Model Checking and Strategy Synthesis for Multi-Agent Systems for Resource Allocation – Proofs

Nils Timm and Josua Botha

Department of Computer Science, University of Pretoria, Pretoria, South Africa
ntimm@cs.up.ac.za

Here we provide the proofs of the theorems of the paper *Model Checking and Strategy Synthesis for Multi-Agent Systems for Resource Allocation*, submitted to the *24th Brazilian Symposium on Formal Methods*, 2021.

Theorem 1 (Model Checking). *Let* $[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi]$ *be a strategic bounded model checking problem and let* $[M, \langle\langle A, \Sigma \rangle\rangle\, \varphi, k]$ *be its encoding over* $Vars$. *Then:*

$$[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi] \;\equiv\; \mathbf{sat}\big([M, \langle\langle A, \Sigma \rangle\rangle\, \varphi, k]\big)$$

Theorem 2 (Strategy Synthesis). *Let* $[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi]$ *be a strategic bounded model checking problem, let* $[M, \langle\langle A, \Sigma \rangle\rangle\, \varphi, k]$ *be its encoding over* $Vars$ *and let* $\alpha : Vars \rightarrow \{\mathbf{0}, \mathbf{1}\}$ *with* $\alpha\big([M, \langle\langle A, \Sigma \rangle\rangle\, \varphi, k]\big) = \mathbf{1}$. *Then for the strategy*

$$\alpha_A = \big(\{(s_a, act^a) \mid s_a \in S_a \wedge act^a \in Act \wedge \alpha([s_a.act^a]) = \mathbf{1}\}_{a \in A}\big)$$

the following holds: $\forall\, \pi \in \Pi(s, \alpha_A, \Sigma) : [M, \pi \models_k \varphi]$.

The correctness of Theorem 1 and Theorem 2 is closely linked. The correctness follows from the subsequent lemmas.

Proof of Theorem 1 and Theorem 2.
Firstly, we show that the part $[M, k]$ of the overall encoding characterises k-bounded paths of M that are conform with the evolution.

Lemma 1 (Evolution Paths). *Let* $[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi]$ *be a strategic bounded model checking problem and let* $[M, k] = [Init]_0 \wedge \bigwedge_{t=0}^{k-1} [Evolution]_{t,t+1}$ *be the encoding of all* k*-bounded paths of* M *over* $Vars$. *Then for each truth assignment* $\alpha : Vars \rightarrow \{true, false\}$ *with* $\alpha([M, k]) = true$ *there exists a sequence of states* $\pi = s_0 \ldots s_k$ *and a sequence of action profiles* $(act_t^{a_1}, \ldots, act_t^{a_n}), 0 \le t < k$ *in* M *such that*

$$\forall\, 0 \le t \le k : \forall\, a \in Agt^+ : \forall\, r \in Res : s_t(r) = a \text{ iff } \alpha([r = a]_t) = true$$

and

$$\forall\, 0 \le t < k : \delta(s_t, (act_t^{a_1}, \ldots, act_t^{a_n}), s_{t+1}) = true \text{ iff } \forall\, a \in Agt : \alpha([act^{a_i}]_t) = true$$

Proof of Lemma 1.
We have that s_0 is the initial state of M, where $s(r) = a_0$ for each $r \in Res$, i.e.

initially all resources are unallocated. According to Definition 12, the encoding of the initial state is $[Init]_0 = \bigwedge_{r \in Res} [r = a_0]_0$. Hence, any truth assignment α that satisfies $[M, k]$ must have the property that $\alpha([r = a_0]_0) = true$ for each $r \in Res$. Moreover, we have that the evolution of an MRA is a relation $\delta \subseteq S \times AP \times S$ where $(s, ap, s') \in \delta$ iff ap is executable in s and for each $r \in Res$:

1. if $s(r) = a_0$ then:
   (a) if $\exists\, a : ap(a) = req_r^a \wedge \forall\, a' \neq a : ap(a') \neq req_r^{a'}$ then $s'(r) = a$;
   (b) otherwise $s'(r) = a_0$;
2. if $s(r) = a$ for some $a \in Agt$ then:
   (a) if $ap(a) = rel_r^a \vee rel_{all}^a$ then $s'(r) = a_0$;
   (b) otherwise $s'(r) = a$.

And we have that evolution of an MRA M from time step t to $t+1$ is encoded as $[Evolution]_{t,t+1} = \bigwedge_{r \in R} [r.evolution]_{t,t+1}$ where $[r.evolution]_{t,t+1} =$

$$
\begin{aligned}
\bigvee_{a \in Acc^{-1}(r)} \Big(\quad & \big([r = a]_{t+1} \;\wedge [req_r^a]_t \wedge \textstyle\bigwedge_{a' \neq a} \neg [req_r^{a'}]_t\big) \\
& \vee \big([r = a]_{t+1} \;\wedge [r = a]_t \wedge \neg [rel_r^a]_t \wedge \neg [req_{all}^a]_t\big) \\
& \vee \big([r = a_0]_{t+1} \wedge [rel_r^a]_t\big) \\
& \vee \big([r = a_0]_{t+1} \wedge [r = a]_t \wedge [rel_{all}^a]_0\big) \\
\Big) \quad & \\
& \vee \big([r = a_0]_{t+1} \wedge [r = a_0]_t \wedge \textstyle\bigwedge_{a \in Acc^{-1}(r)} \neg [req_r^a]_t\big) \\
& \vee \big([r = a_0]_{t+1} \wedge [r = a_0]_t \wedge \textstyle\bigvee_{a, a' \in Acc^{-1}(r), a \neq a'} ([req_r^a]_t \wedge [req_r^{a'}]_t\big)
\end{aligned}
$$

Consequently, we get that $[Init]_0 \wedge [Evolution]_{0,1}$ only evaluates to $true$ for assignments α such that for all $r \in Res$ $\alpha([r = a]_1) = true$ if and only if there is a prefix $s_0 s_1$ in M and $s_1(r) = a$. Moreover, if according to the evolution, the agents $a \in Agt$ have chosen the actions act^a in state s_0, then $\alpha([act^a]) = true$ must hold exactly for these actions. This argumentation can be extended to all prefixes $s_0 \dots s_k$ of length k, which completes the proof of Lemma 1 □

We now consider Lemma 2 which shows that there is an exact correspondence between k-prefixes of M for which the goal-achievability property φ holds and satisfying assignments of $[M, k] \wedge [\varphi, k]$.

Lemma 2 (Evolution Paths Satisfying φ). *Let $[M, s \models_k \langle\!\langle A, \Sigma \rangle\!\rangle\, \varphi]$ be a strategic bounded model checking problem and let $[M, k] \wedge [\varphi, k]$ be the encoding of all k-bounded paths of M over Vars that satisfy φ. Then for each truth assignment $\alpha : Vars \to \{true, false\}$ with $\alpha([M, k]) = true$ there exists a sequence of states $\pi = s_0 \dots s_k$ and a sequence of action profiles $(act_t^{a_1}, \dots, act_t^{a_n}), 0 \le t < k$ in M such that all properties of Lemma 1 hold and additionally*

$$\forall\, a \in A : \exists\, 0 \le t \le k : \alpha([a.goal]_t) = true$$

Proof of Lemma 2.
The goal-achievability property is $\varphi = \big(\bigwedge_{a \in A} (\mathbf{F}\, a.goal)\big)$ where $\mathbf{F}\, a.goal$ holds

for a k-bounded path π if $\exists\, 0 \leq t \leq k : |\pi(t)^{-1}(a)| = d(a)$. The corresponding k-bounded encoding is $[\varphi, k] = \bigwedge_{a \in A} \left(\bigvee_{t=0}^{k} [a.goal]_t \right)$ where $[a.goal]_t = \bigvee_{\substack{R \subseteq Acc(a) \\ |R| = d(a)}} \left(\bigwedge_{r \in R} [r = a]_t \right)$. If in some state $\pi(t)$ some agent a has reached its demand, then there must be some subset $R \subseteq Acc(a)$ such that the size of R equals the agent's demand and a holds all resources of R in state $\pi(t)$. So if there is a path $s_0 \ldots s_k$ in M that satisfies $\left(\bigwedge_{a \in A} (\mathbf{F}\, a.goal) \right)$, then the truth assignment α corresponding to $s_0 \ldots s_k$ must also have the following property: $\alpha(\bigwedge_{a \in A} \left(\bigvee_{t=0}^{k} [a.goal]_t \right)) = true$. This complete the proof of Lemma 2. $\square$

We now consider Lemma 3 which shows that there is an exact correspondence between k-prefixes of M for which the goal-achievability property φ holds and where the opposition B follows the fixed strategy β, and satisfying assignments of $[\beta, k] \wedge [M, k] \wedge [\varphi, k]$.

Lemma 3 (Evolution Paths Satisfying φ and β). *Let $[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi]$ be a strategic bounded model checking problem and let $[\beta, k] \wedge [M, k] \wedge [\varphi, k]$ be the encoding of all k-bounded paths of M over Vars that satisfy φ and where the opposition B adheres to the strategy β. Then for each truth assignment α : Vars $\rightarrow \{true, false\}$ with $\alpha([M, k]) = true$ there exists a sequence of states $\pi = s_0 \ldots s_k$ and a sequence of action profiles $(act_t^{a_1}, \ldots, act_t^{a_n}), 0 \leq t < k$ in M such that all properties of Lemma 1 and Lemma 2 hold and additionally*

$$\forall\, b \in B : \forall\, act^b \in Act : \forall\, 0 \leq t \leq k : \beta((s_t)_b) = act^b \text{ iff } \alpha([s_b.act^b]) = true$$

where $(s_t)_b$ denotes the observation of agent b in state s_t.

Proof of Lemma 3.

Lemma 4 (Evolution Paths Satisfying φ, β and Uniform Protocol Behaviour of A). *Let $[M, s \models_k \langle\langle A, \Sigma \rangle\rangle\, \varphi]$ be a strategic bounded model checking problem and let $[\langle\langle A \rangle\rangle, k] \wedge [\beta, k] \wedge [M, k] \wedge [\varphi, k]$ be the encoding of all k-bounded paths of M over Vars that satisfy φ where the opposition B adheres to the strategy β and A follows the protocol in a uniform manner. Then for each truth assignment α : Vars $\rightarrow \{true, false\}$ with $\alpha([M, k]) = true$ there exists a sequence of states $\pi = s_0 \ldots s_k$ and a sequence of action profiles $(act_t^{a_1}, \ldots, act_t^{a_n}), 0 \leq t < k$ in M such that all properties of Lemma 1, 2 and 3 hold and additionally for the strategy*

$$\alpha_A = \left(\{ (s_a, act^a) \mid s_a \in S_a \wedge act^a \in Act \wedge \alpha([s_a.act^a]) = true \right)$$

the following holds: $\forall\, \pi \in \Pi(s, \alpha_A, \{\beta\}) : [M, \pi \models_k \varphi]$.