15th Triennial World Congress, Barcelona, Spain

NET TRANSFORMATION AND THEORY OF REGIONS FOR OPTIMAL SUPERVISORY CONTROL OF PETRI NETS

Asma Ghaffari, Nidhal Rezg and Xiaolan Xie

INRIA and LGIPM, ISGMP-ILE DU SAULCY
57045 METZ CEDEX, FRANCE

Abstract: In a previous work, we applied the theory of regions to design optimal Petri net controller by adding so-called control places to the plant Petri net model with uncontrolable transitions and forbidden states. Unfortunately, such a simple control-place-based solution does not always exist. In the present paper, we propose a new approach for designing optimal controller for ordinary bounded Petri nets using control places. The key idea consists in transforming the plant Petri net model, for which a control-place-based solution was not found, into a safe Petri net. Then, exploiting the result stating that forbidden state problems of safe Petri nets always have control-place-based solutions, the control problem of the transformed model is optimally solved using our previous result. Besides, by assigning a priority to transitions of the transformed model, the complexity is considerably reduced.

Keywords: Discrete event systems, Petri nets, Supervisory control, Manufacturing systems, Optimal control.

1. INTRODUCTION

Forbidden state problem of discrete event systems is one of the control problems that has triggered great interest. In particular, it was shown that if the set *L* of legal markings is expressed by a set of n_c linear inequality constraints (or General Mutual Exclusion Constraints: GMEC) and if *L* is controllable, i.e., from any marking $m \in L$ no forbidden marking is reachable by firing a sequence containing only uncontrollable transitions, then a Petri net based solution exits and is maximally permissive (Basile and al. 1998). Otherwise, general forbidden marking constraint may be enforced by PN-based controller only if the Petri net model of the system is safe (Basile and al. 1998) (Giua, DiCesare and Silva 1993).

Yamalidou et al. (1996) used place invariants to compute, with matrix multiplication, feedback controller that enforces GMEC's, they perform transformations on the system's specifications to obtain constraints in the desired form. The Petri net controller is defined by its incidence matrix. The approach is maximally permissive except when the constraints are written in terms of the firing vector. Moody et al. (1996) extend the use of the concept of Petri net place invariants to nets with uncontrollable and unobservable transitions, but in this case the maximally permissiveness cannot be guaranteed.

We have already addressed the forbidden state problem of bounded Petri (PN) nets with uncontrollable transitions (Ghaffari and al. 2001), and we have proposed an optimal solution method that uses the theory of regions. The controller is a set of control Petri net places. We call such a control PN control or PN solution of the control problem. When added to the Petri net model of the plant, control places ensure a live and maximally permissive behavior of the closed loop system with respect to the forbidden states or markings. The controller design has a linear complexity in the number of systm states.

However, there are cases where such PN controller does not exist. Notably, when the set of legal markings is not convex, there does not exist any PN place that can forbid the reachability of bad markings when allowing all legal ones.

In the present work, we propose an extension of the aforementioned approach to design optimal PN controllers, even when the set of legal markings is not convex. The key idea is to transform the PN model of the plant into a safe model. Then, based on the known result stating that forbidden state problems of safe PN's always have PN solutions, the control problem is optimally solved using our previous work. The transformation technique is based on replacing the places of the original net by paths of binary places. Further, a priority structure is assigned to transitions of the transformed model making the complexity increase only linearly w.r.t. the original state space.

The paper is organized as follows. The following section gives an overview of the design of live and maximally permissive PN controllers using the theory of regions. An example of control problem unsolvable with Petri net places is also provided. Section 3 presents the principle of the transformation of ordinary bounded Petri nets into so-called essentially safe Petri nets, proves the control existence for such nets and gives the control mechanism of the initial net through the transformed net. The problem complexity is considerably reduced by introducing in section 4 the concept of prioritized transformed net.

2. OPTIMAL SUPERVISORY CONTROL USING THE THEORY OF REGIONS

This section briefly presents the controller design method we already proposed (Ghaffari and al. 2001). The controller synthesis using the theory of regions consists of two main steps. The first step determines the desired behavior of the controlled system. The theory of regions is used in the second step to compute control places that will optimally realize the desired behavior.

2.1. Computing the controlled behavior

Let (N, M_0) be the Petri net model of the plant to control, M_0 being its initial state. The set of transitions is portioned into two subsets: T_u is the set of uncontrollable transitions and T_c is the set of controllable transitions. Let (N_c, M_0) be the controlled Petri net we look for and R_c its reachability graph.

The desired behavior computation is mainly based on a state space search and a Ramadge-Wonham-like reasoning. It can be summerized by the following steps.

1. Identify the set of forbidden markings for which the control specifications do not hold
2. Generate the partial reachability graph of the plant model $R_p(N,M_0)$: From M_0, reachable markings are computed step by step. At a state M, if M is a forbidden marking, then no successors are developed for M.
3. Identify the set M_D of dangerous markings, markings that lead to forbidden markings by uncontrollable transitions.

To respect both liveness and control specifications, the reachability graph R_c of the controlled net N_c should be a *strongly connected graph* included in $R_p(N,M_0)$ – M_D and containing M_0. Further, any transition leaving the set R_c should be controllable.

4. Derive the legal and live behavior R_c by computing the largest strongly connected sub-graph of $R_p(N,M_0)$ – M_D containing M_0 such that any state transition yielding outside R_c corresponds to the firing of a controllable transition.

So, to restrict the behavior of the controlled system to the graph R_c, the controller has to prevent any state transition (M,t), that transforms a legal marking M of R_c into a marking outside R_c by firing a controllable transition t. Let Ω be the set of these state transitions which will be called the set of *event separation instances*. Now, given markings in R_c and the set Ω, the theory of regions will be used to design the set of control places, if it exists.

2.2. Control places design using the theory of regions

The theory of regions was initially proposed to synthesize a bounded Petri net from a given finite reachability graph (Badouel and al. 1995). In a supervisory control problem, rather than reconstruct a whole net model for the controlled system, it is question of computing a convenient set of places $\{p_c\}$ to add to the original plant model to act as a controller. This section shows how to adopt the principle of the theory of regions to compute PN controllers.

Consider a new control place p_c to add to the uncontrolled model. Every marking M in the legal behavior R_c must still be reachable after the addition of p_c which implies that p_c has to satisfy the reachability conditions, i.e.:

$$M(p_c) = M_0(p_c) + C(p_c,\cdot)\vec{\Gamma}_M \geq 0, \quad \forall M \in R_c \qquad (1)$$

where Γ_M is any non oriented path in R_c from M_0 to M.

Similarly, each place p_c should satisfies cycle equations for cycles in R_c, i.e.

$$\sum_{t \in T} C(p_c,t) \cdot \vec{g}[t] = 0, \quad \forall g \in S_c \qquad (2)$$

where S_c is the set of basis cycles of the reachability graph R_c.

On the other hand, as it is explained in the previous subsection, to obtain R_c from initial reachability graph $R(N,M_0)$, only event separation instances of the set Ω need to be forbidden. Event separation conditions of Ω have to be solved, each by the addition of a control place p_c. This means that the number of new places to add is at most equal to, in practice much smaller than, the number of state transitions to inhibit.

Hence, each place p_c to add solves at least one event separation instance (M,t) in Ω, i.e.:

$$M_0(p_c) + C(p_c,\cdot)\vec{\Gamma}_M + C(p_c,t) < 0 \qquad (3)$$

The relations (1),(2) and (3) allow to determine the control place p_c((M,t)).

The following algorithm summarizes the controller computation using the theory of regions.

Algorithm 1: Petri net controller synthesis
Given a Petri net plant model (N,M_0) and a control specification.

1. *Determine the set of forbidden markings M_F.*
2. *Generate the partial graph $R_p(N,M_0)$.*
3. *Determine M_D by exploring $R_p(N,M_0)$ backward from markings in M_F. Let R_c be the reachability graph derived from $R_p(N, M_0)$ by removing markings in M_D.*
4. *If R_c is strongly connected, then goto step 9. Otherwise goto step 6.*
5. *Compute the SCC (Strongly Connected Component) of R_c that contains M_0.*
6. *Compute $M_b = \{M \mid \exists \sigma \in T_u^*$ s.t. $M[\sigma > M' \wedge M \in SCC \wedge M' \notin SCC\}$*
7. *Remove all markings in M_b from R_c and go to step 5.*
8. *Set R_c as the legal behavior, M_L the set of markings in R_c, and Ω the set of event separation instances (M,t) (where $M \in R_c$, M[t>M' and $M' \notin R_c$).*
9. *Solve repeatedly the linear system defined by relations (1), (2) et (3) for each event instance (M,t) in Ω. Let $(M_0(p_{c(M,t)}),C(p_{c(M,t)}, .))$ be the solution defining the new control place $p_{c(M,t)}$ if it exists.*
10. *Remove redundant control places and return the resulting controlled net $(N_c,M_0) = (N,M_0) \cup \{(p_{c(M,t)},M_0(p_{c(M,t)})) \mid (M,t) \in \Omega\}$.*

The control synthesized by algorithm 1 is optimal in the sense of maximally permissiveness (Ghaffari and al. 2001).
But, there are examples where some event separation instances cannot be solved by any control place. Consider for instance the net of figure 1, where only t1 and t2 are controllable. The single constraint to enforce is to keep the marking of p3 no more than 1 token. This control problem cannot be optimally solved by means of Petri net places.

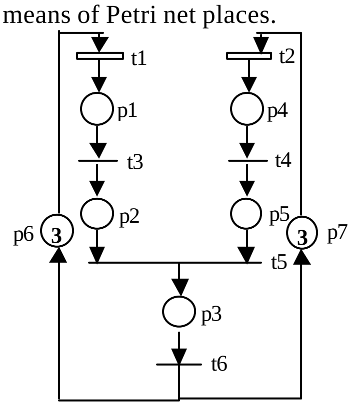


Figure 1: Example

Such situations motivated us to more investigate on forbidden state problems with uncontrollable transitions.

3. TRANSFORMATION FOR CONTROL OF ORDINARY BOUNDED PETRI NET

We define the transformation of ordinary bounded Petri nets into so-called *essentially* safe Petri nets, so that we can circumvent the difficulty of PN control existence. Indeed, similarly to safe nets, we claim that control problem for essentially safe nets always has PN solutions. Moreover, it is shown in the following that the determination of the control decision for the transformed net leads simply to the control decision to apply to the original net. The counterpart of this interesting result is the exponential growth of the reachability graph size.

3.1 Essentially safe nets

First, we will distinguish in a Petri net model two sets of places:

- R: is the set of resource places which represent the availability of system resources.
- S: is the set of state places which correspond to system states.

More formally, we define resource places as following:

Definition 1:
A place r of a Petri net model is a resource place, if there exits at least one p-invariant π such that $\pi[r] > 0$ and any other place s with $\pi[s] > 0$ is a state place.

As a result, if we assume given the markings of all the state places of a net, then, the determination of the global marking of the net is straightforward.

Definition 2:
An essentially safe net is a Petri net such that all state places are safe.

The Petri net of figure 2.b is essentially safe with P_1, p^1_2, p^2_2 and P_3 as state places and P_5, p^1_6 and p^2_6 as resource places.

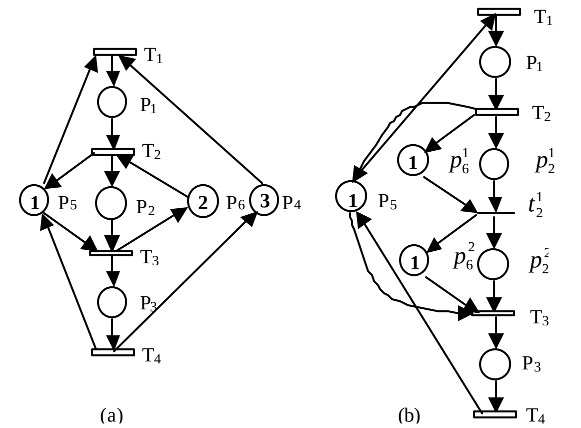
Theorem 1
Any forbidden state problem of an essentially safe Petri net with uncontrollable transitions can always be optimally solved by adding control places.

3.2. Transformed Petri nets

To derive an essentially safe net from any given bounded Petri net model, each state place P of the original net is replaced by a path of transitions and binary places $p_1t_1p_2\ldots t_{n-1}p_n$ that will be denoted by FIFO(P), such that °P = °p_1 and P° = p_n° and for any i, $t_i = p_i° = p_{i+1}°$, where °s (resp. s°) is the input (resp. output of s). A dual place p'_i constrains to one the capacity of any place p_i belonging to FIFO(P). Transitions (resp.places) of a path FIFO are called FIFO-transitions (resp.FIFO-places) and will be denoted by lower-case letters, while original places and transitions are in upper-case letters. We assume that the FIFO-transitions are uncontrollable.

Clearly, the number *n* of places in FIFO(P) is the maximum number of tokens that P can contain in the original model, since the net is bounded. Moreover, the place P may be subject to some control constraints, that is, its capacity in the controlled net may not exceed a given bound. As a result, *n* is the maximum number of tokens that P can contain in the original model under control specifications.

Example:



original transition —— FIFO-transition

Figure 2: a. A Petri net model.b. The corresponding essentially safe model.

Consider the net of figure 2.a. The unique forbidden state is the deadlock marking $(1,2,0,0,0,0)^T$. To transform the net, only P_1, P_2 and P_3 will be replaced. To proceed, the upper bound of the marking of each state place under specifications has to be determined. We have:

Max $(M(P_1))$ = Max $(M(P_3))$ =1 and Max $(M(P_2))$ = 2. So, P_1 and P_3 have already a capacity of one unit whereas P_2 has to be replaced by the sequence $FIFO(P_2) = p^2{}_1 t^2{}_1 p^2{}_2$. The resource places P_4 and P_6 becomes redundant and are removed in the transformed model.

Consider again the example of figure 2. Let M be any marking of the original model corresponding to one token in P_2. In the transformed model, the same situation corresponds to two markings M'1 and M'2 according to whether $p^2{}_1$ or $p^2{}_2$ is marked. We say that M'1 as well as M'2 are *equivalent* markings of M.

Definition 3:

A marking M' of the transformed model N' is an equivalent marking of a marking M of the original model N if, for any state place P of N, we have M(P) = M'(FIFO(P)) = $\sum_{p_i \in FIFO(P)} M'(p_i)$.

Clearly the reachability graph of the transformed net consists of and only of all equivalent markings of markings in the original reachability graph. Each state transition (M1,M2) in the reachability graph of the original model is transformed into a set of paths connecting equivalent markings of M1 and M2.

3.3 Control of the transformed net

Since the transformed net is an essentially safe Petri net, the existence of PN control solution is ensured by theorem 1.

Concerning the control design using the theory of regions, as shown in section 2, two steps are to be performed. The first one consists in the computation of the legal behavior. Naturally, the legal behavior of the transformed net is the set of equivalent markings of original legal markings. The computation phase is exactly the same, based on the reachability graph of the transformed model. This step leads to the definition of legal markings and the set of event separation instances to solve. Note that, for each event separation instance (M,T) of the original net corresponds a set of instances {(M',T)} where M' are the equivalent markings of M in the transformed model.

The second step is the determination of the control places to add to the transformed model. It is led exactly as detailed in steps 9 and 10 of algorithm 1.

3.4. Relationship between the transformed net control and the original net control

Theorem 2

There exists a control place that solves an event separation instance (M,T) in the original Petri net model if and only if there exists one control place that solves the instances (M',T) for any equivalent marking M' of M in the transformed model.

The proof of this theorem is omitted here. This result implies that, if it is proved that there is no solution for an event separation instance of the original net, then, the instances corresponding to the equivalent markings are solved by at least two control places.

Example:

Consider the net of figure 3.a. All transitions are controllable. Assume that T has to be prevented from firing at a marking M, such that M(P) = 1, and allowed to fire at M1 and M2, such that M1(P) = 0 and M2(P) = 2. There does not exist any PN controller that can separate the event instance (M,T), because the set of markings at which T is allowed is not convex. But, if we proceed to the transformation of the given net into a safe one according to the principle given above (figure 3.b), the specification is equivalent to forbid the event instances (M'_1,T) and (M'_2,T), where M'_1 is the equivalent marking of M corresponding to one token in p_1, and M'_2 is the equivalent marking of M corresponding to one token in p_2. Now, it becomes possible to satisfy the specification by the addition of two control places c1 and c2 as shown in figure 4. Note that there is no control of the transformed net with only one control place

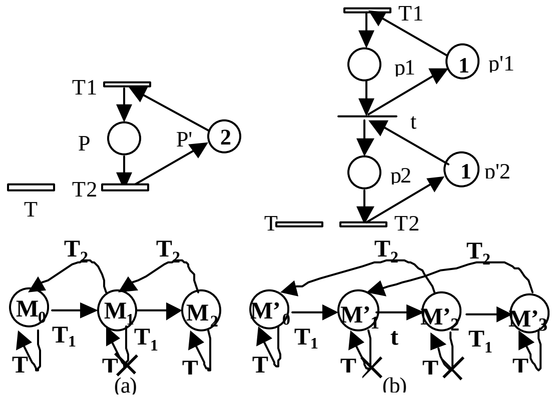


Figure 3: a. The original model and the corresponding reachability graph. b. The transformed model and the corresponding reachability graph.

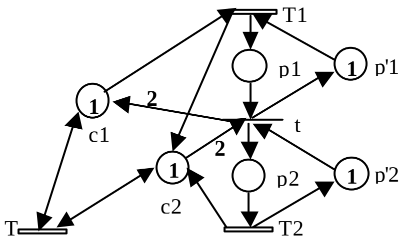


Figure 4: The controlled transformed model

The following algorithm makes clear how the decision control is taken for the original model through the control of the transformed model.

Algorithm 2: Control decision mechanism for the original net

Given an original net N, its transformed net N' under the control C. Let M be the current marking of N and M' its equivalent current marking of N'.

1. *Determine the set* ***P*** *of enabled transitions in N.*
2. *Fire FIFO-transitions till all transitions in* ***P*** *become enabled in the uncontrolled transformed model. Let* ***P'*** *be the set of transitions in N' enabled under the control C.*
3. *Let t be an arbitrary element of* ***P È P'****.*
    - 3.1. *If t* ***Î P'*** *but t* ***Ï P****, t is a FIFO-transition of N', fire t in N' and goto step 4.*
    - 3.2. *If t* ***Î P*** *but t* ***Ï P'****, t is an original transition that is prevented by the control C, so eliminate t from* ***P È P'*** *and goto step 3.*
    - 3.3. *If t* ***Î P Ç P'****, fire t in N and in N' and goto step 4.*
4. *Update the markings of N and N' and goto step1.*

Clearly, the price to pay for always having PN solution is the high number of markings and event separation instances to consider, as the result of the net transformation. The reachability graph size of the original model may increase exponentially when transformed into an essentially safe net. Consequently, the number of control places needed to solve the problem is likely to be great too.

4. PRIORITIZED TRANSFORMED NET

In the previous section, we highlighted one major drawback of the net transformation into essentially safe net, which is the exponential growth of the reachability graph size. To get around this difficulty, we introduce in the present section the concept of prioritized transformed net. The existence of PN control places is always ensured, and the control problem complexity is considerably reduced.

4.1. The priority concept

By transforming an ordinary bounded Petri net into an essentially safe net, we insert in a state transition of the reachability graph some additional sequences. As a result, there may be many ways to get from one node to another node according to the order in which transitions are fired.

However, it is possible to reduce the number of sequences between two nodes, and hence the number of equivalent markings if we assume that FIFO-transitions have higher priority over original transitions and a total order of priority is associated to FIFO-transitions.

Definition 4:
A firing transition priority associated to a transformed net is a map h that assigns to each net transition t a non negative integer h(t), such that:

a. $h(T) = 0$ for all original transitions T;
b. $h(t) > 0$ for all FIFO-transitions t;
c. $h(t) \neq h(t')$ for any two FIFO-transitions t and t'.

Defintion 5:
A prioritized transformed net is a transformed net with a firing transition priority h as defined in definition 4.

So, in a prioritized transformed net, any FIFO-transition has always the priority to be fired before any original transition. For the example of figure 3, the reachability graph of the prioritized transformed net is the same as that of the net without priority (figure 3.b). The marking M'_1 is said instable and will be called *instable* marking, whereas markings M'_0, M'_2 and M'_3 are called *stable* markings.

Definition 6:
A marking M is a stable marking if there does not exist any FIFO-transition enabled at M. Otherwise it is an instable marking.

In other terms, a stable marking is reached in the transformed net when all tokens are moved as far as possible in FIFO(P) for any original state place P.

Let M_1 and M_2 be two markings in the original model of figure 2.a such that $M_1 = (1,0,0,2,0,2)^T$ and M_2 is obtained by the firing of T_2 from M_1. According to the definition above, the stable equivalent marking of

M_1 in the transformed net (fig. 2.b) is M'_1 such that there is one token in P_1. After firing T_2, M'_2, the stable equivalent marking of M_2 is reached when the token is moved to $p^2{}_2$.

4.2. Control of prioritized transformed net

The reachability graph of the prioritized transformed net has too important features. First, each marking of the original net has one and only one stable equivalent marking. Second, event separation instances related to instable markings need not be considered as a result of the priority structure.

Theorem 3
Forbidden state problem of prioritized transformed net always has optimal PN solution.

Based on the existence result stated above, we can define the control design for prioritized transformed nets. According to the definition of these nets, we can already claim that the problem complexity increases only lineraly with respect to the original state space.

So, assume given the reachability graph of the prioritized transformed model, generated according to the corresponding firing transition priority. The controlled behavior and the event separation instances are identified and control places are synthesized using algorithm 1.

It is worth noticing here that the number of event separation instances to solve is exactly the same as for the original problem. Indeed, to an event separation instance (M,T) of the original model corresponds the event separation instance (M',T) where M' is the equivalent stable marking of M in the prioritized transformed model.

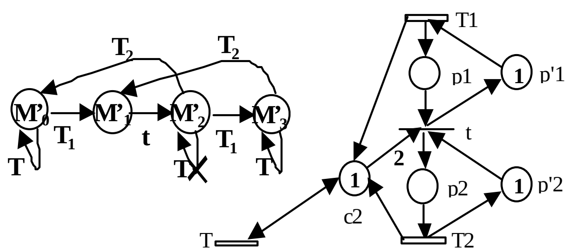


Figure 5: The solution of the example of figure 3 using the prioritized transformed model.

Let us solve the control problem of figure 3 by using the concept of transition priority. There is only one event separation instance (M'_2,T) solved by the control place c2 (see figure5), instead of two event separation instances without priority (figure 4).

The following theorem states that the control of the prioritized transformed net is just equivalent to the original net control.
Theorem4
Any controllable transition in the original model is control-disabled at a marking M if and only if it is control-disabled at the stable marking M' corresponding to M.

5. CONCLUSION

The work presented in this paper is the extension of an approach we already proposed for the design of maximally permissive and live PN control for forbidden state problems with uncontrollable transitions. The main idea consists in transforming the plant Petri net model, for which a PN solution was not found, into a safe Petri net. Then, exploiting the result stating that forbidden state problems of safe Petri nets always have PN solutions, the control problem of the transformed model is optimally solved using our previous result. Further, thanks to the concept of prioritized transformed net, the problem complexity increases only linearly w.r.t. to the original state space. The transformation technique introduced in this paper is applicable to generalized nets and nets with self-loops. Current investigations concern the study of the relationship that may exist between the priority structure assigned to the transformed net and the control solution quality. We are also focusing on reducing the problem complexity.

REFERENCES

F. Basile, P. Chiacchio and A. Giua, "*Supervisory control of Petri nets based on suboptimal monitor places*", Proc. WODES'98, Sardinia, Italy, pp.85-87, 1998.

E. Badouel, L. Bernardinello and P. Darondeau, "Polynomial algorithms for the synthesis of bounded nets", Proceedings of CAAP'95, Springer Verlag LNCS 915 (364-378), 1995.

A. Ghaffari, N. Rezg and X. Xie, "Live and maximally permissive controller synthesis using the theory of regions", SCODES'01, Paris, july 2001.

A. Ghaffari, N. Rezg and X. Xie, "Conception du superviseur optimal vivant à l'aide de la théorie des régions", MSR'01, Toulouse, France, october 2001.

A. Giua, F. DiCesare and M. Silva, "Petri net supervisors for generalized mutual exclusion constraints ", Proc. 12th IFAC World Congress, Sidney, Australia, July 1993, pp. I: 267-270.

J. O. Moody, M. Lemmon and P. Antsaklis, "Supervisory control of Petri nets with uncontrollable/unobservable transitions", Proc. Of the 35th IEEE CDC, Kobe, Japan, 1996.

K. Yamalidou, J. Moody, M. D. Lemmon and P. J. Antsaklis, "Feedback Control of Petri Nets Based on Place Invariants," Automatica, Vol 32, No 1, pp 15-28, January 1996.