第39卷第3期
2011年3月

同济大学学报(自然科学版)
JOURNAL OF TONGJI UNIVERSITY(NATURAL SCIENCE)

Vol.39 No.3
Mar. 2011

**文章编号**：0253-374X(2011)03-0427-07

DOI:10.3969/j.issn.0253-374x.2011.03.022

# 组合E-服务的活动链行为模式设计及验证

陈　波[1,2]，曾国荪[1]，李　莉[1]，鲍　宇[1]

(1.同济大学 计算机科学与技术系，上海 201804；2.广西工学院 计算机工程系，广西 柳州 545006)

**摘要**：提出一种新颖的活动链的行为规范概念，该概念的粒度介于活动和场景概念之间，并根据基于活动链的行为刻画需求，设计“链存在、链缺失、链前提和链因果”四个行为模式，并给出这些模式到标记迁移系统LTS的映射规则，精确刻画了行为模式的操作语义，通过定义组合E-服务满足活动链模式的内涵，给出可满足性验证的充要条件和判定算法，最后给出实例分析.

**关键词**：活动链；行为模式；组合E-服务；可满足性验证；标记迁移系统

**中图分类号**：TP 309　　**文献标识码**：A

## Design of Activity Chain Behavioral Modes for Composite E-Service and Verification

*CHEN Bo*[1,2], *ZENG Guosun*[1], *LI Li*[1], *BAO Yu*[1]

(1. Department of Computer Science and Technology, Tongji University, Shanghai 201804, China; 2. Department of Computer Engineering, Guangxi University of Technology, Liuzhou 545006, China)

**Abstract**: The paper presents a novel concept of behavior specifications based on activity chain in which granularity is between activity and scenario. Four behavioral modes, such as chain existence mode, chain absence mode, chain precondition mode and chain response mode, are designed to express usual behavioral requirements based on activity chain and encoded on labeled transition system (LTS) with exact operation semantics. Compliance of composite E-service against activity chain modes is fitly defined to check whether composite E-services based on LTS correspond with activity chain modes. Finally, the paper presents the sufficient, necessary condition and algorithm for checking.

**Key words**: activity chain; behavior mode; composite E-service; compliance verification; labeled transition system

组合E-服务通过互联网上标准的通信协议自动发现、调用网上现有的、独立的、无状态的原子服务，从而组合成新的、跨组织、跨平台的有状态的复杂服务，成为最有前途的分布式环境下的计算范式和电子商务应用开发方法.然而，服务的分布性使服务的互操作和集成面临许多挑战，具有不同隶属关系的服务合成的E-服务流程极可能不满足用户特定需求，服务流程未能遵循特定的行为规则.

本文通过讨论在组合E-服务执行场合中，用户对基于活动链的行为规范表达问题，探讨设计简洁明了的形式化表达方法，给出四个基于活动链的行为模式，通过这些活动链模式，可以快捷地表达组合E-服务基于活动链的时态关系，通过定义活动链模式到标记传递系统的映射规则，给出了活动链模式的操作语义，并给出判定组合E-服务是否满足这些规范的方法和算法.

## 1　相关工作

已有工作的重点是用各种形式化工具对组合服务的行为进行建模，如mealy自动机[1]、有限自动机[2]、Petri网[3]、LTS[4]以及进程代数类方法[5].验证的规范是消息收发活动的时态关系[1]、CTL公式表达的基于活动的计算树时态关系[2]、Petri网表达的设计规范[3]、CTL* 表达的时序关系和MSC表达的消息序列时序关系[4-6].

这些工作都没有对验证的行为规范进行更多的探索，而是采用两类通常的方法来表达行为规范：其一为LTL、CTL类时态逻辑规范；其二为消息序列图(MSC)、统一建模语言(UML)等类图式规范.前者刻

收稿日期：2009-10-17

基金项目：国家“八六三”高技术研究发展计划项目(2007AA01Z425，2009AA012201)；国家“九七三”重点基础研究发展计划项目(2007CB316502)；国家自然基金项目(90718015)；NSFC-微软亚洲研究院联合资助项目(60970155)；教育部高等学校博士学科点专项科研基金项目(20090072110035)；高效能服务器和存储技术国家重点实验室开放基金项目(2009HSSA06)

第一作者：陈　波(1963—)，男，博士生，主要研究方向为可信软件、模型检测.E-mail:cb31@sina.com.

画的基本单元是活动,描述的是基于活动的时态关系;后者刻画的对象是场景,描述的是基于场景的时态关系. Pistore[7]、Rouached[8]分别对服务的行为规范描述作了研究,这些方法本质上仍然属于基于活动(或事件)粒度的表达方法,而且更加复杂,不利于用户使用. 在组合 E-服务情形下,用户对组合 E-服务的行为需求往往会表现为多个子服务的组合行为规范,即由子服务活动组成的活动链之间的时态关系,这是一种粒度介于活动和场景的行为规范.

## 2 行为活动链和活动链模式

### 2.1 活动链

**定义 2.1** 一个 E-服务的活动可归纳定义如下:

$WS=\{ws_1,ws_2,\cdots,ws_k,ws_{orch}\}$为 E-服务实例名集合,其中 $ws_{orch}$ 是服务编制引擎.

$O_{ws}=\{o_{ws}\mid o_{ws}=$ op[? $m$] 或 op[! $m$]$\}$是服务 ws 端口上的操作集合,其中 op 是操作名,$m$ 是消息名,? $m$ 表示接受的消息,! $m$ 表示发送的消息.

$A_{ws}=\{a_{ws}\mid a_{ws}=$ receive[o]$ws_{orch}$ 或 reply[o]$ws_{orch}\}$为服务 ws 的基本活动集合,活动分为两类,分别对应于接收编制服务 $ws_{orch}$ 对操作 $o$ 的引用,回复编制服务 $ws_{orch}$ 对操作 $o$ 的要求.

$A_{orch}=\{a_{orch}\mid a_{orch}=$ receive[o]ws 或 reply[o]ws 或 invoke[$o_{ws}$]$\}$为服务 $ws_{orch}$ 的三类基本活动,其中的 invoke[$o_{ws}$]为引用服务 ws 的操作 $o$.

$O=\bigcup\{o_{ws}\mid ws\in WS\}$是组合 E-服务 WS 的操作集.

$Act=\bigcup\{a_{ws}\mid a_{ws}\in A_{ws},ws\in WS\}$称为组合 E-服务的活动集.

每个 E-服务的操作遵循 WSDL 的规范,有四种类型 notification, solicit, request-response, solicit-response,分别对应定义中 $o$[! $m$], $o$[? $m$], $o$[! $m$,? $m$], $o$[? $m$,! $m$], $m$ 表示执行操作 $o$ 时所接收或发送的消息,消息本身是 XML 类型. 由于后两种 two-way 类型操作可以由前两种 one-way 类型操作组合而成,实际中可以限制操作只有前两种 one-way 类型. 在省略消息情况下,操作可以表示为 $o$. 在不引起歧义的情况下,服务 ws 的活动 $a_{ws}$ 可简记为 $a$.

**定义 2.2** 组合 E-服务 WS 中的一个活动链 $C=<a_1,\cdots,a_k>$,$_i.\in Act$,1.$\leqslant$i$\leqslant$k,是组合 $E$-服务某次执行过程中顺序执行且紧密相连的有限个活动组成的元组.

特别地,如果一个活动链由组合 $E$-服务一次执行过程的所有活动依序组成,则称之为组合 $E$-服务的一个行为迹($trace$),记为 $\sigma$. 一个迹可能是有限迹,也可能是无穷迹.

### 2.2 活动链模式

**定义 2.3** $C=<a_1,\cdots,a_n>$是一个活动链,对组合 E-服务的一个行为迹 $\sigma=<\sigma_1,\cdots,\sigma_z,\cdots>$,$\sigma_i\in$Act,1$\leqslant i$. 如果存在 $\sigma$ 的一个子序列$(\sigma_{i1},\cdots,\sigma_{in})$,满足 $\sigma_{ij}=a_j$,1$\leqslant j\leqslant n$,称 $C$ 在迹 $\sigma$ 中出现,$C$ 和 $\sigma$ 满足链存在关系(Chain-Existence),记 C C-EX $\sigma$. 如果活动链 C 在组合 E-服务的任意迹 $\sigma$ 中出现,则称 C 在系统中满足链存在模式,记 C C-EX Globally. 这时活动链 C 称为是必须的(required).

特别地,当 $C$ 是单个活动情形 $C=<a>$时,$C$ 在 $\sigma$ 中出现就是 $a$ 在 $\sigma$ 中出现,称为 $a$ 与 $\sigma$ 满足存在关系,记为 $a$ C-EX $\sigma$,类似有 $a$ C-EX Globally.

**定义 2.4** $C=<a_1,\cdots,a_n>$是一个活动链,对组合 E-服务的一个行为迹 $\sigma=<\sigma_1,\cdots,\sigma_z,\cdots>$,如果对任意 $\sigma$ 的一个子序列 $\sigma_i=<\sigma_{i1},\cdots,\sigma_{in}>$,满足 $\sigma_i\neq C$ 时,称 $C$ 在迹 $\sigma$ 中不出现,$C$ 和 $\sigma$ 满足链缺失关系(Chain-Absence),记为 $C$ $C$-AB $\sigma$. 如果对组合 E-服务中任意的行为迹 $\sigma$,活动链 $C$ 在 $\sigma$ 中缺失,则称 $C$ 满足全局链缺失模式,记 $C$ $C$-AB Globally. 这时的活动链 C 称为是不可能的(unreachable).

如果 $C$ 在 $\sigma$ 中出现,则可能有多次出现,这样 $C$ $C$-EX $\sigma$ 成立,令 Occurset$(C,\sigma)=\{\sigma_i\mid\sigma_i$是 $\sigma$ 的子序列,$C=\sigma_i\}$是迹 $\sigma$ 中出现活动链 $C$ 的子序列集合,Occurset(Q,$\sigma$)上的次序关系$\prec$定义如下.

**定义 2.5** 对组合 E 服务的活动链 $C$ 和行为迹 $\sigma$,如果 Occurset$(C,\sigma)\neq\Theta$,$\sigma_i,\sigma_j\in$ Occurset$(C,\sigma)$,$\sigma_i=\sigma_0<\sigma_{ik},\sigma_{ik+1},\cdots,\sigma_{in}>$,$\sigma_j=\sigma_0<\sigma_{jk},\sigma_{jk+1},\cdots,\sigma_{jn}>$,$\sigma_0$ 是 $\sigma_i$和 $\sigma_j$的最长的公共部分,且 $ik<jk$,则称 $\sigma_i\prec\sigma_j$.

关系$\prec$定义了活动链 $C$ 在 $\sigma$ 中多次出现时的次序,由于它是一个良序关系,因而可以确定 Occurset$(C,\sigma)$的最小元素,即最早出现 $C$ 的 $\sigma$ 的子序列,记为 first(C,$\sigma$)$=(\sigma_{C1},\sigma_{C2},\cdots,\sigma_{Cn})$. 特别地,如果 $C$ 是单个活动 $a$ 时,first$(a,\sigma)=\sigma_{a1}$代表了 $\sigma$ 中第一次出现 $a$ 的活动.

**定义 2.6** 如果活动链 $C$ 和活动 $a$ 满足:对任意一个行为迹 $\sigma$,当 $C$ 满足 $C$ $C$-EX $\sigma$,first$(C,\sigma)=(\sigma_{C1},\sigma_{C2},\cdots,\sigma_{Cn})$时,则有活动 $a$ 满足 $a$ $C$-EX $\sigma$,first$(a,\sigma)=\sigma_{a1}$,且下标 $a_1<C_1$,则称活动链 $C$ 和活动 $a$

满足前提模式(precondition)，记为 $\alpha$ $C$-PR $C$.

前提模式表达了活动链 $C$ 的出现之前必定有活动 $\alpha$ 的出现.

**定义 2.7**　如果活动链 $C$ 和活动 $\alpha$ 满足：对任意一个行为迹 $\sigma$，当 $C$ 满足 $C$ $C$-EX $\sigma$，first$(C,\sigma)=(\sigma_{C1},\sigma_{C2},\cdots,\sigma_{Cn})$时，一定有 $\alpha$ 满足 $\alpha$ $C$-EX $\sigma$，first$(\alpha,\sigma)=\sigma_{a1}$，且 $C_n<a_1$，则称活动链 $C$ 和活动 $\alpha$ 满足因果模式(Response)，记为 $\alpha$ $C$-RE $C$.

因果模式表达了活动链 C 的出现一定导致活动 a 在其后出现.

### 2.3　例子

例：Flight 和 Hotel 是两个已有的 E-服务，分别提供旅游的航空机票购买和旅馆预定服务，旅行社 F_H 是他们的组合 E-服务，提供面向客户的集成服务. 采用编制方式实现服务组合，F_H 是编制引擎，它负责引用 Flight 和 Hotel 的操作，同时和客户交互，提供完整的服务流程，图 1 描述组合 E-服务行为交互的场景，F_H 接受客户的请求，并行调用服务 F 和 H，返回排序后的航班目录，按照客户的要求提供指定航空公司的航班和特定住宿方案的整体方案，并由客户确认；最后提供服务(机票和住宿订单). 用户对该组合 E-服务的行为提出了如下需求 R.

(1) 服务一定响应用户请求，启动特定航空公司的机票过滤功能.

(2) 机票过滤完成后不会启动价格排序.

(3) 机票过滤启动的前提是服务提供给用户住宿的方案.

(4) 用户提供 nack 答复后，就不可能得到最终服务.

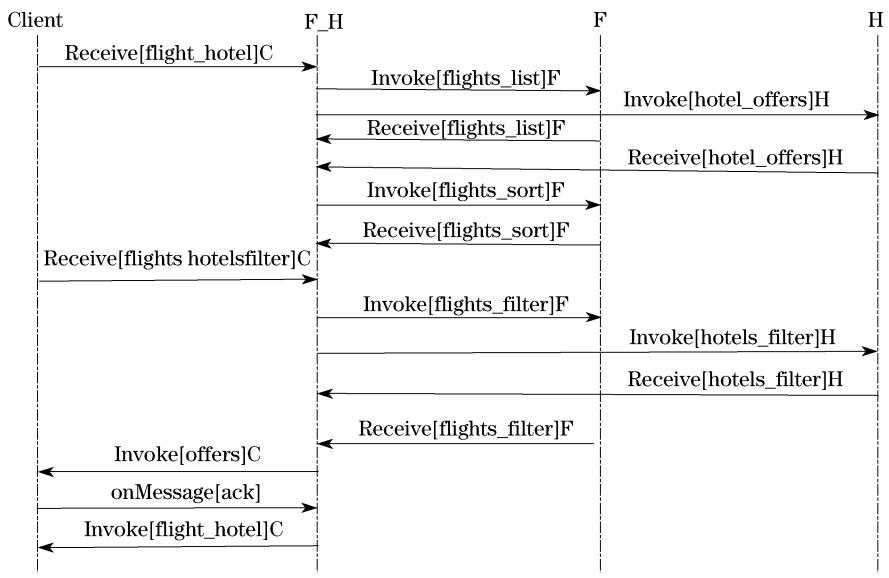



**图 1　组合 E-服务 F_H 的一个执行场景**

**Fig.1　An execution scenario of composite E-service F_H**

对 R 类的 4 个行为规范，它们表现为活动链之间的时态关系，其关系列在表 1 中. 如果活动链模式中仅有一个活动链，该活动链模式是一元的，如需求(1)和(2)，它们可看作基于活动的安全关系和活性关系在活动链情形的扩展. 如果活动链模式中有两个活动链，该活动链模式是二元的，如需求(3)和(4).

**表 1　例子的活动链模式**

**Tab.1　Activity chain modes in example**

| 需求 | 需求模式 | 活动链 |
|---|---|---|
| R(1) | $C_1$ $C$-EX Globally | $C_1=<$receive[flights_hotels_filter]$C$, invoke[flights_filter]$F>$ |
| R(2) | $C_1$ $C$-AB Globally | $C_1=<$receive[flights_filter]$F$, invoke[flights_sort]$F>$ |
| R(3) | $\alpha$ $C$-PR $C_1$ | $\alpha=$ receive[hotel_offers]$H$, $C_1=<$receive[flights_hotels_filter]$C$, invoke[flights_filter]$F>$ |
| R(4) | $\alpha$ $C$-RE $C_1$ | $\alpha=$ invoke[nack]$C$, $C_1=<$invoke[offers]$C$, onMessage[nack]$C>$ |

## 3　活动链行为模式的语义

用行为模式表达基于活动链的行为需求，其的好处是便于用户使用，但其确切的行为含义还需要给出准确解释. 一般用于行为验证的行为语义模型有自动

机模型、petri网的语义模型、标记迁移系统LTS的语义模型等,LTS广泛用于并发、分布式系统的行为进行建模,支持服务行为的组合,本文选取LTS作为活动链模式的操作语义模型.

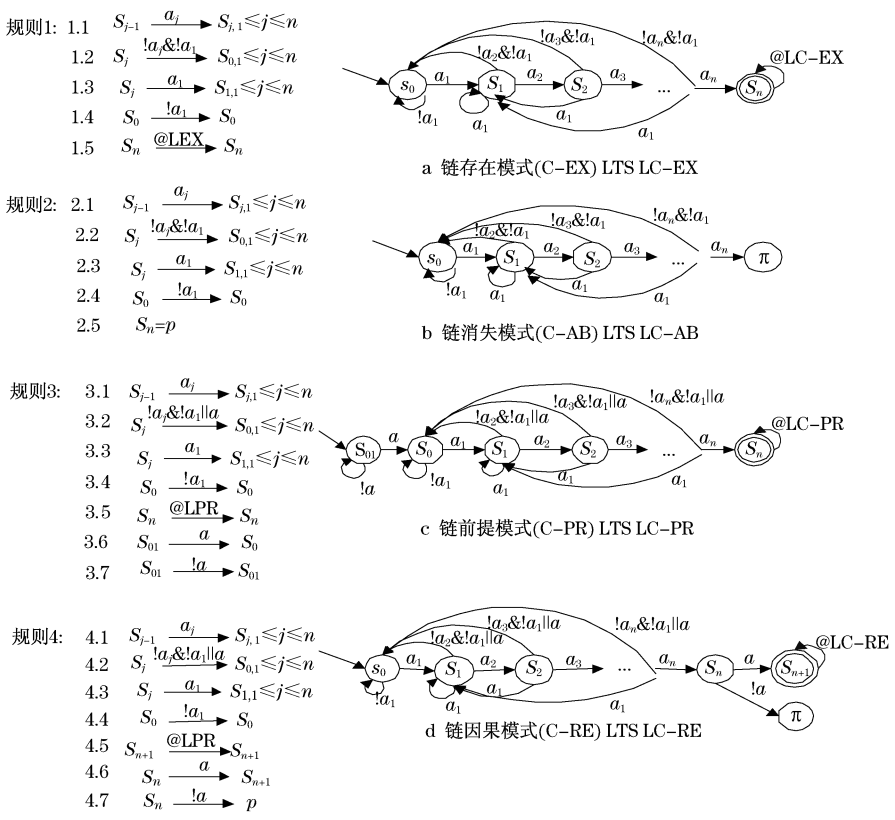
**定义 3.1**[9] 一个LTS是个四元组记为:LTS $L=(S,A,\rightarrow,s)$,$S$是有限状态集合,$A\subseteq$Act是活动的有限集合,也记为$A=_{\alpha}P$,$\rightarrow\subseteq S\times A_{\tau}\times S$是状态之间的变迁关系,$A_{\tau}=A\cup\{\tau\}$,$s$代表初始状态,$\tau$为服务内部不可见的活动.一个LTS P发生一个活动$a\in A_{\tau}$传递变成LTS $L'=(S,A,\rightarrow,s')$,记为$L\xrightarrow{a}L'$当且仅当$s\xrightarrow{a}s'$,这里$s\xrightarrow{a}s'$表示$(s,a,s')\in\rightarrow$,$a\in A_{\tau}$.

$\rho=s_0a_1s_1a_2s_2\cdots$表示$L$的一次执行,$\sigma=\langle a_1,a_2,\cdots\rangle$是该次执行的行为迹,$\|$表示两个LTS的并,它们的定义见文献[9].

**定义 3.2** 设$L=<S,A,\rightarrow,s_0>$,$A=_{\alpha}L$,是一个LTS,$s\in S$,$a\in{}_{\alpha}L\cup\{\tau\}$,$\mathrm{Post}(s,a)=\{s'\mid s\xrightarrow{a}s'\}$表示状态$s$在活动$a$的直接后继,$\mathrm{Post}(s)=\bigcup_{a\in{}_{\alpha}L\cup\{\tau\}}\mathrm{Post}(s,a)$表示$s$的直接后继.

一个状态$s$是$L$的终止状态,当且仅当$\mathrm{Post}(s)=\Theta$.如果$L$的一次执行在有限步后进入终止状态,即.$\rho=s_0a_1s_1\cdots s_n$,且$\mathrm{Post}(s_n)=\Theta$,则称该执行有限终止.

图2是活动链模式到LTS的映射规则.这些模式LTS作了扩展,增加了接收状态和接收边,或者增加了出错状态.




a 链存在模式(C-EX) LTS LC-EX

b 链消失模式(C-AB) LTS LC-AB

c 链前提模式(C-PR) LTS LC-PR

d 链因果模式(C-RE) LTS LC-RE

**图2 活动链模式的映射规则和LTS**

**Fig.2 Mapping rules of activity chain modes and LTS**

## 4 活动链模式的可满足性验证

正常情况下,一个LTS代表一个永不停息的反应式系统,它的执行是无限,当它进入终止状态时,该终止状态是该LTS的死锁状态.在本文中,一个LTS代表一个服务或一个活动链模式,这样的LTS可以无限执行,也可以是有限执行后正常结束,当一个LTS进入一个终止状态时,它可能进入一个死锁状态,也可能进入一个正常结束状态,称为接收态.活动链可满足性验证是在组合E-服务无死锁的情况下展开,因此,首先扩展LTS模型以排除死锁

情形.

### 4.1　LTS的扩展和死锁的排除

**定义 4.1**　(服务或模式LTS的扩展规则)

(1) 对一个LTS L(模式或服务),如果状态 $s$ 是其接收状态,则在其上添加自回边(接收边),标记@L(接收符),状态以双圆表示.图2a,2c的 $s_n$ 和2d中的 $s_{n+1}$ 都是模式LTS的接收状态.

(2) 将组合E-服务 $L_W = L_1 \| L_2 \| \cdots \| L_k$ 的子服务的接收活动符和待验证的模式LTS $L_M$ 的接收活动符 $@L_M$ 看作一致,即 $@L_1 = @L_2 = \cdots = @L_k = @L_W = @L_W$,按照并规则同步执行.

如果扩展后的组合E-服务 $L_W$ 进入接收状态 $s = (s_1, \cdots, s_k)$,则 $s_i$,$1 \leqslant i \leqslant k$,是 $L_i$ 的接收状态,按照并规则,其后 $L_W$ 执行无限活动符序列 $(@L)^\omega$,由此 $L_W$ 正常结束的执行也变成无限的执行序列,其后缀为 $s@L_W s@L_W \cdots$.如果扩展后的组合E-服务 $L_W$ 经过有限步后进入终止状态 $s = (s_1, \cdots, s_k)$,则 $s$ 为 $L_W$ 的死锁状态,其检测可采用深度优先算法(DFS)遍历生成 $L_W$ 对应的可达图,判断每个节点是否有后继来达到[9].

因此,给出在下面的验证中的前提:

**前提 1**　每个子服务 $L_i$,$1 \leqslant i \leqslant k$,都没有死锁.

**前提 2**　组合E-服务 $L_W$ 没有死锁.

**前提 3**　组合E-服务 $L_W$ 与待验证的行为模式LTS $L_M$ 的并 $L_W \| L_M$ 没有死锁状态.

### 4.2　活动链存在模式可满足性验证

验证过程需要活动符号的匹配.设 $L_M = \langle S_M, A_M, \rightarrow_M, s_{M0} \rangle$ 是图2中的一个行为模式LTS,$A_M = A_{M1} \cup A_{M2} \cup \{@L_M\}$ 或 $A_M = A_{M1} \cup A_{M2}$,$A_{M1} \subseteq$ Act,Act是组合服务正常的活动符,$A_{M2} = \{!\ a \mid a \in A_{M1}\}$,$@L$ 是定义4.1中的接收符.设 $a \in A_M$,$b \in$ Act,称 $a$ 匹配 $b$,记为 $a \sim b$,当且仅当 i) $a \in A_{M1} \wedge a = b$,ii) $a = !\ c \in A_{M2} \wedge b \neq c$.对接收符 $@L'$,$a \sim @L$,当且仅当 $a \in \{A_{M2} \cup \{@L_M\}\}$.

**定义 4.2**(链模式可满足性)　设 $L_W = L_1 \| L_2 \| \cdots \| L_k$ 是一个组合E-服务,$L_M$ 是一个链模式LTS,满足4.1节中的前提1、前提2、前提3.如果 $L_M \neq L_{C-AB}$,且对于 $L_W$ 的任意行为迹 $\sigma$,都有 $\sigma \downarrow_M$ 是 $L_M$ 的行为迹,则称组合E-服务 $L_W$ 满足链模式 $L_M$,记为 $L_W \models L_M$;如果 $L_M = L_{C-AB}$,对于 $L_W$ 的任意行为迹 $\sigma$,去掉4.1中扩展后带有的无限个 $@L_W$ 后缀,都有 $\sigma \downarrow_M$ 不是 $L_M$ 的行为迹,称组合 $E$-服务 $L_W$ 满足链缺失模式 $L_{C-AB}$,记为 $L_W \models L_{C-AB}$.其中 $\sigma \downarrow_M$ 表示将行为迹 $\sigma$ 投影到 $L_M$ 的活动符号集上.

**引理 4.1**　对给定的链存在模式 $L_{C\text{-}EX}$ 如图2a,$s_n$ 是其接收态,则在不考虑其接收活动符 $@L_{C\text{-}EX}$ 产生的无限活动链 $(@L_{C\text{-}EX})^\omega$ 的情况下,其正常结束执行所产生的行为迹必定是 $(!\ a_1)^* (a_1 \cdots a_{i1})^* (!\ a_1)^* (a_1 \cdots a_{i2})^* (!\ a_1)^* \cdots (a_1 \cdots a_{ik})^* (!\ a_1)^* a_1 a_2 \cdots a_n$ 形式.

**证明**　对一次正常结束的执行在到达状态 $s_n$ 前发生中断返回前面状态的次数 $k$ 进行数学归纳,可以得到结论.

**引理 4.2**　设 $\sigma$ 是 $L = L_1 \| L_2 \| \cdots \| L_m$ 的一条行为迹,则 $\sigma \downarrow_i$ 一定是 $L_i$ 的一条行为迹.

**证明**　设 $\sigma = \langle a_1 a_2 \cdots \rangle$,$\sigma \downarrow_i = \langle a_{i1} a_{i2} \cdots \rangle$,因此 $a_{ik} \in A_i$,$k = 1, \cdots$,所以,$\sigma \downarrow_i$ 是 $L_i$ 的活动符序列,而且 $\sigma$ 中在 $a_{i1}$ 之前的活动符 $a_1, a_2, \cdots a_{ik-1}$ 都不在 $A_i$ 中,所以,$a_{i1}$ 是 $L$ 的对应 $\sigma$ 的执行序列.$\rho$ 中第一个属于 $A_i$ 的活动符,由LTS并操作的定义,$a_{i1}$ 是 $L_i$ 从初始态 $s_{i0}$ 执行的活动,类似,由于 $\sigma$ 在 $a_{ii}$ 和 $a_{ij+1}$ 之间没有 $A_i$ 中的活动符,所以,$a_{ii}$ 和 $a_{ij+1}$ 是 $L_i$ 中紧密相连的活动,因而,$\sigma \downarrow_i$ 是 $L_i$ 的行为迹.

**定理 4.3**　给定一个组合E-服务 $L_W = \langle S_W, A_W, \rightarrow_W, s_{W0} \rangle$ 和链存在模式 $L_{C\text{-}EX} = \langle S_{C\text{-}EX}, A_{C\text{-}EX}, \rightarrow_{C\text{-}EX}, s_{C\text{-}EX0} \rangle$,$L = L_W \| L_{C\text{-}EX}$,则组合E-服务满足链存在模式C C-EX Globally的充要条件是:$L$ 中任意一个环路都可达且包含了 $L_{C\text{-}EX}$ 的标以接收符 $@L_{C\text{-}EX}$ 的接收边.

**证明**　(充分性),设 $\rho = (s_{W0}, s_{EX0}) a_1 (s_{W1}, s_{EX1}) a_1 \cdots$ 为 $L$ 的任意一条执行路径,$\sigma$ 是相对应于 $\rho$ 的行为迹.由于前提1、前提2、前提3的假设,可以得出 $\rho$ 必定是无穷序列,由于 $L$ 的状态是有限状态,所以 $\rho$ 中必定存在 $L$ 的环.由充分条件得标志 $@L_{C\text{-}EX}$ 中的接收边必定在 $\rho$ 中环出现.由 $\rho$ 得到的 $L$ 的行为迹 $\sigma$ 也一定存在接收活动 $@L_{C\text{-}EX}$ 无穷次,设 $\sigma \downarrow_{C\text{-}EX}$ 是 $\sigma$ 在 $A_{C\text{-}EX}$ 上的投影,由引理4.2得 $\sigma \downarrow_{C\text{-}EX}$ 是相对应 $\rho$ 的 $L_{C\text{-}EX}$ 的行为迹,于是活动符 $@L_{C\text{-}EX}$ 一定出现在 $\sigma \downarrow_{C\text{-}EX}$ 上.因此,$L_{C\text{-}EX}$ 的接收态 $s_n$ 一定是可达的.由引理4.1,$\sigma \downarrow_{C\text{-}EX}$ 一定是 $(!\ a_1)^* (a_1 a_2 \cdots a_{i2})^* (!\ a_1)^* \cdots (a_1 a_2 \cdots a_{ik})^* (!\ a_1)^* a_1 a_2 \cdots a_n$ 形式,因而,$\sigma$ 一定包含活动链 $< a_1 a_2 \cdots a_n >$.再由 $\rho$ 的任意性,得 $L$ 的行为满足链存在模式C C-EX Globally.

(必要性),假设必要性不成立,有一个 $L$ 的可达

环路没有包含标志@$L_{C\text{-}EX}$的接收边,则该可达路径 $\rho$ 从初始状态出发,最后在环上无穷循环,该环上状态不会是($s_W$,$s_n$),其中 $s_W$为$L_W$的状态,$s_n$为$L_{C\text{-}EX}$的接收态,否则,如果($s_W$,$s_n$)在环上,因为 $L_{C\text{-}EX}$的状态 $s_n$只有@$L_{C\text{-}EX}$这样的后继同步接收活动,而且在前提1、前提2、前提3情况下排除了死锁.因此,当到达($s_W$,$s_n$)状态,$L_{C\text{-}EX}$处于 $s_n$等待$L_W$的@$L_{C\text{-}EX}$活动,而环中没有该活动,于是,状态($s_W$,$s_n$)在环中经过后继活动 $a \in A_W \backslash A_{C\text{-}EX}$而到另一个状态($s'_W$,$s_n$),类似,可得 $L_W$的环,该环上活动都是与 $L_{C\text{-}EX}$无关的活动,在组合E-服务 $L_W$执行有限步后,沿该路径永远不会执行达到 $L_{C\text{-}EX}$接收态所需的同步活动 $a_n$,所以,$s_n$一定不可达,C C-EX Globally 不成立.与假设矛盾.

组合E-服务活动链存在模式可满足性判断的算法:

Checking_EX_seq(LTS $L_i$,activity chain $C$)

(1) 构造链存在模式 LTS $L_{C\text{-}EX}$.

(2) 按照定义4.1扩展 $L_{C\text{-}EX}$、$L_i$包含接收态,接收边.

(3) 求 LTS 并 $L = L_1 \| \cdots \| L_m \| L_{C\text{-}EX}$

(4) DFS 遍历 $L$,检测 $L$ 中的每一个环,如果没有环被检测到,转(6).

(5) 如果环中没有接收活动符@$L_{C\text{-}EX}$,则存在模式不满足,结束;若有返回(4).

(6) 若 L 遍历完,且每一个环均有活动符@$L_{C\text{-}EX}$,则组合E-服务满足链模式 $L_{C\text{-}EX}$,否则不满足该模式.

### 4.3 活动链缺失模式可满足性验证

链缺失模式相当于基于活动的安全性在活动链上的扩展,其含义为不允许活动链出现,如果在某次执行中活动链出现了,则判定该模式不满足.为验证组合E-服务是否满足链缺失模式,首先对模式 LTS $L_{C\text{-}AB}$作如下扩展.

**定义 4.3** 设一个 LTS $L = <S, A, \rightarrow, s_0>$,$\pi$ 表示错误状态,$\Pi = <\{\pi\}, A, \Theta, \pi>$表示陷入错误状态进程的 LTS.

一个进程陷入错误状态是指该进程不能再参加进一步的活动.引入错误状态后,LTS 的操作规则要稍作调整:

一个进程 $L = <S, A, \rightarrow, s_0>$,执行一个活动 $a$ 变成 $L'$,记为 $L \xrightarrow{a} L'$,其中 $L' = \begin{cases} <S, A, \rightarrow, s'_0 & \text{if } s_0 \neq \pi \\ \Pi & \text{if } s'_0 = \pi \end{cases}$.

**定义 4.4**(映像模式 LTS) 设一个特性 LTS $L = <S, A, \rightarrow, s_0>$,则 LTS $L' = <S \cup \{\pi\}, A, \rightarrow', s_0>$称为映像 LTS,其中$\rightarrow'$定义为:$\rightarrow \cup \{s \xrightarrow{a} \pi \mid s \in S, a \in A, \nexists s' \cdot s \xrightarrow{a} s'\}$

图2(c)就是链缺失模式的映像 LTS,记为 $L_{C\text{-}AB}$.对于组合E-服务的链缺失模式的可满足性验证,有如下结论.

**定理 4.3** 给定组合E-服务 $L_W = L_1 \| \cdots \| L_m$,链缺失模式的映像 LTS $L_{C\text{-}AB}$,$L = L_W \| L_{C\text{-}AB}$,组合E-服务 $L_W$满足链缺失模式的充分必要条件是 $L$ 的出错状态是不可达的.

证明思路类似文献[9],略.

类似,可容易得出组合E-服务活动链缺失模式的可满足性判断算法.

### 4.4 链前提模式和链因果模式的可满足性验证

链前提模式的 LTS $L_{C\text{-}PR}$和链存在模式 $L_{C\text{-}EX}$结构上相类似,它们的可满足性验证也相似.链因果模式的 LTS $L_{C\text{-}RE}$可看做链存在模式 $L_{C\text{-}EX}$与或链缺失模式 $L_{C\text{-}AB}$的组合,容易得下面结论.

**定理 4.4** 给定组合E-服务 $L_W = L_1 \| \cdots \| L_n$,给定链因果模式 $L_{C\text{-}RE}$,$L = L_W \| L_{C\text{-}RE}$,则组合E-服务满足链因果模式的充分必要条件是:$L$ 的出错状态是不可达的且 $L$ 的任一个环是可达的而且包含接收边.

## 5 实例分析和结束语

图3是 F_H 的 LTS 描述和活动链模式 LTS,其中的活动是 Client 对组合E-服务要求的活动,都出现在 $L_{F_H}$中,为简化起见用 $L_{F_H}$代替其和 $L_F$及 $L_H$的并.而可以看出:$L_{F_H} \| L_{C\text{-}EX}$一个执行路径包含环(13,2)$e_2$(15,2)$e^*$(13,2),其上的活动符和接收活动符 @$L$ 都不匹配,所以服务不满足链存在模式.事实上,该执行路径包含的活动链为$<c, d_1, \cdots>$,而给定的活动链$<c, c_1>$并没有出现.对链缺失模式 $L_{C\_AB}$,$L_{F_H} \| L_{C\text{-}AB}$中并没有出现出错状态,所以,组合E-服务满足缺失模式.由于篇幅有限,文中仅给出两个模式的结果.

提出的活动链模式的思想来源于 Dwyer[10] 和 Yu[11] 的属性模版工作,但他们描述的是基于活动的时态关系,本文描述的是基于活动链的时态关系.将来的工作侧重于可满足性的组合验证.

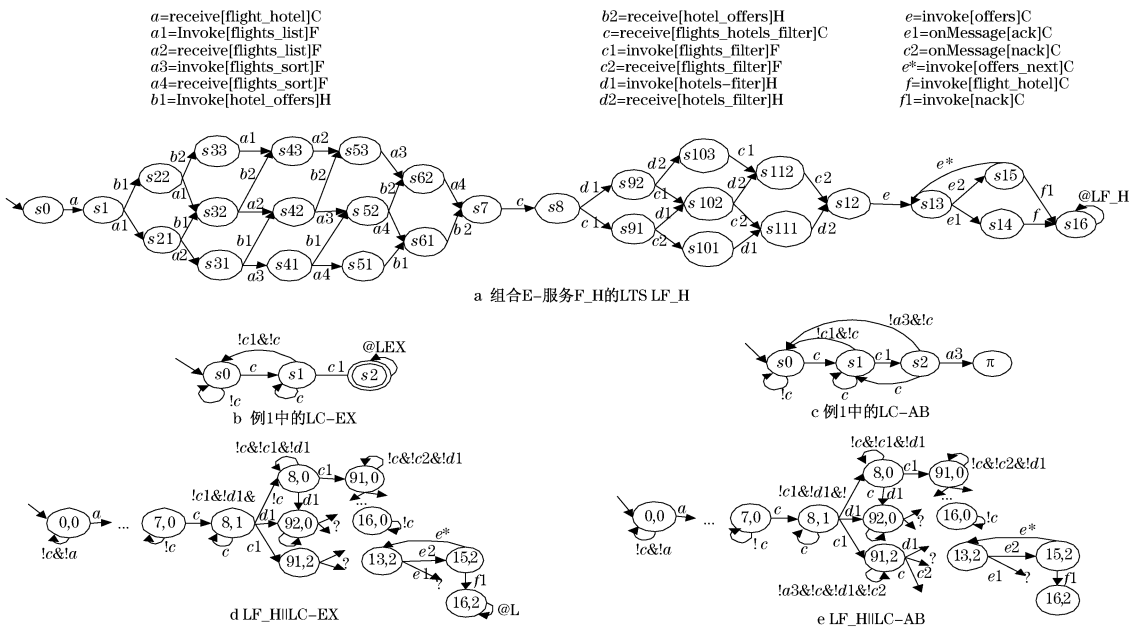



**图 3　组合 E-服务 F_H 和活动链模式 LTS 及它们的并**

**Fig.3　Composite E-service F_H, activity chain modes and their parallel**

## 参考文献:


[1] Fu X, Bultan T, Su J. Analysis of interacting BPEL Web services[C]// Proceedings of the 13th International Conference on World Wide Web, New York: ACM, 2004: 624 - 630.

[2] Mongiello M, Castelluccia D. Modeling and verification of BPEL business processes[C] // The 4th Workshop on Model-Based Development of Computer-Based Systems and the 3rd International Workshop on Model-Based Methodologies for Pervasive and Embedded Software. Berlin: IEEE Computer Society, 2006: 144 - 148.

[3] Aalst V D. Conformance checking of service behavior[J]. ACM Transactions on Internet Technology, 2008, 8(3): 1.

[4] Foster H, Uchitel S, Magee J, et al. Model-based verification of Web service compositions[C] // IEEE the 18th International Conference on Automated Software Engineering, Montreal: IEEE Computer Society, 2003: 152 - 163.

[5] Salaun G, Bordeaux L, Schaerf M. Describing and reasoning on Web services using process algebra[C] // Proceedings of the 2nd International Conference on Web Services, San Diego: IEEE Computer Society, 2004: 43 - 50.

[6] 胡军,于笑丰,张岩,等. 基于场景规约的构件式系统设计分析与验证[J]. 计算学报, 2006, 29(4): 513.
HU Jun, YU Xiaofeng, ZHANG Yan, et al. Checking component-based designs for scenario-based specifications[J]. Chinese Journal of Computer, 2006, 29(4): 513.

[7] Pistore M, Roveri M, Busetta P. Requirements-driven verification of Web services[J]. Electronic Notes in Theoretical Computer Science, 2004, 105(3): 95.

[8] Rouached M, Godart C. Requirements-driven verification of WSBPEL processes[C] // IEEE International Conference on Web Services, Salt Lake City: IEEE Computer Society, 2007: 354 - 363.

[9] Giannakopoulou D. Model checking for concurrent software architectures[D]. London: Imperial College of Science, Technology and Medicine University of London, 1999.

[10] Dwyer M B, Avrunin G S, Corbett J C. Patterns in property specifications for finite-state verification[C] // Proceedings of the 1999 International Conference on Software Engineering, Los Angeles: ACM, 1999: 411 - 420.

[11] Yu J, Manh T P, Han J, et al. Pattern based property specification and verification for service composition[J]. Lecture Notes in Computer Science, 2006, 4255: 156.