Let $\phi$ be an arbitrary $\text{ML}^+_1$ sentence and suppose that $\Phi = \{\phi\}$. We derive $G^*\phi$ as follows:

1. $\phi$ (GP)
2. $\mathfrak{N}\phi$ (1,N)
3. $(\phi \rightarrow (\mathfrak{N}\phi \rightarrow (\phi \rightarrow (\phi \land \mathfrak{N}\phi))))$ (T)
4. $(\mathfrak{N}\phi \rightarrow (\phi \rightarrow (\phi \land \mathfrak{N}\phi)))$ (1.3,MP)
5. $(\phi \rightarrow (\phi \land \mathfrak{N}\phi))$ (2,4,MP)
6. $\phi \rightarrow G^*\phi$ (5,Ind)
7. $G^*\phi$ (1,6,MP)

$\text{ML}^+_1$ is noncompact

▷ Let $\Phi = \{(p \rightarrow \mathfrak{N}^nq) : n \in \mathbb{N}\}$ and $\phi = (p \rightarrow G^*q)$.
▷ Now $\Phi \vdash \phi$, but for every finite $\Phi' \subset \Phi$ it holds that $\Phi' \not\vdash \phi$.
▷ Consider any deductive proof system for $\text{ML}^+_1$ that is sound.
▷ Derivations are finite sequences that in particular use a finite number of premises. Consequently, if $\Phi \vdash \phi$, then there exists a finite $\Phi' \subset \Phi$ such that $\Phi' \vdash \phi$.
▷ Since the proof system is sound, $\Phi' \not\vdash \phi$, a contradiction.
▷ So, $\Phi \not\vdash \phi$.

$\text{ML}^+_1$ admits no deductive proof system that is both sound and complete.

▷ The notion of completeness has to be relaxed.

**Definition.** A deductive proof system is *weakly complete* if $\Phi \vdash \phi$ implies $\Phi \vdash \phi$ whenever $\Phi$ is finite.

**Theorem (Deduction).** Let $\psi, \phi \in \text{ML}^+_1$. Then, $\psi \vdash \phi$ if and only if $\vdash G^*\psi \rightarrow \phi$.

**Proposition.** A deductive proof system for $\text{ML}^+_1$ is weakly complete if and only if $\vdash \phi$ implies $\vdash \phi$. 

petteri.kanki@hut.fi
Theorem. The $ML^+_1$ proof system is weakly complete.

Proof sketch.

\( \Rightarrow \) We again prove the contrapositive claim \( \not \vdash \phi \) implies \( \not \vdash \phi \).

\( \Rightarrow \) It suffices to construct a model \( \mathcal{M} = (U, \mathcal{I}, w) \) such that \( \mathcal{M} \not \models \phi \).

\( \Rightarrow \) The model is again based on syntactic consistency.

\( \Rightarrow \) A set \( \Psi \subseteq ML^+_1 \) is consistent if there exists no finite subset \( \{\psi_1, \ldots, \psi_n\} \subseteq \Psi \) such that \( \vdash \neg(\psi_1 \land \cdots \land \psi_n) \).

Define

\[
U \overset{\text{def}}{=} \{ \Psi \subseteq \text{ESF}(\phi) \cup \neg \text{ESF}(\phi) : \Psi \text{ is consistent and maximal} \}, \\
\mathcal{I}(\neg) \overset{\text{def}}{=} \{ (\Psi_0, \Psi_1) \in U \times U : \Psi_0^X \subseteq \Psi_1 \}, \\
\mathcal{I}(p) \overset{\text{def}}{=} \{ \Psi \in U : p \in \Psi \},
\]

where \( \Psi^X \overset{\text{def}}{=} \{ \neg \psi : -X\psi \in \Psi \} \).

\( \Rightarrow \) Lemma (Truth). For every \( \psi \in \text{ESF}(\phi) \) and every \( \Psi \in U \), we have \( \psi \in \Psi \) if and only if \( \Psi \models \psi \).

\( \Rightarrow \) Recall that we assume \( \vdash \phi \).

\( \Rightarrow \) So, \( \{\neg\} \subseteq \text{ESF}(\phi) \) must be consistent.

\( \Rightarrow \) Let \( \Psi_0 \in U \) be any maximal consistent extension of \( \{\neg\} \).

\( \Rightarrow \) Then, since \( \neg \phi \in \Psi_0 \), we have \( (U, \mathcal{I}, \Psi_0) \not \models \phi \).

\( \Rightarrow \) Let \( \phi \in ML^+_1 \). The set of extended subformulas of \( \phi \), denoted \( \text{ESF}(\phi) \), is the minimal set of formulas that satisfies

1. \( \phi \in \text{ESF}(\phi) \).
2. If \( (\psi_1 \rightarrow \psi_2) \in \text{ESF}(\phi) \), then \( \psi_1 \in \text{ESF}(\phi) \) and \( \psi_2 \in \text{ESF}(\phi) \).
3. If \( X\psi \in \text{ESF}(\phi) \), then \( \psi \in \text{ESF}(\phi) \).
4. If \( F^*\psi \in \text{ESF}(\phi) \), then \( \psi \in \text{ESF}(\phi) \) and \( X F^*\psi \in \text{ESF}(\phi) \).

\( \Rightarrow \) The set \( \text{ESF}(\phi) \) is finite for every \( \phi \in ML^+_1 \).

\( \Rightarrow \) A consistent set \( \Psi \subseteq \text{ESF}(\phi) \cup \neg \text{ESF}(\phi) \) is maximal if either \( \psi \in \Psi \) or \( \neg \psi \in \Psi \) for every \( \psi \in \text{ESF}(\phi) \).

\( \Rightarrow \) Lemma. Every consistent set \( \Psi \subseteq \text{ESF}(\phi) \cup \neg \text{ESF}(\phi) \) can be extended to a maximal consistent set.

Consequences of the completeness proof

\( \Rightarrow \) Let \( \phi \in ML^+_1 \). Then, \( \not \vdash \phi \) if and only if \( \exists \) finite \( (U, \mathcal{I}, w) \) such that \( (U, \mathcal{I}, w) \not \models \phi \).

\( \Rightarrow \) \( \not \vdash \phi \) implies \( \not \vdash \phi \) by the soundness theorem, so \( (U, \mathcal{I}, w) \) exists.

\( \Rightarrow \) \( \not \vdash \phi \) implies \( \not \vdash \phi \).

\( \Rightarrow \) The size of the finite model is bounded by \( |U| \leq 2^{|\text{ESF}(\phi)|} \).

\( \Rightarrow \) The problem of determining whether \( \vdash \phi \) is decidable:

Exhaustively search through all models of size \( \leq 2^{|\text{ESF}(\phi)|} \).
Other logics

- Sound and (weakly) complete deductive proof systems exist for
  - CTL, LTL with/without past operators.
  - LTL with natural models.
  - qTL, μTL.

Decision procedures

> A decision procedure for a logic \( L \) is an algorithm that determines for a finite \( \Phi \subseteq L \) and a \( \phi \in L \) whether \( \Phi \models \phi \).

> In practice, the algorithms determine satisfiability.

- \( \Phi \) is satisfiable subject to premises \( \Phi \) if there exists a frame \( \mathcal{F} = (U, \mathcal{I}) \) and a state \( w \in U \) such that \( \mathcal{F} \models \Phi \) and \( (U, \mathcal{I}, w) \models \phi \).

> \( \Phi \models \phi \) if and only if \( \neg \phi \) is unsatisfiable subject to \( \Phi \).

ML decision procedure (1/3)

> Let \( \Phi \subseteq ML \) be finite and let \( \phi \in ML \).

> Denote by \( SF \) the set of all subformulas of the formulas in \( \Phi \cup \{ \phi \} \).

> A subset \( w \subseteq SF \) is propositionally consistent if
  1. \( \bot \not\in w \); and
  2. if \( (\psi_1 \rightarrow \psi_2) \in SF \), then
     \( (\psi_1 \rightarrow \psi_2) \in w \) if and only if \( \psi_1 \not\in w \) or \( \psi_2 \in w \).
  3. if \( \neg \psi \in SF \), then \( \neg \psi \in w \) if and only if \( \psi \not\in w \).
  4. if \( (\psi_1 \lor \psi_2) \in SF \), then
     \( (\psi_1 \lor \psi_2) \in w \) if and only if \( \psi_1 \in w \) or \( \psi_2 \in w \).
  5. if \( (\psi_1 \land \psi_2) \in SF \), then
     \( (\psi_1 \land \psi_2) \in w \) if and only if \( \psi_1 \in w \) and \( \psi_2 \in w \).

ML decision procedure (2/3)

> Take as \( U \) the set of all \( w \subseteq SF \) that satisfy
  1. \( w \supseteq \Phi \); and
  2. \( w \) is propositionally consistent.

> Take \( I(R) = U \times U \). (Only \( R \in R \) that appear in \( SF \) need to be considered.)

> Now remove repeatedly bad points and bad arcs until none exist.

> If \( U \) contains a state \( w \) with \( \phi \in w \), then output "satisfiable";
  otherwise output "unsatisfiable."
**ML decision procedure (3/3)**

- **Bad arcs and points are defined as follows:**
  * An arc \((w, w') \in \mathcal{I}(R)\) is bad if \(\langle R \rangle \psi \notin w \) but \(\psi \in w'\).
  * A point \(w \in U\) is bad if \(\langle R \rangle \psi \in w\) but \(\psi \notin w'\) for all \(w' \in U\) such that \((w, w') \in \mathcal{I}(R)\).

- **The above procedure is a sound and weakly complete proof system for ML.**
  * For finite \(\Phi\), let \(\Phi \vdash \phi\) if and only if the procedure outputs "unsatisfiable" on input \(\Phi, \neg \phi\).
  * For finite \(\Phi\), \(\Phi \vdash \phi\) if and only if \(\Phi \vdash \phi\).

---

**ML\(\_\) decision procedure (2/2)**

- **Recall ML\(\_\) axiom**
  \[
  (G^* q \rightarrow (q \land \neg G^* q)) \quad \rightarrow \quad ((q \lor X F^* q) \rightarrow F^* q)
  \]

- **A point \(w \in U\) is bad if**
  1. \(X \psi \in w\) but \(\psi \notin w'\) for all \(w' \in U\) such that \((w, w') \in \mathcal{I}(\sim)\); or
  2. \(F^* \psi \notin w\) but \(\psi \in w\); or
  3. \(F^* \psi \in w\) but \(\psi \notin w\) and no point reachable from \(w\) contains \(\psi\).

- **An arc \((w, w') \in \mathcal{I}(\sim)\) is bad if**
  1. \(X \psi \notin w\) but \(\psi \in w'\); or
  2. \(F^* \psi \notin w\) but \(F^* \psi \in w'\).

---

**Efficiency and implementation**

- **The number of propositionally consistent sets that contain \(\Phi\) in general exponential (in \(|\mathcal{S}|\)).**
- **The ML and ML\(\_\) decision algorithms require worst case exponential time.**
- **A large number of propositionally consistent sets need to be stored.**
- **Either bottom-up or top-down construction possible**
  * top-down: remove states and arcs until a satisfying model is reached.
  * bottom-up: add states and arcs until a satisfying model is reached. (Problem: what to add \(\Rightarrow\) backtracking)
- **Bottom-up more suitable for linear time (and natural models).**
Satisfiability algorithms for natural models

▷ Natural model: \( ((w_0, w_1, \ldots), I, w_0) \), where \( w_i \sim w_{i+1} \) for all \( i \).

▷ Deterministic monomodal logic.
  * One modal operator (e.g. \( \Box \)).
  * Each state has at most one successor.

▷ Satisfiability of \( \phi \) subject to \( \Phi \) and linear models:
  * Construct \( w_0, w_1, \ldots \) step by step using backtracking search.
  * Initial state \( w_0 \):
    Consider all prop. consistent \( w_0 \subseteq SF \) with \( \Phi \subseteq w_0 \) and \( \phi \in w_0 \).
  * Search step \( i \sim i + 1 \):
    Given \( w_i \subseteq SF \) as input, attempt to construct a successor \( w_{i+1} \subseteq SF \) so that all future obligations are fulfilled.

Obligations in constructing \( w_{i+1} \)

1. Positive future obligations: \( \psi \in w_{i+1} \) for all sentences \( X\psi \in w_i \).
2. Negative future obligations: \( \psi \notin w_{i+1} \) for all sentences \( \neg X\psi \in w_i \).
3. Premises: \( \Phi \subseteq w_{i+1} \).
4. Consistency: \( w_{i+1} \) must be propositionally consistent.

Termination

▷ No positive obligations \( \Rightarrow \) the sequence \( (w_0, \ldots, w_i) \) is a model.
▷ \( w_{i+1} \) is identical to a \( w_j \) constructed earlier \( \Rightarrow \) the sequence \( (w_0, \ldots, w_{j-1}) \circ (w_j, \ldots, w_i) \) is a model.
▷ Finite number of \( w \subseteq SF \) \( \Rightarrow \) algorithm always terminates.