Intelligent Control and Automation, **2011, 2, 24-30**
doi:10.4236/ica.2011.21003 Published Online February 2011 (http://www.SciRP.org/journal/ica)

α-Siphons of a Suboptimal Control Model of a Subclass of Petri Nets*

Daniel Yuh Chao
Department of Management and Information Systems, National ChengChi University, Chinese Taipei
E-mail: *yuhyaw@ gmail.com*
Received October 12, 2010; *revised January* 9, 2011; *accepted January* 10, 2011

Abstract

It has been a hot research topic to synthesize maximally permissive controllers with fewest monitors. So far, all maximally permissive control models for a well-known benchmark are generalized Petri net, which complicates the system. In addition, they all relied on time-consuming reachability analysis. Uzam and Zhou apply First-met-bad-marking (FBM) method to the benchmark to achieve a near maximal permissive control policy with the advantage of no weighted control (WC) arcs. To improve the state of the art, it is interesting to synthesize optimal controller with as few weighted arcs as possible since it is unclear how to optimize the control for siphon involving WC arcs, This paper explores the condition to achieve optimal controller without WC and defining a new type of siphon, called α-siphon. If the condition is not met, one can apply the technique by Piroddi *et al*. to synthesize optimal controllers with WC.

Keywords: Petri Nets, Siphons, Controllability, FMS, S^3PR

1. Introduction

Petri nets are a popular and powerful formalism to handle deadlock problems in a resource allocation system that is a technical abstraction of contemporary technical systems. Petri nets (PN) have been employed to model FMS to discover that insufficiently marked siphons cause deadlocks [1-4].

Uzam and Zhou [5] propose an iterative approach. At each iteration, a first-met bad marking (FBM) is singled out from the reachability graph of a given Petri net model. The objective is to prevent this marking from being reached via a place invariant of the Petri net. A well-established invariant-based control method is used to derive a control place. This process is carried out until the net model becomes live. The proposed method is generally applicable, easy to use, effective and straightforward although its off-line computation is of exponential complexity. Two FMS are used to show its effectiveness and applicability.

Although reaching 19 states fewer and 6 more monitors than that the optimal one by Piroddi *et al.* for a well-known benchmark, it does not employ weighted control arcs and runs more efficiently. Piroddi *et al.* [6,7] further increase it to the optimal 21581 states using the set covering approach. However, the computation is expensive since the set-covering problem involves a large system of **inequalities with numerous (the number of minimal siphons)** variables. Redundant monitors must be identified based on the method in [8] during each iteration, which entails exponential time complexity. Thus, the computational burden remains high and the method is not applicable to large FMS.

Furthermore, unlike that in [5], quite a few control arcs are weighted rendering the net to be a general Petri net (GPN), which are much harder to analyze than the ordinary control net by Uzam and Zhou. The traditional MIP method cannot be extended to GPN. Hence, Piroddi *et al.* transformed weighted arcs into ordinary ones, which sometimes may cause unnecessary deadlocks as mentioned in [5].

Our approach [9-11] categorizes SMS into basic, compound, control and mixture siphons and derives their controllability. If one carefully selects a sequence of emptiable siphons to add monitors, the number of monitors required can be reduced. Mixture siphons containing nonsharing resource places may be emptiable.

This method does not need to enumerate all minimal siphons, nor to compute the reachability graph. Also no iterations are required and no need to remove redundant

*This work was supported by the National Science Council under Gant NSC 99-2221-E-004-002.

monitors. Hence, the computation burden is much less than those by Uzam *et al.* as well as Piroddi *et al.* In addition, no control arcs are weighted.

However, the resulting model of the well-known S^3PR reaches fewer (21363) states than the one (21562) in [5], but with 11 monitors and 50 control arcs fewer than 19 monitors and 120 control arcs reported in [5].

Without the knowledge of unmarked siphons, Uzam and Zhou employ a simplified generalized mutual-exclusion constraints (GMECs) equivalently setting the number of tokens in the complementary set [*S*] of a siphon *S* fewer than the initial number of tokens in *S* by one. This excludes some live states where the number of tokens in [*S*] may equal the initial number of tokens in *S*. The GMEC by Piroddi *et al.* sets *S* to be always marked and does not cause states to be lost.

To avoid WC while not losing live states, we need to understand why the state loss occurs. An earlier paper helps this by proposing one way to list all lost states and estimating the number of lost states without reachability analysis. Analyzing these state losses, one may find some enhancements to reach more states.

However, it assumes that the siphon responsible for the lost states is known a priori. This paper focuses on developing theory to find the responsible siphon and the conditions where weighted arcs cannot be avoided.

Without theory, one could waste much time failing to reach more states. Thus, it is important to find out the condition where more states can be reached. If no more states can be reached, one simply stop and satisfy with the suboptimal model obtained or to employ weighted control arcs to reach more states following the approach by Piroddi *et al.*

The rest of the paper is organized as follows. Section 2 presents the preliminaries about Petri nets and S^3PR. Section 3 presents different types of siphons: basic, compound, mixture and α-siphons. It shows that only α-siphons siphons are responsible for state losses. Section 4 develops the condition for an α-siphon to incur state losses. Finally, Section 5 concludes the paper.

2. Preliminaries

A *Petri net* (or *Place/Transition net*) is a 3-tuple $N = (P,T,F)$, where $P = \{p_1, p_2, \cdots, p_a\}$ is a set of *places*, $T = \{t_1,t_2, \cdots ,t_b\}$ a set of *transitions*, with $P \cup T \neq \varnothing$ and $P \cap T = \varnothing$ and F a mapping from $(P \times T) \cup (T \times P)$ to non-negative integers indicating the weight of directed arcs between places and transitions. In the special case that the flow relation F maps onto {0, 1}; the Petri net is said to be *ordinary* (otherwise, *general*). $M_0 : P \rightarrow \{0,1,2, \cdots\}$ denotes an *initial marking* whose *ith* component, $M_0(p_i)$, represents the number of tokens in place p_i. *N* is *strongly connected iff* there is a directed path from any node to any other node. A node x in $N = (P, T, F)$ is either a $p \in P$ or a $t \in T$. The post-set of node x is $x^\bullet = \{y \in P \cup T \mid F(x,y) > 0\}$, and its pre-set ${}^\bullet x = \{y \in P \cup T \mid F(y,x) > 0\}$.

t_i is *firable* if each place p_j in ${}^\bullet t_i$ holds no less tokens than the weight $w_j = F(p_j,t_i)$. Firing t_i under M_0 removes w_j tokens from p_j and deposits $w_k = F(t_i,p_k)$ tokens into each place p_k in $t_i^\bullet$; moving the system state from M_0 to M_1. Repeating this process, it reaches *M'* by firing a sequence σ of transitions. *M'* is said to be reachable from M_0; *i.e.*, $M_0 [\sigma > M'$.

$R(N, M_0)$ is the set of markings reachable from M_0. A transition $t \in T$ is live under M_0 if $\forall M \in R(N, M_0)$, $\exists M' \in R(N, M)$, t is firable under *M'*. A transition $t \in T$ is dead under M_0 if $\nexists M \in R(N, M_0)$ where t is firable. A marking $M \in R(N, M_0)$ is a (total) deadlock if $\forall t \in T$, t is dead. A PN is *live* under M_0 if $\forall t \in T$, t is live under M_0.

For a Petri net (N, M_0), a non-empty subset $S(\tau)$ of places is called a *siphon* (*trap*) if ${}^\bullet S \subseteq S^\bullet ({}^\bullet \tau \subseteq \tau^\bullet)$, *i.e.*, every transition having an output (input) place in *S* has an input (output) place in S (τ). If $M_0(S) = \sum_{p \in S} M_0(p) = 0$, *S* is called a *empty siphon* at M_0. A *minimal siphon* does not contain a siphon as a proper subset. It is called a *strict minimal siphon* (*SMS*), if it does not contain a trap.

A *P-vector* (place vector) is a column vector $Y : P \rightarrow Z$ indexed by P where Z is the set of integers. For economy of space, we use $\sum_{p \in P} L(p)p$ to denote a *P*-vector. The *incidence matrix* of *N* is a matrix $[N] : P \times T \rightarrow Z$ indexed by P and T such that $[N]^+ - [N]^-$ where $[N]^+(p, t) = F(t, p)$ and $[N]^-(p, t) = F(p, t)$. We denote column vectors where every entry equals 0(1) by $\mathbf{0}(\mathbf{1})$. Y^T and $[N]^T$ are the transposed versions of a vector Y and a matrix $[N]$, respectively. Y is a *P-invariant* (place invariant) if and only if $Y \neq \mathbf{0}$ and $Y^T [N] = \mathbf{0}^T$ hold. $\|Y\| = \{p \in P \mid Y(p) \neq 0\}$ is the *support* of *Y*. A *minimal P-invariant* does not contain another P-invariant as a proper subset. If a siphon $S \subset \|Y\|$, then $[S] = \|Y\| \setminus S$ is called the *complementary siphon* of *S* and $S \cup [S]$ is the *support* of a P-invariant. Let Y_V be the minimal P-invariant associated with control place *V*. $H(V) = [V] = \|Y_V\| \setminus \{V\}$ is called the *controller* (or *disturbed*) *region or the set of holder places of V*.

Definition 1 [1]: *A simple sequential process* (S^2P) *is a net* $N = (P \cup \{p^0\},T,F)$ *where:* 1) $P \neq \varnothing$, $p^0 \notin P$ (p^0 *is called the process idle or initial or final operation place*); 2) *N is strongly connected state machine* (*SM*) *and* 3) *every circuit C of N contains the place* p^0.

Definition 2 [1]: *A simple sequential process with resources* (S^2PR), *also called a working processes* (*WP*), *is a net* $N = (P \cup \{p^0\} \cup P_R,T,F)$ *so that* 1) *the subnet generated by* $X = P \cup \{p^0\} \cup T$ *is an* S^2P; 2) $P_R \neq \varnothing$ *and* $P \cup \{p^0\} \cap P_R = \varnothing$; 3) $\forall p \in P$, $\forall t \in {}^\bullet p$, $\forall t' \in p^\bullet$, $\exists r_p \in P_R$, ${}^\bullet t \cap P_R = t'^\bullet \cap P_R = \{r_p\}$; 4) *The two following statements are verified:* $\forall r \in P_R$, *a)* ${}^{\bullet\bullet} r \cap P = r^{\bullet\bullet} \cap P \neq \varnothing$; *b)* ${}^\bullet r \cap$

$r^\bullet = \varnothing$. 5) $^{\bullet\bullet}(p^0) \cap P_R = (p^0)^{\bullet\bullet} \cap P_R = \varnothing$. $\forall p \in P$, *p is called an operation* (*or activity*) *place.* $\forall r \in P_R$, *r is called a resource place.* $H(r) = {}^{\bullet\bullet}r \cap P$ *denotes the set of holders of r* (*operation places that use r*). $\boldsymbol{\rho(r) = \{r\} \cup H(r)}$ *denotes the union of* $H(r)$ *and* $\{r\}$ *and is the support of a minimal P-invariant* Y_r *that contains r.*

Definition 3 [1]: *A system of* S^2PR (S^3PR) *is defined recursively as follows:* 1) *An* S^2PR *is defined as an* S^3PR*;* 2) *Let* $N_i = (P_i \cup P_i^0 \cup P_{Ri}, T_i, F_i)$, $i \in \{1,2\}$ *be two* S^3PR *so that* $(P_1 \cup P_1^0) \cap (P_2 \cup P_2^0) = \varnothing$. $P_{R1} \cap P_{R2} = P_C$ ($\neq \varnothing$) *and* $T_1 \cap T_2 = \varnothing$. *The net* $N = (P \cup P^0 \cup P_R, T, F)$ *resulting from the composition of* N_1 *and* N_2 *via* P_C (*denoted by* N_1 *o* N_2) *defined as follows:* 1) $P = P_1 \cup P_2$*;* 2) $P^0 = P_1^0 \cup P_2^0$*;* 3) $P_R = P_{R1} \cup P_{R2}$*;* 4) $T = T_1 \cup T_2$ *and* 5) $F = F_1 \cup F_2$ *is also an* S^3PR. ***A directed circuit in N is called a resource circuit, if*** $\forall p \in \Gamma$, $p \in R$. ***An elementary resource circuit is both a resource and an elementary circuit****.*

3. Types of SMS and Siphon Responsible for Lost States

In [12-14], we show that SMS can be synthesized from resource or core subnets. New types (such as control siphons) of SMS can be synthesized from control subnets formed by control places. If we add monitors to these different types of siphons in a certain order, then some siphons may be redundant.

We construct an SMS based on the concept of handles. Roughly speaking, a "handle" is an alternate disjoint path between two nodes. A *PT-handle* starts with a *place* and ends with a *transition* while a *TP-handle* starts with a *transition* and ends with a *place*. A core subnet can be obtained from an elementary circuit, called *core circuit*, by repeatedly adding handles.

The control place and arcs for siphon *S*, similar to resource places, form a number of elementary circuits. Hence, there is an elementary circuit containing adjacent control places, from which we can synthesize new problematic siphons.

Definition 4: *An elementary resource circuit is called a basic circuit, denoted by* c_b*. The siphon constructed from* c_b *is called a basic siphon. A compound circuit* $c = c_1$ *o* c_2 *o* $\cdots$ c_{n-1} *o* c_n *is a circuit consisting of multiply interconnected elementary circuits* $c_1, c_2, \cdots, c_n$ *such that* $c_i \cap c_{i+1} = \{r_{pi}\}$, $r_{pi} \in R$ (*i.e.,* c_i *and* c_{i+1} *intersects at a resource place* r_i). r_{pi} *is called an* ***inter-place****. The SMS synthesized from compound circuit c* (*resp. control, mixture*) *using the Handle-Construction Procedure in* [9] *is called an n-compound* (*resp. control, mixture*) *siphon S, denoted by* $S = S_1$ *o* S_2 *o* $\cdots$ S_{n-1} *o* S_n*. A siphon is called a resource siphon if it does not contain any control place. The set of compound, control, and mixture siphons for an n-compound siphon is called a family set of siphons of the n-compound siphon.*

Definition 5: *A mixture subnet is obtained by adding non-resourceless TP-handles* (*containing no operation places*) *upon a core circuit. A siphon synthesized from a mixture subnet is called a mixture siphon. A full mixture subnet is a mixture subnet upon which we can no longer add non-resourceless TP-handles to form a larger subnet to synthesize a new siphon. Otherwise, it is called a partial mixture* (*briefed as p-mix*) *subnet. A siphon synthesized from a full* (*resp. partial*) *mixture subnet is called a full* (*resp. partial*) *mixture siphon, briefed as f-mix* (*resp. p-mix*). R_S (*resp.* C_S) *the set of resource* (*resp. control*) *places in S. An α-siphon is a mixture one with non-sharing places.*

For the benchmark in **Figure 1**, S_{11} is an α-siphon (where p_{43} is a non-sharing place.), whose core subnet can be obtained by adding handles $[t_3\ p_{40}\ t_2\ p_{30}\ t_{22}\ V_{11}]$, $[t_{22}\ p_{42}\ t_7\ p_{30}]$, $[t_{20}\ p_{43}\ t_{19}\ p_{32}\ t_5\ V_{16}]$, $[V_{16}\ t_8 V_{11}]$, $[p_{32}\ t_{10}\ p_{43}]$, $[t_{10}\ V_{16}]$, and $[t_8\ p_{42}]$ to Core circuit $c = [V_{16}\ t_3 V_{11}\ t_{20}\ V_{16}]$. $c_1 = [p_{31}\ t_3\ p_{40}\ t_2\ p_{30}\ t_{22}\ p_{42}\ t_{21}\ p_{31}]$, $c_2 = [p_{31}\ t_{20}\ p_{43}\ t_{19}\ p_{32}\ t_5\ p_{41}\ t_4\ p_{31}]$, $c_1 \cap c_2 = \{p_{31}\}$, and $M_0\ \{r_p = p_{31}\} = 1$. **Table 1** lists the controlled model by Uzam *et al.* based on the FBM approach.

In a mixture siphon, $\exists t \in (S^\bullet / {}^\bullet S)$, $|{}^\bullet t \cap S| > 1$, and each firing of *t* may remove multiple (say x) tokens from *S*. This is the reason that the arc from V_S to *t* must be weighted by x if $M_0(V_S) = M_0(S) - 1$. Thus, $M_{max}([S]) < M_0(S)$. In order to avoid empty *S*, one may set $M_0(V_S) = M_{max}([S]) - 1$ with ordinary control arcs.

On the other hand, for a siphon *S* where all non-operation places are resource ones, $\forall t \in (S^\bullet / {}^\bullet S)$, $|{}^\bullet t \cap S| = 1$, each firing of *t* (called sink transitions of the siphon) removes one token from V_S and *S* respectively. Thus, $M_{max}([S]) = M_0(S)$. The same holds true for a control siphon.

Based on the above discussion, there will be no live state losses if $M_0(V_S) = M_0(S) - 1$ for the resource or control siphon since state losses occur iff there are live states *M* such that $M([S]) > M_0(V_S)$(Theorem 1 in [11]). For a mixture siphon to be emptiable, it must be an *α-siphon*.

Lemma 1: *Let S be a siphon in the family set of a 2-compound siphon involved in some state loss, then S must be an α-siphon.*

Proof: The state loss would not occur if no monitor is added to *S*. The thesis holds since there is no state loss if *S* is not emptiable and a mixture siphon is emptiable and needs a monitor iff it is an α-siphon.

Monitor V_{17} is added to S_{11} to make 19 live states to be forbidden and lost via reachability analysis in [2]. In the sequel, we will develop the condition for state loss for an α-siphon since other siphons in the family set of a 2-compound do not incur state loss.

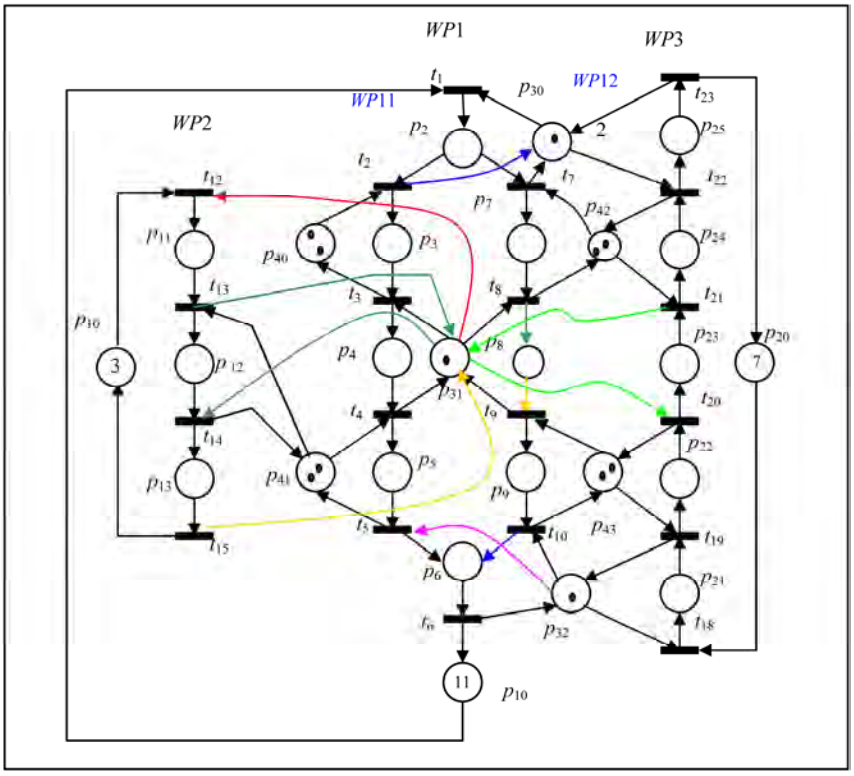

Figure 1. A well-known example of S^3PR [1].

Table 1. Control model by Uzam *et al.* for the benchmark in Figure 1.

i	FBM($M_0(V_i)$)	S	$^\bullet V_i$	$V_i^\bullet$
1	$p_{11} + 2p_{12}(2)$	$\{p_5, p_8, p_{13}, p_{23}, p_{31}, p_{41}\}$	t_{14}	t_{12}
2	$p_4 + 2p_{12}(2)$	S_1	t_4, t_{14}	t_3, t_{13}
3	$2p_7 + p_{23}(2)$	$S_2 = \{p_4, p_8, p_{11}, p_{13}, p_{24}, p_{31}, p_{42}\}$	t_8, t_{21}	t_7, t_{20}
4	$p_8 + 2p_{22}(2)$	$S_3 = \{p_4, p_9, p_{11}, p_{13}, p_{23}, p_{31}, p_{43}\}$	t_9, t_{20}	t_8, t_{19}
5	$2p_7 + p_{22}(3)$	$S_4 = \{p_8, p_{23}, V_2, V_3\}$	t_8, t_{20}	t_7, t_{19}
6	$2p_9 + p_{21}(2)$	$S_5 = \{p_6, p_{22}, p_{32}, p_{43}\}$	t_{10}, t_{19}	t_9, t_{18}
7	$2p_7 + p_8 + p_{21} + p_{22}(4)$	$S_6 = \{p_6, p_{23}, V_3, V_8\}$	t_9, t_{20}	t_7, t_{18}
8	$p_8 + p_9 + p_{21} + p_{22}(3)$	$S_7 = \{p_6, p_{23}, p_{31}, p_{32}, p_{43}\}$	t_{10}, t_{20}	t_8, t_{18}
9	$2p_7 + p_9 + p_{21} + p_{22}(4)$	S_6	t_8, t_{10}, t_{20}	t_7, t_9, t_{18}
10	$p_5 + p_{11} + p_{12} + p_{21} + 2p_{22}(5)$	$S_8 = \{p_6, p_{13}, p_{23}, p_{31}, p_{32}, p_{41}, p_{43}\}$	t_5, t_{14}, t_{20}	t_4, t_{12}, t_{18}
11	$p_2 + 2p_3 + p_7 + p_{23} + p_{24}(5)$	$S_9 = \{p_4, p_8, p_{11}, p_{13}, p_{25}, p_{30}, p_{31}, p_{40}, p_{42}\}$	t_3, t_8, t_{22}	t_1, t_{20}
12	$p_4 + p_5 + p_{12} + p_{21} + 2p_{22}(5)$	S_8	t_5, t_{14}, t_{20}	t_3, t_{13}, t_{18}
13	$p_5 + 2p_7 + p_{11} + p_{12} + p_{21} + 2p_{22}(6)$	$S_{10} = \{p_6, p_{23}, p_{31}, p_{32}, p_{41}, V_2\}$	t_5, t_8, t_{14}, t_{20}	t_4, t_7, t_{12}, t_{18}
14	$p_5 + p_9 + p_{11} + p_{12} + p_{21} + 2p_{22}(5)$	S_8	$t_5, t_{10}, t_{14}, t_{20}$	t_4, t_9, t_{12}, t_{18}
15	$p_4 + p_5 + 2p_7 + p_{12} + p_{21} + p_{22}(6)$	S_{10}	t_5, t_8, t_{14}, t_{20}	t_3, t_7, t_{13}, t_{18}
16	$p_4 + p_5 + p_9 + p_{12} + p_{21} + p_{22}(5)$	S_8	$t_5, t_{10}, t_{14}, t_{20}$	t_3, t_8, t_{13}, t_{18}
17	$p_2 + 2p_3 + p_4 + p_5 + p_7 + p_9 + p_{21} + p_{22} + p_{24}(9)$	$S_{11} = \{p_6, p_{11}, p_{13}, p_{25}, p_{30}, p_{32}, p_{40}, p_{42}, p_{43}, V_8, V_{11}, V_{16}\}$	$t_5, t_8, t_{10}, t_{20}, t_{22}$	t_1, t_9, t_{18}, t_{21}
18	$p_2 + 2p_3 + 2p_5 + p_7 + p_9 + p_{21} + p_{22} + p_{23}(9)$	$S_{12} = \{p_6, p_{11}, p_{13}, p_{25}, p_{30}, p_{32}, p_{40}, p_{43}, V_9, V_{11}, V_{16}\}$	$t_3, t_5, t_8, t_{10}, t_{21}$	t_1, t_4, t_9, t_{18}
19	$p_2 + p_3 + 2p_5 + p_7 + p_8 + p_{21} + p_{22} + p_{24}(9)$	$S_{13} = \{p_6, p_{11}, p_{13}, p_{25}, p_{30}, p_{32}, p_{40}, p_{42}, V_4, V_{11}, V_{16}, V_{17}\}$	$t_3, t_5, t_9, t_{20}, t_{22}$	t_1, t_4, t_{18}, t_{21}

4. Condition for State Loss

To have lost live states, some live states must be forbidden by the addition of Monitor V_S. For states to be live, the α-siphon S must be always marked. For states to be forbidden, the total number of tokens in the complementary set $[S]$ of S must remain at its maximum, which cannot occur in the presence of ordinary V_S. To turn $M(S) > 0$ (live) from $M'(S) = 0$ while maintaining $M([S]) = M'([S]) = M_{max}([S])$ (forbidden), a token must be shifted from one place in $[S]$ to another place in $[S]$. In the sequel, we first deal with liveness of lost states followed by two different cases where state loss may or may not occur.

Lemma 2: *Let S be a siphon and* $M_0(S) > 0$. $M(S) > 0$ $[M \in R(N, M_0)]$, *if no transitions in* $S^\bullet \setminus {}^\bullet S$ *ever fire.*

Proof: Only transitions in $S^\bullet \setminus {}^\bullet S$ can fire to move tokens from S into $[S]$. Transitions in $S^\bullet \cap {}^\bullet S$ fire to move tokens from S into S itself. Hence, the thesis holds.

Observation 1: *Let S be an α-siphon,* $\exists V_{S'} \in S$, $(S^\bullet \setminus {}^\bullet S) \cap V_{S'}{}^\bullet \neq \varnothing$.

For the α-siphon $S = S_{11}$ in **Table 1**, $S^\bullet \cap {}^\bullet S = \{t_1, t_{18}\}$. If t_1 and t_{18} never fire, tokens in S cannot leak out from S. There are 3 $V_{S'}$ in S_{11}: V_8, V_{11} and V_{16}. $S^\bullet \cap {}^\bullet S = \{t_1, t_{18}\}$ and $t_1 \in V_{11}{}^\bullet$, $t_{18} \in V_{16}{}^\bullet$.

Lemma 3: *Let S be an α-siphon,* $\forall V_{S'} \in S$, $M(V_{S'}) = 0$, $M \in R(N, M_0)$. *Then no transitions in* $S^\bullet \setminus {}^\bullet S$ *can ever fire.*

Proof: The thesis holds since all transitions in $V_{S'}{}^\bullet$ are disabled owing to the fact that $M(V_{S'}) = 0$ and $(S^\bullet \setminus {}^\bullet S) \cap V_{S'}{}^\bullet \neq \varnothing$ by Observation 1.

The above lemmas help prove that markings, where an α-siphon is always marked, are live ones.

Definition 6: *Let S be an α-siphon,* $R_C = \{r \mid r \in P_R, r \in R(c_{Si}), c_{Si} \in C_S\}$ *the set of resource places whose holder places are also in that of control places of* C_S *and* $\varpi = R_C \setminus \{r_p\}$, *where* r_p *is an inter-place.* $p' \in H(r_p)$ *is called a skew place.*

Theorem 1: *Let S be an α-siphon,* $M_a(p) = 0$, $M_a(H(p) \cap [S]) = M_0(p)$, $\forall p \in \varpi \cup C_S$, $M_a \in R(N, M_0)$. *Then all transitions in* $S^\bullet$ *are dead.*

Proof: It is easy to see that $M_a(S) = 0$ and all transitions in $S^\bullet$ are dead.

For the example, $C_S = \{V_{11}, V_{16}\}$, $R(V_{16}) = \{p_{31}, p_{32}, p_{41}, p_{43}\}$, $R_C = \{p_{30}, p_{31}, p_{32}, p_{40}, p_{41}, p_{42}, p_{43}\}$, $r_p = p_{31}$, and $\varpi = R_c \setminus \{r_p\} = \{p_{30}, p_{32}, p_{40}, p_{41}, p_{42}, p_{43}\}$, where p_{30}, p_{32}, p_{40}, p_{42}, p_{43} are unmarked under FBM17. $H(r_p) = \{p_4, p_8, p_{23}\}$ and each place in $H(r_p)$ is a skew place. $M_a(p_2) = M_a(H(p_{30}) \cap [S]) = M_0(p_{30}) = 1$, $M_a(p_3) = M_a(H(p_{40}) \cap [S]) = M_0(p_{40}) = 2$, $M(p_{21}) = M_a(H(p_{32}) \cap [S]) = M_0(p_{32}) = 1$, and $M_a(p_7) + M_a(p_{24}) = M_a(H(p_{42}) \cap [S]) = M_0(p_{42}) = 2$, $M_a(p_9) + M_a(p_{22}) = M_a(H(p_{43}) \cap [S]) = M_0(p_{43}) = 2$. Note that $M_a(p) = 0$, $\forall p \in \varpi \cup C_S$. Thus all output transitions of p are dead. The rest transitions are output transitions of p_6, p_{25}, p_4, p_8, p_{23}, which are also dead since $M_a(p_6) = M_a(p_{25}) = M_a(p_4) = M_a(p_8) = M_a(p_{23}) = 0$.

We first add Monitor V', so that $H(V') = \Psi$. This induces dead submarkings (markings restricted to operation places or Ψ) $FBM_a = p_2 + 2p_3 + p_4 + p_5 + p_7 + p_9 + p_{21} + p_{22} + p_{24}$, $FBM_b = p_2 + 2p_3 + 2p_5 + p_7 + p_9 + p_{21} + p_{22} + p_{23}$ and $FBM_c = p_2 + 2p_3 + 2p_5 + p_7 + p_8 + p_{21} + p_{22} + p_{24}$. Monitors V_{17}, V_{18}, and V_{19} (called *induced monitors*) are added with $M_0(V_{17}) = 9$, $M_0(V_{18}) = 9$ and $M_0(V_{19}) = 9$, respectively.

Now Monitor V' is redundant since its controller region $\Psi' = \{p_2, p_3, p_5, p_7, p_9, p_{21}, p_{22}, p_{24}\}$ is a subset of that ($\Psi = \{p_2, p_3, p_4, p_5, p_7, p_9, p_{21}, p_{22}, p_{24}\}$) for Monitor V_{17} by the following lemma.

Lemma 4 [11]: *Let S be an SMS.* $\delta_1 \subset \delta \subset [S]$. $M, M_1 \in R(N, M_0)$ *such that* $M(\delta) = M_1(\delta_1) = M_{max}([S])$, V *and* V_1 *are two monitors added such that* $M_0(V) = M_0(V_1) = M_{max}([S]) - 1$ *and* $[V] = \delta$, $[V_1] = \delta_1$. *Then* V_1 *is redundant.*

δ_1 and δ are the controller regions for Monitors V and V_{11}, respectively. In the sequel, we will prove that when the above redundant monitor appears, there are lost states, and vice versa.

Theorem 2: *Let S be an α-siphon,* Ψ *the set of marked operation places when S is unmarked under* M_a, *and* V_S *is the monitor added to S with* $M_0(V_S) = M_{max}([S]) - 1$ *and* $H(V_S) = \Psi$. *Let* $M_b(p) = M_b(r) = 1$, $M_b(p') = M_a(p') - 1$, $M_b(p^*) = M_a(p^*)$, $\forall p^* \in P \setminus (\{p, p'\}, M_b \in R(N, M_0)$, *where* $p \in H(r_p)$, r_p *an inter-place,* $r \in ({}^\bullet(p^\bullet)) \cap \varpi$, $p' \in p^{\bullet\bullet} \cap H(r)$ *and* M_a *was defined in Theorem* 1. *If* $H(r) \cap [S] = \{p'\}$ *and* $r \notin S$, *then* 1) M_b *is a nonlive marking.* 2) *There are no lost live states iff* $M_b(p') = 0$ *or* $M_0(r) = 1$ *and a monitor has been added to prevent* M_b *from being reached.*

Proof: 1) Among all dead transitions under M_a, only output transitions of r may be enabled under M_b since $M_b(r) = 1$. If $H(r) \cap [S] = \{p'\}$, the only possibly enabled transition is the output transition of both r and p. However, after t fires, it reaches M_a, which is a dead marking. Thus, M_b is a nonlive marking. But t is disabled by V_S since t is the output transition of V_S and $M(V_S) = 0$ ($M_b([S]) = M_a([S]) + M_b(p) - M_a(p) + M_b(p') - M_a(p') = M_a([S])$.

2) First assume a) $M_b(p') > 0$ (or $M_0(r) > 1$). Let $M_c \in R(N, M_0)$ be such that $M_c(p') = M_b(p') + 1$ (*i.e.*, adding a token to p'), $M_c(p^\wedge) = M_b(p^\wedge) - 1$ (to ensure $M_b(V) = 0$), $M_c(p^*) = M_b(p^*)$, $\forall p^* \in P \setminus (\{p', p^\wedge\}$, *where* $p^\wedge \in H(r') \cap H(V)$, $p' \in H(V)$, $V \in S$, $r' \in R_C$.

Then $M(H(r') \cap S) = 1$. By Lemma 2, S remains marked since V is unmarked to disable its output transition in $S^\bullet \setminus {}^\bullet S$. All markings M' where S and all other siphons in the final live controlled net are marked and

$M'(p) = M_c(p)$, $\forall p \in S \cup [S]$. Such states are live as proved below. Assume it necessarily evolves to a deadlock state M^*, then there exist an unmarked siphon under M^*, which violates the fact that all siphons have been controlled.

These states are lost since $M_c(\Psi) = M_b(\Psi) = M_{max}([V_S])$, which are not reachable by Monitor V_S with $M_0(V_S) = M_{max}([S]) - 1$.

Next consider b) $M_b(p') = 0$ (or $M_0(r) = 1$). Ψ now does not include p'. One can no longer add a token to p' to induce $M(H(r') \cap S) = 1$. Thus, there are no lost states. a) and b) together prove the thesis.

For the example, $p' = p_5$, $r = p_{41}$ and $H(r) \cap [S] = \{p'\}$. r has only one output transition t_4 with an input operation place in Ψ. The above theorem indicates that when $M_0(p_{41}) = 1$ (instead of 2 as in **Figure 1**), there will be no loss of good states. V_S is not redundant and cannot be removed for the control.

a) If $M_0(p_{41}) > 1$, then there will be lost live states by adding a token to p_5 so that $M_c(p_5) = M_b(p_5) + 1$. These live states must be such that $M_c(\Psi) = M_{max}(\Psi)$, which are not reachable by adding Monitor V_S to make $M_c(\Psi) < M_{max}(\Psi)$. To make $M_c(\Psi) = M_{max}(\Psi)$, it must be that $M_c(V) = M_b(V) = M_a(V) = 0$, $V = V_{16}$. This leads to $M_c([V_{16}]) = M_0(V_{16}) = 5$ or

$$M_c(p_4) + M_c(p_5) + M_c(p_8) + M_c(p_9) + M_c(p_{21}) + M_c(p_{22}) = M_0(V_{16}) = 5$$

$M_c(p_8) = 0$, implies that

$$\alpha = M_c(p_4) + M_c(p_5) + M_c(p_9) + M_c(p_{21}) + M_c(p_{22}) = 5.$$

Note that the addition of Monitor V_{16} limits α to be no more than 5. However, setting α to 5 may not make S unmarked since some resource place (e.g., p_{43} or p_{32}) in S may be marked ($M_c(S) > 0$) even though V_{16} is unmarked. These states $M_c(S) > 0$ will stay so (and are live as proved above) since transitions in $S^\bullet \setminus {}^\bullet S$ are disabled by output control arcs from unmarked V_{16} **and** V_{11}. Note that V_S is redundant and can be removed.

b) If $M_0(p_{41}) = 1$, then there will be no lost live states since $M_c(p_5) = 0$ and the set Ψ_c of marked operation places under M_c does not include p_5. One can no longer add a token to Ψ_c to make $M_c(S) > 0$. Hence, there are no lost states.

Theorem 3: *Let S be an α-siphon,* Ψ *the set of marked operation places when S is unmarked under* M_a*, and* V_S *is the monitor added to S with* $M_0(V_S) = M_{max}(\Psi) - 1$ *and* $H(V_S) = \Psi$. *Let* $M_b(p) = M_b(r) = 1$, $M_b(p^*) = M_a(p^*)$, $\forall p^* \in P \setminus (\{p, p'\}, M_b \in R(N, M_0), M_b(p') = 0$, *where* $p \in H(r_p)$, $r \in ({}^\bullet(p^\bullet)) \cap \varpi$, $p' \in p^{\bullet\bullet} \cap H(r)$. *If* $r \in S$ *and* $H(r) \cap [S] \supset \{p'\}$, *then* 1) M_b *is a nonlive marking, and* 2) *there are no lost live states by adding a monitor to prevent* M_b *from being reached.*

Proof: 1) Similar to the proof of Theorem 2, the output transition of both r and p is an output transition of V_S (Monitor for S) and disabled by unmarked V_S. Other output transitions t' of r are also disabled as explained here. If $H(r) \cap [S] \supset \{p'\}$, then $\mu = \varphi \setminus \{p'\}$ ($\varphi = (H(r) \cap [S]) \cup \{p\}$) is the complementary set of another siphon S'; the output transition set of $V_{S'}$ (control place for S') contains t'. $M_b(p') = 0$ implies that $M_b(\mu) = M_0(r_p) + M_0(r) - 1 = M_0(r) = M_b(p) + M_b(H(r) \cap [S]) - M_b(p') = M_0(S') - 1 = M_0(V_{S'})$. Thus, $V_{S'}$ is unmarked to disable t' and all possible enabled transitions are dead and M_b is a nonlive marking, which needs a monitor V' with $H(V')$ the set of unmarked operation places in $[S]$.

2) Note that $H(V')$ does not include p' since $M_b(p') = 0$. Since $M_b(\mu \setminus \{p\}) + M_b(r) = M_0(r)$, there is no way to add a token (to reach states forbidden by V') to enable some transition. Hence, such states are nonlive and there are no lost live states.

For the example, there are two possible pairs of (r p p'): 1. (p_{43} p_8 p_9) and 2. (p_{42} p_{23} p_{24}) for the above theorem. For Case 1, $H(r) \cap [S] = \{p_9, p_{22}\} \supset \{p' = p_9\}$. For Case 2, $H(r) \cap [S] = \{p_7, p_{24}\} \supset \{p' = p_{24}\}$. r has more than one output transition (1. t_9, t_{19} and 2. t_7, t_{21}) with an input operation place in Ψ. $\varphi_1 = (H(r) \cap [S]) \cup \{p\} = \{p_8, p_9, p_{22}\}$, $\mu_1 = \varphi_1 \setminus \{p'\} = \{p_8, p_{22}\} = [S_4]$, $\varphi_2 = (H(r) \cap [S]) \cup \{p\} = \{p_7, p_{23}, p_{24}\}$, $\mu_2 = \varphi_2 \setminus \{p'\} = \{p_7, p_{23}\} = [S_3]$.

The corresponding submarkings are $\mathrm{FBM_b} = p_2 + 2p_3 + 2p_5 + p_7 + p_9 + p_{21} + p_{22} + p_{23}$ ($M_b(p') = M_b(p_{24}) = 0$) and $\mathrm{FBM_c} = p_2 + 2p_3 + 2p_5 + p_7 + p_8 + p_{21} + p_{22} + p_{24}$($M_b(p') = M_b(p_9) = 0$),respectively. Thus, the set Ψ_b of marked operation places under M_b does not include p'. One cannot add a token to a skew place inΨ_b to make $M_c(S) > 0$. Hence, there are no lost states. Combining Theorems 2 and 3, we have

Theorem 4: *Let S be an α-siphon and all necessary monitors have been added such that there are no marked set* Ψ ($\Psi \subset S$) *of operation places with dead output transitions. Then there are no lost live states iff* $M_b(p') = 0$ *for all possible* p' (*defined in Theorem* 3).

Proof: Theorems 2 and 3 consider all cases where $H(r) \cap [S] = \{p'\}$ and $H(r) \cap [S] \supset \{p'\}$, respectively. Theorem 2 proves that there are no lost live states *iff* $M_b(p') = 0$ for all possible p'. Theorem 3 proves that if $M_b(p') = 0$, then M_b is a nonlive marking and there are no lost states. Similar to the proof for Theorem 2, one can show that if there are no lost states, then it must be that $M_b(p') = 0$. All cases have been considered and the thesis is proved.

In summary, this section develops the condition for a mixture siphon S to be involved in reaching fewer live states. After adding a monitor V_S to S, new unmarked siphons may be generated. One new set of unmarked operation places may cover $H(V_S)$ of V_S, as a proper subset. This makes V_S redundant and some live states lost.

The physics of loss of live states is as follows. Adding a token to a skew place (e.g., p_4 in **Figure 1**) of S reduces

a token in the holder set (e.g., p_{21} in **Figure 1**) of a resource place r (e.g., p_{32} in **Figure 1**) in S, which in turn induces a token in r, thus making S marked. Such a state is live and forbidden since the total number of tokens in ψ' remains unchanged.

5. Conclusions

This paper enhances an earlier paper (which estimates the number of lost states without reachability analysis) and develops theory to identify the siphon responsible for lost states for a well-known benchmark and explores the condition to achieve optimal controller without WC. If the condition is not met, one can apply the technique by Piroddi *et al*. to synthesize optimal controllers with WC. Future work should be addressed to synthesize suboptimal controller without WC when the condition cannot be satisfied.

6. References

[1] J. Ezpeleta, J. M. Colom and J. Martinez, "A Petri Net Based Deadlock Prevention Policy for Flexible Manufacturing Systems," *IEEE Transactions on Robotics and Automation*, Vol. 11, No. 2, 1995, pp. 173-184. doi: 10.1109/70.370500

[2] Z. W. Li, J. Zhang and M. Zhao, "Liveness-Enforcing Supervisor Design for a Class of Generalized Petri Net Models of Flexible Manufacturing Systems," *IEE Proceedings Control Theory & Applications*, Vol. 1, No. 4, 2007, pp. 955-967. doi:10.1049/iet-cta:20060218

[3] C.-F. Zhong and Z.-W. Li, "Design of Liveness-Enforcing Supervisors via Transforming Plant Petri Net Models of FMS," *Asian Journal of Control* (*Special Issue on the Control of Discrete Event Systems*), Vol. 6, No. 2, 2010, pp. 270-280.

[4] J. W. Guo and Z. W. Li, "A Deadlock Prevention Approach for a Class of Timed Petri Nets Using Elementary Siphons," *Asian Journal of Control*, Vol. 12, No. 3, 2010, pp. 347-363. doi:10.1002/asjc.189

[5] M. Uzam and M. C. Zhou, "An Iterative Synthesis Approach to Petri Net Based Deadlock Prevention Policy for Flexible Manufacturing Systems," *IEEE Transactions on Systems, Man, and Cybernetics A*, Vol. 37, No. 3, 2007, pp. 362-371. doi:10.1109/TSMCA.2007.893484

[6] L. Piroddi, R. Cordone and I. Fumagalli, "Selective Siphon Control for Deadlock Prevention in Petri Nets," *IEEE Transactions on Systems, Man, and Cybernetics A*, Vol. 38, No. 6, 2008, pp. 1337-1348. doi:10.1109/TSMCA.2008.2003535

[7] L. Piroddi, R. Cordone and I. Fumagalli, "Combined Siphon and Marking Generation for Deadlock Prevention in Petri Nets," *IEEE Transactions on Systems, Man, and Cybernetics A*, Vol. 39, No. 3, 2009, pp. 650-661. doi:10.1109/TSMCA.2009.2013189

[8] M. Uzam, Z. W. Li and M. C. Zhou, "Identification and Elimination of Redundant Control Places in Petri Net Based Liveness Enforcing Supervisors of FMS," *International Journal of Advanced Manufacturing Technology*, Vol. 35, No. 1-2, 2007, pp. 150-168. doi:10.1007/s00170-006-0701-5

[9] D. Y. Chao, "Improvement of Suboptimal Siphon- and FBM-Based Control Model of a Well-Known S^3PR," *IEEE Transactions on Automation Science and Engineering*, Vol. 8, 2011.

[10] Y.-Y. Shih and D. Chao, "Sequence of Control in S^3PMR," *Computer Journal*, Vol. 53, No. 10, 2010, pp. 1691-1703. doi:10.1093/comjnl/bxp081

[11] D. Chao and G. J. Liu, "A Simple Suboptimal Siphon-Based Control Model of a Well-Known S^3PR," *Asian Journal of Control*, December 2010. http://onlinelibrary.wiley.com/doi/10.1002/asjc.292/full

[12] D. Y. Chao, "Computation of Elementary Siphons in Petri Nets for Deadlock Control," *Computer Journal*, Vol. 49, No. 4, 2006, pp. 470-479. doi:10.1093/comjnl/bxl019

[13] D. Y. Chao, "A Graphic-Algebraic Computation of Elementary Siphons of BS^3PR," *Journal of Information Science and Engineering*, Vol. 23, No. 6, 2007, pp. 1817-1831.

[14] D. Y. Chao, "Incremental Approach to Computation of Elementary Siphons for Arbitrary S^3PR," *IEE Proceedings Control Theory & Applications*, Vol. 2, No. 2, 2007, pp. 168-179.

