

文章编号:1001-9081(2010)01-0266-04

## 基于事件的局部行为模型的合并

郭正虎, 陈中育, 张纪昌

(浙江师范大学 数理与信息工程学院, 浙江 金华 321004)

(guozhenghu@foxmail.com)

**摘要:**采用模态迁移系统描述系统行为, 针对局部行为模型中存在的的行为, 提出一种基于事件的局部行为模型合并方法。该方法首先定义局部行为模型之间的精化关系, 利用精化关系产生合并规则, 运用合并规则产生行为模型的极小共同精化模型或最小共同精化模型, 从而消除局部行为模型中存在的的行为。最后通过一个示例对该方法的有效性作出说明。

**关键词:**模态迁移系统; 不确定行为; 精化; 合并规则

**中图分类号:** TP311.5 **文献标志码:** A

## Event-based merging of partial behavior models

GUO Zheng-hu, CHEN Zhong-yu, ZHANG Ji-chang

(College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua Zhejiang 321004, China)

**Abstract:** System behaviors are described by modal transition systems. In allusion to unknown behaviors in partial behavior models, the authors formally defined model merging method based on event and refinement. Merging rules were defined based on refinement relation; with merging rules consistent models were merged for ruling out unknown behavior and resulted in a minimal common refinement or least common refinement. Finally, a case study illustrates the effectiveness of the method.

**Key words:** Modal Transition Systems (MTS); unknown behavior; refinement; merging rule

### 0 引言

场景是一种分析与验证需求的有效工具, 因此基于场景的分析与设计受到广泛关注<sup>[1]</sup>。一个系统需求由多个局部场景构成, 这些场景是由不同的相关人员根据自己所关注的业务功能并结合自己的知识给出, 每个场景描述系统中不同用户的需求, 多个场景所描述的用户需求可能存在某些业务需求的重叠<sup>[2]</sup>, 如何把这些局部场景中抽取的行为模型合并成一个完整的系统行为模型值得研究。文献[1]使用标号迁移系统(Label Transition System, LTS)从基于场景的规约中合成行为模型, LTS模型实现了系统行为建模和推理的形式化, 为各种自动分析技术提供理论基础。但LTS模型所描述的行为必须是系统中的确定行为, 而在系统逐步详细描述过程中局部场景可能含有不确定行为, LTS模型的不确定性假设限制了在软件开发过程中对含有不确定行为的建模和分析, 因此本文希望对系统行为进行建模和分析过程中能够区分确定行为和不确定行为, 并消除不可能行为。目前支持不确定行为的形式化方法主要有混合迁移系统<sup>[2]</sup>、多值Kripke结构<sup>[3]</sup>和模态迁移系统<sup>[4]</sup>等。

行为模型的并行复合主要针对不同构件系统的行为组合, 而行为模型的合并是从同一构件系统的两个局部行为模型中获得一个精化的模型。本文采用模态迁移系统对系统行为进行建模, 在精化关系的基础之上结合隐藏操作, 给出共同精化模型, 并根据精化程度定义了极小共同精化和最小共同精化。本文在分析现有合并算法的基础上, 指出现有合并算法的局限性, 即总是假设模型之间同一事件的源状态和目标

状态是一致的, 针对此局限性, 文中提出了源状态一致标号集和目标一致标号集, 在基于事件合并的同时结合事件的源状态和目标状态给出了新的合并规则。运用合并规则可以产生极小共同精化模型或最小共同精化模型。在对合并规则进行解释说明之后又通过水泵控制系统对合并规则的有效性进行说明。

### 1 背景知识

本章将介绍模态迁移系统及其精化等概念, 其中与行为模型合并相关的一些概念主要参考文献[2, 5]。

标号迁移系统(LTS)用于分布式系统行为的形式化描述, 成为分布式系统规约、实现和测试研究的有效工具。LTS是一个状态迁移的系统, 其中迁移被标上了行为。LTS的行为集称为通信字母表, 构成模型系统与环境的相互作用。此外, LTS可以含有不被环境观察的内部行为 $\tau$ 。

**定义1** 标号迁移系统LTS。假设States是一个状态集合, Act是一个可观测行为标号集合,  $Act_\tau = Act \cup \{\tau\}$ 。一个标号迁移系统是一个四元组  $P = (S, L, \Delta, s_0)$ , 其中:  $S \subseteq States$  是一个有限状态集合;  $L \subseteq Act_\tau$  是一个有限的标号集合;  $\Delta \subseteq (S \times L \times S)$  是两个状态之间的转换关系;  $s_0 \in S$  是初始状态。

文中使用  $\alpha P = L \setminus \{\tau\}$  来定义P的通信字母表。

标号迁移系统虽然可以描述系统行为, 但是不包含不确定的行为。模态迁移系统(Model Transition Systems, MTS)能明确描述出系统中的未知行为模型, 模态迁移系统是标号迁移系统的扩展, 添加了系统中不确定的迁移关系集。

**定义2** 模态迁移系统MTS。一个模态迁移系统是五元

收稿日期: 2009-07-19; 修回日期: 2009-08-27。

**作者简介:** 郭正虎(1982-), 男, 河南濮阳人, 硕士研究生, 主要研究方向: 软件工程、形式化方法; 陈中育(1964-), 男, 浙江浦江人, 教授, 主要研究方向: 软件工程、形式化方法; 张纪昌(1984-), 男, 河南开封人, 硕士研究生, 主要研究方向: 软件工程。

组  $M = (S, L, \Delta', \Delta^p, s_0)$ 。其中:  $\Delta' \subseteq \Delta^p$ ;  $(S, L, \Delta', s_0)$  表示系统必然迁移的 LTS;  $(S, L, \Delta^p, s_0)$  表示系统的允许迁移(但不一定必然)的 LTS。

文中使用  $\alpha M = L \setminus \{\tau\}$  来定义  $M$  的通信字母表。

$\Delta'$  表示必然迁移关系集,  $\Delta^p$  表示允许迁移关系集, 本文使用  $\Delta^p - \Delta'$  表示可能迁移关系集。在行为模型图中可能性迁移标号用问号来标记, 以便区分必然迁移(在  $\Delta'$  中), LTS 是只有必然迁移的特殊 MTS。文中使用  $\Delta^-(e)$  表示必然迁移  $\Delta'$  中事件  $e$  的源状态,  $\Delta^+(e)$  表示必然迁移  $\Delta'$  中的目标状态, 同样使用  $\Delta^p(e)$  表示允许迁移  $\Delta^p$  中事件  $e$  的源状态,  $\Delta^p(e)$  表示允许迁移  $\Delta^p$  中事件  $e$  的目标状态。

给定一个 MTS,  $M = (S, L, \Delta', \Delta^p, s_0)$ , 使用  $M_s \xrightarrow{l} M_t$  表示在模型  $M$  中状态  $s$  可以通过标号  $l$  必然迁移到状态  $t$ , 也就是  $(s, l, t) \in \Delta'$ 。同样  $M_s \xrightarrow{l} M_t$  表示表示状态  $s$  可以通过标号  $l$  可能迁移到状态  $t$ , 也就是  $(s, l, t) \in \Delta^p - \Delta'$ 。

MTS 精化是从不确定的行为描述中获取一个确定的行为描述, 可以理解为是两个不确定行为模型的更确定的关系。直观上说, MTS 的精化是把行为模型中的可能迁移转化为必然迁移, 或者排除不必要的可能迁移。如果 MTS  $N$  保留了  $M$  的所有必然和允许迁移, 或者说  $N$  能模拟  $M$  的必然迁移,  $M$  能模拟  $N$  的可能迁移, 就说  $N$  是  $M$  的精化。

**定义 3 精化。** 假设  $\mathcal{P}$  是所有 MTS 的论域。  $N$  是  $M$  的一个精化, 记为  $M \leq N$ , 其中  $\alpha N = \alpha M$ , 且  $(M, N)$  包含的精化关系  $R \subseteq \mathcal{P} \times \mathcal{P}$ , 并且对于任意  $l \in Act$ , 满足如下规则:

- 1)  $(M \xrightarrow{l} M') \Rightarrow (\exists N' \cdot N \xrightarrow{l} N' \wedge (M', N') \in R)$
- 2)  $(N \xrightarrow{l} N') \Rightarrow (\exists M' \cdot M \xrightarrow{l} M' \wedge (M', N') \in R)$

注意: 条件 2) 保证如果  $N$  有一个必然迁移,  $M$  会有一个可能迁移或者必然迁移, 但是如果  $N$  有一个可能迁移, 那么  $M$  一定是一个可能迁移; 否则就与条件 1) 相违背。

图 1 中模型  $C$  是模型  $A$  的精化 ( $A \leq C$ ), 模型  $C$  把  $A$  中的可能迁移  $(1, b?, 2)$  和  $(1, c?, 3)$  都精化为必然迁移。当然模型  $C_1$  和  $C_2$  也是  $A$  的精化, 只不过在精化中选择了不同的可能迁移标号进行精化。

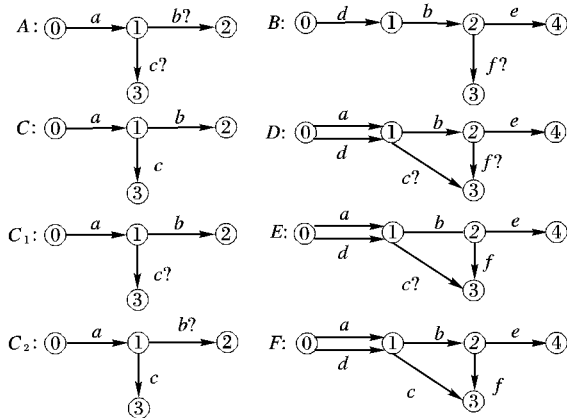


图1 MTS 模型

尽管精化可以获取更加详细的模型描述, 但是要求有相同的通信字母表。实际上模型的详细描述扩大了系统模型的通信字母表, 来描述先前没有考虑到的系统行为。为了获取模型细化的这一特性引入隐藏概念。

**定义 4 隐藏。** 假设  $M = (S, L, \Delta', \Delta^p, s_0)$  是一个 MTS,

$X \subseteq Act$  是一组可观察的动作, 隐藏动作  $X$  的  $M$  是  $(S, L \setminus X, \Delta', \Delta^p, s_0)$ , 表示成  $M \setminus X$ , 其中  $\Delta'$  和  $\Delta^p$  是满足隐藏操作规则的最小关系。使用  $M @ \alpha X$  来定义  $M \setminus (Act \setminus X)$ 。

$$\frac{M \xrightarrow{e} M'}{(M \setminus X) \xrightarrow{e} (M' \setminus X)} \quad e \notin X$$

$$\frac{M \xrightarrow{e} M'}{(M \setminus X) \xrightarrow{e} (M' \setminus X)} \quad e \in X$$

直观上看, 通过合并从同一系统的两个不确定描述中获取更多信息, 在这种情况下精化概念是在两个不确定行为模型中获得更确定的关系。因此, 合并同一个系统的两个模型就是找到一个共有(共同)精化, 也就是找到一个比这两个模型都更完整的模型。

**定义 5 共同精化 CR。** 如果 MTS 中  $P$  满足  $\alpha P \supseteq \alpha M \cup \alpha N$ ,  $M \leq P @ \alpha M$  和  $N \leq P @ \alpha N$ , 那么  $P$  就是 MTS 的  $M$  和  $N$  的共同精化。

图 1 中模型  $D, E, F$  都是  $A$  和  $B$  的共同精化,  $E$  和  $F$  也是  $D$  的一个精化。  $F$  是其他共有精化的精化, 称  $D$  是极小共同精化。

**定义 6 极小共同精化 LCR。** 假设模态迁移系统  $P$  是  $M$  和  $N$  的一个共同精化, 且  $\alpha P = \alpha M \cup \alpha N$ , 如果对于  $M$  和  $N$  的任一共同精化  $Q$  都满足  $P \leq Q @ \alpha P$ , 则称  $P$  是  $M$  和  $N$  的极小共同精化。

由定义中可以看出极小共同精化是独一无二的, 使用  $LCR_{M,N}$  来表示  $M$  和  $N$  的极小共同精化。  $M$  和  $N$  的共同精化存在并不能保证  $LCR_{M,N}$  的存在, 为此提出了最小共同精化的概念。

**定义 7 最小共同精化 MCR。** 如果模态迁移系统  $P$  是  $M$  和  $N$  的一个最小共同精化, 且  $\alpha P = \alpha M \cup \alpha N$ , 那么一定不存在另一个  $M$  和  $N$  共同精化  $Q \neq P$  使得  $Q @ \alpha P \leq P$ 。

由定义可以看出最小共同精化并不满足唯一性, 文中使用  $MCR(M, N)$  来表示  $M$  和  $N$  的最小共同精化集。  $M$  和  $N$  的  $LCR_{M,N}$  是它们一个 MCR, 如果  $M$  和  $N$  的 MCR 是唯一的, 此 MCR 也是  $LCR_{M,N}$ 。

行为模型的合并实质就是求两个行为原有模型的 MCR 或者 LCR。

## 2 合并算法

尽管合并的算法已经有人提出, 但是一个完整且普遍适用的算法还没有提出, 本章首先分析两种不同的合并算法, 最后提出一种新的算法, 该算法可以对状态不一致的行为模型进行合并。

### 2.1 现有算法的局限性

首先介绍文献[6]中提出的模型之间的连接操作。

**定义 8 连接 Conjunction。** MTS 中  $M$  和  $N$  的连接定义为  $M \wedge N = (S_M \times S_N, L, \Delta'_{M \wedge N}, \Delta^p_{M \wedge N}, (m_0, n_0))$ , 记为  $CJ_{M,N}$ , 其中  $\Delta'_{M \wedge N}, \Delta^p_{M \wedge N}$  是满足下列规则的最小关系:

$$RP: \frac{M \xrightarrow{l} M', N \xrightarrow{l} N'}{(M, N) \xrightarrow{l} (M', N')}$$

$$PR: \frac{M \xrightarrow{l} M', N \xrightarrow{l} N'}{(M, N) \xrightarrow{l} (M', N')}$$

$$PP: \frac{M \xrightarrow{l} M', N \xrightarrow{l} N'}{(M, N) \xrightarrow{l} (M', N')}$$

连接的局限性就是有时 LCR 存在,但是并没有给出结果,实际上在这种情况下,这个运算就没有一个共同精化。

为了解决连接运算带来的问题,文献[4]中提出了合并运算,文献[5]又对这种算法进行了改进。并通过  $+_u$  产生所有最小共同精化的一个上界,通过  $+_l$  运算产生所有最小共同精化的一个下界,当条件充足时  $+_l$  产生的就是极小共同精化。

无论是文献[6]的连接运算还是文献[4,5]的合并都是假定模型的状态一致。也就是说,同一个事件  $e$  在两个模型中源状态和目标状态总是假定是一致的,这种合并只是基于事件的合并。但是在实际中这种假设受到很大限制,因此本文提出了针对状态不一致的行为模型提出了新合并算法。

## 2.2 新的合并算法

由于新算法考虑到标号的源状态和目标状态是否一致,为此给出源状态一致标号集和目标状态一致标号集两个定义,还给出了 MTS 一致性定义,因为只有满足一致性的 MTS 才能进行合并。

**定义9** 源状态一致标号集。对于给定的 MTS 中  $M$  和  $N$ ,  $M$  和  $N$  的源状态一致标号集  $\zeta_{M,N}^{src}$  满足以下条件,

- 1)  $\forall e \in (\alpha M \cap \alpha N)$ , 如果存在  $\Delta_M^{-\gamma}(e) = \Delta_N^{-\gamma}(e)$ ,  $\gamma \in \{r, m, p\}$ , 那么  $e \in \zeta_{M,N}^{src}$ ;
- 2)  $e \in \zeta_{M,N}^{src}$ , 一定满足  $\Delta_M^{-\gamma}(e) = \Delta_N^{-\gamma}(e)$ ,  $\gamma \in \{r, m, p\}$ 。

**定义10** 目标状态一致标号集。对于给定的 MTS 中  $M$  和  $N$ ,  $M$  和  $N$  的目标状态一致标号集  $\zeta_{M,N}^{trg}$  满足以下条件,

- 1)  $\forall e \in (\alpha M \cap \alpha N)$ , 如果存在  $\Delta_M^{\gamma}(e) = \Delta_N^{\gamma}(e)$ ,  $\gamma \in \{r, m, p\}$ , 那么  $e \in \zeta_{M,N}^{trg}$ ;
- 2)  $\forall e \in \zeta_{M,N}^{trg}$ , 一定满足  $\Delta_M^{\gamma}(e) = \Delta_N^{\gamma}(e)$ ,  $\gamma \in \{r, m, p\}$ 。

**定义11** 一致性。给定 MTS  $M = (S_M, L_M, \Delta_M^r, \Delta_M^p, s_{0M})$  和  $N = (S_N, L_N, \Delta_N^r, \Delta_N^p, s_{0N})$ ,  $\forall e \in \alpha M \cap \alpha N$  如果  $\Delta_M^{-r}(e) = \Delta_N^{-r}(e)$ , 那么一定有  $\Delta_M^r(e) = \Delta_N^r(e)$ , 就说  $M$  和  $N$  满足一致性。

本文中所讨论的行为模型都要满足一致性。因为我们认为从相同的源状态经过相同的标号  $e$  应该迁移到达相同的目标状态。

**定义12** 迁移不确定状态。假设  $M = (S, L, \Delta^r, \Delta^p, s_0)$  是 MTS, 对于状态  $s$  如果  $M$  中存在状态  $q$  和  $r$ , 使得  $M_s \xrightarrow{e} M_q$  和  $M_s \xrightarrow{e} M_r$  成立且  $M_q \neq M_r$ , 就说  $M_s$  在  $e$  上的迁移是不确定的, 状态  $s$  是迁移不确定的状态。

MTS 之间的一致性保证两个行为模型中的两个必要迁移  $e$  迁移到确定的同一状态, 而对于每一个行为模型同样要确保不包含迁移不确定的状态。

下面介绍  $+_{cr}$  运算,  $M +_{cr} N$  的结果是  $M$  和  $N$  的一个极小共同精化。

**定义13**  $+_{cr}$  运算。假设  $M$  和  $N$  是 MTS, 其中  $M = (S_M, L_M, \Delta_M^r, \Delta_M^p, s_{0M})$  和  $N = (S_N, L_N, \Delta_N^r, \Delta_N^p, s_{0N})$ ,  $M +_{cr} N$  是 MTS  $M = (S_M \times S_N, L_M \cup L_N, \Delta^r, \Delta^p, (s_{0M}, s_{0N}))$ ,  $\Delta^r$  和  $\Delta^p$  是满足  $+_{cr}$  运算规则的最小关系。

$$RD: \frac{M \xrightarrow{e} M'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N}, e \notin \alpha N$$

$$DR: \frac{N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \notin \alpha M$$

$$MD: \frac{M \xrightarrow{e} M'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N}, e \notin \alpha N$$

$$DM: \frac{N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \notin \alpha M$$

$$RM_{EE}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \in \zeta_{M,N}^{trg}$$

$$RM_{ED}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N, M +_{cr} N \not\xrightarrow{e} M +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \notin \zeta_{M,N}^{trg}$$

$$MR_{ED}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \not\xrightarrow{e} M' +_{cr} N, M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \notin \zeta_{M,N}^{trg}$$

$$RR_{EE}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \in \zeta_{M,N}^{trg}$$

$$RR_{DB}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N, M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}$$

$$MM_{EE}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \in \zeta_{M,N}^{trg}$$

$$MM_{ED}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N \text{ 或 } M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}, e \notin \zeta_{M,N}^{trg}$$

$$MM_{DB}: \frac{M \xrightarrow{e} M', N \xrightarrow{e} N'}{M +_{cr} N \xrightarrow{e} M' +_{cr} N, M +_{cr} N \xrightarrow{e} M +_{cr} N'}, e \neq \tau \text{ 且 } e \in \zeta_{M,N}^{src}$$

下面解释上述规则, 直观上说行为模型合并就是行为模型的组合, 就是合并后的模型中包含两个模型迁移, 但是不同的是合并过程可以对行为模型中的可能迁移用其他行为模型的必要迁移替换或者在合并过程中删除一些可能迁移。例如当行为模型  $M$  在  $e$  上是可能迁移, 而模型  $N$  在  $e$  上是必要迁移, 如果  $e \in \zeta_{M,N}^{src}, e \in \zeta_{M,N}^{trg}$ , 根据合并规则  $RM_{EE}$  和  $MR_{EE}$ , 那么  $M +_{cr} N$  中是必要迁移。以图1中的行为模型  $A$  中必要迁移  $b$ ? 和行为模型  $B$  中的可能迁移  $b$ , 在  $A$  和  $B$  的共同精化模型  $D$  中是必要迁移。如果  $e \in \zeta_{M,N}^{src}, e \notin \zeta_{M,N}^{trg}$ , 又根据 MTS 满足一致性, 我们可知必有一个标号为可能迁移, 在合并中我们可以将其可能迁移删除只保留必然迁移。如果两个模型中都是可能迁移, 那么在合并过程中可以让操作人员进行选择, 也就是合并规则中的  $MM_{ED}$  规则。

$$\begin{array}{l}
 MD \xrightarrow{M \xrightarrow{e} M'} M +_{cr} N \xrightarrow{e} M' +_{cr} N \quad e \notin \alpha N \\
 DM \xrightarrow{N \xrightarrow{e} N'} M +_{cr} N \xrightarrow{e} M +_{cr} N' \quad e \notin \alpha M
 \end{array}$$

如果MTS中的 $M$ 和 $N$ 中都不含有迁移不确定状态,按照隐藏操作规则所产生的共同精化就是极小共同精化。如果我们改变 $MD$ 和 $DM$ 规则,得到的 $M$ 和 $N$ 的共同精化就是最小共同精化。图1中的行为模型 $D$ 是 $A$ 和 $B$ 的共同精化同时也是 $A$ 和 $B$ 的极小共同精化, $F$ 是模型 $A$ 和 $B$ 的最小共同精化。

### 2.3 实例

下面用一个水泵控制器<sup>[7]</sup>的实例来进一步说明合并规则,该控制器要求在高水位时,开启泵(switchOn),在低水位时关闭泵(switchOff),但是如果有甲醛出现(methAppears)必须关闭泵,也就是说有甲醛出现时不管水位是不是高水位,泵必须关闭。模型 $M$ 是从有甲醛出现的场景中抽取的泵关闭模型,模型 $N$ 是从没有甲醛出现的场景中抽取一个泵开启行

为模型。要对局部的不确定行为模型 $M$ 和 $N$ 进行合并,合并成一个完整的行为模型。用 $M = (S_M, L_M, \Delta_M^r, \Delta_M^p, s_{0M})$ 来表示图2中模型 $M$ ,用 $N = (S_N, L_N, \Delta_N^r, \Delta_N^p, s_{0N})$ 表示模型 $N$ 。

因为 $(0, \text{methAppears}, 1) \in \Delta_M^r$ ,  $(0, \text{methAppears?}, 1) \in \Delta_N^p - \Delta_N^r$ 。因此根据 $+_{cr}$ 合并规则 $RM_{EE}$ ,在共同精化模型中事件methAppears从状态0到状态1的迁移是必然迁移。同样的道理,  $(3, \text{switchOn}, 4)$ 、 $(4, \text{lowWater}, 5)$ 、 $(5, \text{switchOn}, 0)$ 和 $(4, \text{switchOn}, 6)$ 在共同精化模型中都是必然迁移。

对于事件methLeaves在 $M$ 中的变迁是 $(2, \text{methLeaves}, 3) \in \Delta_M^r$ ,而在 $N$ 中是 $(1, \text{methLeaves?}, 0) \in \Delta_N^p - \Delta_N^r$ 。此事件的源状态和目标状态都不相同,因此在共同精化行为模型中这两个模型不能进行合并,应该保留这两个迁移。

根据 $+_{cr}$ 合并规则得到 $M$ 和 $N$ 的极小共同精化 $P$ 。如果用MCR的 $MD$ 和 $DM$ 规则替换 $+_{cr}$ 中的 $MD$ 和 $DM$ 规则,也就是把 $N$ 中 $(1, \text{methLeaves?}, 0)$ 精化为 $(1, \text{methLeaves}, 0)$ 得到 $M$ 和 $N$ 的最小共同精化 $Q$ 。

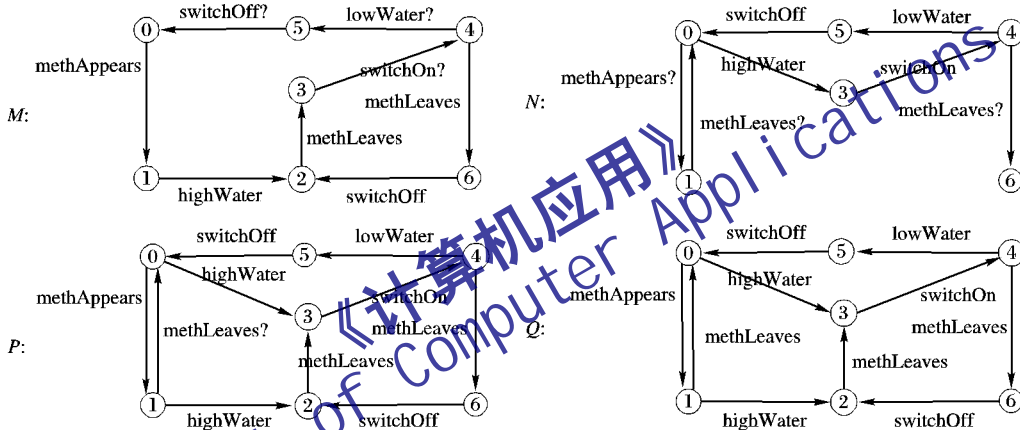


图2 泵关闭和开启模型

### 3 结语

文中采用模态迁移系统描述系统行为模型,通过对行为模型精化关系的分析提出了精化模型,使用隐藏操作解决了精化定义中要求有相同通信字母表的问题,并在此基础上给出两个行为模型的共同精化模型,根据共同精化模型的精化程度定义出极小共同精化模型和最小共同精化模型。针对现有合并算法的局限性,给出了源状态一致标号集和目标状态一致标号集来解决合并过程中总是假定事件的源状态和目标状态一致的问题,并结合精化关系给出了新的合并规则。使用行为模型的一致性和迁移不确定状态规定被合并行为模型要满足的条件,行为模型的一致性确保被合并的两个模型之间不存在互相矛盾的迁移关系,行为模型不含有迁移不确定状态保证了行为模型的每个状态通过同一事件迁移到唯一状态。本文主要解决了局部行为模型的合并问题,对于能够进行合并的MTS模型只提到要满足一致性和不能含有迁移不确定状态,接下来我们将进一步研究局部行为模型能够进行合并要满足的条件,并希望给出MTS模型一致性检验的方法。

#### 参考文献:

[1] UCHITEL S, KRAMER J, MAGEE J. Synthesis of behavioural

models from scenarios[J]. IEEE Transactions on Software Engineering, 2003, 29(2): 99 - 115.

[2] DAMS D. Abstract interpretation and partition refinement for model checking[D]. Eindhoven, Netherlands: Eindhoven University of Technology, 1996.

[3] CHECHIK M, DEVEREUX B, EASTERBROOK S, et al. Multi-valued symbolic model-checking[J]. ACM Transactions on Software Engineering and Methodology, 2003, 12(4): 1 - 38.

[4] BRUNET G. A characterization of merging partial behavioural models[EB/OL]. [2009 - 04 - 15]. <http://www.cs.toronto.edu/~chechik/pubs/GregBrunetMSThesis.pdf>.

[5] UCHITEL S, CHECHIK M. Merging partial behavioural models[C]// Proceedings of 12th ACM SIGSOFT International Symposium on Foundations of Software Engineering. New York: ACM, 2004: 43 - 52.

[6] LARSEN K G, STEFFEN B, WEISE C. A constraint oriented proof methodology based on modal transition systems[C]// Proceedings of the 1st International Workshop on Tools and Algorithms for Construction and Analysis of Systems. London: Springer-Verlag, 1995: 17 - 40.

[7] DAMAS C, LAMBEAU B, DUPONT P. Generating annotated behavior models from end-user scenarios[J]. IEEE Transactions on Software Engineering, 2005, 31(12): 1056 - 1073.