Extending Supervisory Controller Synthesis to Deterministic Pushdown Automata—Enforcing Controllability Least Restrictively


* Modelle und Theorie Verteilter Systeme, Technische Universität Berlin
** Regelungssysteme, Technische Universität Berlin, Germany
*** Max-Planck-Institut für Dynamik komplexer technischer Systeme, Magdeburg, Germany

Abstract: In this paper a step towards the generalization of supervisory control theory to situations where the specification is modeled by a deterministic pushdown automaton (DPDA) is provided. In particular, this paper presents an algorithm to calculate the largest controllable marked sublanguage of a given deterministic context free language (DCFL) by least restrictively removing controllability problems in a DPDA realization of this DCFL. It also provides a counterexample which shows that the algorithm by Griffin (2008) intended to solve the considered problem is not minimally restrictive.

Keywords: Supervisory Control Theory, Supremal Controllable Sublanguage, Minimally Restrictive Supervisor, Deterministic Context Free Languages, Pushdown Automata

1. INTRODUCTION

Ramadge and Wonham (1984) established supervisory control theory (SCT) for controller synthesis on formal languages. Given a plant and a specification, SCT defines a proper minimally restrictive supervisor as a controller which generates a closed loop system (i.e., a plant restricted by a controller) that contains as many words allowed by the plant as possible while respecting the specification, not preventing uncontrollable events and always guiding the system to a satisfactory (marking) state. Wonham and Ramadge (1987) presented an implementable fixed point algorithm to calculate the desired marked closed loop language \( L_{clm} \) using finite automaton representations of the involved languages and therefore restricting its applicability to regular plant and specification languages. This fixed point algorithm iteratively executes the following on the product automaton of plant and specification: (i) it removes controllability problems, i.e., situations where the controller attempts to prevent uncontrollable events. (ii) It resolves blocking issues, i.e., situations where the closed loop cannot reach a marking state. Obviously, step (i) may generate new blocking issues, while step (ii) may lead to new controllability problems. The algorithm terminates iff no more controllability problems or blocking situations are present.

The class of deterministic context free languages (DCFL) contains the class of regular languages, and DCFL can be represented by deterministic pushdown automata (DPDA). It was shown by Sreenivas (1993) and Masopust (2012) that step (i) of the fixed point algorithm to calculate \( L_{clm} \) cannot be realized for the case where both the plant and the specification language are DCFL. However, this is possible for the case where only the specification language

is generalized to DCFL. The resulting generalized supervisory control problem is practically relevant, as it allows to consider a broader class of specifications. The main contribution of this paper is a new algorithm which realizes step (i) for DPDA. Step (ii) is discussed by Schneider and Nestmann (2014). Soundness issues involving the overall iteration, including the existence of a unique fixed point, are discussed in a companion paper by Schneider, Schmuck, Raisch, and Nestmann (2014). Griffin (2008) suggested an algorithm for the more restrictive setting of a prefix closed regular plant and a prefix closed deterministic context free specification language. However, as shown by the counterexample in Appendix A, Griffin’s algorithm does not construct the minimally restrictive supervisor. The paper is structured as follows. After introducing all required notation in Section 2, we summarize the necessary parts of SCT in Section 3. In Section 4, we present an algorithm working on DPDA, realizing step (i) of the fixed point algorithm to calculate \( L_{clm} \).

2. PRELIMINARIES

Let \( \Sigma \) be the external alphabet. Then \( \Sigma^* \) denotes the set of all finite-length strings over symbols from \( \Sigma \). Furthermore, we use the abbreviations \( \Sigma^+ = \Sigma^* \setminus \{\lambda\} \) and \( \Sigma^{\leq 1} = \Sigma \cup \{\lambda\} \), where \( \lambda \) is the empty string. Throughout this paper, we denote elements of the set \( \Sigma^{\leq 1} \) by \( \sigma \), i.e., \( \sigma \) can also be the empty string. We denote the projection of a tuple or string \( a \) on its \( i \)th element by \( \pi_i(a) \) and the concatenation of two strings \( w, w' \in \Sigma^* \) by \( w \cdot w' \), meaning that \( w' \) is appended to \( w \). The prefix relations on strings are defined by \( w \sqsubseteq w' \) if \footnote{Throughout this paper we use the notation \"\( \exists \cdot \cdot \cdot \)\", meaning that all statements after the dot hold for all variables in front of the dot. \"\( \exists \cdot \cdot \cdot \)\" is interpreted analogously.} \( \exists w'' \in \Sigma^* : w \cdot w'' = w' \) and by \( w \sqsubset w' \) if \( \exists w'' \in \Sigma^+ : w \cdot w'' = w' \). Any subset of
\( \Sigma^* \) is called a language. The prefix closure of a language \( L \) is defined by \( \overline{L} = \{ w \in \Sigma^* \mid \exists w' \in L \mid w \subseteq w' \} \). A language \( L_1 \) is nonblocking w.r.t. a language \( L_2 \) iff \( L_1 \subseteq \overline{L_2} \). On an alphabet \( \Sigma \) partitioned into controllable (in the sense of preventable) and uncontrollable events, i.e., \( \Sigma = \Sigma_c \cup \Sigma uc \), \( \Sigma_c \cap \Sigma uc = \emptyset \), a prefix-closed language \( L_1 = L_1 \) is controllable w.r.t. a prefix-closed language \( L_2 = L_2 \) if \( L_1 \cap \Sigma uc \cap L_2 \subseteq L_1 \). In particular, a word \( w \in L_1 \) is controllable w.r.t. \( L_2 \) (written \( \text{ContW}(L_1, L_2, \Sigma uc, w) \)) iff \( \forall \mu \in \Sigma uc, w \mu \in L_2 \rightarrow \exists \mu' \in L_1 \).

A discrete event system (DES) is a tuple \( D = (\Sigma, \Sigma_c, \Sigma uc, L_m) \), where \( \Sigma uc = \Sigma \setminus \Sigma^* \) is defined by \( \exists \) the same pre and post state are depicted by one edge with (with the right-most symbol first). Two transitions with then \( \gamma \) is defined by \( D \) by its marked and unmarked language only and write \( D = \{ L_m, L_m \} \). We say that \( D \) is nonblocking, if \( L_m \) is nonblocking w.r.t. \( L_m \).

A pushdown automaton (PDA) is a tuple \( M = (Q, \Sigma, \Gamma, \delta, q_0, \sqcup, F) \) s.t. (i) the state set \( Q \), the external alphabet \( \Sigma \), the stack alphabet \( \Gamma \), and the set of transitions \( \delta \) are finite, (ii) \( \delta \subseteq Q \times \Sigma^{\geq 1} \times \Gamma \times \Gamma^* \times Q \), (iii) the end-of-stack marker \( \sqcup \) is contained in \( \Gamma \), (iv) the set of marking states \( F \) and the initial state \( q_0 \) are contained in \( Q \), and \( (v) \) \( \sqcup \) is never removed from the stack (i.e., \( (q, \sigma, \sqcup, s, q') \) implies \( \exists s' \in \Gamma^*, s = s'(\sqcup) \)).

Example 1. Consider the external alphabet \( \Sigma = \{a, b, c, d, u\} \), the stack alphabet \( \Gamma = \{\sqcup, \bullet\} \), the state set \( Q = \{q_0, \ldots, q_5\} \) and the set of marking states \( F = \{q_2, q_3\} \). Then \( M_o \) in Figure 1 is a PDA, and the transition \( (q, \sigma, \gamma, s, q') \in \delta \) is depicted by an edge from \( q \) to \( q' \) labeled by \( \sigma, \gamma, s \) denoting that by taking this transition, \( \sigma \in \Sigma^{\geq 1} \) is generated, \( \gamma \in \Gamma \) (called “stack-top”) is popped from the top of the stack, and \( s \in \Gamma^* \) is pushed onto the stack (with the right-most symbol first). Two transitions with the same pre and post state are depicted by one edge with two labels.

\[ \begin{align*}
\text{Figure 1.} \quad & M_o \text{ in Example 1.} \\
& \text{Note that } M \text{ can do silent moves (called } \lambda \text{-transitions),} \\
& \text{possibly modifying the stack but not generating an external} \\
& \text{symbol (e.g., see Figure 1, from } q_1 \text{ to } q_2). \text{ We collect} \\
& \text{the starting states of all } \lambda \text{-transitions in the set} \\
& Q_{\lambda}(M) := \{ q \in Q \mid (q, \lambda, \gamma, \lambda, \gamma, s, q') \in \delta \}. \\
\end{align*} \]

A PDA \( M \) is livelock free (written \( M \in LLF \)) iff there exists no reachable infinite sequence of \( \lambda \)-transitions. Since livelock free PDA and PDA are equally expressive, we only consider \( M \in LLF \). From a system theoretic point of view, a system state would be a pair \( (q, s) \), where \( q \in Q \) and \( s \in \Gamma^* \) represents the current stack content. Hence, from this point of view, a PDA with \( |Q| < \infty \) has infinite state space since the stack is not restricted. The pair \( (q, s) \) is sometimes referred to as a configuration. For our purposes, it turns out to be convenient to add the string of generated external symbols to this pair. We therefore define the set of configurations \( C(M) := Q \times \Sigma^* \times \Gamma^* \) where \( (q, w, \sigma) \in C(M) \) consists of a state \( q \), a history variable \( w \) (storing the external symbols generated), and a stack variable \( \sigma \) (storing the current stack content). The initial configuration is \( (q_0, \lambda, \sqcup) \). Now observe that a transition from one configuration to another occurs when \( M \) takes a transition \( e \in \delta \). To make this step visible we choose to include the taken transition \( e \) into the definition of a transition from one configuration to another. The single-step transition relation \( \tau_M \subseteq ((\delta \cup \{\sqcup\}) \times C(M))^2 \) is therefore defined by \( (e, (q, w, \gamma, s')) \in \tau_M \) \( (e', (q', w, \sigma, s')) \) for \( e' = (q, \sigma, \gamma, s', q') \), where \( \sqcup \) denotes an undefined\(^3\) pre-transition. The set \( \mathcal{D}(M) \) contains all finite-length\(^4\) derivations \( f: N \rightarrow ((\delta \cup \{\sqcup\}) \times C(M)) \) s.t.

\[ \forall n < \max(\text{dom}(f)) \cdot f(n) \mid M \Rightarrow f(n + 1) \]

with \( \text{dom}(f) \) being the domain of \( f \). The set \( \mathcal{D}_{\text{max}}(M, w) \) contains all elements of \( \mathcal{D}(M) \) starting with the initial element \( f(0) = (\sqcup, (q_0, \lambda, \sqcup)) \). Furthermore, the set \( \mathcal{D}_{\text{max}}(M, w) \) of maximal finite-length derivations of a word \( w \in \Sigma^* \) is defined by \( \mathcal{D}_{\text{max}}(M, w) := \left\{ f \mid f \in \mathcal{D}(M) \right\} \). The set of reachable configurations is defined by \( \mathcal{R}(M) := \{ c \in C(M) \mid \exists d \in \mathcal{D}(M), e, n \cdot d(n) = (e, c) \} \). Using this definition, we define the marked and the unmarked languages generated by \( M = (Q, \Sigma, \Gamma, \delta, q_0, \sqcup, F) \) in PDA by \( \mathcal{L}(M) := \{ w \mid (q, w, \sigma) \in \mathcal{R}(M) \wedge q \in F \} \) and \( \mathcal{L}_{\text{un}}(M) := \{ w \mid (q, w, \sigma) \in \mathcal{R}(M) \} \), respectively. The class of languages generated by PDA is the class of context free languages (CFL). We say that a PDA \( M \) realizes a DES \( D = (\mathcal{L}(M), L_m) \) if \( \mathcal{L}(M) \subseteq \mathcal{L}_{\text{in}}(M) \) and \( \mathcal{L}_{\text{un}}(M) \subseteq \mathcal{L}(M) \) and, with some abuse of terminology, we say \( D \in \text{CFL} \) if \( \mathcal{L}_{\text{un}}(M) \subseteq \mathcal{L}(M) \).

A PDA \( M \) is a deterministic pushdown automaton (DPDA) (written \( M \in \text{DPDA} \)) iff distinct steps from a reachable configuration append distinct elements of \( \Sigma \) to the history variable. Note that this implies that the existence of an outgoing \( \lambda \)-transition in state \( q \) requiring stack-top \( \gamma \) prevents other outgoing transition in \( q \) requiring stack-top \( \gamma \). The class of languages generated by DPDA is the class of deterministic context free languages (DCFL).

Example 2. The PDA \( M_o \) depicted in Figure 1 is also a DPDA since all required properties hold. Furthermore, the marked and unmarked language of \( M_o \) are given by \( \mathcal{L}_{\text{marked}}(M_o) = \{ \text{ac, aac, a}^{2k-1}d(bb)^{l}, a^{2k-2}d(bb)^{l}, a^{2k-3}d(bb)^{l}, b^{u}, a^{2k+2}d(bb)^{u}, \text{a}^{2k+1}d(bb)^{u}\} \) and \( \mathcal{L}_{\text{unmarked}}(M_o) = \{ \text{ac, aac, a}^{2k+1}d(bb)^{l}, a^{2k+2}d(bb)^{l}, b^{u}, a^{2k+1}d(bb)^{u}, b^{u}, a^{2k}d(bb)^{u}\} \) where \( k, l \in \mathbb{N}, k > 0, l \leq k \). We use the dummy symbol \( \sqcup \) to define the initial transition, and, occasionally, when the \( \lambda \)-transition is irrelevant for the context.

\(^3\) since \( M \in LLF \)

\(^4\) We use the dummy symbol \( \sqcup \) to define the initial transition, and, occasionally, when the \( \lambda \)-transition is irrelevant for the context.
and \(L_{\text{um}}(M_O) = L_{\text{m}}(M_O)\), since no blocking situations occur in \(M_O\). This can be verified in Figure 1 (i) by checking that in every non-marking state \(q\) either (a) an outgoing transition exists for both stack-tops \(\square\) and \(\star\), or (b) the configuration \((q, \cdot, \gamma)\) is not reachable if no outgoing transition with stack-top \(\gamma\) exists (e.g., \((q_1, \cdot, \Box)\) is not reachable) and (ii) observing that no dead locks or infinite loops visiting only non-marking states exist.

A nondeterministic finite automaton (NFA) can be viewed as a special PDA which does neither have \(\lambda\)-transitions, nor a stack (see Figure 2). Therefore, we can formally define a PDA \(M = (Q, \Sigma, \Gamma, \delta, q_0, \square, F)\) to be an NFA (written \(M \in \text{NFA}\)) iff whenever \((q, \sigma, \gamma, s, q') \in \delta\), then \(\gamma = s = \square\) and \(\sigma \in \Sigma\). Additionally, deterministic finite automata (DFA) are NFA which are deterministic. The class of languages generated by DFA is the class of regular languages (REG)\(^5\).

**Example 3.** Consider the input alphabet \(\Sigma = \{a, b, c, d, u\}\), the state set \(Q = \{p_0, p_1, p_2, p_3\}\), the set of marking states \(F = \{p_1, p_3\}\) and the initial state \(p_0\). Then the automaton \(M_P\) in Figure 2 is a DFA. The transition \((p, \sigma, \square, \square, p') \in \delta\) is depicted by an edge from \(p\) to \(p'\) labeled by \(\sigma\).

![Figure 2. DFA \(M_P\) in Example 3.](image)

The marked and unmarked languages of \(M_P\) are given by\(^6\)
\[
L_m(M_P) = \{a^n(c + d), a^n(c + d)(bb)^n(bu + \lambda) | n, m \in \mathbb{N}\}
\]
and \(L_{\text{um}}(M_P) = L_{\text{m}}(M_P)\), since no blocking situations occur in \(M_P\).

### 3. SUPERVISORY CONTROL REVISITED

In the context of SCT, a controller \(D_C = \{L_{\text{Cum}}, L_{\text{cm}}\}\) is a proper minimalistic supervisor for a plant \(D_P = \{L_{\text{Pum}}, L_{\text{Pm}}\}\) and a specification \(D_S = \{L_{\text{Sm}}, L_{\text{Sm}}\}\), if \(D_C\) (i) is not preventing uncontrollable events (i.e., \(\{L_{\text{Pum}} \cap L_{\text{Cum}}\} \cup \{L_{\text{Pm}} \cap L_{\text{Cum}}\}\) ⊆ \(L_{\text{Pm}} \cap L_{\text{Cum}}\)), (ii) generates a closed loop \(D_o = L_{\text{clm}} \cap L_{\text{cm}}\), with \(L_{\text{clm}} = L_{\text{Pum}} \cap L_{\text{Cum}}\) and \(L_{\text{cm}} = L_{\text{Pm}} \cap L_{\text{Cum}}\), which contains as many words generated by the plant as possible while respecting the specification, and (iii) always guides the system to a marking state (i.e., \(L_{\text{clm}} \subseteq L_{\text{clm}}\)). In this case \(L_{\text{clm}}\) is the so-called marked supremal controllable (non-blocking) sublanguage of \(L_{\text{Pm}} \cap L_{\text{Sm}}\) (see Wonham and Ramadge, 1987). Since different controllers can generate the same closed loop, there exists no unique minimalistic supervisory controller for \(D_P\) and \(D_S\). Obviously, the closed loop itself is a proper supervisor, giving \(D_C = L_{\text{clm}} \cap L_{\text{cm}}\).

By iteratively applying \(\Omega\), starting with \(L_{\text{sm}} \cap L_{\text{pm}}\), one obtains \(L_{\text{clm}}\) as the (unique) greatest fixed point. Wonham and Ramadge (1987, Lemma 2.1) showed that for \(L_{\text{sm}}, L_{\text{pm}} \in \text{REG}\) an implementable algorithm working on DFA to calculate \(L_{\text{clm}}\) in REG exists.

Now consider a plant \(D_P = \{L_{\text{Pum}}, L_{\text{Pm}}\}\) in REG and a specification \(D_S = \{L_{\text{Sm}}, L_{\text{Sm}}\}\) in DCFL. In this case we have \(\{L_{\text{Sm}} \cap L_{\text{Pum}}, L_{\text{Sm}} \cap L_{\text{Pm}}\} \in \text{DCFL}\) (see Hopcroft and Ullman, 1979, p.135), realizable by a DPDA.

Now observe the following: in one iteration of the fixed-point algorithm the language \(L_{\text{cm}}\) is needed to calculate \(\Omega(L_{\text{cm}})\). When implementing this algorithm using a DPDA-realization of the DES \(D = \{L_{\text{um}}, L_{\text{m}}\}\), the language \(L_{\text{cm}}\) is (in general) not easily obtained. However, if \(D\) is nonblocking, we can use \(L_{\text{cm}} = L_{\text{m}}\). Therefore, to implement the iterative calculation of \(\Omega\), starting with \(L_{\text{sm}} \cap L_{\text{pm}} \in \text{DCFL}\), one has to iteratively (i) construct a DPDA \(M_O\) from a nonblocking DPDA \(M_O\) s.t. \((L_{\text{m}}(M_O)) \subseteq L_{\text{m}}(M_O)\) and (ii) make \(M_O\) nonblocking.

We show in the remainder of this paper that there exists an algorithm working on DPDA which realizes step (i) and returns a DPDA. An algorithm realizing step (ii) is presented by Schneider and Nestmann (2014).

**Remark 1.** The implementable algorithm to calculate \(L_{\text{clm}}\) in REG presented by Wonham and Ramadge (1987, Lemma 5.1) iteratively calculates the unmarked controllable sublanguage of \(L_{\text{um}} = L_{\text{m}}\), i.e.,
\[
\Omega(L_{\text{um}}) = \{w \in L_{\text{um}} | \text{ContW}(L_{\text{um}}, L_{\text{Pum}}, \Sigma_{uc}, w)\}\]
and its nonblocking sublanguage \(\Omega(L_{\text{m}}) \cap L_{\text{Sm}} \cup L_{\text{Pm}}\). In contrast, the algorithm introduced in the next section iteratively calculates the marked controllable sublanguage \(\Omega(L_{\text{m}})\) and its prefix closure.

### 4. COMPUTABILITY OF \(\Omega\) FOR DCFL

In this section, using the DFA \(M_P\) realizing \(\Omega(L_{\text{um}}) \cap L_{\text{Pm}}\), we derive a sequence of automaton manipulations starting with the DPDA \(M_O\) and generating a DPDA \(M_O'\) s.t. \(\Omega(L_{\text{m}}(M_O)) = L_{\text{m}}(M_O')\). We assume that \(L_{\text{m}}(M_O) \subseteq L_{\text{Pm}}\). This is not a restriction of generality, as \(\Omega\) is monotonic and its iterative application is initialized with \(L_P \cap L_{\text{Sm}}\). We furthermore assume that \(M_O\) is nonblocking, i.e., \(L_{\text{m}}(M_O) \subseteq L_{\text{m}}(M_O)\). If this assumption does not hold, the algorithm to remove blocking situations is applied first.

The first task is to find all controllability problems in \(M_O\). Intuitively, a controllability problem occurs when a word \(w \in \Sigma^*\) generated by \(M_P\) and \(M_O\) reaching states \(p\) and \(q\) (by using maximal derivations), respectively, and \(M_P\) can generate an uncontrollable symbol \(\sigma \in \Sigma_{uc}\) in \(p\) while \(M_O\) cannot generate this symbol in \(q\). To obtain the states \(p\) and \(q\) reached when generating the same word \(w \in \Sigma^*\), a product automaton is constructed, following, e.g., Hopcroft and Ullman (1979, p.135).

\(^5\) Note that for every language \(L_{\text{um}}\) generated by a NFA, there also exists a DFA generating \(L_{\text{um}}\) (see Hopcroft and Ullman, 1979, p.22). However, this is not true for PDA and DPDA, implying DCFL ⊂ CFL.

\(^6\) The term \((x + y)\) denotes \(\cdot x \cdot y\).
Definition 1. Let $M_P = (Q_P, \Sigma, \{\square\}, \delta_P, q_{p0}, \square, F_P) \in$ DFA and $M_O = (Q_O, \Sigma, \Gamma, \delta_O, q_{o0}, \square, F_O) \in$ DPDA. Then the product automaton $M_x = M_P \times M_O$ is defined by $M_x = (Q_x, \Sigma, \Gamma, \delta_x, q_{x0}, \square, F_x)$ with $Q_x = Q_P \times Q_O$, $q_{x0} = (q_{p0}, q_{o0})$, $F_x = F_P \times F_O$ and

$$
\delta_x = \begin{cases}
(p,q), \sigma, s, (p',q') | \sigma = \lambda \\
(q,p,\gamma, s, q') \in \delta_O \\
(p,\lambda, \gamma, s, q') \in \delta_P
\end{cases}.
$$

Lemma 1. Let $M_P \in$ DFA and $M_O \in$ DPDA s.t. $L_m(M_O) \subseteq L_m(M_P)$ and $L_m(M_O) \subseteq L_m(M_O)$. Then (i) $L_m(M_P \times M_O) = L_m(M_O)$, (ii) $L_m(M_P \times M_O) = L_m(M_O)$, (iii) $M_x = M_P \times M_O \in$ DPDA, and (iv) $\times$ is implementable.

Proof 1. Since $M_x = M_P \times M_O$ is a product automaton in the usual sense, we have $L_m(M_P \times M_O) = L_m(M_P) \cap L_m(M_O)$ and $L_m(M_P \times M_O) = L_m(M_P) \cap L_m(M_O)$. Having $L_m(M_P) \subseteq L_m(M_P)$, $L_m(M_O) \subseteq L_m(M_O)$ and $L_m(M_P) = L_m(M_P)$ implies $L_m(M_O) \subseteq L_m(M_P)$, which immediately proves (i) and (ii). (iii) and (iv) follow from Hopcroft and Ullman (1979, p.135).

Example 4. Consider the DPDA $M_O$ in Figure 1 and the DFA $M_P$ in Figure 2. It can be easily verified that $L_m(M_O) \subseteq L_m(M_P)$, since the state and transition structures of $M_O$ and $M_P$ are identical and the usage of a stack only prevents certain transitions. Furthermore, $L_m(M_O) \subseteq L_m(M_O)$ from Example 2. The (accessible part of the) product automaton $M_x = M_P \times M_O$ is depicted in Figure 3 and does obviously generate the same marked and unmarked language as $M_O$.

Unfortunately, in contrast to the DFA algorithm by Wonham and Ramadge (1987, Lemma 5.1), it is not possible to remove controllability problems in $M_O$ in a minimally restrictive fashion by deleting states or edges in $M_x$. This is due to the following observations: (i) it is possible that controllability problems occur in one state for a subset of possible stack-tops only (e.g., if $u \in \Sigma_{uc}$, $M_x$ in Figure 3 has a controllability problem in $(p_2, q_4)$ for stack-top $\square$, only). Therefore, removing this state may falsely delete uncontrollable words. (ii) It is generally not possible to uniquely prevent a certain stack-top symbol in a given state by removing certain pre-transitions as one incoming transition can generate more than one stack-top (e.g., the transition $((p_1, q_3), b, \square, \lambda, (p_2, q_1))$ in Figure 3 generates as stack-top the symbol which is currently in the stack underneath $\bullet$). (iii) Controllability problems are not easily observable in states $(p, q) \in Q_\lambda$ (e.g., $(p_1, q_1)$, $(p_1, q_2)$ in Figure 3) as it is not possible to determine in $(p, q)$ whether

$$\delta_{Sp} = \begin{cases}
\{(p,\gamma) | p \in Q, \gamma \in \Gamma \} \\
\cup \{(p,\gamma, s, p') | p \in Q, \gamma \in \Gamma \} \\
\cup \{(p,\gamma, s, p') | p \in Q, \gamma \in \Gamma \} \\
\cup \{(p,\gamma, s, p') | p \in Q, \gamma \in \Gamma \} \\
\cup \{(p,\gamma, s, p') | p \in Q, \gamma \in \Gamma \}
\end{cases}
$$

Example 5. Consider the product automaton $M_x$ in Example 4 depicted in Figure 3. By using the abbreviation in Figure 4, its split version $M_{Sp} = \text{SPLIT}(M_x)$ is defined by $M_{Sp} = (Q_{Sp}, \Sigma, \delta_{Sp}, q_{Sp0}, \square, F_{Sp})$ with $Q_{Sp} = M(Q) \cup A(Q, \Gamma)$, $q_{Sp0} = (q_0)_{r, p}$ and $F_{Sp} = (A_r(F, \Gamma) \cup A_u(Q, \Gamma)) \setminus Q_\lambda(M_{Sp})$.
the set $Q_\lambda(M_{Sp})$ or do not have outgoing $\lambda$-transitions at all. This uniquely defines the subset of states (i.e., $A(Q,\Gamma) \setminus Q_\lambda(M_{Sp})$) for which controllability can and must efficiently be tested. Finally, the new special states are used to ensure that only the states reached by maximal derivations of words $w \in L_m(M_D)$ are marking. Observe that the construction in SPLIT ensures, that final states of maximal derivations always end in the set $A(Q,\Gamma) \setminus Q_\lambda(M_{Sp})$, formally,

$$\forall w \in L_m(M_{Sp}), f \in D_{max,M_{Sp}}(w) . \quad \pi_1(\pi_2(f(\max(\text{dom}(f))))) \in (A(Q,\Gamma) \setminus Q_\lambda(M_{Sp})).$$

\hspace{1cm} (5)

Therefore, shifting the marking into those states ensures that uncontrollable words can be removed from the marked language by removing states in the set $A(Q,\Gamma) \setminus Q_\lambda(M_{Sp})$. Before removing states with controllability problems we show that SPLIT does not change the marked and unmarked language of its input.

**Lemma 2.** Let $M = (Q,\Sigma,\Gamma,\delta,q_0,\square,F)$ and $M_{Sp} = \text{SPLIT}(M)$. Then (i) $L_m(M_{Sp}) = L_m(M)$, (ii) $L_m(M) = L_m(M_{Sp})$, (iii) $\text{SPLIT}(M) \in \text{DPDA}$, and (iv) SPLIT is implementable. □

**Proof 2.** see Appendix B.

Technically, we are now ready to delete all states that have a controllability problem. However, both $\times$ and SPLIT introduce non-accessible states and transitions. Trimming the automaton $M_{Sp}$ prior to the removal of controllability problems has the advantage that termination of the fixed point algorithm over $\Omega$ can be easily verified, since no states are removed, if the automaton is trim, nonblocking and no further controllability problems are present. Therefore, following Griffin (2006, Thm.4.1), we introduce an algorithm to remove non-accessible states and transitions in DPDA. Here, in contrast to DFA, transitions can be non-accessible even if they connect accessible states, since the required stack-top might not be available at its prestate.

**Definition 3.** Let $M = (Q,\Sigma,\Gamma,\delta,q_0,\square,F)$. Then the accessible part $\text{AC}(M)$ of $M$ is defined by $M_{Ac} = (Q_{Ac},\Sigma,\Gamma,\delta_{Ac},q_0,\square,F_{Ac})$ s.t. $Q_{Ac} = Q \setminus Q_{na}(M)$, $F_{Ac} = F \setminus Q_{na}(M)$ and $\delta_{Ac} = \delta \setminus \delta_{na}(M)$, where $Q_{na}(M) := \{q \in Q \setminus \{q_0\} \mid L_m((Q,\Sigma,\Gamma,\delta,q_0,\square,\{q\})) = \emptyset\}$ are the non accessible states and

\[
\delta_{na}(M) := \begin{cases} 
    e = (q, x, \gamma, s, q') \in \delta \\
    \forall r \notin Q, \delta' = (\delta \cup \{(q, \lambda, \gamma, r)\}) \setminus \{e\} \\
    L_{na}(\{(q \setminus \{q_0\}, \Sigma, \Gamma, q_0, \square, \{r\})\}) = 0 \\
  \end{cases}
\]

are the non accessible transitions. □

**Example 6.** The accessible part of the automaton $M_{Sp}$ in Example 5, depicted in Figure 5, is obtained by removing the dotted states, giving $M_{Ac} = \text{AC}(M_{Sp})$. □

Trimming a DPDA does not change its marked and unmarked languages.

**Lemma 3.** Let $M = (Q,\Sigma,\Gamma,\delta,q_0,\square,F)$. Then (i) $L_m(\text{AC}(M)) = L_m(M)$, (ii) $L_m(\text{AC}(M)) = L_m(M)$, (iii) $\text{AC}(M) \in \text{DPDA}$, and (iv) AC is implementable. □

**Proof 3.** Observe that $Q_{na}(M)$ is the set of states not reachable by derivations of words $w \in L_m(M)$ and $\delta_{na}(M)$ is the set of transitions that are not part of derivations of words $w \in L_m(M)$. Therefore removing these states and transitions does not change the unmarked language, implying (ii). Since accessible marking states are preserved, also the marked language (as a subset of the unmarked language) is left unchanged, implying (i). Since $M \in \text{DPDA}$, (iii) immediately follows as we only remove states and transitions. (iv) follows, as the emptiness of a CFL is decidable(see Hopcroft and Ullman, 1979, p.137).

As the final step of our algorithm, we will now identify auxiliary states that have a controllability problem with respect to the plant, and remove them. This is done in analogy to the DFA algorithm by Wonham and Ramadge (1987), while ignoring all states in $Q_{\lambda}$.

**Definition 4.** Let $\Sigma_{nc} \subseteq \Sigma$, $M_{P} \in \text{DPDA}$, $M_{O} \in \text{DPDA}$, $M_{Ac} = M_{P} \times M_{O} = (Q_{Ac},\Sigma,\Gamma,\delta_{Ac},q_0,\square,F_{Ac})$, and $M_{Ac} = \text{AC}(\text{SPLIT}(M_{Ac})) = (Q_{Ac},\Sigma,\Gamma,\delta_{Ac},q_0,\square,F_{Ac})$. Then the automaton with removed non-controllable auxiliary states is defined by $\text{RNCS}(M_{Ac}) = (Q_{R},\Sigma,\Gamma,\delta_{R},q_0,\square,F_{R})$, where $Q_{R} = Q_{Ac} \setminus \text{NCS}$, $F_{R} = F_{Ac} \setminus \text{NCS}$ and $\delta_{R} = \{(q, x, \gamma, w, q') \in \delta' | q, q' \in Q_{R}\}$, where

\[
\text{NCS} := \begin{cases} (p, \mu, \square, s, r) \in \delta_{Ac} \\
\exists \mu \in \Sigma_{nc} . \quad (\exists p' . \ (p, \mu, \square, p' \in \delta_{P} \wedge \forall s, r . \ (\{p, \gamma\}, \mu, \gamma, s, r) \notin \delta_{Ac}) \\
\end{cases}
\]
Example 7. Consider the accessible split automaton $M_{Ac}$ in Example 6 depicted in Figure 5 and let $\Sigma_{uc} = \{u\}$. Then the nonblocking version $M'_{Ac}$ of $M_{Ac}$ in Figure A.2, by making $M$ scan its entire input, using the algorithm by Hopcroft and Ullman (1979, Lem. 10.3).

In this paper, we have presented an extension of SCT to situations, where the plant is realized by a DFA, but the specification is modeled as a DPDA, i.e., the specification language is a DCFL. In particular, we have presented an algorithm consisting of a sequence of automaton manipulations which, starting with a nonblocking DPDA, removes all (and only those) marked words having a prefix which is uncontrollable w.r.t. the plant. This algorithm was implemented as a plug-in in libFAUDES (2006-2013). The remaining part of a procedure to obtain a proper minimally restrictive supervisor, namely an algorithm removing blocking situations in DPDA, is presented by Schneider and Nestmann (2014). The connection between a language-theoretic characterization and the automata-based implementation is investigated in detail in the companion paper by Schneider, Schmuck, Raisch, and Nestmann (2014).

Appendix A. COUNTEREXAMPLE

In this section, the algorithm presented in (Griffin, 2008, p.827) and (Griffin, 2007, p.64) is applied to an example. It will be shown that this represents a counterexample to (Griffin, 2008, Theorem 3.5) and (Griffin, 2007, Theorem 5.2.5) since the final DPDA does not realize the supremal controllable sublanguage of the given prefix closed deterministic context free specification language (which is required to be a subset of the given prefix closed regular plant language). Therefore we claim that the problem of automatically calculating a supremal controllable sublanguage of a DCFL was not solved by Griffin (2007, 2008).

The algorithm is initialized with a DFA $G$ and a DPDA $M$ realizing the plant and the specification, respectively, s.t. $L(G) = L_{um}(G)$, $L(M) = L_{um}(M)$ and $L(M) \subseteq L_{um}(G)$. Observe that the DFA $G$ and the DPDA $M$ depicted in Figure A.1 satisfy these requirements since their languages are given by

\[ L(G) = L_{um}(G) = \{a^n, a^nb, a^nbu | n \in \mathbb{N}\} \]

\[ L(M) = L_{um}(M) = \left\{ a^n, a^mb, a^mbu | n,m,k \in \mathbb{N}, m > 0, k > 1 \right\}. \]

Using these automata, the construction follows seven steps.

1. Construct $M'$, depicted in Figure A.2, by making $M$ scan its entire input, using the algorithm by Hopcroft and Ullman (1979, Lem.10.3.).
2. Construct a DPDA $M''$ that accepts the complement of $L_m(M)$ using the algorithm by Hopcroft and Ullman (1979), Thm.10.1. Here $M''$ is identical to $M'$ in Figure A.2 but with exchanged non-marking and marking states, i.e., $F''$ = $\{q_d\}$.

3. Construct a DPDA $M'''$ that accepts $L_m''(M) \cap L_m(G)$, i.e., calculate the cross product of $G$ and $M''$ using the algorithm by Hopcroft and Ullman (1979), Thm.6.5.

4. Construct $M_1$, depicted in Figure A.3, as the accessible part of $M'''$, using the algorithm by Griffin (2006), Thm.4.1.

5. Construct a predicting machine to observe so called $\mu$-reverse paths using the algorithm by Hopcroft and Ullman (1979), p.240. Here, the construction simply defines an additional stack symbol $\mu, \forall \gamma \in \Gamma$ s.t.

$$\mu_\gamma := \begin{cases} \{q \in Q_1 \mid \exists q' \in F_1, v \in \Sigma_{\text{uc}} \mid (q, q', w, v, s') \in M_1 \} & \text{if } \gamma \neq \text{null} \end{cases}$$

which denotes the set of unmarked states in $M_1$ from which a derivation starting with stack-top $\gamma$, generating a sequence of uncontrolable symbols $v \in \Sigma_{\text{uc}}$ and reaching a marking state $q'$ (i.e., a so called $\mu$-reverse path), exists. For $M_1$, depicted in Figure A.3, this gives $\mu_\text{null} = \{(p_1, q_1)\}$ and $\mu_\text{null} = \emptyset$. The predicting machine $M''_p$, depicted in Figure A.4, is then identical to $M_1$ but uses pairs $[\gamma, \mu]$ as stack.

6. Construct $M_2$, depicted in Figure A.5, by deleting all transitions

$$\delta_{cp} := \{ (q, \sigma, \gamma, \gamma', s, q') \in \delta_M \mid$$

$$\exists (q, \sigma, \gamma, [\gamma'], \mu_{\gamma'}) \cdot s, q' \in \mu_{\gamma'} \}$$

in $M$ which produce a stack-top in $q'$ which enables a $\mu$-reverse path starting in $q$. For $M$ and $M''_p$, depicted in Figure A.1 and A.4, respectively, observe that $e = ((p_0, q_0), (p_1, q_1)) \in \delta_{M''_p}$ is the only ingoing transition to $(p_1, q_1)$ (where the only $\mu$-reverse path starts for stack-top $\square$, since $\mu_\square = \{(p_1, q_1)\}$, and, since $M_1$ is trim, eventually leads to the stack-top $\square$ in $(p_1, q_1)$. Using the corresponding transition to $e$ in $M$, this gives $\delta_{cp} = \{(q_0, b, \lambda, \lambda, q_1)\}$. By deleting $\delta_{cp}$ in $M$, we obtain $M_2$, depicted in Figure A.5.

7. Construct $M_3$, depicted in Figure A.6, as the accessible part of $M_2$, using the algorithm by Griffin (2006), Thm.4.1. If $\delta_{cp}$ in step 6 is empty, the algorithm terminates. Otherwise, the algorithm is restarted with $M = M_3$.

Figures A.1. DFA $G$ (left) and DPDA $M$ (right) realizing plant and specification, respectively.

Figure A.2. DPDA $M'$, with $\Psi = \Phi \setminus \{u, \mu\}$ and $\Phi = \{a, a, a, a, a, \ldots\}$. Thm.4.1.

Figure A.3. DPDA $M_1$, with $((q_1), q_1)$.

Figure A.4. DPDA $M''_p$ with $\mu_\text{null} = \{(p_1, q_1)\}$ and $\mu_\text{null} = \emptyset$. The set of $\mu$-reverse paths is depicted in red (dashed) while the set of edges in $\delta_{cp}$ is depicted in blue (dotted).

Figure A.5. DPDA $M_2$

Figure A.6. DPDA $M_3$

Obviously, $M_3$ does not have further controllability problems. Therefore, the algorithm would redo steps 1-6 and then return $M_3$.

Now observe that the specification language $L_m(M)$ restricts the plant language $L_m(G)$ such that $u$ cannot occur after exactly one $a$. This generates a controllability for the word $ab$ only. Using (4) in Section 3, the supremal controllable sublangauge of $L_m(M)$ for this example is given by

$$L_{clm} = \{w \in L_m(M) \mid \forall u' \subseteq w, u' \neq ab \}$$

(A.1)

$$= L_m(M) \setminus \{ab\} = \{a^n, a^m b, a^k b u | n, m, k > 1\}$$

implying that $L_m(M_3) = \{a^n | n \in \mathbb{N}\}$ is a strict subset of $L_{clm}$ which is an obvious contradiction to (Griffin, 2008, Thm.3.5). Furthermore, $L_{clm}$ in (A.1) cannot be realized using the state and transition structure of $M$ and only deleting existing transitions.

The automatic synthesis of a DPDA realizing $L_{clm}$ for this example is provided as an example within our pushdown-plug-in for libFAUDES (2006-2013).

Appendix B. PROOF OF LEMMA 2

Here we give the proof of Lemma 2.

Proof 2. To simplify notation, we collect all states $q$, reachable by a finite sequence of $\lambda$-transitions from a configuration $(\tilde{q}, w, \tilde{s})$ with $\tilde{q} \in F$ in the set

$$Q_{\text{el}}(M, w) := \{q \in Q \mid \exists f \in D_l(M), n \in \mathbb{N}, \tilde{q} \in F :$$

$$\exists f(n) = (\tilde{e}, (\tilde{q}, w, \tilde{s})) \land \exists m' > n, \lambda (f(n')) = (e, (q, w, s)) \in \Gamma^* \}$$

(i) $L_{\text{um}}(M_{SP}) = L_{\text{um}}(M)$: Let $q \in Q$, $w \in \Sigma^*$, $\gamma \in \Gamma$, $s \in \Gamma^*$ and $(q, w, \gamma; s)$ be an arbitrary configuration reachable
by the initial derivation \( f \in D_I(M) \), implying \( w \in L_{um}(M) \). Observe that the state \( q \) is mapped to the controllable sublanguage of a given language. In SIAM Journal on Control and Optimization, volume 25, 637–659.

Now observe that all states in \( A_\lambda(Q,\Gamma) \cap Q_\lambda(Q_{SP}) \) can only have outgoing \( \lambda \)-transitions, due to the determinism of \( Q \) that is preserved in \( Q_{SP} \). Therefore, we have \( \langle \tilde{q}, \gamma \rangle_s \notin Q_\lambda(Q_{SP}) \) and therefore \( \langle \tilde{q}, \gamma \rangle_s \notin F_{SP} \) by definition. This implies that there exists a derivation \( f' \in D_I(M_{SP}), n'' \in N \) s.t. \( f'(n'') = (h, (p, w, r)) \) s.t. \( p \in F_{SP} \), implying \( w \in L_{um}(M_{SP}) \) and therefore \( L_{um}(M) \subseteq L_{um}(\text{SPLIT}(M)) \). For the proof of \( L_{um}(\text{SPLIT}(M)) \subseteq L_{um}(M) \) observe that if \( w \) is accepted by a state \( (q, \gamma)_r \in F_{SP} \), it follows from (i) and the construction of \( F_{SP} \) that \( w \) is accepted by \( q \in F \) in \( M \). Now let \( w \) be accepted by a state \( (q, \gamma)_s \in F_{SP} \). Then it follows from case (b) in the proof of (i) that there exists some state \( p \in F \) that accepts \( w \), since otherwise, \( (q, \gamma)_s \in F_{SP} \) is not reachable by \( w \). This again gives \( w \in L_{um}(M) \).

Therefore, using induction, we can always construct a derivation \( f' \in D_I(M_{SP}), n'' \in N \) s.t. \( f'(n'') = (e', (q', w, \gamma)) \) giving \( w \in L_{um}(M_{SP}) \) and therefore, \( L_{um}(M_{SP}) \subseteq L_{um}(M) \). Using the fact that the relations in case (a)-(d) only occur, iff there exists a matching relation (B.1) in \( M \) and derivations in \( M_{SP} \) can only be concatenated iff this is possible in \( M \), the construction of single-step relations in \( M_{SP} \) gives the same cases as before, implying \( L_{um}(M) \subseteq L_{um}(M_{SP}) \).

(ii) Show \( L_{um}(M_{SP}) = L_{um}(M) \): Let \( w \in L_{um}(M) \) and \( f \in D_I(M) \), \( n \in N, q \in F \) s.t. \( f(n) = (e, (q, w, \gamma)) \) is the starting configuration in (B.1). If \( \sigma \neq \lambda \) in (B.1), we know from part (i) and cases (a) and (d) that there exists a derivation \( f' \in D_I(M_{SP}), n' \in N \) s.t. \( f'(n') = (e, (q, \gamma)_r, w, \gamma) \) with \( (q, \gamma)_r \in F_{SP} \) (since \( q \in F \) and \( (q, \gamma)_r \notin Q_{\lambda}(M_{SP}) \)), giving \( w \in L_{um}(M_{SP}) \). Now let \( \sigma = \lambda \). Since \( M \in LLF \), there exists \( \sigma' \neq \lambda \) and a finite chain of single-step relations, s.t.

\[
(\bar{e}, (q, w, \gamma)) \vdash^*_M (\bar{e}, (q, w, \gamma)) \text{ or } (B.2)
\]

\[
\vdash_M ((\bar{q}, \sigma', \gamma, \tilde{s}', \tilde{q}'), (q', w, \sigma', \tilde{s}'))
\]

Then we can combine case (b), (c) and (d) from the proof of part (i) to mimic (B.2) by the finite chain

\[
(\bar{e}, ((q, w, \gamma)) \vdash_{M_{SP}} (\bar{h}, ((\bar{q}, \gamma)_s, w, \gamma)) \text{ and } (B.3)) \text{ by the finite chain }
\]

\[
\vdash_{M_{SP}} (((\bar{q}, \gamma)_s, \sigma', \gamma, \tilde{s'}, \tilde{q}'), (q', w, \sigma', \tilde{s}'))
\]

and (B.3) by the finite chain

\[
(\bar{e}, ((q, w, \gamma)) \vdash_{M_{SP}} (\bar{h}, ((\bar{q}, \gamma)_s, w, \gamma)) \vdash_{M_{SP}} \text{.}
\]

10Observe that reaching \( q \) with a different initial derivation \( f' \) might result in a different mapping. E.g., the state \( (p_1, q_2) \) in Figure 3 is mapped to \( \{(p_1, q_2), (p_1, q_2), (p_1, q_2), \} \) and \( \{(p_1, q_2), (p_1, q_2), \} \) when reached by an initial derivation generating the words \( w = ad \) and \( w = ac \), respectively.

REFERENCES


