

Machine Verification of the Existence Theorem of Configuration 7_3 Based on Alloy

Yue Xu¹, Jianguo Jiang¹, Ke Zou¹, Xingang Zhang²

¹School of Mathematics, Liaoning Normal University, Dalian Liaoning

²School of No. 24 High School, Dalian Liaoning

Email: xuyuebox@163.com, jjgbox@sina.com, 756592738@qq.com, 52904097@qq.com

Received: Nov. 10th, 2017; accepted: Nov. 22nd, 2017; published: Nov. 29th, 2017

Abstract

The existence of the configuration 7_3 is a basic problem in finite geometry. This paper presents a method for automatically verifying the existence of configuration 7_3 using an Alloy analyzer. This method uses Alloy language to formalize Fano's axiom system and the need to validate the theorem, and then uses the Alloy analyzer to analyze whether the theorem satisfies the attribute requirement. It is shown that the proposed method of verification is feasible.

Keywords

Configuration 7_3 , Finite Geometry, Alloy, Machine Verification

基于Alloy的 7_3 构形存在性定理的机器验证

徐月¹, 江建国¹, 邹科¹, 张新钢²

¹辽宁师范大学数学学院, 辽宁 大连

²大连市第二十四中学, 辽宁 大连

Email: xuyuebox@163.com, jjgbox@sina.com, 756592738@qq.com, 52904097@qq.com

收稿日期: 2017年11月10日; 录用日期: 2017年11月22日; 发布日期: 2017年11月29日

摘要

7_3 构形的存在性是有限几何中的一个基本问题。本文给出了一种用Alloy分析器自动验证 7_3 构形的存在性的方法。该方法使用 Alloy语言对Fano提出的公理系统和需要验证的定理进行形式化, 然后利用Alloy分析器分析定理是否满足属性要求。实验结果表明本文提出的机器验证方法是可行的。

关键词

7₃构形, 有限几何, Alloy分析器, 机器验证

Copyright © 2017 by authors and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

构形的存在性问题是有限几何领域内一个主要的研究课题, 其研究方法和研究结果已在组合学、射影几何学、仿射几何学、拓扑学等领域得到广泛的应用[1] [2] [3]。特别是在射影几何学中, 其研究方法对不同维数射影平面的研究起到至关重要的作用。

历史上, 数学家们对构形的存在性问题进行过研究。1876年, Reye首次提出构形的概念[4] [5], 即构形是点和线之间满足某些条件的有限关联结构。随后, Reye证明了 $v_3 (7 \leq v \leq 14)$ 构形是存在的。数十年后, Martinetti用递归法验证了 $v_3 (7 \leq v \leq 14)$ 构形的存在性[6]。1892年, 意大利数学家Fano给出了含有6条公理的公理系统[7], 并证明了7₃构形存在性问题。近年来, 许多专家和学者提出了多种验证点线数较小的构形存在性问题的方法, 并取得了丰硕的成果[8] [9] [10]。

随着构形中点线数目不断增多, 构形存在性问题的验证就会变得十分困难。为此, 我们提出利用计算机对此问题进行机器验证的思想。在本文中, 我们尝试用Alloy分析器[11]来验证一个比较简单的构形存在性问题, 即: 7₃构形的存在性问题。Alloy [12] [13]是一个表达能力很强的关系逻辑建模语言, 我们发现这种语言非常适合用于建模构形存在性问题。另外, Alloy的分析器是一个完全自动的模型查找工具, 它能够地在有限范围内非常高效查找满足约束条件的模型。我们希望Alloy的这两个特性对人们验证更难的构形存在性问题有所帮助, 更希望它能够成为一个帮助人们攻克构形存在性猜想的利器。

本文结构如下: 第1节具体介绍7₃构形和构形的相关知识; 第2节介绍Alloy建模语言以及Alloy分析器的分析方法; 第3节对Fano公理系统进行建模, 然后使用Alloy分析器对模型进行分析验证; 第4节为结论, 并给出有待于进一步研究的工作。

2. 相关知识

有限几何中的主要研究对象是点、线之间的关联结构, 在引入关联结构的概念之后, 对构形的概念作详细的介绍。

定义 1 设 V 与 B 为两个不相交的集合, i 为 V 与 B 之间的一个二元关系, 即 $I \subseteq V \times B$, 则称 $\Pi = (V, B, I)$ 为一个关联结构。 V 的元素叫做点, B 的元素叫作直线, i 叫作关联关系。设 $p \in V$, $B \in B$, 若 $(p, B) \in I$, 则称“点 p 在直线 B 上”或“直线 B 经过点 p ”并记作 pIB 。

本文只讨论有限关联结构, 即 V 与 B 都是有限集的关联结构。当 $\Pi = (V, B, I)$ 为有限关联结构时, 常以 v 表示集合 V 的基数, 以 b 表示集合 B 的基数, 即 $v = |V|$, $b = |B|$, 并称 v 为 V 的阶。

定义 2 (v, b_k) 构形是满足如下性质的有限关联结构。

- 1) 存在 v 个点和 b 条直线;
- 2) 每条直线上含有 k 个点, 每个点经过 r 条直线;
- 3) 任意两条直线至多有一个交点, 两点间至多存在一条直线。

解决 (v_r, b_k) 构形问题的前提是验证构形是否是存在的, 下面给出构形存在性的必要条件。

引理 3 若 (v_r, b_k) 构形存在, 则以下条件成立:

- 1) $v \leq b$ 且 $k \leq r$;
- 2) $vr = bk$;
- 3) $v \geq r(k-1)+1$ 。

在上述定义 2 中, 若 $v = b$ (即 $k = r$), 则称为对称构形, 简记为 v_k 构形。

v_k 构形是有限几何中研究的主要问题, 目前人们用不同的数学方法对 v_k 构形的存在性问题进行研究, 取得了重要的成果。

本文具体研究的 7_3 构形是 v_k 构形中的一种, 是最基本的构形问题。在这里, 点的个数为 7, 线的个数为 7, 每条线经过 3 个点, 每个点经过 3 条线。经验证, 7_3 构形满足构形存在性的必要条件。1892 年, Fano 给出满足 7_3 构形的图形如图 1 所示。

同时 Fano 用数学的方法对图形做进一步的分析, 即得 7_3 构形的七个点分别是三角形的重心、三个顶点以及三边中点, 七条线分别是三角形的三条边、三条中线以及三边中点的圆周。

由于 7_3 构形是含点个数为 7 的有限结构, 同时 Alloy 分析器恰好是在有限范围内查找模型, 以此我们可以用 Alloy 分析器来验证 7_3 构形的存在性。

3. Alloy 建模语言及 Alloy 分析器

在前面提到的体系构架中, Alloy 建模语言是公理系统形式化的表达方式, 利用 Alloy 建模语言描述的公理系统在 7_3 构形验证的过程中具有重要的作用, 下面将简单介绍 Alloy 建模语言。

Alloy 是由 MIT 软件设计工作组于 1997 年设计出原型的, 已在多个领域中应用。Alloy 是基于关系的一阶逻辑语言, 同时也是轻量级的、描述性的、说明性的建模语言。Alloy 建模语言综合了模型检验和语义蕴含的优点, 模型检验使得验证自动化, 而语义蕴含使得建模语言对系统模型描述的更加简洁。这两个优点使得 Alloy 成为非常有效的形式化语言。

一个典型的 Alloy 模型是由一系列签名(signature)、域(field)、事实(fact)、谓词(predicate)和断言(assert)组成。签名表示一类原子的集合, 在其中可以包含域声明(表示签名之间的关系); 事实和谓词都是对签名之间的约束条件, 其中事实要求签名之间的约束关系总是成立的, 谓词是可以拥有参数的约束条件, 它可以用于事实中; 断言是系统需要满足的属性。如果我们认定的属性系统不符合, Alloy 分析器就可以产生一个反例。

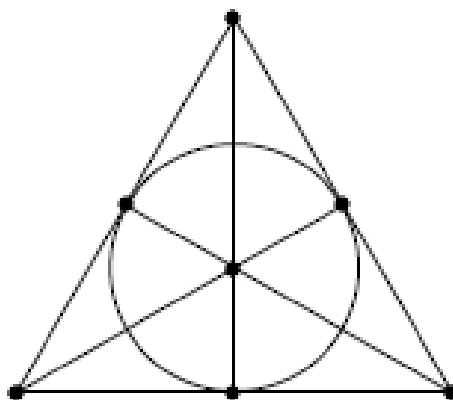


Figure 1. Configuration 7_3

图 1. 7_3 构形

Alloy 分析器是分析使用 Alloy 描述的模型的自动化分析工具。与 Alloy 是同时开发的，在当时只是个原型系统，功能十分有限。随着版本的增加和功能的改进，Alloy 分析器已经成为一个功能强大的分析工具。更重要的是，Alloy 分析器提供了可视化的模型实例来帮助建模人员分析模型，这种直观的感受是其他模型分析工具所不具备的。到目前为止，Alloy 分析器已经被用于多个领域，包括网络配置[14]，抽象代数的群理论[15]等。

Alloy 分析器的分析原理是约束求解的过程。无论是通过 run 命令查找一个实例还是通过 check 命令查找一个反例。所以，Alloy 分析器其实是一个一阶逻辑的约束求解器。但是在 Alloy 分析器在实际实现中是不可能直接求解约束的，它是通过将约束转换为一个布尔表达式，然后使用现有的 SAT 求解器来求解该约束。SAT 求解器给转换成的布尔表达式赋值来满足该布尔表达式，即通过各种赋值使得布尔表达式成立。Alloy 分析器提供了 MiniSat、SAT4J、Zchaff 等多个 SAT 求解器可供选择，默认的是 SAT4J 求解器。

4. 模型的建立与验证

首先，我们给出有限几何的 Fano 公理系统。然后，使用 Alloy 建模语言对公理系统和需要验证的定理进行建模。最后，在计算机上用 Alloy 分析器对定理进行分析、验证。

Fano 公理系统 A 由下列 6 条公理组成：

- 公理 1 两点确定一条直线；
- 公理 2 每条直线上至少包含 3 个点；
- 公理 3 平面上至少存在一条直线；
- 公理 4 不是所有的点都在同一条直线上；
- 公理 5 两条直线有且只有一个交点；
- 公理 6 每条直线上至多包含 3 个点。

Fano 用此公理系统证明了 7_3 构形的存在性定理：

定理 平面上存在 7 个点，存在 7 条直线。

Veblen 证明了 7_3 构形中的七条线不能都用直线画出，须含有一条曲线。但它并不影响结果，只是表示点线之间的关联结构，满足构形的定义。即图 1 所示。

由 Alloy 建模语言的特点，我们将公理形式化。公理系统的实质是点集、线集以及点线之间的关联关系(点在线上或者说线包含点)，首先我们可以定义点集，线集为签名，并将点线之间的关系作为域声明给出，同时约束点和线在构形中，即：

```
sig Point{ }
sig Line{
  hasPoints : set Point
}
One sig configuration {
  points : set Point,
  lines : set Line
} {
  all p : Point | p in points
  all l : Line | l in lines
}
```

其次，约束完点线后，我们知道点线之间必须满足所有的公理条件。因为公理总是成立的，所以我们将公理约束在事实中，即：

```
fact axiom1{
  all disj p1, p2 : Point | one l : Line | p1 in l.hasPoints
  and p2 in l.hasPoints
}
fact axiom2{
  all l : Line | # l.hasPoints >= 3
}
fact axiom3{
  #configuration.lines >= 1
}
fact axiom4{
  all l : Line | some p : Point | not p in l.hasPoints
}
fact axiom5{
  all disj l1, l2 : Line | one p : Point | p in l1.hasPoints
  and p in l2.hasPoints
}
fact axiom6{
  all l : Line | #l.hasPoints <= 3
}
```

最后，我们使用断言表述定理为：

```
assert theorem{
  #configuration.lines = 7
  #configuration.points = 7
}
check theorem for 10 Point, 10 Line
```

`check` 命令用于检测断言在规定的范围内是否成立，若断言成立，系统不会产生反例；若断言不成立，系统会产生一个违反断言的实例，即反例。这样我们可以用 `check` 命令来验证所需要的定理是否成立。如果出现反例，我们可根据提供的反例快速找到错误的根源。

要注意的是，通常情况下，若没有出现反例，并不能表示就没有反例。但对于每个属性的验证是在一定范围内对所有的实例进行穷举式的检查，所以若没有出现反例时，就可以判断在该范围内所有的实例这个属性是成立的。另外，根据 Alloy 分析器针对小范围假设原理[16]得到的结果显示，大部分的错误在小范围内的实例中就可以检查出来，因此我们可以将要验证的范围进行扩大，若仍没有反例则我们可以得到经过验证后的定理属性基本是成立的。

基于此，我们不断扩大范围，重复做大量实验，得到结果如表 1。

Table 1. Theorem property range validation table

表 1. 定理属性范围验证表

点线数量 (点数, 线数)	10,10	15,15	20,20	30,30	50,50	70,70	100,100
运行时间 (秒)	0.078	0.094	0.156	0.515	2.525	7.370	13.693
有无反例	无	无	无	无	无	无	无

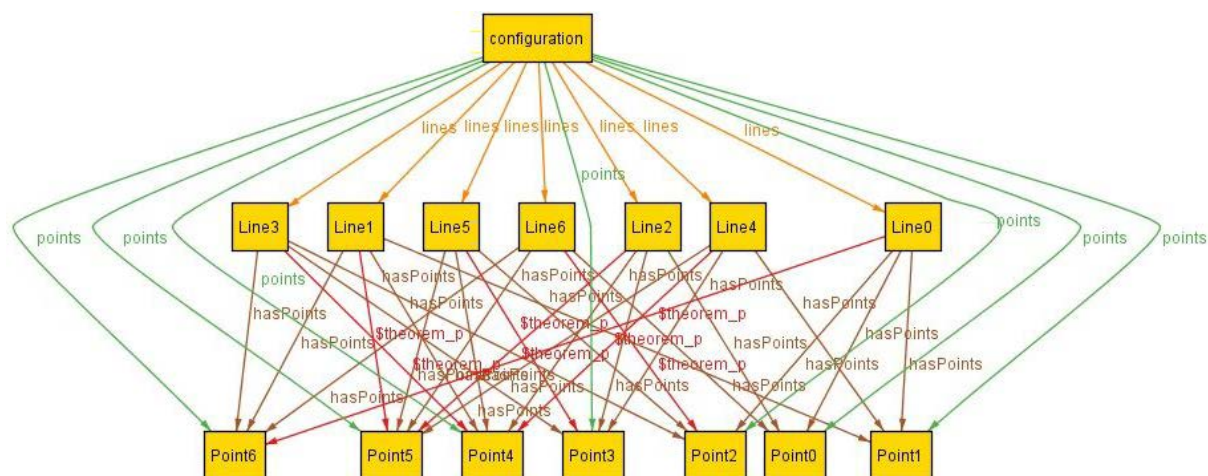


Figure 2. Feasibility examples

图 2. 可行性实例

则由小范围假设原理，可以验证该定理是可行的。

根据需求，我们可以将断言改为谓词。在 Alloy 分析器中 run 命令是用于查找满足属性的实例是否存在，因此我们可以应用 run 命令来查找实例，即：

```

pred theorem{
  #configuration.lines = 7
  #configuration.points = 7
}
run theorem for 10 Point, 10 Line

```

运行后产生的实例如图 2 所示。

它包含 7 点 7 线，同时满足每条线上有 3 个点，每个点经过 3 条直线。分析后即著名的 7_3 构形，即图 1。

5. 结语

虽然 7_3 构形存在性问题是有限几何中一个比较简单的问题，数学家们早已对此问题给出了严格的数学证明，但我们使用 Alloy 分析器给出了一种新的机器验证方法。虽然我们的方法并不完备，不能代替严格的数学证明，但却为更难的构形存在性问题提供了一种新的求解思路。

参考文献 (References)

- [1] Gropp, H. (2004) Configuration between Geometry and Combinatorics. *Discrete Applied Mathematics*, **138**, 79-88. [https://doi.org/10.1016/S0166-218X\(03\)00271-3](https://doi.org/10.1016/S0166-218X(03)00271-3)
- [2] Sturmfels, B. (1991) Computational Algebraic Geometry of Projective Configuration. *Journal of Symbolic Computation*, **11**, 595-618. [https://doi.org/10.1016/S0747-7171\(08\)80121-6](https://doi.org/10.1016/S0747-7171(08)80121-6)
- [3] van Straten, M.P. (1948) The Topology of the Configurations of Desargues and Pappus. *Rep. Math. Colloquium*, 3-17.
- [4] Gropp, H. (1990) On the History of Configuration. In: Diez, A., Ed., *Internet, Symposium on Structures in Math, Theories*, Bilbao, 263-268.
- [5] Gropp, H. (1994) On Symmetric Spatil Configurations. *Discrete Mathematics*, **125**, 201-209. [https://doi.org/10.1016/0012-365X\(94\)90161-9](https://doi.org/10.1016/0012-365X(94)90161-9)
- [6] Kantor, S. (1881) Die Configurationen $(3,3)_{10}$. *Sitzungsber Akad Wiss Wien Math Natural Kl*, **84**, 1291-1314.

-
- [7] Fano, G. (1892) Sui Postulate Fondamentali Della Geometria Proiettiva. *Giornale di Matematiche*, **30**, 106-132.
- [8] Coxeter, H.M. (1983) My Graph. *Proceedings of the London Mathematical Society*, **s3-46**, 117-136. <https://doi.org/10.1112/plms/s3-46.1.117>
- [9] Grünbaum, B. and Rigby, J.F. (1990) The Real Configuration (21₄). *Journal of London Mathematical Society*, **41**, 336-346. <https://doi.org/10.1112/jlms/s2-41.2.336>
- [10] Grünbaum, B. (2006) Configurations of Points and Lines. Davis, C. and Ellers, W.W., Eds., American Mathematical Society, Rhode Island, 179-225.
- [11] Jackson, D. (2000) Automating First-Order Relational Logic. *ACM SIGSOFT Software Engineering Notes*, **25**, 130-139. <https://doi.org/10.1145/357474.355063>
- [12] Jackson, D. (2006) Software Abstractions: Logic, Language, and Analysis. The MIT Press, Cambridge.
- [13] Jackson, D. (2002) Alloy: A Language & Tool For Relational Models. <http://alloy.mit.edu/alloy>
- [14] Khurshid, S. and Marinov, D. (2004) TestEra: Specification-Based Testing of Java Problems Using SAT. *Automated Software Engineering*, **11**, 403-434. <https://doi.org/10.1023/B:AUSE.0000038938.10589.b9>
- [15] Narain, S. (2004) Network Configuration Management Via Model Finding. *Conference on Large Installation System Administration Conference*, **2**, 15.
- [16] Andoni, A., Daniliuc, D., Khurshid, S. and Mariniv, D. (2002) Evaluating the “Small Scope Hypothesis”. *POPL Proceedings of ACM Symposium on the Principles of Programming Languages*, MA, 1-12.

知网检索的两种方式:

1. 打开知网页面 <http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD>
下拉列表框选择: [ISSN], 输入期刊 ISSN: 2324-7991, 即可查询
2. 打开知网首页 <http://cnki.net/>
左侧“国际文献总库”进入, 输入文章标题, 即可查询

投稿请点击: <http://www.hanspub.org/Submission.aspx>

期刊邮箱: aam@hanspub.org