时间区间时序逻辑的判定性与表达能力

朱维军[1,2] 周清雷[2]
(西安电子科技大学计算机学院 西安 710071)[1] (郑州大学信息工程学院 郑州 450052)[2]

摘 要 模型检测技术在实时系统验证中被广泛使用。离散时间区间时序逻辑满足性是可判定的,因而也是可模型检测的。连续时间域时间区间时序逻辑是否可模型检测,则并不清楚。约束时间域到非负实数,证明了其可满足性是不可判定的,但存在该逻辑的可判定子集,并发现了这样的子集。由于模型检测问题可归约为时序逻辑满足性判定问题,因此结果表明,时间区间时序逻辑不可模型检测,但其可判定子集可模型检测。

关键词 时间区间时序逻辑,可满足性判定,表达能力,模型检测
中图法分类号 TP301 **文献标识码** A

On the Decidability and Expressive Power of Timed Interval Temporal Logic

ZHU Wei-jun[1,2] ZHOU Qing-lei[2]
(School of Computer Science, Xidian University, Xi'an 710071, China)[1]
(School of Information Engineering, Zhengzhou University, Zhengzhou 450052, China)[2]

Abstract Model checking is used widely in verification of real-time system. Satisfiability of discrete Timed Interval Temporal Logic is decidable, so is model checking of it. But in dense-time domain, the problem of model checking Timed Interval Temporal Logic is not clear. We prove that Satisfiability of Timed Interval Temporal Logic is un-decidable and we find a subset of Timed Interval Temporal Logic which can be decidable. So, it can be decidable to model checking the subset.

Keywords Timed interval temporal logic, Checking the satisfiability, Expressive power, Model checking

1 引言

模型检测的形式化理论、计算模型与验证算法是近年来计算机科学的研究热点之一,基于各种模型检测算法的验证工具也被广泛使用在实时系统、电路设计、网络协议、软件规范等领域。在实时领域,Alur 提出的时间自动机[1]已经成为建立模型的事实标准,各种实时逻辑被提出并用来描述系统的实时性质[2-7],模型检测工具则自动给出时间自动机模型是否满足逻辑公式所描述性质的结论。

经典时序逻辑建立在基于连续点的语义基础上,公式只能在各个孤立点上被满足,而区间逻辑的优点则在于可以描述更复杂的时间区间及区间时间段之间的性质。完全版的基于区间的时段演算[6]不可判定,对它强力约束得到的可判定子集的模型检测算法遭遇到状态空间爆炸问题,这也导致了难以寻找逻辑规范可执行子集。时间区间时序逻辑[8](Timed interval temporal logic, TITL)的时序版 EITL(Extend interval temporal logic)具有一个规范可执行子集 Extend tempura 语言[9],其可通过执行规范的方法验证时序性质,因而已在一系列验证实例中取得成功[9]并正在被扩展到实时领域。这样,TITL 的子集将在区间验证领域成为第一个规范可执行的实时逻辑,这是用 TITL 逻辑实时区间验证的独特优势。

然而存在的问题是:TITL 公式所描述的工业实时系统性质是否可自动验证(模型检测),即稠密时间域上的 TITL 其可满足性是否可判定,以及它描述性质时的表达能力如何,这些目前并不清楚。我们对此进行研究。

2 时间区间时序逻辑 $TITL_R$

定义 1 状态 s 是一个二元组(a,t),其中 a 是命题集 P 在{true,false}上的映射,它的规范形式是一个集合 $a_P=\{x \mid x\in P\wedge x=\text{true}\}$,$t$ 是一个映射 $t:T\to N$,表示当前状态的时间。

定义 2 时间状态序列定义为 $\sigma=\langle s_0,s_1,\cdots,s_i,\cdots\rangle$,其中 s_i 为状态。

2.1 语法

定义 3 $TITL_R$ 公式构造

1) term $t::=T\mid T_f$

2) formula $\delta::=T_f\leqslant a\mid T_f<a\mid T_f>a\mid T_f\geqslant a\mid\delta_1\wedge\delta_2$

3) formula $\varphi::=p\mid\delta\mid skip\mid\varphi_1\vee\varphi_2\mid\neg\varphi\mid\varphi_1;\varphi_2$

定义 4 $TITL_R$ 公式缩写

到稿日期:2009-12-17 返修日期:2010-03-05 本文受国家(863)高技术研究发展计划(No. 2007AA010408),河南省重大科技攻关计划(No. 092101210104)资助。

朱维军(1976—),男,博士生,讲师,主要研究方向为时序逻辑、model checking、实时系统,E-mail:zhuweijun76@163.com;周清雷 男,教授,博士生导师,主要研究方向为 model checking、自动机与时序逻辑、信息安全。

1) $p \wedge q ::= \neg(\neg p \vee \neg q)$

2) $p \rightarrow q ::= \neg p \vee q$

3) $Op ::= skip; p$

4) $\Box p ::= \neg \Diamond \neg p$

5) $more ::= Otrue$

6) $empty ::= \neg more$

7) $p;_{TQ} q ::= (p \wedge T_f \in I); q$

定义 5 $TITL_R$ 公式的解释是 $I=(\sigma,i,k,j)$，其中 σ 是一个在 $\langle s_i,\cdots,s_k,\cdots,s_j\rangle$ 上的时间状态序列，$i,k,j \in N$，s_k 为当前状态，$len(\sigma)=j-i$ 为区间的时序长度，$len_t(\sigma)=s_t(j)-s_t(i)$ 为区间的时间长度，其中 $s_t(i)$ 为状态 s_i 对应的时间。

在时序逻辑与实时逻辑的很多文献中，为描述反应式系统的非终止运行，通常只包含无穷模型，而区间性质的验证需要我们考滤有穷模型，我们的定义中，$TITL_R$ 同时具有两种模型。在无穷区间中，$len(\sigma)=j-i=\omega$，$len_t(\sigma)=s_t(j)-s_t(i)=+\infty_N$。

2.2 语义

定义 6 令 $c \in N$，令 $s_p(k)$ 表示 $p \in AP$ 在状态 s_k 下的真值，$TITL_R$ 语义定义为：

Term：

1) $T=s_t(k)$

2) $T_f=s_t(j)-s_t(k)$

Timed formula：

1) $I| = T_f \leqslant C$ 当且仅当 $s_t(j)-s_t(k) \leqslant C$

2) $I| = T_f \geqslant C$ 当且仅当 $s_t(j)-s_t(k) \geqslant C$

3) $I| = T_f < C$ 当且仅当 $s_t(j)-s_t(k) < C$

4) $I| = T_f > C$ 当且仅当 $s_t(j)-s_t(k) > C$

5) $I| = \delta_1 \wedge \delta_2$ 当且仅当 $I| = \delta_1$ 且 $I| = \delta_2$

State and temporal formula：

1) $I| = p$ 当且仅当 $s_p(k)=\text{true}$

2) $I| = \neg\varphi$ 当且仅当 $I| \neq \varphi$

3) $I| = \varphi_1 \vee \varphi_2$ 当且仅当 $I| = \varphi_1$ 或 $I| = \varphi_2$

4) $I| = skip$ 当且仅当 $len(\sigma)=1$

5) $I| = \varphi_1;\varphi_2$ 当且仅当 $\exists r, k \leqslant r \leqslant j$，使得 $(\sigma,i,k,r)| = \varphi_1$ 且 $(\sigma,i,k,r)| = \varphi_2$

3 时间区间时序逻辑可满足性判定问题

定义 7[10] 设模态二阶语言 Ld 在命题集 P 上的时间状态序列 $TSS(P)$，语言为 $Ld(P)$，令 $c \in N, x,y \in R, \# \in \{=, \neq, <, >, \leqslant, \geqslant\}$，令 $d(x,y) \# c$ 是一个距离公式，表示 $|t_j - t_i| \# c$，直接距离公式被定义为：$\vec{d}(x,X) \# c \triangleq \exists y(x<y \wedge y \in X \wedge \neg \exists x'(x<x'<y \wedge x' \in X) \wedge d(x,y) \# c)$

定义 8[10] 直接距离模态逻辑 $\overleftrightarrow{Ld}$ 只包含具有下列形式的 Ld 公式：$\varphi \in \overleftrightarrow{Ld}(P)$ 当且仅当 φ 有形式 $\exists X_1 \cdots \exists X_m \psi$，其中 ψ 是 $x \in Q_P$，$x<y$，$x \in X$，$\vec{d}(x,X_i) \# c$ 等公式的布尔连接、一阶量词和 X_i 之外的集合变量。

引理 1[10] $\overleftrightarrow{Ld}(P)$ 定义的 $TSS(P)$ 子集和稠密时间自动机 TA_R 等价。

定理 1 $TITL_R$ 和 TA_R 不等价

证明：考滤 $TITL_R$ 的这样的子集 $TITL_{R\text{-}SUB}$，它与 $TITL_R$ 的唯一区别是不允许在 $\neg$ 的辖域内出现时间约束公式，即 $p;_{TQ}$ 不允许在 $\neg$ 的辖域内出现，根据定义有，$I| = p;_{TQ}$ 当且仅当 $\exists r, i \leqslant r \leqslant j$，使得，$(\sigma,i,k,r)| = p \wedge (\sigma,r,r,j)| = q \wedge T_f = s_t(r) - s_t(k) \# c$，由定义 7，令 $X=\{t_i \mid empty \in Q_P\}$，$x=s_t(k)$，则 $T_f \# c$ 是一个直接距离公式，$p;_{TQ}$ 是一个 $\overleftrightarrow{Ld}(P)$ 公式，进而根据定义 8，$TITL_{R\text{-}SUB}$ 公式是 $\overleftrightarrow{Ld}$ 公式，即 $TITL_{R\text{-}SUB} \subseteq \overleftrightarrow{Ld}(P)$。

假设 $TITL_R$ 与 TA_R 等价，则根据引理 1，必有一个公式 $\varphi \in TITL_R \wedge \varphi \notin TITL_{R\text{-}SUB}$，且存在一个 $A \in TA_R$，使得对任意 $(a,t) \in L(A)$，有 $(a,t)| = \varphi$ 成立，因此，$\varphi \in \overleftrightarrow{Ld}(P)$。我们考查 $\neg(p;_{TQ})$，根据定义有，$I| = \neg p;_{TQ}$ 当且仅当 $\forall r, i \leqslant r \leqslant j$，使得 $(\sigma,i,k,r)| = \neg p$ 或 $(\sigma,r,r,j)| = \neg q$ 或 $T_f = s_t(r) - s_t(k) \overline{\#} c$，因而 $\neg p;_{TQ}$ 不具有 $\overleftrightarrow{Ld}$ 的形式，$\varphi \notin \overleftrightarrow{Ld}(P)$，与 $\varphi \in \overleftrightarrow{Ld}(P)$ 矛盾。因此，$TITL_R$ 和 TA_R 不等价。

定义 9 设状态 s 是命题集 P 在 {true, false} 上的映射，$untime(TITL_R)$ 被定义为：$\varphi ::= p \mid skip \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \varphi_1;\varphi_2$

引理 2[11] $L_{TIL} = L_{untime(TITL_R)} \subset L_{PPTL^*} = L_{BA}$，其中 BA 表示 buchi 自动机。

定理 2 $L_{TA_R} \nsubseteq L_{TITL_R}$

证明：反证法。假设 $L_{TA_R} \subseteq L_{TITL_R}$，则 $\forall l.\ l \in L_{TA_R} \Rightarrow l \in L_{TITL_R}$，因此 $\forall l' = untime(l).\ l' \in (untime(L_{TA_R}) = L_{BA}) \Rightarrow l' \in untime(L_{TITL_R})$，因此 $L_{BA} \subseteq L_{untime(TITL_R)}$，与引理 2 矛盾，因此 $L_{TA_R} \nsubseteq L_{TITL_R}$。

引理 3[1] 给定一个时间自动机 $A \in TA_R$，则 $L_A = \phi$? 可在 PSPACE 空间内判定。

引理 4[1] 给定时间自动机 $A \in TA_R$，$B \in TA_R$，则 $L_A \cap L_B = \phi$? 可在 PSPACE 空间判定。

引理 5[12] 设 $\varphi' \in untime(TITL_R)$，$M'$ 为其模型空间，则 $\exists (m' \in M').\ m'| = \varphi'$? 至少需 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$ 判定时间。

定理 3 设 $\varphi \in TITL_{R\text{-}SUB}$，$M$ 为模型空间，则 $\exists (m \in M).\ m| = \varphi$? 至少需 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$ 判定时间。

证明：由定理 2 知，$L_{TITL_{R\text{-}SUB}} = L_{TA_R}$，因此对 $\varphi \in TITL_{R\text{-}SUB}$，$\exists f \exists (A \in TA_R).\ f(\varphi)=A$，其中 f 为一一映射函数。由引理 3 知 $\exists f'.\ f'(A) = (L_A = \phi?)$，即 $L_A = \phi$? 可判定，因此 $L_\varphi = \phi$? 可判定，即 $\exists (m \in M).\ m| = \phi$? 可判定。

设 $\varphi' = untime(\varphi) \in untime(TITL_R)$，则 $\exists (m \in M).\ m| = \varphi? \Rightarrow \exists (m' \in untime(M)).\ m'| = \varphi'?$，由引理 5，$\exists (m' \in untime(M)).\ m'| = \varphi'?$ 判定时间至少为 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$，因此 $\exists (m \in M).\ m| = \varphi?$ 判定时间至少为 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$。

定理 4 设 $\varphi \in TITL_{R\text{-}SUB}$，$A \in TA_R$，则 $A| = \varphi?$ 至少需 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$ 判定时间。

证明：$A| = \varphi?$ 判定问题可归约为 $L_A \cap L_{f(\neg\varphi)} = \varphi?$ 的判定问题，由引理 4，该问题可判定。由定理 3 证明知，$\exists (m \in M).\ m| = \varphi \Leftrightarrow f(\varphi)| = \varphi$，而判定 $\exists (m \in M).\ m| = \varphi?$ 至少用时 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$，因此计算 $f(\varphi) \in TA_R$ 至少用时 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$，由引理 4 知 $L_A \cap L_B = \varphi?$ 可在 PSPACE 空间判定，因此 $L_A \cap L_{f(\neg\varphi)} = \phi?$ 至少需要的时空资源是 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}} + PSPACE(|\varphi|)$，又因为 $PSPACE(|\varphi|) \leqslant 2^{|\varphi|} \ll 2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$，所以 $L_A \cap L_f(\neg\varphi) = \phi?$ 至少需 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$ 判定时间，即 $A| = \varphi?$ 至少需 $2^{O(|\varphi|)\cdot^{O(|\varphi|)}}$ 判定时间。

推论 1 设 $\varphi\in TITL_R$，M 为模型空间，则 $\exists(m\in M).\ m\models\varphi$? 不可判定。

推论 2 设 $\varphi\in TITL_R$，$A\in TA_R$，则 $A\models\varphi$? 不可判定。

由定理 1 和定理 2，易得以下推论。

推论 3 $L_{TITL_R}\cap L_{TA_R}=L_{TITL_{R\text{-}SUB}}$

引理 6[2] $L_{TA_R}\supseteq L_{MITL}$

推论 4 $L_{TITL_R}\Leftrightarrow L_{TITL_{R\text{-}SUB}}\supseteq L_{MITL}$

结束语 我们的结果是定理 3、定理 4、推论 1、推论 2、推论 3、推论 4。这些定理从 3 方面给出了结论。

关于 TITL 满足性判定问题。定理 3 证明了 $TITL_{R\text{-}SUB}$ 满足性可判定；定理 4 证明了 $TITL_{R\text{-}SUB}$ 性质可模型检测；而推论 1、推论 2 则证明，$TITL_R$ 满足性不可判定，也不可模型检测。这些定理表明：不允许在“逻辑非”的辖域内出现时间约束公式，这样得到的实数域时间区间时序逻辑的约束子集所描述的实时系统 TITL 性质，是可以开发出工具来自动验证的。而“非”辖域内出现时间约束这样的性质，则不可自动验证。

关于 TITL 可判定子集的判定效率问题。定理 3 和定理 4 表明：$TITL_{R\text{-}SUB}$ 判定可满足性与模型检测的问题固有时间复杂度的下限是非初等。也就是说，任何相应的实时系统模型检测工具在最坏情况下，至少需要非初等时间来判定模型是否满足给定的 TITL 性质。

关于 TITL 逻辑表达能力问题。推论 3 和推论 4 表明：时间区间时序逻辑 $TITL_R$ 的表达能力超出了时间自动机所接受的时间正则语言的范围，如图 1 所示，与表达能力低于时间自动机的普通实时逻辑 MITL[2,4] 相比，区间实时逻辑无疑有更强大的描述工业实时系统性质的能力。

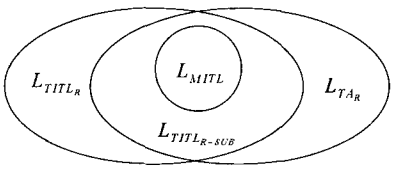

图 1 几种逻辑与自动机的表达能力

参 考 文 献

[1] Alur R, Dill D L. A Theory of Timed Automata[J]. Theoretical Computer Science, 1994, 126(2): 183-236

[2] Alur R, Feder T, Henzinger T A. The benefits of relaxing punctuality[J]. Journal of the ACM, 1996, 43(1): 116-146

[3] Alur R, Henzinger T A. A really temporal logic[J]. Journal of the ACM, 1994, 41(1): 181-204

[4] Alur R, Henzinger T A. Logics and models of real time: A survey[C]// Lecture Notes in Computer Science. Springer-Verlag, 1992, 600: 74-106

[5] Thomas A, Henzinger T A, Manna Z, et al. What good are digital clocks?[C]// Proc. ICALP'92, volume 623 of LNCS. Springer, 1992: 545-558

[6] Zhou C, Hoare C A, Ravn A P. A calculus of duration[J]. Information Processing Letters, 1991, 40(5): 269-276

[7] Li G, Tang Z. Translating a Continuous-Time Temporal Logic into Timed Automata[C]// Proceedings of the first Asian Symposium on Programming Languages and Systems (APLAS 2003). Lecture Notes in Computer Science 2895. Springer-Verlag, 2003: 322-338

[8] Duan Z. Modeling of hybrid systems[M]. Beijing: science press, 2004: 11-30

[9] Duan Z, Koutny M. A framed temporal logic programming language[J]. Journal of Computer Science and Technology, 2004, 19(3): 314-351

[10] Wilke T. Specifying timed state sequences in powerful decidable logics and timed automata[C]// Lecture Notes in Computer Science. Springer, 1994, 863: 694-715

[11] Tian C, Duan Z. Propositional Projection Temporal Logic, Büchi Automata and omega-Regular Expressions[C]// Proceedings, Theory and Applications of Models of Computation, Lecture Notes in Computer Science, 4978. Springer, 2008: 47-58

[12] Moszkowski B. Reasoning about Digital Circuits[D]. Stanford University, 1983

[13] Fränzle M. Model-checking dense-time duration calculus [J]. Formal Aspects of Computing, 2004, 16(2): 121-139

[14] Zhou C, Hansen M R, Sestoft P. Decidability and Undecidability Results for Duration Calculus[C]// STACS'93, Lecture Notes in Computer Science, 665. Springer-Verlag, 1993: 58-68

[15] Duan Z, Tian C, Zhang L. A decision procedure for propositional projection temporal logic with infinite models[J]. Acta Informatica, 2008, 45(1): 43-78

[16] 张海宾，段振华. 混合投影时序逻辑与混合系统的形式化验证[J]. 计算机科学，2007，34(11)：279-282

(上接第 226 页)

时存在的各种可能性。因此，本文把并发循环网系统(如 C/E 系统)中对并发事件序列化处理后产生的循环序列称之为交叠式序列。进一步，我们讨论了各种不同的并发情况下并发循环网系统中交叠式序列数目的计算，给出了相应的计算公式。通过这些计算，可以进一步指示两种不同的并发概念之间的差异和联系。

参 考 文 献

[1] 吴鹤龄，崔林. ACM 图灵奖(1966-2006)—计算机发展史的缩影(2 版)[M]. 北京：高等教育出版社，2008

[2] Milner R. Flow graph and flow algebras[J]. Journal of Association for Computing Machinery, 1979, 26(4): 794-818

[3] Milner R. A calculus of communicating system [J]. Lecture Notes in Computer Science, 1980, 92: 1-168

[4] Petri C A. Kommunikation mit automaten[J]. Bonn: Institue fur Instrumentelle Mathematik, Suhrifton des IIM Nr. 2, 1962 (In German)

[5] 袁崇义. Petri 网[M]. 南京：东南大学出版社，1989

[6] Petri C A. Concurrency[J]. Lecture Notes in Computer Science, 1980, 84: 251-260

[7] Genrich H J, Lautenback K, Thiagrajan P S. Elements of general net theory[J]. Lecture Notes in Computer Science, 1980, 84: 21-163

[8] 袁崇义. Petri 网原理与应用[M]. 北京：电子工业出版社，2005

[9] 吴哲辉. Petri 网导论[M]. 北京：机械工业出版社，2006