文章编号：1006-2475(2010)08-0058-04

一种基于 Büchi自动机的 LTL程序模型检测方法

罗清胜

(江西财经大学国际学院，江西 南昌 330013)

摘要：时序逻辑程序的形式化验证对提高程序的正确性具有重要意义。基于自动机的理论，用标签转移系统(S)表示程序的行为，用时序逻辑公式(F)描述程序的性质，构建相应的 Büchi自动机，从而证明形式化公式 S⊨ F是否可满足。

关键词：线性时序逻辑；Büchi自动机；模型检测

中图分类号：TP18 **文献标识码**：A doi：10.3969/j.issn.1006-2475.2010.08.017

A Method for Linear Temporal Logic Programs Model Checking Based on Büchi Automaton

LUO Qing-sheng

(International School of Jiangxi University of Finance & Economics, Nanchang 330013, China)

Abstract: Formal verification of temporal logic programs plays an important role in improving program correctness. Corresponding Büchi Automaton is constructed based on automata theory, in which labeled transition system(S) indicating programs' acts, temporal logic formulas(F) indicating programs' property. Thus, it proves that whether formal formula S⊨ F is satisfiable or not.

Key words: Linear time temporal logic; Büchi automaton; model checking

0 引 言

随着计算机软硬件系统日益复杂，如何保证其正确性和可靠性成为紧迫的问题。形式化方法由于是建立在严格的数学基础之上，可以通过符号化的手段来描述系统的属性，支持系统属性的推理及系统描述的正确性验证[1]。程序的形式化验证方法主要有定理证明和模型检测。定理证明的验证方法过程复杂，只能判断系统是否满足性质，不能找出违反性质的原因[1-2]。而模型检测具有较高的自动化程度，当系统不满足性质时还能够给出反例，便于调试程序，因而是当前研究的热点之一，并已被用于验证通讯协议、安全协议和控制系统等[3-4]。

在基于自动机理论的模型检测方法中，首先是将抽象出的系统模型用 Büchi自动机来表示，然后将需要验证的属性用一个 LTL公式[5]来描述，并将该公式取反后转化为 Büchi自动机[6]。最后检查系统自动机的接受语言是否被包含在性质自动机的接受语言中。如果是，则说明此系统具有 LTL公式所描述的性质，反之则没有。对此，本文给出如何构造 Büchi自动机，并用形式化的方法对给定的系统是否具有所期望的性质进行验证[4,7-8]。

1 LTL的语法和语义

在线性时序逻辑的构想中，在语法和语义层次上把动作看作一阶对象，首先考虑由动作索引的下一状态模式的 LTL的版本[9]。

给定一个原子命题的有限非空集 $P=\{p_1, p_2, \cdots\}$，且令 p q取值于 P，$LTL(\sum)$公式的集合由以下语法定义：$LTL(\sum)::=p\mid \neg\alpha\mid\alpha\vee\beta\mid<\alpha>\alpha\mid\alpha\cup\beta$。

$LTL(\sum)$模型是 $M=(\sigma, V)$，其中 $\sigma\in\sum^w$ 且 V：$prf(\sigma)\rightarrow 2^p$ 是计算函数。令 $M=(\sigma, V)$为一模型，$\tau\in prf(\sigma)$和 α都是公式，那么 $M,\tau\models\alpha$表示τ在模型 M上满足 α，此概念演绎定义如下：

(1)$M,\tau\models p$当且仅当 $p\in V(\tau)$；

(2)$M,\tau\models\neg\alpha$当且仅当 $M,\tau\not\models\alpha$；

(3)$M,\tau\models\alpha\vee\beta$当且仅当 $M,\tau\models\alpha$或 $M,\tau\models\beta$；

(4)$M,\tau\models<a>\alpha$当且仅当$\tau\alpha\in prf(\sigma)$并且 $M,\tau a\models\alpha$；

收稿日期：2010-04-09

作者简介：罗清胜(1980-)，男，江西丰城人，江西财经大学国际学院助理研究员，硕士，研究方向：软件工程，形式化方法。

(5)M,τ⊨ α∪ β当且仅当存在τ′使得τ⌢τ′∈ prf(σ)并且 M,τ⌢τ′⊨ β,而且对于每一个τ″使得 ε≤τ″≤τ′,有 M,ττ″⊨ α。

除了常用的命题连接词∧,⇒,≡,还使用命题常量 tt≝p1∨¬ p1且 ff≝¬ tt。

据此有派生模式:

(1)Oα≝∨a∈Σ<a>α;

(2)◇α≝tt∪α;

(3)□α≝¬◇¬α。

令 M=(σ, V)为一模型且τ∈ prf(σ),因此很容易得到如下断言:

(1)M,τ⊨ Oα当且仅当 M,τ⌢⊨ α其中τ′∈ prf(σ)使得 |τ′|=|τ|+1;

(2)M,τ⊨◇α当且仅当存在一个τ′∈Σ*,ττ′∈ prf(σ)使得 M,ττ′⊨ α;

(3)M,τ⊨□α当且仅当对每一个τ′∈Σ*,ττ′∈ prf(σ)蕴含 M,ττ′⊨ α。

Oα是 LTL中下一状态操作符。

2　LTL的可满足性及模型检测问题

公式 α∈ LTL(Σ)是可满足的,当且仅当存在一个模型 M=(σ, V)且τ∈ prf(σ)使得 M,τ⊨ α。由于该逻辑无论在语法上还是在语义上都不能表示过去,因此公式 α是可满足的,当且仅当存在一个模型 M使得 M, ε⊨ α。LTL的可满足性问题就是开发一个判定程序以判断给定的公式 α是否满足[4-5]。

现在构造 LTL(Σ)的模型检测问题。Σ上的一个有限状态程序为 Pr=(S,→, S_{in}, V_{Pr}),其中:

(1)S是有限状态集;

(2)→⊆S×Σ×S是一个转换关系;

(3)S_{in}⊆S是程序的初始状态集;

(4)V_{Pr}: S→2^P指派 P的一个子集到程序的每个状态。

很容易实现使得程序的每一可达状态至少有一个转换被执行。本文中指的程序都是有限状态程序。

程序 Pr的计算是一对(σ, ρ),其中 σ∈Σ^w且映射 ρ: prf(σ)→S满足:

(1)ρ(ε)∈ S_{in};

(2)$\rho(\tau) \xrightarrow{a} \rho(\tau a)$,对于每一τa∈ prf(σ)。

令(σ, ρ)是程序的一次计算,那么该计算典型的产生模型为 $M_{\sigma,\rho}$=(σ, V_ρ),其中 V_ρ由对于每一 τ∈ prf(σ)有 $V_\rho(\tau)=V_{Pr}(\rho(\tau))$给出。

令 Pr是一程序且 α是 LTL(Σ)的一个公式,如果对 Pr的每一个计算(σ, ρ),有 M, ε⊨ α,其中 M是由计算(σ, ρ)产生的模型,就说 Pr满足规约 α(用 Pr⊨ α表示)。模型检查的问题就是判定对于一个给定的程序 Pr和给定的公式 α是否有 Pr⊨ α。下面给出一个解决方案。

令 N=(B, E, F, c_{in})是一个系统,该系统的条件集合 B和事件集合 E都是有限集合,把程序 P_N=(S,→, S_{in}, V_{Pr})与 N作如下联系:

(1)Σ=E且 P=B。

(2)S是 2^B的最小子集且→是满足如下条件的 S×Σ×S的最小子集。

① c_{in}∈ S;

②如果 c∈ S且 e∈ E使得 ·e⊆c且 e·∩c=∅,那么 c′∈ S且(c, e, c′)∈→其中 c′=(c−·e)∪e·;

(3)S_{in}={c_{in}};

(4)对于每一个 c∈ S有 $V_{pr}(c)$=c。

因此所谓的用例图就是底层的转换系统,条件作为原子命题。

对于 c⊆B,令 α_c是公式∧b∈c b,考虑规约□¬α_c(对某些 c⊆B)。当且仅当 c是 N中可达的状态(比如 c∈ S),那么 P_N⊭□¬α_c。如果 e, e′是两个事件,那么 P_N⊨□◇<e>tt⇒□◇<e′>tt可知在 N中的每一个计算,如果事件 e发生,那么 e′也发生。大量的存在性和安全性属性能用 LTL(Σ)表达[6]。

3　基于 Büchi自动机的 LTL模型检测

3.1　Büchi自动机的构建

Σ上的 Büchi自动机为一个元组 B=(Q,→, Q_{in}, F),其中:

(1)Q是有限非空状态集;

(2)→⊆Q×Σ×Q是标签转移系统;

(3)Q_{in}⊆Q为初始状态集;

(4)F⊆Q是可接受状态集。

令 σ∈Σ^ω,那么 σ上的一次 B运行是一个映射 ρ: prf(σ)→Q使得:

(1)ρ(ε)∈ Q_{in};

(2)$\rho(\tau) \xrightarrow{a} \rho(\tau a)$(对于每一个τa∈ prf(σ))。

B的一次运行 ρ是可接受的,当且仅当 inf(ρ)∩F≠∅(其中 inf(ρ)⊆Q由 q∈ inf(ρ),当且仅当对于无限多的τ∈ prf(σ)有 ρ(τ)=q给出)。B接受的 ω字的语言 L(B)是:

L(B)={σ|存在一个基于 σ的 B运行}。

由 Büchi自动机识别的语言称为 ω正规

语言[12]。

定理 1 Büchi自动机的空问题能在线性时间内解决。

定理 2 判定由 Büchi自动机接受的语言是否为空的问题能在自动机的大小范围之内的线性时间里解决。

现在说明如何有效地构建对于 $\alpha\in LTL(\Sigma)$的自动机 B_α使得当且仅当 α可满足时 B_α接受的 ω字语言为非空。对此,基于动作的解决方案在文献[8]中提出了。

给定一个公式 α_0,为了构建自动机 B_{α_0},首先定义 α_0的闭包 $cl(\alpha_0)$。为了方便起见,假定派生的下一状态模态 O被包含在 $LTL(\Sigma)$的语法中。$cl(\alpha_0)$是满足如下情况的公式的最小的集合:

(1)$\alpha_0\in cl(\alpha_0)$;

(2)如果$\neg\beta\in cl(\alpha_0)$,那么 $\beta\in cl(\alpha_0)$;

(3)如果 $\alpha\vee\beta\in cl(\alpha_0)$,那么 $\alpha,\beta\in cl(\alpha_0)$;

(4)如果 $<a>\alpha\in cl(\alpha_0)$,那么 $\alpha\in cl(\alpha_0)$;

(5)如果 $O\alpha\in cl(\alpha_0)$,那么 $\alpha\in cl(\alpha_0)$;

(6)如果 $\alpha\cup\beta\in cl(\alpha_0)$,那么 $\alpha,\beta\in cl(\alpha_0)$且 $O(\alpha\cup\beta)\in cl(\alpha_0)$。

现在 α_0的闭包 $CL(\alpha_0)$定义为:

$CL(\alpha_0)=cl(\alpha_0)\cup\{\neg\beta\mid\beta\in cl(\alpha_0)\}$。

为了方便起见, $CL(\alpha_0)$简记为 CL。

$A\subseteq CL$称为一个原子,当且仅当它满足:

(1)$\beta\in A$当且仅当$\neg\beta\notin A$;

(2)$\alpha\vee\beta\in A$当且仅当 $\alpha\in A$或 $\beta\in A$;

(3)$\alpha\cup\beta\in A$当且仅当 $\beta\in A$或 $\alpha, O(\alpha\cup\beta)\in A$;

(4)如果 $<a>\alpha\in A$且 $<b>\beta\in A$,那么 $a=b$;

$AT(\alpha_0)$是原子的集合,简记为 AT。设 α_0的 Until需求的集合 $U_{\alpha_0}=\{\alpha\cup\beta\mid\alpha\cup\beta\in CL\}$,简记为 U_0。

Büchi自动机 B_{α_0}(简记为 B)现在被定义为 $B=(Q,\rightarrow,Q_{in},F)$,其中的各部分定义如下:

(1)$Q=AT\times 2^{U_0}$为状态集。

(2)转移关系$\rightarrow\subseteq Q\times\Sigma\times Q$由 $(A,x)\xrightarrow{a}(B,y)$给出,当且仅当满足如下条件:

①对每一个 $<a>\alpha\in CL$,当且仅当 $\alpha\in\beta$时,有 $<a>\alpha\in A$,并且对每一个 $O(\alpha)\in CL$,当且仅当 $\alpha\in\beta$时,有 $O(\alpha)\in A$;

②如果 $<b>\beta\in A$,那么 $b=a$;

③如果 $x\neq\phi$,那么 $y=\{\alpha\cup\beta\mid\alpha\cup\beta\in x$且 $\beta\notin B\}$;

④如果 $x=\phi$,那么 $y=\{\alpha\cup\beta\mid\alpha\cup\beta\in B$且 $\beta\notin B\}$。

(3)$Q_{in}\subseteq Q$由 $(A,x)\in Q_{in}$给出,当且仅当 $\alpha_0\in A$且 $x=\phi$。

(4)$F\subseteq Q$由 $(A,x)\in F$,当且仅当 $x=\phi$。

很容易证明当且仅当 α_0是可满足的,有 $L(B)\neq\phi$。前面提到的对于 Büchi自动机的空问题在自动机的大小范围之内的线性时间可解决,因此得出:

定理 3 $LTL(\Sigma)$的可满足性问题在指数时间内是可判定的。

3.2 模型检测算法

基于 LTL的模型验证方法需要构造一个非确定的 Büchi自动机,这恰好能接收违反规约性质的全部运行。模型检测的基本思想是用状态迁移系统(S)表示系统的行为,用时序逻辑公式(F)描述系统的性质。这样"系统是否具有所期望的性质"就转化为数学问题"状态迁移系统是否是公式的一个模型"。用公式表示为 $S\models F$? 对有穷状态系统,这个问题是可判定的,即可用计算机程序在有限时间内自动确定[9]。

对于模型检查问题,Büchi自动机的交错问题很容易解决。换句话说,让 B_1、B_2是基于Σ上的两个Büchi自动机。可以有效地构建一个基于相同字母集上的 Büchi自动机 B,使得由 B接受的语言是由 B_1接受的语言与由 B_2接受的语言的交集,并且 B的大小是 $2n_1n_2$,其中 n_1、n_2分别是 B_1、B_2的大小。

现在令 $Pr=(S,\rightarrow,S_{in},V_{Pr})$是一个程序。考虑与该程序 Pr相关的基于字母$\Sigma\times 2^P$上的 Büchi自动机 $B_{Pr}=(S,\rightsquigarrow,S_{in},S)$,其中$\rightsquigarrow$由以下给出,$(s(a,R),s')\in\rightsquigarrow$,当且仅当 $(s,a,s')\in\rightarrow$并且 $V_{Pr}(s)=R$。

令 α是一个规格说明,接着构建与 α的否对应的 Büchi自动机 $B_{\neg\alpha}$。令 $B_{\neg\alpha}=(Q,\Rightarrow,Q_m,F)$。已知 Q中的每一状态是形式 (A,x),其中 A是一原子,现在转换这个自动机为基于字母$\Sigma\times 2^P$上的自动机 $\hat{B}=(Q,\Rightarrow,Q_{in},F)$,其中$\Rightarrow$意思为:$(A,x),(a,R),(B,y)\in\Rightarrow$当且仅当 $(A,x),(a,(B,y))\in\Rightarrow$并且 $A\cap P=R$。最后令 B是接受由 B_{Pr}及 $\hat{B}$接受的语言的交集的自动机。因此,证明了 $Pr\models\alpha$当且仅当由 B接受的语言为空。对于自动机 B大小的分析可得:

定理 4 $LTL(\Sigma)$的模型检测问题在时间 $O(|Pr|\square 2^{|\alpha|})$上是可判定的。

4 结束语

本文对程序的形式化验证方法——模型检测作了比较详细的阐述。重点是对基于 LTL的模型验证方法构造一个非确定的 Büchi自动机,并在此基础

上,对程序是否具有期望的性质提出了解决方案。

参考文献:

[1] 李平福,陈冬火,张广泉.面向对象系统的时序逻辑描述[J].苏州大学学报(工科版),2008,28(4):12-13.

[2] 王小兵,段振华.时序逻辑程序的模型检测[J].计算机科学,2009,36(10):164-165.

[3] 林惠民,张文辉.模型检测:理论、方法与应用[J].电子学,2002,30(12):1908-1909.

[4] Jesper Gulmann Henriksen. Logics and Automata for Verification: Expressiveness and Decidability Issues[D]. University of Aarhus,2000.

[5] 王小兵,段振华.面向投影时序逻辑的 Web服务模型检测[J].西安交通大学学报,2009,43(4):39-43,124.

[6] Lasota S,Walukiewicz I. Alternating timed automata[C]//Proceedings of FOSSACS'05,LNCS 3441. Springer-Verlag,2005:250-265.

[7] Ouaknine J,Worrell J. On the decidability and complexity of Metric Temporal Logic over finite words[J]. Logical Methods in Computer Science,2007,3(1):1-27.

[8] Van Glabbeek R J. The linear time-branching time spectrum[C]//Proceedings of Theories of concurency: Unification and Extension(CONCUR'90),Lecture Notes in Computer Science 458. Springer-Verlag,199:278-297.

[9] Lasota S,Walukiewicz I. Alternating timed automata[J]. ACM Transactions on Computational Logic,2008,9(2):1-27.

[10] 郭建,边明明,韩俊岗. LTL公式到自动机的转换[J].计算机科学,2008,35(7):241-243,276.

[11] 易锦,张文辉.从基于迁移的扩展 Büchi自动机到 Büchi自动机[J].软件学报,2006,17(4):720-728.

[12] WU Zhi-Lin,ZHANG Wen-Hui. The complexity of dual models problem of propositional linear temporal logics[J]. Journal of Software,2007,18(7):1574-1576.

[13] Souza D,Madhusudan P. On-the-fly verification for product-LTL[C]//Proceedings of the 7th Indian National Seminar of Theoretical Computer Science(NSTCS'97). Indian,1997.

[14] Ouaknine J,Worrell J. On the decidability of metric temporal logic[C]//Proceedings of LICS'05. IEEE Computer Society Press,2005:188-197.

(上接第 57页)

的成功率和效率。同样,将该算法应用于传球过程中,也可以提高传球的效率。但是,此方法也存在一定的不足之处,在规划射门及传球路径时,应预先对各节点进行预处理以避免出现无穷大斜率和多值问题,以及 Hermite曲线有可能超出场地边界的可能。

参考文献:

[1] Kim J H,Kim H S,Jung M J,et al. A cooperative multi-agent system and its real-time application to robot soccer[C]//Proc of IEEE Conf on Robotics and Automation. New Mexico: Albuquerque,1997:638-643.

[2] Jung M J,Kim H S,Shim H S,et al. Fuzzy rule extraction for shooting action controller of soccer robot[C]//IEEE-int'l Fuzzy Systems Conference Seoul Korea,1999:556-561.

[3] Fassi H,Scarpettini F,Santos J. Development of the UBA-SOT simulation team[C]//Proceedings of FIRA Robot World Congress 2003. Viena,Austria,2003.

[4] 许翠微,孙绳武.计算方法引论[M].北京:高等教育出版社,2002.

[5] 郭路生,杨林权,吕维先.基于 Bézier曲线的机器人足球射门算法[J].哈尔滨工业大学学报,2005,37(7):921-923.

[6] 王进戈,王强,姚进.基于模糊评判的机器人足球比赛策略研究[J].哈尔滨工业大学学报,2005,37(7):953-955.

[7] 张玉文,许东来,余跃庆,等.基于四腿机器人足球比赛的多智能体协调控制[J].微计算机信息,2006,22(7):249-251.

[8] 余杨,任庆生,戚飞虎.一个基于遗传编程的机器人足球系统[J].计算机仿真,2005,22(4):178-182.

[9] 徐昶.人工智能在机器人足球赛中的应用[D].武汉:武汉理工大学硕士论文,2007.

[10] 朱春友.仿真机器人足球赛协作战术研究与实现[D].沈阳:沈阳工业大学硕士论文,2008.

[11] 雷大江.基于模糊技术的机器人足球策略研究[D].武汉:武汉科技大学硕士论文,2005.

[12] 吴丽娟,张春晖,徐心和.足球机器人决策系统推理模型[J].东北大学学报,2001(6):597-599.