On the "counter-example" in the article "Max′-controlled siphons for liveness of S^3PGR^2" regarding the results in [1]

Spyros Reveliotis

Abstract— **The main purpose of this correspondence is to establish that, contrary to the claims that are made in [2], the results of [1] concerning the liveness characterization of the S^3PGR^2 nets by means of the structural object of deadly marked siphon, are correct and complete.**

I. Introduction

In the paper by D. Y. Chao that is quoted in the title of this document, to be referred as [2], the author claims that the main result published in [1] regarding the structural characterization of liveness of a class of Petri nets (PNs) known as S^3PGR^2 nets, is erroneous. The author of [2] tries to base his claim on a "counter-example" to the disputed result of [1]. The main purpose of this correspondence is to show that the original result of [1] is actually correct, while the "counter-example" claimed by [2] is just an erroneous and very inadequate interpretation of the results in [1].

Hence, the material of this document is organized as follows: In the next section, we overview some concepts and results that are introduced in [1], and are necessary for an intelligent discussion of the "counter-example" of [2]. The claimed "counter-example", itself, is introduced in Section III, and subsequently, Section IV shows that the example S^3PGR^2 net that is introduced in Section III actually adheres to the developments in [1], when these developments are properly understood and applied. Finally, some closing remarks are provided in Section V. In the following developments, we assume that the reader is familiar with the basic PN theory. Also, this document follows the basic notation that was introduced in [1] and was further adopted in [2]; hence, we refer to these two papers for a more systematic introduction of this notation.

II. S^3PGR^2 nets and their liveness characterization in [1]

The S^3PGR^2 nets is a PN class that models sequential resource allocation of a finite set of reusable resources to a set of concurrently executing processes. A formal definition of this PN class is as follows:

Definition 1: [1] A well-marked S^3PGR^2 net is a marked PN $\mathcal{N} = (P, T, W, M_0)$ such that

i. $P = P_S \cup P_0 \cup P_R$, where $P_S = \bigcup_{j=1}^{n} P_{S_j}$ s.t. $P_{S_i} \cap P_{S_j} = \emptyset$, $\forall i \neq j$, $P_0 = \bigcup_{j=1}^{n}\{p_{0_j}\}$ s.t. $P_0 \cap P_S = \emptyset$, and $P_R = \{r_1, \ldots, r_m\}$ s.t. $(P_S \cup P_0) \cap P_R = \emptyset$;

ii. $T = \bigcup_{j=1}^{n} T_j$;

iii. $W = W_S \cup W_R$, where $W_S : ((P_S \cup P_0) \times T) \cup (T \times (P_S \cup P_0)) \rightarrow \{0, 1\}$ s.t. $\forall j \neq i$, $((P_{S_j} \cup P_{0_j}) \times T_i) \cup (T_i \cup (P_{S_j} \cup P_{0_j})) \rightarrow \{0\}$, and $W_R : (P_R \times T) \cup (T \times P_R) \rightarrow \mathbb{Z}_0^+$;

iv. $\forall j,\ j = 1, \ldots, n$, the subnet $\mathcal{N}_j$ generated by $P_{S_j} \cup \{p_{0_j}\} \cup T_j$ is a strongly connected state machine such that every circuit contains p_{0_j};

v. $\forall r \in P_R$, $\exists$ a unique minimal p-semiflow y_r s.t. $||y_r|| \cap P_R = \{r\}$, $||y_r|| \cap P_0 = \emptyset$, $||y_r|| \cap P_S \neq \emptyset$, and $y_r(r) = 1$. Furthermore, $P_S = \bigcup_{r \in P_R}(||y_r|| - P_R)$;

vi. $\mathcal{N}$ is pure and strongly connected;

vii. $\forall p \in P_S,\ M_0(p) = 0$; $\forall r \in P_R,\ M_0(r) \geq \max_{p \in ||y_r||} y_r(p)$; and $\forall p_{0_j} \in P_0,\ M_0(p_{0_j}) \geq 1$.

In Definition 1 the strongly connected state machines $\mathcal{N}_j,\ j = 1, \ldots, n$, of item (iv) model the process plans of the n process types that are supported by the underlying RAS. The places in P_{S_j} define the processing stages of these process plans, and they are referred to as the "process places" of net $\mathcal{N}_j$. On the other hand, the places p_{0_j} are characterized as the "idle places" of the corresponding subnets $\mathcal{N}_j$, and the tokens in these places model instances of the corresponding process type that are waiting for their initiation. In the modeling framework of the S^3PGR^2 nets, the various resource types are modelled by the places in P_R. The initial marking of these places defines the availability (or the "capacity") of corresponding resource types, and the p-seminflows of item (v) in Definition 1 model the resource allocation function that takes place in the underlying RAS. Finally, the conditions on the initial marking of the places in P_R in item (vii) of Definition 1 ensure that each resource has sufficient capacity to support the execution of any realization of the process plan of any process type, when this realization is executed by a process instance that runs alone in the entire RAS. In the standard PN terminology, this last capability implies the quasi-liveness of net $\mathcal{N}$; i.e., for every transition t in T, there is a transition sequence fireable from the initial marking M_0 that enables t.

On the other hand, the considered net $\mathcal{N}$ might not be live due to the fact that the underlying RAS might possess partial deadlocks, i.e., RAS states where a subset of the activated process instances are permanently blocked in their current processing stages because each of them requires for its further advancement some resource that is currently held by some other process in the same set. In the S^3PGR^2 setting, the permanent blocking of the deadlocked processes is represented by the deadness of the corresponding transitions that would advance these processes. A key result of [1], that is disputed in [2], relates the liveness of S^3PGR^2 nets to the formation of a particular structure in this net that is essentially a characterization of the partial deadlock developed in the underlying RAS, expressed, however, in the semantics of the PN modeling framework and some pertinent primitives from that framework. Next we introduce these primitives that are necessary for the formal statement of the aforementioned result in [1].[1]

We begin with the notion of a deadly marked siphon, which plays a central role in the statement of the considered

S. Reveliotis is with the School of Industrial & Systems Engineering, Georgia Institute of Technology, email: `spyros@isye.gatech.edu`

[1]Due to space considerations, we have limited the subsequent discussion to the most essential concepts and results that are necessary for carrying out an intelligent discussion of the considered "counter-example" and our objections to it. A more leisurely treatment of this material that also provides important insights behind the formal statement of the results presented herein can be found in [4], [5], [6].

result.

Definition 2: For any given PN $\mathcal{N} = (P, T, W, M_0)$:
i. A siphon S is a subset of the place set P s.t. the set of transitions that bring tokens in the places of S is a subset of the set of transitions that require tokens from some place in S for their firing; or, in standard PN notation, $S \subseteq P$ is a siphon if and only if (iff) $\bullet S \subseteq S \bullet$.
ii. A siphon S is deadly marked at a given marking M iff every transition $t \in \bullet S$ is disabled by some place $p \in S$.

It is well known that all the disabling places in a PN total deadlock (i.e., a PN marking where no transition is fireable) constitute a deadly marked siphon.[2] However, this last result is not adequate to interpret the non-liveness of the S^3PGR^2 nets, since, as explained above, the latter is due to the formation of *partial* deadlock in the underlying RAS, which is manifested by the presence of dead transitions in the corresponding S^3PGR^2 net but not necessarily any total deadlocks. To see the validity of this last remark, just notice that, while some processes might be in deadlock in the considered RAS, some of the remaining process types can still execute repetitively making use of the system resources that are not engaged in the deadlock. The result of [1] seeks to address this complication by introducing the notion of "modified marking" of S^3PGR^2 nets, and looking for deadly marked siphons that will interpret the non-liveness of these nets in the "modified reachability space". A formal definition of these concepts is as follows:

Definition 3: Consider a well-marked S^3PGR^2 net $\mathcal{N} = (P_S \cup P_0 \cup P_R, T, W, M_0)$. Then:
i. Given a marking M in the reachable state space $R(\mathcal{N}, M_0)$, the corresponding modified marking $\overline{M}$ is defined by

$$\overline{M}(p) = \begin{cases} M(p) & \text{if } p \notin P_0 \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

ii. The space of the modified reachable markings $\overline{R(\mathcal{N}, M_0)}$, is defined by

$$\overline{R(\mathcal{N}, M_0)} = \{\overline{M} : M \in R(\mathcal{N}, M_0)\} \tag{2}$$

In plain terms, the modified (reachable) marking $\overline{M}$ of a (reachable) marking M of the S^3PGR^2 net $\mathcal{N}$ essentially removes from the original marking M any tokens that are located in the idle places p_{0_j}, $j = 1, \ldots, n$, in an effort to control the recirculation of tokens that correspond to non-deadlocked processes. Then, for any a marking M that contains a partial deadlock, we can consider the modified marking $\overline{M'}$ of the marking M' that is obtained from marking M by further advancing all the tokens in M that correspond to non-deadlocked processes as far as possible in their process plans, while preventing the initiation of any new processes. By construction, $\overline{M'}$ is a total deadlock. Hence, for the modified marking $\overline{M'}$, there is a deadly marked siphon associated with it, according to the logic of Lemma 4 in [1]. But there is one last caveat that must be addressed before this line of reasoning can provide, indeed, a correct connection between the formation of partial deadlock in the considered RAS, the resulting non-liveness of the corresponding S^3PGR^2 nets, and the interpretation of this non-liveness through deadly marked siphons. This caveat has to do with the fact that the modified marking $\overline{M_0}$, that results from the initial marking M_0, is also a total deadlock (since, in $\overline{M_0}$, all tokens modeling process instances have been removed from the net). To cope with this complication, we need to qualify further the deadly marked siphons that are sought in the modified reachability space. The complete result is given in Lemma 5 of [1], which is reproduced as Lemma 1 in [2]:

[2]c.f. Lemma 4 in [1], but the result holds for more general PNs than the class of the S^3PGR^2 nets.

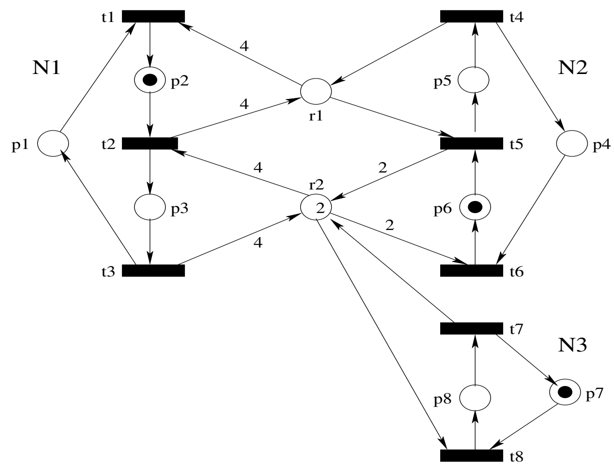

Fig. 1. The S^3PGR^2 net that is used in [2] as a "counter-example" to the result of Theorem 1 in [1].

Lemma 1: [1] Let $\mathcal{N} = (P, T, W, M_0)$ be a well-marked S^3PGR^2 net. If there exists a dead transition at $M \in R(\mathcal{N}, M_0)$, then there exists a marking $M' \in R(\mathcal{N}, M)$ with its modified marking $\overline{M'}$ containing a deadly marked siphon, S, such that (i) $S \cap P_R \neq \emptyset$, and (ii) every place in $S \cap P_R$ is a disabling place.

Lemma 1 subsequently enables the main result of [1] that characterizes the liveness of S^3PRG^2 nets; this result is provided below and it corresponds to "Theorem 1" in, both, [1] and [2].

Theorem 1: Let $\mathcal{N} = (P, T, W, M_0)$ be a well-marked S^3PGR^2 net. The net is live iff the space of modified reachable markings, $\overline{R(\mathcal{N}, M_0)}$, contains no deadly marked siphon such that (i) $S \cap P_R \neq \emptyset$, and (ii) every place in $S \cap P_R$ is a disabling place.

After the presentation of Theorem 1, the work of [2] proceeds with a claim that this theorem is erroneous. In particular, the author claims that he has constructed a "counter-example" for Theorem 1 which establishes that the absence of the considered deadly marked siphons does not imply the liveness of the underlying S^3PGR^2 nets (in the exact words of [2]: "…the absence of DMSs does not imply the liveness of an S^3PGR^2.") We proceed to discuss this "counter-example" in the next sections and reveal all the fallacies that underlie its employment in [2].

III. The "counter-example" of [2]

The "counter-example" of [2] to the result of Theorem 1 in the previous section is based on the PN marking that is depicted in Fig. 1. The depicted net is indeed an S^3PGR^2 net with the resource places being the places r_1 and r_2 and the process subnets N_1, N_2 and N_3 being respectively defined by the circuits $\langle p_1, t_1, p_2, t_2, p_3, t_3, p_1\rangle$, $\langle p_4, t_6, p_6, t_5, p_5, t_4, p_4\rangle$ and $\langle p_7, t_8, p_8, t_7, p_7\rangle$. In these three process subnets, the corresponding idle places are $p_{0_1} = p_1$, $p_{0_2} = p_4$ and $p_{0_3} = p_7$. The remaining places in each of these nets define the corresponding set of process places, P_{S_j}, $j = 1, 2, 3$. Also, it is easy to check that in the marking that is depicted in Fig. 1, the two tokens in the places p_2 and p_6 correspond to RAS processes that are in deadlock. On the other hand, the token in the idle place p_7 is a currently inactive process, which, however, can execute repetitively using one of the two free units of resource r_2. Hence, the depicted marking contains a RAS partial deadlock but it is not a total deadlock (in the PN sense).

In the developments of [2], the S^3PGR^2 marking that is described above is claimed as a "counter-example" of Theorem 1 as follows:

"A counter example is shown in [the figure depicting the considered marking] where the net N is a well-marked S^3PGR^2 net; all transitions in N_3 are live, whereas all transitions in N_1 and N_2 are dead. Thus, N is not live, yet the only problematic siphon $S = \{r_1, r_2, p_3, p_5, p_8\}$ is not deadly marked. Thus, unlike S^3PR, the absence of DMSs, does not imply the liveness of an S^3PGR^2."

We admit that we have a very hard time to understand the thinking process that underlies the above argument, since it seems to not even try to connect to the actual content of Theorem 1 that, in [2], is stated a few lines before the quoted statements. On the other hand, the author seems to appeal to the concept of the S^3PR net, which is a class of PNs that model RAS with a different (more restrictive) structure and behavior than those supported by the RAS class corresponding to the S^3PGR^2 nets, and for some unexplained reason, he is focusing on the siphon $S = \{r_1, r_2, p_3, p_5, p_8\}$, pronouncing it as "the only problematic siphon". In the next section we show that, when properly interpreted, the result of Theorem 1 in Section II provides a deadly marked siphon corresponding to the partial deadlock in the marking of Fig. 1.

IV. A correct application of the results of [1] on the example S^3PGR^2 marking presented in [2]

As stated in Theorem 1, and for the reasons explained in Section II, the deadly marked siphon must be sought in the modified reachability space defined in Definition 3. The modified marking of the marking depicted in Fig. 1 is provided in Fig. 2. This marking is obtained from the original marking of Fig. 1 by just removing the token in the idle place p_7. Then, it is easy to check that in the marking depicted in Fig. 2, the set $S' = \{r_1, r_2, p_3, p_5, p_8, p_7\}$ is a deadly marked siphon that also satisfies the additional two requirements of Theorem 1: i.e., $S' \cap P_R \neq \emptyset$, and (ii) every place in $S' \cap P_R$ is a disabling place. Hence, contrary to the claims of [2], the RAS partial deadlock that is depicted in Fig. 1 results in non-live behavior for the corresponding S^3PGR^2 net, which, however, is effectively identified by the criterion of Theorem 1 (i.e., the original results of [1]).

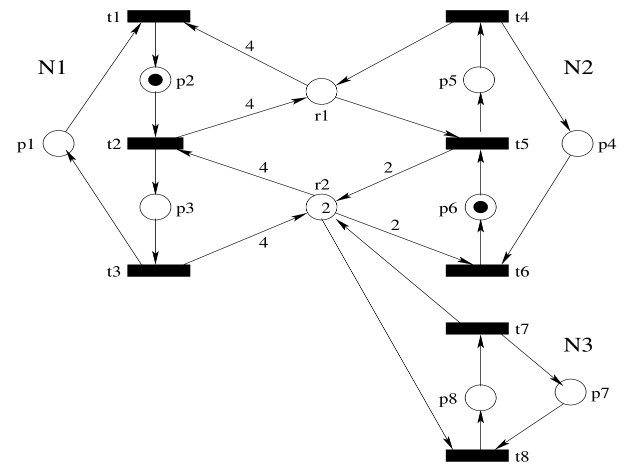

Fig. 2. The modified marking of the S^3PGR^2 marking that is depicted in Fig. 1.

We close the discussion of this example by noticing that the logic behind the construction of the siphon S' that was introduced in the previous paragraph, is detailed in the proof of Lemma 5 in [1]. This construction parallels, to a certain extent, the construction of the empty siphons that interpret the partial deadlocks developing in the simpler class of the S^3PR nets [3], but it also introduces the necessary modifications to address the complications that arise in the class of S^3PGR^2 nets and were discussed in Section II.[3]

V. Concluding remarks

It should be evident from the discussion of Section IV that the claimed "counter-example" of [2] for the seminal result of Theorem 1 in [1] is not correct, and therefore, it provides no reason for questioning the validity of any of the results that are presented in [1]. In fact, the siphon-based characterization of [1] for the liveness of S^3PGR^2 nets has been extended to RAS-modeling PNs with a more complex

[3] Most importantly, this construction is carried out on the *modified* marking, $\overline{M'}$, of the marking M' that is obtained from a marking M containing a RAS partial deadlock by draining the process subnets of any non-deadlocked process instances. Since, by its construction, the modified marking $\overline{M'}$ is a total deadlock involving active processes (i.e., possessing some tokens in the process places of the underlying S^3PGR^2 net), another way to identify a deadly marked siphon S'' in $\overline{M'}$ that also satisfies the two additional requirements of Theorem 1, is by having S'' collect all the disabling places in $\overline{M'}$. The presence of marked process places in marking $\overline{M'}$ implies that some of the disabling places in S'' will be resource places. This specification of S'' is a simpler and, admittedly, a more natural way to identify a siphon that meets the requirements of Theorem 1 than the construction in the proof of Lemma 5 of [1]. For the marking of Fig. 2, $S'' = \{p_1, p_3, p_4, p_5, p_7, p_8, r_1, r_2\}$. On the other hand, it is also true that, due to their construction logic, $S' \subseteq S''$, and therefore, S' is a "tighter" characterization of the corresponding partial deadlock than S''.

structure and behavior in [4], [5], [6], [7]. All these works also provide pertinent discussion[4] on the substantial role that is played by the concept of the modified marking in the provided characterizations of the liveness of the corresponding nets, and the first three of these works predate the publication of [2] by a number of years.

Finally, the authors of [1] regret the fact that the problematic material of [2] that is considered in this note, was published by IET without the relevant editorial process giving them any notice about this development, and an opportunity to discuss / counter the claims made in [2] about the results of [1]; such an approach would have avoided the unfortunate situation faced at this point.

References

[1] J. Park and S. A. Reveliotis, "Deadlock avoidance in sequential resource allocation systems with multiple resource acquisitions and flexible routings," *IEEE Trans. on Automatic Control*, vol. 46, pp. 1572–1583, 2001.

[2] D. Y. Chao, "Max'-controlled siphons for liveness of S^3PGR^2," *IET Control Theory Appl.*, vol. 1, pp. 933–936, 2007.

[3] J. Ezpeleta, J. M. Colom, and J. Martinez, "A Petri net based deadlock prevention policy for flexible manufacturing systems," *IEEE Trans. on R&A*, vol. 11, pp. 173–184, 1995.

[4] S. A. Reveliotis, "On the siphon-based characterization of liveness in sequential resource allocation systems," in *Applications and Theory of Perti Nets 2003*, 2003, pp. 241–255.

[5] ——, *Real-time Management of Resource Allocation Systems: A Discrete Event Systems Approach.* NY, NY: Springer, 2005.

[6] ——, "Siphon-based characterization of liveness and liveness-enforcing supervision for sequential resource allocation systems," in *Deadlock Resolution in Computer-Integrated Systems*, M. C. Zhou and M. P. Fanti, Eds. Marcel Dekker, Inc., 2005, pp. 283–307.

[7] H. Liao, Y. Wang, H. K. Cho, J. Stanley, T. Kelly, S. Lafortune, S. Mahlke, and S. Reveliotis, "Concurrency bugs in multithreaded software: Modeling and analysis using Petri nets," *Discrete Event Systems: Theory and Applications*, vol. 23, pp. 157–195, 2013.

[4]The relevant discussion in [5] also offers a series of elucidating examples; c.f. pgs 134-138.