文章编号: 1001- 2486(2008) 01- 0089- 05

可组合仿真模型的语义形式描述及组合判定方法*

周东祥, 李 群, 王维平
(国防科技大学 信息系统与管理学院, 湖南 长沙 410073)

摘 要: 如何判定仿真组件之间是否可组合是组合仿真中的关键问题之一。建立了组合判定问题的参考模型, 基于Hoare 逻辑给出仿真模型语义的描述方法, 并以此为基础通过构造模型语义之间的组合匹配规则, 从组合相容性及可替换性两个方面刻画模型的可组合性质, 形成语义层次的组合判定方法; 对组合相容性与可替换性质之间的关系进行了分析。

关键词: 组合仿真; 组合判定; 语义相容性; 语义可替换性
中图分类号: TP391. 9 文献标识码: A

Formal Representation of Semantics for Composable Simulation Models and Checking Rules for Semantic Composablity

ZHOU Dong-xiang, LI Qun, WANG Wei-ping
(College of Information Systems and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: How to perform the composability checking between models is one crucial issue in the composable simulation development. In light of this, the reference model of composability checking problem was proposed, then an approach to semantic representation of simulation models based on Hoare Logic was presented. As the compatibility and substitutability are the two flip sides of composability coin, the rules to check the compatibility and substitutability between semantics of simulation models were constructed, and the formal approach to semantic composability checking was established. Finally, the relations between the semantic compatibility and substitutability were analyzed.

Key words: composable simulation; composability checking; semantic compatibility; semantic substitutability

随着武器装备体系日趋复杂化和军事需求逐渐多样化, 建模仿真不再局限于单个组织的行为, 而是强调仿真系统和模型的联合开发, 需要跨领域、跨组织的协同工作。针对当前不断发展的组合仿真需求, 美国防部建模仿真办公室(DMSO) 于 2002 年提出可组合使命空间(CMSE) 的研究倡议, 旨在全面提高仿真模型及应用的可组合能力, 实现仿真系统的柔性、敏捷组合开发[1], 目前组合仿真已经成为复杂系统建模及军用仿真的研究热点之一[2]。

组合仿真面临的一个关键问题是判断两个模型组件是否可组合, 在什么层次上可以组合, 即组合判定问题。目前大多数组合仿真研究集中在工程实现层次, 即设计或借鉴某种建模仿真框架, 实现基于组件的仿真开发的过程[3], 这些方法的共同特性是基于组件模型的语法约束进行组合, 即连接在一起的组件在接口类型、变量个数等语法要素上可以组合, 这种组合只能保证组件正确地连接在一起, 属于模型的静态组合, 无法准确地描述和保证组件在语义上是否具备可组合性。针对语义层次的组合判定问题, Petty 从模型及组合模型有效性的角度出发建立了语义可组合理论[4], 该理论本质上是关于模型验证及校核的研究, 它只能在理想状况下(存在完美模型的完全行为轨迹序列) 判断组合模型的观测行为是否有效, 从而给出是否能够组合的结论。Petty 语义组合理论无法说明究竟什么因素导致不可组合、模型语义究竟在哪些地方无法匹配等问题。导致这些问题的原因, 一是没有对模型的语义进行清晰的界定, 二是没有深入分析模型组合过程中的匹配关系。Hoare 逻辑是用于证明程序正确性的逻辑系统, 它在形

* 收稿日期: 2007- 06- 27
基金项目: 国家自然科学基金资助项目(60574056)
作者简介: 周东祥(1978—), 男, 博士生。

式语言研究中通常用于建立程序语言的公理语义[5]。本文在 Hoare 逻辑的基础上建立了模型动态语义的形式描述,并通过构造模型语义间的组合相容性规则及组合替换性规则,建立语义层次上的组合判定方法。

1 可组合仿真模型的形式语义描述

根据 Zeigler 的层次化系统规范[6],可以在不同的层次上定义系统。在层次化系统规范中,可以将输入- 输出(I/O)层次上的系统视为一个转换式系统,即给定该系统一个输入,经过若干计算步骤最终得到一个输出。转换式系统定义了输入与输出之间的函数关系,可把它看作是从初始状态到终止状态(或终止结果)的函数,函数可以是多变量函数。

定义 1 模型是可计算的函数,它表示为 $M:(S,I)\rightarrow(S,O)$。其中 S 为模型的状态变量,I,O 分别为模型的输入变量及输出变量。

模型定义中的"可计算"在计算理论中有严格的形式定义。可计算函数是指能被某个算法,或图灵机、计算机,用有限数目的计算步骤完成的函数。模型的可计算性能够保证模型计算可以终止,因此可采用 Hoare 逻辑描述模型在输入- 输出层次上的行为性质。Hoare 逻辑系统 $\mathscr{H}$ 的合式公式称为前后断言公式,它是形如 $\{P\}\ \alpha\ \{Q\}$ 的公式[5],表示对于所有满足 P 的状态 σ,如果在 σ 下执行 α 后终止在状态 σ',则 σ' 满足 Q,P 和 Q 一般是一阶谓词逻辑或命题逻辑公式。

语义层次组合建立在正确的语法组合之上,因此在本文讨论语义组合时假定模型之间可以实现正确的语法组合。Hoare 逻辑的前、后谓词都包含对系统状态的形式约束,而组合过程中模型之间通过输入- 输出进行交互,模型内部状态对于组合而言并不重要,为了描述模型在输入- 输出层次(行为层次)的动态性质,本节在前后断言公式的基础上引入模型行为的前条件以及后条件。令 $Input_M$ 表示模型 M 的输入参数集合,$Output_M$ 表示输出参数集合。

定义 2 模型 M 行为的前条件 pre_M 由序偶 $(Input_M, P(Input_M))$ 描述。其中 $P(Input_M)$ 为定义在 $Input_M$ 上的谓词公式集合。

同理可以定义 M 行为的后条件 $post_M:(Output_M, P(Output_M))$。模型的行为可视为模型的输入- 输出序列,其中每个输入- 输出对称为模型的原子行为,根据模型原子行为的前条件和后条件,其动态语义可以借鉴 Hoare 逻辑定义:

定义 3 模型 M 原子行为的语义由 $H_M=(pre_M, post_M)$ 描述,pre_M,$post_M$ 定义同上,二者都用一阶谓词公式表示。

2 模型语义组合判定规则

所谓仿真可组合性(Composability),是指以不同的组合形式选取和装配仿真组件形成仿真系统,从而满足特定用户需求的一种能力[4]。借鉴模型互操作领域的研究思路,组合判定问题可以从相容性及可替换性两个方面考虑。相容性指组件之间是否能够协调地工作,可替换性关注组件被替换后是否影响其观测行为、影响到何种程度等问题。仿真模型可以存在多个组合层次,分别为技术层次、语法层次、语义层次及概念层次[2]。除组合层次之外,组合判定问题需要明确组合的上下文环境,本文将组合上下文限定在组合过程的特定机制,分别是顺序组合、选择组合、嵌入(插件)组合以及混合组合模式。顺序组合指模型之间的协作类似于流水线上的前后加工工序,顺序组合的模型具有先后执行的顺序运行关系;选择组合模式是指根据上下文环境参数,执行其中一个仿真组分的功能;嵌入组合模式常用于描述仿真组分之间具有功能或结构上的"外包"或"委托"关系,也可以描述组分之间的"整体- 部分"关系;混合组合模式可以将上述不同模式混合起来使用,以应对更加复杂的组合需求,进而构造出功能更加强大的仿真组分。在不同组合模式规定的上下文中,本文将组合判定问题进一步限定在语义层次的仿真可组合问题上,即研究模型组件在语义层次上的相容性及可替换性问题。

判断两模型原子行为的交互序列是否满足某种组合性质,最终可以归结为原子行为语义之间的组

合是否满足某种组合性质。因此可通过考察两个原子行为的前条件、后条件之间的关系, 构造模型语义组合匹配规则作为组合判定依据。在给出一般意义上的语义组合规则之前, 首先需要声明在组合匹配规则中使用的扩展逻辑关系操作符。

令 $LR=\{\leftrightarrow, \overrightarrow{}, \oplus, nil\}$, 其组成元素分别表示逻辑等价连接符、逻辑蕴涵连接符, 异或连接符及无连接符, 用于连接两个一阶谓词公式。若在由 $r_i \in LR$ 连接的一系列谓词公式中, 其中某个连接符为 nil, 则规定表示可将它们从原来的谓词公式中忽略掉, 即 $P\ nil\ Q$ 表示一阶谓词公式 P 和 Q 之间可以具有任意逻辑关系, 因此可将其忽略掉。在参考组件检索领域对组件功能相似问题的研究基础上[7], 定义一般意义上的动态语义组合规则, 然后将组合条件弱化, 构造针对不同组合性质即相容性及可替换性的判断规则。

定义 4 语义组合规则: M 与 N 具备语义可组合性, 如果 $GenCR(M, N)=(pre' \mathscr{R}_1 pre_N) \wedge (post' \mathscr{R}_2 post_M)$ 在 M、N 解释下为真, 此时也可称 M 和 N 满足语义组合规则 $GenCR$。

pre' 根据不同组合需求, 可取值 pre_M 或 $pre_M \wedge post_M$, $post'$ 可取值 $post_N\ pre_N \wedge post_N$, $\mathscr{R}_1$, $\mathscr{R}_2$ 不必相同, 当 $\mathscr{R}_1$ ($\mathscr{R}_2$) 取值为 nil 时, pre' ($post'$) 取值不做要求, 用 × 表示可以忽略该项。注意 M 与 N 之间的这种组合匹配关系不一定是对称的, 即 $GenCR(M, N)$ 成立并不表示 $GenCR(N, M)$ 也成立, 反之亦然。

3 模型组合的相容性质判定

模型组合的语义相容性主要考察模型交互过程中一方提供的语义信息是否能够满足对方期望的语义约束, 若能满足则具备语义相容性。首先考虑顺序执行情况下的相容判定准则, 考虑如下过程: M 执行完毕后为 N 提供输入, 然后 N 继续执行。

定义 5 顺序执行相容性规则: 将 $GenCR$ 中的 R_1 实例化为“$\overrightarrow{}$”, R_2 为“nil”, pre' 为 $post_M$, $post'$ 为 ×, 令 $CR_{seq}(M, N)=post_M \overrightarrow{} pre_N$, 若 M 和 N 使 $CR_{seq}(M, N)$ 成立, 则 M 与 N 具备顺序执行相容性。

顺序执行相容性保证 M 执行完毕后能够满足 N 继续执行的前条件, 它只判断 M 的后条件及 N 的前条件之间是否能够匹配, 有时为了对相容模型施加更强的约束, 可通过对前条件的判断以加强对相容模型在后条件上的要求。加入的判断类似于状态转移图中的守卫条件(guard)判断, 因此将类似的判断规则称为守卫相容性规则。

定义 6 顺序执行守卫相容性规则: 将 $GenCR$ 中的 R_1 实例化为“$\overrightarrow{}$”, R_2 为“nil”, pre' 为 $pre_M \wedge post_M$, $post'$ 为 ×, 令 $CR_{guard}(M, N)=pre_M \wedge post_M \overrightarrow{} pre_N$, 若 M 和 N 使 $CR_{guard}(M, N)$ 成立, 则 M 与 N 具备守卫顺序执行相容性。

由于选择执行过程中 M 和 N 不能同时运行, 因此 M 的前条件不能同时为真。

定义 7 选择执行相容性规则: 将 $GenCR$ 中的中 R_1 实例化为异或关系“$\oplus$”, R_2 为“nil”, pre' 为 pre_M, $post'$ 为 ×, 令 $CR_{sel}(M, N)=pre_M \oplus pre_N$, 若 M 和 N 使 $CR_{sel}(M, N)$ 成立, 则 M 与 N 具备选择执行相容性。

4 模型组合的语义可替换性质

组合仿真开发过程的一般模式是将粒度更小、功能相对单一的组件组装在一起, 从而形成满足预期需求的复杂系统, 此时如何判断仿真模型是否可以替换其他模型是一个十分关键的问题, 即语义可替换性的问题。是否能够互换, 语义可替换性主要考察两个模型原子行为的语义是否具备一致性, 从而用一个模型代替其他模型所引起的观测行为差异不超出事先预期的范围。

定义 8 严格替换规则: 将 $GenCR$ 中的 R_1, R_2 实例化为“$\leftrightarrow$”, pre' 为 pre_M, $post'$ 为 $post_N$, 令 $SR_E(M, N)=(pre_M \leftrightarrow pre_N) \wedge (post_N \leftrightarrow post_M)$, 如果 M 和 N 使 $SR_E(M, N)$ 为真, 则称 M 可以严格组合匹配 N。

严格替换关系表示模型行为等价, 模型互换不会观测层次上的行为变化, 且 SR_E 具有对称性。

定义 9 插件替换规则: 将 $GenCR$ 中的 R_1、R_2 实例化为“$\overrightarrow{}$”, pre' 为 pre_M, $post'$ 为 $post_N$, 令 $SR_{plug}(M, N)=(pre_M \overrightarrow{} pre_N) \wedge (post_N \overrightarrow{} post_M)$, 若 M、N 使 SR_{plug} 为真, 则称 N 可插件替换 M。

SR_{plug} 要求 N 比 M 的前条件弱,后条件强。在有些情况下并不需要完全遵守插件替换规则,如模型 A、B 组合过程中 A 只要求 B 的行为结果满足某个条件即可,即 A 只对 B 的后置条件有要求,而不约束 B 的前置条件。此时只考虑后条件之间是否满足插件组合匹配关系,略掉 A 与 B 前条件之间的关系,这种弱化的插件组合关系称为后置替换组合。

定义 10 后置替换规则:将 $GenCR$ 中 R_1 实例化为"nil",R_2 为"$\rightarrow$",pre' 为 $\times$,$post'$ 为 $post_N$,令 $SR_{post}(M,N) = post_N \rightarrow post_M$,若 M 和 N 使 SR_{post} 为真,则 N 可以后置插件替换 M。

后置替换组合还存在另外一种比较严格的替换规则,即后条件需要严格等价。

定义 11 严格后置替换规则:$GenCR$ 中 R_2 实例化为"$\leftrightarrow$",其余与后置替换规则相同,即 $SR_{E-post}(M,N) = post_N \leftrightarrow post_M$。$\leftrightarrow$ 具有对称性,因此严格后置替换规则具有对称性。

与守卫相容性规则类似,为了对替换模型加以更严格的约束,可以引入以下守卫替换规则:

定义 12 插件守卫替换规则:将 $GenCR$ 中 R_1、R_2 全部实例化为"$\rightarrow$",pre' 为 pre_M,$post'$ 为 $pre_N \wedge post_N$,令 $SR_{g-plug}(M,N) = (pre_M \rightarrow pre_N) \wedge (pre_N \wedge post_N \rightarrow post_M)$,若 M 和 N 使 SR_{g-plug} 为真,则 N 可插件守卫替换 M。

定义 13 后置守卫替换规则:将 $GenCR$ 中 R_1 实例化为"nil",R_2 为"$\rightarrow$",pre' 为 $\times$,$post'$ 为 $pre_N \wedge post_N$,令 $SR_{g-post}(M,N) = pre_N \wedge post_N \rightarrow post_M$,若 M 和 N 使 SR_{g-post} 为真,则 N 可后置守卫替换 M。

5 相容性与可替换性的关系

相容性与可替换性是模型可组合性质的两个方面。相容性与可替换性之间具有相互校准的约束机制,组件之间的相容性并不受组件替换影响。若模型 A 与 B 具备可替换性,并且模型 A 与 C 是相容的,则要求 B 替换 A 后仍与 C 保持相容性。即可替换性保证 A 的语义约束性质能够保持。

性质 1 模型可替换性规则对相容性规则具有保持作用。

证明:针对每条相容性规则,证明任意替换规则对其具有保持作用。首先证明插件替换规则对顺序相容规则的保持作用。设 A 与 B 满足插件替换关系,即 $(pre_A \rightarrow pre_B) \wedge (post_B \rightarrow post_A)$ 恒真,因此 $pre_A \Rightarrow pre_B$ 并且 $post_B \Rightarrow post_A$;$A$ 与 C 满足顺序相容关系,即 $post_A \Rightarrow pre_C$ 成立,因此有 $post_B \Rightarrow post_A \Rightarrow pre_C$,这表明 B 替换 A 后与 C 仍具备相容性关系。其他替换规则与相容规则之间的关系证明过程与此类似,限于篇幅将其他规则间的关系证明省略。由于守卫规则引入了守卫条件,因此守卫替换和相容规则之间并不满足性质 1 的保持作用。

性质 2 不同组合替换规则之间的逻辑关系如图 1 所示,其中"$\rightarrow$"表示逻辑蕴含关系"$\Rightarrow$"。

证明:由一阶谓词逻辑知:若 $A \Leftrightarrow B$ 成立,则 $A \Rightarrow B$,$B \Rightarrow A$ 均成立;并且 $A \wedge B \Rightarrow A$,B 成立。若 M、N 满足严格替换规则,由定义知 $(pre_M \leftrightarrow pre_N) \wedge (post_N \leftrightarrow post_M)$ 恒为真,于是 $pre_M \leftrightarrow pre_N$ 与 $post_N \leftrightarrow post_M$ 同时恒真,即 $pre_M \Leftrightarrow pre_N$ 与 $post_N \Leftrightarrow post_M$ 同时成立,于是 $pre_M \Rightarrow pre_N$,$post_N \Rightarrow post_M$ 成立,可以推出 $(pre_M \rightarrow pre_N) \wedge (post_N \rightarrow post_M)$ 恒真,因此 $SR_E \Rightarrow SR_{plug}$ 成立。同理可证 $SR_E \Rightarrow SR_{E-post}$,$SR_{E-post} \Rightarrow SR_{post}$。

由一阶谓词逻辑知 $A \wedge C \Rightarrow A$ 成立,此时若 $A \Rightarrow B$ 成立,则 $A \wedge C \Rightarrow B$ 也成立。M、N 满足插件替换规则 $(pre_M \rightarrow pre_N) \wedge (post_N \rightarrow post_M)$,运用上述推理过程可得 $(pre_M \rightarrow pre_N) \wedge (pre_N \wedge post_N \rightarrow post_M)$ 成立,即满足插件守卫替换规则,因此 $SR_{plug} \Rightarrow SR_{guard}$。同理可证 $SR_{post} \Rightarrow SR_{g-post}$。$SR_{g-plug} \Rightarrow SR_{g-post}$ 的证明过程与上述类似,限于篇幅省略其证明。

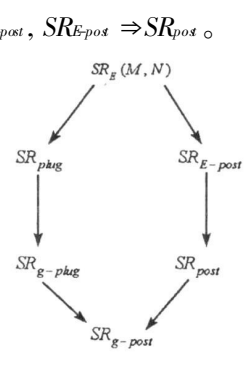

图 1 语义组合规则之间的逻辑关系图

Fig. 1 The logic relation of semantic composability rules

各组合替换规则之间除了具有上述基本关系外,还存在其他性质,如:

$$SR_{plug}(M,N) \wedge SR_{plug}(N,M) \Leftrightarrow SR_E(M,N);$$

$$SR_{post}(M,N) \wedge SR_{post}(N,M) \Leftrightarrow CM_{E-post}(M,N)$$

6 结 论

如何判断仿真模型之间是否能够组合, 在何种程度上能够组合, 是组合仿真方法中急需解决的关键问题之一。组合判定问题存在多个层次, 目前大多数基于组件的仿真都只能在语法层次上判断组件之间是否可以组合, 但仅有语法组合对于保证组合过程的正确性及合理性是不够的, 本文试图在模型语义层次上建立判定可组合性的方法, 主要工作集中在模型的语义描述、组合相容性、可替换性分析及其组合匹配规则。

本文以Hoare 逻辑作为描述模型语义的方法, 并据此建立语义组合判定方法。由于Hoare 逻辑只能描述模型单次计算即原子行为的语义约束, 而无法描述模型的行为序列(可能不终止) 的语义性质, 因此本文研究范围限定在模型原子行为层次, 将模型在时间与空间上孤立起来分析组合过程的特征与约束, 空间上孤立是指不考虑两个模型与外部环境之间的交互作用, 时间上孤立是指只研究连续交互行为序列中原子行为所表现的动态语义之间的相容性及可替换性, 并且只考虑两个模型的组合, 没有涉及多个模型之间的组合问题。下一步的研究工作将逐步集中在模型行为序列的动态语义间的组合判定, 分布并发环境下模型间组合机制等问题。

参 考 文 献:

[1] Morse K L, Petty M D, Reynolds P F, et al. Findings and Recommendations from the 2003 Composable Mission Space Environments Workshop [C]// Proceedings of the Spring Simulation Interoperability Workshop, Arlington, VA, 2004.

[2] 周东祥, 仲辉, 李群, 等. 复杂系统仿真的可组合问题研究综述[J]. 系统仿真学报, 2007, 19 (8).

[3] Weisel E W, Petty M D, Mielke R R. A Survey of Engineering Approaches to Composability [C]// Proceedings of the Spring Simulation Interoperability Workshop. Arlington, VA, 2004.

[4] Petty M D, Weisel E W, Mielke R R. A Formal Approach to Composability[C]// Proceedings of the Interservice/ Industry Training, Simulation and Education Conference Orlando, FL, 2003.

[5] 陈意云. 形式语义学基础[M]. 合肥: 中国科技大学出版社, 1994.

[6] Zeigler B P, Praehofer H, Kim T G. Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems[M]. San Diego, CA: Academic Press, 2000.

[7] Zaremski A M, WING J M. Specification Matching of Software Components[J]. ACM Transactions on Software Engineering and Methodology, 1997, 6 (4): 333- 369.

(上接第 77 页)

参 考 文 献:

[1] Kirwan B. A Guide to Practical Human Reliability Assessment [M]. Taylor & Francis, 1994.

[2] Swain A D, Guttmann H E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR- 1278) [R]. Washington, DC: US Nuclear Regulatory Commission, 1983.

[3] Reason J, Human Error [M]. Cambridge University Press, New York, 1990.

[4] Hollnagel E. Cognitive Reliability and Error Analysis Method (CREAM) [M]. Elsevier Science Ltd, 1998.

[5] Wickens C D, Hollands J G. 工程心理学与人的作业[M]. 朱祖祥, 葛列众, 张智军, 等译. 上海: 华东师范大学出版社, 2003.

[6] Shorrock S T, Errors of Perception in Air Traffic Control [J]. Safety Science, 2007, 45(8): 890- 904.

[7] Shorrock S T, Errors of Memory in Air Traffic Control [J]. Safety Science, 2005, 43(8): 571- 588.

[8] Zhang J J, Patel V L, Johnson T R, et al. A Cognitive Taxonomy of Medical Errors [J]. Journal of Biomedical Informatics, 2004, 37(2): 193- 204.