Home Assignment 2: Model Checking Basic Parallel Processes

To hand in before or on February 22, 2011.
The penalty for delays is 2 points per day.

February

	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28						

Electronic versions (PDF only) can be sent by email to ⟨schmitz@lsv.ens-cachan.fr⟩, paper versions should be handed in on the 22nd or put in my mailbox at LSV, ENS Cachan.

This assignment is concerned with the verification of a rather simple class of infinite-state systems with parallelism: *basic parallel processes* (BPPs). They are easily seen to be equivalent to a subclass of Petri nets (Exercise 1), but enjoy more decidable properties and lower complexities than general Petri nets.

1 Basic Parallel Processes

BPPs can be compared to context-free grammars in Greibach normal form that employ a parallel composition operator. Here is one way to define BPPs that emphasizes the resemblance:

Definition 1. Given a set $\mathcal{X}$, we note $\langle \mathcal{X}^{\otimes}, \|, 0\rangle$ the free commutative monoid built from the elements of $\mathcal{X}$ using an associative, commutative operation $\|$ with identity 0. If α is in $\mathcal{X}^{\otimes}$, then we define $\alpha^0 = 0$ and $\alpha^{i+1} = \alpha^i \| \alpha$ for all i in $\mathbb{N}$.

A *BPP* is a tuple $\mathcal{B} = \langle \Sigma, \mathcal{X}, R, Y\rangle$ where Σ is a finite set of *atomic actions*, $\mathcal{X}$ a finite set of *process variables* disjoint from Σ, $R \subseteq \mathcal{X} \times \Sigma \times \mathcal{X}^{\otimes}$ is a finite set of *transition rules* of form $X \xrightarrow{a} \alpha$ where X is a variable in $\mathcal{X}$, a an action in Σ, and α a parallel composition in $\mathcal{X}^{\otimes}$, and Y is a *leading variable* in $\mathcal{X}$.

The semantics of a BPP is captured by a (generally infinite) labeled transition system $\langle Q, \Sigma, T, I\rangle$ with $Q = \mathcal{X}^{\otimes}$ as set of states, Σ as set of actions, $I = \{Y\}$ as set of initial states, and a transition relation $T \subseteq \mathcal{X}^{\otimes} \times \Sigma \times \mathcal{X}^{\otimes}$ defined by $T = \{\beta \| X \xrightarrow{a} \beta \| \alpha \mid \beta \in \mathcal{X}^{\otimes}, X \xrightarrow{a} \alpha \in R\}$. As usual, the transition relation is lifted to $\mathcal{X}^{\otimes} \times \Sigma^* \times \mathcal{X}^{\otimes}$ by $\alpha \xrightarrow{\varepsilon} \alpha$ for all α in $\mathcal{X}^{\otimes}$ and $\alpha \xrightarrow{au} \gamma$ if there exists β in $\mathcal{X}^{\otimes}$ with $\alpha \xrightarrow{a} \beta \xrightarrow{u} \gamma$, for all α, γ in $\mathcal{X}^{\otimes}$, a in Σ, and u in Σ^*.

The *size* of a BPP is defined as the sum of the sizes of its transition rules, i.e. $|\mathcal{B}| = \sum_{X \xrightarrow{a} \alpha} |\alpha| + 3$, where the size of a parallel composition α is defined as its number of $\|$ operators, i.e. $|0| = 0$ and $|\, X_1 \| \cdots \| X_m \,| = m - 1$.

Exercise 1 (BPPs as Petri nets)**.** Recall that a marked labeled *Petri net* is a tuple $\mathcal{N} = \langle P, T, \Sigma, W, \ell, m_0 \rangle$ where P is a finite set of *places*, T a finite set of *transitions*, Σ a finite alphabet, $W : (P \times T) \cup (T \times P) \to \mathbb{N}$ the *arc weight mapping*, $\ell : T \to \Sigma$ is a *labeling morphism*, and $m_0 : P \to \mathbb{N}$ is the *initial marking*.

A transition t in T is *firable* in a marking m in $\mathbb{N}^P$ if $m(p) \geq W(p,t)$ for all $p \in P$, and results in a new marking m' defined by $m'(p) = m(p) - W(p,t) + W(t,p)$ for all p in P; we note $m \xrightarrow{t} m'$ in this case. Thus a Petri net defines a labeled transition system $\langle Q, \Sigma, T', I \rangle$ with state set $Q = \mathbb{N}^P$, action set Σ, initial state set $I = \{m_0\}$, and transition relation $T' = \{m \xrightarrow{\ell(t)} m' \in \mathbb{N}^P \times \Sigma \times \mathbb{N}^P \mid \forall p \in P,\, m(p) \geq W(p,t) \wedge m'(p) = m(p) - W(p,t) + W(t,p)\}$.

[1] 1. Show that to every BPP $\mathcal{B}$ one can associate a marked labeled Petri net $\mathcal{N}$ that defines an isomorphic labeled transition system.

[1] 2. Call a Petri net *communication-free* if the sum of the inbound weights of each transition is at most 1, i.e. if for all t in T, $\sum_{p \in P} W(p,t) \leq 1$. Show that to every communication-free marked labeled Petri net $\mathcal{N}$ one can associate a BPP $\mathcal{B}$ that defines an isomorphic labeled transition system.

2 Model-Checking

Since BPPs define in general infinite-state transition systems, CTL model-checking for BPPs cannot proceed as in the finite case, and requires special techniques. As we will see, model-checking is indeed significantly harder than for finite systems (where it is in PTIME), even for fragments of CTL.

The fragments of CTL we are going to use do not feature atomic propositions. They include instead a relativized EX modality for each action in Σ, noted $\mathsf{E}\langle a \rangle$, such that the classical EX can be expressed as $\mathsf{EX}\varphi \equiv \bigvee_{a \in \Sigma} \mathsf{E}\langle a \rangle \varphi$.

Definition 2. Let Σ be a finite set of actions. The syntax of CTL(EF, EG) is defined by

$$\varphi ::= \top \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathsf{E}\langle a \rangle \varphi \mid \mathsf{EF}\varphi \mid \mathsf{EG}\varphi \,,$$

where a ranges over Σ. By CTL(EF) (resp. CTL(EG)), we refer to the above fragment *without* the EG (resp. EF) modality.

Given a labeled transition system $\langle Q, \Sigma, T, I \rangle$ and a state q in Q, note $\mathsf{Paths}(q)$ the set of infinite paths starting in q, i.e. $\mathsf{Paths}(q) = \{q_0 q_1 \cdots \in Q^\omega \mid q_0 = q \wedge \forall i \geq 0, \exists a_i \in$

$\Sigma, q_i \xrightarrow{a_i} q_{i+1}\}$. The satisfaction relation is then defined by

$$\begin{array}{ll} q \models \top & \text{always} \\ q \models \neg\varphi & \text{iff } q \not\models \varphi \\ q \models \varphi \wedge \psi & \text{iff } (q \models \varphi) \wedge (q \models \psi) \\ q \models \mathsf{E}\langle a\rangle\varphi & \text{iff } \exists q' \in Q,\, q \xrightarrow{a} q' \wedge q' \models \varphi \\ q \models \mathsf{EF}\varphi & \text{iff } \exists q_0q_1\cdots \in \mathsf{Paths}(q), \exists i \geq 0, q_i \models \varphi \\ q \models \mathsf{EG}\varphi & \text{iff } \exists q_0q_1\cdots \in \mathsf{Paths}(q), \forall i \geq 0, q_i \models \varphi\,. \end{array}$$

Turning to BPPs, a BPP $\mathcal{B}$ *satisfies* φ, noted $\mathcal{B} \models \varphi$, if $Y \models \varphi$ holds for its implicit labeled transition system—Y being the leading variable of $\mathcal{B}$. The corresponding model-checking problem is then, given $\langle \mathcal{B}, \varphi\rangle$, to decide whether $\mathcal{B} \models \varphi$.

2.1 The EF Case

We prove in this section a PSPACE lower for the CTL(EF) model-checking problem on BPPs.[1] The proof for the lower bound consists of a reduction from QBF.

Definition 3 (QBF)**.** The QBF problem consists of deciding whether a quantified boolean formula φ without free variables evaluates to "true". More precisely, φ is defined as

$$\varphi = \exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n.\, \bigwedge_{j=1}^{m} c_j$$

where each clause c_j for $1 \leq j \leq m$ is of form

$$c_j = \ell_{j,1} \vee \ell_{j,2} \vee \ell_{j,3}$$

where each literal $\ell_{j,k}$ for $1 \leq j \leq m$ and $1 \leq k \leq 3$ is of form

$$\ell_{j,k} = x_i$$

or of form

$$\ell_{j,k} = \neg x_i$$

for some $1 \leq i \leq n$. Note that we assume an alternation on the quantifiers, without loss of generality, since one can introduce phony variables that are never used in the clauses.

Exercise 2 (Reducing QBF)**.** In order to prove PSPACE-hardness, we need to exhibit a polynomial reduction from $\langle\varphi\rangle$ to $\langle \mathcal{B}, \varphi'\rangle$ where $\mathcal{B}$ is a BPP and φ' a CTL(EF) formula, such that φ evaluates to true iff $\mathcal{B} \models \varphi'$.

For all $1 \leq i \leq n$, let $\mathsf{Cl}(i) = \{1 \leq j \leq m \mid \exists 1 \leq k \leq 3, \ell_{j,k} = x_i\}$ (resp. $\mathsf{NCl}(i) = \{1 \leq j \leq m \mid \exists 1 \leq k \leq 3, \ell_{j,k} = \neg x_i\}$) be the set of clause indices validated by setting x_i

[1] In fact, the problem is PSPACE-complete, but the proof for the upper bound is too long to be included in this assignment. Also, the problem is undecidable for general Petri nets.

to true (resp. to false). Here is a suitable BPP for the reduction: let $\mathcal{B} = \langle \Sigma, \mathcal{X}, R, Y \rangle$ where

$$\begin{aligned}
\Sigma &= \{y\} \cup \{x_i \mid 1 \leq i \leq n\} \cup \{c_j \mid 1 \leq j \leq m\} \\
\mathcal{X} &= \{Y\} \cup \{X_i \mid 1 \leq i \leq n\} \cup \{C_j \mid 1 \leq j \leq m\} \\
R &= \{X_i \xrightarrow{x_i} \|_{j \in \mathsf{Cl}(i)} C_j,\ X_i \xrightarrow{x_i} \|_{j \in \mathsf{NCl}(i)} C_j \mid 1 \leq i \leq n\} \\
&\quad \cup \{C_j \xrightarrow{c_j} C_j \mid 1 \leq j \leq m\} \\
&\quad \cup \{Y \xrightarrow{y} \|_{1 \leq i \leq n} X_i\} \ .
\end{aligned}$$

[3] 1. Provide a CTL(EF) formula φ' s.t. φ is valid iff $\mathcal{B} \models \varphi'$ (prove the equivalence!).

[1] 2. Deduce that the CTL(EF) model checking problem for BPPs is PSPACE-hard.

2.2 The EG Case

Our goal in this section is to prove that model-checking for the EG fragment is undecidable for BPPs. The proof consists of a reduction from the halting problem of Minsky machines.

Definition 4 (Minsky Machines)**.** A *2-counter Minsky machine* is a tuple $\mathcal{M} = \langle Q, C, \delta, q_0, q_f \rangle$ where Q is a finite set of states with distinguished initial state q_0 and halting state q_f, $C = \{1, 2\}$ are two counter indices, and $\delta : Q \backslash \{q_f\} \to (C \times Q) \cup (C \times Q^2)$ is a state labeling function that associates to each state q except q_f a unique transition instruction. If j is in $\{1, 2\}$, let $\bar{j} = 3 - j$.

The *run* of a 2-counter Minsky machine is the infinite sequence $((q_i, c_{i,1}, c_{i,2}))_{i \geq 0}$ of configurations in $Q \times \mathbb{N}^2$ holding the current state and the current values of the two counters, where $(q_0, c_{0,1}, c_{0,2}) = (q_0, 0, 0)$, and respecting the transition instructions for all $i \geq 0$:

1. either $\delta(q_i) = (j, q)$ in $C \times Q$, and then $q_{i+1} = q$, $c_{i+1,j} = c_{i,j} + 1$, and $c_{i+1,\bar{j}} = c_{i,\bar{j}}$, corresponding to the instruction

$$q_i\texttt{:}\quad c_j\texttt{++; goto } q,$$

2. or $\delta(q_i) = (j, q, q')$ in $C \times Q^2$, and

   - either $c_{i,j} = 0$ and then $q_{i+1} = q$, $c_{i+1,j} = c_{i,j}$, and $c_{i+1,\bar{j}} = c_{i,\bar{j}}$,
   - or $c_{i,j} > 0$ and then $q_{i+1} = q'$, $c_{i+1,j} = c_{i,j} - 1$, and $c_{i+1,\bar{j}} = c_{i,\bar{j}}$,

   corresponding to the instruction

$$q_i\texttt{:}\ \ \texttt{if (}c_j\texttt{ == 0) \{ goto } q\texttt{ \} else \{ }c_j\texttt{--; goto } q'\texttt{ \},}$$

3. or $q_i = q_f$, and then $q_i + 1 = q_f$, $c_{i+1,1} = c_{i,1}$, and $c_{i+1,2} = c_{i,2}$, corresponding to the instruction

q_f : `halt`.

The run $((q_i, c_{i,1}, c_{i,2}))_{i\geq 0}$ *halts* if $q_n = q_f$ for some $n \in \mathbb{N}$ (regardless of the counter values). It is undecidable, given $\langle \mathcal{M} \rangle$, whether its run halts.

Reducing the Halting Problem Given a 2-counter Minsky machine $\mathcal{M} = \langle Q, \{1,2\}, \delta, q_0, q_f \rangle$, we want to construct a pair $\langle \mathcal{B}, \varphi \rangle$ consisting of a BPP and a CTL(EG) formula s.t. $\mathcal{M}$ halts iff $\mathcal{B} \models \varphi$.

The idea is that $\mathcal{B}$ will be able to simulate the run of $\mathcal{M}$, but also many "incorrect" runs. The formula φ will have to filter the incorrect runs out and ensure that the halting state q_f is eventually reached in the correct run.

Exercise 3 (The BPP $\mathcal{B}$)**.** Define the BPP $\mathcal{B}$ as $\langle \Sigma, \mathcal{X}, R, X_{q_0} \rangle$ with

$$\begin{aligned}
\Sigma &= \{x_q \mid q \in Q\} \cup \{a_q \mid q \in Q \wedge \delta(q) \in C \times Q\} \cup \{c_q, d_q, e_q \mid q \in Q \wedge \delta(q) \in C \times Q^2\} \\
&\quad \cup \{x_j, y_j, z_j \mid j \in \{1,2\}\} \cup \{b_{q_f}\} \\
\mathcal{X} &= \{X_q | q \in Q\} \cup \{A_q \mid q \in Q \wedge \delta(q) \in C \times Q\} \cup \{C_q, D_q, E_q \mid q \in Q \wedge \delta(q) \in C \times Q^2\} \\
&\quad \cup \{X_j, Y_j, Z_j \mid j \in \{1,2\}\} \cup \{B_{q_f}\} \\
R &= \{X_q \xrightarrow{x_q} A_q, A_q \xrightarrow{a_q} X_j \| X_{q'} \mid q \in Q \wedge \delta(q) = (j, q')\} \\
&\quad \cup \{X_q \xrightarrow{x_q} E_q, E_q \xrightarrow{e_q} X_{q'}, X_q \xrightarrow{x_q} C_q, C_q \xrightarrow{c_q} D_q, D_q \xrightarrow{d_q} X_{q''} \mid q \in Q \wedge \delta(q) = (j, q', q'')\} \\
&\quad \cup \{X_{q_f} \xrightarrow{x_{q_f}} B_{q_f}, B_{q_f} \xrightarrow{b_{q_f}} X_{q_f}\} \\
&\quad \cup \{X_j \xrightarrow{x_j} Y_j, Y_j \xrightarrow{y_j} Z_j, Z_j \xrightarrow{z_j} 0 \mid j \in \{1,2\}\}
\end{aligned}$$

Your goal in this exercise is to identify the relationships between the run of $\mathcal{M}$ and some specific runs of $\mathcal{B}$.

Let us call a configuration α in $\mathcal{X}^\otimes$ of $\mathcal{B}$ *significant* if it has the form $\alpha = X_q \| X_1^{c_1} \| X_2^{c_2}$ for some (q, c_1, c_2) in $Q \times \mathbb{N}^2$. Define the homomorphism π from $(\mathcal{X}^\otimes)^\infty$ to $(Q \times \mathbb{N}^2)^\infty$ generated by

$$\pi(\alpha) = \begin{cases} (q, c_1, c_2) & \text{if } \alpha = X_q \| X_1^{c_1} \| X_2^{c_2} \\ \varepsilon & \text{otherwise} \end{cases}$$

that maps runs in $\mathcal{B}$ to configuration sequences of $\mathcal{M}$ by discarding insignificant configurations of $\mathcal{B}$. Note that $\pi(\rho)$ with ρ in $\mathsf{Paths}(X_{q_0})$ is not necessarily the run of $\mathcal{M}$.

Conversely, define another homomorphism ψ from $(Q \times \mathbb{N}^2)^\infty$ to $(\mathcal{X}^\otimes)^\infty$ by setting $\psi(q, c_1, c_2)$ to be the finite sequence

$$\begin{cases}
(X_q \| X_j^{c_j} \| X_{\bar{j}}^{c_{\bar{j}}})\,(A_q \| X_j^{c_j} \| X_{\bar{j}}^{c_{\bar{j}}}) & \text{if } \delta(q) = (j, q') \\
(X_q \| X_{\bar{j}}^{c_{\bar{j}}})\,(E_q \| X_{\bar{j}}^{c_{\bar{j}}}) & \text{if } \delta(q) = (j, q', q'') \wedge c_j = 0 \\
(X_q \| X_j^{c_j} \| X_{\bar{j}}^{c_{\bar{j}}})\,(C_q \| X_j^{c_j} \| X_{\bar{j}}^{c_{\bar{j}}})\,(C_q \| Y_j \| X_j^{c_j - 1} \| X_{\bar{j}}^{c_{\bar{j}}}) & \\
\cdot (D_q \| Y_j \| X_j^{c_j - 1} \| X_{\bar{j}}^{c_{\bar{j}}})\,(D_q \| Z_j \| X_j^{c_j - 1} \| X_{\bar{j}}^{c_{\bar{j}}})\,(X_{q''} \| Z_j \| X_j^{c_j - 1} \| X_{\bar{j}}^{c_{\bar{j}}}) & \text{if } \delta(q) = (j, q', q'') \wedge c_j > 0 \\
(X_q \| X_1^{c_1} \| X_2^{c_2})\,(B_{q_f} \| X_1^{c_1} \| X_2^{c_2}) & \text{otherwise, i.e. if } q = q_f
\end{cases}$$

[1] 1. Show that, if ρ in $(Q \times \mathbb{N}^2)^\omega$ is the run of $\mathcal{M}$, then $\psi(\rho)$ in $(\mathcal{X}^\otimes)^\omega$ is a run in $\mathsf{Paths}(X_{q_0})$. We say in this case that $\psi(\rho)$ is the *honest* run of $\mathcal{B}$.

[1] 2. Show that, if ρ is the honest run of $\mathcal{B}$, then $\pi(\rho)$ is the run of $\mathcal{M}$.

Exercise 4 (The CTL(EG) formula φ)**.** Set

$$\varphi = \neg\, \mathsf{EG}(\varphi_h \wedge \neg \mathsf{E}\langle x_{q_f}\rangle \top)$$

where φ_h is a CTL(EG) formula ensuring that the run of $\mathcal{B}$ is honest, and $\mathsf{E}\langle x_{q_f}\rangle\top$ that the run halts. Your goal in this exercise is to find φ_h and prove it correct.

More precisely, let $\rho = \alpha_0\alpha_1\cdots$ be in $\mathsf{Paths}(X_{q_0})$: propose a CTL(EG) formula φ_h s.t.

[5] (a) if $\forall i \geq 0$, $\alpha_i \models \varphi_h$, then ρ is honest, and

[3] (b) if ρ is honest, then $\forall i \geq 0$, $\alpha_i \models \varphi_h$.

Hint: One only needs to check rather "local" constraints, thus φ_h can be chosen with only $\mathsf{E}\langle a\rangle$ modalities, a in Σ. The proofs should contain, among other things:

(a) for (a) above, given the ith configuration $(q_i, c_{i,1}, c_{i,2})$ in the run of $\mathcal{M}$, draw four (large) trees of possible transitions of $\mathcal{B}$ out of $X_{q_i} \| X_1^{c_{i,1}} \| X_2^{c_{i,2}}$ depending on whether

(i) $\delta(q_i) = (j, q)$,
(ii) $\delta(q_i) = (j, q', q'') \wedge c_{i,j} = 0$,
(iii) $\delta(q_i) = (j, q', q'') \wedge c_{i,j} > 0$, or
(iv) $q_i = q_f$,

and annotate every branch that deviates from the sequence

$$\psi(q_i, c_{i,1}, c_{i,2}) \cdot (X_{q_{i+1}} \| X_1^{c_{i+1,1}} \| X_2^{c_{i+1,2}}) \tag{1}$$

with a proof of why it is *eventually* ruled out by φ_h, thus φ_h selects the *only* honest run out of all the possible ones;

(b) for (b) above, you need to show that every step in (1) is compatible with φ_h in the same four cases.

[2] **Exercise 5** (Conclusion)**.** Prove that $\mathcal{M}$ halts iff $\mathcal{B} \models \varphi$.