A Petri-Net Based Approach to Verifying Compositional Correctness of System Components

K.S. Cheung

The University of Hong Kong
Hong Kong

Abstract

In component-based system design, one need to obtain from a given set of components an integrated system which is correct in the sense that the system is live, bounded and reversible. In this paper, based on the composition of augmented marked graphs, we propose a method for verifying correctness of the integrated system. The method begins with specifying the components as augmented marked graphs. These augmented marked graphs are then composed via common resource places into an integrated system. By the preservation of properties of this composition, the liveness, boundedness, reversibility and conservativeness of the integrated system can be readily derived.

Keywords: Petri net, augmented marked graph, component-based system design, system synthesis.

1. Introduction

In the past decade, component-based system design has emerged as a promising paradigm to meet the ever increasing needs for managing system complexity and maximising re-use as well as for deriving software engineering into standards. In component-based system design, a system is synthesised from a given set of components. Even that the components are correct in the sense that they are live (implying freeness of deadlock), bounded (implying absence of capacity overflow) and reversible (implying the capability of being reinitialised from any reachable states), the integrated system may not be correct, especially when there involves shared resources.

This paper investigates the compositional correctness of system components. Based on the property-preserving composition of augmented marked graphs, we propose a method for synthesising the components into an integrated system whose correctness can be readily verified.

A subclass of Petri nets, augmented marked graphs possess a structure which is especially desirable for modelling systems with common resources. They possess a number of desirable properties pertaining to deadlock-freeness, liveness, boundedness, reversibility and conservativeness. Chu and Xie first investigated their deadlock-freeness, liveness and reversibility using siphons and mathematical programming [1]. We earlier proposed siphon-based and cycle-based characterisations for live and reversible augmented marked graphs, and transform-based characterisations for bounded and conservative augmented marked graphs [2, 3, 4]. Besides, Huang et al. investigated the composition of augmented marked graphs via common resource places [5]. Recently, we also conducted preliminary investigation on the composition of augmented marked graphs [6].

This paper investigates the composition of augmented marked graphs via common resource places, with a focus on the preservation of properties. These properties include liveness, boundedness, reversibility and conservativeness. They collectively characterise a well-behaved system. We show how this property-preserving composition of augmented marked graphs can be applied to component-based system design, so that the system correctness can be readily verified.

The rest of this paper is organised as follows. Section 2 is a brief description of augmented marked graphs. In Section 3, we present the composition of augmented marked graphs and study the preservation of properties in the composition process. Section 4 then shows its application to verifying compositional correctness of system components. Section 5 concludes this paper. Readers are expected to have basic knowledge of Petri nets [7, 8, 9].

2. Augmented Marked Graphs

This section briefly describes augmented marked graphs.

Definition 2.1 [1]**.** An augmented marked graph (N, M_0; R) is a PT-net (N, M_0) with a subset of places R called resource places, such that : (a) Every place in R is marked by M_0. (b) The net (N', M_0') obtained from (N, M_0; R) by removing the places in R and their associated arcs is a marked graph. (c) For each $r \in R$, there exist $k_r \geq 1$ pairs of transitions $D_r = \{ \langle t_{s1}, t_{h1} \rangle, \langle t_{s2}, t_{h2} \rangle, ..., \langle t_{skr}, t_{hkr} \rangle \}$ such that $r^\bullet = \{ t_{s1}, t_{s2}, ..., t_{skr} \} \subseteq T$, $^\bullet r = \{ t_{h1}, t_{h2}, ..., t_{hkr} \} \subseteq T$, and for each $\langle t_{si}, t_{hi} \rangle \in D_r$, there exists in N' an elementary path ρ_{ri} connecting t_{si} to t_{hi}. (d) In (N', M_0'), every cycle is marked and no ρ_{ri} is marked.

Definition 2.2. For a PT-net (N, M_0), a set of places S is called a siphon if and only if $^\bullet S \subseteq S^\bullet$. S is said to be minimal if and only if there does not exist a siphon S' in N such that $S' \subset S$. S is said to be empty at a marking $M \in [M_0\rangle$ if and only if S contains no places marked by M.

Definition 2.3. For a PT-net (N, M_0), a set of places Q is called a trap if and only if $Q^\bullet \subseteq {}^\bullet Q$. Q is said to be maximal if and only if there does not exist a trap Q' in N such that $Q \subset Q'$. Q is said to be marked at a marking $M \in [M_0\rangle$ if and only if Q contains a place marked by M.

Property 2.1 [1]**.** An augmented marked graph is live and reversible if and only if it does not contain any potential deadlock. (A potential deadlock is a siphon which would eventually become empty.)

Definition 2.4. For an augmented marked graph (N, M_0; R), a minimal siphon is called a R-siphon if and only if it contains at least one place in R.

Property 2.2 [1, 2, 3]**.** An augmented marked graph (N, M_0; R) is live and reversible if every R-siphon contains a marked trap.

Property 2.3 [2, 3]**.** An augmented marked graph (N, M_0; R) is live and reversible if and only if no R-siphons eventually become empty.

Definition 2.5 [4]**.** Suppose an augmented marked graph (N, M_0; R) is transformed into a PT-net (N', M_0') as follows. For each $r \in R$, where $D_r = \{ \langle t_{s1}, t_{h1} \rangle, \langle t_{s2}, t_{h2} \rangle, ..., \langle t_{skr}, t_{hkr} \rangle \}$, replace r with a set of places $\{ q_1, q_2, ..., q_{kr} \}$ such that $M_0'[q_i] = M_0[r]$ and $q_i^\bullet = \{ t_{si} \}$ and $^\bullet q_i = \{ t_{hi} \}$ for $i = 1, 2, ..., k_r$. (N', M_0') is called the R-transform of (N, M_0; R).

Property 2.4 [4]. Augmented marked graph (N, M_0; R) is bounded and conservative if and only if every place in its R-transform (N', M_0') belongs to a cycle.

3. Composition of Augmented Marked Graphs

This section first describes the composition of augmented marked graphs via a set of common resource places. Preservation of properties are then studied.

Property 3.1. Let $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ be two augmented marked graphs, where $R_1' = \{ r_{11}, r_{12}, ..., r_{1k} \} \in R_1$ and $R_2' = \{ r_{21}, r_{22}, ..., r_{2k} \} \in R_2$ are the common places that r_{11} and r_{21} are to be fused into one single place r_1, r_{12} and r_{22} into r_2, ..., r_{1k} and r_{2k} into r_k. Then, the resulting net obtained after the fusion is also an augmented marked graph $(N, M_0; R)$, where $R = (R_1 \setminus R_1') \cup (R_2 \setminus R_2') \cup \{ r_1, r_2, ..., r_k \}$. (obvious)

Definition 3.1. With reference to Property 3.1, $(N, M_0; R)$ is called the composite of $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ via a set of common resource places $\{ (r_{11}, r_{21}), (r_{12}, r_{22}), ..., (r_{1k}, r_{2k}) \}$, where $r_{11}, r_{12}, ..., r_{1k} \in R_1$ and $r_{21}, r_{22}, ..., r_{2k} \in R_2$. $R_F = \{ r_1, r_2, ..., r_k \}$ is called the set of fused resource places that are obtained after fusing $(r_{11}, r_{21}), (r_{12}, r_{22}), ..., (r_{1k}, r_{2k})$.

Property 3.2 [5, 6]. Let $(N, M_0; R)$ be the composite of two augmented marked graphs $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ via a set of common resource places. $(N, M_0; R)$ is bounded if and only if $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ are bounded.

Property 3.3 [6]. Let $(N, M_0; R)$ be the composite of two augmented marked graphs $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ via a set of common resource places. $(N, M_0; R)$ is conservative if and only if $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ are conservative.

Definition 3.2. Let $(N, M_0; R)$ be the composite of two augmented marked graphs via a set of common resource places, and $R_F \subseteq R$ be the set of fused resource places. For $(N, M_0; R)$, a minimal siphon is called a R_F-siphon if and only if it contains at least one place in R_F.

Property 3.5 [6]. Let $(N, M_0; R)$ be the composite of two augmented marked graphs $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ via a set of common resource places. $(N, M_0; R)$ is live and reversible if and only if $(N_1, M_{10}; R_1)$ and $(N_2, M_{20}; R_2)$ are live and no R_F-siphons eventually become empty.

4. Compositional Correctness of System Components

Liveness, boundedness and reversibility are key attributes of a correct or well-behaved system. In component-based system design, a system is synthesised from a set of components [10, 11, 12]. The integrated system may not be live, bounded nor reversible even that the components are live, bounded and reversible, especially as there involves competition of shared resources. Hence, an important step in system design is to verify if the integrated system is correct in the sense that it is live, bounded and reversible.

This section presents the application of the property-preserving composition of augmented marked graphs to verifying compositional correctness of system components. By modelling the components as augmented marked graphs and composing them via their common resource places which represent the common resources, based on the results in the previous section, the properties of the integrated system can be readily derived. In brief, if the components are bounded and conservative, the integrated system will be bounded and conservative. If the components are live and reversible, the integrated system will be live and reversible under a pretty simple condition.

Consider a flexible assembly system, comprising 4 conveyors (Y_1, Y_2, Y_3 and Y_4) and 4 robots (B_1, B_2, B_3 and B_4). There are 4 components (C_1, C_2, C_3 and C_4). They used to perform different functionalities, exhibiting asynchronous and concurrent processes. In performing the functionalities, the components require resources - some are private resources while others are common resources. The conveyors are private resources exclusively used by individual components. The robots are common resources shared among different components. Figure 1 outlines the system configuration.

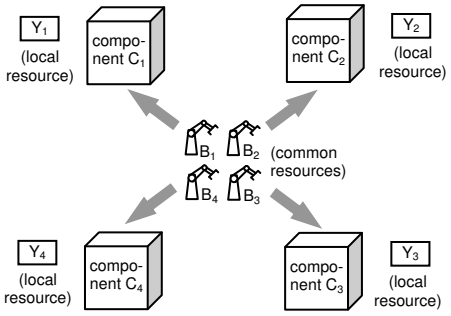

Fig. 1: Outline of system components.

The components are briefly described as follows.

C_1 : C_1 performs an assembly process which involves Y_1, B_1 and B_2. At the initial idle state, once Y_1 is available, C_1 requests B_1 and B_2 simultaneously. After acquiring B_1 and B_2, C_1 performs assembly and then releases Y_1, B_1 and B_2.

C_2 : C_2 performs an assembly process which involves Y_2, B_2 and B_3. At the initial idle state, once Y_2 is available, C_2 requests B_2 and B_3 simultaneously. After acquiring B_2 and B_3, C_2 performs assembly and then releases Y_2, B_2 and B_3.

C_3 : C_3 performs an assembly process which involves Y_3, B_3 and B_4. At the initial idle state, once Y_3 is available, C_3 requests B_3 and B_4 simultaneously. After acquiring B_3 and B_4, C_3 performs assembly and then releases Y_3, B_3 and B_4.

C_4 : C_4 performs an assembly process which involves Y_4, B_4 and B_1. At the initial idle state, once Y_4 is available, C_4 requests B_4 and B_1 simultaneously. After acquiring B_4 and B_1, C_4 performs assembly and then releases Y_4, B_4 and B_1.

Component C_1 is specified as augmented marked graph (N_1, M_{10}; R_1) where $R_1 = \{ r_{11}, r_{12} \}$. C_2 is specified as (N_2, M_{20}; R_2) where $R_2 = \{ r_{21}, r_{22} \}$. C_3 is specified as (N_3, M_{30}; R_3) where $R_3 = \{ r_{31}, r_{32} \}$. C_4 is specified as (N_4, M_{40}; R_4) where $R_4 = \{ r_{41}, r_{42} \}$. They are shown in Figure 2, while Table 1 lists the semantic meanings of the places and transitions.

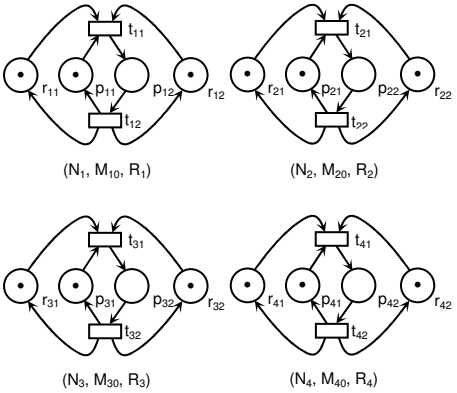

Fig. 2: System components represented as augmented marked graphs.

P / T	Semantic Meaning
p_{11}	Y_1 is ready
p_{12}	Y_1 is occupying B_1 and B_2 and performing assembly
p_{21}	Y_2 is ready
p_{22}	Y_2 is occupying B_2 and B_3 and performing assembly
p_{31}	Y_3 is ready
p_{32}	Y_3 is occupying B_3 and B_4 and performing assembly
p_{41}	Y_4 is ready
p_{42}	Y_4 is occupying B_4 and B_1 and performing assembly
r_{11}, r_{41}	B_1 is available
r_{12}, r_{21}	B_2 is available
r_{22}, r_{31}	B_3 is available
r_{32}, r_{42}	B_4 is available
t_{11}	C_1 acquires B_1 and B_2 and starts assembly
t_{12}	C_1 finishes assembly and releases Y_1, B_1 and B_2
t_{21}	C_2 acquires B_2 and B_3 and starts assembly
t_{22}	C_2 finishes assembly and releases Y_2, B_2 and B_3
t_{31}	C_3 acquires B_3 and B_4 and starts assembly
t_{32}	C_3 finishes assembly and releases Y_3, B_3 and B_4
t_{41}	C_4 acquires B_4 and B_1 and starts assembly
t_{42}	C_4 finishes assembly and releases Y_4, B_4 and B_1

Table 1: Semantic meaning of places and transitions in Figure 1.

In Figure 2, r_{12} in (N_1, M_{10}; R_1) and r_{21} in (N_2, M_{20}; R_2) refer to the same resource B_2. r_{22} in (N_2, M_{20}; R_2) and r_{31} in (N_3, M_{30}; R_3) refer to the same resource B_3. r_{32} in (N_3, M_{30}; R_3) and r_{41} in (N_4, M_{40}; R_4) refer to the same resource B_4. r_{42} in (N_4, M_{40}; R_4) and r_{11} in (N_1, M_{10}; R_1) refer to the same resource B_1. We first obtain the composite augmented marked graphs (N', M_0'; R') of (N_1, M_{10}; R_1) and (N_2, M_{20}; R_2) via $\{ (r_{12}, r_{21}) \}$, and composite augmented marked graph (N", M_0"; R") of (N_3, M_{30}; R_3) and (N_4, M_{40}; R_4) via $\{ (r_{32}, r_{41}) \}$.

Figure 3 shows (N', M_0'; R'), where r_2 is the place after fusing r_{12} and r_{21}. Figure 4 shows (N", M_0"; R"), where r_4 is the place after fusing r_{32} and r_{41}.

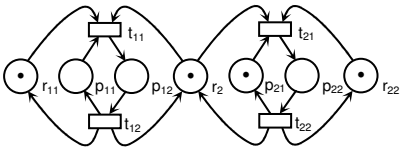

Fig. 3: Composite augmented marked graph (N', M_0'; R').

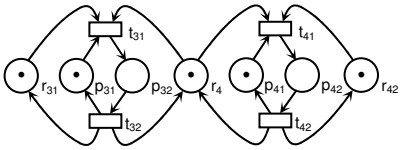

Fig. 4: Composite augmented marked graph (N", M_0"; R").

(N_1, M_{10}; R_1), (N_2, M_{20}; R_2), (N_3, M_{30}; R_3) and (N_4, M_{40}; R_4) are live, bounded, reversible and conservative. According to Properties 3.2 and 3.3, the composite augmented marked graphs (N', M_0'; R') and (N", M_0"; R") are bounded and conservative. For (N', M_0', R') where $R_F' = \{ r_2 \}$, no R_F'-siphons would eventually become empty. According to Property 3.5, (N', M_0', R') is live and reversible. For (N", M_0", R") where $R_F" = \{ r_4 \}$, no $R_F"$-siphons would eventually become empty. According to Property 3.5, (N", M_0", R") is live and reversible.

Next, we obtain the final composite augmented marked graph (N, M_0; R) of (N', M_0'; R') and (N", M_0"; R") via { (r_{11}, r_{42}), (r_{22}, r_{31}) }. Figure 5 shows (N, M_0; R), where r_1 is the place after fusing r_{11} and r_{42}, and r_3 is the place after fusing r_{22} and r_{31}. Table 2 lists the semantic meanings of its places and transitions.

Since (N', M_0'; R') and (N", M_0"; R") are live, bounded, reversible and conservative, according to Properties 3.2 and 3.3, the composite augmented marked graph (N, M_0; R) is bounded and conservative. For (N, M_0; R) where $R_F = \{ r_1, r_3 \}$, no R_F-siphons would eventually become empty. According to Property 3.5, (N, M_0; R) is live and reversible. It can be concluded that the integrated system is correct or well-behaved.

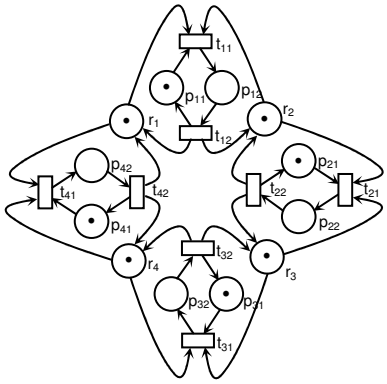

Fig. 5: The final composite augmented marked graphs (N, M_0; R).

P / T	Semantic Meaning
p_{11}	Y_1 is ready
p_{12}	Y_1 is occupying B_1 and B_2 and performing assembly
p_{21}	Y_2 is ready
p_{22}	Y_2 is occupying B_2 and B_3 and performing assembly
p_{31}	Y_3 is ready
p_{32}	Y_3 is occupying B_3 and B_4 and performing assembly
p_{41}	Y_4 is ready
p_{42}	Y_4 is occupying B_4 and B_1 and performing assembly
r_1	B_1 is available
r_2	B_2 is available
r_3	B_3 is available
r_4	B_4 is available
t_{11}	C_1 acquires B_1 and B_2 and starts assembly
t_{12}	C_1 finishes assembly and releases Y_1, B_1 and B_2
t_{21}	C_2 acquires B_2 and B_3 and starts assembly
t_{22}	C_2 finishes assembly and releases Y_2, B_2 and B_3
t_{31}	C_3 acquires B_3 and B_4 and starts assembly
t_{32}	C_3 finishes assembly and releases Y_3, B_3 and B_4
t_{41}	C_4 acquires B_4 and B_1 and starts assembly
t_{42}	C_4 finishes assembly and releases Y_4, B_4 and B_1

Table 2: Semantic meaning of places and transitions in Figure 5.

5. Conclusion

This paper investigates the compositional correctness of system components, based on the property-preserving composition of augmented marked graphs.

It has been shown that, in composing two augmented marked graphs via their common resource places, boundedness and conservativeness are preserved while liveness and reversibility can be preserved under a pretty simple condition. We apply this composition of augmented marked graphs to component-based system design. By modelling the components as augmented marked graphs with the common resources denoted by the resource places, an integrated system can be obtained by composing these augmented marked graphs via their common resource places. Based on the property-preservation of this composition, the liveness, boundedness, reversibility and conservativeness of the integrated system can be readily derived.

Liveness, boundedness, reversibility and conservativeness are key attributes that collectively characterise the correctness and well-behavedness of a system. In synthesising a system from its components, it is important to assure that these essential properties can be preserved, especially as there involve shared resources wherein erroneous situations such as deadlocks and capacity overflows can be easily induced. The composition of augmented marked graphs proposed in this paper contributes to component-based system design to provide an effective means of synthesising a system from its components, where the system correctness can be readily verified.

6. References

[1] F. Chu and X. Xie, "Deadlock Analysis of Petri Nets Using Siphons and Mathematical Programming", *IEEE Transactions on Robotics and Automation*, Vol. 13, No. 6, pp. 793-804, 1997.

[2] K.S. Cheung, "New Characterisations for Live and Reversible Augmented Marked Graphs", *Information Processing Letters*, Vol. 92, No. 5, pp. 239-243, 2004.

[3] K.S. Cheung and K.O. Chow, "Cycle Inclusion Property of Augmented Marked Graphs", *Information Processing Letters*, Vol. 94, No. 6, pp. 271-276, 2005.

[4] K.S. Cheung, "Boundedness and Conservativeness of Augmented Marked Graphs", *IMA Journal of Mathematical Control and Information*, Vol. 24, No. 2, pp. 235-244, 2007.

[5] H.J. Huang, L. Jiao and T.Y. Cheung, "Property-Preserving Composition of Augmented Marked Graphs that Share Common Resources", *Proceedings of the IEEE International Conference on Robotics and Automation*, Vol. 1, pp. 1446-1451, IEEE, 2003.

[6] K.S. Cheung and K.O. Chow (2007), "Compositional Synthesis of Augmented Marked Graphs", *Proceedings of the IEEE International Conference on Control and Automation*, pp. 2810-2814, IEEE, 2007.

[7] W. Reisig, *Petri Nets : An Introduction*, Springer, 1985.

[8] T. Murata, "Petri Nets : Properties, Analysis and Applications", *Proceedings of the IEEE*, Vol. 77, No. 4, pp. 541-580, 1989.

[9] J. Desel and W. Reisig, "Place Transition Petri Nets", *Lectures on Petri Nets : Basic Models, Lecture Notes in Computer Science*, Vol. 1491, pp. 122-173, Springer-Verlag, 1998.

[10] G.T. Heineman and W.T. Councill, *Component-Based Software Engineering : Putting the Pieces Together*, Addison-Wesley, 2002.

[11] I. Crnkovic and M. Larsson, *Building Reliable Component-Based Software Systems*, Artech House, 2002.

[12] C. Szyperski, *Component Software : Beyond Object-Oriented Programming*, Addison-Wesley, 2002.