An Abstract Framework for Deadlock Prevention in BIP*

Paul C Attie[1], Saddek Bensalem[2], Marius Bozga[3], Mohamad Jaber[4], Joseph Sifakis[5], and Fadi A Zaraket[6]

[1]Department of Computer Science, American University of Beirut, Beirut, Lebanon
[2]UJF-Grenoble 1 / CNRS VERIMAG UMR 5104, Grenoble, F-38041, France
[3]UJF-Grenoble 1 / CNRS VERIMAG UMR 5104, Grenoble, F-38041, France
[4]Department of Computer Science, American University of Beirut, Beirut, Lebanon
[5]Rigorous System Design Laboratory, EPFL, Lausanne, Switzerland
[6]Department of Electrical and Computer Engineering, American University of Beirut, Beirut, Lebanon

July 22, 2015

Abstract

We present a sound but incomplete criterion for checking deadlock freedom of finite state systems expressed in BIP: a component-based framework for the construction of complex distributed systems. Since deciding deadlock-freedom for finite-state concurrent systems is PSPACE-complete, our criterion gives up completeness in return for tractability of evaluation. Our criterion can be evaluated by model-checking subsystems of the overall large system. The size of these subsystems depends only on the local topology of direct interaction between components, and *not* on the number of components in the overall system.

We present two experiments, in which our method compares favorably with existing approaches. For example, in verifying deadlock freedom of dining philosphers, our method shows linear increase in computation time with the number of philosophers, whereas other methods (even those that use abstraction) show super-linear increase, due to state-explosion.

1 Introduction

Deadlock freedom is a crucial property of concurrent and distributed systems. With increasing system complexity, the challenge of assuring deadlock freedom and other correctness properties becomes even greater. In contrast to the alternatives of (1) deadlock detection and recovery, and (2) deadlock avoidance, we advocate deadlock prevention: design the system so that deadlocks do not occur.

Deciding deadlock freedom of finite-state concurrent programs is PSPACE-complete in general [15, chapter 19]. To achieve tractability, we can either make our deadlock freedom check

*The research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7/2007-2013] under grant agreement no. 288175 (CERTAINTY) and no 257414 (ASCENS).

incomplete (sufficient but not necessary), or we can restrict the systems that we check to special cases. We choose the first option: a system meeting our condition is free of both local and global deadlocks, while a system which fails to meet our condition may or may not be deadlock free.

We generalize previous works [2, 3, 4] by removing the requirement that interaction between processes be expressed pairwise, and also by applying to BIP [6], a framework from which efficient distributed code can be generated. In contrast, the model of concurrency in [2, 3, 4] requires shared memory read-modify-write operations with a large grain of atomicity. The full paper, including proofs for all theorems, is available on-line, as is our implementation of the method.

2 BIP — Behavior Interaction Priority

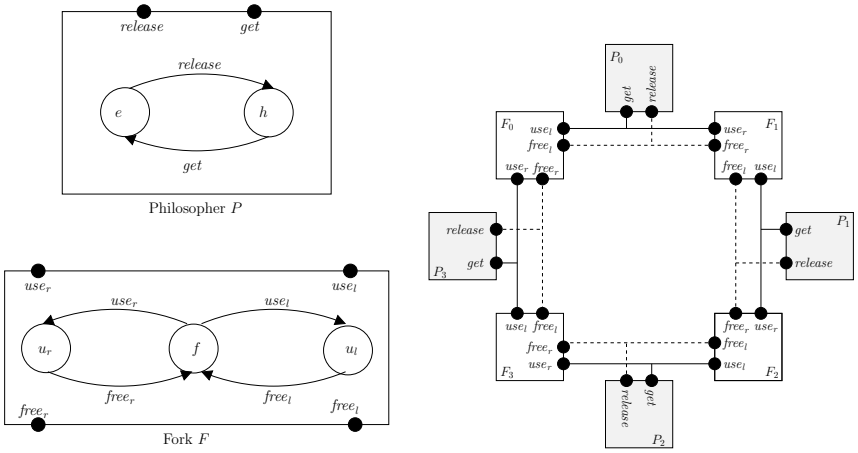
BIP is a component framework for constructing systems by superposing three layers of modeling: Behavior, Interaction, and Priority. A technical treatment of priority is beyond the scope of this paper. Adding priorities never introduces a deadlock, since priority enforces a choice between possible transitions from a state, and deadlock-freedom means that there is at least one transition from every (reachable) state. Hence if a BIP system without priorities is deadlock-free, then the same system with priorities added will also be deadlock-free.

Definition 1 (Atomic Component) *An* atomic component B_i *is a labeled transition system represented by a triple* $(Q_i, P_i, \rightarrow_i)$ *where* Q_i *is a set of* states*,* P_i *is a set of* communication ports*, and* $\rightarrow_i \subseteq Q_i \times P_i \times Q_i$ *is a set of* possible transitions*, each labeled by some port.*

For states $s_i, t_i \in Q_i$ and port $p_i \in P_i$, write $s_i \xrightarrow{p_i}_i t_i$, iff $(s_i, p_i, t_i) \in \rightarrow_i$. When p_i is irrelevant, write $s_i \rightarrow_i t_i$. Similarly, $s_i \xrightarrow{p_i}_i$ means that there exists $t_i \in Q_i$ such that $s_i \xrightarrow{p_i}_i t_i$. In this case, p_i is *enabled* in state s_i. Ports are used for communication between different components, as discussed below.

In practice, we describe the transition system using some syntax, e.g., involving variables. We abstract away from issues of syntactic description since we are only interested in enablement of ports and actions. We assume that enablement of a port depends only on the local state of a component. In particular, it cannot depend on the state of other components. This is a restriction on BIP, and we defer to subsequent work how to lift this restriction. So, we assume the existence of a predicate $enb^i_{p_i}$ that holds in state s_i of component B_i iff port p_i is enabled in s_i, i.e., $s_i(enb^i_{p_i}) = true$ iff $s_i \xrightarrow{p_i}_i$.

Figure 1(a) shows atomic components for a philospher P and a fork F in dining philosophers. A philosopher P that is hungry (in state h) can eat by executing *get* and moving to state e (eating). From e, P releases its forks by executing *release* and moving back to h. Adding the thinking state does not change the deadlock behaviour of the system, since the thinking to hungry transition is internal to P, and so we omit it. A fork F is taken by either: (1) the left philosopher (transition get_l) and so moves to state u_l (used by left philosopher), or (2) the right philosopher (transition get_r) and so moves to state u_r (used by right philosopher). From state u_r (resp. u_l), F is released by the right philosopher (resp. left philosopher) and so moves back to state f (free).



(a) Philosopher P and fork F atomic components.

(b) Dining philosophers composite component with four philosophers.

Figure 1: Dining philosophers.

Definition 2 (Interaction) *For a given system built from a set of n atomic components $\{\mathsf{B}_i = (Q_i, P_i, \rightarrow_i)\}_{i=1}^n$, we require that their respective sets of ports are pairwise disjoint, i.e., for all i, j such that $i, j \in \{1..n\} \wedge i \neq j$, we have $P_i \cap P_j = \emptyset$. An* interaction *is a set of ports not containing two or more ports from the same component. That is, for an interaction a we have $a \subseteq P \wedge (\forall\, i \in \{1..n\} : |\mathsf{a} \cap P_i| \leq 1)$, where $P = \bigcup_{i=1}^n P_i$ is the set of all ports in the system. When we write $a = \{p_i\}_{i \in I}$, we assume that $p_i \in P_i$ for all $i \in I$, where $I \subseteq \{1..n\}$.*

Execution of an interaction $\mathsf{a} = \{p_i\}_{i \in I}$ involves all the components which have ports in a. We denote by *components*(a) the set of atomic components participating in a, formally: *components*$(\mathsf{a}) = \{\mathsf{B}_i \mid p_i \in \mathsf{a}\}$.

Definition 3 (Composite Component) *A* composite component *(or simply* component*)* $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *is defined by a composition operator parameterized by a set of interactions $\gamma \subseteq 2^P$. B has a transition system $(Q, \gamma, \rightarrow)$, where $Q = Q_1 \times \cdots \times Q_n$ and $\rightarrow \subseteq Q \times \gamma \times Q$ is the least set of transitions satisfying the rule*

$$\frac{\mathsf{a} = \{p_i\}_{i \in I} \in \gamma \qquad \forall i \in I : s_i \xrightarrow{p_i}_i t_i \qquad \forall i \notin I : s_i = t_i}{\langle s_1, \ldots, s_n \rangle \xrightarrow{\mathsf{a}} \langle t_1, \ldots, t_n \rangle}$$

This inference rule says that a composite component $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ can execute an interaction $\mathsf{a} \in \gamma$, iff for each port $p_i \in \mathsf{a}$, the corresponding atomic component B_i can execute a transition labeled with p_i; the states of components that do not participate in the interaction stay unchanged. Figure 1(b) shows a composite component consisting of four philosophers and the four forks between them. Each philosopher and its two neighboring forks share two interactions: $Get = \{get, use_l, use_r\}$ in which the philosopher obtains the forks, and $Rel = \{release, free_l, free_r\}$ in which the philosopher releases the forks.

Definition 4 (Interaction enablement) *An atomic component* $\mathsf{B}_i = (Q_i, P_i, \rightarrow_i)$ *enables a port* $p_i \in P_i$ *in state* s_i *iff* $s_i \xrightarrow{p_i}_i$. B_i *enables interaction* a *in state* s_i *iff* $s_i \xrightarrow{p_i}_i$, *where* $\{p_i\} = P_i \cap a$ *is the port of* B_i *involved in* a. *That is,* B_i *enables* a *in state* s_i *iff* B_i *enables port* $\mathsf{a} \cap P_i$ *in state* s_i.

Let $enb^i_{p_i}$ *denote the enablement condition for port* p_i *in component* B_i, *that is,* $enb^i_{p_i}$ *holds iff* s_i *is the current state of* B_i *and* $s_i \xrightarrow{p_i}_i$. *Let* enb^i_a *denote the enablement condition for interaction* a *in component* B_i, *that is,* $enb^i_a = enb^i_{p_i}$ *where* $\{p_i\} = a \cap P_i$.

Let $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *be a composite component, and let* $s = \langle s_1, \ldots, s_n \rangle$ *be a state of* B. *Then* B *enables* a *in* s *iff every* $\mathsf{B}_i \in components(\mathsf{a})$ *enables* a *in* s_i.

The definition of interaction enablement is a consequence of Definition 3. Interaction a being enabled in state s means that executing a is one of the possible transitions that can be taken from s.

To avoid pathological cases of deadlock due solely to a single component refusing to enable any interaction at all, we assume that every component always enables at least one interaction. Structurally, this means that there is no local state zero transitions, and every port labeling a transition is part of at least one interaction.

Definition 5 (Local Enablement Assumption) *For every component* $\mathsf{B}_i = (Q_i, P_i, \rightarrow_i)$, *the following holds. In every* $s_i \in Q_i$, B_i *enables some interaction* a.

Definition 6 (BIP System) *Let* $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *be a composite component with transition system* $(Q, \gamma, \rightarrow)$, *and let* $Q_0 \subseteq Q$ *be a set of initial states. Then* (B, Q_0) *is a BIP system.*

Figure 1(b) gives a BIP-system with philosophers initially in state h (hungry) and forks initially in state f (free).

To avoid tedious repetition, we fix, for the rest of the paper, an arbitrary BIP-system (B, Q_0), with $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$, and transition system $(Q, \gamma, \rightarrow)$.

Definition 7 (Execution) *Let* (B, Q_0) *be a BIP system with transition system* $(Q, \gamma, \rightarrow)$. *Let* $\rho = s_0 a_1 s_1 \ldots s_{i-1} a_i s_i \ldots$ *be an alternating sequence of states of* B *and interactions of* B. *Then* ρ *is an execution of* (B, Q_0) *iff (1)* $s_0 \in Q_0$, *and (2)* $\forall\, i > 0 : s_{i-1} \xrightarrow{a_i} s_i$.

Definition 8 (Reachable state, transition) *A state or transition that occurs in some execution is called* reachable.

Definition 9 (State Projection) *Let* (B, Q_0) *be a BIP system where* $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *and let* $s = \langle s_1, \ldots, s_n \rangle$ *be a state of* (B, Q_0). *Let* $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\} \subseteq \{\mathsf{B}_1, \ldots, \mathsf{B}_n\}$. *Then* $s{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\} \triangleq \langle s_{j_1}, \ldots, s_{j_k} \rangle$. *For a single* B_i, *we write* $s{\restriction}\mathsf{B}_i = s_i$. *We extend state projection to sets of states element-wise.*

Definition 10 (Subcomponent) *Let* $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *be a composite component, and let* $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ *be a subset of* $\{\mathsf{B}_1, \ldots, \mathsf{B}_n\}$. *Let* $P' = P_{j_1} \cup \cdots \cup P_{j_k}$, *i.e., the union of the ports of* $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. *Then the subcomponent* B' *of* B *based on* $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ *is as follows:*

1. $\gamma' \triangleq \{\mathsf{a} \cap P' \mid \mathsf{a} \in \gamma \wedge \mathsf{a} \cap P' \neq \emptyset\}$
2. $\mathsf{B}' \triangleq \gamma'(\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k})$

That is, γ' consists of those interactions in γ that have at least one participant in $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$, and restricted to the participants in $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$, i.e., participants not in $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ are removed.

We write $s{\restriction}\mathsf{B}'$ to indicate state projection onto B', and define $s{\restriction}\mathsf{B}' \triangleq s{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$, where $\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}$ are the atomic components in B'.

Definition 11 (Subsystem) *Let (B, Q_0) be a BIP system where $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$, and let $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ be a subset of $\{\mathsf{B}_1, \ldots, \mathsf{B}_n\}$. Then the subsystem (B', Q_0') of (B, Q_0) based on $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ is as follows:*

1. *B' is the subcomponent of B based on $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$*
2. *$Q_0' = Q_0{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$*

We write $s{\restriction}\mathsf{B}'$ as an abbreviation for $s{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$.

Definition 12 (Execution Projection) *Let (B, Q_0) be a BIP system where $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$, and let (B', Q_0'), with $\mathsf{B}' = \gamma'(\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k})$ be the subsystem of (B, Q_0) based on $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. Let $P' = P_{j_1} \cup \cdots \cup P_{j_k}$,i.e., P' is the set of ports of (B', Q_0'). Let $\rho = s_0\mathsf{a}_1 s_1 \ldots s_{i-1}\mathsf{a}_i s_i \ldots$ be an execution of (B, Q_0). Then, $\rho{\restriction}(\mathsf{B}', Q_0')$, the projection of ρ onto (B', Q_0'), is the sequence resulting from:*

1. *replacing each s_i by $s_i{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$, i.e., replacing each state by its projection onto $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$*
2. *removing all $\mathsf{a}_i s_i$ where $\mathsf{a}_i \cap P' = \emptyset$*
3. *replacing each a_i by $\mathsf{a}_i \cap P'$, i.e., replacing each interaction by its projection onto the port set P'*

Proposition 1 (Execution Projection) *Let (B, Q_0) be a BIP system where $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$, and let (B', Q_0'), with $B' = \gamma'(\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k})$ be the subsystem of (B, Q_0) based on $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. Let $P' = P_{j_1} \cup \cdots \cup P_{j_k}$, i.e., the union of the ports of $\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. Let $\rho = s_0\mathsf{a}_1 s_1 \ldots s_{i-1}\mathsf{a}_i s_i \ldots$ be an execution of (B, Q_0). Then, $\rho{\restriction}(\mathsf{B}', Q_0')$ is an execution of (B', Q_0').*

Proof. Let $\rho = s_0\mathsf{a}_1 s_1 \ldots s_{i-1}\mathsf{a}_i s_i \ldots$, be an execution of (B, Q_0), and let $s_0' = s_0{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$.

Then, by Definitions 11 and 12, $s_0' \in Q_0'$ and $\rho{\restriction}(B', Q_0') = s_0' b_1 s_1' b_2 s_2' \ldots$ for some $b_1 s_1' b_2 s_2' \ldots$, where $s_j' \in Q' = Q{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ for $j \geq 1$.

Consider an arbitrary step (s_{j-1}', b_j, s_j') of $\rho{\restriction}(\mathsf{B}', Q_0')$. Since $b_j s_j'$ was not removed in Clause 2 of Definition 12, we have

(1) $s_j' = s_k{\restriction}\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ for some $k > 0$ and such that $\mathsf{a}_k \cap P' \neq \emptyset$
(2) $b_j = \mathsf{a}_k \cap P'$

(3) $s'_{j-1} = s_\ell\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ for the smallest ℓ such that
$\ell < k$ and $\forall\, m : \ell + 1 \leq m < k : \mathsf{a}_m \cap P' = \emptyset$

From (3) and Definitions 3 and 12, $s_\ell\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\} = s_{k-1}\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. Hence $s'_{j-1} = s_{k-1}\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. From $s_{k-1} \xrightarrow{\mathsf{a}_k} s_k$, $\mathsf{a}_k \cap P' \neq \emptyset$, and Definition 3, we have $s_{k-1}\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\} \xrightarrow{\mathsf{a}_k} s_k\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$. Hence $s'_{j-1} \xrightarrow{b_j} s'_j$ from $s'_{j-1} = s_{k-1}\restriction\{\mathsf{B}_{j_1}, \ldots, \mathsf{B}_{j_k}\}$ established above and (1), (2).

Since (s'_{j-1}, b_j, s'_j) was arbitrarily chosen, we conclude that every step of $\rho\restriction(\mathsf{B}', Q'_0)$ is a step of (B', Q'_0). Since the first state of $\rho\restriction(\mathsf{B}', Q'_0)$ is s_0, and $s_0 \in Q'_0$, we have established that $\rho\restriction(\mathsf{B}', Q'_0)$ is an execution of (B', Q'_0). □

Corollary 2 *Let (B', Q'_0) be a subsystem of (B, Q_0), and let P' be the port set of (B', Q'_0). Let s be a reachable state of (B, Q_0). Then $s\restriction\mathsf{B}'$ is a reachable state of (B', Q'_0). Let $s \xrightarrow{\mathsf{a}} t$ be a reachable transition of (B, Q_0), and let a be an interaction of (B', Q'_0). Then $s\restriction\mathsf{B}' \xrightarrow{\mathsf{a}\cap P'} t\restriction\mathsf{B}'$ is a reachable transition of (B', Q'_0).*

Proof. Immediate corollary of Proposition 1. □

3 Characterizing Deadlock-freedom

Definition 13 (Global Deadlock-freedom) *A BIP-system (B, Q_0) is* free of global deadlock *iff, in every reachable state s of (B, Q_0), some interaction a is enabled. Formally, $\forall\, s \in rstates(\mathsf{B}, Q_0), \exists\, \mathsf{a} : s \xrightarrow{\mathsf{a}}_{\mathsf{B}}$.*

Definition 14 (Local Deadlock-freedom) *A BIP-system (B, Q_0) is* free of local deadlock *iff, for every subsystem (B', Q'_0) of (B, Q_0), and every reachable state s of (B, Q_0), (B', Q'_0) has some interaction enabled in state $s\restriction\mathsf{B}'$. Formally:*
for every subsystem (B', Q'_0) of (B, Q_0):
$\forall\, s \in rstates(\mathsf{B}, Q_0), \exists\, \mathsf{a} : s\restriction\mathsf{B}' \xrightarrow{\mathsf{a}}_{\mathsf{B}'}$.

Proposition 3 states that the existence of a supercycle implies a local deadlock: all components in the supercycle are blocked forever.

Proposition 4 states that the existence of a supercycle is necessary for a local deadlock to occur: if a set of components, *considered in isolation*, are blocked, then there exists a supercycle consisting of exactly those components, together with the interactions that each component enables.

3.1 Wait-for graphs

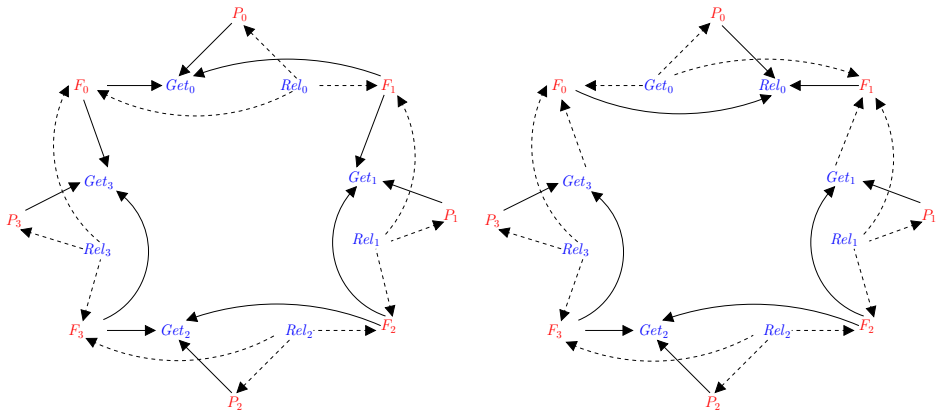
The wait-for-graph for a state s is a directed bipartite and-or graph which contains as nodes the atomic components $\mathsf{B}_1, \ldots, \mathsf{B}_n$, and all the interactions γ. Edges in the wait-for-graph are from a B_i to all the interactions that B_i enables (in s), and from an interaction a to all the components that participate in a and which do not enable it (in s).

Definition 15 (Wait-for-graph $W_{\mathsf{B}}(s)$) *Let $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ be a BIP composite component, and let $s = \langle s_1, \ldots, s_n \rangle$ be an arbitrary state of B. The* wait-for-graph *$W_{\mathsf{B}}(s)$ of s is a directed bipartite and-or graph, where*

1. *the nodes of $W_{\mathsf{B}}(s)$ are as follows:*
   (a) *the and-nodes are the atomic components B_i, $i \in \{1..n\}$,*
   (b) *the or-nodes are the interactions $\mathsf{a} \in \gamma$,*
2. *there is an edge in $W_{\mathsf{B}}(s)$ from B_i to every node a such that $\mathsf{B}_i \in components(\mathsf{a})$ and $s_i(enb^i_{\mathsf{a}}) = true$, i.e., from B_i to every interaction which B_i enables in s_i,*
3. *there is an edge in $W_{\mathsf{B}}(s)$ from a to every B_i such that $\mathsf{B}_i \in components(\mathsf{a})$ and $s_i(enb^i_{\mathsf{a}}) = false$, i.e., from a to every component B_i which participates in a but does not enable it, in state s_i.*

A component B_i is an and-node since all of its successor actions (or-nodes) must be disabled for B_i to be incapable of executing. An interaction a is an or-node since it is disabled if any of its participant components do not enable it. An edge (path) in a wait-for-graph is called a wait-for-edge (wait-for-path). Write $\mathsf{a} \to \mathsf{B}_i$ ($\mathsf{B}_i \to \mathsf{a}$ respectively) for a wait-for-edge from a to B_i (B_i to a respectively). We abuse notation by writing $e \in W_{\mathsf{B}}(s)$ to indicate that e (either $\mathsf{a} \to \mathsf{B}_i$ or $\mathsf{B}_i \to \mathsf{a}$) is an edge in $W_{\mathsf{B}}(s)$. Also $\mathsf{B}_i \to \mathsf{a} \to \mathsf{B}'_i \in W_{\mathsf{B}}(s)$ for $B_i \to \mathsf{a} \in W_{\mathsf{B}}(s) \wedge \mathsf{a} \to B'_i \in W_{\mathsf{B}}(s)$, i.e., for a wait-for-path of length 2, and similarly for longer wait-for-paths.

Consider the dining philosophers system given in Figure 1. Figure 2(a) shows its wait-for-graph in its sole initial state. Figure 2(b) shows the wait-for-graph after execution of get_0. Edges from components to interactions are shown solid, and edges from interactions to components are shown dashed.



(a) Wait-for-graph in initial state.

(b) Wait-for-graph after execution of get_0.

Figure 2: Example wait-for-graphs for dining philosophers system of Figure 1.

3.2 Supercycles and deadlock-freedom

We characterize a deadlock as the existence in the wait-for-graph of a graph-theoretic construct that we call a *supercycle*:

Definition 16 (Supercycle) *Let* $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ *be a composite component and* s *be a state of* B*. A subgraph* SC *of* $W_{\mathsf{B}}(s)$ *is a supercycle in* $W_{\mathsf{B}}(s)$ *if and only if all of the following hold:*

1. *SC is nonempty, i.e., contains at least one node,*
2. *if B_i is a node in SC, then for all interactions a such that there is an edge in $W_{\mathsf{B}}(s)$ from B_i to a:*
   (a) *a is a node in SC, and*
   (b) *there is an edge in SC from B_i to a,*

   that is, $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(s)$ implies $\mathsf{B}_i \to \mathsf{a} \in SC$,
3. *if a is a node in SC, then there exists a B_j such that:*
   (a) *B_j is a node in SC, and*
   (b) *there is an edge from a to B_j in $W_{\mathsf{B}}(s)$, and*
   (c) *there is an edge from a to B_j in SC,*

   that is, $\mathsf{a} \in SC$ implies $\exists\, \mathsf{B}_j : \mathsf{a} \to \mathsf{B}_j \in W_{\mathsf{B}}(s) \wedge \mathsf{a} \to \mathsf{B}_j \in SC$,

where $\mathsf{a} \in SC$ means that a is a node in SC, etc. Also, write $SC \subseteq W_{\mathsf{B}}(s)$ when SC is a subgraph of $W_{\mathsf{B}}(s)$.

Definition 17 (Supercycle-free) $W_{\mathsf{B}}(s)$ *is* supercycle-free *iff there does not exist a supercycle SC in $W_{\mathsf{B}}(s)$. In this case, say that state s is supercycle-free. Formally, we define the predicate $sc\_free_B(s) \triangleq \neg\exists\, SC : SC \subseteq W_{\mathsf{B}}(s)$ and SC is a supercycle.*

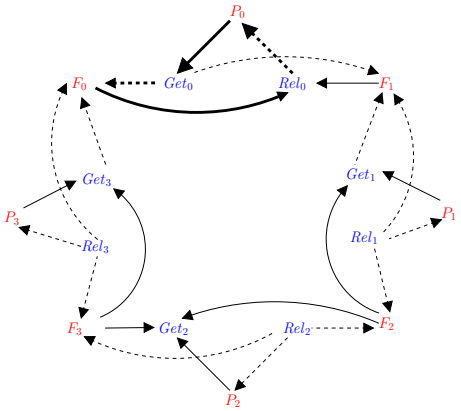


Figure 3: Example supercycle for dining philosophers system of Figure 1.

Figure 3 shows an example supercycle (with boldened edges) for the dining philosophers system of Figure 1. P_0 waits for (enables) a single interaction, Get_0. Get_0 waits for (is disabled by) fork F_0, which waits for interaction Rel_0. Rel_0 in turn waits for P_0. However, this supercycle occurs in a state where P_0 is in h and F_0 is in u_l. This state is not reachable from the initial state.

Figure 4 shows an "abstract" example, where these is a cycle of wait-for-edges, without there being a supercycle.This shows that a cycle does not necessarily imply a supercycle, and hence deadlock. Adding a wait-for-edge from d to B_1 would create a supercycle in Figure 4.

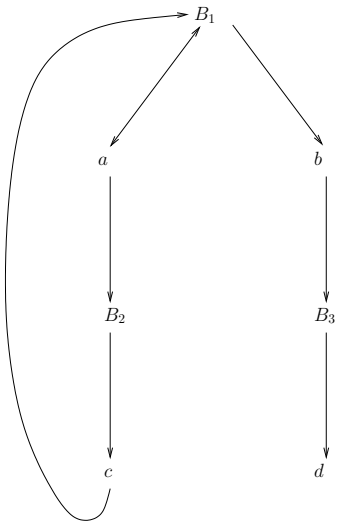


Figure 4: Example where a wait-for cycle does not imply deadlock

The existence of a supercycle is sufficient and necessary for the occurrence of a deadlock, and so checking for supercycles gives a sound and complete check for deadlocks. Proposition 3 states that the existence of a supercycle implies a local deadlock: all components in the supercycle are blocked forever.

Proposition 3 *Let s be a state of B. If $SC \subseteq W_{\mathsf{B}}(s)$ is a supercycle, then all components B_i in SC cannot execute a transition in any state reachable from s, including s itself.*

Proof. Let B_i be an arbitrary component in SC. By Definition 16, every interaction that B_i enables has a wait-for-edge to some other component B_j in SC and so cannot be executed in state s. Hence in any transition from s to another global state t, all of the components B_i in SC remain in the same local state. Hence $SC \subseteq W_{\mathsf{B}}(t)$, i.e., the same supercycle SC remains in global state t. Repeating this argument from state t and onwards leads us to conclude that $SC \subseteq W_{\mathsf{B}}(u)$ for any state u reachable from s. □

Proposition 4 states that the existence of a supercycle is necessary for a local deadlock to occur: if a set of components, *considered in isolation*, are blocked, then there exists a supercycle consisting of exactly those components, together with the interactions that each component enables.

Proposition 4 *Let B' be a subcomponent of B, and let s be an arbitrary state of B such that B', when considered in isolation, has no enabled interaction in state $s{\restriction}\mathsf{B}'$. Then, $W_{\mathsf{B}}(s)$ contains a supercycle.*

Proof. Let B_i be an arbitrary atomic component in B', and let a_i be any interaction that B_i enables. Since B' has no enabled interaction, it follows that a_i is not enabled in B', and therefore

has a wait-for-edge to some atomic component B_j in B'. Let SC be the subgraph of $W_{\mathsf{B}}(s)$ induced by:

1. the atomic components of B',
2. the interactions a that each atomic component B_i enables, and the edges $\mathsf{B}_i \to \mathsf{a}$, and
3. the edges $\mathsf{a} \to \mathsf{B}_j$ from each interaction to some atomic component B_j in B' that does not enable B_j.

SC satisfies Definition 16 and so is a supercycle. □

We consider subcomponent B' in isolation to avoid other phenomena that prevent interactions from executing, e.g., conspiracies [5]. Now the converse of Proposition 4 is that absence of supercycles in $W_{\mathsf{B}}(s)$ means there is no locally deadlocked subsystem.

Corollary 5 (Supercycle-free implies free of local deadlock) *If, for every reachable state s of (B, Q_0), $W_{\mathsf{B}}(s)$ is supercycle-free, then (B, Q_0) is free of local deadlock.*

Proof. We establish the contrapositive. Suppose that (B, Q_0) is not free of local deadlock. Then there exists a subsystem (B', Q_0') of (B, Q_0), and a reachable state s of (B', Q_0'), such that B' enables no interaction in state $s{\restriction}\mathsf{B}'$. By Proposition 4, $W_{\mathsf{B}}(s)$ contains a supercycle. □

In the sequel, we wil say "deadlock-free" to mean "free of local deadlock".

3.3 Structural properties of supercycles

We present some structural properties of supercycles, which are central to our deadlock-freedom conditions.

Definition 18 (Path, path length) *Let G be a directed graph and v a vertex in G. A path π in G is a* finite *sequence $v_0, v_1, \ldots, v_n$ such that (v_i, v_{i+1}) is an edge in G for all $i \in \{0, \ldots, n-1\}$. Write $path_G(\pi)$ iff π is a path in G. Define $first(\pi) = v_0$ and $last(\pi) = v_n$. Let $|\pi|$ denote the length of π, which we define as follows:*

- *if π is simple, i.e., all v_i, $0 \leq i \leq n$, are distinct, then $|\pi| = n$, i.e., the number of edges in π*
- *if π contains a cycle, i.e., there exist v_i, v_j such that $i \neq j$ and $v_i = v_j$, then $|\pi| = \omega$ (ω for "infinity").*

Definition 19 (In-depth, Out-depth) *Let G be a directed graph and v a vertex in G. Define the in-depth of v in G, notated as $in\_depth_G(v)$, as follows:*

- *if there exists a path π in G that contains a cycle and ends in v, i.e., $|\pi| = \omega \wedge last(\pi) = v$, then $in\_depth_G(v) = \omega$,*
- *otherwise, let π be a longest (simple) path ending in v. Then $in\_depth_G(v) = |\pi|$.*

Formally, $in\_depth_G(v) = (\text{MAX } \pi : path_G(\pi) \wedge last(\pi) = v : |\pi|)$.

Likewise define the out-depth of v in G, notated as $out\_depth_G(v)$, as follows:

- *if there exists a path π in G that contains a cycle and starts in v, i.e., $|\pi| = \omega \wedge first(\pi) = v$, then $out\_depth_G(v) = \omega$,*
- *otherwise, let π be a longest (simple) path starting in v. Then $out\_depth_G(v) = |\pi|$.*

Formally, $out\_depth_G(v) = (\text{MAX } \pi : path_G(\pi) \wedge first(\pi) = v : |\pi|)$.

We use $in\_depth_{\mathsf{B}}(v, s)$ for $in\_depth_{W_{\mathsf{B}}(s)}(v)$, and also $out\_depth_{\mathsf{B}}(v, s)$ for $out\_depth_{W_{\mathsf{B}}(s)}(v)$.

Proposition 6 *A supercycle SC contains no nodes with finite out-depth.*

Proof. By contradiction. Let v be a node in SC with finite out-depth. Hence by Definition 19 all outgoing paths from v are simple (and finite), and end in a sink node w, so w has no outgoing wait-for-edges. By assumption, all atomic components are individually deadlock-free, i.e., they always enable at least one interaction. So if w is an atomic component B_i, we have a wait-for-edge $\mathsf{B}_i \rightarrow \mathsf{a}$ for some interaction a, contradicting the fact that w is a sink node. Hence w is some interaction a. Since a has no outgoing edges, it violates clause 3 in Definition 16, contradicting the assumption that SC is a supercycle. □

Proposition 7 *Every supercycle SC contains at least two nodes.*

Proof. By Definition 16, SC is nonempty, and so contains at least one node v. If v is an interaction a, then by Definition 16, SC also contains some component B_i such that $\mathsf{a} \rightarrow \mathsf{B}_i$. If v is a component B_i, then, by assumption, B_i enables at least one interaction a, and by Definition 16, every interaction that B_i enables must be in SC. Hence in both cases, SC contains at least two nodes. □

Proposition 8 *Every supercycle SC contains at least one cycle.*

Proof. By contradiction. Suppose that SC is a supercycle and is also acyclic. Then every path in SC is simple, and therefore finite. Hence every node in SC has finite out-depth. By Proposition 6, SC cannot be a supercycle. □

Proposition 9 *Let $\mathsf{B} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ be a composite component and s a state of B. Let SC be a supercycle in $W_{\mathsf{B}}(s)$, and let SC' be the graph obtained from SC by removing all vertices of finite in-depth and their incident edges. Then SC' is also a supercycle in $W_{\mathsf{B}}(s)$.*

Proof. A vertex with finite in-depth cannot lie on a cycle in SC. Hence by Proposition 8, $SC' \neq \emptyset$. Thus SC' satisfies clause (1) of the supercycle definition (16). Let v be an arbitrary vertex of SC'. Thus $v \in SC$ and $in\_depth_{SC}(v) = \omega$ by definition of SC'. Let w be an arbitrary successor of v in SC. $in\_depth_{SC}(w) = \omega$ by Definition 19. Hence $w \in SC'$, by definition of SC'. Furthermore, w is a successor of v in SC', since SC' consists of *all* nodes of SC with infinite in-depth. Hence the successors of v in SC' are the same as the successors of v in SC Now since SC is a supercycle, every vertex v in SC has enough successors in SC to satisfy clauses (2) and (3) of the supercycle definition (16). It follows that every vertex v in SC' has enough successors in SC' to satisfy clauses (2) and (3) of the supercycle definition (16). □

Proposition 10 *Every supercycle SC contains a maximal strongly connected component CC such that (1) CC is itself a supercycle, and (2) there is no wait-for-edge from a node in CC to a node outside of CC.*

Proof. SC is a directed graph, and so consider the decomposition of SC into its maximal strongly connected components (MSCC). Let $\overline{SC}$ be the graph resulting from replacing each MSCC by a single node. By its construction, $\overline{SC}$ is acyclic, and so contains at least one node x with no outgoing edges. Let CC be the MSCC corresponding to x. It follows that CC is nonempty, and hence CC satisfies clause (1) of the supercycle definition (16). It also follows from the construction of CC that no node in CC has a wait-for-edge going to a node outside of CC, and so Clause (2) of the Proposition is established.

Let v be an arbitrary node in CC. Since $CC \subseteq SC$, v is a node of SC. Let w be an arbitrary successor of v in SC. Since no node in CC has an edge going to a node outside of CC, it follows that w is a node of CC. Hence v has the same successors in CC as in SC. Now since SC is a supercycle, every vertex v in SC has enough successors in SC to satisfy clauses (2) and (3) of the supercycle definition (16). It follows that every vertex v in CC has enough successors in CC to satisfy clauses (2) and (3) of the supercycle definition (16).

Hence, by Definition 16, CC is itself a supercycle, and so Clause (1) of the Proposition is established. □

Note also that by Proposition 7, CC contains at least two nodes. Hence CC is not a trivial strongly connected component.

3.4 Membership constraints for supercycles

Define $scyc^s_{\mathsf{B}}(\mathsf{B}_i)$, $scyc^s_{\mathsf{B}}(\mathsf{a})$ to mean that B_i, a, respectively, are nodes of a supercycle of $W_{\mathsf{B}}(s)$. If a component or interaction is not a node of a supercylcle, then we say that it has an *SC-violation.*

Definition 16, the definition of a supercycle, imposes certain constraints on membership of supercycles, for a given pattern of wait-for-edges. We outline these as follows:

1. If a component B_i has an interaction a such that $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(t)$ and a has a supercycle violation, then a cannot be part of a supercycle, and therefore neither can B_i, by Definition 16, Clause 2. Formally, if $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(s)$ then $\neg scyc^s_{\mathsf{B}}(\mathsf{a}) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)$.

2. If a component B_i has an interaction a such that $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(t)$ and a has a supercycle violation, then a cannot be part of a supercycle, and therefore neither can B_i, by Definition 16, Clause 3, since if B_i were in a supercycle, then a would be too. Formally, if $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(s)$ then $scyc^s_{\mathsf{B}}(\mathsf{B}_i) \Rightarrow scyc^s_{\mathsf{B}}(\mathsf{a})$, and so $\neg scyc^s_{\mathsf{B}}(\mathsf{a}) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)$.

From Clauses 1 and 2, we conclude that B_i has an SC-violation if $\exists\, \mathsf{a} : \mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(s) \vee \mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(s)$ and a has an SC-violation.

In some, but not all, cases, we gain some information by considering all the interactions (components) that a component (action) waits for:

1. For a given interaction a, let $\mathsf{B}_i, \ldots, \mathsf{B}_j$ be all the components B such that $\mathsf{a} \to B \in W_{\mathsf{B}}(s)$. Then $scyc^s_{\mathsf{B}}(\mathsf{a}) \Rightarrow (\exists\, B \in \mathsf{B}_i, \ldots, \mathsf{B}_j : scyc^s_{\mathsf{B}}(\mathsf{B}_i))$, by Definition 16, Clause 3. So a is in a

supercycle implies that some $B \in \mathsf{B}_i, \ldots, \mathsf{B}_j$ is in a supercycle. Taking the contrapositive, $(\forall\, B \in \mathsf{B}_i, \ldots, \mathsf{B}_j : \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{a})$. Thus, if no component that a waits for is in a supercycle, then a cannot be in a supercycle.

2. For a given interaction a, let $\mathsf{B}_i, \ldots, \mathsf{B}_j$ be all the components B such that $B \rightarrow \mathsf{a} \in W_{\mathsf{B}}(s)$. Then $\neg scyc^s_{\mathsf{B}}(\mathsf{a}) \Rightarrow (\forall\, B \in \mathsf{B}_i, \ldots, \mathsf{B}_j : \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i))$. So a has an SC-violation implies that $\forall\, B \in \mathsf{B}_i, \ldots, \mathsf{B}_j : B$ has an SC-violation. This can be seen as a repetitive application of Clause 1 of the previous list, and so it provides no new information.

3. For a given component B_i, let $\mathsf{a}_1, \ldots, \mathsf{a}_m$ be all the interactions a such that $\mathsf{B}_i \rightarrow \mathsf{a} \in W_{\mathsf{B}}(s)$. Then $\neg scyc^s_{\mathsf{B}}(\mathsf{B}_i) \Rightarrow (\exists\, \mathsf{a} \in \mathsf{a}_1, \ldots, \mathsf{a}_m : \neg scyc^s_{\mathsf{B}}(\mathsf{a}))$. Thus B_i has an SC-violation implies that some a has an SC-violation. This is not useful, since it does not determine the particular a with the violation. Hence this observation will not play a role in our future development.

4. For a given component B_i, let $\mathsf{a}_1, \ldots, \mathsf{a}_m$ be all the interactions a such that $\mathsf{a} \rightarrow \mathsf{B}_i \in W_{\mathsf{B}}(s)$. Then $scyc^s_{\mathsf{B}}(\mathsf{B}_i) \Rightarrow (\forall\, \mathsf{a} \in \mathsf{a}_1, \ldots, \mathsf{a}_m : scyc^s_{\mathsf{B}}(\mathsf{a}))$. Hence $(\exists\, \mathsf{a} \in \mathsf{a}_1, \ldots, \mathsf{a}_m : \neg scyc^s_{\mathsf{B}}(\mathsf{a})) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)$. Thus B_i has an SC-violation if some a that waits for B_i has an SC-violation. This can be seen as a repetitive application of Clause 2 of the previous list, and so it provides no new information.

Hence from the above 4 clauses, only clause 1 provides new information. Combining clauses 1 and 2 from the first list, and clause 1 from the second list, we obtain the following.

Proposition 11 (Supercycle-membership constraints) *scyc satisfies the following constraints.*

1. $(\exists\, \mathsf{a} : \mathsf{B}_i \rightarrow \mathsf{a} \in W_{\mathsf{B}}(s) : \neg scyc^s_{\mathsf{B}}(\mathsf{a})) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)$
2. $(\exists\, \mathsf{a} : \mathsf{a} \rightarrow \mathsf{B}_i \in W_{\mathsf{B}}(s) : \neg scyc^s_{\mathsf{B}}(\mathsf{a})) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)$
3. *For a given interaction* a*, let* $\mathsf{B}_i, \ldots, \mathsf{B}_j$ *be all the components* B *such that* $\mathsf{a} \rightarrow B \in W_{\mathsf{B}}(s)$*. Then* $(\forall\, B \in \mathsf{B}_i, \ldots, \mathsf{B}_j : \neg scyc^s_{\mathsf{B}}(\mathsf{B}_i)) \Rightarrow \neg scyc^s_{\mathsf{B}}(\mathsf{a})$.

Proof. Immediate from the preceding observations. □

4 Supercycle Formation and its Consequences

4.1 The supercycle formation condition

To proceed, we show that wait-for edges not involving some interaction a and its participants $\mathsf{B}_i \in components(\mathsf{a})$ are unaffected by the execution of a. Say that edge e in a wait-for-graph is B_i*-incident* iff B_i is one of the endpoints of e.

Proposition 12 (Wait-for edge preservation) *Let* $s \xrightarrow{\mathsf{a}} t$ *be a transition of composite component* $B = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$*, and let* e *be a wait-for edge in* $W_{\mathsf{B}}(s)$ *that is not* B_i*-incident, for every* $\mathsf{B}_i \in components(\mathsf{a})$*. Then* $e \in W_{\mathsf{B}}(s)$ *iff* $e \in W_{\mathsf{B}}(t)$*.*

Proof. Fix e to be an arbitrary wait-for-edge that is not B_i-incident. e is either $\mathsf{B}_j \to b$ or $b \to \mathsf{B}_j$, for some component B_j of B that is not in *components*(a), and an interaction b (different from a) that B_j participates in. Now $s\restriction \mathsf{B}_j = t\restriction \mathsf{B}_j$, since $s \xrightarrow{\mathsf{a}} t$ and $\mathsf{B}_j \notin$ *components*(a). Hence $s(enb_b^j) = t(enb_b^j)$. It follows from Definition 15 that $e \in W_{\mathsf{B}}(s)$ iff $e \in W_{\mathsf{B}}(t)$. □

Proposition 13 (Supercycle formation condition) *Assume that $s \xrightarrow{\mathsf{a}} t$ is a transition of (B, Q_0), $W_{\mathsf{B}}(s)$ is supercycle-free, and that $W_{\mathsf{B}}(t)$ contains a supercycle. Then, in $W_{\mathsf{B}}(t)$, there exists a CC such that*

1. *CC is a subgraph of $W_{\mathsf{B}}(t)$*
2. *CC is strongly connected*
3. *CC is a supercycle*
4. *in $W_{\mathsf{B}}(t)$, there is no wait-for edge from a node in CC to a node outside of CC.*
5. *there exists a component $\mathsf{B}_i \in$ components(a) such that B_i is in CC*

Proof. By assumption, there is a supercycle SC that is a subgraph of $W_{\mathsf{B}}(t)$. By Proposition 10, SC contains a subgraph CC that is strongly connected, is itself a supercycle, and such that there is no wait-for-edge from a node in CC to a node outside of CC. This establishes Clauses 1–4.

Now suppose $\mathsf{B}_i \notin CC$ for every $\mathsf{B}_i \in$ *components*(a). Then, no edge in CC is B_i-incident. Hence, by Proposition 12, every edge in CC is an edge in $W_{\mathsf{B}}(s)$. Hence CC is a subgraph of $W_{\mathsf{B}}(s)$.

Let v be an arbitrary node in CC. Suppose v is a component B_j. By assumption, $\mathsf{B}_j \notin$ *components*(a), and so $s\restriction \mathsf{B}_j = t\restriction \mathsf{B}_j$ by Definition 3. Hence B_j enables the same set of interactions in state s as in state t. in $W_{\mathsf{B}}(t)$, all of B_j's wait-for-edges must end in an interaction that is in CC, since CC is a a supercycle in $W_{\mathsf{B}}(t)$. Hence the same holds in $W_{\mathsf{B}}(s)$.

If v is an interaction, it must also have a wait-for-edge e' to some component $\mathsf{B}_j \in CC$, since CC is a supercycle in $W_{\mathsf{B}}(t)$.

Hence v has enough successors in CC to satisfy the supercycle definition (Def. 16),

Hence CC by itself is a supercycle in $W_{\mathsf{B}}(s)$, which contradicts the assumption that $W_{\mathsf{B}}(s)$ is supercycle-free. Hence, $\mathsf{B}_i \in CC$ for some $\mathsf{B}_i \in$ *components*(a), and so Clause 5 is established. □

4.2 Violations of the supercycle formation condition

We wish to check whether supercycles can be formed or not, i.e., whether the supercycle formation condition is satisfied or not. In principle, we could check directly whether $W_{\mathsf{B}}(t)$ contains a supercycle, for each reachable state t. However, this approach is subject to state-explosion, and so is usually unlikely to be viable in practice. Instead, we formulate global conditions for supercycle-freedom, and then "project" these conditions onto small subsystems, to obtain local versions of these conditions that are efficiently checkable.

For transition $s \xrightarrow{\mathsf{a}} t$, we determine for every component $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$ whether it is possible for B_i to be a node in a supercycle in $W_{\mathsf{B}}(t)$. If not, then we say that B_i satisfies the *supercycle violation* condition, and we formalize this condition below.

There are two ways for B_i to not be a node in a strongly-connected supercycle:

1. *no supercycle membership*: B_i is not a node of any supercycle, i.e., $\neg \mathit{scyc}^s_{\mathsf{B}}(\mathsf{B}_i)$.
2. *no strong-connectedness*: B_i is a node in a supercycle, but not a node in a *strongly-connected* supercycle.

4.3 Supercycle membership and supercycle violation

We use the term *supercycle-violation* to indicate that a node is not in any supercycle.

Definition 16 implies that the supercycle-membership status of a node v depends solely on its outgoing wait-for edges, and the outgoing wait-for edges of the nodes that v waits for, etc. so that v's supercycle-membership is a function of the subgraph of the wait-for graph that is reachable from v. Hence, we only look at outgoing wait-for edges in computing supercycle-violation, which is just the negation of supercycle-membership.

A node that is not in any supercycle may nevertheless be a node of a wait-for cycle, since a cycle of wait-for-edges does not necesarily imply a supercycle. Hence, to compute the supercycle violation condition properly, we introduce a notion of the *level* of a violation. A node with no outgoing wait-for edges has a level-1 violation. A node whose violation is based on outgoing edges to neighbors whose violation level is at most $d-1$, has itself a level-d violation. Hence we formalize the notion of *level-d supercycle violation* as the predicate $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$.

Definition 20 (Supercycle violation, $\mathsf{scViolate}_{\mathsf{B}}(v,d,t)$) *Let t be a state of (B, Q_0), v be a node of $W_{\mathsf{B}}(t)$, and d an integer ≥ 1. We define the predicate $\mathsf{scViolate}_{\mathsf{B}}(v,d,t)$ by induction on d, as follows. We indicate the justification for each clause of the definition.*

Base case, $d = 1$. $\mathsf{scViolate}_{\mathsf{B}}(v,1,t)$ *iff v is an interaction* a *and it has no outgoing wait-for-edges, otherwise* $\neg\mathsf{scViolate}_{\mathsf{B}}(v,1,t)$. *Justification: if v has no outgoing wait-for-edges, then it cannot be in a supercycle. Note that v must be an interaction in this case, since a component must have at least one outgoing wait-for edge at all times.*

Inductive step, $d > 1$. $\mathsf{scViolate}_{\mathsf{B}}(v,d,t)$ *iff any of the following cases hold. Otherwise* $\neg\mathsf{scViolate}_{\mathsf{B}}(v,d,t)$.

1. *v is a component B_i and there exists interaction a such that $\mathsf{B}_i \rightarrow \mathsf{a} \in W_{\mathsf{B}}(t)$ and $(\exists\, d' : 1 \leq d' < d : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{a}, d', t))$. That is, B_i enables an interaction a which has a level-d' supercycle-violation, for some $d' < d$. Justification is Proposition 11, Clause 1.*
2. *v is an interaction a and for all components B_i such that $\mathsf{a} \rightarrow \mathsf{B}_i \in W_{\mathsf{B}}(t)$, we have $(\exists\, d' : 1 \leq d' < d : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d', t))$. That is, each component B_i that a waits for has a level-d' supercycle-violation, for some $d' < d$. Justification is Proposition 11, Clause 3.*

Figure 5 gives a formal, recursive definition of $\mathsf{scViolate}_{\mathsf{B}}(v,d,t)$. The notation $v = \mathsf{B}_i$ means that v is some component B_i. Likewise, $v = \mathsf{a}$ means that v is some interaction a. Line 0

corresponds to the base case, line 1 corresponds to item 1 of the inductive case, and line 2 corresponds to item 2 of the inductive case. Line 3 handles all cases that do not return true.

$\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$
0. **if** $(d = 1 \wedge v = \mathsf{a} \wedge \neg(\exists\, \mathsf{B}_i : \mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(t)))$ **return**(`tt`) **fi** ▷base case for `tt` result
1. **if** $(v = \mathsf{B}_i \wedge (\exists\, \mathsf{a} : \mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(t) : (\exists\, d' : 1 \leq d' < d : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{a}, d', t))))$ **return**(`tt`) **fi**
2. **if** $(v = \mathsf{a} \wedge (\forall\, \mathsf{B}_i : \mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(t) : (\exists\, d' : 1 \leq d' < d : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d', t))))$ **return**(`tt`) **fi**
3. **return**(`ff`) ▷no case for `tt` result, so result is `ff`

Figure 5: Formal definition of $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$

In the sequel, we say sc-violation rather than "supercycle violation." The crucial result is that, if v has a level-d sc-violation, for some $d \geq 1$, then v cannot be a node of a supercycle.

Proposition 14 *If* $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v, d, t))$ *then* v *is not a node of a supercycle in* $W_{\mathsf{B}}(t)$.

Proof. Proof is by induction in d.

Base case, $d = 1$. v has no outgoing edges. Hence v cannot be in a supercycle.

Induction step, $d > 1$. Assume that v has a level d *SC*-violation. We have two cases.

Case 1: v is a component B_i. Hence there exists an interaction a such that $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(t)$ and a has a level-$(d-1)$ *SC*-violation. By the induction hypothesis, a cannot occur in a supercycle in $W_{\mathsf{B}}(t)$. By Proposition 11, Clause 1, B_i cannot be in a supercycle.

Case 2: v is an interaction a. Hence for all components B_i such that $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(t)$, B_i has a level-$(d-1)$ *SC*-violation. By the induction hypothesis, B_i cannot occur in a strongly connected supercycle in $W_{\mathsf{B}}(t)$. By Proposition 11, Clause 3, a cannot be in a supercycle.

□

Proposition 15 *If* $(\forall\, d \geq 1 : \neg\mathsf{scViolate}_{\mathsf{B}}(v, d, t))$ *then* v *is a node of a supercycle in* $W_{\mathsf{B}}(t)$.

Proof. Let V be the set of nodes in $W_{\mathsf{B}}(t)$ with a supercycle-violation, i.e., $V = \{w \mid w \in W_{\mathsf{B}}(t) \wedge (\exists\, d : \mathsf{scViolate}_{\mathsf{B}}(w, d, t))\}$. Let $\bar{V}$ be the remaining nodes, i.e., all nodes in $W_{\mathsf{B}}(t)$ that do not have a supercycle-violation, so $\bar{V} = \{w \mid w \in W_{\mathsf{B}}(t) \wedge (\forall\, d \geq 1 : \neg\mathsf{scViolate}_{\mathsf{B}}(v, d, t))\}$.

if $\bar{V}$ is empty then the proposition holds vacuously and we are done. So assume that $\bar{V}$ is non-empty and let v be an arbitrary node in $\bar{V}$.

Case 1: v is a component B_i. Suppose that there is a wait-for-edge from v to some interaction a that is in V. Then, by Definition 20, v has a supercycle violation, which contradicts the choice of v as a member of $\bar{V}$. Hence all wait-for-edges starting in v must end in a node in $\bar{V}$.

Case 2: v is an interaction a. Suppose that every wait-for-edge from v to some component B_i that is in V. Then, by Definition 20, v has a supercycle violation, which contradicts the choice of v as a member of $\bar{V}$. Hence some wait-for-edge starting in v must end in a node in $\bar{V}$.

Hence we have that $\bar{V}$ satisfies all three clauses of Definition 16: it is nonempty, each component in $\bar{V}$ has all its enabled interactions also in $\bar{V}$, and each interaction in $\bar{V}$ waits for a component in $\bar{V}$. Hence $\bar{V}$ as a whole is a supercycle. Since the nodes of $\bar{V}$ are, by definition

of $\bar{V}$, exactly the nodes v such that $(\forall\, d \geq 1 : \neg \mathsf{scViolate}_{\mathsf{B}}(v, d, t))$, we have that any such node is a node of a supercycle in $W_{\mathsf{B}}(t)$. Hence the Proposition is established. □

Proposition 16 *v is not a node of a supercycle in $W_{\mathsf{B}}(t)$ iff $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v, d, t))$.*

Proof. Immediate from Propositions 14 and 15. □

4.4 Strong connectedness condition

Given that B_i is a node in a supercycle, we wish to determine whether or not it is a node in a *strongly-connected* supercycle. We do this by removing all nodes with supercycle-violations, and then finding the maximal strongly connected components of the resulting wait-for subgraph.

Definition 21 (Strong connectedness violation, $\mathsf{sConnViolate}_{\mathsf{B}}(v,t)$) *Let v be a node of $W_{\mathsf{B}}(t)$. Then $\mathsf{sConnViolate}_{\mathsf{B}}(v,t)$ holds iff there does not exist a strongly connected supercycle SSC such that $v \in SSC$ and $SSC \subseteq W_B(t)$.*

4.5 Supercycle formation violation condition

Definition 22 (Formation violation, $\mathsf{formViolate}_{\mathsf{B}}(v,t)$) *Let v be a node of $W_{\mathsf{B}}(t)$. Then* $\mathsf{formViolate}_{\mathsf{B}}(v,t) \triangleq (\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v,d,t)) \vee \mathsf{sConnViolate}_{\mathsf{B}}(v,t)$.

Let $s \xrightarrow{\mathsf{a}} t$ be a reachable transition. If, for every $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$, $\mathsf{formViolate}_{\mathsf{B}}(v,t)$ holds, then $s \xrightarrow{\mathsf{a}} t$ does not introduce a supercycle, i.e., if s is supercycle-free, then so is t. We establish this in the sequel.

We remark that, as shown above $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v,d,t))$ implies that v cannot be in a supercycle. Hence, v cannot be in a strongly-connected supercycle. Hence $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v,d,t))$ implies $\mathsf{sConnViolate}_{\mathsf{B}}(v,t)$. It is however convenient to state the formation violation condition in this manner, since, in the sequel, we formulate a "local" version for each of $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v,d,t))$ and $\mathsf{sConnViolate}_{\mathsf{B}}(v,t)$, and the implication does not necessarily hold for the local versions. The advantage of the local versions is that they are usually efficiently computable, as we show in the sequel.

5 Global Conditions for Deadlock Freedom

The supercycle formation condition (Definition 13) tells us that, when a supercycle SC is created, some component B_i that participates in the interaction a whose execution created SC, must be a node of a strongly connected component CC of SC, and moreover CC is itself a supercycle in its own right. In a sense, CC is the "essential" part of SC.

Our fundamental condition for the prevention of supercycles then, is to require that, for every reachable transition $s \xrightarrow{\mathsf{a}} t$ resulting from execution of a, that every component B_i of a must exhibit a supercycle-violation (Definition 20) in global state t, i.e., the state resulting from the execution of a. For a given interaction a, we denote that condition $\mathcal{GALT}(\mathsf{a})$, and define

it formally below. This condition is, in a sense, the "most general" condition for supercycle-freedom.

If $\mathcal{GALT}(\mathsf{a})$ holds, and global state s is supercycle-free, and $s \xrightarrow{\mathsf{a}} t$, then it follows (as we establish below) that global state t is also supercycle-free. So, by requiring (1) that all initial states are supercycle-free, and (2) that $\mathcal{GALT}(\mathsf{a})$ holds for all interactions $\mathsf{a} \in \gamma$, we obtain, by straightforward induction on length of executions, that every reachable state is supercycle-free.

It also follows that any condition which implies $\mathcal{GALT}(\mathsf{a})$ is also sufficient to guarantee supercycle-freedom, and hence deadlock-freedom. We exploit this in two ways:

1. To provide a "linear" condition, $\mathcal{GLIN}$, that is easier to evaluate than $\mathcal{GALT}$, since it requires only the evaluation of lengths of wait-for-paths, i.e., it does not have the "alternating" character of $\mathcal{GALT}$.
2. To provide "local variants" of $\mathcal{GALT}$ and $\mathcal{GLIN}$, which can often be evaluated in small subsystems of (B, Q_0), thereby avoiding state-explosion. The local conditions imply the corresponding global ones, i.e., they are sufficient but not necessary for deadlock-freedom.

Since we will present several conditions for supercycle-freedom, we now present an abstract definition of the essential properties that all such conditions must have. First, we define a condition for the prevention of supercycles as a "behavioral restriction condition". Moreover, since implication of $\mathcal{GALT}(\mathsf{a})$ can be on a "per interaction" basis, with different conditions being applied to different interactions, we have:

Definition 23 *A behavioral restriction condition $\mathcal{BC}$ is a predicate $\mathcal{BC} : (\mathsf{B}, Q_0, \mathsf{a}) \to \{\mathtt{tt}, \mathtt{ff}\}$.*

$\mathcal{BC}$ is a predicate on the effects of a particular interaction a within a given system (B, Q_0).

Definition 24 (Supercycle-freedom preserving) *A behavioral restriction condition $\mathcal{BC}$ is supercycle-freedom preserving iff, for every system (B, Q_0) and $\mathsf{a} \in \gamma$ such that $\mathcal{BC}(\mathsf{B}, Q_0, \mathsf{a}) = \mathtt{tt}$, the following holds:*

for every reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0)
if s is supercycle-free, then t is supercycle-free.

Theorem 17 (Deadlock-freedom via supercycle-freedom preserving restriction) *Assume that*

1. *for all $s_0 \in Q_0$, $W_{\mathsf{B}}(s_0)$ is supercycle-free, and*
2. *there exists a supercycle-freedom preserving restriction $\mathcal{BC}$ such that, for all $\mathsf{a} \in \gamma$: $\mathcal{BC}(\mathsf{B}, Q_0, \mathsf{a}) = \mathtt{tt}$*

Then for every reachable state u of (B, Q_0): $W_{\mathsf{B}}(u)$ is supercycle-free.

Proof. Let u be an arbitrary reachable state. The proof is by induction on the length of the finite execution α that ends in u. Assumption 1 provides the base case, for α having length 0, and so $u \in Q_0$. For the induction step, we establish: for every reachable transition $s \xrightarrow{\mathsf{a}} t$, $W_{\mathsf{B}}(s)$

is supercycle-free implies that $W_{\mathsf{B}}(t)$ is supercycle-free. This is immediate from Assumption 2, and Definition 24. □

We notice that the above proof does not make any use of the requirement that there is a single restriction $\mathcal{BC}$ for all interactions. Hence we can (superficially) strengthen the result by allowing different restriction predicates for different interactions: This is convenient for later application.

Corollary 18 (Deadlock-freedom via several supercycle-freedom preserving restrictions) *Assume that*

1. *for all* $s_0 \in Q_0$, $W_{\mathsf{B}}(s_0)$ *is supercycle-free, and*
2. *for all* $\mathsf{a} \in \gamma$, *there exists a supercycle-freedom preserving restriction* $\mathcal{BC}$: $\mathcal{BC}(\mathsf{B}, Q_0, \mathsf{a}) = \mathtt{tt}$

Then for every reachable state u *of* (B, Q_0): $W_{\mathsf{B}}(u)$ *is supercycle-free.*

Proof. As for Theorem 17. □

5.1 A Global AND-OR Condition for Deadlock Freedom

Our first global condition is the most general possible: simply assert that, after execution of interaction a, some $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$ exhibits a supercycle-violation, as given by $\mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d, t)$ (Definition 20).

Definition 25 ($\mathcal{GALT}(\mathsf{B}, Q_0, \mathsf{a})$) *Let* $s \xrightarrow{\mathsf{a}} t$ *be a reachable transition of* (B, Q_0). *Then, in* t, *the following holds. For every component* $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$, *the formation violation condition holds. Formally,*

$$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}), \mathsf{formViolate}_{\mathsf{B}}(\mathsf{B}_i, t).$$

We now show that $\mathcal{GALT}$ is supercycle-freedom preserving.

Theorem 19 $\mathcal{GALT}$ *is supercycle-freedom preserving.*

Proof. We must establish: for every reachable transition $s \xrightarrow{\mathsf{a}} t$, $W_{\mathsf{B}}(s)$ is supercycle-free implies that $W_{\mathsf{B}}(t)$ is supercycle-free. Our proof is by contradiction, so we assume the existence of a reachable transition $s \xrightarrow{\mathsf{a}} t$ such that $W_{\mathsf{B}}(s)$ is supercycle-free and $W_{\mathsf{B}}(t)$ contains a supercycle.

By Proposition 13 there exists a component $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$ such that B_i is in CC, where CC is a strongly connected supercycle that is a subgraph of $W_{\mathsf{B}}(t)$.

Since CC is a strongly connected supercycle, we have, by Definition 21, that $\neg\mathsf{sConnViolate}_{\mathsf{B}}(\mathsf{B}_i, t)$ holds.

Since CC is a supercycle, we have, by Proposition 16, that $\neg(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d, t))$ holds.

Hence, by Definition 22, $\neg\mathsf{formViolate}_{\mathsf{B}}(\mathsf{B}_i, t)$ But, by Definition 25, we have $\mathsf{formViolate}_{\mathsf{B}}(\mathsf{B}_i, t)$. Hence, we have the desired contradiction, and so the theorem holds. □

5.2 A Global Linear Condition for Deadlock Freedom

In some cases, a simpler condition suffices to guarantee deadlock-freedom. This simpler condition is "linear", i.e., it lacks the AND-OR alternation aspect of $\mathcal{GALT}$. After execution of a reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0), we consider the in-depth and out-depth of the components $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$. There are three cases:

Case 1 B_i has finite in-depth in $W_{\mathsf{B}}(t)$: then, if $\mathsf{B}_i \in SC$, it can be removed and still leave a supercycle SC', by Proposition 9. Hence SC' exists in $W_{\mathsf{B}}(s)$, and so B_i is not essential to the creation of a supercycle.

Case 2 B_i has finite out-depth in $W_{\mathsf{B}}(t)$: by Proposition 6, B_i cannot be part of a supercycle, and so $SC \subseteq W_{\mathsf{B}}(s)$.

Case 3 B_i has infinite in-depth and infinite out-depth in $W_{\mathsf{B}}(t)$: in this case, B_i is possibly an essential part of SC, i.e., SC was created in going from s to t.

We thus impose a condition which guarantees that only Case 2 or Case 3 occur.

Definition 26 ($\mathcal{GLIN}(\mathsf{a})$) *Let $s \xrightarrow{\mathsf{a}} t$ be a reachable transition of BIP-system (B, Q_0). Then, in t, the following holds. For every component B_i of $\mathit{components}(\mathsf{a})$: either B_i has finite in-depth, or finite out-depth, in $W_{\mathsf{B}}(t)$. Formally,*

$$\forall\, \mathsf{B}_i \in \mathit{components}(a) : \mathit{in\_depth}_{\mathsf{B}}(\mathsf{B}_i, t) < \omega \vee \mathit{out\_depth}_{\mathsf{B}}(\mathsf{B}_i, t) < \omega.$$

Proposition 20 *Assume that node v of $W_{\mathsf{B}}(t)$ has a finite in-depth of d in $W_{\mathsf{B}}(t)$, i.e., $\mathit{in\_depth}_{\mathsf{B}}(v, t) = d$. Then $\mathsf{sConnViolate}_{\mathsf{B}}(v, t)$.*

Proof. A node with finite in-depth cannot be in a wait-for-cycle, and therefore cannot be in a strongly connected supercycle. □

Proposition 21 *Assume that node v of $W_{\mathsf{B}}(t)$ has a finite out-depth of d in $W_{\mathsf{B}}(t)$, i.e., $\mathit{out\_depth}_{\mathsf{B}}(v, t) = d$. Then $\mathsf{scViolate}_{\mathsf{B}}(v, d+1, t)$.*

Proof. Proof is by induction on d.

Base case, $d = 0$. Hence by $\mathit{out\_depth}_{\mathsf{B}}(v, t) = 0$ and Definitions 18 and 19, v has no outgoing wait-for-edges in $W_{\mathsf{B}}(t)$. Hence by Definition 20, $\mathsf{scViolate}_{\mathsf{B}}(v, 1, t)$.

Inductive step, $d > 0$. Let u be an arbitrary successor of v, i.e., a node u such that $v \rightarrow u \in W_{\mathsf{B}}(t)$. By Definitions 18 and 19, u has an out-depth d' that is less than d. That is, $\mathit{out\_depth}_{\mathsf{B}}(u, t) = d' < d$. By the induction hypothesis applied to d', we obtain $\mathsf{scViolate}_{\mathsf{B}}(u, d'+1, t)$. Hence by Definition 20, Clauses 1 and 2, $\mathsf{scViolate}_{\mathsf{B}}(v, d+1, t)$. □

Lemma 22 $\forall\, \mathsf{a} \in \gamma : \mathcal{GLIN}(\mathsf{B}, Q_0, \mathsf{a}) \Rightarrow \mathcal{GALT}(\mathsf{B}, Q_0, \mathsf{a})$.

Proof. Assume, for arbitrary $\mathsf{a} \in \gamma$, that $\mathcal{GLIN}(\mathsf{a})$ holds. That is,

For every reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0),
$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathit{in\_depth}_{\mathsf{B}}(\mathsf{B}_i, t) < \omega \vee \mathit{out\_depth}_{\mathsf{B}}(\mathsf{B}_i, t) < \omega.$

By Propositions 20 and 21,

For every reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0),
$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathsf{sConnViolate}_{\mathsf{B}}(\mathsf{B}_i, t) \vee (\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d, t))$.

Hence by Definition 22,

For every reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0),
$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathsf{formViolate}_{\mathsf{B}}(\mathsf{B}_i, t)$

Hence $\mathcal{GALT}(\mathsf{a})$ holds. □

Theorem 23 *$\mathcal{GLIN}$ is supercycle-freedom preserving*

Proof. Folows immediately from Lemma 22 and Theorem 19. □

5.3 Deadlock freedom using global restrictions

Corollary 24 (Deadlock-freedom via $\mathcal{GALT}$, $\mathcal{GLIN}$) *Assume that*

1. *for all $s_0 \in Q_0$, $W_{\mathsf{B}}(s_0)$ is supercycle-free, and*
2. *for all interactions a of B (i.e., $\mathsf{a} \in \gamma$), $\mathcal{GALT}(\mathsf{a}) \vee \mathcal{GLIN}(\mathsf{a})$ holds.*

Then for every reachable state u of (B, Q_0): $W_{\mathsf{B}}(u)$ is supercycle-free, and so (B, Q_0) is free of local deadlock.

Proof. Immediate from Theorems 19, 23 and Corollary 18. □

6 Local Conditions for Deadlock Freedom

Evaluating the global restrictions $\mathcal{GALT}(B, Q_0, \mathsf{a})$, $\mathcal{GLIN}(B, Q_0, \mathsf{a})$ requires checking all reachable transitions of (B, Q_0), which is, in general, subject to state-explosion. We need restrictions which imply a global restriction, and which can be checked efficiently. To this end, we first develop some terminology, and a projection result, for relating the waiting-behavior in a subsystem of (B, Q_0) to that in (B, Q_0) overall.

6.1 Projection onto Subsystems

Definition 27 (Structure Graph G_{B}, G^{ℓ}_{a}) *The structure graph G_{B} of composite component $B = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$ is a bipartite graph whose nodes are the $\mathsf{B}_1, \ldots, \mathsf{B}_n$ and all the $\mathsf{a} \in \gamma$. There is an edge between B_i and interaction a iff B_i participates in a, i.e., $\mathsf{B}_i \in \mathit{components}(\mathsf{a})$. Define the* distance *between two nodes to be the number of edges in a shortest path between them. Let G^{ℓ}_{a} be the subgraph of G_{B} that contains a and all nodes of G_{B} that have a distance to a less than or equal to ℓ.*

Definition 28 (Deadlock-checking subsystem, D^{ℓ}_{a}) *Define D^{ℓ}_{a}, the* deadlock-checking subsystem for interaction a and depth ℓ, *to be the subsystem of (B, Q_0) based on the set of components in $G^{2\ell}_{\mathsf{a}}$.*

Definition 29 (Border node, interior node of D^ℓ_{a}) *A node v of D^ℓ_{a} is a* border-node *iff it has an edge in G_{B} to a node outside of D^ℓ_{a}. If node v of D^ℓ_{a} is not a border node, then it is an* internal node.

Note that all border nodes of D^ℓ_{a} are interactions, since 2ℓ is even. Hence all component nodes of D^ℓ_{a} are interior nodes.

Proposition 25 (Wait-for-edge projection) *Let (B', Q'_0) be a subsystem of (B, Q_0). Let s be a state of (B, Q_0), and $s' = s\restriction\mathsf{B}'$. Let a be an interaction of (B', Q'_0), and $\mathsf{B}_i \in components(\mathsf{a})$ an atomic component of B'. Then (1) $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(s)$ iff $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}'}(s')$, and (2) $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(s)$ iff $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}'}(s')$.*

Proof. By Definition 15, $\mathsf{a} \to \mathsf{B}_i \in W_{\mathsf{B}}(s)$ iff $s\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = \mathit{false}$. Since $s' = s\restriction\mathsf{B}'$, we have $s'\restriction i = s\restriction i$. Hence $s\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = s'\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}})$. By Definition 15, $a \to \mathsf{B}_i \in W_{\mathsf{B}'}(s')$ iff $s'\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = \mathit{false}$. Putting together these three equalities gives us clause (1).

By Definition 15, $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}}(s)$ iff $s\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = \mathit{true}$. Since $s' = s\restriction\mathsf{B}'$, we have $s'\restriction i = s\restriction i$. Hence $s\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = s'\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}})$. By Definition 15, $\mathsf{B}_i \to \mathsf{a} \in W_{\mathsf{B}'}(s')$ iff $s'\restriction i(enb^{\mathsf{B}_i}_{\mathsf{a}}) = \mathit{true}$. Putting the above three equalities together gives us clause (2). □

6.2 A Local AND-OR Condition for Deadlock Freedom

We now seek a local condition, which we evaluate in D^ℓ_{a}, and which implies $\mathcal{GALT}$. We define local versions of both $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$ and $\mathsf{sConnViolate}_{\mathsf{B}}(v, t)$.

To achieve a local and conservative approximation of $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$, we make the "pessimistic" assumption that the violation status of border nodes of D^ℓ_{a} cannot be known, since it depends on nodes outside of D^ℓ_{a}. Now, if an internal node v of D^ℓ_{a} can be marked with a level d sc-violation, by applying Definition 20 only within D^ℓ_{a}, and with the border nodes marked as non-violating, then it is also the case, as we show below, that v has a level d sc-violation overall.

To achieve a local and conservative approximation of $\mathsf{sConnViolate}_{\mathsf{B}}(v, t)$, we project onto a subsystem.

6.2.1 Local supercycle violation condition

We define the predicate $\mathsf{scViolateLoc}(v, d, t, D^\ell_{\mathsf{a}})$ to hold iff node v in $W_B(t)$ has a level-d supercycle-violation *that can be confirmed within D^ℓ_{a}*.

Definition 30 (Local supercycle violation, $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$) *Let t_{a} be a state of D^ℓ_{a} and v be a node of D^ℓ_{a}. We define $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$ by induction on d, as follows.*

Base case, $d = 1$. $\mathsf{scViolateLoc}(v, 1, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$ *iff v is an interaction* aa *and* aa *is an interior node of D^ℓ_{a} that has no outgoing wait-for edges in $W_{D^\ell_{\mathsf{a}}}(t_{\mathsf{a}})$. Otherwise $\neg\mathsf{scViolateLoc}(v, 1, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$.*

Inductive step, $d > 1$. $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$ *iff either of the following two cases hold. Otherwise $\neg\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$.*

1. *v is a component B_i and there exists an interaction aa such that $B_i \to \mathsf{aa} \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a})$ and $(\exists\, d' : 1 \le d' < d : \mathsf{scViolateLoc}(\mathsf{aa}, d', t_\mathsf{a}, D_\mathsf{a}^\ell))$. That is, B_i enables an interaction aa which has a level-d' supercycle-violation in D_a^ℓ, for some $d' < d$.*

2. *v is an interaction aa and an internal node of D_a^ℓ and for all components B_i such that $\mathsf{aa} \to \mathsf{B}_i \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a})$, we have $(\exists\, d' : 1 \le d' < d : \mathsf{scViolateLoc}(\mathsf{B}_i, d', t_\mathsf{a}, D_\mathsf{a}^\ell))$. That is, each component B_i that aa waits for has a level-d' supercycle-violation in D_a^ℓ, for some $d' < d$*

Note that if v is an interaction aa and a border node, then $\mathsf{scViolateLoc}(\mathsf{aa}, d, t_\mathsf{a}, D_\mathsf{a}^\ell)$ is false, for all d. This is because aa has some component that is outside D_a^ℓ, and so this component cannot be checked. A component cannot have a level-1 supercycle-violation since it must have at least one outgoing wait-for edge at all times. Figure 6 gives a formal, recursive definition of $\mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)$. The notation $v = \mathsf{B}_i$ means that v is some component B_i. Likewise, $v = \mathsf{aa}$ means that v is some interaction a, and "$v = \mathsf{aa}$ is interior" means that v is an interaction a and also an internal node. Line 0 corresponds to the base case, line 1 corresponds to item 1 of the inductive case, and line 2 corresponds to item 2 of the inductive case. Line 3 handles all cases that do not return true.

$\mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)$
$\triangleright$ Precondition: v is a node of D_a^ℓ and $d \ge 1$
0. **if** $(d = 1 \wedge v = \mathsf{aa}$ is interior $\wedge\, \neg(\exists\, \mathsf{B}_i : \mathsf{aa} \to \mathsf{B}_i \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a})))$ **return**(`tt`);
1. **if** $(v = \mathsf{aa}$ is interior $\wedge\, (\forall\, \mathsf{B}_i : \mathsf{aa} \to \mathsf{B}_i \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a}) : (\exists\, d' : 1 \le d' < d : \mathsf{scViolateLoc}(\mathsf{B}_i, d', t_\mathsf{a}, D_\mathsf{a}^\ell))))$
return(`tt`);
2. **if** $(v = \mathsf{B}_i \wedge (\exists\, \mathsf{aa} : \mathsf{B}_i \to \mathsf{aa} \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a}) : (\exists\, d' : 1 \le d' < d : \mathsf{scViolateLoc}(\mathsf{aa}, d', t_\mathsf{a}, D_\mathsf{a}^\ell))))$ **return**(`tt`);
3. **return**(`ff`)

Figure 6: Formal definition of $\mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)$.

We now show that a local supercycle-violation implies (global) supercycle-violation.

Proposition 26 *Let t be an arbitrary reachable state of BIP-system (B, Q_0). For all interactions $\mathsf{a} \in \gamma$, and $\ell \ge 1$, let $t_\mathsf{a} = t{\restriction}D_\mathsf{a}^\ell$. Then*

$$\forall\, d \ge 1 : \mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell) \Rightarrow \mathsf{scViolate}_\mathsf{B}(v, d, t).$$

Proof. Proof is by induction on d.

Base case, $d = 1$. Assume $\mathsf{scViolateLoc}(v, 1, t_\mathsf{a}, D_\mathsf{a}^\ell)$ for some node v. Then, by Figure 6, v is an interior node and an interaction aa of D_a^ℓ, and has no outgoing wait-for edges. Therefore, in $W_\mathsf{B}(t)$, it is still the case that v has no outgoing wait-for edges. Hence $\mathsf{scViolate}_\mathsf{B}(v, 1, t)$ holds.

Inductive step, $d > 1$. Assume $\mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)$ for some node v and some $d > 1$. We proceed by cases on Figure 6.

1. v is an interior interaction aa and
$(\forall\, \mathsf{B}_i : \mathsf{aa} \to \mathsf{B}_i \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a}) : (\exists\, d' : 1 \le d' < d : \mathsf{scViolateLoc}(\mathsf{B}_i, d', t_\mathsf{a}, D_\mathsf{a}^\ell)))$.

   Choose an arbitrary B_i such that $\mathsf{aa} \to \mathsf{B}_i \in W_{D_\mathsf{a}^\ell}(t_\mathsf{a})$. By the induction hypothesis applied to $\mathsf{scViolateLoc}(\mathsf{B}_i, d', t_\mathsf{a}, D_\mathsf{a}^\ell)$, we have $\mathsf{scViolate}_\mathsf{B}(\mathsf{B}_i, d', t)$ for some $d' < d$. Since

$W_{D^\ell_{\mathsf{a}}}(t_{\mathsf{a}}) \subseteq W_{\mathsf{B}}(t)$ by construction, we have $\mathsf{aa} \to B_i \in W_{\mathsf{B}}(t)$ and $\mathsf{scViolate}_{\mathsf{B}}(\mathsf{B}_i, d', t)$. Hence by Definition 20, Clause 1, we have $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$.

2. v is a component B_i and
$(\exists\, \mathsf{aa} : \mathsf{B}_i \to \mathsf{aa} \in W_{D^\ell_{\mathsf{a}}}(t_{\mathsf{a}}) : (\exists\, d' : 1 \leq d' < d : \mathsf{scViolateLoc}(\mathsf{aa}, d', t_{\mathsf{a}}, D^\ell_{\mathsf{a}})))$.

   By the induction hypothesis applied to $\mathsf{scViolateLoc}(\mathsf{aa}, d', t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$, we have $\mathsf{scViolate}_{\mathsf{B}}(\mathsf{aa}, d', t)$ for some $d' < d$. Since $W_{D^\ell_{\mathsf{a}}}(t_{\mathsf{a}}) \subseteq W_{\mathsf{B}}(t)$ by construction, we have $\mathsf{B}_i \to \mathsf{aa} \in W_{\mathsf{B}}(t)$ and $\mathsf{scViolate}_{\mathsf{B}}(\mathsf{aa}, d', t)$. Hence by Definition 20, Clause 1, we have $\mathsf{scViolate}_{\mathsf{B}}(v, d, t)$.

□

6.2.2 Local strong connectedness condition

We now present the local version of the strong connectedness violation condition, given above in Definition 21.

Definition 31 (Local strong connectedness violation, $\mathsf{sConnViolateLoc}(v, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$) *Let L be the nodes of $W_{D^\ell_a}(t_{\mathsf{a}})$ that have no local supercycle violation, i.e., $L = \{v \mid v \in D^\ell_a \wedge \neg(\exists\, d \geq 1 : \mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^\ell_{\mathsf{a}}))\}$. Let v be an arbitrary node in L. Let $WL = W_{D^\ell_a}(t_{\mathsf{a}})\restriction L$, i.e., WL is the subgraph of $W_{D^\ell_a}(t_{\mathsf{a}})$ consisting of the nodes in L, and the edges between those nodes that are also edges in $W_{D^\ell_a}(t_{\mathsf{a}})$.*

Then, $\mathsf{sConnViolateLoc}(v, t_{\mathsf{a}}, D^\ell_{\mathsf{a}})$ holds iff:

1. *there does not exist a nontrivial strongly connected supercycle SSC such that $v \in SSC$ and $SSC \subseteq WL$, and*
2. *either*
   (a) *every wait-for path π from v to a border node of D^ℓ_a contains at least one node with a local supercycle violation*
   or
   (b) *every wait-for path π' from a border node of D^ℓ_a to v contains at least one node with a local supercycle violation*

We show that the local strong connectedness condition implies the global strong connectedness condition.

Proposition 27 *Let t be an arbitrary reachable state of BIP-system (B, Q_0). For all interactions $\mathsf{a} \in \gamma$, and $\ell > 0$, let $t_{\mathsf{a}} = t\restriction D^\ell_{\mathsf{a}}$. Then*
$\mathsf{sConnViolateLoc}(v, t_{\mathsf{a}}, D^\ell_{\mathsf{a}}) \Rightarrow \mathsf{sConnViolate}_{\mathsf{B}}(v, t)$.

Proof. By contradiction. Assume there exists a node v in D^ℓ_a such that $\mathsf{sConnViolateLoc}(v, t_{\mathsf{a}}, D^\ell_{\mathsf{a}}) \wedge \neg\mathsf{sConnViolate}_{\mathsf{B}}(v, t)$. By $\neg\mathsf{sConnViolate}_{\mathsf{B}}(v, t)$ and Definition 21, there exists a strongly connected supercycle SSC such that $v \in SSC$ and $SSC \subseteq W_B(t)$. Then, there are two cases:

1. $SSC \subseteq W_{D_a^\ell}(t_\mathsf{a})$: let x be any node in SSC. Since x is a node in a supercycle, we have by Proposition 14, that $\neg(\exists\, d \geq 1 : \mathsf{scViolate}_\mathsf{B}(x, d, t))$. Hence $(\forall\, d \geq 1 : \neg\mathsf{scViolate}_\mathsf{B}(x, d, t))$. Hence by Proposition 26, we have $(\forall\, d \geq 1 : \neg\mathsf{scViolateLoc}(x, d, t_\mathsf{a}, D_\mathsf{a}^\ell))$. Let L, WL be as given in Definition 31. Then $x \in L$, and since x is an arbitrary node of SSC, we have $SSC \subseteq WL$. Thus Clause 1 of Definition 31 is violated.

2. $SSC \not\subseteq W_{D_a^\ell}(t_\mathsf{a})$: then there exists a node $x \in SSC - D_a^\ell$. Since $v \in SSC$, there must exist a wait-for path π from v to x and a wait-for path π' from x to v. Since $v \in D_a^\ell$ and $x \notin D_a^\ell$, it follows that both π, π' cross a border node of D_a^ℓ. Furthermore, since π, π' are part of SSC, every node along π, π' is in a supercycle, and so cannot have a supercycle violation. By Proposition 26, the nodes on π, π' cannot have a local supercycle violation. Hence Clauses 2a and 2b of Definition 31 are violated, since they require that at least one node along π, π' respectively, have a local supercycle violation.

In both cases, Definition 31 is violated. But Definition 31 must hold, since we have $\mathsf{sConnViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$. Hence the desired contradiction. □

6.2.3 Local formation violation condition

We showed above that local supercycle violation implies global supercycle violation, and local strong connecteness violation implies global string conectedness violation. The global supercycle formation condition is the disjunction of global supercycle violation and global strong connecteness violation. Hence we formulate the local supercycle formation condition as the disjunction of local supercycle violation and local strong connecteness violation. It follows that the local supercycle formation condition implies the global supercycle formation condition.

Definition 32 (Local Formation violation, $\mathsf{formViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$) *Let v be a node of D_a^ℓ. Then* $\mathsf{formViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell) \triangleq (\exists\, d \geq 1 : \mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)) \vee \mathsf{sConnViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$.

Proposition 28 *Let t be an arbitrary reachable state of BIP-system (B, Q_0). For all interactions $\mathsf{a} \in \gamma$, and $\ell > 0$, let $t_\mathsf{a} = t{\restriction}D_\mathsf{a}^\ell$. Then*

$$\mathsf{formViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell) \Rightarrow \mathsf{formViolate}_\mathsf{B}(v, t).$$

Proof. Assume that $\mathsf{formViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$ holds. Then, by Definition 22, $(\exists\, d \geq 1 : \mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell)) \vee \mathsf{sConnViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$. We proceed by cases:

1. $(\exists\, d \geq 1 : \mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D_\mathsf{a}^\ell))$: hence $(\exists\, d \geq 1 : \mathsf{scViolate}_\mathsf{B}(v, d, t))$ by Proposition 26.

2. $\mathsf{sConnViolateLoc}(v, t_\mathsf{a}, D_\mathsf{a}^\ell)$: hence $\mathsf{sConnViolate}_\mathsf{B}(v, t)$ by Proposition 27.

By Definition 22, $\mathsf{formViolate}_\mathsf{B}(v, t) \triangleq (\exists\, d \geq 1 : \mathsf{scViolate}_\mathsf{B}(u, d, t)) \vee \mathsf{sConnViolate}_\mathsf{B}(v, t)$. Hence we conclude that $\mathsf{formViolate}_\mathsf{B}(v, t)$ holds. □

6.2.4 Local AND-OR Condition

The actual local condition, $\mathcal{LALT}$, is given by applying the local supercycle formation condition to every reachable transition of the subsystem D_a^ℓ being considered, and to every component $B_i \in \mathit{components}(\mathsf{a})$.

Definition 33 ($\mathcal{LACLT}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$) *Let $\ell > 0$, and let $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ be an arbitrary reachable transition of D^ℓ_a. Then, in t_a, the following holds. For every component B_i of components(a): B_i has a supercycle formation violation that can be confirmed within D^ℓ_a. Formally,*

$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathsf{formViolateLoc}(\mathsf{B}_i, t_\mathsf{a}, D^\ell_\mathsf{a})$.

We showed previously that $\mathcal{GACLT}$ implies deadlock-freedom, and so it remains to establish that $\mathcal{LACLT}$ implies $\mathcal{GACLT}$.

Lemma 29 *Let $\mathsf{a} \in \gamma$ be an interaction of BIP-system (B, Q_0). Then*

$(\exists\, \ell > 0 : \mathcal{LACLT}(\mathsf{B}, Q_0, \mathsf{a}, \ell))$ *implies* $\mathcal{GACLT}(\mathsf{B}, Q_0, \mathsf{a})$

Proof. Assume $\mathcal{LACLT}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ for some $\ell > 0$. Let $s \xrightarrow{\mathsf{a}} t$ be an arbitrary reachable transition of BIP-system (B, Q_0), and let $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ be the projection of $s \xrightarrow{\mathsf{a}} t$ onto D^ℓ_a. By Corollary 2, $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ is a reachable transition of D^ℓ_a.

By Definition 33, we have for some $\ell > 0$:

for every reachable transition $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ of D^ℓ_a:

$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathsf{formViolateLoc}(\mathsf{B}_i, t_\mathsf{a}, D^\ell_\mathsf{a})$.

From this and Proposition 28,

for every reachable transition $s \xrightarrow{\mathsf{a}} t$ of (B, Q_0):

$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathsf{formViolate}_\mathsf{B}(B_i, t)$

Hence, by Definition 25, $\mathcal{GACLT}(\mathsf{B}, Q_0, \mathsf{a})$ holds. □

Theorem 30 *$\mathcal{LACLT}$ is supercycle-freedom preserving*

Proof. Follows immediately from Lemma 29 and Theorem 19. □

$\mathsf{scViolate}_\mathsf{B}(v, d, t)$	v confirmed at depth d to not be in supercycle
$\mathsf{scViolateLoc}(v, d, t_\mathsf{a}, D^\ell_\mathsf{a})$	v locally determined to not be in a supercycle
$\mathsf{sConnViolate}_\mathsf{B}(v, t)$	v not in a strongly connected supercycle
$\mathsf{sConnViolateLoc}(v, t_\mathsf{a}, D^\ell_\mathsf{a})$	v locally determined to not be in a strongly connected supercycle
$\mathsf{formViolate}_\mathsf{B}(v, t)$	v does not contribute to a supercycle
$\mathsf{formViolateLoc}(v, t_\mathsf{a}, D^\ell_\mathsf{a})$	v locally determined to not contribute to a supercycle

Figure 7: Summary of predicates

6.3 A Local Linear Condition for Deadlock Freedom

We now formulate a local version of $\mathcal{GLIN}$. Observe that if $\mathit{in\_depth}_\mathsf{B}(\mathsf{B}_i, t) < \omega \vee \mathit{out\_depth}_\mathsf{B}(\mathsf{B}_i, t) < \omega$, then there is some finite ℓ such that $\mathit{in\_depth}_\mathsf{B}(\mathsf{B}_i, t) = \ell \vee \mathit{out\_depth}_\mathsf{B}(\mathsf{B}_i, t) = \ell$.

Definition 34 ($\mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$) *Let $\ell > 0$ and $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ be an arbitrary reachable transition of D^ℓ_a. Then, in t_a, the following holds. For every component B_i of components(a): either B_i has in-depth less than $2\ell - 1$, or out-depth less than $2\ell - 1$, in $W_{D^\ell_\mathsf{a}}(t_\mathsf{a})$. Formally,*

$\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathit{in\_depth}_{D^\ell_\mathsf{a}}(\mathsf{B}_i, t_\mathsf{a}) < 2\ell - 1 \vee \mathit{out\_depth}_{D^\ell_\mathsf{a}}(\mathsf{B}_i, t_\mathsf{a}) < 2\ell - 1$.

To infer deadlock-freedom in (B, Q_0) by checking $\mathcal{LLIN}(\mathsf{B}, Q_0, a, \ell)$, we show that wait-for behavior in B "projects down" to any subcomponent B', and that wait-for behavior in B' "projects up" to B.

Since wait-for-edges project up and down, it follows that wait-for-paths project up and down, provided that the subsystem contains the entire wait-for-path.

Proposition 31 (In-projection, Out-projection) *Let $\ell > 0$, let B_i be an atomic component of B, and let (B', Q_0') be a subsystem of (B, Q_0) which is based on a superset of $G_a^{2\ell}$. Let s be a state of (B, Q_0), and $s' = s{\restriction}B'$. Then (1) $in\_depth_{\mathsf{B}}(\mathsf{B}_i, s) < 2\ell-1$ iff $in\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') < 2\ell-1$, and (2) $out\_depth_{\mathsf{B}}(\mathsf{B}_i, s) < 2\ell - 1$ iff $out\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') < 2\ell - 1$.*

Proof. We establish clause (1). The proof of clause (2) is analogous, except we replace paths ending in B_i by paths starting from B_i. The proof of clause (1) is by double implication.

$in\_depth_{\mathsf{B}}(\mathsf{B}_i, s) < 2\ell - 1$ implies $in\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') < 2\ell - 1$: Let π be an arbitrary wait-for-path in $W_{\mathsf{B}'}(s')$ that ends in B_i. Since (B', Q_0') is a subsystem of (B, Q_0), by Definition 15 and $s' = s{\restriction}B'$, $W_{\mathsf{B}'}(s')$ is a subgraph of $W_{\mathsf{B}}(s)$. Hence π is a wait-for-path in $W_{\mathsf{B}}(s)$. By $in\_depth_{\mathsf{B}}(\mathsf{B}_i, s) < 2\ell - 1$, we have $|\pi| < 2\ell - 1$. Hence $in\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') < 2\ell - 1$ since π was arbitrarily chosen.

$in\_depth_{\mathsf{B}}(\mathsf{B}_i, s) < 2\ell - 1$ follows from $in\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') < 2\ell - 1$: Let π be an arbitrary wait-for-path in $W_{\mathsf{B}}(s)$ that ends in B_i. Suppose that $|\pi| \geq 2\ell - 1$. Hence π has a suffix ρ of length $2\ell - 1$. Since (B', Q_0') is a subsystem of (B, Q_0), by Definition 15 and $s' = s{\restriction}\mathsf{B}'$, $W_{\mathsf{B}'}(s')$ is a subgraph of $W_{\mathsf{B}}(s)$. Since (B', Q_0') is based on a superset of $G_a^{2\ell}$, and since the distance from B_i to the border of G_a^{ℓ} is $2\ell - 1$, we conclude that ρ is a wait-for-path that is contained in $W_{\mathsf{B}'}(s')$. Hence $in\_depth_{\mathsf{B}}(\mathsf{B}_i, s) \geq 2\ell - 1$ implies $in\_depth_{\mathsf{B}'}(\mathsf{B}_i, s') \geq 2\ell - 1$. The contrapositive is our desired result. □

We now show that $\mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ implies $\mathcal{GLIN}(\mathsf{B}, Q_0, \mathsf{a})$, which in turn implies deadlock-freedom.

Lemma 32 *Let a be an interaction of B, i.e., $\mathsf{a} \in \gamma$. If $\mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ holds for some finite $\ell > 0$, then $\mathcal{GLIN}(\mathsf{B}, Q_0, \mathsf{a})$ holds.*

Proof. Let $s \xrightarrow{\mathsf{a}} t$ be a reachable transition of (B, Q_0) and let $\mathsf{B}_i \in components(\mathsf{a})$, $s_{\mathsf{a}} = s{\restriction}D_{\mathsf{a}}^{\ell}$, $t_{\mathsf{a}} = t{\restriction}D_{\mathsf{a}}^{\ell}$. Then $s_{\mathsf{a}} \xrightarrow{\mathsf{a}} t_{\mathsf{a}}$ is a reachable transition of D_{a}^{ℓ} by Corollary 2. By $\mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$, $in\_depth_{D_{\mathsf{a}}^{\ell}}(\mathsf{B}_i, t_{\mathsf{a}}) < 2\ell - 1 \vee out\_depth_{D_{\mathsf{a}}^{\ell}}(\mathsf{B}_i, t_{\mathsf{a}}) < 2\ell - 1$. Hence by Proposition 31, $in\_depth_{\mathsf{B}}(\mathsf{B}_i, t) < 2\ell - 1 \vee out\_depth_{\mathsf{B}}(\mathsf{B}_i, t) < 2\ell - 1$. So $in\_depth_{\mathsf{B}}(\mathsf{B}_i, t) < \omega \vee out\_depth_{\mathsf{B}}(\mathsf{B}_i, t) < \omega$. Hence $\mathcal{GLIN}(\mathsf{B}, Q_0, \mathsf{a})$. □

Theorem 33 *$\mathcal{LLIN}$ is supercycle-freedom preserving*

Proof. Follows immediately from Lemma 32 and Theorem 23. □

6.4 Deadlock freedom using local and global restrictions

Theorem 34 (Deadlock-freedom via $\mathcal{LALT}$, $\mathcal{LLIN}$) *Assume that*

1. *for all* $s_0 \in Q_0$, $W_{\mathsf{B}}(s_0)$ *is supercycle-free, and*

2. *for all interactions* a *of* B *(i.e.,* $\mathsf{a} \in \gamma$*), one of the following holds:*

   (a) $\mathcal{GALT}(\mathsf{B}, Q_0, \mathsf{a})$
   (b) $\mathcal{GLIN}(\mathsf{B}, Q_0, \mathsf{a})$
   (c) $\exists\, \ell > 0 : \mathcal{LALT}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$
   (d) $\exists\, \ell > 0 : \mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$

Then for every reachable state u *of* (B, Q_0)*:* $W_{\mathsf{B}}(u)$ *is supercycle-free, and so* (B, Q_0) *is free of local deadlock.*

Proof. Immediate from Theorems 19, 23, 30, 33 and Corollary 18. □

7 Implementation and Experiments

7.1 Checking that initial states are supercycle-free

Our deadlock-freedom theorem require that all initial states be sueprcycle-free. We assume that the number of initial states is small, so that we can check each explicitly.

checkInitSupercycleFree(Q_0)
▷ returns true iff all initial states are supercycle-free
1. **forall** $s_0 \in Q_0$
2. compute $W_{\mathsf{B}}(s_0)$
3. let U be the result of removing from $W_{\mathsf{B}}(s_0)$ all nodes v such that $(\exists\, d \geq 1 : \mathsf{scViolate}_{\mathsf{B}}(v, d, t))$
4. **if** (U is nonempty) **then return**(`ff`) ▷ s_0 not supercycle-free, so return false
5. **else return**(`tt`)

Figure 8: Procedure to check that all initial states are supercycle-free

Proposition 35 checkInitSupercycleFree*(Q_0) returns true iff all initial states are supercycle-free.*

Proof. Consider the execution of checkInitSupercycleFree(Q_0) for an arbitrary $s_0 \in Q_0$.

Suppose that U is nonempty. By Proposition 15, U is a supercycle. Since $U \subseteq W_{\mathsf{B}}(s_0)$, we conclude that s_0 not supercycle-free, so false is the correct result in this case.

Now suppose that U is empty. Hence every node in $W_{\mathsf{B}}(s_0)$ has a supercycle violation, and so by Proposition 14, no node of $W_{\mathsf{B}}(s_0)$ can be in a strongly-connected supercycle. Hence $W_{\mathsf{B}}(s_0)$ does not contain a strongly-connected supercycle. So, by Proposition 10, $W_{\mathsf{B}}(s_0)$ does not contain a supercycle. □

7.2 Implementation and Experimentation for the AND-OR Condition

Our implementation evaluates $\mathcal{LALT}$. Figure 10 presents the pseudocode, and Figure 11 presents the pseudocode for computing supercycle violations based on D^{ℓ}_{a}.

LALT(B, Q_0) verifies $\mathcal{LALT}$ by iterating over all $\mathsf{a} \in \gamma$. LALTINT$(\mathsf{B}, Q_0, \mathsf{a})$ checks $(\exists\, \ell > 0 : \mathcal{LALT}(B, Q_0, \mathsf{a}, \ell))$, i.e., if $\mathcal{LALT}$ for a can be verified in some D^{ℓ}_{a}. We start with $\ell = 1$ since D^{1}_{a} is the smallest system, in which a supercycle-violation can be confirmed. LALTINTDIST$(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ checks $\mathcal{LALT}(B, Q_0, \mathsf{a}, \ell)$ for a particular ℓ.

For a given D^{ℓ}_{a} and state t_{a} of D^{ℓ}_{a}, procedure LOCSCVIOL$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}})$ computes $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$ for $d = 1, \ldots, dd$ where dd is the length of the longest simple path in the structure graph of D^{ℓ}_{a}. We use a "memoizing" strategy; we iterate over d, starting with $d = 1$ and incrementing. The iteration for d assumes that the iteration for $d-1$ has already been computed. The results of each iteration are stored in an array $V_{D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}}} : (\{B_1, \ldots, B_n\} \cup \gamma) \times \{1, \ldots, dd\} \to \{\mathtt{tt}, \mathtt{ff}\}$. LOCSCVIOLDIST$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}}, d)$ computes the supercycle violations for a given distance d, and LOCSCVIOLDISTNODE$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}}, d, v)$ determines the level-d supercycle-violation of node v, if any, i.e., it computes $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$.

Complexity. The running time of our implementation is ....TO BE DONE....

LALT(B, Q_0)	true iff $(\forall\, \mathsf{a} \in \gamma, \exists\, \ell > 0 : \mathcal{LALT}(B, Q_0, \mathsf{a}, \ell))$
LALTINT$(\mathsf{B}, Q_0, \mathsf{a})$	true iff $(\exists\, \ell > 0 : \mathcal{LALT}(B, Q_0, \mathsf{a}, \ell))$
LALTINTDIST$(\mathsf{B}, Q_0, \mathsf{a}, \ell)$	true iff $\mathcal{LALT}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$
LOCFORMVIOL$(B_i, D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}})$	true iff B_i has local sc-formation violation in state t_{a} of D^{ℓ}_{a}, i.e., $\mathsf{formViolateLoc}(B_i, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$ holds
LOCSCONNSCVIOL$(B_i, D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}})$	true iff B_i has local strong connectedness violation in t_{a}, i.e., $\mathsf{sConnViolateLoc}(B_i, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$ holds
LOCSCVIOL$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}})$	compute local supercycle violations in state t_{a} of D^{ℓ}_{a}, i.e., $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$ forall v, d
LOCSCVIOLDIST$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}}, d)$	compute level-d local supercycle violations in state t_{a} of D^{ℓ}_{a}, i.e., $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$ forall v
LOCSCVIOLDISTNODE$(D^{\ell}_{\mathsf{a}}, t_{\mathsf{a}}, d, v)$	compute level-d local supercycle violation of node v in state t_{a} of D^{ℓ}_{a}, i.e., $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D^{\ell}_{\mathsf{a}})$

Figure 9: Summary of procedures

7.2.1 Experiments

TO BE DONE:

1. Implement above algorithm
2. Select case studies. We need examples that have "branching waiting"behavior, i.e., a process waits for alternatives. For example, dining philosopher is NOT an example of this.

   One possilbe source is the paper "Evaluating Deadlock Detection Methods for Concurrent Software", IEEE Transactions on Software Engineering, Vol. 22, No. 3, March 1996

LALT(B, Q_0), where $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$
▷ returns tt iff $(\forall\, \mathsf{a} \in \gamma, \exists\, \ell > 0 : \mathcal{LALT}(\mathsf{a}, \ell))$
1. **forall** interactions $\mathsf{a} \in \gamma$
2. **if** (LALTINT($\mathsf{B}, Q_0, \mathsf{a}$) = ff) **return**(ff) **fi**
3. **endfor**;
4. **return**(tt) ▷ return tt if check succeeds for all $a \in \gamma$

LALTINT($\mathsf{B}, Q_0, \mathsf{a}$), where $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n), \mathsf{a} \in \gamma$
▷ returns tt iff $(\exists\, \ell > 0 : \mathcal{LALT}(B, Q_0, \mathsf{a}, \ell))$
1. $\ell \leftarrow 1$; ▷ start with $\ell = 1$
2. **while** (tt)
3. **if** (LALTINTDIST(a, ℓ) = tt) **return**(tt) **fi**; ▷ success, so return true
4. **if** ($D^\ell_\mathsf{a} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$) **return**(ff) **fi**; ▷ exhausted all subsystems, return false
5. $\ell \leftarrow \ell + 1$ ▷ increment ℓ until success or intractable or failure
6. **endwhile**

LALTINTDIST($\mathsf{B}, Q_0, \mathsf{a}, \ell$)
▷ returns tt iff $\mathcal{LALT}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$
1. **forall** reachable transitions $s_\mathsf{a} \xrightarrow{\mathsf{a}} t_\mathsf{a}$ of D^ℓ_a
2. **forall** $\mathsf{B}_i \in$ *components*(a)
3. **if** ¬LOCFORMVIOL($B_i, D^\ell_\mathsf{a}, t_\mathsf{a}$) **then return**(ff) **fi** ▷return ff if no violation for B_i
4. **endfor**
5. **endfor**;
6. **return**(tt) ▷return tt if all $\mathsf{B}_i \in$ *components*(a) violate local supercycle formation

LOCFORMVIOL($B_i, D^\ell_\mathsf{a}, t_\mathsf{a}$)
▷returns true iff formViolateLoc($B_i, t_\mathsf{a}, D^\ell_\mathsf{a}$) holds (Definition 32)
▷i.e., B_i has a local supercycle formation violation in state t_a of subsystem D^ℓ_a
1. **repeat** until one of the following returns true, or run out of resources
2. LOCSCVIOLDISTNODE($D^\ell_\mathsf{a}, t_\mathsf{a}, d, B_i$) for increasing d
3. LOCSCONNSCVIOL($B_i, D^\ell_\mathsf{a}, t_\mathsf{a}$)
4. **endrepeat**

LOCSCONNSCVIOL($B_i, D^\ell_\mathsf{a}, t_\mathsf{a}$)
▷returns true iff sConnViolateLoc($B_i, t_\mathsf{a}, D^\ell_\mathsf{a}$) holds (Definition 31)
▷i.e., B_i has a local strong connectedness supercycle formation violation in state t_a of subsystem D^ℓ_a
1. LOCSCVIOL($D^\ell_\mathsf{a}, t_\mathsf{a}$)
2. remove all nodes with local supercycle violation
3. compute maximal strongly connected components of remaining wait-for graph
4. **forall** maximal strongly connected components C
5. **if** C contains a strongly connected supercycle which contains B_i as a node, **then return**(ff) **fi**
{ Definition 31, Clause 1 holds here }
6. **forall** wait-for paths π from B_i to the border of D^ℓ_a
7. **if** some node of π has a local supercycle violation **then return**(tt) **fi** ▷Clause 2a holds
8. **forall** wait-for paths π' from the border of D^ℓ_a to B_i
9. **if** some node of π' has a local supercycle violation **then return**(tt) **fi** ▷Clause 2b holds
10. **return**(ff) ▷Definition 31, Clause 2 does not hold

Figure 10: Pseudocode for the implementation of the local AND-OR condition.

LocScViol($D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}$)
▷ compute supercycle violations in state t_{a} of D_{a}^{ℓ}
▷ Postcondition: $\forall\, v \in D_{\mathsf{a}}^{\ell}, d' = 1, \ldots, dd : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d'] = \mathsf{scViolateLoc}(v, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
1. $dd \leftarrow$ length of the longest simple path in structure graph of D_{a}^{ℓ}
2. **forall** $d \leftarrow 1$ *to* dd
3. LocScViolDist($D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}, d$)
4. **endfor**

LocScViolDist($D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}, d$)
▷ compute level-d supercycle violations in state t_{a} of D_{a}^{ℓ}
▷ Precondition: $\forall\, v \in D_{\mathsf{a}}^{\ell}, d' = 1, \ldots, d-1 : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d'] = \mathsf{scViolateLoc}(v, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
▷i.e., all violations up to level $d-1$ have already been computed and stored in $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d']$
▷ Postcondition: $\forall\, v \in D_{\mathsf{a}}^{\ell}, d' = 1, \ldots, d : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d'] = \mathsf{scViolateLoc}(v, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
▷i.e., compute next level of violations
1. **forall** $v \in \{B_1, \ldots, B_n\} \cup \gamma$
2. LocScViolDistNode($D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}, d, v$)
3. **endfor**

LocScViolDistNode($D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}, d, v$)
▷ compute level-d supercycle violation of node v in state t_{a} of D_{a}^{ℓ}, i.e., computes $\mathsf{scViolateLoc}(v, d, t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
▷ Precondition: $\forall\, w \in D_{\mathsf{a}}^{\ell}, d' = 1, \ldots, d-1 : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[w, d'] = \mathsf{scViolateLoc}(w, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
▷ Postcondition: $\forall\, w \in D_{\mathsf{a}}^{\ell} - v, d' = 1, \ldots, d-1 : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[w, d'] = \mathsf{scViolateLoc}(w, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell}) \wedge$
▷ $\forall\, d' = 1, \ldots, d : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d'] = \mathsf{scViolateLoc}(w, d', t_{\mathsf{a}}, D_{\mathsf{a}}^{\ell})$
1. **if** $(d = 1)$
2. **if** (v is an interior interaction aa and $\neg(\exists\, \mathsf{B}_i : \mathsf{aa} \rightarrow \mathsf{B}_i \in W_{D_{\mathsf{a}}^{\ell}}(t_{\mathsf{a}}))$)
3. $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, 1] \leftarrow \mathtt{tt}$ ▷no outgoing wait-for-edges
4. **else** $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, 1] \leftarrow \mathtt{ff}$
5. **fi**
6. **fi**
▷ here $d > 1$
7. **if** (v is an interior interaction aa and $(\forall\, \mathsf{B}_i : \mathsf{aa} \rightarrow \mathsf{B}_i \in W_{D_{\mathsf{a}}^{\ell}}(t_{\mathsf{a}}) : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[B_i, d-1])$)
8. $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d] \leftarrow \mathtt{tt}$
9. **else if** (v is a component B_i and $(\exists\, \mathsf{aa} : \mathsf{B}_i \rightarrow \mathsf{aa} \in W_{D_{\mathsf{a}}^{\ell}}(t_{\mathsf{a}}) : V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[\mathsf{aa}, d-1])$)
10. $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d] \leftarrow \mathtt{tt}$
11. **else** $V_{D_{\mathsf{a}}^{\ell}, t_{\mathsf{a}}}[v, d] \leftarrow \mathtt{ff}$
12. **fi**

Figure 11: Procedure to compute all supercycle-violations in state t_{a} of D_{a}^{ℓ}

7.3 Implementation and Experimentation for the Linear Condition

LDFC-BIP, ($\sim$ 1500 LOC Java) implements our method for finite-state BIP-systems. Pseudocode for LDFC-BIP is shown in Figure 12. LLin(B, Q_0) iterates over each interaction a of (B, Q_0), and checks $(\exists\, \ell > 0 : \mathcal{LLIN}(B, Q_0, \mathsf{a}, \ell))$ by starting with $\ell = 1$ and incrementing ℓ until either $\mathcal{LLIN}(B, Q_0, \mathsf{a}, \ell)$ is found to hold, or D_{a}^{ℓ} has become the entire system and $\mathcal{LLIN}(B, Q_0, \mathsf{a}, \ell)$ does not hold. In the latter case, $\mathcal{LLIN}(B, Q_0, \mathsf{a}, \ell)$ does not hold for any finite ℓ, and, in practice, computation would halt before D_{a}^{ℓ} had become the entire system, due to exhaustion of resources.

LLinIntDist$(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ checks $\mathcal{LLIN}(B, Q_0, \mathsf{a}, \ell)$ by examining every reachable transition that executes a, and checking that the final state satisfies Definition 34.

Complexity. The running time of our implementation is $O(\Sigma_{a\in\gamma}|D_{\mathsf{a}}^{\ell_a}|)$, where ℓ_a is the smallest value of ℓ for which $\mathcal{LLIN}(\mathsf{a}, \ell)$ holds, and where $|D_{\mathsf{a}}^{\ell_a}|$ denotes the size of the transition system of $D_{\mathsf{a}}^{\ell_a}$.

LLin(B, Q_0), where $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n)$
1. **forall** interactions $\mathsf{a} \in \gamma$
2. **if** (LLinInt$(\mathsf{B}, Q_0, \mathsf{a}) = \mathtt{ff}$) **return**(ff) **fi**
3. **endfor**;
4. **return**(tt) ▷ return tt if check succeeds for all $\mathsf{a} \in \gamma$

LLinInt$(\mathsf{B}, Q_0, \mathsf{a})$, where $\mathsf{B} \triangleq \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n), \mathsf{a} \in \gamma$
▷ check $(\exists\, \ell > 0 : \mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell))$
1. $\ell \leftarrow 1$; ▷ start with $\ell = 1$
2. **while** (tt)
3. **if** (LLinIntDist$(\mathsf{a}, \ell) = \mathtt{tt}$) **return**(tt) **fi**; ▷ success, so return true
4. **if** $(D_{\mathsf{a}}^{\ell} = \gamma(\mathsf{B}_1, \ldots, \mathsf{B}_n))$ **return**(ff) **fi**; ▷ exhausted all subsystems, return false
5. $\ell \leftarrow \ell + 1$ ▷ increment ℓ until success or intractable or failure
6. **endwhile**

LLinIntDist$(\mathsf{B}, Q_0, \mathsf{a}, \ell)$
1. **forall** reachable transitions $s_{\mathsf{a}} \xrightarrow{\mathsf{a}} t_{\mathsf{a}}$ of D_{a}^{ℓ}
2. **if** $(\neg(\forall\, \mathsf{B}_i \in \mathit{components}(\mathsf{a}) : \mathit{in\_depth}_{D_{\mathsf{a}}^{\ell}}(\mathsf{B}_i, t_{\mathsf{a}}) \geq 2\ell - 1 \vee \mathit{out\_depth}_{D_{\mathsf{a}}^{\ell}}(\mathsf{B}_i, t_{\mathsf{a}}) \geq 2\ell - 1))$
3. **return**(ff) ▷ check Definition 34
4. **fi**
5. **endfor**;
6. **return**(tt) ▷ return tt if check succeeds for all transitions

Figure 12: Pseudocode for the implementation of the linear condition.

7.3.1 Experiment: Dining Philosophers

We consider n philosophers in a cycle, based on the components of Figure 1. Figure 14(a) provides experimental results. The x axis gives the number n of philosophers (and also the number of forks), and the y axis gives the verification time (in milliseconds). We verified that $\mathcal{LLIN}(a, \ell)$ holds for $\ell = 1$ and all interactions a. Hence dining philosophers is deadlock-free. We increase n and plot the verification time for both LDFC-BIP and D-Finder 2 [8]. D-Finder 2 implements a compositional and incremental method for the verification of BIP-systems. D-Finder (the precursor of D-Finder 2) has been compared favorably with NuSmv and SPIN, outperforming both NuSmv and SPIN on dining philosophers, and outperforming NuSmv on the gas station example [7], treated next. Our results show that LDFC-BIP has a linear increase of computation time with the system size (n), and so outperforms D-Finder 2.

7.3.2 Experiment: Gas Station

A gas station [13] consists of an operator, a set of pumps, and a set of customers. Before using a pump, a customer has to prepay. Then the customer uses the pump, collects his change and starts a new transaction. Before being used by a customer, a pump has to be activated by the operator. When a pump is shut off, it can be re-activated for the next operation.

Figure 13 gives the model for a gas station system for one pump and two customers. The operator has two control locations and three ports. The transition labeled with *prepay* accepts a customer's prepay and activates the pump for the customer. When a customer is served, the transition labeled with *finish* synchronizes the pump and the customer. A pump has three control locations and three ports. Besides the synchronization between the operator and customer through activate and finish ports, a pump and a customer are synchronized through *start* ports.

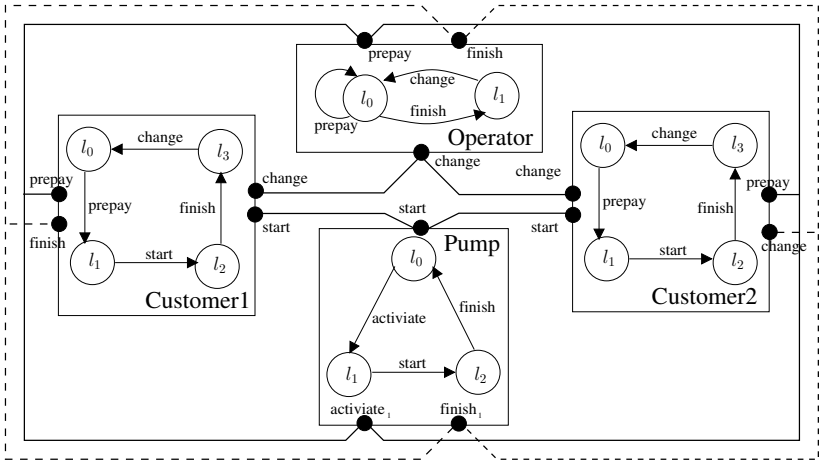
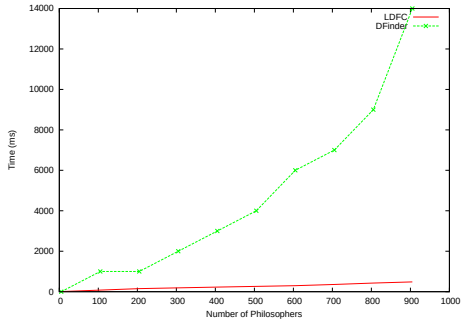
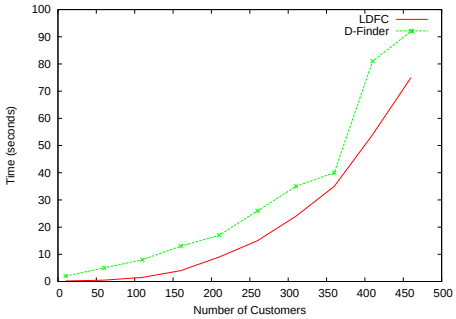


Figure 13: Sketch of Gas Station

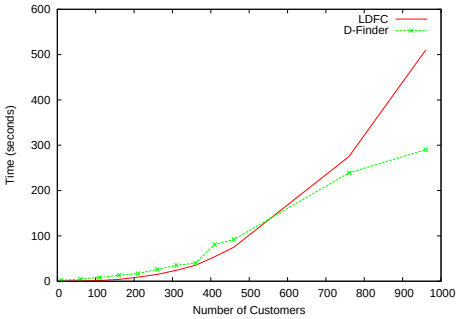
We verified $\mathcal{LLIN}(\mathsf{B}, Q_0, \mathsf{a}, \ell)$ for $\ell = 2$ and all interactions a. Hence gas station is deadlock-free. Figures 14(b), 14(c), and 14(d) present the verification times using LDFC-BIP and D-Finder 2. We consider a system with 3 pumps and variable number of customers. In these figures, the x axis gives the number n of customers, and the y axis gives the verification time (in



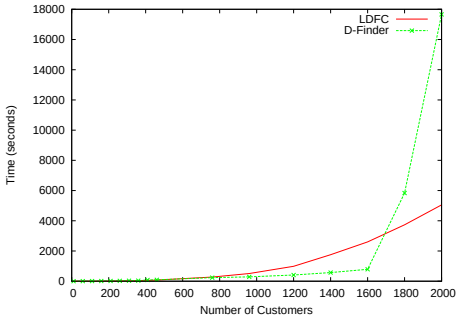
(a) Dining philosophers benchmark.



(b) Gas station benchmark 1.



(c) Gas station benchmark 2.



(d) Gas station benchmark 3.

Figure 14: Benchmarks generated by our experiments.

seconds). D-Finder 2 suffers state-explosion at $n = 1800$, because we consider only three pumps, and so the incremental method used by D-Finder 2 deteriorates. LDFC-BIP outperforms D-Finder 2 as the number of customers increases.

8 Discussion, Related Work, and Further Work

Related work. The notions of wait-for-graph and supercycle [3, 4] were initially defined for a shared memory program $P = P_1 \parallel \cdots \parallel P_K$ in *pairwise normal form*: a binary symmettric relation I specifies the directly interacting pairs ("neighbors") $\{P_i, P_j\}$. If P_i has neighbors P_j and P_k, then the code in P_i that interacts with P_j is expressed separately from the code in P_i that interacts with P_k. These synchronization codes are executed synchronously and atomically, so the grain of atomicity is proportional to the degree of I. Attie and Chockler [3] give two polynomial time methods for deadlock freedom. The first checks subsystems consisting of three processes. The second computes the wait-for-graphs of all pair subsystems $P_i \parallel P_j$, and takes their union, for all pairs and all reachable states of each pair. The first method considers only wait-for-paths of length ≤ 2. The second method is prone to false negatives, because wait-for edges generated by different states are all merged together, which can result in spurious supercycles

Gössler and Sifakis [12] use a BIP-like formalism, Interaction Models. They present a criterion for global deadlock freedom, based on an and-or graph with components and constraints as the two sets of nodes. A constraint gives the condition under which a component is blocked. Edges are labeled with conjuncts of the constraints. Deadlock freedom is checked by traversing every cycle, taking the conjunction of all the conditions labeling its edges, and verifying that this conjunction is always false, i.e., verifying the absence of cyclical blocking. No complexity bounds are given. Martens and Majster-Cederbaum [14] present a polynomial time checkable deadlock freedom condition based on structural restrictions: "the communication structure between the components is given by a tree." This restriction allows them to analyze only pair systems. Brookes and Roscoe [11] provide criteria for deadlock freedom of CSP programs based on structural and behavioral restrictions combined with analysis of pair systems. No implementation, or complexity bounds, are given. Aldini and Bernardo [1] use a formalism based on process algebra. They check deadlock by analysing cycles in the connections between software components, and claim scalability, but no complexity bounds are given.

We compared our implementation LDFC-BIP to D-Finder 2 [8]. D-Finder 2 computes a finite-state abstraction for each component, which it uses to compute a global invariant I. It then checks if I implies deadlock freedom. Unlike LDFC-BIP, D-Finder 2 handles infinite state systems. However, LDFC-BIP had superior running time for dining philosophers and gas station (both finite-state).

All the above methods verify global (and not local) deadlock-freedom. Our method verifies both. Also, our approach makes no structural restriction at all on the system being checked for deadlock.

Discussion. Our approach has the following advantages:

Local and global deadlock Our method shows that no subset of processes can be deadlocked, i.e., absence of both local and global deadlock.

Check works for realistic formalism By applying the approach to BIP, we provide an efficient deadlock-freedom check within a formalism from which efficient distributed implementations can be generated [9].

Locality If a component B_i is modified, or is added to an existing system, then $\mathcal{LLIN}(a, \ell)$ only has to be re-checked for B_i and components within distance ℓ of B_i. A condition whose evaluation considers the entire system at once, e.g., [1, 8, 12] would have to be re-checked for the entire system.

Easily parallelizable Since the checking of each subsystem D_a^ℓ is independent of the others, the checks can be carried out in parallel. Hence our method can be easily parallelized and distributed, for speedup, if needed. Alternatively, performing the checks sequentially minimizes the amount of memory needed.

Framework aspect Supercycles and in/out-depth provide a *framework* for deadlock-freedom. Conditions more general and/or discriminating than the one presented here should be devisable in this framework. This is a topic for future work.

Further work. Our implementation uses explicit state enumeration. Using BDD's may improve the running time when $\mathcal{LLIN}(a, \ell)$ holds only for large ℓ. An enabled port p enables all interactions containing p. Deadlock-freedom conditions based on ports could exploit this interdepence among interaction enablement. Our implementation should produce *counterexamples* when a system fails to satisfy $\mathcal{LLIN}(a, \ell)$. *Design rules* for ensuring $\mathcal{LLIN}(a, \ell)$ will help users to produce deadlock-free systems, and also to interpret counterexamples. A *fault* may create a deadlock, i.e., a supercycle, by creating wait-for-edges that would not normally arise. Tolerating a fault that creates up to f such spurious wait-for-edges requires that there do not arise during normal (fault-free) operation subgraphs of $W_B(s)$ that can be made into a supercycle by adding f edges. We will investigate criteria for preventing formation of such subgraphs. Methods for evaluating $\mathcal{LLIN}(a, \ell)$ on *infinite state* systems will be devised, e.g.,, by extracting proof obligations and verifying using SMT solvers. We will extend our method to *Dynamic BIP*, [10], where participants can add and remove interactions at run time.

References

[1] Alessandro Aldini and Marco Bernardo. A General Approach to Deadlock Freedom Verification for Software Architectures. *FME*, 2805:658–677, 2003.

[2] Paul C. Attie. Synthesis of large concurrent programs via pairwise composition. In *CONCUR'99*, number 1664 in LNCS. Springer-Verlag, August 1999.

[3] Paul C. Attie and H. Chockler. Efficiently Verifiable Conditions for Deadlock-freedom of Large Concurrent Programs. In *VMCAI*, France, January 2005.

[4] Paul C. Attie and E. Allen Emerson. Synthesis of Concurrent Systems with Many Similar Processes. *TOPLAS*, 20(1):51–115, January 1998.

[5] P.C. Attie, N. Francez, and O. Grumberg. Fairness and Hyperfairness in Multiparty Interactions. *Distributed Computing*, 6:245–254, 1993.

[6] Ananda Basu, Marius Bozga, and Joseph Sifakis. Modeling Heterogeneous Real-time Components in BIP. In *SEFM*, pages 3–12, September 2006.

[7] S. Bensalem, M. Bozga, T.H. Nguyen, and J. Sifakis. Compositional verification for component-based systems and application. *Software, IET*, 4(3):181–193, 2010.

[8] Saddek Bensalem, Andreas Griesmayer, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, and Rongjie Yan. D-finder 2: Towards efficient correctness of incremental design. In *NASA Formal Methods*, pages 453–458, 2011.

[9] Borzoo Bonakdarpour, Marius Bozga, Mohamad Jaber, Jean Quilbeuf, and Joseph Sifakis. From High-level Component-based Models to Distributed Implementations. In *EMSOFT*, pages 209–218, 2010.

[10] Marius Bozga, Mohamad Jaber, Nikolaos Maris, and Joseph Sifakis. Modeling Dynamic Architectures Using Dy-BIP. In *Software Composition*, pages 1–16, 2012.

[11] S.D. Brookes and A.W. Roscoe. Deadlock analysis in networks of communicating processes. *Distributed Computing*, 4:209–230, 1991.

[12] Gregor Gössler and Joseph Sifakis. Component-based construction of deadlock-free systems. In *FSTTCS*, pages 420–433. Springer, 2003.

[13] David Heimbold and David Luckham. Debugging Ada tasking programs. *Software, IEEE*, 2(2):47 –57, March 1985.

[14] Moritz Martens and Mila Majster-Cederbaum. Deadlock-freedom in component systems with architectural constraints. *FMSD*, 41:129–177, 2012.

[15] Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994.