

一种可编程逻辑控制程序的竞态检测方法

黄颖坤, 罗继亮

(华侨大学 信息科学与工程学院, 福建 厦门 361021)

摘要: 针对可编程逻辑控制器中竞态检测的高计算复杂性,提出一种基于梯形图程序的特征结构用于检测竞态的方法.提出关系图的概念,并给出梯形图到关系图的转化方法.通过关系图的环形结构与可编程逻辑控制器的竞态之间的必然关系,给出梯形图中无竞态的判据.结果表明:该方法可以快速判断梯形图无竞态,并具有多项式级计算复杂度.

关键词: 竞态; 梯形图; 关系图; 可编程逻辑控制器

中图分类号: TP 271.8 **文献标志码:** A

梯形图具有形象、直观、实用等特点,是目前使用最多的一种可编程逻辑控制器(programmable logic controller,PLC)的编程语言^[1].但是,梯形图容易产生竞态,而竞态很难用传统的方法检测出来^[2],且验证程序的正确性需要极大的代价,动辄就是上百万美元.由于验证需要耗费大量时间,使得工厂、企业长时间停工.目前的研究成果大多是基于形式化方法^[3-4],包括模型检测和定理证明.模型检测是用一种形式化语言描述系统,生成系统行为的形式化描述,遍历系统模型的状态空间检验系统行为是否与需求相一致.国内外学者^[5-11]普遍使用 Petri 网或自动机为系统建模,将系统行为用另一种形式化语言描述,再用模型检测工具进行竞态检测.虽然模型检测可以实现检验过程的自动化,但是要遍历系统模型的状态空间,面临着“状态空间爆炸”的问题.定理证明可以处理无限的状态空间,它使用类似于结构化的推导过程来证明具有无限状态的系统.Kramer 等^[12]提出了 Higher Order Logic 分析 PLC 程序的方法.陈钢等^[13]用 COQ 定理证明器辅助 PLC 程序验证和分析.但是,定理证明大多数是交互的,需要人的参与,所以不仅提高了出错的概率,也降低了自动验证的可行性.尽管目前出现了用依赖图^[14-15]描述程序之间关系的研究,但是它将一个梯级看成结点,忽略了很多细节,无法清楚地表达梯形图各元素的逻辑关系.因此,本文提出了关系图的概念,通过梯形图转化为关系图;然后,从关系图的结构检验梯形图不存在竞态;最后,通过实例探讨该方法在竞态检验上的应用.

1 梯形图和竞态

梯形图是在原继电器-接触器控制系统的继电器梯形图基础上演变而来的一种图形语言.由于梯形图直观易懂,成为目前使用最广泛的一种 PLC 编程语言.梯形图的一个执行周期可以看成能量流从左垂直线经过 A,B 到达 C,然后从下一梯级的左母线经过 C 到达 B 的过程,如图 1 所示.

梯形图的竞态是指在输入和功能模块状态不变的情况下,输出发生变化.如图 1 的梯形图存在竞态,假设线圈 C 是输出线圈,触点 A 是输入触点.保持触点 A 是导通的,由于触点 B 是常闭触点,所以第一 PLC 扫描周期线圈 C 为高电平,当第二梯级执行完后,触点 B 为高电平;第二 PLC 扫描周期,由于触点 B 是常闭触点,此时为高电平,所以 C 变为低电

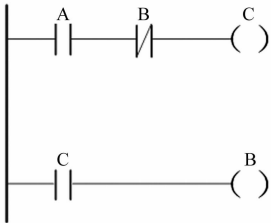


图 1 简单的梯形图
Fig.1 Simple ladder diagram

平. 因为输出状态的变化不是功能模块引起的, 所以梯形图存在竞态.

2 关系图的定义

从形式化的角度, 一个关系图 D 由非空有限集 $V(D)$, $V'(D)$, $A(D)$ 和 c 构成, 可以被定义为一个四元组, 记为 $D=(V, V', A, c)$. 其中: $V=\{v_1, v_2, \cdots, v_n\}$ 表示有限非空实结点的集合; $V'=\{v'_1, v'_2, \cdots, v'_m\}$ 表示有限非空虚结点的集合, $V \cap V' = \varnothing, V \cup V' \neq \varnothing$; $A \subseteq (V \times V') \cup (V' \times V)$ 是实结点和虚结点组成的二元组的集合, 表示从实结点到虚结点或虚结点到实结点的有向弧集合; $c: A \rightarrow \mathbf{Z}^+$ 表示关系图中每一条弧上的权值, \mathbf{Z}^+ 表示正整数集合.

用关系图描述梯形图的逻辑关系. 关系图的实结点用“□”表示, 对应为梯形图的图符单元, 如触点、线圈、功能模块等; 虚结点表示逻辑关系“与”, 用“|”来表示, 没有具体的意义; 弧上权值大小为对应梯形图的梯级, 如权值为“1”表示第一个梯级, “2”表示第二个梯级, 以此类推. 图 1 梯形图对应的关系图, 如图 2 所示. 图 2 表示的逻辑关系为实结点 V_c 受实结点 V_a, V_b 同时控制的, 对应到梯形图表示为线圈 C 的状态受触点 A, B 的状态共同控制, 符合图 1 梯形图的描述. 同理, 实结点 V_b 受实结点 V_c 控制, 对应到梯形图表示为触点 B 受线圈 C 控制, 也符合梯形图的描述. 因此, 可以用关系图等价的描述梯形图的逻辑关系.

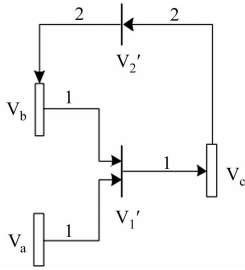


图 2 图 1 梯形图的关系图模型
Fig. 2 Relation graphs model of ladder diagram shown in figure 1

为了更好地认识关系图, 引入几个概念. 如果一个实结点只有输入有向弧没有输出有向弧, 称该实结点为根结点; 实结点到虚结点的有向弧或虚结点到实结点的有向弧, 称为关系图的线路, 简称线路; 如果一个实结点, 存在一条线路, 使之沿着这条线路能回到原点, 称该线路是一个关系图的环.

3 梯形图转化为关系图方法

梯形图间的逻辑关系较复杂, 从梯形图的结构无法直观地表示变量之间的逻辑关系. 因此, 提出将梯形图的逻辑关系转化为关系图来表示, 使梯形图内各元素之间的逻辑关系清晰化, 便于竞态的检测.

定义 1 在梯形图中, 由触点、功能模块以及连接它们之间的导线组成的线路称为梯形图的路径.

定义 2 可使能量流从左母线到线圈(右母线)的路径, 称为梯级路径. 从图 1 的梯形图实例可以看出: 梯形图有 2 条梯级路径. 梯级路径的个数等于梯形图的梯级数.

定义 3 由梯级路径中的触点、功能模块组成的集合, 并且删除该集合内的任意元素, 都会使梯级路径断开, 则称该集合为梯级路径的割集, 简称割集.

定义 4 从左母线到功能模块所有端口的路径, 由这些路径上的触点组成的集合, 并且删除该集合内的任意元素, 都会使功能模块不能正常工作, 称该集合为模块割集.

提出梯形图到关系图的转化方法, 给定一个梯形图, 假设其第一个梯级为 1, 以此类推. 转化方法为以下 7 个步骤.

步骤 1 将梯形图的触点、线圈、功能模块模拟为实结点.

步骤 2 任选梯形图的一个线圈, 假设该线圈为 C_x , 对应的实结点为 V_x .

步骤 3 确定 C_x 的割集的个数 m , 创建 m 个虚结点.

步骤 4 遍历 1 个割集内的元素, 连接元素对应实结点到该割集对应的虚结点的有向弧; 连接虚结点到 V_x 的有向弧; 为从实结点到实结点的有向弧赋予权值. 重复上述步骤, 直到遍历完所有的割集.

步骤 5 取 C_x 梯级路径上的一个触点, 判断梯形图是否存在以该触点为输出线圈的路径, 如果有, 重复步骤 3, 4; 如果没有, 取另一个触点进行判断, 直到遍历完所有触点.

步骤 6 若还存在其他没有遍历的线圈, 重复步骤 2~5, 直到遍历完所有线圈.

步骤 7 取梯形图的 1 个功能模块, 假设对应的实结点为 V_y . 确定模块割集的数目 n , 创建 n 个虚结点. 遍历一个模块割集内的元素, 连接元素对应的实结点到该模块割集对应的虚结点的有向弧; 连接虚结点到 V_y 的有向弧; 为弧赋予权值. 重复上述步骤, 直到遍历完所有的模块割集.

4 梯形图不存在竞态的充分条件

通过分析关系图的结构,可得出梯形图不存在竞态的充分条件.

定理 1 给定一个梯形图,如果它的关系图中不存在环,那么该梯形图中一定不存在竞态.

证明 反证法.假设一个无环的关系图对应的梯形图存在竞态.对于无环的关系图,取任意非根结点,假设为 V_1 ,可以找到控制其状态的实结点,假设为 V_2 ;同样, V_2 如果不为根结点,可以找到控制其状态的实结点,以此类推,直到遍历到根节点.非根结点 V_1 最后总可以看成控制了一个根结点的状态.由于根结点的状态在 PLC 的扫描周期内是不变的,所以 V_1 不变.如果 V_1 对应梯形图的输出线圈,说明输出线圈在程序执行的过程中状态不变,结论与假设矛盾,所以该充分条件成立.

根据竞态的定义和上述的充分条件可得:如果关系图存在环,且环内包含有实结点对应为梯形图的功能模块,对应的梯形图不存在竞态.

5 实例分析

梯形图存在计数器 C0,计数器的预设值为“2”,如图 3 所示.当计数器的脉冲输入端 CU 为上升沿时,计数器加“1”;当计数器达到预设值时,C0 输出高电平;如果 R 端为高电平时,计数器清零,输出为低电平.根据前面提出的方法,将该梯形图中的触点、线圈、功能模块模拟为实结点,得到的实结点集合 $V=\{v_{m_{0,0}},v_{m_{0,1}},v_{m_{0,2}},v_{q_{0,0}},v_{q_{0,1}},v_{i_{0,0}},v_{c0}\}$;选取线圈 $Q_{0,1}$,其对应的实结点为 $v_{q_{0,1}}$.遍历线圈 $Q_{0,1}$ 可以得到 $Q_{0,1}$ 的割集为 $\{M_{0,1},M_{0,2}\},\{M_{0,2},M_{0,3}\}$,所以创建 2 个虚结点 v'_1,v'_2 ;遍历 2 个割集内的元素,连接对应结点之间的有向弧,然后给弧赋上相应的权值.

通过遍历线圈 $Q_{0,1}$ 梯级路径上的触点可知:不存在以梯级路径上的触点为输出线圈的路径,所以取另一个线圈 $M_{0,0}$ 进行遍历.步骤同上,可知 $M_{0,0}$ 的割集只有 1 个 $\{M_{0,1}\}$,所以创建 1 个虚结点 v'_3 ,连接对应结点之间的有向弧,最后给弧赋上相应的权值.

遍历所有线圈直到没有可遍历的线圈.由于该梯形图存在功能模块,所以遍历功能模块,确定其模块割集 $\{I_{0,0},M_{0,0},Q_{0,0}\}$;创建 1 个虚结点 v'_5 ;连接模块割集内的元素对应的结点之间的有向弧,即连接 $v_{i_{0,0}},v_{m_{0,0}},v_{q_{0,0}}$ 到 v'_5 的有向弧;连接 v'_5 到 v_{c0} 的有向弧;为弧赋予权值.得到的关系图,如图 4 所示.图 4 的关系图存在环结构,但是环内有代表功能模块的结点,根据提出的竞态判据,该梯形图不存在竞态.

从时序图的角度观察,如图 5 所示.从图 5 中可以看出:输出 $Q_{0,0}$ 的变化是由计数器 C0 到达预设值引发的,当计数器 C0 为低电平时,输出 $Q_{0,0}$ 为低电平,根据竞态的定义可知,梯形图不存在竞态.

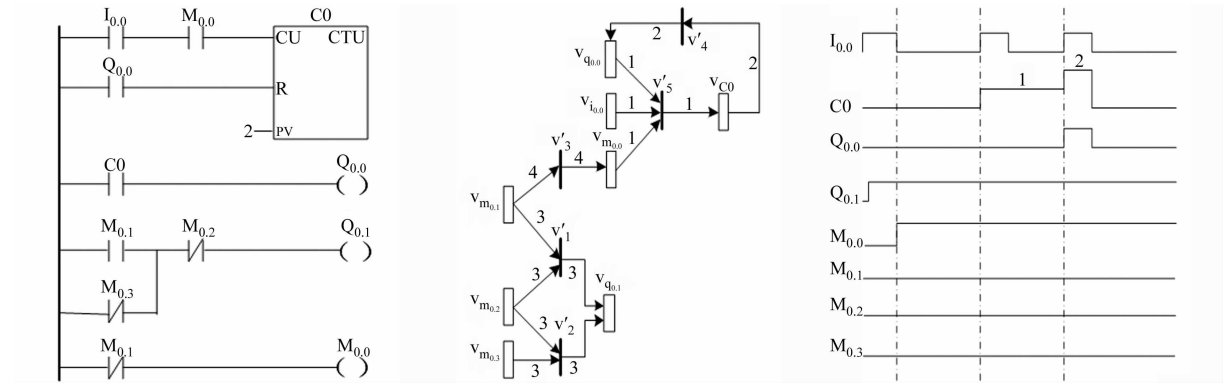


图 3 不存在竞态的梯形图
Fig. 3 A ladder diagram free of race

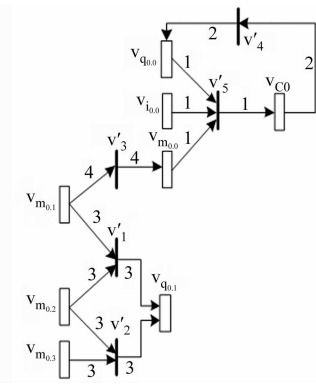


图 4 图 3 梯形图的关系图模型
Fig. 4 Relation graphs model of ladder diagram shown in figure 3

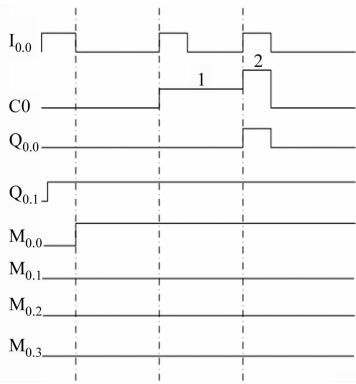


图 5 图 3 梯形图的时序图
Fig. 5 Timing chart of ladder diagram shown in figure 3

6 结束语

竞态本质上是由梯形图内部触点以及梯级的排列顺序产生的,即梯形图的结构影响到竞态的产生.所以从梯形图的结构入手,提出了用关系图来描述梯形图的逻辑关系,从而快速的判断出梯形图不存在

竞态. 当需要检测一个大型梯形图程序是否存在竞态,传统的模型检测会耗费大量的时间,文中为竞态的检测提出了一个新的思想. 通过将梯形图转化为关系图,根据所提出的充分条件,可以较快的判断梯形图不存在竞态. 为了实现构建过程的自动化及完善关系图的判断方法,未来的工作主要是基于提出的方法给出转化算法,并给出梯形图存在竞态在关系图中的充分条件.

参考文献:

[1] 吕卫阳. PLC 技术综述[J]. 自动化博览,2008(增刊 1):16-19.

[2] AIKEN A,FAHNDRICH M,SU Zhen-dong. Detecting races in relay ladder logic programs[J]. International Journal on Software Tools for Technology Transfer,2000,3(1):93-105.

[3] 吕毅. 形式化方法介绍及其在工程中的应用[J]. 微电子学与计算机,2003(10):26-34.

[4] 张广泉. 关于软件形式化方法[J]. 重庆师范学院学报:自然科学版,2002,19(2):1-4.

[5] 杨年华,虞芑群,孙华. 带抑制弧的时延着色 Petri 网模型检测技术[J]. 计算机科学,2011,38(1):170-176.

[6] 沈云付,解晓方. 基于 on-the-fly 的 Petri 网模型检查技术研究 with 实现[J]. 计算机应用与软件,2011,28(5):82-85.

[7] BENDER D F,COMBEMALE B,CRÉGUT X,et al. Ladder metamodeling and PLC program validation through time Petri nets[C]// 4th European Conference on Model Driven Architecture-Foundations and Applications. Berlin: Springer,2008:121-136.

[8] NGALAMOU L,MYERS L. Combining software methods for effective deployment of programmable logic controllers[J]. International Journal of Computer Science and Network Security,2010,10(12):134-145.

[9] WIGHTKIN N,BUY U,DARABI H. Formal modeling of sequential function charts with time Petri nets[J]. IEEE Transactions on Control Systems Technology,2011,19(2):455-464.

[10] MOKADEM H B,BERARD B,GOURCUFF V,et al. Verification of a timed multitask system with UPPAAL[J]. IEEE Transactions on Automation Science and Engineering,2010,7(4):921-932.

[11] TSAI J,TENG C C. Constructing an abstract model for ladder diagram using Petri nets[J]. Asian Journal of Control,2010,12(3):309-322.

[12] KRAMER B J,VAOLKER N. A highly dependable computing architecture for safety-critical control application [J]. Real-Time Systems,1997,13(3):237-251.

[13] 陈钢,宋晓宇,顾明. COQ 定理证明辅助 PLC 程序验证和分析[J]. 北京大学学报:自然科学版,2010,46(1):30-34.

[14] FERRANTE J,OTTENSTEIN K J,WARREN J D. The program dependence graph and its use in optimization[J]. ACM Transactions on Programming Languages and Systems,1987,9(3):319-349.

[15] 赵营,严义. 基于梯形图复杂依赖关系的分解研究[J]. 机电工程,2012,29(5):605-608.

A Race Detection Method for Programs in Programmable Logic Controllers

HUANG Ying-kun, LUO Ji-liang

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: For the high computational complexity of detecting races in the programmable logic controller, a race detection method based on ladder diagram is proposed. The relation graph is defined, and a method is presented to transform ladder diagrams into relation graphs. It is proved that races depend on loop structures in a relation graph. According to it, a criterion is presented to judge whether a ladder diagram is free of race. The results show that this method can quickly detect the free of race in ladder diagrams, and its computational complexity is polynomial.

Keywords: race; ladder diagram; relation graph; programmable logic controller