國防科学技術大学

全国优秀博士学位论文丛书

传值CCS和π-演算互模拟等价的验证理论和算法

李舟军 著

国防科技大学出版社

传值 CCS 和 π－演算互模拟等价的验证理论和算法

李舟军　著

国防科技大学出版社
·长沙·

图书在版编目(CIP)数据

传值 CCS 和 π－演算互模拟等价的验证理论和算法/李舟军著.—长沙:国防科技大学出版社,2005.4
(国防科学技术大学全国优秀博士学位论文;7/曾淳主编)
ISBN 7－81099－152－3

Ⅰ.传… Ⅱ.李… Ⅲ.电子计算机—算法理论 Ⅳ.TP301.6

中国版本图书馆 CIP 数据核字(2005)第 005572 号

国防科技大学出版社出版发行
电话:(0731)4572640 邮政编码:410073
E-mail:gfkdcbs@public.cs.hn.cn
责任编辑:耿 筠 责任校对:肖 滨
新华书店总店北京发行所经销
国防科技大学印刷厂印装
*
开本:787×1092 1/16 印张:12 字数:242 千
2005 年 4 月第 1 版第 1 次印刷
ISBN 7－81099－152－3/N·1
全套定价:280.00 元

序　言

当今世界，科学技术日新月异，科技创新已经成为社会生产力解放和发展的重要标志。科学技术的迅猛发展，正在引发一场广泛而深刻的军事变革，知识军事的时代已经来临。在新的历史条件下，面对世界新军事变革的严峻挑战，面对推进中国特色军事变革和军事斗争准备的紧迫需求，军队研究生教育的地位和作用比以往任何时候都更加突出。

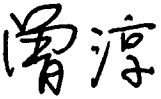
博士学位论文水平反映了高层次创新型人才培养的质量，同时学位论文也是博士生学科专业知识水平、特别是创新能力的集中体现。教育部每年评选100篇左右的全国优秀博士学位论文，作为国家21世纪教育振兴计划的重要内容，已成为提高研究生培养质量，鼓励创新，促进高层次创造性人才脱颖而出的重要措施。国防科技大学作为我军工程技术的最高学府，承担着为国家安全和军队信息化建设、研究开发国防高科技和先进武器装备、培养军队高级工程技术和指挥人才的重要历史使命，是我军实现新军事变革和军队信息化建设的人才培养和科学研究重要基地。提高人才培养的质量已成为我们现阶段迫切需要解决的问题之一。

自1999年教育部开展全国优秀博士学位论文评选以来，我校积极参加评选工作，并以全国优秀博士学位论文评选为契机，组织学校博士学位论文的评优工作，同时参加湖南省和军队优秀博士、硕士学位论文的评选，在我校研究生中大力倡导科学严谨的学风和勇攀高峰的精神，营造鼓励人才积极创新、支持人才实现创新的浓厚氛围，为学生的禀赋和潜能的充分开发创造一种宽松的环境。同时通过深化博士学位论文评阅制度改革；实施创新

工程，资助博士研究生创新研究；加强学校研究生指导教师队伍建设；建立激励机制，鼓励优秀人才脱颖而出等措施不断完善质量保证体系的建设。

博士学位论文是博士生学术水平、科研能力、创造性成果的集中体现，也是学校研究生教育水平、学术水平和创新能力的重要标志。全国优秀博士学位论文是我国优秀博士学位论文中的杰出代表，全国优秀博士学位论文作者是具有创造能力和竞争能力的高层次创造性人才，是支撑国家崛起的骨干创新力量。认真总结全国优秀博士学位论文的成功经验，对于进一步提高博士生教育的整体水平，培养数量更多、水平更高的高层次创造性人才，具有十分重要的启示作用。我校已有五篇博士学位论文获全国优秀博士学位论文，有五篇博士学位论文被评为全国优秀博士学位论文提名论文。现将这些优秀论文汇集出版，旨在为广大在学博士生及其导师树立高水平博士学位论文的范本和学习榜样，也期望进一步推动我校研究生教育改革的深入发展，以培养高层次创新性人才为目标，认真总结创新性人才的培养经验和方法，深入探讨博士生教育改革的思路和措施。

努力提高我军新型军事科技人才培养质量，为我校的快速发展和我军现代化服务，是我们今后一个阶段十分重要的任务。我们要在培养大批各类专业人才的同时，努力为优秀人才的脱颖而出创造条件。尤其要下功夫造就一批真正能站在世界科学技术前沿的学术带头人和尖子人才，以应对世界新军事变革的严峻挑战，为推进中国特色军事变革做出新的更大贡献。

国防科学技术大学研究生院 

2005 年 3 月于长沙

历届国防科学技术大学
全国优秀博士学位论文及
全国优秀博士学位论文提名论文

2001年三篇全国优秀博士学位论文：

信息与通信工程学科，王雪松博士的论文《宽带极化信息处理的研究》，导师庄钊文教授；

计算机科学与技术学科，王意洁博士的论文《面向对象数据库的并行查询处理与事务管理》，导师胡守仁教授；

控制科学与工程学科，王正明博士的论文《弹道跟踪自校准方法》，导师黄柯棣教授。

2004年二篇全国优秀博士学位论文：

机械工程学科，胡茑庆博士的论文《转子碰摩非线性行为与故障辨识的研究》，导师温熙森教授；

航空宇航科学与技术学科，黄玉辉博士的论文《液体火箭发动机燃烧稳定性理论、数值模拟和实验研究》，导师王振国教授。

2003年三篇全国优秀博士学位论文提名论文：

机械工程学科，刘耀宗博士的论文《碰摩转子混沌振动识别与控制技术研究》，导师温熙森教授；

计算机科学与技术学科，彭伟博士的论文《移动自组网络中的广播与路由技术研究》，导师卢锡城教授；

航空宇航科学与技术学科，黄玉辉博士的论文《液体火箭发动机燃烧稳定性理论、数值模拟和实验研究》，导师王振国教授。

2004 年二篇全国优秀博士学位论文提名论文：

原子与分子物理学科，曾交龙博士的论文《使用细致谱项模型研究铝等离子体的辐射不透明度》，导师袁建民教授；

计算机科学与技术学科，李舟军博士的论文《传值 CCS 和 π - 演算互模拟等价的验证理论和算法》，导师陈火旺教授。

分类号 TP311
UDC
学号
密级

工学博士学位论文

传值 CCS 和 π－演算互模拟等价的验证理论和算法

博士生姓名：李舟军
学科专业：计算机科学与技术
研究方向：计算机软件和理论
指导教师：陈火旺教授

国防科学技术大学研究生院
一九九九年九月

Theories and Algorithms for the Verification of Bisimulation Equivalences in Value-Passing CCS and the π-Calculus

Candidate: **Li Zhoujun**
Supervisor: **Prof. Chen Huowang**

A Dissertation
Submitted in Partial Fulfillment of the Requirements for the Degree of
Doctor of Engineering
in Computer Science and Technology
Graduate School of National University of Defense Technology
Changsha, Hunan, P. R. China
September, 1999

摘　要

随着计算机技术和网络通信技术的高速发展，以并发性、分布性、实时性、异构性和互操作性等为主要特征的并发分布式系统已成为当前计算机技术的主流方向，并已在国民经济和国防建设中得到广泛应用。由于并发分布式系统本身非常复杂，因此其开发过程不仅难度大，效率低，周期长，而且很难避免和发现其中隐含的错误和缺陷。对于安全攸关系统（safety critical systems），其失误和崩溃可能会造成生命和财产的重大损失，甚至导致灾难。

形式化方法被公认为是一种行之有效的减少设计错误、提高系统可靠性的重要途径。传统的形式化方法以严格的数学理论为支撑，对顺序计算的本质作了深刻的诠释。并发现象以其固有的复杂性，对计算机科学家提出了挑战。并发理论的研究主要集中在并发系统的形式模型和形式语义上，各种从不同侧面反映并发本质的模型被相继提出。在这些模型和方法中，以通信系统演算 CCS 为代表的进程代数，因概念简洁，可用的数学工具丰富，在并发分布式系统的规约、分析、设计和验证等方面获得了广泛应用。

传值 CCS 和 π - 演算是对 CCS 的继承和发展，其传值和传名的特性更适合于对并发通信系统进行直接的建模。传值 CCS 和 π - 演算互模拟等价的验证理论和算法是进程代数领域的研究热点，也是使进程代数从理论研究走向实际应用的关键环节。本文以 Hennessy 和 Lin 所提出的符号化方法为工具，对传值 CCS 和 π - 演算互模拟等价的语义理论、公理化系统和验证算法进行了系统、深入的研究，主要工作包括以下五个方面：

（1）通过引入符号观察图和符号同余图，首次给出了传值 CCS 的迟/早弱互模拟等价和观察同余的验证算法，成功地将 Hennessy 和 Lin 的强互模拟验证算法推广至弱互模拟和观察同余的验证。同时给出并证明了 τ - 循环和 τ - 边消去定理，在应用任何弱互模拟和观察同余验证算法之前，均可利用这些定理对所给符号迁移图进行化简。

（2）基于 Lin 提出的带赋值符号迁移图（STGA），引入了一种先动作 - 后赋值的 STGA，它与原模型的不同之处在于将符号迁移上赋值和符号动作的执行次序颠倒。基于此种 STGA，既能定义其结点间的符号双迁移关系，又能得到正则传值 CCS 更为自然

简洁的有穷表示。本文不仅给出了从正则传值 CCS 的语法表示生成此类 STGA 的全部产生规则，而且分别讨论了此类 STGA 的强/弱、迟/早互模拟等价和观察同余的验证问题，并给出了相应的转换算法。

(3) 提出以符号迁移图为π－演算进程的有穷表示模型，并给出了将有穷控制π－演算进程转换成有穷符号迁移图的全部产生规则，从而将上述关于传值进程的互模拟验证算法全部推广至有穷控制π－演算。利用关于其布尔表达式的可判定理论，本文对有穷控制π－演算的互模拟验证问题给出了一种新的解决方法。

(4) 给出了π－演算强开互模拟的完全符号刻画，并证明了该刻画的可靠性和完备性。从而证实了 Boreale 和 De Nicola 的如下猜想：符号强开互模拟可由符号强迟(早)互模拟通过禁止划分(分情况分析)而得到。同时提出了强开互模拟的符号证明系统，并证明了该系统的可靠性和完备性。在此基础上，首次从符号刻画和符号证明系统两个方面对开/迟/早这三种以不同方式定义的π－演算的互模拟等价关系进行了精确的比较研究。最后不仅给出了弱开互模拟和开观察同余的完全符号刻画，而且利用四个τ－法则，成功地将强开互模拟的符号证明系统提升至开观察同余。

(5) 如何将 Sangiorgi 为π－演算引入的开互模拟推广至带不等名测试的π－演算一直是一个久悬未决的难题，本文对该问题提出了一个合理的解决方案。我们不仅给出了带不等名测试的π－演算的开互模拟定义，而且给出了开互模拟的符号刻画。然后提出了开互模拟的符号证明系统，并证明了该系统的可靠性和完备性。最后我们针对该演算的不含并行组合算子的子语言给出了弱开互模拟和开观察同余的定义及其符号刻画，并通过在开互模拟的符号证明系统的基础上增加五个τ－法则，得到了开观察同余的完备推理系统。

上述结果既具有重要的理论意义，又具有潜在的应用价值。最后我们简要地总结了本文的主要贡献，介绍了我们在传值 CCS 和π－演算的模型检测算法和验证工具方面所做的初步工作，并阐述了对后续工作的一些设想。

关键词：传值 CCS；π－演算；互模拟；符号互模拟；符号迁移图；符号证明系统

ABSTRACT

With the rapid development of computer technology and network communication, concurrent and distributed systems that feature concurrency, distribution, real time, heterogeneity and interoperability have become the main direction of current computer technology, and have been widely applied to national economy and the construction of national defense. Because of the complexity, the concurrent distributed systems are difficult, inefficient and time-consuming in their development, and it is hard to avoid and find the implied errors and shortcomings. As for safety critical systems, their errors and collapse will cause the loss of lives and properties, and even catastrophe.

Formal methods are widely considered as a feasible and important approach to reducing design errors and increasing system reliability. Traditional formal methods deeply explain the essence of sequential computing, with the support of strict mathematical theories. The phenomenon of concurrency challenges computer scientists by its intrinsic complexity. The study of concurrency theory focuses on the formal model and formal semantics of concurrent systems. Thus various models that reflect the essence of concurrency from different aspects are proposed one after another. Among these models and methods, the process algebra, which is represented by Calculus of Communicating Systems (CCS), are widely applied to the specification, analysis, design and verification of concurrent distributed systems because of its concise concepts and rich available mathematical tools.

Value-passing CCS and the π-calculus are the inheritance and development of CCS, their characteristics of value-passing and name-passing are fit for the direct modeling of concurrent communicating systems. The verification theories and algorithms of value-passing CCS and the π-calculus bisimulation equivalences are the hot point of research in the area of process algebra, and the critical step for the application of process algebra in practice. By means of the symbolic approach presented by Hennessy and Lin, this thesis performs a systematic and deep study of the

semantic theories, axiomatisational systems and verification algorithms of value-passing CCS and the π-calculus bisimulation equivalences. The main task includes the following five aspects:

(1) By introducing symbolic observation graphs and symbolic congruence graphs, we present algorithms for verifying late/early weak bisimulation and observation congruence of value-passing CCS for the first time, thus generalize successfully the strong bisimulation algorithm by Hennessy and Lin to the weak case. Moreover, two theorems ensuring the elimination of τ-cycle and τ-edge are proved. Therefore STGs can be simplified significantly once the weak bisimulation or observation congruence is to be checked.

(2) Based on the symbolic transition graph with assignment (STGA) of Lin, we introduce a variant of STGA. The distinction of our model is that the assignment of a transition is performed after rather than before the action. We can not only define the symbolic double transition relations over nodes on top of such STGAs, but also get more compact finite representation of regular value-passing CCS. The rules which generate such STGAs from regular value-passing CCS are presented. Finally, we discuss the problem of checking strong/weak bisimulation equivalences and observation congruence of such STGAs, and present corresponding transformational algorithms.

(3) Symbolic transition graph (STG) is proposed as a compact semantic model for the π-calculus processes. The rules which generate such STGs from finite-control π-calculus processes are presented. Thus the above bisimulation checking algorithms for value-passing processes can all be lifted to finite-control π-calculus. By means of the decidable theory of boolean expressions, we present a new approach to check bisimulations of the finite-control π-calculus.

(4) A symbolic characterization of strong open bisimulation of the π-calculus is presented and the soundness and completeness of such characterization are proved. This result verifies a conjecture put forth by Boreale and De Nicola: symbolic open bisimulation can be obtained from symbolic late or early bisimulation by omitting case analysis. A symbolic proof system for strong open bisimulation is also proposed and its soundness and completeness are proved. Moreover, based on the previous work on the π-calculus, accurate comparisons between open, late and early bisimulations are accomplished in both aspects of symbolic characterizations and symbolic proof systems. Finally, symbolic characterizations of weak open bisimulation equivalence and open observation congruence are presented. By using four τ-laws, we lift the symbolic proof system for

strong open bisimulation to open observation congruence.

(5) The challenging problem that what is the most reasonable way to define open bisimulation for the π-calculus with mismatch operator is still open. In the thesis, we give a reasonable solution to this problem. A definition of open bisimulation is presented and its symbolic characterization is given. Then a symbolic proof system for open bisimulation is put forth and its soundness and completeness are proved. Finally, symbolic characterizations of weak open bisimulation equivalence and open observation congruence are presented for the calculus without the parallel composition operator. By adding five τ-laws to the symbolic proof system, we obtain a complete inference system for open observation congruence.

These results are not only of theoretical significance, but also of potential application value. Finally, we summarize what we have achieved and briefly introduce the primary work we have done both in the model-checking of value-passing CCS and the π-calculus and in the implementation of the algorithms put forth in the thesis. In addition, we discuss our possible future work.

Keywords: Value-passing CCS, π-calculus, Bisimulation, Symbolic bisimulation, Symbolic transition graph, Symbolic proof system

目　　录

第六章 π－演算开互模拟的符号刻画和完备推理系统:强和弱

第七章 带不等名测试的π－演算的开互模拟:强和弱

第八章 结束语