MIT
Aero-Astro Department

Academic year 2004/2005

Course 16.399 « Abstract Interpretation »

P. Cousot

Final exam of Monday, May 15, 2005, 9:00–12:00

The exam is composed of questions than can be answered in any order (assuming the results of previous questions if necessary). If a question is ambiguous or imprecise, it is then part of that question to solve the ambiguity or imprecision. The difficulty of each question is roughly estimated by a number of stars, from one for the easiest questions to three for the most difficult ones. Documents and computers are accepted.

1. LTL model-checking

Model-checking consists in verifying that a transition system (or Kripke structure) is a model of a temporal logic formula (LTL, CTL, CTL*, etc). It is easily shown, thanks to the following questions, that this is an abstract interpretation [1].

1.1 Models

A model or transition system or Kripke structure is a quadruple $M = \langle \Sigma, I, t, L\rangle$ where Σ is a set of states, $I \subseteq \Sigma$ is a set of initial states, $t \subseteq \Sigma \times \Sigma$ is a transition relation between a state and its possible successors and $L \in \Sigma \mapsto \wp(AP)$ is a labeling of states by a set of atomic predicates chosen in a given set AP (with the interpretation that $p \in L(s)$ if and only if predicate p holds in state s). The model is *finite* when Σ and AP are finite.

We assume, as usual in model checking, that t is *total* so that any state has at least one possible successor, formally $\forall s \in \Sigma : \exists s' \in \Sigma : \langle s, s'\rangle \in t$.

1.2 Paths

Let $\pi = \pi_0\pi_1 \ldots\pi_n \ldots \in \Sigma^\omega$ be a *path* (or trace or trajectory), that is an infinite sequence $\pi \in \omega \mapsto \Sigma$ of states π_n, $n \geq 0$ in Σ. We write $\pi^k = \pi_k\pi_{k+1}\ldots\pi_n\ldots$ for the *suffix of* π *at rank* k. In particular $\pi^0 = \pi$ and $\pi^1 = \pi_1\pi_2\ldots\pi_n\ldots$. We write t^ω for the *set of paths* of t, that is to say:

$$t^\omega \quad = \quad \{\pi \in \Sigma^\omega \mid \forall i \geq 0 : \langle \pi_i, \pi_{i+1}\rangle \in t\}$$

We write $\mathrm{lfp}^{\sqsubseteq} f$ (respectively $\mathrm{gfp}^{\sqsubseteq} f$) for the least (resp. the greatest) fixpoint of f for the partial order $\sqsubseteq$, if any.

Question 1.1 *($\star$) Given a model $M = \langle \Sigma, I, t, L\rangle$, characterize t^ω as a fixpoint.*

1.3 LTL (syntax and semantics)

The formulæ f of Amir Pnueli's temporal logic LTL [3] are given as follows:

$$\begin{array}{rcl} p & \in & AP \\ f & ::= & p \mid \neg f \mid f_1 \vee f_2 \mid \mathbf{X} f \mid f_1 \,\mathbf{U}\, f_2 \mid \mathbf{G} f \end{array}$$

We define the semantics of LTL as the subset of paths of Σ^ω for which a formula f of LTL is true:

$$\begin{array}{rcl} [\![f]\!] & \in & \mathrm{LTL} \mapsto \wp(\Sigma^\omega) \\ [\![p]\!] & \triangleq & \{\pi \in \Sigma^\omega \mid p \in L(\pi_0)\} \\ [\![\neg f]\!] & \triangleq & \Sigma^\omega \setminus [\![f]\!] \\ [\![f_1 \vee f_2]\!] & \triangleq & [\![f_1]\!] \cup [\![f_2]\!] \\ [\![\mathbf{X} f]\!] & \triangleq & \{\pi \in \Sigma^\omega \mid \pi^1 \in [\![f]\!]\} \\ [\![f_1 \,\mathbf{U}\, f_2]\!] & \triangleq & \{\pi \in \Sigma^\omega \mid \exists k \geq 0 : \pi^k \in [\![f_2]\!] \wedge \forall i < k : \pi^i \in [\![f_1]\!]\} \\ [\![\mathbf{G} f]\!] & \triangleq & \{\pi \in \Sigma^\omega \mid \forall i \geq 0 : \pi^i \in [\![f]\!]\} \end{array}$$

Question 1.2 *($\star$) Prove that:*

$$\begin{array}{rcl} [\![f_1 \,\mathbf{U}\, f_2]\!] & = & \mathrm{lfp}^{\subseteq} F[\![f_1, f_2]\!] \\ \textit{where} \quad F[\![f_1, f_2]\!](X) & \triangleq & [\![f_2]\!] \cup \{\pi \in [\![f_1]\!] \mid \pi^1 \in X\} \end{array}$$

Question 1.3 *($\star\star$) Characterize $[\![\mathbf{G} f]\!]$ as a fixpoint.*

1.4 Classical semantics of LTL

The classical semantics of LTL [2] is not defined as we did in Sec. 1.3, but instead as the set of paths $\pi \in t^\omega$ of a model $M = \langle \Sigma, I, t, L \rangle$ which satisfy an LTL formula f. The classical definition is the following:

$$\begin{array}{rcl} M, \pi \models p & \triangleq & p \in L(\pi_0) \\ M, \pi \models \neg f & \triangleq & M, \pi \not\models f \\ M, \pi \models f_1 \vee f_2 & \triangleq & M, \pi \models f_1 \text{ or } M, \pi \models f_2 \\ M, \pi \models \mathbf{X} f & \triangleq & M, \pi^1 \models f \\ M, \pi \models f_1 \,\mathbf{U}\, f_2 & \triangleq & \exists k \geq 0 : M, \pi^k \models f_2 \wedge \forall i : (0 \leq i < k) \Rightarrow M, \pi^i \models f_1 \\ M, \pi \models \mathbf{G} f & \triangleq & \forall j \geq 0 : M, \pi^j \models f \end{array}$$

Question 1.4 *($\star$) Prove that for any LTL formula f and any path $\pi \in t^\omega$ of the model M $= \langle \Sigma, I, t, L \rangle$, we have:*

$$M, \pi \models f \quad \Leftrightarrow \quad \pi \in [\![f]\!] \ .$$

1.5 Abstraction

Given a model $M = \langle \Sigma, I, t, L \rangle$, we consider the abstraction:

$$\begin{array}{rcl} \alpha_M & \in & \wp(\Sigma^\omega) \mapsto \wp(\Sigma) \\ \alpha_M(X) & \triangleq & \{\pi_0 \mid \pi \in X \cap t^\omega\} \end{array}$$

Question 1.5 *(⋆) Prove that α_M is a surjective Galois connection:*

$$\langle \wp(\Sigma^\omega), \subseteq \rangle \underset{\alpha_M}{\overset{\gamma_M}{\leftarrow\!\!\twoheadrightarrow}} \langle \wp(\Sigma), \subseteq \rangle$$

Question 1.6 *(⋆) Prove that α_M is a complete meet ($\cap$) morphism.*

1.6 Model checking

Let us define $s\pi = \pi'$ such that $\pi'_0 = s$ and $\forall i \geq 0 : \pi'_{i+1} = \pi_i$. Checking of formula f for a model $M = \langle \Sigma, I, t, L \rangle$ consists in verifying that:

— Existential verification:

$$\exists s \in I : \exists s\pi \in t^\omega : s\pi \in [\![f]\!]$$

— Universal verification:

$$\forall s \in I : \nexists \pi \in \Sigma^\omega : s\pi \in t^\omega \wedge s\pi \notin [\![f]\!]$$

The two verifications derive from one another since:

$$\begin{array}{ll} & \forall s \in I : \nexists \pi \in \Sigma^\omega : s\pi \in t^\omega \wedge s\pi \notin [\![f]\!] \\ \Leftrightarrow & \forall s \in I : \forall \pi \in \Sigma^\omega : s\pi \notin t^\omega \vee s\pi \in [\![f]\!] \\ \Leftrightarrow & \forall s \in I : \forall \pi \in \Sigma^\omega : s\pi \notin t^\omega \vee s\pi \notin [\![\neg f]\!] \\ \Leftrightarrow & \neg(\exists s \in I : \exists \pi \in \Sigma^\omega : s\pi \in t^\omega \wedge s\pi \in [\![\neg f]\!]) \end{array}$$

So we choose to study existential verification:

$$\begin{array}{ll} & \exists s \in I : \exists s\pi \in t^\omega : s\pi \in [\![f]\!] \\ \Leftrightarrow & I \cap \{s \in \Sigma \mid \exists \pi \in \Sigma^\omega : s\pi \in t^\omega \wedge s\pi \in [\![f]\!]\} \neq \emptyset \\ \Leftrightarrow & I \cap \{s \in \Sigma \mid \exists \pi \in \Sigma^\omega : s\pi \in [\![f]\!] \cap t^\omega\} \neq \emptyset \\ \Leftrightarrow & I \cap \{\pi_0 \mid \pi \in [\![f]\!] \cap t^\omega\} \neq \emptyset \\ \Leftrightarrow & I \cap \alpha_M([\![f]\!]) \neq \emptyset \end{array}$$

so that universal verification will be:

$$\begin{array}{ll} & \neg(I \cap \alpha_M([\![\neg f]\!]) \neq \emptyset) \\ \Leftrightarrow & I \cap \alpha_M([\![\neg f]\!]) = \emptyset \\ \Leftrightarrow & I \subseteq \neg\alpha_M([\![\neg f]\!]) \\ \Leftrightarrow & I \subseteq \neg\alpha_M(\neg[\![f]\!]) \end{array}$$

using the notation $\neg X \triangleq \Sigma \setminus X$.

When the model is finite (and enough time and memory resource is available, otherwise "We don't know"), one can start by computing $\alpha_M(\llbracket f \rrbracket)$ before checking that $I \cap \alpha_M(\llbracket f \rrbracket) \neq \emptyset$.

We let:

$$\mathrm{pre}[t]X \quad \triangleq \quad \{s \in \Sigma \mid \exists s' \in X : \langle s, s' \rangle \in t\} \ .$$

Existential model checking, that is essentially the computation of $\alpha_M(\llbracket f \rrbracket)$ can be done by the the following algorithm (the iterative fixpoint computation terminating under the finiteness hypothesis):

Question 1.7 *(⋆⋆) Prove by induction on the syntax of f and abstraction that:*

$$\begin{array}{rcl} \alpha_M(\llbracket p \rrbracket) & = & \{s \in \Sigma \mid p \in L(s)\} \\ \alpha_M(\llbracket \neg f \rrbracket) & = & \neg \widetilde{\alpha}_M(\llbracket f \rrbracket) \\ \alpha_M(\llbracket f_1 \vee f_2 \rrbracket) & = & \alpha_M(\llbracket f_1 \rrbracket) \cup \alpha_M(\llbracket f_2 \rrbracket) \\ \alpha_M(\llbracket \mathbf{X} f \rrbracket) & = & \mathrm{pre}[t](\alpha_M(\llbracket f \rrbracket)) \\ \alpha_M(\llbracket f_1 \, \mathbf{U} \, f_2 \rrbracket) & = & \mathrm{lfp}^{\subseteq} \, \boldsymbol{\lambda} X \boldsymbol{\cdot} \alpha_M(\llbracket f_2 \rrbracket) \cup (\alpha_M(\llbracket f_1 \rrbracket) \cap \mathrm{pre}[t](X)) \\ \alpha_M(\llbracket \mathbf{G} f \rrbracket) & = & \mathrm{gfp}^{\subseteq} \, \boldsymbol{\lambda} X \boldsymbol{\cdot} \alpha_M(\llbracket f \rrbracket) \cap \mathrm{pre}[t](X) \end{array}$$

where $\neg X \triangleq \Sigma \backslash X$ and $\widetilde{\alpha}_M(X) \triangleq \neg \alpha_M(\neg X)$ for which $\widetilde{\alpha}_M(\llbracket f \rrbracket)$ will be calculated by structural induction on f.

2. Model checking for CTL and CTL*

We now consider Allen Emerson's temporal logic CTL* [2] which syntax is the following:

p	$\in$	AP	atomic formulæ
f	$::=$	$p \mid \neg f \mid f_1 \vee f_2 \mid \mathbf{E}[\phi]$	state formulæ
ϕ	$::=$	$f \mid \neg \phi \mid \phi_1 \vee \phi_2 \mid \mathbf{X}\phi \mid \phi_1 \, \mathbf{U} \, \phi_2 \mid \mathbf{G}\phi$	path formulæ

Classically, the satisfaction relation for a CTL* formula and a model $M = \langle \Sigma, I, t, L \rangle$ is defined as follows ($s \in \Sigma$, $\pi \in \Sigma^\omega$):

$$\begin{array}{rcl} M, s \models p & \triangleq & p \in L(s) \\ M, s \models \neg f & \triangleq & M, s \not\models f \\ M, s \models f_1 \vee f_2 & \triangleq & M, s \models f_1 \text{ or } M, s \models f_2 \\ M, s \models \mathbf{E}[\phi] & \triangleq & \exists \pi \in t^\omega : s = \pi_0 \wedge M, \pi \models \phi \\ M, \pi \models f & \triangleq & M, \pi_0 \models f \\ M, \pi \models \neg \phi & \triangleq & M, \pi \not\models \phi \\ M, \pi \models \phi_1 \vee \phi_2 & \triangleq & M, \pi \models \phi_1 \text{ or } M, \pi \models \phi_2 \\ M, \pi \models \mathbf{X}\phi & \triangleq & M, \pi^1 \models \phi \\ M, \pi \models \phi_1 \, \mathbf{U} \, \phi_2 & \triangleq & \exists k \geq 0 : M, \pi^k \models \phi_2 \wedge \forall i : (0 \leq j < k) \Rightarrow M, \pi^j \models \phi_1 \\ M, \pi \models \mathbf{G}\phi & \triangleq & \forall j \geq 0 : M, \pi^j \models \phi \end{array}$$

CTL is the subset of CTL* obtained by using only $\neg$, $\vee$, $\mathbf{E}[\mathbf{X}f]$, $\mathbf{E}[f_1 \mathbf{~U~} f_2]$ and $\mathbf{E}[\mathbf{G}f]$ where f, f_1 and f_2 are state formulæ:

$$\begin{array}{rcll} p & \in & AP & \text{atomic formulæ} \\ f & ::= & p \mid \neg f \mid f_1 \vee f_2 \mid \mathbf{E}[\phi] & \text{state formulæ} \\ \phi & ::= & \mathbf{X}f \mid f_1 \mathbf{~U~} f_2 \mid \mathbf{G}f & \text{path formulæ} \end{array}$$

Question 2.1 *($\star\star\star$) Provide a structural fixpoint algorithm to verify existentially a model $M = \langle \Sigma, I, t, L \rangle$ for a state formula f of CTL:*

$$I \cap \{s \mid M, s \models f\} \neq \emptyset$$

(or else universal verification, if prefered) by abstract interpretation. The answer should be inspired by Sec. ***1.**, in particular by question* ***1.7***

Question 2.2 *($\star\star\star$) Taking inspiration from Sec.* ***2.1**, do the same for CTL*.*

References

[1] P. Cousot and R. Cousot. Temporal abstract interpretation. In *Conference Record of the Twentyseventh Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 12–25, Boston, Massachusetts, January 2000. ACM Press, New York, New York, United States.

[2] A. Emerson and Ed. Clarke. Using Branching Time Temporal Logic to Synthesize Synchronization Skeletons. Science of Computer Programming 2(3): Pages 241–266, 1982

[3] A. Pnueli. The Temporal Logic of Programs. In Proceedings of the 18th IEEE Symposium Foundations of Computer Science (FOCS 1977), pages 46-57, 1977.