Home Assignment 1: Alternation-Free μ-Calculus

To hand in before or on November 7, 2012.

	22	23	24	25	26	27	28
	29	30	31				
November				1	2	3	4
	5	6	7	8	9	10	11

Electronic versions (PDF only) can be sent by email to ⟨schmitz@lsv.ens-cachan.fr⟩, paper versions should be handed in on the 7th or put in my mailbox at LSV, ENS Cachan.

This assignment is concerned with the *μ-calculus*, which can be seen as an extension of CTL with fixed point computations. We consider the model-checking problem for the *alternation-free* fragment and show that it can be solved in linear time (in the product of the sizes of the model and of the formula).

The numbers in the margins next to exercises are indications of time and difficulty.

1 Modal μ-Calculus

1.1 Definitions and Basic Properties

Syntax. In addition to the usual set AP of atomic propositions, we also employ a countable set of variables $\mathcal{X}$. A μ-calculus formula is a term φ defined by the abstract syntax

$$\varphi ::= \top \mid p \mid x \mid \neg\varphi \mid \varphi \vee \varphi \mid \Diamond\varphi \mid \mu x.\varphi \qquad (\mu\text{-formulæ})$$

where p ranges over AP and x over $\mathcal{X}$. A formula that does not use any "$\mu x.\varphi$" operator is called a *modal formula*, while a formula of the form $\mu x.\varphi$ is called a *least fixed-point* (lfp) formula, where x is bound by the μ operator. The notions of free variables $\mathrm{FV}(\varphi)$ of φ and of closed formulæ are defined as usual. An lfp formula $\mu x.\varphi$ is well-formed if and only if x is in $\mathrm{FV}(\varphi)$ and appears only positively in φ, i.e. under the scope of an even number of negations. We only consider well-formed formulæ in the following.

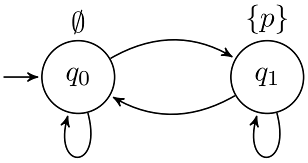
The syntax can be extended with dual operators: $\bot \overset{\text{def}}{=} \neg\top$, $\varphi \wedge \psi \overset{\text{def}}{=} \neg(\neg\varphi \vee \neg\psi)$, $\Box\varphi \overset{\text{def}}{=} \neg\Diamond\neg\varphi$, and $\nu x.\varphi \overset{\text{def}}{=} \neg(\mu x.(\neg\varphi[x/\neg x]))$ where $\neg x$ is substituted for x in φ (this ensures that x also appears positively in $\neg(\varphi[x/\neg x])$). Unsurprisingly, a μ-formula of form $\nu x.\varphi$ is called a *greatest fixed-point* (gfp) formula.

Semantics. Given a Kripke structure $\mathfrak{M} = \langle S, T, I, \mathrm{AP}, \ell\rangle$—where as in the lectures S is a set of states, $T \subseteq S \times S$ is a transition relation, $I \subseteq S$ is a set of initial states, and ℓ is a labeling function from S to 2^{AP}—and a valuation v from $\mathrm{FV}(\varphi)$ to 2^S, a μ-calculus formula φ defines a *satisfiability set* $[\![\varphi]\!]_v \subseteq S$ by induction over the structure of φ:

$$\begin{aligned}
[\![\top]\!]_v &\stackrel{\text{def}}{=} S\;,\\
[\![p]\!]_v &\stackrel{\text{def}}{=} \{s \in S \mid p \in \ell(s)\}\;,\\
[\![x]\!]_v &\stackrel{\text{def}}{=} v(x)\;,\\
[\![\neg\varphi]\!]_v &\stackrel{\text{def}}{=} S \setminus [\![\varphi]\!]_v\;,\\
[\![\varphi \vee \psi]\!]_v &\stackrel{\text{def}}{=} [\![\varphi]\!]_v \cup [\![\psi]\!]_v\;,\\
[\![\Diamond\varphi]\!]_v &\stackrel{\text{def}}{=} T^{-1}([\![\varphi]\!]_v)\;,\\
[\![\mu x.\varphi]\!]_v &\stackrel{\text{def}}{=} \bigcap\{X \subseteq S \mid X \supseteq [\![\varphi]\!]_{v[x\mapsto X]}\}\;.
\end{aligned}$$

If φ is a closed formula and s a state of a structure $\mathfrak{M}$, then $\mathfrak{M}$ *satisfies* φ in s, written $\mathfrak{M}, s \models \varphi$, if $s \in [\![\varphi]\!]$ (using the empty valuation).

Exercise 1 (Example)**.** Consider the Kripke structure below with $\mathrm{AP} \stackrel{\text{def}}{=} \{p\}$:



[2] What are the satisfiability sets of the formulæ $\Box p$, $\nu y.p \wedge \Box y$, and $\mu x.\nu y.((p \wedge \Box y) \vee \Diamond x)$? *Hint: Detail your computations: for instance, what is* $[\![\neg p \vee \Diamond y]\!]_{[y\mapsto Y]}$ *depending on* $Y \subseteq \{q_0, q_1\}$*?*

Exercise 2 (Fixed-Point Semantics)**.** Another viewpoint on the semantics is that, as both satisfiability sets of formulæ and valuations of variables ranges over 2^S, one can see the semantics of a modal formula $\varphi(x)$ with a free variable x as a function $f\colon 2^S \to 2^S$: if v is a valuation of $\mathrm{FV}(\varphi) \setminus \{x\}$, $f(X) \stackrel{\text{def}}{=} [\![\varphi]\!]_{v[x\mapsto X]}$. We focus here on a modal formula appearing inside a fixed-point formula $\mu x.\varphi(x)$ or $\nu x.\varphi(x)$, i.e. the well-formedness restriction applies.

[1] 1. Show that this function f is *monotonic* for the inclusion ordering over 2^S.

[1] 2. Justify that f has a both a least and a greatest fixed-point verifying $[\![\mu x.\varphi]\!]_v = \mathrm{lfp}\, f$ and $[\![\nu x.\varphi]\!]_v = \mathrm{gfp}\, f$. *Hint: use the Knaster-Tarski Theorem; what is the name of a set X verifying $X \supseteq f(X)$?*

[1] 3. Show that, if S is a finite set of cardinal n, then $f^n(\emptyset) = \mathrm{lfp}\, f$ and $f^n(S) = \mathrm{gfp}\, f$.

1.2 Alternation

Thanks to the dualities, any μ-formula can be put in negative normal form (nnf):

$$\varphi ::= \top \mid \bot \mid p \mid \neg p \mid x \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \Diamond\varphi \mid \Box\varphi \mid \mu x.\varphi \mid \nu x.\varphi$$

A μ-formula φ in nnf is *alternation free* if, for all lfp subformulæ $\mu x.\psi$ of φ, if $\nu y.\psi'$ is a direct (i.e. not under the scope of another binding operator) gfp subformula of ψ, then $x \notin \mathrm{FV}(\psi')$, and conversely, for all gfp subformulæ $\nu x.\psi$ of φ, if $\mu y.\psi'$ is a direct lfp subformula of ψ, then $x \notin \mathrm{FV}(\psi')$. For instance, $\mu x.(\nu y.p \wedge \Box y) \vee \Diamond x$ is alternation-free, but $\mu x.\nu y.((p \wedge \Box y) \vee \Diamond x)$ is not.

Exercise 3 (CTL)**.** We want to prove that, for any CTL formula φ, there exists an equivalent closed alternation-free μ-formula φ', where equivalence means that for any Kripke structure $\mathfrak{M}$ and state s, $\mathfrak{M}, s \models \varphi$ if and only if $\mathfrak{M}, s \models \varphi'$.

[1] 1. Show that, if $\varphi \equiv \varphi'$, then $\mathsf{EX}\,\varphi \equiv \Diamond\varphi'$.

[2] 2. Show that, if $\varphi \equiv \varphi'$, then $\mathsf{EF}\,\varphi \equiv \mu x.\varphi' \vee \Diamond x$.

[3] 3. Complete the proof.

2 Model-Checking for the Alternation-Free Fragment

Given a *total* and *finite* Kripke structure $\mathfrak{M} = \langle S, T, I, \mathrm{AP}, \ell\rangle$—totality means that $T(s) \neq \emptyset$ for all s in S—and a closed alternation-free μ-formula φ, we want to compute $[\![\varphi]\!]$ in time $O(|\mathfrak{M}| \cdot |\varphi|)$. This generalizes the linear-time algorithm seen in class for CTL.

The idea in the following exercise is to define a deduction system working over pairs (s, ψ) where s is a state of $\mathfrak{M}$ and ψ a subformula of φ, s.t. a pair (s, ψ) can be deduced in the system if and only if $\mathfrak{M}, s \models \psi$.

In order to avoid confusions, we assume that each variable x bound by a $\mu x.\varphi$ or $\nu x.\varphi$ operator is written with a subscript x_φ. This amounts to having distinct variable names for each occurrence of a μ or ν operator, and then an occurrence of a variable x_φ denotes unambiguously an occurrence of x bound by $\mu x.\varphi$. For instance, the formula $\mu x.(\mu x.p \vee \Diamond x) \vee \Diamond x$ would be rewritten as $\mu x_\varphi.(\mu x_\psi.p \vee \Diamond x_\psi) \vee \Diamond x_\varphi$ where φ denotes $(\mu x_\psi.p \vee \Diamond x_\psi) \vee \Diamond x_\varphi)$ and ψ denotes $p \vee \Diamond x_\psi$—do not let the recursivity bother you, this is just a convenient notation.

Exercise 4 (LFP of a Modal Formula)**.** We begin with a particular case of an alternation-free closed formula, where it is of the form $\mu x_\varphi.\varphi$ with φ a modal formula—i.e. without fixed point operators.

Given $\mathfrak{M}$ and φ, we construct the following deduction system $\mathfrak{D}_\mu$ over $S \times \mathrm{Sub}(\varphi)$:

$$\frac{}{(s,p)}\,p \in \ell(s) \qquad \frac{}{(s,\neg p)}\,p \notin \ell(s) \qquad (\mathrm{AP}_\mu)$$

$$\frac{(s,\varphi)}{(s,x_\varphi)} \qquad (\mathcal{X}_\mu)$$

$$\frac{(s,\psi)}{(s,\psi\vee\psi')} \qquad \frac{(s,\psi')}{(s,\psi\vee\psi')} \qquad (\vee_\mu)$$

$$\frac{(s,\psi) \quad (s,\psi')}{(s,\psi\wedge\psi')} \qquad (\wedge_\mu)$$

$$\frac{(s',\psi)}{(s,\Diamond\psi)}\,s' \in T(s) \qquad (\Diamond_\mu)$$

$$\frac{(s_1,\psi)\;(s_2,\psi)\dots(s_m,\psi)}{(s,\Box\psi)}\,\{s_1,\dots,s_m\} = T(s) \qquad (\Box_\mu)$$

[2] 1. Show that $\mathfrak{D}_\mu$ is sound, i.e. that if (s,φ) can be deduced, then $\mathfrak{M}, s \models \mu x_\varphi.\varphi$.

[2] 2. Show that $\mathfrak{D}_\mu$ is complete, i.e. that if $\mathfrak{M}, s \models \mu x_\varphi.\varphi$, then (s,φ) can be deduced.

[1] 3. Explain why $\mathfrak{D}_\mu$ can be used to compute $\llbracket \mu x_\varphi.\varphi \rrbracket_v$ in time linear in the product of the sizes of $\mathfrak{M}$ and φ. *Hint: This is a consequence of a well-known result.*

Exercise 5 (General Case)**.** Let us now turn to the full model-checking algorithm:

[2] 1. Define a sound and complete "anti-"deduction system $\mathfrak{D}_\nu$ for model-checking formulæ of the form $\nu x_\varphi.\varphi$ where φ is a modal formula: (s,φ) can be deduced in $\mathfrak{D}_\nu$ if and only if $\mathfrak{M}, s \not\models \nu x_\varphi.\varphi$.

[5] 2. Complete the proof: add rules for lfp and gfp subformulæ, and provide an algorithm in time $O(|\mathfrak{M}| \cdot |\varphi|)$ for the model-checking problem.