模型检验中对 CTL 公式的空属性探测

郭 建[1]，金乃咏[2]

(1. 西安电子科技大学 微电子学院，陕西 西安 710071；
2. 华东师范大学 软件学院，上海 200062)

摘要：在模型检验中建立了一种新方法：检验可计算时态逻辑(CTL)公式描述的系统属性是否为空属性.根据原子命题的极性，用 TRUE 或 FALSE 替换原子命题，得到一系列的 CTL 公式，再对这些 CTL 公式用模型检验工具验证，若 CTL 公式中有一个通过了验证，则可得出该系统属性是一个空属性.该方法对 CTL 公式的空属性的探测不需要对它的所有子公式用 TRUE 或 FALSE 替换，只需对原子命题替换，这样检验的次数与原子命题的个数呈线性关系.利用验证综合系统对十字路口交通控制器规范的空属性进行了检验.

关键词：模型检验；空属性探测；可计算时态逻辑公式；验证综合系统系统

中图分类号：TP301.1 **文献标识码**：A **文章编号**：1001-2400(2007)05-0794-06

Vacuity detection in computation temperal logic

GUO Jian[1]，*JIN Nai-yong*[2]

(1. School of Microelectronics, Xidian Univ., Xi′an 710071, China;
2. Software Institute, East China Normal Univ., Shanghai 200062, China)

Abstract: In model checking a new method is proposed on checking whether a system property represented by a computation temperal logic (CTL) formula is vacuity. From the polarity of atomic proposition, a series of CTL formulae is derived by substituting the atomic proposition with TRUE or FALSE, before they are verified by model checking tools. If one of the CTL formulae has passed the verification, then it is concluded that the system property is a vacuity. In this solution, to check the vacuity of the CTL formula, it is not necessary to substitute all of its sub-formulae by TRUE or FALSE, but instead, it is enough to substitute its atomic proposition, and thus the number of times for checking is linear with the number of atomic propositions. With a VIS system, effectiveness of this solution is further verified by checking the vacuity of specification on the cross-road traffic controller.

Key Words: model checking; vacuity detection; CTL formula; VIS system

利用模型检验工具的好处就是对一个规格描述的回答是否定时，能够给出反例，这些反例是非常重要的，有利于用户从复杂的设计中探测出一些细节问题.而对于规格描述的回答是正确的时候，大部分模型检验工具并不提供在系统中满足规格描述的正例，认为正确的回答就意味着关于规格描述是正确的，这个结论看起来似乎是正确的，但仔细思考一下，就会发现里面有些问题，例如，验证一个系统关于一个可计算时态逻辑(CTL)规格描述ϕ=AG(req→AF grant).若 req 一直没有到来，则 ϕ 对于这个系统就是正确的，显然此检验并没有真正地验证公式 ϕ.

Beatty 和 Bryant[1]最早提出了的一个公式是空有效的概念.如果一个公式是空有效，就应给用户指出，因为空有效的公式不是用户所希望的规范.I. Beer 在文[2]中进一步扩展了空有效的概念，并指出了对一个公式的空属性(空有效)进行自动探测的方法，但仅给出了 ACTL 公式的空探测的方法.在文[3]中，提出了

收稿日期：2006-12-30

基金项目：国家自然科学基金重大项目资助(90607008)；陕西省教育厅自然科学基金资助(07JK373)

作者简介：郭 建(1969-)，女，西安电子科技大学博士研究生.

对 CTL* 公式进行空属性探测的一般方法,该方法检验的次数与 ϕ 的子公式幂集的大小呈线性关系. 笔者在文[3]的基础上,给出了一种改进的方法,对一个 CTL 公式,只需对它的原子命题用 FALSE 或 TRUE 来替换,然后再进行模型检验,就可探测此公式所表示的属性是否为一个系统的空属性. 此方法的检验次数与公式中原子命题的个数呈线性关系.

1　基本概念

1.1　CTL 公式

定义 1　一个在原子命题集合 P 上的 CTL 公式定义为 $\psi ::= p \mid \neg\phi \mid (\phi_1 \wedge \phi_2) \mid E_X\phi \mid E(\phi U \psi) \mid E_G\phi$,其中 $p \in P$.

对于其他的运算符可以通过上面的运算符进行等价变换得到[4].

1.2　Kripke 结构

定义 2　设 AP 是一组原子命题,在 AP 上的一个 Kripke 结构定义为四元组 $M=(S,S_0,R,L)$,其中:S 是一个有限状态集合;$S_0 \subseteq S$ 是初始状态集合;$R \subseteq S \times S$ 是转移关系,要求是完全的,即对 $\forall s \in S$ 都存在一个状态 $s' \in S$,使得 $(s,s') \in R$ 成立;$L: S \to 2^{AP}$ 是一个标记函数,函数为标记每个状态下所有为真的原子命题集合[5].

在 Kripke 结构中,从一个状态 s 开始的一条路径是一个无限状态序列 $\pi = s_0 s_1 \cdots$,其中 $s_0 = s$,且 $R(s_i, s_{i+1})$ 对所有 $i \geqslant 0$ 成立.

如果 CTL 公式 ϕ 在 M 下的一个状态 s 为真,则用 $M,s \models \phi$ 表示,在 M 一定的情况下,可以用 $s \models \phi$ 表示. 若 $M,s_0 \models \phi, s_0 \in S_0$,则用 $M \models \phi$ 表示.

定义 3　CTL 公式的语义定义如下:

(1) $s \models p$　　iff p 是原子公式, $p \in L(s)$.

(2) $s \models \neg\phi$　　iff $s \models \phi$ 为假.

(3) $s \models \phi \wedge \psi$　　iff $s \models \phi$ 且 $s \models \psi$.

(4) $s \models E_X\phi$　　iff 存在一条路径 $\pi = s_0 s_1 s_2 \cdots, s = s_0$ 使 $s_1 \models \phi$.

(5) $s \models E_G\phi$　　iff 存在一条开始于 $s = s_0$ 路径 $\pi = s_0 s_1 s_2 \cdots$,使 π 上的每一个状态 s' 都有 $s' \models \phi$.

(6) $s \models E[\phi U \psi]$　　iff 存在一条路径 $\pi = s_0 s_1 s_2 \cdots, s = s_0$ 对于某个 $j \geqslant 0$,都有 $s_j \models \psi$,且对于所有 $i < j, s_i \models \phi$.

1.3　空 属 性

定义 4　影响　公式 ϕ 的一个子公式 ψ 在模型 M 下影响 ϕ,如果存在一个公式 ψ',使得 ϕ 的真值与 $\phi[\psi \leftarrow \psi']$(把 ϕ 中的 ψ 换成 ψ')的真值在 M 下不同.

定义 5　空属性　如果 ϕ 中有一个子公式 ψ,使得 ψ 不影响 M 下的 ϕ,则公式 ϕ 在模型 M 下是空属性的.

空属性的概念就是对 ϕ 中的某个子公式 ψ,用任何公式替换后,都不会影响 ϕ 在 M 下的真值.

1.4　逻辑的极性

在定义逻辑的极性之前,先给出一个符号表示使公式 ϕ 有效的所有模型

$$[\![\phi]\!] = \{M \mid M \models \phi\} \quad , \quad [\![\phi]\!]^C = \{M \mid M \not\models \phi\} \quad ,$$

其中 $[\![\mathrm{TRUE}]\!] = \{M \mid M$ 是一个模型$\}$, $[\![\mathrm{FALSE}]\!] = \varnothing$.

定义 6　一个操作数的极性. 如果 σ 是某种逻辑的 n 元操作符,固定它的 $n-1$ 个操作数 $\varphi_1, \varphi_2, \cdots, \varphi_{i-1}, \varphi_{i+1}, \cdots, \varphi_n$,给出两个公式 ψ_1, ψ_2,若 $[\![\psi_1]\!] \subseteq [\![\psi_2]\!]$ ($[\![\psi_2]\!] \subseteq [\![\psi_1]\!]$) 有

$$[\![\sigma(\varphi_1, \varphi_2, \cdots, \varphi_{i-1}, \psi_1, \varphi_{i+1}, \cdots, \varphi_n)]\!] \subseteq [\![\sigma(\varphi_1, \varphi_2, \cdots, \varphi_{i-1}, \psi_2, \varphi_{i+1}, \cdots, \varphi_n)]\!] \quad ,$$

即 σ 的第 i 个操作数是单调递增(递减)的,则称 σ 的第 i 个操作数为正(负)极性的.

例如, $[\![a \wedge b]\!] = [\![a]\!] \cap [\![b]\!]$ 对"$\wedge$"的两个操作数来说是正极性的.

若一个运算符的每个操作数都是有极性的,则这个操作符也是有极性的. 若在一种逻辑中的每个操作符都是有极性的,则这种逻辑也是有极性的.

定理 1 CTL 是具有极性的逻辑.

证明 见文[2].

对一个公式中子公式的极性的定义[3]如下.

定义 7 子公式的极性. 给出一个公式 ϕ,对 ϕ 的子公式的极性是进行如下递归定义的:

(1) ϕ 是正极性;

(2) 如果 $x=\sigma(x_1, x_2, \cdots, x_i, \cdots, x_n)$,并且 x 是一个正(负)极性,则

若 σ 的第 i 个操作数是正(负)极性,则 x_i 是正极性;

若 σ 的第 i 个操作数是负(正)极性,则 x_i 是负极性.

2 公式的空属性探测

2.1 子公式集合的空属性探测

定义 8 前序关系(pre-order)($\leqslant$):若在子公式集合上的关系 R 满足自反、传递关系,则 R 是前序关系.

例如,$\phi=A_G(p\rightarrow A_X(q\rightarrow A_X r))$,令 $\psi=A_X(q\rightarrow A_X r)$ 是 ϕ 的一个子公式,而 q 也是 ϕ 的一个子公式,则它们之间满足前序关系:$q\leqslant\psi\leqslant\phi$.

引理 1 若 $x\leqslant\psi\leqslant\phi$,并且子公式 ψ 不影响在模型 M 下 ϕ 的真值,则 x 不影响在模型 M 下 ϕ 的真值.

证明 见文[2].

定义 9 设 x 是 ϕ 的一个子公式($x\leqslant\phi$),如果 x 不影响 M 下的 ϕ,则在 M 下 ϕ 是 x- 空.

定义 10 设 S 是 ϕ 的一个子公式集($S\subseteq\{x\mid x\leqslant\phi\}$,若存在一个公式 $x\in S$,使得 x 不影响 M 下的 ϕ,则在 M 下 ϕ 是 S- 空.

定义 11 最小子公式集. 设 S 是一个子公式集合,定义 S 的最小子公式集合 $\min(S)$ 为

$$\min(S)=\{x\in S\mid \forall x'\in S,\text{若 } x, x' \text{ 存在前序关系,都有 } x\leqslant x'\}\quad .$$

定义 12 一个 CTL 公式 ϕ 的 $c_l(\phi)$,定义为由 ϕ 的所有子公式组成的集合.

通过前面的定义,可得出下面的性质.

性质 1 对于任何 CTL 公式 ϕ,在 $\min(c_l(\phi))$ 中只包含原子命题.

证明 按结构归纳法证明:

(a) $\phi=p$ 是原子命题,则 $\min(c_l(\phi))$ 仅包含原子命题.

(b) 假设 f,g 满足此定理.

当 $\phi=f\wedge g$,则 $c_l(\phi)=\{f\wedge g\}\cup c_l(f)\cup c_l(g)$,由于 $f\leqslant f\wedge g$,则

$$\min(c_l(\phi))=\min(c_l(f))\cup\min(c_l(g))\quad .$$

根据假设 $\min(c_l(f))$ 与 $\min(c_l(g))$ 仅含有原子命题,则 $\min(c_l(\phi))$ 也仅含有原子命题

$\phi=E_X f$, $c_l(\phi)=\{E_X f\}\cup c_l(f)$, 而 $f\leqslant E_X f$, 所以, $\min(c_l(\phi))=\min(f)$.

同理可证 $\phi=\neg f$, $\phi=E(f\,U\,g)$ 和 $\phi=E_G f$.

若在一个公式中,所有原子命题仅出现一次,则通过下面的定理,就可得出对一个公式的空属性探测只需要探测 $\min(S)$ 即可了.

定理 2 在 M 下一个公式 ϕ 是 $c_l(\phi)$- 空,当且仅当在 M 下 ϕ 是 $\min(c_l(\phi))$- 空,即公式中出现的原子命题构成的集合是空属性集.

证明 $\Rightarrow$ 若在 M 下公式 ϕ 是 $c_l(\phi)$- 空的,则在 S 中必存在一个 $x\in S$,使在 M 下 ϕ 是 x- 空,分两种情况:

(1) $x\in\min(c_l(\phi))$,即 x 是一个原子命题,则直接由定义可知在 M 下 ϕ 是 $\min(c_l(\phi))$- 空.

(2) $x\notin\min(c_l(\phi))$,由于 x 在 M 下不影响 ϕ,而子公式集 S 是有限的,根据最小子公式集的定义可知,在 $\min(c_l(\phi))$ 中存在一个 x' 是原子命题,使得 $x'\leqslant x\leqslant\phi$,根据引理 1 可知,$x'$ 在 M 下不影响 ϕ,则在 M 下 ϕ 是 $\min(c_l(\phi))$- 空.

$\Leftarrow$若 ϕ 在 M 下是 $\min(c_l(\phi))$- 空的,$x\in\min(c_l(\phi))\subseteq c_l(\phi)$,则 ϕ 是 S- 空的.

现在对一个公式的空属性探测只需要对其原子命题进行探测,虽然在一个公式中原子命题是有限的,但

用定义对它进行空探测也是不可行的.下面将通过极性的概念,指出一个原子命题用 TRUE 或 FALSE 替换,再进行检验就可以.

2.2　有极性的 CTL 公式的空探测

引理 2　在 CTL 中,如果 $x \leqslant f$,并且 x 是一个正(负)极性,则若$[\![x]\!] \subseteq [\![x']\!]$($[\![x']\!] \subseteq [\![x]\!]$),有$[\![f]\!] \subseteq [\![f[x \leftarrow x']]\!]$.

证明　对 f 的大小进行归纳证明:

(1) 基础　$|f|=1$,f 是一个原子命题,所以 $x=f$,同样 x 也是一个原子命题,且 $f[x \leftarrow x']=x'$.因此,若$[\![x]\!] \subseteq [\![x']\!]$,则有$[\![f]\!] \subseteq [\![f[x \leftarrow x']]\!]$.

(2) 归纳　当 $|f|=n$ 命题成立.

若 $f = h \wedge g$,假设 h,g 都满足结论."∧"的两个操作数是有极性的.

若 $x=f$,则 $f[x \leftarrow x'] = x'$.当$[\![x]\!] \subseteq [\![x']\!]$,则有$[\![f]\!] \subseteq [\![f[x \leftarrow x']]\!]$.

若 $x \leqslant h$,由于 h 是正极性,那么 x 在 h 中的极性与在 f 中的极性是一样的.有$[\![h]\!] \subseteq [\![h[x \leftarrow x']]\!]$.

而 h 是"∧"的第一个操作数,是正极性,由操作数极性的定义可知:$[\![f = h \wedge g]\!] \subseteq [\![f[x \leftarrow x']]\!]$.

对于 $f = g \vee h$, $f = E(h\,U\,g)$, $f = E_X h$ 都有类似的证明.

若 $f = \neg h$, 由于 h 是负极性,就有$[\![h[x \leftarrow x']]\!] \subseteq [\![h]\!]$,有定义可知:$[\![f]\!] \subseteq [\![f[x \leftarrow x']]\!]$.

有了上面引理,就可以证明,一个公式 ϕ 的子公式 ψ 是否影响 ϕ,只需要把子公式用 TRUE 或 FALSE 替换就可以了.

把子公式集合与极性的空属性探测结合起来,将得到下列定理.

定理 3　设 ϕ 是一个 CTL 公式,$\min(c_l(\phi))$ 是 ϕ 的子公式集合的最小集合,即公式中出现的原子命题的集合,那么对于任何一个模型 M,下面的两种论述是等价的:

(1) ϕ 是 $\min(c_l(\phi))$ 在 M 下空的;

(2) 存在一个原子命题 $p \in \min(c_l(\phi))$,使得 $M \models \phi \Leftrightarrow M \models \phi[p \leftarrow \perp]$,$\perp$=FALSE,若 $M \models \phi$ 且 p 是正极性;或 $M \not\models \phi$,且 p 是负极性.否则,$\perp$=TRUE.

证明　略.

2.3　空探测的方法

从前面的定理中得出对一个 CTL 公式 ϕ 的空属性探测,可以通过下列步骤完成:

(1) 检查 ϕ;

(2) 若 $M \not\models \phi$,则给出反例;

(3) 若 $M \models \phi$,则对它进行空属性探测,对每个原子命题 p 做替换 $\phi[p \leftarrow \perp]$ 形成新公式,检查这些公式.若这些新形成的公式中至少有一个能够在模型下推出,则公式 ϕ 是空属性有效.

从这个过程中,可以看出需要进行检查的次数是 ϕ 中原子命题个数加 1 次.

3　一个例子

下面将通过一个例子来验证上面给出的有关理论.这个例子是关于十字路口交通控制器的例子.在一个很少有车辆的乡村小路与一个多道的主公路的十字路口,有一个交通灯控制着这个十字路口,这个控制要求在主公路上保留最大限制的绿灯,只有当小路有车,并在主公路上绿灯已经停留了一个"长"的时间间隔后,才能允许小路上的车辆通行.

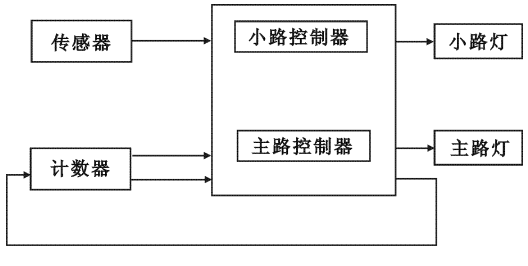

图 1　交通灯的模块连接图

3.1　总体设计

交通灯的模块连接图见图 1.在该设计中,一共有 4 个模块:计数器、传感器、小路控制和主路控制.

传感器模块是用来探测在小路上是否有汽车等待过十字路口,计数器模块用来计数黄灯停留的时间和绿灯停留的时间. 小路控制器控制灯一直保持为红灯,直到被主公路启动,这时重置计数器,并由红灯转到绿灯,一直停留在绿灯,直到没有汽车通过,或到达绿灯保留的最长时间,这时,它由绿灯转换成黄灯,然后转换成红灯,并启动主公路控制器. 在主公路控制器中,与小路的类似,只是它在小路无车辆或未达到最大停留时间时,一直保持绿灯.

这 4 个模块用 Verilog 语言基于状态机实现的.

3.2 描 述

在这里,用 CTL 公式表示将要检验的属性:

1) 若小路灯是绿灯,则终久会变成红灯,在小路上不可能总保留绿灯.

$$AG((farm\_light=GREEN)\rightarrow AF(farm\_light=RED)) \quad .$$

2) 在小路和主路上,不能同时为绿灯.

$$AG(!(farm\_light=GREEN * hwy\_light=GREEN)) \quad .$$

3) 在小路上有车,并且计数器达到长的计数后,小路上的灯终久会变成绿灯.

$$AG(((car\_present=YES * timer\_state=LONG)\rightarrow AF(farm\_light=GREEN))) \quad .$$

4) 在主路上的灯终久会变成绿灯.

$$AG(AF(hwy\_light=GREEN)) \quad .$$

5) 在小路上出现汽车,小路上的灯并不一定终久变成绿灯. 因为有可能会出现后,又返回了.

$$!(AG((car\_present=YES)\rightarrow AF(farm\_light=GREEN))) \quad .$$

3.3 模型检验及属性的空探测

用 Berkeley 大学的验证综合(VIS)原型系统[6]实现对属性的空探测,VIS 以 Verilog 为其输入语言,通过编译器 vl2mv 将 Verilog 转换成 blif_mv 格式,然后再进行模型检验.

把要检验的公式写到了一个文件 tlc.ctl,在 VIS 下检验,检验结果是它们都通过的检验,结果如下:

vis> model_check tlc.ctl .

#MC: formula passed——AG((farm_light=GREEN→ AF(farm_light=RED))) .

#MC: formula passed——AG(! ((farm_ligth=GREEN * hwy_light=GREEN))) .

#MC: formula passed——AG(((car_present=YES * timer.state=LONG)→ AF(farm_light=GREEN))) .

#MC: formula passed——AG(AF(hwy_light=GREEN)) .

#MC: formula passed——! (AG((car_present=YES→ AF(farm_light=GREEN)))) .

下面对这 5 个公式进行空探测,根据前面的理论,可以得到需要检验的公式,写入到一个文件中,然后对此文件中的公式进行模型检验,结果为:

vis> model_check tlc.ctl .

#MC: formula passed——AG((farm_light=GREEN→AF(farm_light=RED)) .

#MC: formula passed——AG((TRUE→AF(farm_light=RED))) .

#MC: formula passed——AG(! ((farm_light=GREEN) * (hwy_light=GREEN))) .

#MC: formula failed——AG(! (hwy_light=GREEN)) .

#MC: formula failed——AG(! (farm_light=GREEN)) .

#MC: formula passed——AG(((car_present=YES) * (timer.state=LONG))→ AF(farm_light=GREEN)) .

#MC: formula failed——AG((timer.state=LONG)→AF(farm_light=GREEN)) .

#MC: formula failed——AG((car_present=YES)→AF(farm_light=GREEN)) .

#MC: formula failed——AG(((car_present=YES) * (timer.state=LONG))→AF FALSE) .

#MC: formula failed——AG((TRUE)→AF(farm_light=GREEN)) .

#MC: formula passed——AG(AF(hwy_light=GREEN)) .

#MC: formula failed——AG(AF(FALSE)) .

#MC: formula passed——! (AG((car _ present=YES)→ AF(farm _ light=GREEN))) .

#MC: formula failed——! (AG (FALSE→AF(farm _ light=GREEN))) .

#MC: formula failed——! (AG((car _ present=YES)→ AF TRUE)) .

从结果可以看出第一个公式相对于它的子公式集是空的,而其余 4 个都不是空的,它们是有效的.

4 结 束 语

模型检验是目前应用较广的技术,在对模型检验时,往往把精力放在反例上,当出现一个反例时,马上意识到设计有问题.但对于通过模型检验的逻辑公式可能也有问题,空属性会造成公式被简单的通过.这里把注意力集中在对 CTL 公式进行空属性探测的研究上,给出当一个探测空属性的判断方法,该方法检验的次数与被测公式原子命题个数呈线性关系.下一步的工作将重点对原子命题在一个 CTL 公式中多次出现时,如何探测其空属性的研究上.

参考文献:

[1] Beatty D, Bryant R. Formally Verifying a Microprocessor Using a Simulation Methodology[EB/OL]. [2006-03-01]. http://citeseer. ist. psu. edu/cache/papers/cs/3060/ftp: zSzzSzn3. sp. cs. cmu. eduzSzusrzSzbryantzSzftpzSzdac94. pdf/beatty94formally. pdf.

[2] Beer I, David S B, Eisner C. Efficient Detecting of Vacuity in Temporal Model Checking[C]//Formal Methods in System Design of 18th. Manufactured in the Netherlands: Kluwer Academic Publishers, 2001: 141-163.

[3] Kupferman O, Vardi M Y. Vacuity Tetection in Temporal Model Checking[J]. Software Tools for Technology Transfer, 2003, 4(2): 224-233.

[4] Clarke E M, Grumberg O, Peled D A. Model Checking[M]. Massachusetts: MIT Press, 1999.

[5] 郭建, 韩俊刚. 基于模态转移系统的三值逻辑模型检验[J]. 计算机辅助设计几图形学学报, 2006,18(6):881-884.

[6] Villa T, Swamy G, Shiple T. VIS User's Mannual [EB/OL]. [2005-12-12]. http://www-cad. eecs. berkeley. edu/Respep/Research/vis/doc/package/index. html.

(编辑: 齐淑娟)

我校新增 2 个一级学科国家重点学科和 1 个二级学科国家重点学科

根据教育部《关于公布国家重点学科名单的通知》,继我校"信号与信息处理"、"电路与系统"、"通信与信息系统"、"微电子学与固体电子学"、"电磁场与微波技术"等 5 个国家重点学科通过考核评估之后,我校国家重点学科建设工作又传喜讯,新增"信息与通信工程"、"电子科学与技术"等 2 个一级学科国家重点学科和"密码学"二级学科国家重点学科.至此,我校现有国家重点学科已涵盖"工学"和"军事学"两个学科门类.

摘自《西电情况》2007.8.31