

DOI: 10.3969/j.issn.1673-4440.2022.05.002

基于B方法的轨道交通控制系统配置数据的形式化验证

程 鹏¹, 王恪铭^{1, 2}, 王 峥³, 姚文华³, 韩 程^{3, 4}

(1. 西南交通大学系统可信性自动验证国家地方联合工程实验室, 成都 610031;

2. 西南交通大学计算机与人工智能学院, 成都 614202;

3. 北京全路通信信号研究设计院集团有限公司, 北京 100070;

4. 通号粤港澳(广州)交通科技有限公司, 广州 511400)

摘要: 轨道交通控制系统对安全性和可靠性要求极高, 其正常运行依赖于正确的配置数据, 因而采用有效的方法保证配置数据的正确性显得十分重要。以轨道交通控制系统的配置数据为研究对象, 选取道岔、信号机、轨道区段、进路等站场型信号设备数据为研究案例, 基于各个配置数据的站场型数据结构, 先用自然语言描述各个配置数据和配置数据需要满足的静态规则, 再使用B语言形式规约各个配置数据及其所需要满足的静态规则, 建立静态形式化模型, 最后使用ProB模型检验工具, 验证分析已生成的各个配置数据是否满足静态规则。验证结果表明, 使用B方法对轨道交通控制系统配置数据进行形式化验证, 有效提高配置数据正确性, 进而为轨道交通控制系统的正常运行提供可靠保障。

关键词: 轨道交通控制系统; 配置数据; B方法; 形式化验证

中图分类号: U284.48

文献标志码: A

文章编号: 1673-4440(2022)05-0007-10

Formal Verification of Configuration Data of Rail Transit Control System Based on B Method

Cheng Peng¹, Wang Keming^{1, 2}, Wang Zheng³, Yao Wenhua³, Han Cheng^{3, 4}

(1. National-Local Joint Engineering Laboratory of System Credibility Automatic Verification, Southwest Jiaotong University, Chengdu 610031, China)

(2. School of Computing and Artificial Intelligence, Southwest Jiaotong University, Chengdu 614202, China)

(3. CRSC Research & Design Institute Group Co., Ltd., Beijing 100070, China)

(4. TongHao GBA (Guangzhou) Smart Control Co., Ltd., Guangzhou 511400, China)

收稿日期: 2022-03-02; 修回日期: 2022-05-06

基金项目: 国家重点研发计划项目 (2016YFB1200602)

第一作者: 程鹏 (1995—), 男, 硕士, 主要研究方向: 形式化建模与验证, 邮箱: pengcswjtu@163.com.

Abstract: Rail transportation control system requires high safety and reliability, and its normal operation depends on correct configuration data. Therefore, it is very important to adopt effective ways to ensure the correctness of configuration data. In this paper, the configuration data of the rail transportation control system is taken as the research object, and the station signaling data such as turnout, signal, section and route are selected as the research cases. Based on the station data structure of each configuration data, the configuration data itself and the static rules that each configuration data needs to satisfy are firstly described with natural language. Then, each configuration data and the static rules that need to be satisfied are defined by B language, and the static formal model is established. Finally, ProB model checking tool is used to verify and analyze whether the generated configuration data satisfied the static rules. The verification results show that using B method to formalize the configuration data of the rail transportation control system can effectively improve the correctness of the configuration data and provide a reliable guarantee for the normal operation of the rail transportation control system.

Keywords: rail transportation control system; configuration data; B method; formal verification

1 概述

在轨道交通运输业中, 轨道交通控制系统^[1]的作用类似于神经中枢, 其正常运行依赖于正确的配置数据, 使用有效方法保证轨道交通控制系统配置数据的正确性十分必要。在目前的实践应用中, 对配置数据的验证方式着重于如下两种手段。

1) 静态检测

根据数据的编写特征进行扫描, 对数据进行静态检测。

优点: 运行速度快, 可较好地发现数据的完整性问题, 如是否空值、长度与结构是否完整等。

缺点: 需要人工设计检查规则和检查办法, 通过代码的形式, 编写专用工具实现检查过程, 忽略了如果需要修改或扩充规则, 就需要重新修改软件代码, 而使得工具的可扩展性和可维护性不强, 即编写和修改规则不灵活。

2) 功能测试

对数据进行功能性测试, 依据设计规范, 检查数据流在系统中是否触发相应的操作。

优点: 测试过程直观, 可发现数据错误导致的问题等。

缺点: 严重依赖于测试案例的完整程度和覆盖面, 很难遍历所有数据及其组合情况。

综上所述, 在目前的研究应用中, 更需要找到一种灵活性好、安全可靠性的方法, 即形式化方

法^[2]。形式化方法是基于严格数学基础, 对计算机软件系统进行描述、开发和验证的技术。该方法能够基于形式规约语言, 建立系统数据静态规则原型, 使用逻辑验证方法, 穷尽数据集, 验证所有数据及其组合情况是否满足所定义的规则, 从而检查数据的完整性和正确性。近 10 年来, 使用形式化方法实现对配置数据的正确性验证, 受到了国内外研究者的关注, 特别是使用基于一阶逻辑和集合论基础的 B 方法实现对配置数据的正确性验证。

文献 [3-4] 展示了自 2009 年来, 各家世界信号行业巨头厂商阿尔斯通 (Alstom)、泰雷兹 (Thales)、西门子 (Siemens) 和 ProB^[5] 开发团队以及 Atelier B 建模平台合作, 实现世界各地地铁线路配置数据的形式化验证的工业应用。

文献 [6-8] 描述英国纽卡斯尔大学的形式化开发小组开发 SafeCap 铁路站场拓扑形式化设计验证平台, 其内部机制是利用 Eclipse Modeling Framework, 定义各个铁路站场型信号设备数据的数据结构。通过利用 Eclipse 开发环境, 生成各个信号设备数据, 并在该平台内部定义数据静态规则, 通过支持将数据及其规则转换为 B 机器文件格式的脚本, 结合 ProB 模型检验器, 实现全自动化判定数据是否满足所定义的规则。

文献 [9] 对 CTCS-1 级列控系统线路数据进行形式化验证, 其过程也类似。首先需要定义数据所需满足的静态规则, 然后使用 NUSMV 模型检验器

实现数据验证。

上述文献聚焦于高铁、地铁、磁浮拓扑线路配置数据的形式化验证技术路线的实现上，与本文不同之处在于研究应用对象不同，本文的应用案例为城市轨道交通列车控制系统^[10]配置数据的形式化验证。

轨道交通控制系统作为一类安全苛求系统，任何潜在的系统缺陷都可能会给行车运营安全带来巨大风险。因此，基于各个控制系统配置数据的数据结构，定义配置数据需要满足的规则，使用B语言，将已生成的各个配置数据和定义好的规则形式化，以建立配置数据的静态规则模型，利用ProB模型检验工具验证静态规则模型，从而验证所有的配置数据及其组合情况是否满足给定的规则，以达到验证配置数据正确性的目的。同时，使用形式化语言对规则进行定义时，能够灵活的修改、扩充规则。

2 配置数据的数据结构

以一个实际的城市轨道交通^[11]站场拓扑的数据为案例，介绍配置数据的数据结构。

如图1所示，这是一个简化的站场拓扑，只考虑站场拓扑中的道岔对象 $P (P_0 - P_n)$ ，轨道区段对象(简称区段, section)和信号机对象 $S (S_0 - S_n)$ ，以及所生成的进路对象，为方便后续验证工作，整个站场拓扑的编号描述如表1所示。

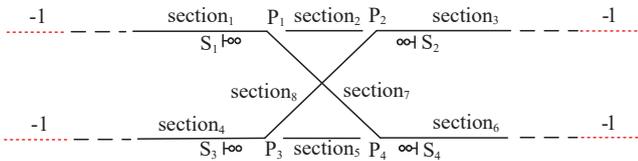


图1 站场拓扑

Fig.1 Station topology graph

表1 信号设备对象编号

Tab.1 Signaling equipment object number

信号对象	编号 (n 取自自然数)
道岔	$P_0 - P_n$, 表示站场拓扑有 $n+1$ 个道岔编号
区段	-1 表示尽头, $0 - n$ 表示站场拓扑有 $n+1$ 个区段编号
信号机	$S_0 - S_n$, 表示站场拓扑有 $n+1$ 个信号机编号
进路	$R_1 - R_n$, 表示基于道岔、区段、信号机编号, 生成了 $n+1$ 条进路编号

从图1中可以看出，这些信号设备对象之间存

在一定的关系。基于图1给出的简化站场拓扑，给出信号设备对象的数据结构。

2.1 道岔设备数据结构

在本案例的道岔数据结构中，考虑道岔的3种链接关系：第一种是道岔编号和区段编号之间的链接关系；第二种是道岔编号和道岔位置之间的关系；第三种是进路编号和道岔编号之间的关系。道岔编号和区段编号之间的链接关系如图2所示。

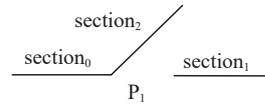


图2 道岔编号

Fig.2 Turnout number

图2中， P_1 为道岔编号， $section_0$ 、 $section_1$ 、 $section_2$ 为区段编号， $section_0$ 是 P_1 的岔尖区段编号， $section_1$ 是 P_1 的定位区段编号， $section_2$ 是 P_1 的反位区段编号。

对于道岔编号和道岔位置间的关系，同进路编号一起组装为一个二次关系，即进路编号-道岔编号-道岔位置。由于每一个进路编号最少有1个道岔编号与之对应，故将进路编号和道岔编号之间的关系组装为一个二次关系，即进路编号-道岔序号-道岔编号，道岔序号可以记录该进路编号有多少个道岔编号。

2.2 区段设备数据结构

在本案例的区段数据结构中，考虑区段有6种链接关系，取图1中的区段编号 $section_1$ ， $section_1$ 的6种链接关系，如图3所示。

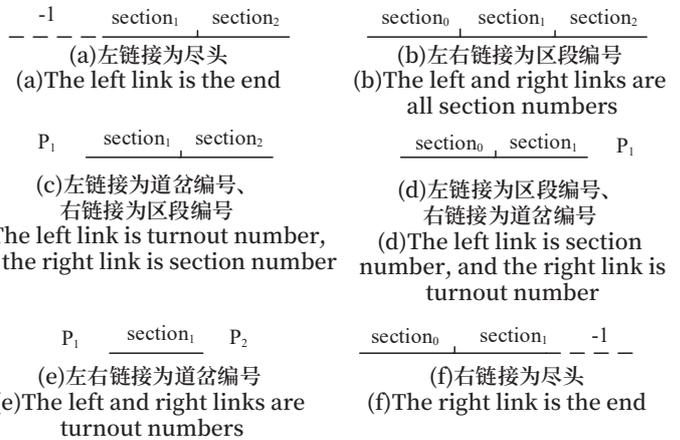


图3 区段设备数据关系

Fig.3 Section equipment data relationships

2.3 信号机设备数据结构

在本案例的信号机数据结构中，考虑信号机编号和区段编号之间的两种关系。每一条进路都有一个始端信号机，而在图 1 中可以看出，每一个始端信号机都对应一个区段。

2.4 进路数据关系

基于上文分析，进路数据共有 3 种链接关系，分别是进路编号 - 道岔序号 - 道岔编号、进路编号 - 道岔编号 - 道岔位置和进路编号 - 信号机编号。除这 3 种关系外，本案例还考虑进路编号 - 进路方向编号关系。

3 配置数据需要满足规则的自然语言描述

根据道岔设备、区段、信号机数据结构的定义

可知，进路数据关系与这些数据结构有关。本文只对进路数据需要满足的规则进行自然语言的描述。设计 3 种类型的规则，以验证进路数据的正确性，这 3 种规则分别有如下验证目的：1) 判断进路编号所对应的信号机编号，该信号机编号所对应的区段编号是否通过道岔设备和区段设备数据关系推理得到的区段编号一致；2) 判断进路编号中的道岔编号是否正确，即进路编号中的道岔编号是相邻的；3) 判断进路编号对应的进路方向编号是否和通过道岔设备和区段设备数据关系推理得到的进路方向编号一致。如表 2 所示，规则 1-6 的进路数据满足第一种类型规则，且将进路编号 - 进路方向编号的完整性规则包含在内。规则 7-8 的进路数据满足第二种类型规则。规则 9-10 的进路数据满足第三种类型规则。

表2 进路数据需要满足的3种类型规则
Tab.2 Three types of rules to be met by route data

规则编号	满足规则类型	含义
1	第一类型	进路方向编号只有 0 或 1
2		任意一条进路编号都有对应的进路方向编号
3		任意一条进路方向编号为 0 的进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号，该区段编号一定是该进路编号所对应的信号机编号所对应的第一区段编号
4		任意一条进路方向编号为 1 的进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号，该区段编号一定是该进路编号所对应的信号机编号所对应的第一区段编号
5		任意一条进路方向编号为 0 的进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号，该区段编号所对应的信号机编号一定是该进路编号所对应的信号机编号
6		任意一条进路方向编号为 1 的进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号，该区段编号所对应的信号机编号一定是该进路编号所对应的信号机编号
7	第二类型	任意一条进路方向编号为 0、且道岔序号大于等于 2 的进路编号，任取该进路编号所对应的 2 个相邻序号的道岔编号，通过道岔设备和区段设备的数据结构，得到 2 个相邻序号道岔编号的 4 个区段编号。如果这 4 个区段编号互不相同，又判断这两个序号相邻的道岔编号，其编号是否是相邻的（若相邻，则该进路编号的区段编号是连续的，在物理世界中该进路编号是正确的）
8		任意一条进路方向编号为 1、且道岔序号大于等于 2 的进路编号，任取该进路编号所对应的 2 个相邻序号的道岔编号，通过道岔设备和区段设备的数据结构，得到 2 个相邻序号的道岔编号的 4 个区段编号，如果这 4 个区段编号互不相同，判断这两个序号相邻的道岔编号，其编号是否是相邻的
9	第三类型	任意一条进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号。如果该区段编号的左链接为道岔编号、右链接为区段编号，那么该进路编号的进路方向编号一定为 0
10		任意一条进路编号，取该进路编号对应的第一个道岔编号，通过道岔设备和区段设备的数据结构，得到该进路编号的第一个区段编号，如果该区段编号的左链接为区段编号、右链接为道岔编号，那么该进路编号的进路方向编号一定为 1

对于第二种类型的规则,进路的道岔编号相邻连续指的是在物理世界里相邻连续,换言之,列车完整通过该进路时,物理空间所经过的道岔编号和数据中的道岔编号是一致的。如图4所示,就是进路中道岔编号不连续的情况,该进路编号包含道岔编号 P_1 和道岔编号 P_2 以及4个互不相同的区段编号,正确的情况是经过依次区段编号 $section_1$ 至 $section_4$, 但实际却经过如图4虚线所示的部分,因此该进路的道岔编号不是相邻连续的。

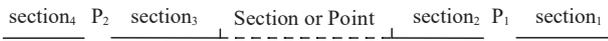


图4 进路和区段数据关系

Fig.4 Data relationship between route and section

如图5(a)所示,当某进路只经过1个道岔时,由道岔设备的数据结构决定,可以推断出该进路的区段编号一定相邻且连续。

当任意2个道岔编号所连接的4个区段编号出现重叠时,如图5(b)所示,道岔编号 P_1 和道岔编号 P_2 存在相同的区段编号 $section_2$, 这种情况也一定相邻且连续。

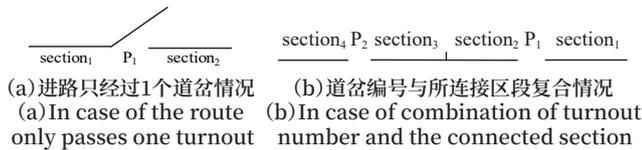


图5 进路和道岔数据关系

Fig.5 Data relationship between route and turnout

4 配置数据及其需要满足规则的形式化定义

4.1 B方法介绍

基于本节第2、3节内容和B方法规则^[12],完成配置数据及其规则的形式化定义。一个完整的B开发相当于生成一个B项目,一个B项目包含很多B模块。每一个B模块由一些B组件构成,这些B组件包含3种类型: B抽象机器、B精化机器和B实现机器3种。本文在抽象机器中实现对规则的形式化定义。集合论和一阶逻辑赋予B方法精确的定义和严格的规范形式。

4.2 配置数据的形式化定义

对于已生成数据的形式化考虑两种形式化表达:

1) 针对各个信号设备对象,分别定义不同的抽象数据类型,每一种抽象数据类型都用一种抽象集合来指代,根据信号设备对象的编号,实例化抽象集合,每一个编号都是一个集合元素。2) 针对各个信号设备对象的数据关系,分别定义不同的常量,而后对常量赋值。

1) 针对各个信号设备对象的形式化定义

道岔对象的抽象数据类型定义为 POINT 的抽象集合,实例化后,得到 P_1 至 P_n 的道岔编号, n 为正整数,如公式(1)所示。

$$POINT = \{P_1, P_2, \dots, P_{n-1}, P_n\} \quad (1)$$

信号机对象的抽象数据类型定义为 SIGNAL 的抽象集合,实例化后,得到 S_1 至 S_n 的信号机编号, n 为正整数,如公式(2)所示。

$$SIGNAL = \{S_1, S_2, \dots, S_{n-1}, S_n\} \quad (2)$$

进路对象的抽象数据类型定义为 ROUTE 的抽象集合。实例化后,得到 R_1 至 R_n 的进路编号, n 为正整数,如公式(3)所示。

$$ROUTE = \{R_1, R_2, \dots, R_{n-1}, R_n\} \quad (3)$$

由于区段编号需要划分为4种类型,比如左链接为区段编号、右链接为道岔编号等4种类型,故区段设备的形式化定义使用常量赋值。

2) 针对各个信号设备数据关系的形式化定义

道岔设备的数据结构考虑3种链接关系,第一种是进路与道岔的关系,即进路编号-道岔序号-道岔编号,定义常量 ROUTE_POINT 表示这种关系,该常量的赋值如公式(4)所示, n 为正整数。

$$ROUTE_POINT = \{R_1 | \rightarrow \{1 | \rightarrow \{P_1\}, \dots, n | \rightarrow \{P_n\}\}, \dots, R_n | \rightarrow \{1 | \rightarrow \{P_1\}, \dots, n | \rightarrow \{P_n\}\}\} \quad (4)$$

第二种是进路、道岔和道岔位置的关系,即进路编号-道岔编号-道岔位置,道岔位置反位用0表示,定位用1表示,定义常量 ROUTE_POINT_POS 表示这种关系,该常量的赋值如公式(5)所示,其中 n 为正整数, p 为0或1。

$$ROUTE_POINT_POS = \{R_1 | \rightarrow \{\{P_1\} | \rightarrow p, \dots, \{P_n\} | \rightarrow p\}, \dots, R_n | \rightarrow \{\{P_1\} | \rightarrow p, \dots, \{P_n\} | \rightarrow p\}\} \quad (5)$$

第三种是道岔与区段的链接关系,为了简化链接关系复杂度,分为道岔编号-岔尖编号-定位编号和道岔编号-岔尖编号-反位编号两种情况,这

两种情况的道岔编号相同。分别定义常量 $point_left_link$ 和 $point_right_link$ 表示。这两个常量的赋值如公式 (6) 所示, 其中 n 为正整数, $sec_0, sec_0, sec_0, sec_0, sec_0$ 为任取的区段编号, sec_0 和 sec_0 是岔尖编号, sec_0 和 sec_0 是定位编号, sec_0 和 sec_0 是反位编号。

$$\begin{aligned} point_left_link &= \{\{P_1\} \rightarrow \{sec_1\} \rightarrow sec_2\}, \dots, \{P_n\} \rightarrow \\ &\{sec_3\} \rightarrow sec_4\} \\ point_right_link &= \{\{P_1\} \rightarrow \{sec_1\} \rightarrow sec_3\}, \dots, \{P_n\} \rightarrow \\ &\{sec_4\} \rightarrow sec_6\} \end{aligned} \quad (6)$$

区段设备的数据结构考虑 0 种链接关系。将左链接为尽头、右链接为区段编号的关系, 左链接为区段编号、右链接为尽头的关系, 以及左右链接均为区段编号的关系, 合并为左右链接均为区段编号关系。合并之后, 就只有 0 种链接关系, 分别定义常量 $section_all_section$ 表示左右链接均为区段编号的区段编号链接关系, $section_left_section$ 左链接为区段编号、右链接为道岔编号的区段编号链接关系, $section_right_section$ 表示左链接为道岔编号、右链接为区段编号的区段编号链接关系, $section_null_section$ 表示左右链接均为道岔编号的区段编号链接关系。对这 0 个常量赋值如公式 (7) 所示, sec_a, sec_d 为任意的区段编号, $sec_b, sec_c, sec_e, sec_f$ 为任意的区段编号或尽头, $point_a, point_b, point_c, point_d$ 为任意的道岔编号。

$$\begin{aligned} section_all_section &= \{sec_a \rightarrow \{sec_b\} \rightarrow sec_c\}, \dots, \\ &sec_d \rightarrow \{sec_e\} \rightarrow sec_f\} \\ section_left_section &= \{sec_a \rightarrow \{sec_b\} \rightarrow \{point_a\}\}, \\ &\dots, sec_d \rightarrow \{sec_e\} \rightarrow \{point_b\}\} \\ section_right_section &= \{sec_a \rightarrow \{\{point_a\}\} \rightarrow sec_b\}, \\ &\dots, sec_d \rightarrow \{\{point_b\}\} \rightarrow sec_e\} \\ section_null_section &= \{sec_a \rightarrow \{\{point_a\}\} \rightarrow \{point_b\}\}, \\ &\dots, sec_d \rightarrow \{\{point_c\}\} \rightarrow \{point_d\}\} \end{aligned} \quad (7)$$

根据信号机设备数据结构的定义, 考虑信号机的两种链接关系, 进路编号 - 信号机编号和信号机编号 - 区段编号, 分别用常量 $ROUTE_SIGNAL$ 和 $SIGNAL_SECTION$ 记录, 对这两个常量的赋值如公式 (8) 所示, n 为正整数, S_a, S_b 为任意的信号机编号, sec_a, sec_b 为任意的区段编号。

$$\begin{aligned} ROUTE_SIGNAL &= \{R_1 \rightarrow S_a, \dots, R_n \rightarrow S_b\} \\ SIGNAL_SECTION &= \{S_1 \rightarrow \{sec_a\}, \dots, S_n \rightarrow \{sec_b\}\} \end{aligned} \quad (8)$$

除了道岔、区段、信号机设备的数据关系外, 本案例还考虑了进路编号 - 进路方向编号关系, 定义常量 $ROUTE_DIRECTION$ 来记录, 进路方向编号只有 0 或 1, 该常量赋值如公式 (9) 所示, a 和 b 为 0 或 1。

$$ROUTE_DIRECTION = \{R_1 \rightarrow a, \dots, R_n \rightarrow b\} \quad (9)$$

4.3 配置数据需要满足规则的形式化定义

在完成已生成的数据对象形式化后, 这个阶段需要考虑之前定义的数据所要满足的规则形式化。这个过程简单描述为, 将每一条自然语言的规则描述为具有逻辑真假性的谓词表达式, 其判定问题属于约束可满足求解问题。约束可满足问题 (Constraint Satisfaction Problem, CSP)^[13] 的定义是, 它由一个三元组 $\langle X, D, C \rangle$ 组成, 其中 X 是变量的集合, D 是变量的取值域, C 是约束的结合, X 中的每一个变量都对应 D 中的一个取值域, C 中的每一个约束都是由 X 的子集和一个不相容赋值集合组成。这里的变量集合 X 可以看成是道岔、信号机、区段设备对象、道岔、信号机、区段设备数据结构包含的关系。取值域 D 为这些信号设备对象所定义的抽象集合的实例化、其数据结构所定义的常量的赋值如公式 (10) 所示。

$$D = \{POINT, ROUTE, SIGNAL, section_all_section, \dots, point_left_link, \dots\} \quad (10)$$

每一个约束 C 就是一个自然语言描述的规则, 这个规则包含部分信号设备对象的描述, 对应变量集合 X 的子集。一般情况下, 一个 CSP 的求解是一个 NP-完全问题。若求解的逻辑值为真, 则可说明数据满足所定义的规则。反之则不满足。

进路数据需要满足的规则, 根据第 3 节分析, 进路数据需要满足的规则除了进路编号 - 进路方向编号外, 分为 3 种类型, 这 3 种类型定义了 8 种规则, 从规则编号 3 至规则编号 10。

首先, 如公式 (11) 所示给出规则编号 1 和规则编号 2 的形式化表达式。

$$/* \text{规则编号 1 和规则编号 2} */ ROUTE_DIRECTION:ROUTE \rightarrow \{0,1\} \quad (11)$$

1) 第一种类型规则

在规则编号 3 的描述中, 需要基于道岔设备、区段设备数据结构的定义, 来获取某进路编号所对应的第一个区段编号, 在本案例站场拓扑结构中, 进路编号的第一区段编号分为如图 6 所示的 3 种情况。

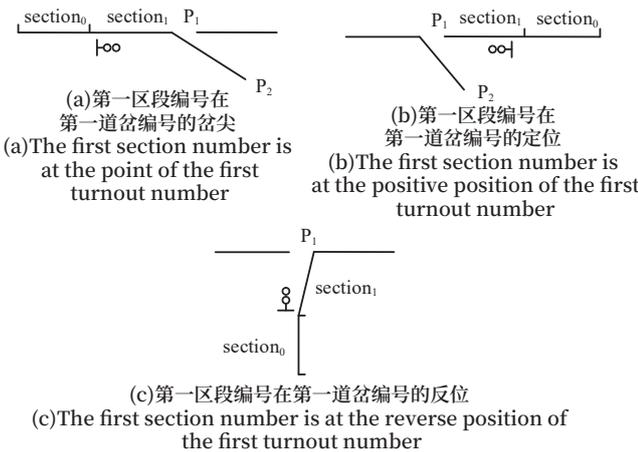


图6 规则编号3的三种情况
Fig.6 Three cases of rule number 3

如图 6 所示, 由于这类规则描述过于复杂, 为简化形式化表达, 特定义道岔位置和道岔数据结构之间的关系, 用常量 `point_link` 表示, 其赋值情况

如公式 (12) 所示。

$$point_link = \{0|->point_right_link, 1|->point_left_link\} \quad (12)$$

道岔位置处于反位由 0 表示, 道岔位置在定位由 1 表示, `point_right_link` 和 `point_left_link` 为之前定义的常量。有了以上的铺垫说明之后, 由于规则编号 4 和规则编号 3 是一种类型, 现给出规则编号 3 的形式化表达式, 如图 7 所示。

在规则编号 3 的形式化表达中, 量词 `xx` 表示进路编号, 量词 `bb` 表示 `xx` 的第一个道岔编号的岔尖区段编号, 量词 `cc` 表示 `xx` 的第一个道岔编号的定位或反位区段编号, 具体是定位、反位区段编号, 取决于 `xx`。由于考虑进路方向是 0, 在本案例的站场拓扑中, 方向是从右到左, 因而 `bb` 和 `cc` 究竟谁是 `xx` 的信号机编号所对应的区段编号, 取决于 `bb` 和 `cc` 谁是左链接为道岔编号、右链接为区段编号的区段编号。若 `bb` 是, 那么 `cc` 一定不会是, 因为 `cc` 的右链接一定是道岔编号, 这是由站场拓扑结构所决定的。反之亦然。规则编号 5、6 和规则编号 3、4 类似。

```
/*规则编号3*/
!(xx,bb,cc).(xx:dom(ROUTE_POINT) &
bb:dom(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(1)))(ROUTE_POINT(xx)(1)))&cc:ran(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(1)))(ROUTE_POINT(xx)(1)))&
ROUTE_DIRECTION(xx)=0 =>
({bb}^/dom(section_right_section)/=) & {bb} = SIGNAL_FIRST(ROUTE_SIGNAL(xx)) or ({cc}^/dom(section_right_section)/=) & {cc} = SIGNAL_FIRST(ROUTE_SIGNAL(xx))&
```

图7 规则编号3的形式化
Fig.7 Formalization of rule number 3

2) 第二种类型规则

规则编号 7 和规则编号 8 属于第二种类型规则, 如图 8 所示给出规则编号 7 的形式化表达式。

在规则编号 7 的形式化中, 量词 `xx` 表示进路编号, 由于对 `xx` 所包含的道岔进行了排序, 量词 `yy` 表示 `xx` 所包含的除最后一个序号的道岔编号。 `bb`

表示区段编号, 在任意两个有序的道岔编号中, 量词 `bb` 是排序靠前的道岔编号的岔尖区段编号, 量词 `cc` 表示排序靠前的道岔编号的定位或反位的区段编号, 是定位还是反位取决于该条进路编号。量词 `dd` 表示区段编号, 在任意两个有序的道岔编号中, `dd` 是排序靠后的道岔编号的岔尖区段编号。量词 `ee` 表

```
/*规则编号7*/
!(xx,yy,bb,cc,dd,ee).(xx:dom(ROUTE_POINT)&yy:1..max(dom(ROUTE_POINT(xx)))-1&
bb:dom(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(yy)))(ROUTE_POINT(xx)(yy)))&
cc:ran(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(yy)))(ROUTE_POINT(xx)(yy)))&
dd:dom(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(yy+1)))(ROUTE_POINT(xx)(yy+1)))&
ee:ran(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(yy+1)))(ROUTE_POINT(xx)(yy+1)))&
{dd}^/cc & ROUTE_DIRECTION(xx)=0 =>
dom(section_left_section(bb)) ^ {dd,ee} /={} or dom(section_left_section(cc)) ^ {dd,ee} /={}&
```

图8 规则编号7的形式化
Fig.8 Formalization of rule number 7

示排序靠后的道岔编号的定位或反位的区段编号, 和 cc 一样, 也取决于进路编号。由于要满足 bb, cc, dd, ee 互不相同, 而再由站场拓扑道岔数据结构所决定, 所以如果 bb, cc, dd, ee 是连续的, 那么集合 $\{bb, cc\}$ 中任意一个元素一定与集合 $\{dd, ee\}$ 中任意一个元素相邻, 因此集合 $\{bb, cc\}$ 中一定有一个元素, 即, 该区段编号一定是左链接为区段编号、右链接为道岔编号的数据结构, 且该区段编号的左链接区段编号一定是 dd 或 ee 。

```
/*规则编号9*/
!(xx,yy,zz).(xx:dom(ROUTE_POINT) &
yy:dom(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(1)))(ROUTE_POINT(xx)(1)))&
zz:ran(point_link(ROUTE_POINT_POS(xx)(ROUTE_POINT(xx)(1)))(ROUTE_POINT(xx)(1)))&
((!yy) = SIGNAL_FIRST(ROUTE_SIGNAL(xx)) & {yy}^dom(section_right_section)= {}) or
({zz} = SIGNAL_FIRST(ROUTE_SIGNAL(xx)) & {zz}^dom(section_right_section)= {})) =>
ROUTE_DIRECTION(xx)=0&
```

图9 规则编号9的形式化
Fig.9 Formalization of rule number 9

在规则编号 9 的形式化中, 量词 xx 表示进路编号, yy 表示区段编号, 在 xx 包含的所有道岔编号中, 顺序为第一个道岔编号, 其岔尖区段编号为 yy , 量词 zz 表示区段编号, 是第一个道岔编号的定位或反位区段编号, 其定、反位取决于 xx 。根据站场拓扑结构, 进路方向为 0 的进路编号, 其包含的第一个区段编号一定是左链接为道岔编号、右链接为区段编号, 根据此性质, 验证了进路编号 - 进路方向编号数据。

5 配置数据的形式化验证

5.1 验证原理

在本文第 4 节中, 定义了很多数据需要满足的规则, 对每一个规则的验证都可以看作一个约束可满足求解, 每一个规则的形式化表达式可抽象为如公式 (13) 所示的表达式

$$A_1 \wedge A_2 \wedge \dots \wedge A_{n-1} \wedge A_n \Rightarrow B_1 \wedge B_2 \wedge \dots \wedge B_{n-1} \wedge B_n \quad (13)$$

公式 (13) 中, A_1, B_1 是谓词, 故蕴含符号的前件可由 n 个谓词表达式组成, 后件也可由 n 个谓词表达式组成, n 为正整数。对这样一个形式化表达式的求解, 可转化为如公式 (14) 所示的表达式。

$$F = \neg A_1 \vee \neg A_2 \vee \dots \vee \neg A_{n-1} \vee \neg A_n \vee B_1 \vee B_2 \vee \dots \vee B_{n-1} \vee B_n \quad (14)$$

3) 第三种类型规则

在第一种和第二种类型规则中, 其整个形式化表达式的前件, 都有使用谓词表达进路方向。而根据霍尔逻辑, 前件中所有谓词的布尔值若为假, 那么整个表达式为真, 因此需要将进路编号所对应的进路方向编号描述在后件中, 以验证进路方向编号是否正确, 故引入第三种类型规则, 编号 10 与编号 9 的表达类似。如图 9 所示, 给出了规则编号 9 形式化表达。

表达式 F 的数学逻辑意义为析取范式 F , 故对形式化表达式的逻辑真假值的求解就转化为对析取范式 F 的逻辑真假值的求解, 这就是自动化约束求解工具的内部求解原理。本文选取的 ProB 模型检验器 (也是约束求解器), 将每一个规则的形式化表达式中的关键量词实例化, 实例化后的量词, 会给出析取范式的真假值, 这样可进一步准确分析错误源, 进而修正错误。

5.2 验证结果及分析

将本文表 1 实例化后, 信号对象如表 3 所示。

表3 实例化后的表1

Tab.3 Instantiated table 1

信号对象	编号
区段	-1 表示尽头, 0-74 表示站场拓扑有 75 个轨道区段
道岔	$P_{75}-P_{98}$, 表示站场拓扑有 24 个道岔
信号机	S_0-S_{31} , 表示站场拓扑有 32 个信号机
进路	R_1-R_{64} , 表示生成了 64 条进路

表 3 给出本实际案例中的各个信号设备对象的个数, 本案例共描述 49 个形式化表达式, 在 ProB 1.9.3 版本运行结束后, 验证报错。经过检查, 错误进路编号 - 信号机编号 27-64 中, 信号机编号为 24, 27, 30 号所对应的区段编号有错误, 与现场数据设计人员反馈后, 实际情况是在验证规则中没有考虑到区段偏移。

修正后，再次运行验证，又发现错误，如图 10 所示。经过检查，发现在 Excel 表中编写的进路编号 - 进路方向编号中的进路方向编号有误，与现场

数据设计人员反馈后，实际上 1-27 号进路还没有开通，进路编号为 14-16 所对应的进路方向编号有误。

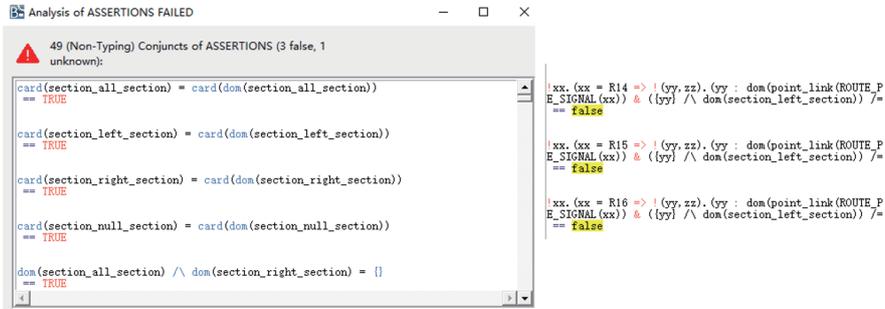


图10 进路方向编号有误
Fig.10 The route direction number is incorrect

修正后再次运行验证，结束后，如图 11 所示，没有再发现错误。验证所有的形式化表达式的逻辑值都为真，至此，数据的静态正确性检测已完成。

5.3 验证小结

基于本文的设计、定义、验证、分析过程，总结数据的形式化验证方案有如下优点。

1) 验证严谨：使用无歧义的数学逻辑符号描述

数据静态规则；

2) 规则可维护性和可扩展性好：编写修改灵活，如果更换开发人员，只要理解形式化数学符号，就能看懂规则；

3) 验证分析过程的直观性好：利用 ProB 模型检验器，能够直观的定位到错误的位置；

4) 验证成本低：体现在验证速度非常快。

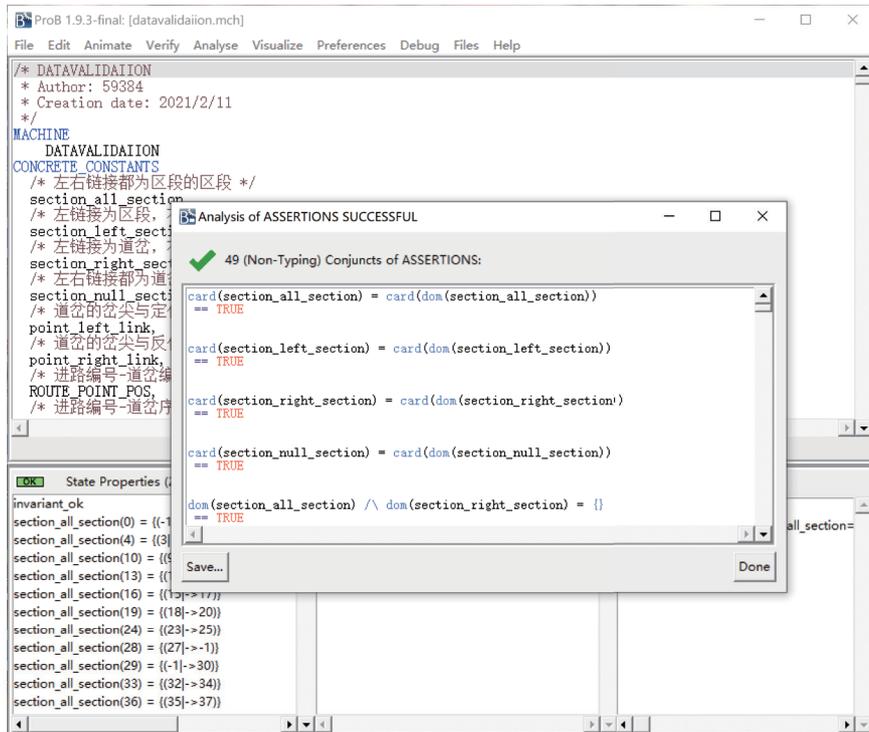


图11 正确的验证结果
Fig.11 Correct verification results

6 结论

本文以轨道交通控制系统配置数据为例, 基于 B 方法建立配置数据静态规则原型, 并进行形式化验证。本方法有助于发现并纠正轨道交通控制系统配置数据存在的错误, 减少因配置数据错误而引发系统缺陷, 验证后的配置数据可以作为系统正常运行的基础, 减少了数据测试阶段的成本投入。未来的研究方向可以考虑针对数据关系更为复杂的配置数据, 研究基于一阶逻辑和集合论的 B 语言如何实现对其的描述, 以及考虑更多场景的应用。

参考文献

- [1] 赵洪军. 轨道交通列车运行控制系统研发集成企业质量成本管理概述 [J]. 铁路通信信号工程技术, 2020, 17(10): 93-98.
Zhao Hongjun. Overview of Quality Cost Management of Enterprise for Development and Integration of Rail Operation Control System[J]. Railway Signalling & Communication Engineering, 2020, 17(10): 93-98.
- [2] Butler RW. What is Formal Methods? [OL]. Washington, United States: NASA, 2021(2021-01-20)[2022-03-01]. <http://shemesh.larc.nasa.gov/fm/fm-what.html>.
- [3] Leuschel M, Falampin J, Fritz F, et al. Automated Property Verification for Large Scale B Models with ProB[J]. Formal Aspects of Computing, 2011, 23(6): 683-709.
- [4] Hansen D, Schneider D, Leuschel M. Using B and ProB for Data Validation Projects[M]//Lecture Notes in Computer Science. Cham:Springer International Publishing, 2016: 167-182.
- [5] Leuschel M, Butler M. ProB: an Automated Analysis Toolset for the B Method[J]. International Journal on Software Tools for Technology Transfer, 2008, 10(2): 185-203.
- [6] Iliasov A, Romanovsky A. SafeCap Domain Language for Reasoning about Safety and Capacity[C]//2012 Workshop on Dependable Transportation Systems/Recent Advances in Software Dependability. November 18-19, 2012, Niigata, Japan: IEEE, 2012:1-10.
- [7] Stankaitis P, Iliasov A. Safety Verification of Modern Railway Signalling with the SafeCap Platform[C]//2017 IEEE International Symposium on Software Reliability Engineering Workshops. October 23-26, 2017, Toulouse, France: IEEE, 2017: 153-156.
- [8] Iliasov A, Taylor D, Laibinis L, et al. Formal Verification of Signalling Programs with SafeCap[C]//Computer Safety, Reliability, and Security, 2018, Västerås, Sweden: Springer, 2018: 91-106.
- [9] 张紫菡. CTCS-1 级列控系统线路数据的生成及验证方法的研究 [D]. 北京: 北京交通大学, 2020.
- [10] 姚文华, 侯锡立, 贾云光, 等. 有轨电车信号控制系统技术方案 [J]. 铁路通信信号工程技术, 2021, 18(4): 59-63.
Yao Wenhua, Hou Xili, Jia Yunguang, et al. Technological Scheme of Signalling Control System for Tram[J]. Railway Signalling & Communication Engineering, 2021, 18(4): 59-63.
- [11] 温业中, 黄仁欢, 杨建华, 等. 有轨信号控制系统的研究与实现 [J]. 铁路通信信号工程技术, 2019, 16(3): 51-55.
Wen Yezhong, Huang Renhuan, Yang Jianhua, et al. Research and Implementation of Tram Signal Control System[J]. Railway Signalling & Communication Engineering, 2019, 16(3): 51-55.
- [12] Abrial J R, Hoare A, Chapron P. The B-Book[M]. Cambridge: Cambridge University Press, 1996.
- [13] Kumar V. Algorithms for Constraint-Satisfaction Problems: a Survey[J]. AI Magazine, 1992, 13(1): 32-44.