

分划扩充命题时态逻辑关于 stutter 不变性的特征定理^{*})

黄 青

(上海交通大学计算机科学与工程系 上海200030)

摘 要 分划扩充命题时态逻辑通过加入分划算子 $P^{1,1}$, 增强了经典命题时态逻辑的表达能力。本文就扩充逻辑关于 stutter 不变性的研究, 给出了它的一个关于 stutter 不变性的特征定理, 即具备 stutter 不变性质的扩充时态逻辑的表达能力和不含 $\bigcirc$ 算子(后继 Next 算子)的分划扩充命题时态逻辑相同。这样在具体的模型检测的实现过程中可以酌情地使用偏序归约技术, 进而可以大大地减少模型的状态空间数, 使相应的模型检测算法效率得到显著提高, 使一些状态个数过大的模型检测成为可能。

关键词 分划逻辑, 扩充时态逻辑, stutter 不变性, 偏序归约, 模型检测

A Stutter-Invariant Characterization for Partition Extended PTL

HUANG Qing

(Dept. of Computer Science & Eng., Shanghai Jiaotong Univ., Shanghai 200030)

Abstract We give a stutter-invariant characterization theorem of partition extended PTL. The main result is that stutter-invariant properties are expressible without next operator. In application, we can associate this result with partial order reduction technique to greatly reduce state space in model checking algorithm and make the latter substantially more efficient.

Keywords Partition logic, EPTL, Stutter invariance, Partial order reduction, Model checking

1 引言

作为检测软件、硬件和协议是否满足设计所要求达到的规范, 模型检测方法已经越来越多地受到重视。

计算机程序流程图、系统的数据流图以及网络通讯的各种协议等等, 经过简化和抽象都可以视为一个状态迁移系统 M , 再给定一个逻辑规范 φ , $M \models \varphi$ 是否成立就是模型检测问题的最一般的定义。然而在现实应用中由于经过抽象展开往往会使 M 的状态个数呈几何级数上升, 这将导致实现该算法程序的效率很低, 当 M 过大时导致模型检测程序实际上根本不终止, 这就是模型检测问题中最棘手的状态空间爆炸问题。因此有很多技术来解决该问题, 例如边展开模型边进行模型检测的“on-the-fly”技术等等。另外也可以通过化简将原模型 M 转为另一个等价的模型 M' , 即 $M \models \varphi$ 当且仅当 $M' \models \varphi$ 成立, 而 M' 的状态数相比于 M 要大大减少, 这样可以显著地提高模型检测的效率, 当然这样的化简是有条件的, 而条件往往和其逻辑规范 φ 相关, 这正是本文所研究的焦点问题。

1977年 Pnueli 提出了时态逻辑^[1], 本质上讲, 它可以视为一阶逻辑在结构 $(\mathbb{N}, <)$ 上的简化逻辑, 这是因为两者具有相同的表达能力, 但是前者可满足性的判定算法是多项式空间完备的, 而后者是非初等的^[7]。时态逻辑是作为一种形式规范语言, 它可以用来刻画一些基于时间先后顺序的系统行为性质, 在工程实践上十分有用。

但是经典线性时态逻辑的表达能力仍然有扩充的余地, 因为在结构 $(\mathbb{N}, <)$ 上单目二阶逻辑(Monadic Second-order Logic)和一系列不同版本的单目分划逻辑(Monadic Partition

Logic)表达能力完全相同^[6], 即都刻画了 ω 正则语言, 而一阶逻辑的表达能力不如前者, 由此提出了各种各样时态逻辑的扩充逻辑来扩充经典时态逻辑的表达能力^[6]。文[1]则提出了一种基于分划思想的扩充时态逻辑 $L(P^{1,1} + \bigcirc)$, 它在扩充时态逻辑表达能力的同时保持了其很好的计算复杂性, 可以证明该扩充时态逻辑的可满足性判定算法的复杂性仍然是多项式空间完备的^[1]。

对于经典线性时态逻辑场合, 如果其所要研究的性质具有 stutter 不变性则它的模型检测算法结合偏序归约技术可以将模型简化, 并且 stutter 不变性和时态逻辑中的 $\bigcirc$ 算子有密切的联系。本文研究的则是以上介绍的分划扩充时态逻辑 $L(P^{1,1} + \bigcirc)$ 的相关结论, 相比较于文[6]提出的扩充时态逻辑 $L(P^{1,1} + \bigcirc)$ 保留了经典时态逻辑良好的静态指称, 使得 stutter 不变性仍然和该逻辑中的 $\bigcirc$ 算子有密切的对应关系, 而这正是文[6]扩充时态逻辑所不具备的, 其很难从语法上找到与该性质对应的语法符号, 只能从语义上硬性规定^[4]。

下文第2, 3节首先介绍了基本概念以及分划扩充时态逻辑的基本定义和相关性质, 第4节证明了本文的主要定理, 即分划扩充时态逻辑关于 stutter 不变性的特征定理, 最后我们说明在应用上该结论可以结合偏序归约技术来提高其相应模型检测算法的效率。

2 基本的概念和定义

前文提到的模型 M , 在时态逻辑的模型检测问题中其理论模型就是 Kripke 结构, 而系统从初态开始的一次运行就对应了 Kripke 结构上的一条无穷路径。以下是 Kripke 结构和

^{*})国家自然科学基金资助项目(项目批准号60273050)。

其上无穷路径的正式定义,其中 AP 是有限非空原子命题集合,它表示了所要求研究系统的基本特性。

定义1 定义在给定 AP 上 Kripke 结构是一个三元组 $\langle K, S, L \rangle$, 其中: K 是有可能状态的集合, $S \subseteq K \times K$ 是状态间的迁移关系, L 表示每个状态到原子公式子集的一个映射, 即 $K \rightarrow 2^{AP}$. 对于每个状态 $s \in K$, 如果在 s 状态基本性质 $p \in AP$ 成立, 则对应 $p \in L(s)$; 反之, $p \notin L(s)$.

定义2 Kripke 结构 $\langle K, S, L \rangle$ 上的一条无穷路径 π 是一个状态的无穷序列 $s_0, s_1, s_2, \dots$, 满足: $s_i \in K$ 和 $(s_i, s_{i+1}) \in S$ (对所有的 $i \in \mathbb{N}$).

为了保证 Kripke 结构中有无穷路径的存在, 我们对 Kripke 结构作些小小的限制, 即每个状态都有相应的后继状态。

下面的工作主要是研究 Kripke 结构上的每条无穷路径, 进而可以将结论推广到整个关于 Kripke 结构上。

首先我们给出无穷路径相同的定义:

定义3 两条无穷路径 $\pi: s_0, s_1, s_2, \dots$ 和 $\rho: r_0, r_1, r_2, \dots$ 是相同的 (简记为 $\pi = \rho$) 当且仅当对于所有的 $i \in \mathbb{N}$ 有 $L(s_i) = L(r_i)$.

这样定义的好处是把重点强调在每一固定后继时刻所要研究的基本性质, 只要这些基本性质都能够对应相同, 那么这两条路径可视为同一。

显然, 对于无穷路径 π , 其第 i 个后缀 $s_i, s_{i+1}, s_{i+2}, \dots$ 仍然是一条无穷路径, 我们简记为 π^i , 特别地 $\pi = \pi^0$.

3 分划扩充时态逻辑

我们给出分划扩充命题时态逻辑的语法定义和语义解释。

定义4 分划扩充命题时态逻辑公式全体 $L(P^{1,1} + \bigcirc)$ 由下列规则生成:

$$\varphi ::= AP \mid \neg \varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc \varphi \mid P^{1,1}(\varphi_1, \varphi_2)$$

相应公式的语义解释如下 (设无穷路径为 $\pi: s_0, s_1, s_2, \dots$):

$$\pi \models p, p \in AP \quad \text{当且仅当} \quad p \in L(s_0);$$

$$\pi \models \neg \varphi \quad \text{当且仅当} \quad \pi \not\models \varphi \text{ 不成立};$$

$$\pi \models \varphi_1 \wedge \varphi_2 \quad \text{当且仅当} \quad \pi \models \varphi_1 \text{ 且 } \pi \models \varphi_2;$$

$$\pi \models \bigcirc \varphi \quad \text{当且仅当} \quad \pi^1 \models \varphi;$$

$\pi \models P^{1,1}(\varphi_1, \varphi_2)$ 当且仅当 存在自然数的一个非平凡的分划 N_a, N_b 使得对于任意的 $i \in N_a$ 和 $j \in N_b$, 有 $\pi \models \varphi_1$ 和 $\pi \models \varphi_2$ 成立¹.

事实上还可以将上述定义进行推广^[1], 如引入具有方向的三分划算子 $\overset{a,b}{p}(\alpha, \beta, \gamma)$, 它对应的语义为: 存在自然数的一个三分划 N_a, N_b, N_c , 第一个分划区间落在 N_a 中 (即 $\subseteq N_a$), 第二个落在 N_b 中, 使得对于任意的 $i \in N_a, j \in N_b$ 和 $k \in N_c$, 均有 $\pi^i \models \alpha, \pi^j \models \beta$ 以及 $\pi^k \models \gamma$ 成立。它们在具体形式规范的时候可能更有用, 由于分划算子具有“塌缩 (Collapsing) 现象”, 这样的推广完全可以用常规的二分划算子所替代。以下引理由文[1]作者给出, 具体证明可以参考该文。

$$\text{引理1} \quad \overset{a,b}{p}(\alpha, \beta, \gamma) \equiv \alpha \wedge p^{1,1}(\alpha, \beta \wedge p^{1,1}(\beta, p^{1,1}(\gamma, \alpha \vee \beta)))$$

分划扩充时态逻辑严格地扩充了时态逻辑的表达能, 一些无法用时态逻辑刻画性质可以由该扩充逻辑来刻画, 如作为线性时间结构的时间轴——自然数全体 $\mathbb{N}$, 偶数时刻

性质 p 成立等等均可以由分划扩充时态逻辑来刻画^[1]。可以证明分划扩充时态逻辑的表达能力和经典时态逻辑的各种扩充逻辑 (QTL, ETL, ETL_i)^[6] 相同, 并且与它们相比分划扩充时态逻辑的突出优点在于其静态指称性, 刻画规范相对比较直观、简洁。

分划扩充时态逻辑在表达能力上扩充时态逻辑, 从某种意义上是一种全局性的扩充, 在刻画那些后继局部性质上仍然需要 $\bigcirc$ 算子来刻画。一个很自然的问题是如果该扩充逻辑中不含 $\bigcirc$ 算子 (即只使用了以上公式构造的 1, 2, 3, 5 规则), 那么它的表达能力如何? 类似于线性时态逻辑场合, 不含 $\bigcirc$ 算子的公式全体也可以视为 $L(P^{1,1} + \bigcirc)$ 的子逻辑 (fragment), 我们简记为 $L(P^{1,1})$ 。

首先我们介绍一下经典时态逻辑场合相应的结论, 文[2]作者给了线性时态逻辑的一个特征定理。

$$\text{定理2} \quad PTL(\triangleright) = PTL(\triangleright, \bigcirc) / \sim_{st}$$

它的具体含义是一个不含 $\bigcirc$ 算子的线性时态逻辑所能刻画的性质恰好是所有线性时态逻辑能够刻画的并且具有 stutter 不变性的性质。

文本主要的工作是将上述结论推广到分划扩充时态逻辑的场合, 给出了一个相应的特征定理, 即:

$$\text{定理3} \quad L(P^{1,1}) = L(P^{1,1} + \bigcirc) / \sim_{st}$$

证明: 该定理是后文定理7和定理9的自然推论。这里还牵涉到一些基本概念, 这些将在下一节中进行详细讨论。

4 stutter 不变性的特征定理

时态逻辑可以规范很多关于时间先后的行为性质, 它们中的许多性质只在乎发生的先后顺序, 例如: “事件 p 先于事件 q 发生”, “只要事件 q 发生事件 p 一定会发生” 等等, 通常把这样的性质称为具备 stutter 不变性, 而和具体发生的时间间隔的长短相关的性质视为不具备 stutter 不变性, 例如: “事件 p 会在今后第 i 个时刻发生”, “事件 p 在事件 q 发生的下一时刻发生”, 当然这只是 stutter 不变性的非正式定义, 严格的定义需要先定义无穷路径的 stutter 等价概念^[2]。

定义5 两条无穷路径 $\pi: s_0, s_1, s_2, \dots$ 和 $\rho: r_0, r_1, r_2, \dots$ 是 stutter 等价的 (用符号 $\pi \sim_{st} \rho$ 表示) 如果存在两个自然数的严格递增序列 $0 = i_0 < i_1 < i_2 < \dots$ 和 $0 = j_0 < j_1 < j_2 < \dots$, 使得对于任意的 $k \in \mathbb{N}$ 有:

$$L(S_{i_k}) = L(S_{i_{k+1}}) = \dots = L(S_{i_{k+1}-1}) = L(r_{j_k}) = L(r_{j_{k+1}}) = \dots = L(r_{j_{k+1}-1}).$$

有了 $\sim_{st}$ 的定义自然可以引出 stutter 不变性的正式定义。

定义6 (stutter 不变性) 无穷路径 π 具有的性质, 如果对于任意的无穷路径 $\rho \sim_{st} \pi$, ρ 仍具备该性质, 则称该性质具有 stutter 不变性。类似地, 该性质所定义的无穷路径结构类关于 $\sim_{st}$ 关系是封闭的, 也称其具有 stutter 不变性。

定义7 stutter 简约路径 $\pi: s_0, s_1, s_2, \dots$ 是一个无穷路径, 满足: 或者存在 $i \in \mathbb{N}$ 使得, 对于所有的 $j < i$, 有 $L(s_j) \neq L(s_{j+1})$, 对于所有的 $j \geq i$, 有 $L(s_j) = L(s_{j+1})$; 或者对于所有的 $j \in \mathbb{N}$ 均有 $L(s_j) \neq L(s_{j+1})$ 。

因此对于任何一条无穷路径 π , 我们都可以定义关于该路径的 stutter 简约路径 $[\pi]_{st}$ 的概念。为此我们要注意以下两个事实:

¹在某些极端的场合, 可以允许退化的分划, 即允许 N_a 或者 N_b 为空集。

引理4 对于任何一条路径 π , 存在唯一一条 stutter 简约路径和它关于 stutter 等价。

引理5 两条 stutter 等价路径 $\pi \sim_{st} \rho$ 其对应的相同的 stutter 简约路径, 即 $[\pi]_{st} = [\rho]_{st}$ 。

两条引理的成立是显然的。需要指出的是引理4说明了 $[\pi]_{st}$ 的良好定义性, 引理5说明了 $[\pi]_{st}$ 可以作为关于包含路径 π 并且关于 stutter 关系封闭集合的代表元。

引理6 对于任意 $\varphi \in L(P^{1,1})$, 有 $\pi \models \varphi$ 当且仅当 $[\pi]_{st} \models \varphi$ 。

证明: 主要是对 φ 的结构进行归纳。若 φ 是原子命题或者主算子是布尔运算, 则结论是显然成立的, 需要说明的是 $\varphi = P^{1,1}(\varphi_1, \varphi_2)$ 的场合。 $[\pi]_{st}$ 可以视为 π 的一个“压缩”, 原先路径 π 一些相邻状态, 如果它们的所有基本属性都相同, 则它们被“压缩”成 $[\pi]_{st}$ 上的一个状态。所有从这些状态为初态的无穷路径仍然和 $[\pi]_{st}$ 上压缩对应状态为初态的无穷路径保持 stutter 等价, 并且后者仍然是 stutter 简约路径。这样, 若 $[\pi]_{st} \models P^{1,1}(\varphi_1, \varphi_2)$, 则根据分划算子的语义, 对应 π 的分划区间选取原则为: π 上的基本属性相同的相邻状态所属分划区间与 $[\pi]_{st}$ 上的“压缩”状态一致; 反之, 若 $\pi \models P^{1,1}(\varphi_1, \varphi_2)$, 则对应 $[\pi]_{st}$ 的分划区间选取原则为: 其上“压缩”状态的分划区间归属和 π 上对应属性相同的相邻状态的任何一个一致即可, 只要保证分划区间的非退化即可, 并且这一点是不难做到的。实际上, 分划算子的操作语义没法精确地规定分划区间的拉伸与压缩, 这就导致了它关于路径的 stutter 不变性在某种程度上“不敏感”。

定理7 不含 $\bigcirc$ 算子的分划扩充逻辑公式定义的性质具有 stutter 不变性。

证明: 假设 φ 为不含 $\bigcirc$ 算子的扩充分划逻辑公式, 路径 $\pi \models \varphi$, 而路径 $\rho \sim_{st} \pi$ 。根据引理6有 $[\pi]_{st} \models \varphi$, 根据引理5有 $[\pi]_{st} = [\rho]_{st}$ 。所以可得 $[\rho]_{st} \models \varphi$, 再次利用引理6可以推得 $\rho \models \varphi$ 。进而证明了不含 $\bigcirc$ 算子的分划扩充逻辑定义的性质具有 stutter 不变性。

下面将证明任何一个分划扩充时态逻辑可以定义的性质如果具有 stutter 不变性, 那么一定可以用不含 $\bigcirc$ 算子的分划扩充时态逻辑定义。这时主要的任务是利用 stutter 不变性去消除原先扩充时态逻辑公式中可能存在的 $\bigcirc$ 算子。为此我们首先引入给定有限非空原子公式集合 AP 上的文字集合的概念。

定义8 有限非空原子公式集合 $AP = \{p_1, p_2, \dots, p_m\}$ 上的文字集 $L_{AP} = \{P_i^s \wedge P_j^t \wedge \dots \wedge P_m^u \mid S \in 2^{AP}\}$, 其中: 如果 $p_i \in S$, $P_i^s := p_i$, 反之则, $P_i^s := \neg p_i$, $1, 2, \dots, m$ 。

L_{AP} 实际上枚举了各种可能的基本性质的组合, 显然如果两个状态 s, t 的某一个基本性质不同的话, 则存在 $\delta \in L_{AP}$, 使得 $s \models \delta$ 成立而 $t \models \delta$ 不成立。

引理8 对于任何 $\varphi \in L(P^{1,1} + \bigcirc)$, 存在 $TL(\varphi) \in L(P^{1,1})$ 使得对于所有的 stutter 简约路径 $\pi: s_0, s_1, s_2, \dots$ 均有: $\pi \models \varphi$ 当且仅当 $\pi \models TL(\varphi)$ 。

证明: 类似对于公式 φ 的结构进行归纳, 唯一的非平凡的转换在于消除公式 φ 中可能出现的 $\bigcirc$ 算子:

$$\begin{aligned} TL(p) &:= p \quad p \in AP; \\ TL(\neg \varphi) &:= \neg TL(\varphi); \\ TL(\varphi_1 \wedge \varphi_2) &:= TL(\varphi_1) \wedge TL(\varphi_2); \end{aligned}$$

$$TL(P^{1,1}(\varphi_1, \varphi_2)) := P^{1,1}(TL(\varphi_1), TL(\varphi_2));$$

$$TL(\bigcirc \varphi) := \bigvee_{\delta \in L_{AP}} ((\neg P^{1,1}(\delta, \rightarrow \delta) \wedge TL(\varphi)) \vee (\bigvee_{\delta' \neq \delta \in L_{AP}} \overset{\alpha, \beta}{P}(\delta, \delta' \wedge TL(\varphi), t)))$$

其中 t 是布尔常元, 表示恒真。

根据引理1, 对于任何 $\varphi \in L(P^{1,1} + \bigcirc)$, $TL(\varphi) \in L(P^{1,1})^2$ 。下面证明对于所有的 stutter 简约路径 π 成立: $\pi \models \varphi$ 当且仅当 $\pi \models TL(\varphi)$ 。根据归纳假设前三种情况与经典逻辑场合类似, 显然成立。对于分划量词, 可以直接按照其定义来证明, 需要指出的是, 对于 stutter 简约路径, 它的第 i 个后缀仍然是 stutter 简约路径。唯一不平凡的是消除 $\bigcirc$ 算子, 也就是证明: $\pi \models \bigcirc \varphi$ 当且仅当 $\pi \models \bigvee_{\delta \in L_{AP}} ((\neg P^{1,1}(\delta, \rightarrow \delta) \wedge TL(\varphi)) \vee (\bigvee_{\delta' \neq \delta \in L_{AP}} \overset{\alpha, \beta}{P}(\delta, \delta' \wedge TL(\varphi), T)))$

根据 L_{AP} 的定义, 存在唯一的 $\delta \in L_{AP}$, 有 $\pi \models \delta$ 。另外, 由于 π 是 stutter 简约路径, 因此以下两种情况必有一种情况成立。

- 1) $L(s_0) = L(s_1) = L(s_2) = \dots$;
- 2) $L(s_0) \neq L(s_1)$ 。

前一种情况对应 $\pi = \pi^1 = \pi^2 = \dots$, 此时对应公式 $\neg P^{1,1}(\delta, \rightarrow \delta) \wedge TL(\varphi)$; 后一种情况则对应公式 $\bigvee_{\delta' \neq \delta \in L_{AP}} \overset{\alpha, \beta}{P}(\delta, \delta' \wedge TL(\varphi), t)$ 。注意到此时必存在 $\delta' \in L_{AP}$, $\delta' \neq \delta$, 使得 $\pi^1 \models \delta'$ 。容易验证这两种情况均有上述等价关系成立。

定理9 能够被分划扩充时态逻辑定义的性质如果具有 stutter 不变性, 则该性质可以被不含 $\bigcirc$ 算子的分划扩充时态逻辑所定义。

证明: 假设路径结构类 C 具有 stutter 不变性, 即关于 stutter 关系封闭, 它可以被 $\varphi \in L(P^{1,1} + \bigcirc)$ 所定义, 那么对于任何无穷路径 $\pi \in C$, $\rho \in C$, 如果能够证明 $\pi \models TL(\varphi)$, 而 $\rho \models TL(\varphi)$ 不成立, 那么该定理就成立了, 下面的证明以 $[\pi]_{st}$ 和 $[\rho]_{st}$ 作为中间桥梁。

由定义 $\pi \sim_{st} [\pi]_{st}$, $\rho \sim_{st} [\rho]_{st}$, 所以 $[\pi]_{st} \in C$, $[\rho]_{st} \notin C$ 。又因为 φ 定义 C , 所以 $[\pi]_{st} \models \varphi$, 而 $[\rho]_{st} \models \varphi$ 不成立。根据引理8, 由于 $[\pi]_{st}$ 和 $[\rho]_{st}$ 是 stutter 简约路径, 因此有 $[\pi]_{st} \models TL(\varphi)$, 而 $[\rho]_{st} \models TL(\varphi)$ 不成立。由于 $TL(\varphi) \in L(P^{1,1})$, 根据引理6可得 $\pi \models TL(\varphi)$, 而 $\rho \models TL(\varphi)$ 不成立。

定理9实际上说明了不含 $\bigcirc$ 算子的分划扩充时态逻辑的“描述完备性”(Expressive Completeness), 定理7和定理9结合起来就构成了本文的中心定理: 即分划扩充时态逻辑关于 stutter 不变性的特征定理。

类似关于 ETL_r 的也有类似 stutter 不变性的特征定理, 只是由于 ETL_r 的语义不直观, 证明相对比较复杂^[4]。文[4]作者指出类似“性质 p 成立之前性质 q 成立的次数为偶数”等具有 stutter 不变性的规范无法由经典时态逻辑刻画, 但是可以由扩充时态逻辑(ETL_r)刻画, 这也间接地说明了 $L(P^{1,1})$ 的表达能力严格地强于 $PTL(\triangleright)$ 。

但是更重要的是由于 ETL_r 是通过引入“动态的”自动机算子来扩充时态逻辑的表达能力, 这样的扩充丧失了原有时态逻辑的良好的静态指称, 也不存在语法上和 stutter 不变性对应的算子。相对于 ETL_r , 分划扩充时态逻辑则继承了经典线性时态逻辑这一良好性质, 并且在其实行的模型检测算法中可以很容易地根据公式的语法构造判别其所形式化的性质

2 严格地讲, $TL(\varphi)$ 未必属于 $L(P^{1,1})$, 因为消除 $\bigcirc$ 算子的同时还引入了析取算子, 广义分划算子和布尔常元, 这些都不在 $L(P^{1,1})$ 中。但是, 根据引理1和布尔定律可以将 $TL(\varphi)$ 再经过逻辑恒等变换形成 $TL^*(\varphi)$, 使得 $TL^*(\varphi) \in L(P^{1,1})$ 。

是否有 stutter 不变性,这是其最突出的优点。

5 结合偏序归约技术

最后我们将上述关于路径的 stutter 等价性概念推广到 Kripke 结构上去,说明该特征定理在实际工程应用中的潜在应用,为此我们首先给出 Kripke 结构 stutter 等价的定义^[3]。

定义9 Kripke 结构 M 和 M' 称为 stutter 等价的 Kripke 结构当且仅当满足以下3个条件:

1. M 和 M' 有相同的初始状态集合;
2. 对于每一条从初始状态 s 出发在 M 中路径 π , 存在一条同样从 s 出发在 M' 中的路径 ρ 满足 $\rho \sim_{st} \pi$;
3. 对于每一条从初始状态 s 出发在 M' 中路径 ρ , 存在一条同样从 s 出发在 M 中的路径 π 满足 $\pi \sim_{st} \rho$ 。

根据以上关于 Kripke 结构 stutter 等价的定义并结合我们关于分划扩充时态逻辑关于 stutter 不变性的特征定理,我们可以很容易地得到以下推论。

推论10 设结构 M 和 M' 是两个 stutter 等价的 Kripke 结构,那么对于所有的 $\varphi \in L(P^{1,1})$ 以及所有初态 s_0 , 有 $M, s_0 \models A\varphi$ 当且仅当 $M', s_0 \models A\varphi$, 其中 $A(\cdot)$ 是全称型的路径算子,表示所有从初态 s_0 出发的路径。

该推论实际上是模型测算法中结合使用偏序归约(Partial Order Reduction)技术的理论前提,只有在规范中定义的性质具有 stutter 不变性时才能在模型检测算法中使用偏序归约技术。

简言之,偏序归约技术是一种利用模型状态迁移关系中的一些特殊性,对抽象展开成模型 M 的深度优先遍历算法加以改进,使得生成模型 M' 和原始算法所生成的 M 仍然保持 stutter 等价性,而其状态个数相比于前者将大大减少,具体技术实现细节可以参考文[3]第10章。

推论10的直接结果说明对于一个原始模型 M , 如果待检查的扩充分划逻辑规范具有 stutter 不变性(即该逻辑语句不含 $\bigcirc$ 算子),则可以利用偏序归约技术来将该模型简约至 M' , 再对 M' 进行模型检测,这样模型检测所需的时间和内存将大大减少,并且使原先不可能的检测变为可能。文[3]中第10章列举了在 SPIN³ 中使用偏序归约技术来简约 leader election 协议的模型状态空间,文[3]中图10.13的实验数据说明使用偏序归约技术所生成模型 M' 的状态空间与原先未使用偏序归约技术所生成模型 M 相比减少了许多;当进程个数为4时, M' 的状态个数不足 M 的2%,模型检测算法所需内存空间前者约为后者10%,而所需时间前者不足后者的1%;而当进程个数为5时检测 M 所需的内存空间超过128兆,运行时间超过40小时,而检测 M' 所需的内存空间只有3.2兆,运行时间只有28.7秒;当进程个数为6时前者的实际模型检测程序不终止,而后者的运行时间仅为4.1分钟。由此可以说明利用规范的 stutter 不变性可以很好地提高模型检测算法的效率,不论是经典的线性时态逻辑还是表达能力更强的分划扩充线性时态逻辑。

结论 本文主要给出并证明了分划扩充时态逻辑的一个特征定理,它拓展了经典时态逻辑关于 stutter 不变性的结论。在应用领域如同经典时态逻辑场合,如果在该扩充时态逻辑框架下定义的性质具有 stutter 不变性,那么该性质一定可以用不含 $\bigcirc$ 算子的分划扩充时态逻辑语句来刻画,检查该性质的模型检测算法就可以结合使用偏序归约技术,大大地减少模型的状态个数,从而可以很好地解决状态空间爆炸问题,在模型检测算法中可以极大程度地提高其算法效率,并且使原先不可实现的模型检测成为可能。

时态逻辑除了 stutter 不变性有相应的特征定理,其关于安全性(Safety,即坏事情不会发生)、活性(Liveness,即好事情总会到来)和公平性(Fairness,即特定事情会不断发生)仍有相应的特征定理^[10~12]。但是相比较于 stutter 不变性它们的语法对应性不明显,往往需要通过“特征公理”的方式引入^[10],所以后继工作就是在分划扩充时态逻辑的框架内探求语法上和这些性质对应的特征公理。

致谢 沈恩绍老师阅读了本文初稿,提出了许多有益的建议,在此表示感谢。

参考文献

- 1 沈恩绍. 命题时态逻辑的分划式扩充. 软件学报, 1996, 7(增刊): 447~454
- 2 Peled D, Wilke T. Stutter-invariant temporal properties are expressible without the nexttime operator. Information Processing Letters, 1997, 63(5): 243~246
- 3 Clark E M, Grumberg J O, Peled D. Model Checking. The MIT Press, 2000
- 4 Etessami K. Stutter-Invariant Languages, ω -Automata, and Temporal Logic. In: Proc. of 11th Int. Conf. on Computer-Aided Verification (CAV'99), 1999. 236~248
- 5 Holzmann G J. The SPIN Model Checker: Primer and Reference Manual. Addison Wesley Professional, 2004
- 6 Vardi M Y, Wolper P. Reasoning about infinite computations. Information and Computation, 1994, 15(1): 1~37
- 7 Reinhardt K. The complexity of translating logic into finite automata. LNCS2500, 2003. 231~238
- 8 Shen Enshao, Tian Qijia. Monadic partition logic and finite automata. Theoretical Computer Science, 1996, 166: 63~81
- 9 Pnueli A. The temporal logic of programs. In: Proc. of the 18th Symposium on foundations of computer Science, 1977. 46~57
- 10 Sistla A P. Safety, liveness and fairness in temporal logic. Formal Aspects of Computing, 1994 6(5): 495~511
- 11 官荷卿, 郭亮. 程序性质的描述及证明. 计算机科学, 2003 30(3): 146~148
- 12 唐稚松, 等. 时序逻辑程序设计与软件工程(上册). 科学出版社, 1999
- 13 古天龙, 蔡国永. 网络协议的形式化分析与设计. 电子工业出版社, 2003

³SPIN 是一种基于经典线性时态逻辑的模型检测工具,其具体设计、实现和使用可以参考文[5]。