1.

2018 届研究生硕士学位论文

分类号：_____ 学校代码：10269

密　级：_____ 学　　号：51151500079

華東師範大學

East China Normal University

硕 士 学 位 论 文

MASTER'S DISSERTATION

论文题目：
自主移动机器人空间永恒探索算法的符号模型检测方法

院　　系：	计算机科学与软件工程学院
专 业 名 称：	软件工程
研 究 方 向：	高可信计算理论与技术
指 导 教 师：	张民 副教授
学位申请人：	蔡晓伟

2017 年 11 月

Dissertation for master degree in 2018 University Code: 10269

Student ID: 51151500079

EAST CHINA NORMAL UNIVERSITY

On Symbolic Model Checking of Mobile Robots Perpetual Exploration Algorithm

Department:	School of Computer Science and Software Engineering
Major:	Software Engineering
Research direction:	Trustworthy Computing Theory and Technique
Supervisor:	Assoc Prof. Zhang Min
Candidate:	Cai Xiaowei

2017.11

华东师范大学学位论文原创性声明

郑重声明：本人呈交的学位论文《自主移动机器人空间永恒探索算法的符号模型检测方法》，是在华东师范大学攻读硕士/博士（请勾选）学位期间，在导师的指导下进行的研究工作及取得的研究成果。除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。

作者签名:_____ 日期: 年 月 日

华东师范大学学位论文著作权使用声明

《自主移动机器人空间永恒探索算法的符号模型检测方法》系本人在华东师范大学攻读学位期间在导师指导下完成的硕士/博士（请勾选）学位论文，本论文的研究成果归华东师范大学所有。本人同意华东师范大学根据相关规定保留和使用此学位论文，并向主管部门和相关机构如国家图书馆、中信所和“知网”送交学位论文的印刷版和电子版；允许学位论文进入华东师范大学图书馆及数据库被查阅、借阅；同意学校将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于（请勾选）

（）1. 经华东师范大学相关部门审查核定的“内部”或“涉密”学位论文 *，于年月日解密，解密后适用上述授权。

（）2. 不保密，适用上述授权。

导师签名:_____ 本人签名:_____

年 月 日

* “涉密”学位论文应是已经华东师范大学学位评定委员会办公室或保密委员会审定过的学位论文（需附获批的《华东师范大学研究生申请学位论文“涉密”

审批表》方为有效），未经上述部门审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权）。

蔡晓伟 硕士学位论文答辩委员会成员名单

姓名	职称	单位	备注
朱惠彪	教授	华东师范大学	主席
章玥	副教授	华东师范大学	无
毛宏燕	副教授	华东师范大学	无

摘　要

随着物联网技术的发展, 自主移动机器人 (autonomous mobile robots) 在网络中的作用也日益重要, 利用形式化的方法验证自主移动机器人行为的正确性逐渐成为新的研究热点. 当前主要的验证方法多以初始状态已知为前提且面临状态爆炸问题. 本文以自主移动机器人空间永恒探索算法为例, 提出自主移动机器人符号模型检测方法, 该方法不依赖某个具体的初始状态, 且适用于不同的同步模型. 同时, 借助符号模型检测的高效性, 有效避免状态爆炸问题. 利用 nuXmv 符号模型验证工具对机器人探索算法在三种同步模型: 完全同步模型 FSYNC(Full-synchronous model)、半同步模型 SSYNC(semi-synchronous model)、异步模型 ASYNC(Asynchronous model) 进行建模并利用 LTL 公式定义算法的性质, 最终实现算法的形式化验证. 验证结果表明在假设初始状态未知的条件下依然可验证性质不被满足并找到反例. 同时, 实验数据表明了符号模型检测对自主移动机器人算法形式化验证的可行性与高效性.

关键词: nuXmv，移动机器人，空间探索，符号模型检测，形式化验证

ABSTRACT

With the development of Internet of Things technology, the role that autonomous mobile robots play in the network is becoming increasingly important. Formal verification of the correctness of autonomous mobile robots has become a new research topic. Most of the exising approaches either suffer state-explosion problem or rely on concrete initial states, which however are usually not undefined and have to be enumerated to make verification complete. In this paper, we propose a symbolic model checking approach to the formal verification of a typical automonous mobile robot system called mobile robot perpetual exploration system. For the symbolicity feature of the model checking, the verifcation does not rely on specific initial states and meanwhile state-explosion problem can be avoided. We use the state-of-the-art symbolic model checker nuXmv to verify the mobile robot perpetual exploration algorithm under three different scheduling modes called full synchronous model (FSYNC), semi-synchronous model (SSYNC) and asynchronous model (ASYNC). Experimental results show that even without providing specific initial states a counterexample can be found in our approach for the perpetual exploration property, which concides with the existing verification result which is obtained by model checking with specific initial states. Meanwhile, the experimental data shows the feasibility and efficiency of symbolic model checking in the formal verification of autonomous mobile robot systems.

Keywords: *nuXmv, LTL, Mobile robots, space exploration, symbolic model checking*

目录

第一章　绪 论

1.1　研究背景与意义

1.2　国内外研究现状

1.3　研究内容和方法

1.4　论文结构

本文结构具体如下：

第一章介绍了自主移动机器人空间探索问题在当前和未来实际应用中的重要性和该领域取得的成果与发展。自主移动机器人空间探索算法的核心问题是根据具体的的物理空间如何定义自主移动机器人的行为以保证其完成预设的任务. 针对该问题，目前主要使用手动推演与模型检测技术，以验证自主移动机器人算法或协议满足一定的性质。对于稍微复杂一点的移动算法或者移动协议，手动推演的方式，不仅过程冗长复杂，而且容易出现错误或者疏漏。尤其是异步模型调度的情况下，手动推演方法根本就无法进行验证。模型检测技术具备自动性、严谨性和高效性，逐渐被用于各种自主移动机器人算法的验证中。并引出 nuXmv 实现符号模型检测的方法用于自主移动机器人探索算法或协议的建模与验证。

第二章对 nuXmv 语言进行详细介绍，包括 nuXmv 的基础语法、表达式、几种常用的关键字，模块组件、异步系统模型。并对 nuXmv 中线性时序逻辑 (LTL) 模型检测进行了介绍。详细介绍了线性时序逻辑 (LTL) 在 nuXmv 中的使用。

第三章以自主机器人永恒空间探索协议为例，详细描述在环形空间模型中机器人、空间路径、位置结点等的数学定义。在此基础上，使用 nuXmv 对自主移动

机器人算法或协议在三种不同调度策略下模型的构建。具体介绍了使用 LTL 公式描述永恒探索性。

第四章本章在模型创建的基础上，分别在三种调度策略的情况下，利用 nuXmv 提供的基于 BDD 方法及 SMT 方法实现了机器人探索协议的符号模型检测，验证不同机器人数和图结点数下，协议是否满足永恒探索的需求. 当出现不满足情况时,nuXmv 给出不满足的状态路径作为反例, 分析性质不被满足的具体原因.

第五章对全文工作做了总结。对实验方法和验证结果进行了分析，总结本文的主要贡献。讨论了 nuXmv 符号模型检测在空间探索协议验证的 BDD 方法和 SMT 方法的选择性，指出了本文工作中的一些不足点，对未来自主机器人领域的研究内容进行了展望。

第二章　nuXmv 的介绍

nuXmv 是一种新的符号模型检测器，支持有限状态系统和无限状态系统的建模分析。nuXmv 继承 NuSMV，支持所有的 NuSMV 的功能。在 NuSMV 功能基础上，不仅在限状态系统和无限状态系统两个方面增加了新的特性，还在其他方面进行了提升。NuSMV 是在一种基于 BDD 算法实现的 SMV 验证器上进行重新实现和功能拓展所得出验证工具。NuSMV 被设计成一种开放式的模型检测框架，作为一个高可信的验证工具被广泛的应用于工业设计以及其他研究领域。在 NuSMV2 版本中，功能得到进一步提升，不仅具备原来由科罗拉多大学研发的 BDD 算法模型检测组件，而且添加了 SAT 模型检测组件，SAT 模型检测组件中包含基于 RBC 的边界模型验证器。到了 2.5.0 版本，热那亚大学为 NuSMV 捐献了 SIM，SIM 中包含最新的 SAT 算法解析器，其中的 RBC 软件包支持边界模型检测算法。

同 NuSMV 相比较，nuXmv 为状态和输入变量新增两种数据类型实数 (real) 和整数 (integer), 这使用户能够对无限状态转换系统的规范进行建模。添加了新的结构，用于指定抽象技术中谓词。nuXmv 不仅支持所有的 NuSMV 交互式命令，而且添加一些新特性对应的新的操作命令，应用于有限状态转移系统中新的模型检测算法和无限状态转移系统中基于 SMT 的新的检测算法。

nuXmv 支持计算树逻辑 (CTL) 和线性时态逻辑 (LTL)，在 nuXmv 代码中使用 CTL 或者 LTL 公式描述初始性质和验证性质，使得代码比较简洁、具备更强的表达能力。在无限状态系统验证过程中使用基于 SMT 的验证方法，大大提升验证的效率，特别是在验证不满足性时，可以高效的求得不满足的反例。nuXmv 不仅可

以构建同步系统模型，而且可以构建异步系统模型，满足一些系统建模的需求。由于 nuXmv 支持多种建模验证方式，用户可以按照自己的需求进行选择。

2.1

2.2 本章小结

第三章　机器人探索算法和调度策略

3.1　机器人和探索空间

3.1.1　探索空间定义

离散模型中，探索空间一般抽象为一个无向连通图，图的每个结点代表空间上机器人可达的位置，边代表机器人可以通过的路径，机器人沿着该路径到达相邻的空间位置。空间中每个位置结点在同一个时间至多只有一个机器人。

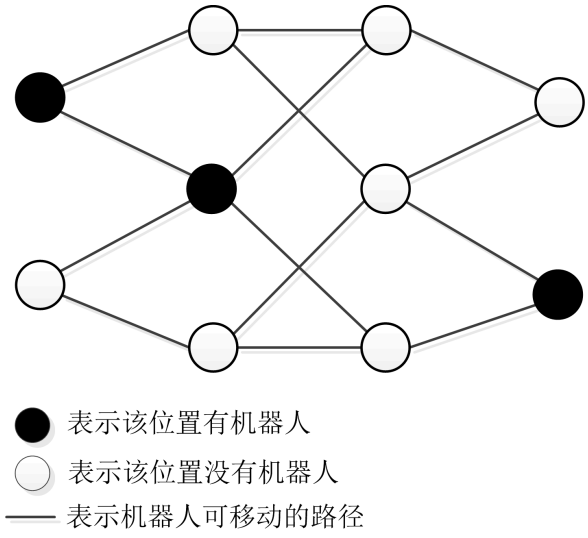

图 3.1: 无向连通图表示探索空间

如图3.1给出了一个简单的离散探索空间的无向连通图表示，黑色结点表示该空间位置在此刻有一个机器人，白色结点说明该空间位置上没有机器人，图中有三个机器人，分别位于三个黑色的空间结点上。类似于计算机网络拓扑结构，探索空间结构也有总线拓扑结构、星型拓扑结构、环形拓扑结构、树形拓扑结构等。

3.1.2 机器人移动三个阶段

离散空间上每个机器人的移动分为三个阶段，分别是观察 (look)、计算 (compute) 和移动 (move). 在观察阶段，机器人通过自身的视觉传感器，获取空间环境中其他机器人的位置快照信息。然后进入计算阶段，计算阶段根据观察阶段获取的位置快照信息，匹配自身预先设置的移动算法，计算得出下一步的移动策略。移动策略包括机器人是否移动，若是移动，则是沿着那条路径进行。移动阶段，机器人的动力装置按照计算阶段的所得移动决策作出对应的移动。

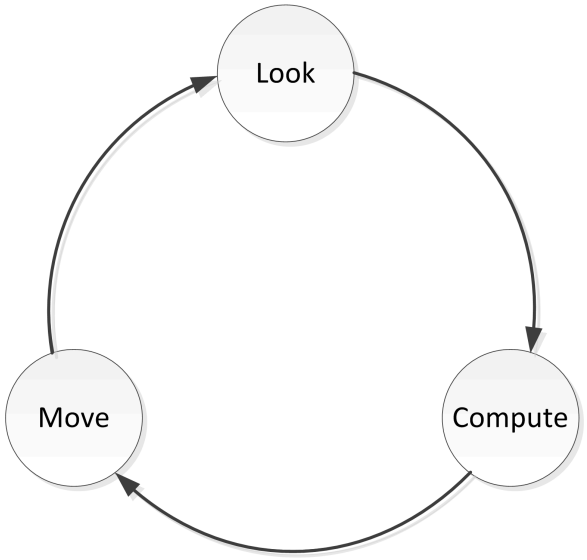

图 3.2: 机器人移动三阶段

如图3.2描述了机器人移动的三个阶段，这三个阶段按照观察阶段、计算阶段、移动阶段，完成移动阶段之后又进入观察阶段，这样不断重复三个移动阶段。

3.1.3 机器人移动调度模型

原有模式中，Suzuki 假设空间中机器人个数大于 0，机器人的移动三个阶段具有原子性，且机器人之间的运动过程是同步的，提出了移动调度策略的两种变体，分别是完全同步调度模型 FSYNC(fully-synchronous model) 和半同步调度模型 SSYNC(semi-synchronous model)。后来由 Flocchini 等人提出了异步调度模型 ASYNC (asynchronous model), 该异步调度模型中，机器人观察, 计算, 移动三个移

动阶段不再具备原子性，这样可能会出现机器人使用过时的快照信息做出移动决策。

下面使用数学和算法知识来描述完全同步调度模型、半同步调度模型、异步调度模型具体的内容。

假设在一个离散空间中存在 $k(k \in N^+)$ 个机器人，使用集合 $Rob = \{r_1, r_2, r_3, ..., r_k\}$ 表示。空间位置结点可以按照一定顺序，对其进行编号，编号是空间位置结点的唯一标识，使用集合 $Pos = \{n \in N^+ | 0, 1, 2, ..., n-1\}$ 表示空间所有空间位置结点，每个元素对应唯一一个空间位置结点。机器人是在空间位置结点上的，所以机器人与空间位置结点的映射关系使用 $p : \{Rob \to Pos\}$ 表示，机器人 r 在某个时间所在图中的位置结点编号就为 $p(r \in Pos$。对于 Rob 中的任意两个机器人 $r_i, r_j\,(i \neq j)$, 在任意一个时刻满足位置结点不相同 $p(r_i) \neq p(r_j)$, 即空间中任意时刻一个位子结点上至多只有一个机器人。

前面使用数学中的集合和映射定义了探索的离散空间、机器人已经机器人在空间结点上的函数关系，在此基础上，下面将介绍机器人移动的三种调度模型。完全同步调度模型是半同步调度模型的一种特殊情况，所以先介绍半同步调度模型，在介绍完全同步调度模型。完全异步调度模型完全与前面两种调度模型由较大区别，所以放在最后介绍。

将机器人移动的一个完整的观察、计算、移动称为完整移动阶段，在半同步调度模型中，Rob 集合中只有选中的机器人才进行完整移动阶段。而半同步调度模型所有机器人都是同步而且观察、计算、移动都是具备原子性，所以可以每次选中的机器人是一个非空集合 $Sched \subseteq Rob$, 在一个完整移动阶段开始之前，只有选入集合 Sched 的机器人才会执行完整移动阶段，即 $\forall r \in Sched$ 执行观察、计算、移动，而 $\forall r \notin Sched$ 不执行。等到下一个完整移动阶段之前，又会从 Rob 随机选择一个机器人 $Sched \subseteq Rob$，重复上述过程。这就是半同步调度模型机器人调度的性质。下面使用简易算法过程，详细描述一下半同步调度模型中机器人执行完整移动阶段的过程。

```
1 SSYNC-SCHEDULE(Rob)
```

```
  while
    choose Sched from Rob
    synchronous {
       foreach r in Sched{
          r.look
          r.compute
          r.move
       }
    }
```

半同步调度模型 SSYNC-SCHEDULE 的传入参数是机器人集合 Rob, 首先从 Rob 集合中选择子集合 Sched 且 $Sched \neq \emptyset$。关键字synchronous 表示同步块中所有机器人同步完成移动阶段。在 Sched 集合中的每个机器人开始同步执行观察、计算、移动。完成之后，又重新开始随机选择子集合 Sched，重复不断执行上述过程。

完全同步调度模型是半同步调度模型中一种很特殊的情况，每次随机选择的集合 $Sched = Rob$, 即每次完整移动阶段之前在集合 Rob 中所有的机器人都被选中。使用算法过程描述如下：

```
FSYNC-SCHEDULE(Rob)
  while
    synchronous {
       foreach r in Sched{
          r.look
          r.compute
          r.move
       }
    }
```

同半同步调度模型相对较而言，完全同步调度模型只是在每次选择集合 $Sched$ 有所不同，其他过成完全相同。

而完全异步调度模型中，所有的机器人观察、计算、移动都是异步，没有原子性。类似于计算机系统的多线程，每个机器人的移动都是并行且互相之间没有同步约束，当一个机器人在观察时，其他机器人可能在执行计算或者移动。每个机器人执行移动的快慢完全是随机的，所以肯能会出现机器人在观察阶段通过视觉传感器获得快照是过时的。

```
ASYNC-SCHEDULE(Rob)
    asynchronous {
       foreach r in Rob{
```

```
4            while{
5                r.look
6                r.compute
7                r.move
8            }
9        }
10   }
```

上述完全异步调度模型算法中，关键字synchronous 表示 Rob 中所有的机器人都异步执行移动，对于每个机器人而言，都是在按照顺序不断重复执行观察、计算和移动过程，即整个过程中机器人都是并行执行完整移动阶段。

3.2 环形空间探索算法

探索空间结构有总线拓扑结构、星型拓扑结构、环形拓扑结构、树形拓扑结构, 不同的探索空间结构有各自的特点，本文以环形拓扑结构空间为例. 首先介绍环形拓扑结构环上的机器人视觉快照、匹配移动算法获取移动决策、移动决策的执行. 在此基础上, 将介绍永恒探索移动算法的相关概念.

3.2.1 机器人视觉快照

图**??**给出一个简单的环形拓扑结构探索空间的例子。根据环形空间的自身特点，沿着环的顺时针方向，从0 开始递增进行编号。所有位置编号组成的集合为Pos，图中黑色结点表示该位置结点上有机器人，白色结点表示该位置结点上没有机器人。下面给出某个时刻某个结点上机器人的数量的定义。

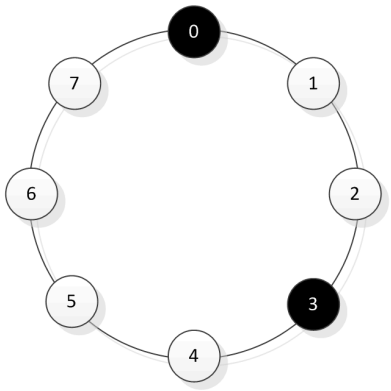

图 3.3: 环形拓扑结构探索空间

定义 1 (结点机器人个数) 结点机器人数 d_j，j 表示结点的编号 $j \in Pos$，当结点j 上有 $k\,(k>0)$ 机器人表示为 $d_j = k$, 当结点j 没有机器人时，表示为 $d_j = 0$。

在环形拓扑结构的离散空间中，空间中的每个机器人可以顺时针观察，也可以逆时针观察。那么机器人每次观察的位置信息快照就有顺时针位置信息快照和逆时针位置信息快照两种，为了方便描述，给出某个位置上机器人获取位置信息快照的定义，如下：

定义 2 (机器人快照) 离散空间上位置结点 $p \in Pos$，j 上的机器人通过视觉传感器获取的位置快照为 δ_p^F，其中 $F \in \{+,-\}$,+ 表示顺时针，-表示逆时针。

在拥有n 个位置结点的环形拓扑结构的探索空间上，任意位置结点j 上机器人的顺时针和逆时针快照如下：

顺时针序列定义： $\delta_p^+ = \langle d_j, d_{j+1}, ..., d_{j+n-1} \rangle$.

逆时针序列定义： $\delta_p^- = \langle d_j, d_{j-1}, ..., d_{j-n+1} \rangle$.

如图**??**中以位置编号为 0 的结点为例，其结点上机器人的顺时针和逆时针位置信息快照如下：

顺时针序列1： $\delta_0^+ = \langle 1,0,0,1,0,0,0,0 \rangle$.

逆时针序列1： $\delta_0^- = \langle 1,0,0,0,0,1,0,0 \rangle$.

虽然上述位置快照信息描述比较简洁和直观，但是当空间结点数 n 较大时，位置快照信息就过长，不利于描述。后来由 lelia.blin 在其文献 [Ring] 中提出了一种新的位置快照F-R 表达方式，F-R 表达方式中使用 F_m 表示连续的m 个空间位置结点上没有机器人，R_n 表示连续的n 个空间位置结点上有机器人。那么顺时针序列 1 和逆时针序列 1 转化为 F-R 的表达方式为：

顺时针F-R序列1： $\delta_0^+ = \langle R_1, F_2, R_1, F_4 \rangle$.

逆时针F-R序列1： $\delta_0^- = \langle R_1, F_4, R_1, F_2 \rangle$.

F-R 快照表达式中 F_m 和 R_n 的脚标值 m, n 都可以使用未知数表示，即可以限制 m, n 的取值范围，这样的表达十分灵活，描述性更强。