Comments on "Maximally permissive supervisor synthesis based on a new constraint transformation method"

Ziyue Ma, Zhiwu Li, and Alessandro Giua

August 24, 2014

Abstract

This note shows by means of simple counterexamples that some key results presented by Luo *et al.* on the synthesis of maximally permissive supervisors based on the *Uncontrollable Transition Gain Transformation* method are incorrect. As a result, the transformation of inadmissible generalized mutual exclusion constraints for Petri nets is still an open issue.

Published as:

[Z. Y. Ma, Z. W. Li, A. Giua, "Comments on 'Maximally Permissive Supervisor Synthesis Based on a New Constraint Transformation Method'," *Automatica*, Vol. 51, pp. 131-134, **2015**.]
DOI: 10.1016/j.automatica.2014.10.099.

Ziyue Ma is with School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (Email: maziyue@gmail.com).

Z. Li is with the School of Electro-Mechanical Engineering, Xidian University, Xian 710071, China, and with the Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: zhwli@xidian.edu.cn; systemscontrol@gmail.com).

A. Giua is with the School of Electro-Mechanical Engineering, Xidian University, Xian 710071, China, with the Aix Marseille Université, CNRS, ENSAM, Université de Toulon, LSIS UMR 7296, Marseille 13397, France, and with DIEE, University of Cagliari, Cagliari 09124, Italy (e-mail: alessandro.giua@lsis.org; giua@diee.unica.it).

1 Introduction

Recently, Luo *et al.* have presented an original approach to design maximally permissive supervisors [2] for Petri nets. In their approach, an algorithm based on an efficient iterative method is presented to transform a given *generalized mutual exclusion constraint* (GMEC) [1,3] which is not admissible into a set of admissible GMECs, the disjunction of which is equivalent to the original constraint.

In this note, we show through a series of counterexamples that some key results in [2] are incorrect. Although we believe that the transformation of an inadmissible GMEC into an equivalent set of admissible constraints is an interesting and potentially fruitful technique for Petri net control, the GMEC transformation problem in arbitrary Petri nets remains open.

In the the rest of the paper, for consistency we use the term *GMEC* to refer to the *linear constraint* in [2].

2 Counterexample for Theorem 2 in [2]

A fundamental result in [2], from which all subsequent results are derived, is Theorem 2 that shows how an inadmissible GMEC $(\mathbf{w},k)$ can be transformed into a disjunction of equivalent GMECs $\bigvee(W)$.

The notion of equivalence used in [2] implies that the sets of admissible markings of the original and transformed constraints are identical, i.e., $\mathscr{A}_{(\mathbf{w},k)} = \mathscr{A}_{\bigvee(W)}$, where

$$\mathscr{A}_{\bigvee(W)} = \bigcup_{(\mathbf{w},k)\in W} \mathscr{A}_{(\mathbf{w},k)}. \tag{1}$$

The following counterexample presents a case in which $\mathscr{A}_{(\mathbf{w},k)} \neq \mathscr{A}_{\bigvee(W)}$, thus showing that the theorem is incorrect.

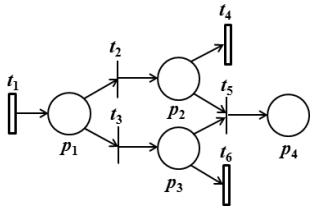

Figure 1: Counterexample 1.

Example 1 *Consider the Petri net in Figure 1 with set of controllable transitions* $T_c = \{t_1, t_4, t_6\}$ *and set of uncontrollable transitions* $T_u = \{t_2, t_3, t_5\}$. *We want to enforce the GMEC* $(\boldsymbol{w}, k) = ([0,0,0,1]^T, 0)$, *i.e.,* $M(p_4) \leq 0$. *Note that in what follows* $C(p,t)$ *denotes the incidence relation of a place* p *and a transition* t.

Since $\boldsymbol{w}^T \cdot C(\cdot, t_5) = 1$*, by applying the* Uncontrollable Transition Gain Transformation *(UTGT, see [2] for its definition) function we have:*

$$\begin{aligned} W &= \mu((\boldsymbol{w},k),t_5) \\ &= \{\rho((\boldsymbol{w},k),t_5,p_2)\} \cup \{\rho((\boldsymbol{w},k),t_5,p_3)\} \\ &= \{([0,1,0,1]^T,0),([0,0,1,1]^T,0)\} \end{aligned} \tag{2}$$

Therefore two new GMECs $(\boldsymbol{w}_1,k_1) = ([0,1,0,1]^T,0)$ *and* $(\boldsymbol{w}_2,k_2) = ([0,0,1,1]^T,0)$ *are obtained.*

One can readily verify that the set of admissible markings, from which no sequence of uncontrollable transitions can lead to a marking violating the original constraint, is

$$\begin{aligned} \mathscr{A}_{(\boldsymbol{w},k)} =& \{[0,0,x,0]^T | x \geq 0\} \\ & \cup \{[0,y,0,0]^T | y \geq 0\} \\ & \cup \{[1,0,0,0]^T\} \end{aligned} \tag{3}$$

while for the transformed constraints $\mathscr{A}_{(\boldsymbol{w}_1,k_1)}$ *and* $\mathscr{A}_{(\boldsymbol{w}_2,k_2)}$ *are*

$$\mathscr{A}_{(\boldsymbol{w}_1,k_1)} = \{[0,0,x,0]^T | x \geq 0\}$$

and

$$\mathscr{A}_{(\boldsymbol{w}_2,k_2)} = \{[0,y,0,0]^T | y \geq 0\}.$$

Hence $\mathscr{A}_{\bigvee(W)} = \mathscr{A}_{(\boldsymbol{w}_1,k_1)} \cup \mathscr{A}_{(\boldsymbol{w}_2,k_2)} \subsetneq \mathscr{A}_{(\boldsymbol{w},k)}$. □

Remark 1 *We will point out where the flaw in the proof of Theorem 2 in [2] lies. In part (b) of the proof, the authors want to show that*

$$\mathscr{A}_{\boldsymbol{w},k} \subseteq \mathscr{A}_{\bigvee(W)} \tag{4}$$

and assume by contradiction that $\mathscr{A}_{\boldsymbol{w},k} \nsubseteq \mathscr{A}_{\bigvee(W)}$*. They say that this condition is equivalent to the following condition:*

$$\exists M \in \mathscr{A}_{\boldsymbol{w},k}, \bigwedge_{(\boldsymbol{w}',k)\in W} \boldsymbol{w}'^T \cdot M > k \tag{5}$$

However, Eq. (5) does not imply $M \notin \mathscr{A}_{\bigvee(W)}$ *but* $M \notin \mathscr{L}_{\bigvee(W)}$*. Therefore the correct conclusion of part (b) is:*

$$\mathscr{A}_{\boldsymbol{w},k} \subseteq \mathscr{L}_{\bigvee(W)} \tag{6}$$

By $\mathscr{A}_{\bigvee(W)} \subseteq \mathscr{L}_{\bigvee(W)}$*, from Eq. (6) we cannot conclude Eq. (4). Theorem 2 in [2] holds in the particular*

case in which $\mathscr{A}_{\bigvee(W)} = \mathscr{L}_{\bigvee(W)}$, e.g., if all constraints in the complement weight set *(CWS, see [2] for its definition) are controllable (a GMEC is said to be controllable if the firing of any uncontrollable transition does not increase its token count).* □

3 Redefining admissibility for disjunctions

We believe that the definition of the admissible markings set for a disjunction of GMECs $\bigvee(W)$ given in Eq. (1) is not sound. In fact, there may exist a marking M that is not admissible for each single constraint in $\bigvee(W)$ and yet from M only legal markings in $\mathscr{L}_{\bigvee(W)}$ are reachable by firing uncontrollable transitions. This is the case of marking $M = [1,0,0,0]^T$ in Example 1.

A reasonable definition of $\mathscr{A}_{\bigvee(W)}$ could be the following one (we will denote the correct solution with a hat to avoid any confusion).

Definition 1 *Given a disjunction of GMECs $\bigvee(W)$ with the set of legal markings $\mathscr{L}_{\bigvee(W)}$, its set of admissible markings consists of all those markings which will never violate $\bigvee(W)$ by only firing uncontrollable transitions, i.e.,:*

$$\hat{\mathscr{A}}_{\bigvee(W)} = \{M \in R(N,M_0) | R_{T_u}(N,M) \subseteq \mathscr{L}_{\bigvee(W)}\} \tag{7}$$

□

We briefly explain the key difference between $\hat{\mathscr{A}}_{\bigvee(W)}$ in this paper and $\mathscr{A}_{\bigvee(W)}$ in Definition 2 in [2]. Under the new definition $\hat{\mathscr{A}}_{\bigvee(W)}$, a marking M is illegal if it may uncontrollably evolve to M' which violates all $(\mathbf{w}_1,k_1),\ldots,(\mathbf{w}_r,k_r)$ in W. However, under the original definition of $\mathscr{A}_{\bigvee(W)}$ in [2], a marking M is illegal if it may uncontrollably evolve to several markings $M_1,\ldots,M_r$ which violates $(\mathbf{w}_1,k_1),\ldots,(\mathbf{w}_r,k_r)$, respectively. Since the trajectory from M to M_i $(1 \leq i \leq r)$ may be different, it may happen that from M the system may violate each single GMEC by firing uncontrollable transitions, but cannot violate all of them at the same time. This is exactly the case in Example 1: $M = [1,0,0,0]^T$ may uncontrollably evolve to $[0,0,1,0]^T$ or $[0,1,0,0]^T$ which violate $(\mathbf{w}_1,k_1)$ and $(\mathbf{w}_2,k_2)$, respectively, indicating $M \notin \mathscr{A}_{\bigvee(W)}$. However, $M \in \hat{\mathscr{A}}_{\bigvee(W)}$ holds since M can never evolve to a marking which violates both $(\mathbf{w}_1,k_1)$ and $(\mathbf{w}_2,k_2)$.

In the following we show that under this new definition, Theorem 2 in [2] holds.

Theorem 2rev. Let $(\mathbf{w},k)$ be a GMEC to be implemented on an ordinary PN, t_x be an uncontrollable transition such that $w(t_x)\cdot C > 0$ and ${}^\bullet t_x \neq \emptyset$, and t_x's CWS be $W = \mu((\mathbf{w},k),t_x)$. Then $\mathscr{A}_{(\mathbf{w},k)} = \hat{\mathscr{A}}_{\bigvee(W)}$.

Proof: (a) $\mathscr{A}_{(\mathbf{w},k)} \subseteq \hat{\mathscr{A}}_{\bigvee(W)}$. We prove this by showing that if a marking M is not in $\hat{\mathscr{A}}_{\bigvee(W)}$, then from M it is possible to uncontrollably reach a marking M'' not in $\mathscr{L}_{(\mathbf{w},k)}$ and thus M is not in $\mathscr{A}_{(\mathbf{w},k)}$. In

fact, if $M \notin \hat{\mathscr{A}}_{\bigvee(W)}$, then from M by firing uncontrollable transitions it is possible to reach a new marking $M' \notin \mathscr{L}_{\bigvee(W)}$, i.e., M' violates all GMECs in W. If M' violates $(\mathbf{w},k)$, then the proof is concluded with $M'' = M'$.

If M' does not violate $(\mathbf{w},k)$ but violates all GMECs $(\mathbf{w}_i,k) = \rho((\mathbf{w},k),t_x,p_i) \in W$, then we show that t_x is enabled at M'. In fact, M' satisfies $\mathbf{w}^T \cdot M' \leq k$ while for each $(\mathbf{w}_i,k)$ in W, the equation $\mathbf{w}_i^T \cdot M' + M'(p_i) > k$ holds, where $p_i \in {}^\bullet t_x$. Then we can conclude that $M'(p_i) > 0$ necessarily holds for all $p_i \in {}^\bullet t_x$ and consequently t_x is enabled, since the net is ordinary.

If t_x is repetitive, i.e., its firing does not decrease the marking of any place in ${}^\bullet t_x$, then t_x can fire infinitely often from M' to continuously increase the token count of $(\mathbf{w},k)$ (because its weight is positive, i.e., $\mathbf{w}^T \cdot C(\cdot,t_x) > 0$) until $(\mathbf{w},k)$ is violated. If t_x is not repetitive, by firing it a suitable number of times from M', a marking M'' is reachable where some place $p_i \in {}^\bullet t_x$ is empty. Now consider the constraint $(\mathbf{w}_i,k)$: by definition of the UTGT function, $\mathbf{w}^T \cdot M'' = \mathbf{w}_i^T \cdot M'' = \mathbf{w}_i^T \cdot M' > k$ holds. In fact the first equality holds since place p_i is not marked at M'', while the second equality holds since the firing of t_x does not modify the token count of $(\mathbf{w}_i,k)$. Hence $M'' \notin \mathscr{L}_{(\mathbf{w},k)}$.

(b) $\mathscr{A}_{(\mathbf{w},k)} \supseteq \hat{\mathscr{A}}_{\bigvee(W)}$. If $M \in \hat{\mathscr{A}}_{\bigvee(W)}$, no marking $M' \notin \mathscr{L}_{\bigvee(W)}$ is reachable from it by only firing uncontrollable transitions. Note that from the definition of the UTGT function, if a marking violates $(\mathbf{w},k)$, then it must violate $\bigvee(W)$, which implies the following relationship between the sets of legal markings: $\mathscr{L}_{(\mathbf{w},k)} \supset \mathscr{L}_{\bigvee(W)}$. Since no marking M' violating $\bigvee(W)$ is reachable from M by only firing uncontrollable transitions, we can conclude that no marking $M' \notin \mathscr{L}_{(\mathbf{w},k)}$ is reachable from M by only firing uncontrollable transitions. Therefore $M \in \hat{\mathscr{A}}_{(\mathbf{w},k)}$ holds. ■

4 Counterexample to Algorithm 1

The main result presented in [2] is Algorithm 1 that proposes a computationally efficient procedure to design a supervisor by repeated constraint transformation. It is claimed in [2] that this algorithm determines a maximally permissive supervisor: here we show that this is not the case.

For easy comprehension we briefly sketch the main steps of Algorithm 1 in [2].

- **(Step 1)** Consider a Petri net and a set W initially containing a single GMEC $(\mathbf{w},k)$ as inputs.
- **(Step 2)** If all $(\mathbf{w},k) \in W$ are admissible[1] then **stop**.
- **(Step 3)** Select a GMEC $(\mathbf{w},k) \in W$ that is not admissible due to a transition t_x and let W' be the set

[1]The algorithm in [2] also considers the notion of weak admissibility but for the sake of simplicity here we ignore this distinction, assuming that all considered constraints are either admissible or not admissible.

obtained from W replacing $(\mathbf{w},k)$ with the CWS $\mu((\mathbf{w},k),t_x)$.

- **(Step 4)** Let $W = W'$ and **goto** 2.

When the algorithm halts, the set W will contain admissible GMECs only, and Theorem 3 in [2] claims that $\mathscr{L}_{\bigvee(W)} = \mathscr{A}_{(\mathbf{w},k)}$. The following counterexample shows, however, that the claim is unfounded.

Example 2 *Consider again the Petri net in Figure 1 and the initial GMEC in W is* $(\boldsymbol{w},k) = ([0,0,0,1]^T,0)$. *In the first iteration* $(\boldsymbol{w},k)$ *will be replaced by* $(\boldsymbol{w}_1,k_1) = ([0,1,0,1]^T,0)$ *and* $(\boldsymbol{w}_2,k_2) = ([0,0,1,1]^T,0)$. *Since* $(\boldsymbol{w}_1,k_1)$ *and* $(\boldsymbol{w}_2,k_2)$ *are not admissible, in the second and the third iteration* $(\boldsymbol{w}_1,k_1)$ *will be replaced by* $(\boldsymbol{w}_3,k_3) = ([1,1,0,1]^T,0)$ *and* $(\boldsymbol{w}_2,k_2)$ *will be replaced by* $(\boldsymbol{w}_4,k_4) = ([1,0,1,1]^T,0)$, *respectively. Since* $(\boldsymbol{w}_3,k_3)$ *and* $(\boldsymbol{w}_4,k_4)$ *are admissible, Algorithm 1 in [2] halts. The output is* $W = \{(\boldsymbol{w}_3,k_3),(\boldsymbol{w}_4,k_4)\}$. *However, we have already shown that* $M = [1,0,0,0]^T$ *is a marking in* $\mathscr{A}_{(\boldsymbol{w},k)}$ *but it is forbidden by* W.

Remark 2 *The reason why Algorithm 1 in [2] fails to give an optimal solution is stated as follows. In the first iteration Theorem 2rev in this note ensures that* $\hat{\mathscr{A}}_{\bigvee(W')} = \hat{\mathscr{A}}_{\bigvee(W)} = \mathscr{A}_{(\boldsymbol{w},k)}$ *since W contains only one GMEC. However, if W contains more than one GMECs, this theorem does not guarantee that* $\bigvee(W) \equiv \bigvee(W')$ *at each iteration.*

We also note that this problem cannot be corrected by minor modifications. Algorithm 1 in [2] is based on the UTGT function, which assumes that for all transformed constraints $(\boldsymbol{w}',k')$, $k' = k$ *holds. Therefore in this example all GMECs in the output W are in the form* $(\boldsymbol{w}',0)$. *Since the legal marking* $M_1 = [1,0,0,0]^T$ *and the illegal marking* $M_2 = [2,0,0,0]^T$ *will simultaneously satisfy or violate* $(\boldsymbol{w}',0)$ *regardless of the value* $\boldsymbol{w}'$, $M_1 = [1,0,0,0]^T$ *and* $M_2 = [2,0,0,0]^T$ *will simultaneously satisfy or violate* $\bigvee(W)$. *Therefore the solution must be suboptimal.* □

Finally we remark that the two GMECs obtained by Algorithm 1 in the previous example are exactly the two possible solutions obtained by Moody and Antsaklis' approach [3]. We believe that Algorithm 1 in [2] is simply another way of constructing all suboptimal solutions in Moody and Antsaklis' approach whose disjunction, however, is not an optimal solution, i.e., it is not always maximally permissive.

5 Counterexample to Lemma 3 in [2]

The last result in [2] that we claim is not correct pertains to the procedure of identifying a class of useless constraints that can be removed from a disjunction without changing the legal marking set. In [2] Definition 5 introduces the notion of *zero constraint*, denoted as $\mathbf{0}$, while Lemma 3 (whose proof is omitted) states that a constraint $(\mathbf{w},k)$ that satisfies $\mathbf{w}^T \cdot M_0 > k$ is equivalent to the zero constraint.

This result is obviously incorrect. In fact, according to Definition 5 in [2], a GMEC $(\mathbf{w},k)$ is the zero constraint with respect to a net system (N,M_0) if $R(N,M_0)\cap\mathscr{A}_{(\mathbf{w},k)}=\emptyset$. On the contrary, the condition $\mathbf{w}^T\cdot M_0>k$ only implies that the initial marking is inadmissible, i.e., $M_0\notin\mathscr{A}_{(\mathbf{w},k)}$ while it may well be possible that some other reachable marking is admissible, i.e., $R(N,M_0)\cap\mathscr{A}_{(\mathbf{w},k)}\neq\emptyset$, which obviously implies that $(\mathbf{w},k)\equiv\mathbf{0}$ does not hold.

Example 3 *Consider again the Petri net in Figure 1 and let* $(\boldsymbol{w},k)=([0,0,0,1]^T,0)$. *Assume that the initial marking is* $M_0=[2,0,0,0]^T$. *This marking is obviously not admissible but by firing, say,* t_2 *twice, we reach* $M=[0,2,0,0]^T$ *that is admissible.* □

Erroneous Lemma 3 in [2] is used to justify a simplification of the constraint transformation procedure. In fact, in Algorithm 1 in [2], when a GMEC $(\mathbf{w},k)$ is added to the set W' (see step 3 in the previous section) the authors suggest testing if $\mathbf{w}^T\cdot M_0>k$ is true. If it is true, $(\mathbf{w},k)$ would be discarded as redundant. However, as the next example shows, discarding such a constraint may lead (once more) to a suboptimal solution, thus providing an additional reason for Algorithm 1 in [2] to fail.

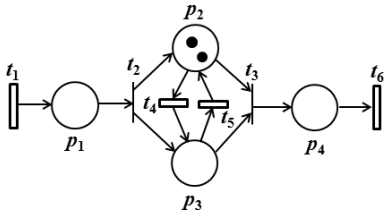

Figure 2: Counterexample 2.

Example 4 *Consider the net N in Figure 2 with set of controllable transitions* $T_c=\{t_1,t_4,t_5,t_6\}$ *and set of uncontrollable transitions* $T_u=\{t_2,t_3\}$. *We want to enforce the GMEC* $(\boldsymbol{w},k)=([0,0,0,1]^T,1)$, *i.e.,* $M(p_4)\leq 1$ *on this net. After applying the UTGT three times, we determine the optimal solution that contains the disjunction of two admissible GMECs:* $(\boldsymbol{w}_1,k_1)=([1,1,0,1]^T,1)$ *and* $(\boldsymbol{w}_2,k_2)=([1,0,1,1]^T,1)$. *Since* $\boldsymbol{w}_1^T\cdot M_0>k_1$, *following Lemma 3 in [2] one may consider the GMEC* $(\boldsymbol{w}_1,k_1)$ *as a zero constraint and remove it. Therefore one would erroneously conclude that* $\mathscr{A}_{(\boldsymbol{w},k)}$ *coincides with* $\mathscr{A}_{(\boldsymbol{w}_2,k_2)}=\{M|M(p_1)+M(p_3)+M(p_4)\leq 1\}$, *and the marking* $M=[0,0,2,0]^T\notin\mathscr{A}_{(\boldsymbol{w}_2,k_2)}$ *will be forbidden by the control policy. However M is a legal marking that belongs to both* $\mathscr{A}_{(\boldsymbol{w},k)}$ *and* $\mathscr{A}_{(\boldsymbol{w}_1,k_1)}$ *and can be legally reached by firing* t_4 *twice at* M_0. □

6 Summary

We summarize what we feel are the main problems with the approach presented in [2].

(1) Definition of $\mathscr{A}_{\bigvee(W)}$: the definition of the admissible set $\mathscr{A}_{\bigvee(W)}$ for a disjunction of constraints in [2] is not sound. We have provided a counterexample to show that Theorem 2 in [2] is not correct under such a definition. We have proposed a proper definition of this set $\hat{\mathscr{A}}_{\bigvee(W)}$ in Definition 1 in this note. In Theorem 2rev presented in this note, we have shown that Theorem 2 in [2] holds under this new definition. We believe that the additional result discussed in [2], namely the characterization of weakly admissible GMECs, still holds under the new definition, but a formal proof is still needed.

(2) Maximal permissiveness: we have presented a counterexample to show that the output of Algorithm 1 in [2] is not optimal as claimed. The reason is that the two GMEC sets W and W' before and after an iteration process are not always equivalent. The solution would be optimal in the particular case in which Algorithm 1 in [2] halts after the first iteration. Our counterexample also shows that a GMEC transformation procedure based on the UTGT function cannot find an optimal solution in all cases. Solving this problem is not straightforward: it needs a major revision of the UTGT function and the CWS computation.

(3) Zero constraints: the last counterexamples show that Lemma 3 in [2] is not correct, which also leads to a suboptimal output of Algorithm 1 in [2]. We believe that this problem can be fixed by removing this lemma and removing the corresponding simplification procedure in the algorithm, i.e., all GMECs in which M_0 is not admissible should be preserved in W'. This would remove one of causes of suboptimality of Algorithm 1 in [2].

The sound contribution of [2] is thus reduced to a stopping criterion (called weakly admissible GMECs) in the constraint transformation approach. We also believe that Algorithm 1 in [2] based on the UTGT function and the CWS computation is meaningful since it gives a suboptimal but more permissive control policy with respect to Moody and Antsaklis's approach, where an inadmissible GMEC is only transformed into a single admissible constraint [3]. However, the constraint transformation problem in arbitrary Petri nets still remains open.

References

[1] A. Giua, F. DiCesare, and M. Silva. Generalized mutual exclusion constraints for Petri nets with uncontrollable transitions. In *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, pages 947–949, Chicago, USA, 1992.

[2] J. L. Luo, H. Shao, K. Nonami, and F. J. Jin. Maximally permissive supervisor synthesis based on a new constraint transformation method. *Automatica*, 48:1097–1101, 2012.

[3] J. Moody and P. Antsaklis. Petri net supervisors for DES with uncontrollable and unobservable transitions. *IEEE Trans. on Automatic Control*, 45:462–476, 2000.