分 类 号: TP309　　密　级: 公开

论文编号: 2016010041

贵 州 大 学

2022届博士研究生学位论文

基于遗忘的反应式系统最弱充分条件研究

学科专业: 软件工程

研究方向: 软件工程技术与人工智能

导　　师: 王以松

研 究 生: 冯仁艳

中国·贵州·贵阳

2022年5月

目　录

目录 ····· **i**

摘要 ····· **vii**

Abstract ····· **ix**

第一章　绪论 ····· **1**

1.1　研究背景与意义 ····· 1

1.1.1　研究背景 ····· 1

1.1.2　研究意义 ····· 3

1.2　研究动态与趋势 ····· 4

1.2.1　研究动态 ····· 5

1.2.2　研究趋势 ····· 9

1.3　关键问题与目标 ····· 11

1.4　研究内容与成果 ····· 12

1.5　论文组织结构 ····· 15

第二章　Kripke结构、时序逻辑、模型检测以及遗忘理论 ····· **17**

2.1　Kripke结构 ····· 17

2.1.1　真假赋值和K-解释 ····· 17

2.1.2　Kripke结构的定义及相关术语 ····· 20

2.2　时序逻辑 ····· 21

2.2.1　计算树逻辑（CTL） ····· 21

2.2.2　CTL的标准形式 ····· 23

2.2.3　CTL下的归结 ····· 26

2.2.4　μ-演算 ····· 27

2.2.5　μ-公式的析取范式 ····· 29

2.3　模型检测 ····· 30

2.4　遗忘理论 ····· 30

2.5　本章小结 ····· 30

第三章 遗忘理论的定义及其语义属性 ····· 31
3.1 引言 ····· 31
3.2 V-互模拟 ····· 31
3.3 遗忘理论及其语义属性 ····· 37
3.4 本章小结 ····· 41

第四章 计算CTL下的遗忘：基于归结的方法 ····· 43
4.1 引言 ····· 43
4.2 二元互模拟 ····· 45
4.3 基于归结的方法计算遗忘 ····· 46
4.3.1 将CTL公式转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合 ····· 46
4.3.2 归结过程 ····· 49
4.3.3 “移除”过程 ····· 51
4.3.4 索引和“**start**”的“消除” ····· 53
4.3.5 替换V'中的原子 ····· 55
4.4 算法的可终止性和计算复杂性 ····· 57
4.5 本章小结 ····· 57

第五章 基于模型的方法计算CTL下的遗忘 ····· 59
5.1 引言 ····· 59
5.2 描述初始K-结构 ····· 59
5.2.1 计算树的V-互模拟 ····· 60
5.2.2 计算树的特征公式 ····· 63
5.2.3 初始K-结构的特征公式 ····· 65
5.3 遗忘理论的封闭性 ····· 70
5.4 基于模型的遗忘理论计算方法 ····· 72
5.5 本章小结 ····· 72

第六章 μ-演算中的遗忘理论 ····· 73
6.1 引言 ····· 73
6.2 系统模型与问题提出 ····· 75
6.3 本章小结 ····· 75

第七章　遗忘理论的应用 ····· **76**
7.1　引言 ····· 76
7.2　最强必要条件和最弱充分条件 ····· 78
7.3　μ-演算下的知识更新 ····· 80
7.4　本章小结 ····· 84

第八章　差分隐私策略机制的均衡优化模型 ····· **85**
8.1　引言 ····· 85
8.2　系统模型与问题提出 ····· 87
8.2.1　系统模型 ····· 87
8.2.2　敌手模型 ····· 88
8.2.3　问题提出 ····· 88
8.3　隐私保护攻防博弈 ····· 90
8.3.1　博弈模型 ····· 90
8.3.2　均衡分析 ····· 92
8.4　策略优化选择算法 ····· 94
8.5　实验与分析 ····· 96
8.5.1　实例分析 ····· 96
8.5.2　数值分析 ····· 97
8.6　本章小结 ····· 98

第九章　总结与展望 ····· **99**
9.1　工作总结 ····· 99
9.2　研究展望 ····· 100

参考文献 ····· **102**

致谢 ····· **105**

攻读博士学位期间科研和论文情况 ····· **106**

表　格

1.1　近三年主要典型隐私泄露事件概览 …… 1
1.2　对比三类隐私保护方法 …… 3
1.3　差分隐私的数据发布方法 …… 5

2.1　转换规则 …… 25
2.2　化简规则。其中$Q \in \{\text{A}, \text{E}\}$且$T \in \{\text{X}, \text{G}, \text{F}\}$。 …… 26
2.3　归结规则 …… 27

8.1　数据概率分布示例 …… 91
8.2　$\varepsilon = \ln 2$的隐私机制 …… 91
8.3　对策博弈的支付矩阵 …… 95
8.4　$|\mathscr{X}| = 6$的概率分布 …… 96
8.5　$|\mathscr{X}| = 6$时提供$\varepsilon = \ln 2$的等价隐私机制 …… 96

插　图

1.1　差分隐私的应用研究 …… 4
1.2　差分隐私多维数据处理流程 …… 7
1.3　本文核心研究内容及其关系 …… 13
1.4　本文的章节内容组织结构图 …… 15

3.1　κ-结构之间的V-互模拟关系 …… 33

4.1　基于归结的遗忘的主要流程图 …… 43

5.1　左图为初始κ-结构$\mathscr{K}_2$ (源于图 **??**)；右图：从左到右表示以s_0为根、深度分别为0、1、2和3的计算树（为简化图，计算树的标签没有给出，但是每个树节点的标签可从$\mathscr{K}_2$找到。） …… 67

8.1　隐私保护数据收集的系统模型 …… 87
8.2　理性决策过程的描述说明 …… 95
8.3　$|\mathscr{X}| = 6$时$I(X;\hat{X})/H(X)$ …… 97
8.4　$|\mathscr{X}| = 12$时$I(X;\hat{X})/H(X)$ …… 97

摘　要

信息化的快速发展和深度应用所引发的隐私安全挑战，成为了制约数据开放、共享、交换和应用的瓶颈，并引起了法律界和学术界的高度关注。从技术的角度，差分隐私保护算法作为一种重要的隐私保护技术，在面向多维及其复杂关联的数据隐私保护方面的研究还不够成熟。首先，由于数据类型混合、稀疏性、域值空间大等原因，差分隐私的多维数据处理面临隐私脆弱性、计算效率低等方面的挑战；其次，数据融合的关联性、背景知识攻击和策略型敌手攻击，数据的隐私性和可用性的矛盾成为了突出问题。针对上述问题，从博弈的角度探讨隐私与效用的均衡及优化，不失为一种较好的解决方案。本文重点围绕隐私与效用均衡这一核心问题，基于信息熵、优化理论和博弈均衡等相关理论和方法，以构建均衡、优化模型为主线，在隐私量化方法设计、隐私与效用博弈模型构建及均衡求解、优化模型建立及求解等方面，取得了一系列的成果，为从技术和管理相结合的视角解决隐私保护问题提供了借鉴。本文所取得的主要研究成果包括：

1. 提出了差分隐私的信息熵度量模型及方法。针对隐私量化问题，基于Shannon基本通信模型，结合差分隐私的随机扰动原理，给出了有噪声信道的差分隐私通信模型及其形式化描述；进一步通过定义差分隐私保护模型中的信息熵、条件熵、联合熵、互信息量以及条件互信息量等概念，设计了以信息熵为核心的隐私度量模型；针对多维属性及其关联问题，基于图模型和马尔可夫模型等提出了面向多关联属性的差分隐私信息熵度量模型及方法，并基于数据处理不等式和Fano 不等式给出了信息泄露量的上下界。理论分析与实验结果表明，所提出的量化模型和方法能够有效地实现差分隐私量化目标，为隐私泄露风险评估和隐私保护机制设计提供了基础支撑。

2. 提出了含背景知识攻击的差分隐私优化模型。在所建立的差分隐私通信模型的基础上，结合所提出的隐私度量模型与方法和损失压缩理论，建立含背景知识的敌手模型，以此为基础提出了含背景知识攻击的差分隐私通信模型；在基于条件互信息量设计的隐私率失真函数基础上，提出了含背景知识攻击的最优化模型；进一步针对所提出优化模型的求解问题，利用Blahut-Arimoto交替最小化方法设计和实现了权衡隐私与效用的迭代最小化算法，并给出了其计算复杂度分析。理论分析和实验仿真结果表明，所提出的相关方法相对于对称信道隐私保护机制具有明显优势。

3. 提出了有序随机响应扰动方案(Orderly Randomized Response Perturbation，ORRP)。针对多维数据差分隐私保护所面临的隐私脆弱性和效率低问题，面向数据收集场景的隐私保护需求，提出了一种有序随机响应扰动方案，有效解决了现有隐私保护机制忽视数据分布的影响、处理域值空间大和数据稀疏导致计算效率低的问题。该方案以所

提出的隐私度量模型为基础，通过对隐私保护与数据可用性之间矛盾的分析和量化，给出了满足数据质量约束下最小化隐私泄露的互信息优化模型的形式化描述，以此实现最优隐私机制的概率密度函数计算并实现随机扰动。同时，参考独立并联信道模型，将上述结果推广到了多维数据情形。最后，从隐私泄露、数据可用性质量、关联度损失等方面给予了理论分析和实验仿真。结果表明，所提出的ORRP方案在数据语义完整性、隐私性和数据可用质量等方面比现有的结果更具有优势。

4. 提出了隐私保护的攻防博弈(Privacy-Preserving Attack Defense，PPAD)模型。针对差分隐私系统中存在消息灵通的策略型敌手问题，围绕数据收集场景设计了差分隐私保护的选择策略，以此为基础提出了隐私保护的攻防博弈模型，并通过均衡求解实现了差分隐私保护中隐私与效用之间的平衡。该方案基于所建立的差分隐私基本通信模型，在分析隐私保护方和策略型敌手方各自目标的基础上，构建了隐私极小极大优化模型，给出了包含参与者集合、策略空间、收益函数等的隐私攻防博弈模型的形式化描述。论文巧妙地利用了隐私互信息量的内涵与外延，构造了隐私保护的效用函数，最终具体实现了一个两方零和对策博弈模型的构建。论文利用极小极大定理和凹凸博弈理论给出了该攻防博弈模型的均衡分析，并进一步基于最优策略响应设计了均衡求解的策略优化选择算法。理论分析与数值实验结果表明，所提出的模型及方法能有效解决等价隐私保护机制之间的比较问题，同时可用于隐私保护程度最差情况下的隐私泄露风险评估。

关键词： 隐私度量，差分隐私保护，率失真函数，博弈均衡，优化模型

Abstract

The challenges of privacy and security caused by the rapid development of informatization and in-depth applications, have become a bottleneck restricting data opening, sharing, exchange, and application, and have attracted great attention from the legal and academic communities. From the perspective of technology, the differential privacy (DP) protection algorithm, as an important privacy protection technology, is not mature enough in the research of data privacy protection for multi-dimensional and complex associations. Firstly, due to the mixed data types, sparseness, and large domain value space etc, the multi-dimensional data processing of DP is faced with the challenges such as privacy vulnerability and low computational efficiency. Secondly, the relevance of data fusion, background knowledge attacks and strategic adversary attacks, and the contradiction between data privacy and usability have become prominent issues. For the problems mentioned above, it is a better solution to investigate the trade-off and optimization of privacy and utility from the perspective of the game theory. Thus, this article mainly focuses on the crucial problem of the trade-off between privacy and utility. Based on information entropy, optimization theory and game equilibrium and other related theories and methods, the equilibrium and optimization models are constructed as the main line of this research. A series of results have been achieved in designing of privacy quantification methods, constructing and solving game model between privacy and utility, optimization model establishment and solving, etc., which provide a reference for solving privacy protection issues from the perspective of combining technology and management. The major contributions can be summarized as follows.

1. The information entropy metric models and methods of DP are proposed. For the quantitative problem of privacy, the noisy DP communication model and formalization statement are defined based on the Shannon's fundamental communication model and the randomized perturbation principle of DP. Further, the notions of information entropy, conditional entropy, joint entropy, mutual information and conditional mutual information, etc., are defined under the differential privacy model, and then, the privacy metric models with information entropy as the core are designed. For the problem of multi-dimensional and correlated attributes, based on the graph and Markov model, etc., a privacy metric model and method for multi-dimensional and correlated attributes is proposed. Then, the upper and lower bounds of privacy leakage are quantified by using data processing inequality and Fano's inequality. Theoretic analysis and experimental results are demonstrating the proposed metric model and method can effectively

achieve the goal of DP quantification, and further provide basic support for privacy leakage risk assessment and privacy protection mechanism design.

2. The differential privacy optimization model with background knowledge attacks is proposed. Based on the established fundamental communication model of the DP, lossy compression theory and the proposed privacy metric model, the adversary model which has relevant background knowledge is established, and further the DP communication model with background knowledge attacks is proposed. By using conditional mutual information measures privacy, this paper updates the form of the well-known rate distortion function, and proposes the differential privacy optimization model with background knowledge attacks. Further, the alternating minimization iteration algorithm solving the proposed optimization model is designed and implemented based on the Blahut-Arimoto alternating minimization method, and the computation complexity analysis is provided. Theoretic analysis and experimental results are demonstrating the proposed method have significant advantages in data quality and privacy leakage when compared with the existing symmetrical channel mechanism.

3. The orderly randomized response perturbation (ORRP) scheme is proposed. For the problem of low efficiency and privacy vulnerability when deal with multi-dimensional data using local differential privacy, and facing the privacy protection requirements of data collection scenarios, this paper proposes an orderly randomized response perturbation scheme. The proposed ORRP scheme effectively solves the impact of the existing privacy protection mechanisms ignoring data distribution, and the problem of low computing efficiency caused by the large processing domain value space and sparse data. To be specific, the proposed ORRP scheme based on the prior proposed privacy metric model. A mutual information optimization model subjects to a given data quality loss constraint to minimize privacy leakage, is proposed by analyzing and quantifying the requirements of privacy and data quality. Further, the probability density function (PDF) of the optimal privacy mechanism is computed by the means above, and it is used to achieve randomized perturbation. Meanwhile, referring to the independent parallel channel model, the above methods are extended to the case of multi-dimensional data. Finally, theoretical analysis and experimental simulations are given in terms of privacy leakage, data usability quality, and correlation loss. The results demonstrate that the proposed ORRP has more advantages than the existing methods in terms of data semantic integrity, privacy and data availability quality.

4. The privacy-preserving attack and defense (PPAD) game model is proposed. For the problem of informed and strategic adversary in the differential privacy system, the selection strategy of differential privacy protection is designed around the data collection scenarios. On the basis of the above, the PPAD game model is proposed, and the trade-off between privacy

and utility in the protection of differential privacy is achieved by solving the equilibrium. The proposed scheme is based on the established differential privacy basic communication model. The privacy minimax optimization model is established by analyzing the privacy goals of defender and strategic attacker, and further the formalization statement of PPAD is provided, which includes players' sets, strategic spaces and payoff functions etc. This paper cleverly uses the connotation and extension of private mutual information to construct the utility function of privacy protection, and finally realized the construction of a two-person zero-sum (TPZS) game model. Then, this paper provides the game analysis by using von Neumann's minimax theorem and concave-convex game, and further designs a strategy optimization selection algorithm to calculate saddle point based on the optimal strategy response. Theoretic analysis and numeric simulation results show that the proposed model and method can effectively solve the problem of comparison between equivalent privacy mechanisms, and also can be used for privacy leakage risk assessment in the worst case of privacy protection.

Keywords: Privacy metric, differential privacy protection, rate-distortion function, game equilibrium, optimization model

第一章　绪论

本章首先介绍研究的立项背景，分析保障数据隐私安全的重要性，并阐述研究意义。其次，综述分析差分隐私的国内外研究动态以及信息论、博弈论方法在差分隐私中的应用研究趋势。然后，围绕研究对象凝练出关键问题与目标。进一步，介绍本文的核心研究内容以及研究取得的主要成果。最后，给出具体章节组织安排。

1.1　研究背景与意义

1.1.1　研究背景

数据安全是网络空间安全的重要组成部分，已成为互联网技术发展中亟需解决的关键问题。为保障网络信息安全，国家制定、公布、实施了《网络安全法》[?]，其中涉及个人信息的使用、保护规范。在基于互联网的应用中(如社交网络、位置服务等)，有关个人的数据不断地被收集、存储、利用，直接的分析、发布、共享这些个人数据将会导致个体隐私泄露问题。为建立健全个人信息安全保护管理制度，《互联网个人信息安全保护指南》[?]明确了个人信息生命周期处理过程中的使用规范。该指南中对个人信息给出了明确的定义，个人信息生命周期阶段的操作做出明确的规范，目的是保障个人隐私信息安全。尽管如此，近年来个人隐私泄露事件依然频频发生，隐私泄露问题引发人们的困扰。下表1.1 调查列举了近三年主要发生的典型隐私泄露事件，由此可见，个人隐私保护的需求不断攀升。

表 1.1: 近三年主要典型隐私泄露事件概览

发生时间	隐私泄露事件	泄露数据类型
2020年04月	青岛胶州中心医院就诊名单泄露	涉及6685人的姓名、电话、身份证号码、居住地址、就诊类型等
2020年03月	万豪连锁酒店数据泄露	包括姓名、生日、电话号码、旅行信息和忠诚计划信息
2020年02月	美高梅酒店旅客信息泄露	10,683,188名客人信息，包括家庭住址、电话号码、电子邮件和生日等
2019年05月	Clinical Pathology Laboratories 数据泄露事件	泄露数据涉及姓名、地址、电话号码、出生日期、治疗信息等
2019年02月	Dubsmash 1.62 亿用户数据泄露	用户姓名、ID、用户名、密码等
2018年08月	华住集团旗下连锁酒店数据泄露	姓名、手机号、邮箱、身份证号等

2020年10月，《中华人民共和国个人信息保护法(草案)》提请十三届全国人大常委会第二十二次会议审议，标志着个人隐私保护问题受到了政府和人民的高度重视，已

成为一个普遍关注的热点问题。当前，解决个人隐私保护问题的途径主要有制定、完善法律法规和研究有效的隐私保护技术两个方面。在法律法规的规范引导下，隐私保护需要强有力的隐私保护技术支撑。为了深入理解具体的隐私保护技术方案，本文调查了不同应用场景下的隐私保护需求。社交网络[???]、地理位置[???]、数据收集[????]、数据发布[??]、数据挖掘[???]等应用中分别产生了用户社交关系、位置移动轨迹、敏感属性保密等隐私保护需求。针对这些场景中的隐私保护问题，学术研究提出了一系列的隐私保护技术方案。依据实现机理的不同，当前的隐私保护技术方案大致可以划分为三类：基于泛化和抑制手段的匿名类隐私保护、基于噪声扰动的差分隐私保护和基于密码方法的隐私保护。首先，匿名类的隐私保护模型(如 k-anonymity[?]，l-diversity[?]，t-closeness[?]，(α,k)-匿名[?]，(k,e)- 匿名[?]，(ε,m)-匿名[?]等)利用泛化和抑制[?]的手段实现基于准标识符的匿名等价类，降低了敏感数据泄露风险。然而，匿名类的隐私保护模型存在着难以抵御连接攻击、同质性攻击和相似性攻击的缺陷。大数据环境下，匿名类的隐私保护模型的局限性凸显。随后，为了解决统计数据库的隐私泄露问题，2006年 Cynthia Dwork 提出了差分隐私(Differential Privacy，DP)[?]保护模型，旨在通过噪声扰动[?]的方式实现相邻数据集上查询输出结果的ε 概率不可区分性。近年来，围绕隐私保护需求，研究者提出了诸多差分隐私保护方案，在隐私保护的数据发布(Privacy-Preserving Data Publishing，PPDP)、隐私保护的数据分析(Privacy-Preserving Data Analysis，PPDA)、隐私保护的数据挖掘(Privacy-Preserving Data Mining，PPDM)等场景中得到了广泛应用[?]。总体上，差分隐私的研究工作主要是围绕噪声抽样分布和噪声扰动的方式展开，也就是研究差分隐私的噪声机制和最优化的隐私预算参数问题，其目的是为了平衡隐私保护与查询数据的精确度。此外，基于密码方法的隐私保护方案也得到了研究，如同态加密、密文搜索技术等[?]在隐私保护方案设计中得到了应用。但是，由于基于密码学的隐私保护方案存在计算复杂度较高的弱点，现阶段还无法满足实际应用中的时间和性能要求，因此尚未得到实际的广泛应用。表1.2总结对比了三类隐私保护方法的特点。匿名类和差分隐私是现阶段主流的隐私保护模型。在现有的两类主流隐私保护技术中，敏感数据的隐私性与数据可用性是隐私保护方案设计的核心关注点，同时也是评价隐私保护机制的重要指标。

近年来，差分隐私保护模型受到了学术界和产业界的热衷，其原因在于差分隐私提供了一种严格数学可证明的隐私保证，在最差的情况下(Worst-case)保障了特定个体的隐私信息被识别的概率不超过ε因子。基于数据失真扰动的差分隐私中隐私度与可用性的权衡问题也一直是学术研究关注的焦点。针对该问题，设计有效的差分隐私方案是一种常见的解决方法。现有的研究工作提出了诸多的差分隐私方案，如几何机制[?]、Alvim等[?]的最优随机化机制、互信息-隐私机制(MI-privacy)[???]等。根据模型假设的不同可以划分为信息论方法和非信息论方法的研究。信息论的模型中对先验分布具有一定的假设，而差分隐私模型中没有考虑先验分布的影响[?]。Dwork差分隐私

表 1.2: 对比三类隐私保护方法

方法类型	代表性技术	实现原理	方法特点
匿名类方法	*k*-anonymity *l*-diversity *t*-closeness ...	泛化、抑制	具有难以抵御连接攻击、同质性攻击和相似性攻击的缺陷
随机扰动方法	差分隐私 本地化差分隐私 ...	随机化扰动	严格数学可证明的理论基础，提供最差情况下隐私保证
密码学方法	同态加密 可搜索加密 ...	加密、密文计算	计算复杂度较高，现阶段尚无法满足实际应用中的时间和性能要求

模型[? ?]提供分布独立的强隐私保障，其中的ε-隐私度量仅依赖于条件概率分布。该模型无法捕捉隐私攻击者对数据具有的先验知识，为此，研究者提出了信息论的差分隐私模型。信息论的模型同时考虑了先验分布和差分隐私的条件分布对隐私泄露的影响，在此方面的研究已取得了一定的进展[? ? ? ?]。如Kalantari 等[?]考虑不同数据分布类型，研究提出了不同分布情况下对称机制和非对称机制的最优性。由此可见，数据先验分布对差分隐私最佳机制设计的影响。但是，目前的研究工作中还存在一些不足之处，尚需要深入的研究，主要表现为以下几个方面：首先，受隐私保护方案应用场景的影响，目前对于隐私的度量尚缺乏明确统一的定量化方法；其次，在面向多维属性或高维属性时，用户的隐私敏感度偏好、属性的相互关联以及相关程度等对隐私泄露、隐私机制的影响尚需要深入研究；进一步，在一些应用中，消息灵通的敌手以及含背景知识的敌手能力的表达以及对隐私泄露风险的影响需要考虑；此外，策略型的敌手能够适应的改变隐私推断策略，追求隐私最大化目标的策略行为也需要在隐私保护中考虑。这些存在的问题对当前差分隐私保护模型提出了研究的新课题。

1.1.2　研究意义

在个人信息保护备受重视的时代背景下，本文针对当前差分隐私模型在应用中面临的挑战，基于个人信息生命周期处理阶段，研究隐私数据发布阶段、数据收集阶段的差分隐私最优化机制问题具有重要的研究意义。

首先，本文针对具体的应用场景和敌手模型，基于信息论、优化与均衡理论开展隐私与效用度量、权衡隐私与效用的最优化模型与隐私机制设计、隐私机制评估与分析等方面的研究，为保护个人隐私信息安全提供一种技术支撑。基于信息量化的隐私度量和均衡优化角度的优化模型及算法为隐私泄露分析、隐私机制设计提供基础理论支撑。本文研究的均衡优化模型在理论上拓展了差分隐私研究的边界，丰富了差分隐私针对多维数据、关联数据、策略型敌手的隐私保护模型的研究。其次，本文研究的

模型求解算法在实践上可为差分隐私应用场景中隐私机制的设计与实现提供重要的参考。本文的研究恰合互联网信息服务中用户隐私保护的诉求，适应互联网技术发展阶段的个人隐私保护需求，对实现互联网数据隐私安全具有明确的现实意义。

1.2 研究动态与趋势

差分隐私(differential privacy，DP)是一种严格的隐私保护模型，为个体隐私信息提供了强隐私保障。标准形式的差分隐私[??]定义相邻兄弟数据集的查询输出结果满足概率ε-不可区分性(ε-indistinguishability)，其中ε是足够小的非负实数。差分隐私利用随机化的方式能够实现在保护个体隐私信息的同时保持数据的统计信息[???]，现已逐渐成为数据隐私的标准。通常，差分隐私被划分为中心化差分隐私和本地化差分隐私两种架构模式[?]。中心化模型(centered model)假设系统中存在一个可信的数据管理者能够访问原始数据，并利用隐私保护机制得到扰动数据。与之对应的，本地化差分隐私(local differential privacy，LDP)[??]是差分隐私(DP)的本地化应用，它是系统中无可信数据管理者的特殊情景。其主要应用于隐私保护的数据收集场景。在本地模型(local model)中，每个用户本地的执行LDP 隐私协议扰动其真实数据得到扰动数据(perturbed data)，并将扰动数据报告给数据收集者。然后，数据聚合者收集、存储、分析这些用户上报的扰动数据。当前，差分隐私已成为隐私保护研究的标准，对其应用的研究涉及社交网络[??]、推荐服务[?]、移动众包计算[?]等领域，图1.1描绘了差分隐私的主要应用领域和具体场景中的核心研究问题。本文中，围绕个人数据生命周期阶段，结合差分隐私的具体应用场景，从隐私保护的数据发布、隐私保护的数据收集、隐私保护的数据分析角度介绍目前国内外学术研究的动态与趋势。

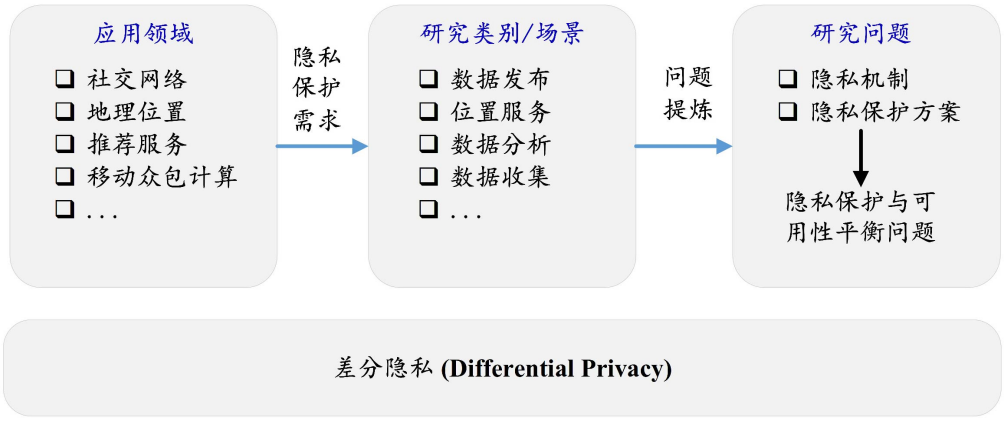

图 1.1: 差分隐私的应用研究

接下来，综述近些年差分隐私应用研究中与本文研究相关的主要代表性成果，进一步分析差分隐私研究的发展趋势。

1.2.1　研究动态

差分隐私的基本思想是在隐私数据中引入随机性来阻止个人的信息被推断。显然地，随机化的程度越高，隐私保护效果越好，对应的数据可用性则降低。这就是隐私与效用原则[?]，也就是著名的隐私与效用权衡问题[??]。该问题是隐私保护研究关注的核心问题，学术研究者围绕该问题做出了一系列有意义的研究工作。这些工作大致可以分为寻找更加有效的扰动机制[???]和研究有效的噪声注入方式[?]两类。如文献[?]提出了几何机制(Truncated $\frac{1}{2}$-geometric mechanism)实现最优的差分隐私扰动。为了提高数据效用，文献[?]提出在注入噪声之前，对数据进行小波变换(Wavelet Transforms)，克服了Dwork方案中Laplace噪声扰动大的问题。文献[?]利用随机投影的方式研究了差分隐私高维数据发布的问题，解决了扰动误差大的问题。结合具体的应用场景，以下阐述差分隐私的学术研究动态。

首先，隐私保护的数据发布场景中，可信数据管理者发布数据以供进一步的数据分析[?]，目标是发布数据的聚合信息而不泄露用户的个体隐私。差分隐私的数据发布包含有交互式发布和非交互式发布两种类型，其中，交互式数据发布包含有事务型数据发布、直方图数据发布、流数据发布、图数据发布；非交互式数据发布主要有批量查询发布、合成数据集发布[?]。隐私保护的数据发布场景中，发布数据的精确度与隐私泄露权衡是主要关注的核心问题。*为了解决数据发布中存在的隐私泄露问题，差分隐私的机制是研究的核心关注点。*近年来，以Dwork的方法[?]为基础，针对不同的发布数据类型，研究者提出了诸多的差分隐私数据发布模型及算法。表1.3列出了差分隐私数据发布的主要部分研究工作。

表 1.3: 差分隐私的数据发布方法

工作模式	数据发布类型	主要研究
交互式数据发布	事务型数据发布	IDC[?]
	直方图数据发布	Laplace[?]，Partitioning[?]
	流数据发布	Pan-Privacy[?]，P-Sums[?]
	图数据发布	Edge DP[?], Node DP[?]
非交互式数据发布	批量查询发布	Batch Query[?]
	合成数据集发布	Sanitization[?]

其次，本地化差分隐私的应用研究[?]已逐渐成为差分隐私的另一个重要研究方向，在隐私保护的数据收集、数据发布场景中都得到了不同程度的应用。围绕本地化差分隐私的应用，主要是研究如何设计可获得的隐私机制实现预期的目标。本地隐私模型中，随机化响应(Randomized Response，RR)[?]技术是一种获得LDP的有效方式，现已发展成为本地化差分隐私机制设计的基本构建模块，在本地差分隐私中的应用取得了显著的效果。近年来，很多著名的LDP隐私机制(如k-RR[?]，O-RR[?]，RAPPOR[??]，

MeanEst[?]等)已经被研究者提出。周异辉等[?]针对隐私-效用均衡问题，从优化理论的角度给出了效用优化模型，并分析了随机响应机制的最优性条件和相应的效用最优机制。此外，对于其它数据结构的本地化差分隐私也得到了研究，如set-value的本地化差分隐私[??]、key-value类型数据的本地化差分隐私[?]以及图数据结构的本地化差分隐私[?]。本地化差分隐私的应用涉及到社交网络[?]、移动众包计算[?]、数据合成发布[??]等场景，也因此日渐受到关注。本地化模型中，攻击模型通常被假设为半诚实(Semi-honest)的敌手模型，也就是说，数据聚合者诚实的执行隐私协议但是试图从报告的扰动数据中推断用户个体的隐私信息[?]。在本地化模型中，隐私与效用的权衡问题仍然是学术研究关注的重点。

最后，隐私保护的数据分析是在保持数据分析的精确度的同时保护个体的隐私信息[?]。近年来，基于学习理论的方法在差分隐私中得到了具体的应用，包括数据分析与机器学习的方法在差分隐私中的应用[???](如概率分布估计[?]，数据训练[?])。2018年，Ren 等[?] 使用 (Expectation Maximization，EM) 和 Lasso 的方法进行分布估计，用于得到联合概率分布，支撑发布数据集合成。2019年，Wang等[?]基于机器学习的线性回归(Linear Regression)、逻辑回归(Logistic Regression)、支持向量机(Support Vector Machines，SVM)分类算法分析了所提出分段机制(Piecewise Mechanism，PM)和混合机制(Hybrid Mechanism，HM)的性能。由此可知，隐私保护的数据分析主要是学习数据的统计特征，体现出扰动数据的质量。

鉴于上述分析可知，差分隐私在隐私保护中占据着重要的地位，它已经涉及到了具有隐私保护需求的各种信息系统应用。现阶段，差分隐私在面向低维数据和独立同分布数据情景的研究相对比较成熟。针对低维的数值型数据和类别型数据，目前已有诸多的隐私保护方案(如Duchi等人[?]提出的数值型方案，Wang等人[?]提出的类别型Optimized Unary Encoding，OUE方案)。但是，随着应用系统的需求升级，面向多维数据且存在数据关联的情景时，直接地拓展当前的方案到多维情景，则会面临性能和效用降低的挑战。此外，多维属性的用户隐私敏感偏好表达也是亟待解决的问题。针对这些问题，研究者积极的探索新的解决方案，以下给出研究进展及现状的介绍。

(1) 面向多维数据的差分隐私

随着用户数据维度的增加，多维或高维数据具有笛卡尔乘积空间大、数据稀疏性的特点，给差分隐私数据处理带来新的挑战。具体地说，差分隐私对于多维数据或高维数据的处理主要面临着隐私脆弱性、计算复杂度高等问题。为了解决这些问题，数据降维是一种通常采用的处理方法。将有关个体的数据元组，拆分为多个属性分量，然后独立的应用差分隐私机制，该处理思想以差分隐私的并行组合原理[?]为基础，其基本的处理流程如图1.2描述。

针对差分隐私的多维数据处理，研究者做了一些有意义的探索，提出了差分隐私的多维数据处理方案。2017年，Xu等[?]针对多维数据发布中存在的扰动误差增加

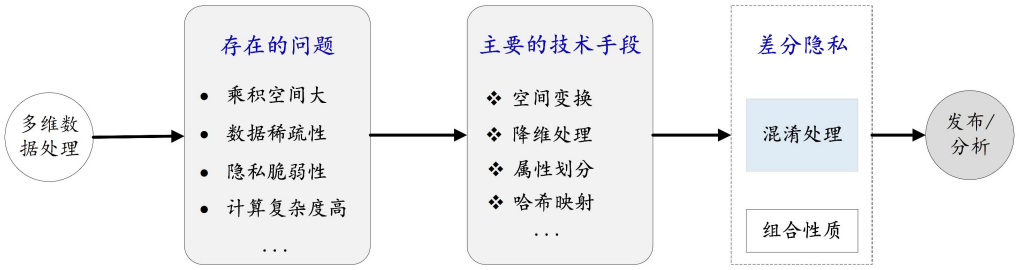

图 1.2: 差分隐私多维数据处理流程

和计算复杂性问题，通过随机投影的方法提出了高维数据发布的DPPro方案。此外的本地化差分隐私模型中，Wang等[?]针对多维数据的收集和分析场景，推广并改进了Duchi等人[?]的方案，提出了分段机制(PM)和混合机制(HM)，其思想是将属性分为数值型和类别型数据，然后依赖于单一数值型扰动方案和存在的任意类别型扰动方案(如OUE[?])，实现多维混合数值型和类别型数据的处理。Ren等[?]将基于Bloom Filter和RR实现的RAPPOR机制拓展应用到高维数据情景，利用属性值拆分、扰动合并和差分隐私的组合定理[?]，考虑了差分隐私高维数据发布的问题，提出了LoPub。其基本思想是将元组进行属性拆分，然后利用Hash函数和Bloom Filter映射属性值到比特串，并逐比特的进行随机扰动，产生扰动的元组。该方法首先将原始数据哈希得到“0”和“1”的比特串，然后随机响应实现随机的扰动。Yang等[?]基于随机响应技术本地转化用户数据到比特串，实现多维数据合成和发布的机制。事实证明这是一种相对有效的处理方法，且被广泛的应用在隐私保护的多维数据情景。该思想在基于地理位置的隐私保护系统中也有相应的应用。如混淆扰动一个元组时，独立的应用存在的隐私保护机制到元组的每一个位置点，然后得到整个响应的混淆元组[?]。近年来，面向多维数据的差分隐私研究逐渐成为一个重要的研究点，但是，目前针对混合数值型和类别型多维数据处理的差分隐私最优化机制的研究还相对较少。面向多维数据处理的差分隐私机制设计仍然是一个重要的研究方向，尚需要进一步的研究。

(2) 面向数据关联的差分隐私

现有的差分隐私处理方法大多假设数据抽样独立，然而实际应用中，多维数据通常不是独立存在，而是存在着相互关联的情况。事实上，这些关联可以分为数据的记录关联、属性关联或隐私攻击者的关联辅助背景知识关联等情况。文献[?]揭示了相关数据上的隐私机制将比期望的泄露更多的信息。为此，近些年数据关联的差分隐私机制设计问题受到研究者关注。

例如，数据集中属性年龄、职业可能和婚姻状态存在属性关联，这种关联使得敌手能够以较高的置信推断用户的隐私信息，从而增加隐私泄露风险。针对数据关联隐私泄露问题，文献[?]揭示由属性导致的元组相关，增加了流感疾病隐私泄露风险；文献[?]分析了敌手背景知识对隐私泄露的影响。针对数据关联的隐私泄露影响，研究者

开展了相关的研究工作。2014年，Zhang 等[?]利用贝叶斯网络考虑了数据集属性关联的情景，借助互信息分析属性之间的相关度[??]，提出利用贝叶斯网络实现差分隐私的高维数据发布。2015年，Zhu等[?]针对非独立同分布的数据集记录关联，改进了差分隐私的敏感度计算方法，减少了噪声注入提升了数据效用。Yang等[?]研究了数据相关对隐私的影响，敌手先验知识对隐私的影响和数据相关时的扰动算法设计，提出了贝叶斯差分隐私。2017年，Song等[?]提出Pufferfish privacy保护关联数据的隐私。2019年，Li 等[?] 基于皮尔逊的相关度分析方法，从强关联、弱关联、正相关和负相关的角度，考虑了隐私攻击者的背景知识和数据关联对差分隐私数据发布的影响。鉴于上述分析，由数据的记录关联、属性关联或隐私攻击者的关联辅助背景知识，导致的隐私泄露问题，或是存在数据关联的高维数据发布问题仍然是学术研究关注的焦点。数据相关的隐私度量分析成为隐私机制设计首要解决的问题。

(3) 面向用户偏好的差分隐私

差分隐私模型扩展应用于多维数据时，差分隐私的隐私特性(ε-度量)由其组合性质保障。通常情况下，差分隐私把多维属性看作等价敏感，提供相同等级的隐私保护。例如，用户个体的隐私数据包含d个属性维度，差分隐私机制的隐私预算设置ε/k，然后依据序列组合性质，隐私保护总体满足ε- 差分隐私。但是，多维的属性之间可能存在不同的隐私敏感度，也就是用户的隐私敏感偏好。为了更好的阐述这个问题，首先给出以下问题引例。

假设个体数据元组由年龄、性别、教育程度、婚姻状态组成，这些数据项都是有关个体的隐私信息。但是，在这些数据项中，用户对其数据具有不同的隐私感受。通常情况下，一个人的性别可能不被认为是隐私数据或者具有较低的隐私敏感性。然而，一个人的婚姻状态(如离婚)是想保持私密性的敏感数据，其隐私私密性高于其它属性。为了能够解决诸如此类的问题，这就要求差分隐私能够提供不同敏感等级的隐私保护对于有区分的属性，满足所提出的隐私保护需求。

针对上述问题，研究者依据属性敏感度等级，提出了有区别隐私数据的个性化差分隐私保护方案[?]。2015年，Jorgensen等[?]考虑个人数据的不同隐私保护需求，提出了个性化差分隐私(Personalized Differential Privacy，PDP)的概念。2019 年，Wang 等[?]利用泛化的$d_{\mathscr{X}}$-privacy[?]研究了个性化隐私保护。Murakami 等[?] 提出了效用最优的本地化差分隐私方案(Utility-optimized LDP，ULDP)用于隐私保护的数据收集与分析。通过划分个体数据为敏感数据和非敏感数据两部分，推广Mangat[?]随机响应到多元字母表情景，提出了ULDP方案，对于敏感数据提供和LDP 等价的隐私保障。2020年，Gu 等[?]通过考虑不同输入数据具有不同的隐私敏感度，提出了一种输入区分(Input-discriminiative)的隐私保护机制(Input-discriminiative LDP，ID-LDP)。由此可见，考虑用户隐私偏好，设计差分隐私机制，实现为不同敏感度的用户数据提供有区分的隐私保护成为一种新的研究方向。

1.2.2　研究趋势

Shannon[?]为解决信息度量问题提出信息熵的概念之后，信息熵在通信、密码学等领域发挥了重要的作用。近年来，基于信息度量的量化信息流思想(Quantitative Information Flow，QIF)[?]逐渐在隐私保护中得到应用。此外，博弈均衡理论作为一种有效的分析工具在隐私保护中也得到了应用。针对差分隐私应用中存在的隐私与效用的平衡问题，基于信息论、博弈论以及交叉学科的方法开展研究逐渐成为一个重要的研究方向。以下从两个方面综述密切相关且具有代表性的研究成果。

(1) 差分隐私的信息论方法

隐私保护模型的本质是数据混淆、扰动机制，它可以表达为一种概率性的函数映射，与信息论的方法密切相关[?]。由此，在隐私保护研究中，信息熵发展成为一种有效的隐私度量方法[??]。以信息熵为基础定义的Rényi熵[???]、条件熵、联合熵、互信息量等在隐私保护研究中得到了应用[????]。首先，隐私度量方面，Mir 等[?]利用信息熵、条件熵、互信息量研究了隐私信息的度量问题，奠定了差分隐私的信息论方法研究基础。Barthe 等[?] 利用信息熵研究了差分隐私的隐私边界问题。Issa等[??]提出Maximal leakage方法测量隐私泄露，随后，Liao等[?]对其扩展提出α-leakage。其次，信息论的方法对于差分隐私的机制研究也有一定的应用[???]。2011年，Alvim 等[???]几乎是最早提出基于量化信息流(QIF) 的思想，将信息熵应用到差分隐私中量化隐私信息的不确定度，抽象差分隐私噪声机制为信息论噪声信道，并从信息论的角度考虑了平衡隐私度与数据效用的方法，同时提出信息论对称信道机制能够达到理论上的最优性。随后，信息论方法研究的差分隐私与标准差分隐私之间的关系得到研究者关注[?]。Cuff 等[?]基于互信息的概念给出了与标准差分隐私等价的信息论差分隐私定义。文献[??]研究建立了互信息约束与差分隐私的关系。进一步，Wang 等[?]提出可辨识识别(Identifiability)的概念、并研究了与差分隐私(Differential Privacy) 和互信息隐私(Mutual Information Privacy) 三个不同隐私概念之间的基本联系。更重要地是，信息论中著名的信源编码定理、限失真编码定理(保真度准则)[?]在隐私保护中均得到了相应地研究[??]。如Sankar等[?]针对统计数据库隐私泄露问题，构建了统计数据库的概率模型，从最佳信源编码、译码方案的角度考虑了信息论方法在数据库中平衡隐私与效用的应用。在允许部分失真的情况下，最小信息传输率的率失真理论在差分隐私[???]最优机制研究中也受到了关注。

随机响应技术是实现本地化差分隐私的有效方法，信息论方法对于随机响应的研究也得到了广泛的应用。事实上，本地化差分隐私的随机响应实现是根据特定的概率密度函数(Probability Density Function，PDF)随机响应。在此方面的研究关键在于设计满足差分隐私的概率密度函数。近年来，信息论方法的研究已从二元随机响应发展到多元随机响应，逐步向复杂数据类型拓展延伸。具体的研究工作从信息论的本地化差分隐私度量[?]，向最优机制设计发展。Sarwate 等[?]抽象二元离散随机响应机制

为Shannon 信息论[?]离散噪声信道，基于率失真理论[?]对本地化差分隐私的二元随机响应机制进行了研究，指出对称信道机制能达到最优性。但是，二元随机响应仅能处理“ 是”和“否”的问题，其应用具有局限性。随后，研究者对其进行了拓展研究，发展了多元随机响应(Multivariate Randomized Response，MRR) 技术。Kairouz等[?]基于互信息提出了k-RR机制，并在此后被进一步研究，发展了一系列先进的差分隐私机制。Kalantari 等[?]考虑不同先验概率分布情况，研究了汉明失真下平衡隐私度与数据效用的最佳差分隐私信道机制问题，指出对称信道机制和非对称信道机制的最优性对不同分布的最优性。Xiong 等[?]在隐私保护的数据收集场景，利用信息论的方法，将差分隐私的数据扰动机制抽象为离散无记忆的噪声信道机制，从限失真约束条件定义差分隐私信道集合，研究了本地化差分隐私的机制问题。

基于这些相关的研究工作，可以看出信息论的方法应用于差分隐私研究，主要是解决两个方面的问题：(1) 隐私信息的度量问题；(2) 差分隐私的机制设计问题。首先，前者的研究主要是从熵的内涵角度理解隐私泄露问题，该研究可用于评估隐私泄露风险(例如，定量分析隐私泄露的界)，同时也是信息论方法对差分隐私机制研究的基础；其次，为了解决隐私与效用的平衡问题，后者的研究主要关注于最优的差分隐私实现机制。对于该问题的解决，信息论方法是从噪声信道角度寻找满足给定约束条件的最优条件概率分布。由此，基于优化理论建模[?]、求解该问题是一种理想的选择。如极大极小定理、Karush-Kuhn-Tucker (KKT)条件等[?]得到了具体的应用。结合凸性或拟凸性形式化隐私与效用平衡问题为拟凸优化问题[?]、隐私失真最优化问题[?](信息论领域的率失真问题) 是较好的解决方法。但是，现阶段信息论方法总是假设数据抽样独立，对多维数据情景、多维属性存在关联、混合数值型和类别型的最优差分隐私机制问题尚未充分研究。

(2) 差分隐私的博弈论方法

隐私与效用的平衡问题(Privacy-utility Tradeoff)是隐私保护数据收集、隐私保护数据发布等应用场景中广泛关注的矛盾冲突问题。直观地，隐私保护效果越好，则噪声扰动导致的数据质量损失越大，从而数据效用降低。反之，数据效用越高，则隐私保护强度减弱，由此引发的隐私泄露量较大，这被称为隐私与效用原则[?]。在隐私保护的模型与算法研究中，如何平衡隐私与效用是一个研究的关键问题。针对此，上述优化理论的方法是一种行之有效的解决方案。除此之外，基于最优性发展起来的博弈论[?]也为隐私保护提供了有效的分析手段。博弈分析方法从理性的角度分析存在矛盾冲突情景下的参与者最优策略选择问题。近年来，在差分隐私研究中得到了一定程度的应用，其基本思想是分析隐私保护系统中参与者的理性行为，以均衡的思想解决隐私保护与数据效用平衡问题。

2013年，Hsu等[?]在差分隐私框架下针对隐私查询发布问题，建立了数据拥有者和数据查询者之间的两方零和博弈模型，提出一种新的隐私机制。2017年，Wu等[?]构

建了一个多方的有限策略型博弈，利用纯策略纳什均衡的存在性条件[?]研究了差分隐私关联数据集发布的隐私预算参数选取问题。2019年，Qu等[?]针对隐私与数据效用之间的权衡问题，提出了一种基于社会距离的个性化差分隐私方法，在用户和敌手之间建立了静态贝叶斯博弈，从贝叶斯纳什均衡的角度权衡隐私与效用。此外，非合作的微分博弈[?]和斯坦伯格博弈(Stackelberg)[??] 也都在差分隐私中得到了研究。值得强调的是，Alvim 等[??]基于量化信息流的思想，采用信息论方法度量隐私泄露，构建了隐私保护攻击与防御的两方零和博弈模型，进一步，基于极大极小理论[?]分析了隐私防护者与隐私攻击者的最佳策略选择。该研究工作将信息论的方法融入到博弈模型中，标志着一种新的研究趋势。但是，该研究工作没有针对具体的差分隐私保护模型展开研究，因此，在该方面仍然存在较大的研究提升空间。博弈模型用于差分隐私的研究，关键问题在于分析具体应用场景中隐私保护参与者和策略集，定义合理的收益函数，解决均衡的问题。

1.3　关键问题与目标

相关研究工作表明信息论度量方法、有损压缩[??]方法用于量化隐私泄露，研究隐私机制具有较好的优势。但是，在面向多维数据处理时，多维属性及相关性给差分隐私机制带来新的挑战。目前的研究尚未充分解决多维数据关联的隐私度量，缺乏敌手关联知识辅助推断用户隐私的定量化研究和隐私攻击者(敌手)拥有关联背景知识情景下的最优化隐私机制研究。此外，当前差分隐私保护系统中主要考虑敌手观察扰动数据后的被动攻击行为[?]，较少考虑敌手的隐私攻击策略对系统的影响。基于此，本文聚焦在差分隐私应用中面临的核心热点问题。受已有工作的启发，本文利用信息论、博弈均衡理论、优化理论的方法，从基础的隐私度量、优化模型、算法设计等方面研究差分隐私最优化隐私机制问题，力图为差分隐私应用中权衡隐私与数据效用提供一种基于均衡、优化的理论支撑。为了实现本文目标，提炼出以下4个关键问题：

(1) 隐私与效用的度量

围绕隐私保护中隐私与效用之间的权衡问题，对数据隐私与效用的合理度量是研究隐私保护机制的基础，但是，由于应用场景的复杂性，隐私信息在不同应用中难以被准确刻画，存在隐私度量缺乏定量化定义[?]的问题。事实上，隐私泄露分析与敌手攻击模型密切相关，不同的系统模型和敌手模型下，隐私与效用的度量应该表达出敌手的隐私偏好和隐私推断能力。重要的是，隐私与效用的度量是研究隐私与效用权衡问题的一项基础且关键的工作，同时也是建立后续模型的基础。因此，隐私与效用的度量成为一个首要解决的关键问题。

(2) 权衡隐私与效用的优化模型

根据隐私与效用原则[?]，隐私保护中的隐私与数据效用之间存在相互依存且矛盾对立的关系，同时，它们也是隐私保护机制的两个重要评价指标。针对此，采用优化

理论的方法寻找一个最优的权衡折中是理想的解决方法。但其关键在于如何将它们形式化为一个约束条件下目标函数最小化形式的可求解问题。如差分隐私数据发布场景中，约束质量损失函数在一定的阈值，最小化隐私泄露的优化模型是一种解决方案。由此可见，在不同的敌手模型下，形式化隐私与效用的权衡问题为具体的优化模型是隐私保护机制设计的关键。针对不同的敌手模型和差分隐私应用场景，差分隐私的机制设计仍需要更进一步的研究。

(3) 隐私保护机制的设计

设计合理的隐私机制是隐私保护的一个核心研究内容。目前的差分隐私随机概率映射机制，大多是具有某些特殊性质的条件概率分布集合，如对称机制[?]、k-RR[?]机制等。如果在差分隐私应用中考虑敌手可能拥有的先验分布知识，则最优化的隐私机制需要考虑数据先验分布的影响。隐私机制设计依赖于先验分布而独立于隐私数据。针对诸如此类的需求，通过隐私分析建立优化模型，求解计算最优隐私保护机制的概率密度函数是一种解决方案。此外，对于优化问题的计算方法，计算开销，以及推广到多维或高维数据时的隐私机制设计都需要进一步的研究，这是完成隐私保护方案设计的关键。

(4) 隐私保护机制的评价方法

隐私保护机制的评价是衡量隐私保护效果的重要方法，涉及到隐私度与数据质量两个方面。通常情况下，隐私度与数据质量(数据效用)是评价隐私保护机制的两个主要指标。在差分隐私中，不可分辨水平ε和数据质量损失(如l-范数距离、均值平方误差、欧几里得距离、失真函数等)是主要的隐私和数据效用的评价指标。但是，不可分辨水平的ε隐私度量仅依赖于差分隐私条件概率的比值。由此，ε隐私度量面对等价的差分隐私机制时，则存在无法评价的问题。另外，在多维属性、数据关联的差分隐私处理环境中，属性的相关度测量以及相关度损失需要进行量化，它们也是评价差分隐私机制的重要指标。鉴于此，对于隐私保护机制的评价尚需要进一步的延伸拓展，需要结合具体的隐私保护系统模型评价隐私保护机制的性能。

1.4 研究内容与成果

围绕差分隐私应用场景中隐私与效用权衡的核心问题，本文研究差分隐私的最优化机制需要解决上述4个关键问题。为此，本文基于信息论方法、最优化理论以及博弈均衡理论研究提出了差分隐私的均衡优化模型及相应算法，实现隐私保护与数据效用的权衡折中。概括地说，本文的研究内容主要有：(1) 差分隐私通信模型及其度量方法；(2) 差分隐私均衡优化模型；(3) 差分隐私均衡优化模型的算法。三个研究内容相辅相成，具有较明确的内在逻辑性，下图1.3展现了本文的核心研究内容及其内在支撑关系。其中，研究内容(1) 为基础，支撑理论模型与算法的研究，研究内容(2)和(3)相

互依赖并支撑计算最优隐私机制的概率分布，三者形成本文的核心研究内容，共同支撑外围差分隐私的应用。

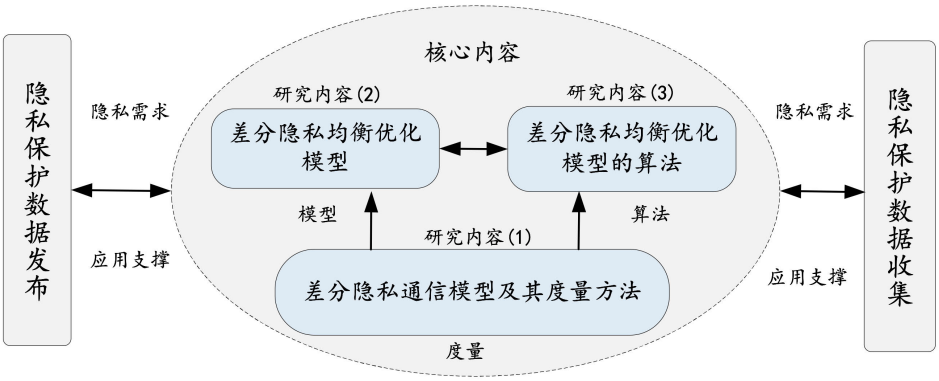

图 1.3: 本文核心研究内容及其关系

针对上述研究内容，本文在国家自然科学基金项目“理性隐私计算及隐私风险可控技术研究”的资助下，针对差分隐私保护模型开展了隐私信息熵度量、均衡与优化模型、隐私机制设计以及算法等方面的研究。本文的主要贡献是针对差分隐私多维及关联数据隐私保护的隐私与效用权衡问题，提出差分隐私的信息熵度量模型，权衡隐私与效用的均衡、优化模型及隐私机制设计方法。具体取得的主要成果有：

(1) 差分隐私通信模型及其度量方法

差分隐私的随机响应机理与信息论的噪声信道机制工作原理不谋而合，具有自然的相似性。以此为基本出发点，信息论方法被应用到差分隐私的研究中，并获得了一定的研究基础。在此方面，信息熵、条件熵、互信息量、率失真等基础方法均获得了具体的应用。但是，综述发现存在的工作中大多针对单一的敏感属性，拓展到多维属性的研究还相对较少。此外，现实中的多维属性极少存在相互独立的情景，大多存在数据关联，这种关联的相关性会增加个体隐私被推断的风险。然而，目前的研究尚缺失多维属性关联的差分隐私度量工作。

针对上述提到的问题，本文首先基于差分隐私的随机化响应原理，借鉴Shannon基本通信模型构建差分隐私的基本通信模型，并给出其形式化表述。以此基本通信模型为基础，考虑差分隐私不同应用场景中的隐私攻击者(敌手)模型，提出差分隐私通信模型中含背景知识的通信模型。在隐私度量方面，以基本的信息熵、条件熵、互信息量为基础，分别针对独立与关联的情景，提出了面向多维属性的隐私度量模型，给出了定量的信源熵、互信息量、联合熵、条件互信息的度量函数。进一步，在面向多维属性关联的差分隐私数据发布中，基于图模型、马尔可夫模型等，提出了多维属性关联的差分隐私信息泄露度量模型及方法。在数据效用度量方面，本文以构建的差分隐私通信模型为基础，借鉴信息论中的率失真理论，利用失真函数(损失函数)从数据重构的视角量化扰动数据表达原始数据的失真程度，给出了多维属性的效用度量，即是

数据质量。最后，在度量随机扰动对多维数据关联的影响时，基于相关度度量、图理论，提出了多维数据关联依赖图的结构信息(Structural Information)度量方法。

(2) 差分隐私均衡优化模型

在差分隐私的应用中，隐私泄露风险及数据可用性与所使用的隐私保护机制密切相关。为了获得理想的隐私保护效果和合理的数据质量，差分隐私的最优化机制问题一直都是学术研究的焦点。学术研究进行了有意义的探索，存在的工作中已提出了一些最优的差分隐私方案。首先是针对“是” 和“ 否”的问题，提出了二元数据的最优随机响应方案。其次，将问题扩展到类别型数据的多元随机响应方案。注意到，诸如此类的差分隐私方案将属性域的笛卡尔积作为信源字母表。如此以来，直接扩展上述方案到多维属性时，由于数据稀疏、域值空间大的问题，给隐私机制带来新的挑战。例如，在处理效率和数据效用方面性能打折。此外，在一些应用中可能是消息灵通的敌手模型，即有关数据拥有一定的先验知识。更有甚者，隐私攻击可以是策略型的敌手模型，这样的敌手不是像传统模型中考虑的敌手在观察到扰动数据后被动的攻击，相反，策略型的敌手可以与隐私保护系统进行交互，利益驱使他们偏爱最大收益的策略[? ?]。针对这些问题的研究还不充分，促使研究者提出新的差分隐私机制方案。

针对上述问题，本文以差分隐私基本通信模型及其度量为基础，利用信息论、优化理论以及博弈均衡理论，提出了权衡隐私与数据效用的差分隐私均衡优化模型。首先，分析隐私保护系统参与者的隐私目标，利用信息熵度量模型及方法，将数据发布系统中数据发布的目标表达为给定数据失真约束条件下互信息隐私泄露的最小化问题，给出基本的优化模型。随后，在基本通信模型基础上引入含背景知识的敌手推断模型，提出了背景知识关联的差分隐私最优化模型，用于数据发布的差分隐私机制设计。此外，在隐私保护的多维数据收集场景中，形式化表达了互信息隐私与失真的优化模型，并进一步将其推广到多维数据情景，设计了面向多维数据收集的有序随机响应扰动(Orderly Randomized Response Perturbation，ORRP) 方案。更多地，在基础通信模型中考虑了策略型的敌手模型，基于量化信息流(QIF) 提出了隐私保护的攻防博弈(Privacy-Preserving Attack and Defense，PPAD)模型，并从博弈均衡的角度分析了差分隐私的最优策略行动。基于冯· 诺依曼- 摩根斯坦效用理论，理性的策略选择为等价的差分隐私机制提供了一种机制比较的方法。最后，分析表明均衡策略是最差情况的隐私泄露上界，其可用于评估隐私风险。

(3) 差分隐私均衡优化模型的算法

本文研究的差分隐私最优化机制，在设计过程中主要包含有两个阶段：第一，依据系统的隐私、效用目标形式化一个均衡优化模型，并求解提出的模型计算出最优化隐私机制的概率分布函数；第二，根据得到的概率分布函数设计出具体的隐私保护方案实现隐私数据的随机扰动。鉴于此，对于所提出的差分隐私均衡优化模型求解的问题，算法的研究是个关键。本文研究在算法方面获得的主要成果有：

首先，针对差分隐私数据发布应用中敌手背景知识关联情景，本文修改了率失真函数，提出最优互信息隐私与失真模型，形式化模型表述与著名的率失真(Rate-distortion)函数具有相似的形式。由此，借鉴率失真求解的双重交替最小化Blahut-Arimoto (B-A)算法[??]提出了隐私与失真模型的求解算法，并给出了算法的计算复杂性分析。其次，针对差分隐私的本地化应用，使用B-A算法作为基本的构建模块，设计了有序随机响应扰动(ORRP)方案的实现算法，遵循两个阶段实现随机元组扰动。此外，针对多维数据关联损失度量问题，设计了多维属性相关度分析及关联损失量化的算法，并从理论上分析了所设计算法的计算复杂性。最后，对于本文所提出的隐私保护攻防博弈(PPAD)模型，基于交替最优响应策略选择，设计了均衡计算的策略优化选择算法。对于算法的研究增强了理论模型的可行性，与所提出的理论模型相辅相成。

1.5　论文组织结构

本文研究了差分隐私数据发布、数据收集场景中隐私与数据效用权衡的差分隐私均衡优化模型与算法。全文共分为七章，组织结构如图1.4所示，各章节内容的具体安排如下：

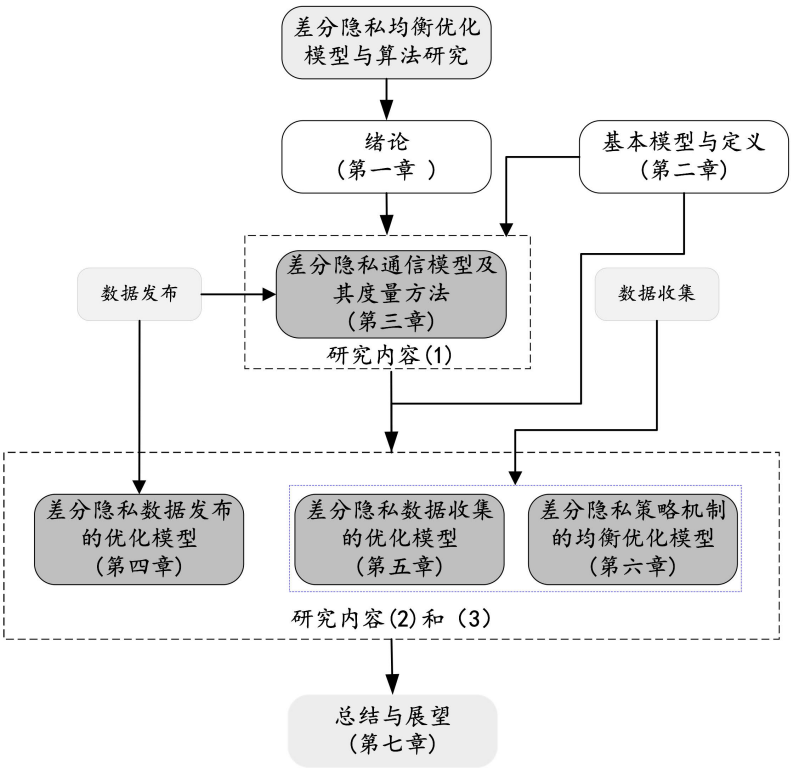

图 1.4: 本文的章节内容组织结构图

第一章为绪论，首先阐述了本文的研究背景及意义，随后针对差分隐私分析了存

在的问题，凝练出本文研究需要解决的关键问题。基于上述分析，阐述了本文的研究内容和研究取得的主要成果。最后给出了本文的章节组织结构安排。

第二章为基本模型与定义，介绍了本文研究所使用的基本模型与定义。首先，给出了隐私、隐私泄露的定义，并阐述了差分隐私模型及定义。其次，叙述了Shannon信息论的通信模型，引入信息熵、条件熵、联合熵、互信息量等概念，以此为基础介绍了数据处理不等式、费诺不等式和率失真理论等内容。随后，阐述了最优化问题、对策博弈以及凹凸博弈的相关知识。最后，以上述为基础，给出了本文中差分隐私均衡优化的定义，界定后续研究的范畴。

第三章为差分隐私通信模型及其度量方法，建立差分隐私与信息论的基本联系，奠定本文的研究基础。首先，基于Shannon基本通信模型，介绍了差分隐私基本通信模型，并给出了形式化的模型表达。其次，以差分隐私的基本通信模型为基础，引入信息熵、互信息、失真的概念对隐私与效用进行度量，提出信息熵度量模型及方法。进一步，在基本的度量基础上，针对多维关联属性的情景，提出面向关联属性的差分隐私信息熵度量方法，本章中的度量模型及方法为开展后续章节的研究奠定了基础。

第四章为差分隐私数据发布的优化模型，研究了隐私与数据效用权衡的最优差分隐私机制。首先，基于第二章基础、第三章差分隐私通信模型及度量方法，分析了隐私系统的目标，借鉴率失真理论构建了面向差分隐私数据发布的优化模型。其次，在基本的通信模型基础上引入敌手模型，并考虑了敌手拥有关联辅助背景知识对隐私泄露的影响，提出了基于联合事件的互信息隐私度量。随后，修改率失真表述形式，提出了最小化隐私泄露的优化模型，用于获得隐私机制的概率分布函数。此外，设计了互信息隐私最优信道机制的近似迭代求解算法，并给出具体的验证分析。

第五章为差分隐私数据收集的优化模型，围绕隐私保护机制设计的两个阶段，研究了面向数据收集的多维数据最优隐私机制。首先，以第三章的度量为基础，形式化互信息隐私(MI-privacy)最优化模型，设计模型求解算法寻找最优机制的概率密度函数。随后，将其作为基本构建模块应用到多维数据，提出有序随机响应扰动(ORRP)方案。最后，针对提出的ORRP方案，介绍了隐私、数据效用以及相关度损失的评估与分析，并利用真实数据集给出了所提方案的实验分析。

第八章为差分隐私策略机制的均衡优化模型，应用博弈均衡理论研究了差分隐私策略机制选择问题。通过分析隐私保护系统参与者的隐私目标，基于信息熵度量模型及方法将隐私目标形式化为隐私泄露的极大极小问题。然后，分析系统参与者的可行策略，构建了隐私保护的攻防博弈(PPAD)模型。针对本文关注的应用，实例化PPAD为两方零和对策博弈模型，并提供了均衡的理论分析以及算法实现。最后，阐述了均衡在隐私保护中的内涵及意义。

第九章为总结与展望，首先总结了本文的研究工作，进一步，展望了未来研究工作的方向和重点。

第二章　Kripke结构、时序逻辑、模型检测以及遗忘理论

本章主要介绍本文用到的符号、术语以及逻辑理论基础，包括：*Kripke*结构、时序逻辑（尤其是计算树逻辑（*CTL*）和μ-演算）、模型检测和遗忘理论。首先，介绍解释时序逻辑语言所需的模型结构，即*Kripke*结构。其次，主要介绍时序逻辑中本文探讨的计算树逻辑和μ-演算。为了更加明确本文的研究动机，本章将详细介绍模型检测的基本概念和一些主要的性质。此外，遗忘理论是本文的研究重点，其概念、性质及在各个研究领域的研究和应用情况将会被当作本章的重点详细介绍。

为了方便，本文将命题变量（也叫原子命题）的集合记作$\mathscr{A}$，$V \subseteq \mathscr{A}$ 是$\mathscr{A}$的子集。此为，规定$\overline{V}$是V在$\mathscr{A}$上的补，也即是$\overline{V} = \mathscr{A} - V$。

2.1　Kripke结构

Kripke结构作为一种表示转换系统（transition system）的数学模型，在理论计算机科学领域有着广泛的应用，尤其是作为解释时序逻辑公式的模型结构。

2.1.1　真假赋值和K-解释

经典命题语言$\mathscr{L}^p$由以下三类符号构成：

- 命题符号：一般用小写拉丁字母p，q，r，...来表示，且这些命题符号来源于$\mathscr{A}$；
- 联结符号：$\neg$（否定），$\wedge$（合取），$\vee$（吸取），$\rightarrow$（蕴涵），$\leftrightarrow$（等值于）；
- 标点符号：(（左括号），)（右括号）。

$\mathscr{L}^p$的原子公式的集合和公式的集合分别记作$Atom(\mathscr{L}^p)$和$\mathscr{F}(\mathscr{L}^p)$。其中，$Atom(\mathscr{L}^p)$是命题符号的集合，且$\varphi \in \mathscr{F}(\mathscr{L}^p)$当且仅当它能由（有限次使用）以下的三条规则生成[?]：

- 如果$\varphi \in Atom(\mathscr{L}^p)$，则$\varphi \in \mathscr{F}(\mathscr{L}^p)$。
- 如果$\varphi \in \mathscr{F}(\mathscr{L}^p)$，则$(\neg\varphi) \in \mathscr{F}(\mathscr{L}^p)$。
- 如果φ，$\varphi' \in \mathscr{F}(\mathscr{L}^p)$，则$(\varphi * \varphi') \in \mathscr{F}(\mathscr{L}^p)$。其中，$* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$。

此外，也称“ture”和“false”为原子公式，分别记为“$\top$”和“$\bot$”。原子命题或其否定称为文字，有限个文字的吸取称为子句。

例 2.1. 下面几个字符串为$\mathscr{L}^p$的公式：

- $(q \vee p)$；
- $(((\neg p) \leftrightarrow (q \vee r)) \rightarrow (r \wedge p))$。

而字符串$p \wedge \vee q$不属于集合$\varphi \in \mathscr{F}(\mathscr{L}^p)$。

为了方便，称$\mathscr{L}^p$的公式为命题公式（在不引起歧义的情况下也称之为公式）。此外，规定联结符号的优先级有助于简化公式（省略掉冗余的标点符号）。为此，规定在下面的序列中，每个左边的联结符号优先于右边的联结符号。

$$\neg \qquad \wedge \qquad \vee \qquad \rightarrow \qquad \leftrightarrow$$

此时，例 2.1中的公式$(((\neg p) \leftrightarrow (q \vee r)) \rightarrow (r \wedge p))$就可写为$(\neg p \leftrightarrow q \vee r) \rightarrow r \wedge p$。当然，为了看起来方便，有的括号可以不必省略。

在讨论了命题公式的语法结构之后，接下来将讨论其语义解释。

定义 2.1 (真假赋值). 真假赋值是以所有命题符号的集为定义域，以真假值的集$\{0,1\}$为值域的函数$v : \mathscr{A} \rightarrow \{0,1\}$。

为了方便，后文中也将$\top$代表1，$\bot$代表0（此时真假赋值为$v : \mathscr{A} \rightarrow \{\bot, \top\}$），且满足对任意的真假赋值$v$都有$\top^v = 1$和$\bot^v = 0$。由该定义可知，真假赋值的个数为$2^{|\mathscr{A}|}$个，因为一个真假赋值要同时给$\mathscr{A}$中的所有命题符号指派一个真假值。真假赋值$v$给公式$\varphi$指派的值记作$\varphi^v$，其被形式化定义为如下：

定义 2.2 (公式的真假值). 真假赋值v给公式指派的真假值递归定义如下：

- $p^v \in \{\bot, \top\}$，其中$p \in \mathscr{A}$。
- $(\neg\varphi)^v = \begin{cases} \top, & \text{如果} \varphi^v = \top; \\ \bot, & \text{否则。} \end{cases}$
- $(\varphi \wedge \psi)^v = \begin{cases} \top, & \text{如果} \varphi^v = \psi^v = \top; \\ \bot, & \text{否则。} \end{cases}$
- $(\varphi \vee \psi)^v = \begin{cases} \top, & \text{如果} \varphi^v = \top \text{或} \psi^v = \top; \\ \bot, & \text{否则。} \end{cases}$
- $(\varphi \rightarrow \psi)^v = \begin{cases} \top, & \text{如果} \varphi^v = \bot \text{或} \psi^v = \top; \\ \bot, & \text{否则。} \end{cases}$

- $(\varphi \leftrightarrow \psi)^v = \begin{cases} \top, & \text{如果} \varphi^v = \psi^v; \\ \bot, & \text{否则。} \end{cases}$

对于任意的命题公式φ和真假赋值v，当$\varphi^v = \top$时，称v是公式φ的一个模型，也可以记为$v \models \varphi$，读作v满足φ。一般地，当存在一个真假赋值v使得$v \models \varphi$，则称公式φ是可满足的。如果φ是可满足的，且$\neg\varphi$是不可满足的，则称φ是有效的。

值得注意的是，命题逻辑的语义也可定义在“解释（interpretation）”上。一个解释I是$\mathscr{A}$的子集。除了对原子命题$p \in \mathscr{A}$，I对公式的解释如真假赋值一样。在解释原子命题$p \in \mathscr{A}$上，p^I为真当且仅当$p \in I$。模型和可满足的定义与真假赋值的类似。

模态逻辑是经典逻辑的扩充，它是经典逻辑中引进“必然”和“可能”这两种模态词得到的。如上所述，命题的真假值只有两种，命题是真的（1）或是假的（0）。而在模态逻辑中，把命题区分为必然真的命题和并非必然真的命题，把假命题区分为必然假的和并非必然假的命题。对于任何命题φ，可以有两种模态命题：“φ是必然的”和“φ是可能的”。值得注意的是，时序逻辑也是模态逻辑的一种[1]。尽管如此，本文在说模态逻辑的时候通常指不带有时序操作符的情况，说时序逻辑时指带有时序操作符的情况。

本文所说的模态逻辑为命题单模态逻辑（propositional mono-modal logic）。模态公式的集合$\mathscr{F}^{\mathscr{M}}$是包含“$\top$”和“$\bot$”的满足如下条件的最小集：

- $\mathscr{A} \subseteq \mathscr{F}^{\mathscr{M}}$；
- 如果$\varphi \in \mathscr{F}^{\mathscr{M}}$，则$(\neg\varphi)$，$(\mathrm{K}\varphi) \in \mathscr{F}^{\mathscr{M}}$；
- 如果φ，$\psi \in \mathscr{F}^{\mathscr{M}}$，则$(\varphi * \psi) \in \mathscr{F}^{\mathscr{M}}$，其中$* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$。

令$\mathrm{B} = \neg\mathrm{K}\neg$，则$\mathrm{B}\varphi \in \mathscr{F}^{\mathscr{M}}$。其中，K和B叫做模态符号，分别表示“必然”和“可能”。

可能世界语义（或*Kripke*语义）是标准的命题模态逻辑语义[?]。Kripke语义是定义在Kripke结构上的，一个Kripke结构是一个三元组(S, R, L)（下一节中将详细介绍）。其中，S是状态的非空集合，$R \subseteq R \times R$是可达性关系。特别地，当R是一个等价关系的时候（模态逻辑S5中），一个Kripke结构可以写成一个二元组$\langle W, w\rangle$，其中W是状态的非空集合，w是W中的元素，每个状态是原子命题的集合。此时，称$\mathscr{M} = \langle W, w\rangle$为一个K-解释（K-interpretation）[?]。

定义 2.3. 给定一个K-解释$\mathscr{M} = \langle W, w\rangle$，其与$\mathscr{F}^{\mathscr{M}}$中的公式的可满足关系被归纳地定义为：

- $\mathscr{M} \not\models \bot$，$\mathscr{M} \models \top$；
- $\mathscr{M} \models p$当且仅当$p \in w$，其中$p \in \mathscr{A}$；

- $\mathscr{M} \models \neg\varphi$当且仅当$\mathscr{M} \not\models \varphi$；
- $\mathscr{M} \models \varphi \supset \psi$当且仅当$\mathscr{M} \not\models \varphi$或$\mathscr{M} \models \psi$；
- $\mathscr{M} \models \mathrm{K}\varphi$当且仅当$\forall w' \in W$有$\langle W, w'\rangle \models \varphi$。

$\mathscr{M} = \langle W, w\rangle$称为公式$\varphi$的K-模型（K-model），当且仅当$\mathscr{M} \models \varphi$。此外，如果存在一个$\mathscr{M} = \langle W, w\rangle$使得公式$\mathscr{M} \models \varphi$，则称公式$\varphi$是可满足的。如果$\mathscr{M} \models \varphi$对于所有的$\mathscr{M} = \langle W, w\rangle$都成立，则称$\varphi$是有效的。

2.1.2 Kripke结构的定义及相关术语

通常一个转换系统（transition system）能够被抽象为一个Kripke结构[2]。如上文所说，一个Kripke结构是一个三元组$\mathscr{M} = (S, R, L)$，其中：

- S是状态的非空集合；
- $R \subseteq S \times S$是状态转换函数；
- $L : S \to 2^{\mathscr{A}}$是一个标签函数。

在本文中，要求R是一个串行关系（serial relation），也即是对于S中的任意元素s，都存在S中的一个元素s'使得$(s, s') \in R$。

给定一个Kripke结构$\mathscr{M} = (S, R, L)$，$\mathscr{M}$上的一条路径是一个无限的状态序列$\pi = (s_0, s_1, \ldots)$且满足对于任意的$j \geq 0$都有$(s_j, s_{j+1}) \in R$，路径上的状态s被记为$s \in \pi$。当给路径π引入一个状态s作为下标，记为π_s，则称该路径是起点为该状态s的一条路径。如果对于$\mathscr{M}$中的任意状态s'，都有一条以s为起点的路径π_s使得$s' \in \pi_s$，那么称状态s为一个*初始状态*。给定s_0为$\mathscr{M}$中的一个初始状态，为了容易看出该初始状态，将该Kripke结构写为四元组(S, R, L, s_0)，并称该结构为*初始结构*以区分于原来的三元组。

*树*是一种只有一个根节点（没有其他节点指向且可达于其他节点的节点）无环图。给定一个初始结构$\mathscr{M} = (S, R, L, s_0)$和一个状态$s \in S$，定义在$\mathscr{M}$上以$s$为根节点的深度为为$n$（$n \geq 0$）的*计算树*$\mathrm{Tr}_n^{\mathscr{M}}(s)$被递归定义如下[3]：

- $\mathrm{Tr}_0^{\mathscr{M}}(s)$ 是只有一个节点s（其标签为$L(s)$）树。
- $\mathrm{Tr}_{n+1}^{\mathscr{M}}(s)$是以$s$为根节点（标签为$L(s)$）的树，并且满足若$(s, s') \in R$，则节点$s$有一棵子树$\mathrm{Tr}_n^{\mathscr{M}}(s')$。

一个初始结构$\mathscr{M} = (S, R, L, s_0)$和一个状态$s \in S$构成一个K-*结构*（或K-解释），写作$\mathscr{K} = (\mathscr{M}, s)$。在K-结构$\mathscr{K} = (\mathscr{M}, s)$中，若$s = s_0$，则称该K-结构为*初始K-结构*，此时有$\mathscr{K} = (\mathscr{M}, s_0)$。

2.2　时序逻辑

时序逻辑是一种描述系统规范的形式化语言，它研究状态随时间变化的系统的逻辑特性。由于软件和硬件的运行的本质是状态变化的过程，所以时态逻辑在软件程序验证和硬件验证中应用得相当广泛。计算树逻辑（Computation Tree Logic, CTL）是分支时态逻辑的一种，其模型检测是多项式时间可行的。然而，CTL表达系统性质的表达能力不如μ-演算（μ-calculus），如：“某给定的系统中存在一条路径使得该路径上的第偶数个状态满足特定的性质”这一规范是不能用其他时态逻辑表示的[18]。充分考虑这两种逻辑语言自身的特性，本节主要介绍CTL和μ-演算。因此，本文所说的公式指CTL（或μ-演算）公式，即用来描述一个规范（或性质）的公式是CTL（或μ-演算）公式。

2.2.1　计算树逻辑（CTL）

CTL由Clark和Emerson等人于1986年提出[4]。CTL的语言$\mathscr{L}$由下面的几类符号构成：

- 原子命题的集合$\mathscr{A}$；
- 常量符号：$\top$和$\bot$，分别表示“真”和“假”；
- 联结符号：$\vee$和$\neg$，分别表示“吸取”和“否定”；
- 路径量词：A和E，分别表示“所有”和“存在”；
- 时序操作符：X、F、G、U和W，分别表示“下一个状态”、“将来某一个状态”、“将来所有状态”、“直到”和“除非”；
- 标点符号：“(”和“)”。

CTL的时序算子是路径量词和时序操作符的组合（路径量词在前，时序操作符在后），如：AX，EX，AF等。与经典命题逻辑一样，给联结符号规定优先级，有时候会带来意想不到的方便。CTL中的联结符号的优先级如下序列所示，每个左边的联结符号优先于右边的联结符号：

$$\neg \quad \mathrm{EF} \quad \mathrm{EG} \quad \mathrm{AX} \quad \mathrm{AF} \quad \mathrm{AG} \quad \wedge \quad \vee \quad \mathrm{EU} \quad \mathrm{EW} \quad \mathrm{AW} \quad \rightarrow$$

因此，语言$\mathscr{L}$的*存在范式(existential normal form, ENF)*可以用巴科斯范式递归定义如下：

$$\phi ::= \bot \mid \top \mid p \mid \neg\phi \mid \phi \vee \phi \mid \mathrm{EX}\phi \mid \mathrm{EG}\phi \mid \mathrm{E}(\phi \ \mathrm{U} \ \phi) \tag{2.1}$$

其中，$p \in \mathscr{A}$。$\mathscr{L}$中其他形式的公式可以通过下面的定义（使用上述定义中(2.1)的形式）得到：

$$\varphi \wedge \psi \stackrel{def}{=} \neg(\neg\varphi \vee \neg\psi) \tag{2.2}$$

$$\varphi \rightarrow \psi \stackrel{def}{=} \neg\varphi \vee \psi \tag{2.3}$$

$$\mathrm{A}(\varphi \mathrm{U} \psi) \stackrel{def}{=} \neg\mathrm{E}(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \neg\mathrm{EG}\neg\psi \tag{2.4}$$

$$\mathrm{A}(\varphi \mathrm{W} \psi) \stackrel{def}{=} \neg\mathrm{E}((\varphi \wedge \neg\psi)\mathrm{U}(\neg\varphi \wedge \neg\psi)) \tag{2.5}$$

$$\mathrm{E}(\varphi \mathrm{W} \psi) \stackrel{def}{=} \neg\mathrm{A}((\varphi \wedge \neg\psi)\mathrm{U}(\neg\varphi \wedge \neg\psi)) \tag{2.6}$$

$$\mathrm{AF}\varphi \stackrel{def}{=} \mathrm{A}(\top \mathrm{U} \psi) \tag{2.7}$$

$$\mathrm{EF}\varphi \stackrel{def}{=} \mathrm{E}(\top \mathrm{U} \psi) \tag{2.8}$$

$$\mathrm{AX}\varphi \stackrel{def}{=} \neg\mathrm{EX}\neg\varphi \tag{2.9}$$

$$\mathrm{AG}\varphi \stackrel{def}{=} \neg\mathrm{EF}\neg\varphi \tag{2.10}$$

此外，对于给定的公式φ，其否定范式（negation normal form, NNF）是将否定联结词“$\neg$”的出现通过上述定义变化到只出现在原子命题之前的形式。

CTL的语义定义在Kripke结构上，可以严格地描述如下。

定义 2.4 (CTL的语义). 给定*CTL*公式φ，初始结构$\mathscr{M} = (S, R, L, s_0)$和状态$s \in S$。$(\mathscr{M}, s)$与$\varphi$之间的可满足关系$(\mathscr{M}, s) \models \varphi$定义如下：

- $(\mathscr{M}, s) \not\models \bot$且$(\mathscr{M}, s) \models \top$；
- $(\mathscr{M}, s) \models p$ 当且仅当$p \in L(s)$；
- $(\mathscr{M}, s) \models \varphi_1 \vee \varphi_2$当且仅当$(\mathscr{M}, s) \models \varphi_1$或$(\mathscr{M}, s) \models \varphi_2$；
- $(\mathscr{M}, s) \models \neg\varphi$当且仅当$(\mathscr{M}, s) \not\models \varphi$；
- $(\mathscr{M}, s) \models \mathrm{EX}\varphi$当且仅当存在$S$中的一个状态$s_1$，使得$(s, s_1) \in R$且$(\mathscr{M}, s_1) \models \varphi$；
- $(\mathscr{M}, s) \models \mathrm{EG}\varphi$当且仅当存在$\mathscr{M}$上的一条路径$\pi_s = (s_1 = s, s_2, \ldots)$，使得对每一个$i \geq 1$都有$(\mathscr{M}, s_i) \models \varphi$；
- $(\mathscr{M}, s) \models \mathrm{E}(\varphi \mathrm{U} \psi)$当且仅当存在$\mathscr{M}$上的一条路径$\pi_s = (s_1 = s, s_2, \ldots)$，使得对某一个$i \geq 1$有$(\mathscr{M}, s_i) \models \psi$，同时对任意的$1 \leq j < i$有$(\mathscr{M}, s_j) \models \varphi$。

与Browne和Bolotov等人的工作类似，本文只将初始K-结构作为模型的候选项[3,5]。换句话说，对于给定的K-结构$(\mathscr{M}, s)$和CTL公式φ，如果$(\mathscr{M}, s) \models \varphi$且$s = s_0$，则称$(\mathscr{M}, s)$为

公式φ的一个模型。更清楚地说，对于给定的初始K-结构$\mathscr{K}=(\mathscr{M},s_0)$，如果$\mathscr{K}\models\varphi$，则称$\mathscr{K}$是$\varphi$的一个模型。

为了符号的统一，这里列出文中出现的一些记号的含义。给定公式φ，公式的所有模型构成的集合记为$Mod(\varphi)$。此时就很容易定义公式的可满足性，即：如果$Mod(\varphi)\neq\emptyset$，则称$\varphi$是可满足的。给定两个公式$\varphi_1$和$\varphi_2$，若$Mod(\varphi_1)\subseteq Mod(\varphi_2)$，则称$\varphi_1$逻辑地蕴涵$\varphi_2$，记为$\varphi_1\models\varphi_2$。特别地，当$\varphi_1\models\varphi_2$且$\varphi_2\models\varphi_1$时，即$Mod(\varphi_1)=Mod(\varphi_2)$，则称$\varphi_1$和$\varphi_2$为逻辑等值公式（简称为等值公式），记作$\varphi_1\equiv\varphi_2$。值得注意的是，上述的记号也适用于讨论的对象为公式的集合的情形。此外，给定一个公式的集合Π和一个初始K-结构$\mathscr{K}$，若对于Π中的任意一个公式φ都有$\mathscr{K}\models\varphi$，则$\mathscr{K}\models\Pi$。

对于给定的公式φ，将出现在φ中的原子命题的集合记为$Var(\varphi)$。此外，给定公式φ和原子命题的集合V，如果存在一个公式ψ使得$Var(\psi)\cap V=\emptyset$且$\varphi\equiv\psi$，那么说$\varphi$与$V$中的原子命题无关，简称为$V$-无关（$V$-*irrelevant*），写作$\mathrm{IR}(\varphi,V)$。一种特殊的形式是$Var(\varphi)\subseteq V$，此时称$\varphi$为集合$V$上的公式。可以类似定义公式的集合与原子命题集合的无关性，也即是：如果对于公式的集合Π中的任意一个公式φ，$\mathrm{IR}(\varphi,V)$都成立，则Π与V中的原子命题无关，记为$\mathrm{IR}(\Pi,V)$。

2.2.2　CTL的标准形式

在讲述CTL的标准形式之前，先引入一种带有索引的CTL，记为CTL_{ind}。这种语言是在CTL的已有符号下加入下面几种符号得到：

- 命题常量符号**start**；
- 一个可数无限的索引集Ind；
- 带有索引ind（$ind\in\mathrm{Ind}$）的时序算子：$\mathrm{E}_{\langle ind\rangle}\mathrm{X}$, $\mathrm{E}_{\langle ind\rangle}\mathrm{F}$, $\mathrm{E}_{\langle ind\rangle}\mathrm{G}$, $\mathrm{E}_{\langle ind\rangle}\mathrm{U}$, 和$\mathrm{E}_{\langle ind\rangle}\mathrm{W}$。

与CTL公式的定义类似，其公式可以递归地定义如下：

$$\phi ::= \bot \mid \top \mid p \mid \neg\phi \mid \phi\vee\phi \mid \mathrm{EX}\phi \mid \mathrm{EG}\phi \mid \mathrm{E}(\phi\ \mathrm{U}\ \phi) \mid \mathrm{E}_{ind}\mathrm{X}\phi \mid \mathrm{E}_{ind}\mathrm{G}\phi \mid \mathrm{E}_{ind}(\phi\ \mathrm{U}\ \phi) \quad (2.11)$$

与CTL不同的是，CTL_{ind}的语义定义在一种扩展的初始-Kripke结构上，该结构被称为Ind-Kripke结构。一个Ind-Kripke结构是一个五元组$\mathscr{M}=(S,R,L,[_],s_0)$，且除了$[_]$，其余元素都跟初始结构中的元素对应。该五元组中的$[_]$是一个以Ind为定义域，$2^{S\times S}$为值域的后继函数，即$[_]:\mathrm{Ind}\to 2^{S\times S}$，且满足对于任意的$s\in S$都存在唯一一个$s'\in S$使得$(s,s')\in[ind]\cap R$。记$\pi_{s_i}^{ind}$是$\mathscr{M}$上的一条路径$(s_i,s_{i+1},s_{i+2},\ldots)$，且对于任意的$j\geq i$都有：

$$(s_j,s_{j+1})\in[ind]$$

一个Ind-Kripke结构$\mathscr{M}$和其上的一个状态s构成一个*ind*-结构，记为$(\mathscr{M},s)$。同理，如果s是初始状态s_0，则称$(\mathscr{M},s_0)$为初始*ind*-结构。

令φ是一个CTL$_{ind}$公式、$\mathscr{K}=(\mathscr{M},s_0)$是一个初始*ind*-结构、且$s$是$\mathscr{M}$上的一个状态，则$\varphi$和$(\mathscr{M},s_0)$的可满足关系$(\mathscr{M},s_0)\models\varphi$被定义如下（这里只列出带有索引的公式的可满足关系，其余公式的可参加CTL部分的定义）：

- $(\mathscr{M},s)\models$ **start**当且仅当$s=s_0$；
- $(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}\mathrm{X}\psi$当且仅当对于路径$\pi_s^{\langle ind\rangle}$，有$(\mathscr{M},s')\models\psi$且$(s,s')\in[ind]$;
- $(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}\mathrm{G}\psi$当且仅当对于任意的$s'\in\pi_s^{\langle ind\rangle}$，$(\mathscr{M},s')\models\psi$;
- $(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}(\psi_1\mathrm{U}\psi_2)$ 当且仅当存在路径$\pi_s^{\langle ind\rangle}=(s=s_1,s_2,\ldots)$上的状态$s_j$（$j\geq 1$），使得$(\mathscr{M},s_j)\models\psi_2$，且对于任意的$s_k\in\pi_s^{\langle ind\rangle}$，若$1\leq k<j$，则$(\mathscr{M},s_k)\models\psi_1$；
- $(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}\mathrm{F}\psi$当且仅当$(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}(\top\mathrm{U}\psi)$；
- $(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}(\varphi\mathrm{W}\psi)$当且仅当$(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}\mathrm{G}\varphi$或$(\mathscr{M},s)\models \mathrm{E}_{\langle ind\rangle}(\varphi\mathrm{U}\psi)$。

对于给定的公式φ和初始*ind*-结构$\mathscr{K}=(\mathscr{M},s_0)$，如果$\mathscr{K}\models\varphi$，则称$\mathscr{K}$是$\varphi$的一个*Ind*-模型，也称$\mathscr{K}$满足$\varphi$。其他的术语与CTL部分的类似，这里不再赘述。

已有结果表明，任意的CTL公式能够在多项式时间内被转换为CTL的全局子句分离的范式（separated normal form with global clauses for CTL，SNF$^g_{\mathrm{CTL}}$子句）[6-7]。SNF$^g_{\mathrm{CTL}}$子句是具有下面几种形式的公式：

$\mathrm{A}\mathrm{G}(\mathbf{start}\rightarrow\bigvee_{j=1}^{k}m_j)$	(初始句，initial clause)
$\mathrm{A}\mathrm{G}(\top\rightarrow\bigvee_{j=1}^{k}m_j)$	(全局子句，global clause)
$\mathrm{A}\mathrm{G}(\bigwedge_{i=1}^{n}l_i\rightarrow\mathrm{A}\mathrm{X}\bigvee_{j=1}^{k}m_j)$	(A-步子句，A-step clause)
$\mathrm{A}\mathrm{G}(\bigwedge_{i=1}^{n}l_i\rightarrow\mathrm{E}_{\langle ind\rangle}\mathrm{X}\bigvee_{j=1}^{k}m_j)$	(E-步子句，E-step clause)
$\mathrm{A}\mathrm{G}(\bigwedge_{i=1}^{n}l_i\rightarrow\mathrm{A}\mathrm{F}l)$	(A-某时子句，A-sometime clause)
$\mathrm{A}\mathrm{G}(\bigwedge_{i=1}^{n}l_i\rightarrow\mathrm{E}_{\langle ind\rangle}\mathrm{F}l)$	(E-某时子句，E-sometime clause)

其中k和n都是大于0的常量，**start**是命题常量符号，l_i（$1\leq i\leq n$）、m_j（$1\leq j\leq k$）和l都是文字，且$ind\in$ Ind。从上述标准形式中，可以看到每个SNF$^g_{\mathrm{CTL}}$子句都是$\mathrm{A}\mathrm{G}(P\rightarrow G)$形式。因此在没有歧义的情况下，下文中将使用$P\rightarrow G$指代这些子句。此外，除了额外说明，本文通常讲SNF$^g_{\mathrm{CTL}}$子句和子句统称为子句。

对于给定的公式φ（其中的$\rightarrow$符号都用$\vee$和$\neg$表示），如果φ中所有原子命题p的出现都有偶数个否定符号在其之前，则称φ关于p是正的，否则称φ关于p是负的。此外，

对于给定的公式集合，如果该集合中的所有公式关于p都是正的，则说该集合关于p是正的，否则该集合关于p是负的。

一个CTL公式φ可以通过表 2.1中的规则将其转换为一个$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合，记为$T_{\varphi}$。

表 2.1: 转换规则

Trans(1) $\dfrac{q \to \mathrm{E}T\varphi}{q \to \mathrm{E}_{\langle ind\rangle}T\varphi}$;	**Trans(2)** $\dfrac{q \to \mathrm{E}(\varphi_1 \mathrm{U} \varphi_2)}{q \to \mathrm{E}_{\langle ind\rangle}(\varphi_1 \mathrm{U} \varphi_2)}$;	**Trans(3)** $\dfrac{q \to \varphi_1 \wedge \varphi_2}{q \to \varphi_1, q \to \varphi_2}$;
Trans(4) $\dfrac{q \to \varphi_1 \vee \varphi_2 \text{ (如果}\varphi_2\text{不是子句)}}{q \to \varphi_1 \vee p, p \to \varphi_2}$;		**Trans(5)** $\dfrac{q \to D}{\top \to \neg q \vee D}$; $\dfrac{q \to \bot}{\top \to \neg q}$; $\dfrac{q \to \top}{\{\}}$
Trans(6) $\dfrac{q \to Q\mathrm{X}\varphi \text{ (如果}\varphi\text{不是子句)}}{q \to Q\mathrm{X}p, p \to \varphi}$;		**Trans(7)** $\dfrac{q \to Q\mathrm{F}\varphi \text{ (如果}\varphi\text{不是文字)}}{q \to Q\mathrm{F}p, p \to \varphi}$;
Trans(8) $\dfrac{q \to Q(\varphi_1 \mathrm{U} \varphi_2) \text{ (如果}\varphi_2\text{不是文字)}}{q \to Q(\varphi_1 \mathrm{U} p), p \to \varphi_2}$;		**Trans(10)** $\dfrac{q \to Q\mathrm{G}\varphi}{q \to p, p \to \varphi, p \to Q\mathrm{X}p}$;
Trans(11) $\dfrac{q \to Q(\varphi \mathrm{U} l)}{q \to l \vee p, p \to \varphi, p \to Q\mathrm{X}(l \vee p), q \to Q\mathrm{F}l}$;		**Trans(12)** $\dfrac{q \to Q(\varphi \mathrm{W} l)}{q \to l \vee p, p \to \varphi, p \to Q\mathrm{X}(l \vee p)}$.

在表 2.1中，$T \in \{\mathrm{X}, \mathrm{G}, \mathrm{F}\}$，$ind$是规则中引入的新的索引且$Q \in \{\mathrm{A}, \mathrm{E}_{\langle ind\rangle}\}$；$q$是一个原子命题, l是一个文字, D是文字的吸取（即子句）, p是新的原子命题；φ，φ_1，和φ_2都是CTL公式。

规则**Trans(1)**和规则**Trans(2)**为每一个存在路径量词E引入一个新的索引ind；规则**Trans(3)**到规则**Trans(5)**通过引入新的替换规则将复杂的公式用新的原子命题替换；规则**Trans(6)**到规则**Trans(12)**用于移除掉那些不能出现在$\mathrm{SNF}^{g}_{\mathrm{CTL}}$中的时序操作符[8]。

给定一个CTL公式φ，将其转换为一个$\mathrm{SNF}^{g}_{\mathrm{CTL}}$字句集合的主要步骤如下：

(1) 将公式CTL转换为其NNF（negation normal form）[1]形式，记为$nnf(\varphi)$；

(2) 使用表 2.2中的等价公式化简$nnf(\varphi)$，得到$simp(nnf(\varphi))$；

(3) 使用表 2.1中的规则将$\{\mathrm{AG}(\mathbf{start} \to z), \mathrm{AG}(z \to simp(nnf(\varphi)))\}$化简为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合。

下面通过一个简单的例子来展示上述转换步骤：

例 2.2. 令$\varphi = \neg\mathrm{AF}p \wedge \mathrm{AF}(p \wedge \top)$，下面给出将$\varphi$转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$的详细步骤。(1) 将公式$\varphi$转换为其NNF形式：$\mathrm{EG}\neg p \wedge \mathrm{AF}(p \wedge \top)$；

(2) 化简(1)中的公式为：$\mathrm{EG}\neg p \wedge \mathrm{AF}p$；

[1]如果公式中的否定符号“¬”仅出现在原子命题之前，且联结符号只有“∨”和“∧”这两种，则称该公式是NNF形式的公式。

表 2.2: 化简规则。其中$Q \in \{\mathrm{A}, \mathrm{E}\}$且$T \in \{\mathrm{X}, \mathrm{G}, \mathrm{F}\}$。

$(\varphi \wedge \top) \to \varphi$;	$(\varphi \wedge \bot) \to \bot$;	$(\varphi \vee \top) \to \top$;
$(\varphi \vee \bot) \to \varphi$;	$\neg\top \to \bot$;	$\neg\bot \to \top$;
$QT\bot \to \bot$;	$QT\top \to \top$;	$Q(\varphi \mathrm{U} \bot) \to \bot$;
$Q(\varphi \mathrm{U} \top) \to \top$;	$Q(\bot \mathrm{U} \varphi) \to \varphi$;	$Q(\top \mathrm{U} \varphi) \to Q\mathrm{F}\varphi$;
$Q(\varphi \mathrm{W} \bot) \to Q\mathrm{G}\varphi$;	$Q(\varphi \mathrm{W} \top) \to \top$;	$Q(\bot \mathrm{W} \varphi) \to \varphi$;
$Q(\top \mathrm{W} \varphi) \to \top$.		

(3) 使用表 2.1中的规则转化$\{\mathrm{AG}(\mathbf{start} \to z), \mathrm{AG}(z \to (\mathrm{EG}\neg p \wedge \mathrm{AF}p))\}$，详细步骤如下：

1. $\mathbf{start} \to z$
2. $z \to \mathrm{EG}\neg p \wedge \mathrm{AF}p$
3. $z \to \mathrm{EG}\neg p$ $(2, \mathbf{Trans(3)})$
4. $z \to \mathrm{AF}p$ $(2, \mathbf{Trans(3)})$
5. $z \to \mathrm{E}_{\langle 1 \rangle}\mathrm{G}\neg p$ $(3, \mathbf{Trans(1)})$
6. $z \to x$ $(5, \mathbf{Trans(10)})$
7. $x \to \neg l$ $(5, \mathbf{Trans(10)})$
8. $x \to \mathrm{E}_{\langle 1 \rangle}\mathrm{G}x$ $(5, \mathbf{Trans(10)})$
9. $\top \to \neg z \vee x$ $(6, \mathbf{Trans(5)})$
10. $\top \to \neg x \vee \neg p$ $(7, \mathbf{Trans(5)})$

因此，得到的φ对应的$\mathrm{SNF}^{g}_{\mathrm{CTL}}$公式为：

1. $\mathbf{start} \to z$
4. $z \to \mathrm{AF}p$
8. $x \to \mathrm{E}_{\langle 1 \rangle}\mathrm{G}x$
9. $\top \to \neg z \vee x$
10. $\top \to \neg x \vee \neg p$.

2.2.3 CTL下的归结

*归结*是一种用于判定给定的命题公式（或一阶公式）是否可满足的规则，该技术可以追溯到1960年Davis等的工作[9]，之后被Robinson加以完善[10]。对于给定的公式，归结给出一个反驳定理证明过程。

在看见了归结在在命题逻辑和一阶逻辑中取得成就之后，科研工作者们开始将精力致力于其他非经典逻辑中，并取得了相当显著的理论成果，如：模态逻辑（K系统，Q系统，T系统，S4和S5系统）中的归结[11]和时态逻辑（尤其是线性时序逻辑（LTL）

表 2.3: 归结规则

(SRES1) $\dfrac{P \to \mathrm{AX}(C \vee l), Q \to \mathrm{AX}(D \vee \neg l)}{P \wedge Q \to \mathrm{AX}(C \vee D)}$;	**(SRES2)** $\dfrac{P \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(C \vee l), Q \to \mathrm{AX}(D \vee \neg l)}{P \wedge Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(C \vee D)}$;
(SRES3) $\dfrac{P \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(C \vee l), Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(D \vee \neg l)}{P \wedge Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(C \vee D)}$;	**(SRES4)** $\dfrac{\mathbf{start} \to C \vee l, \mathbf{start} \to D \vee \neg l}{\mathbf{start} \to C \vee D}$;
(SRES5) $\dfrac{\top \to C \vee l, \mathbf{start} \to D \vee \neg l}{\mathbf{start} \to C \vee D}$;	**(SRES6)** $\dfrac{\top \to C \vee l, Q \to \mathrm{AX}(D \vee \neg l)}{Q \to \mathrm{AX}(C \vee D)}$;
(SRES7) $\dfrac{\top \to C \vee l, Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(D \vee \neg l)}{Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}(C \vee D)}$;	**(SRES8)** $\dfrac{\top \to C \vee l, \top \to D \vee \neg l}{\top \to C \vee D}$;
(RW1) $\dfrac{\bigwedge_{i=1}^{n} m_i \to \mathrm{AX}\ \bot}{\top \to \bigvee_{i=1}^{n} \neg m}$;	**(RW2)** $\dfrac{\bigwedge_{i=1}^{n} m_i \to \mathrm{E}_{\langle ind \rangle}\mathrm{X}\ \bot}{\top \to \bigvee_{i=1}^{n} \neg m}$;
(ERES1) $\dfrac{\Lambda \to \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{G}l, Q \to \mathrm{AF}\neg l}{Q \to \mathrm{A}(\neg \Lambda \mathrm{W} \neg l)}$;	**(ERES2)** $\dfrac{\Lambda \to \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{G}l, Q \to \mathrm{E}_{\langle ind \rangle}\mathrm{F}\neg l}{Q \to \mathrm{E}_{\langle ind \rangle}(\neg \Lambda \mathrm{W} \neg l)}$.

和CTL）中的归结[12-13]。

这里主要介绍与本文直接相关的CTL下的归结。CTL下的归结起源于BolotovF的研究[13]，之后被Zhang等人完善[7]。不论是在BolotovF的工作还是在Zhang等人的工作中，其关键点都是将CTL公式转换为一个$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合。本文使用Zhang等人在[7]中的规则，如表所示。

在表 2.3中P和Q是文字的合取，C和D是文字的吸取，l是一个文字。此外，$\Lambda = \bigvee_{i=1}^{n} \bigwedge_{i=1}^{m_i} P_j^i$和$P_j^i$是文字的吸取，且$1 \le i \le n$和$1 \le j \le m$。值得注意的是，规则**(ERES1)**和**(ERES2)** 的结果都可以转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合（更多详情可以查看文章[7]）。

2.2.4 μ-演算

μ-演算是一种表达能力与S2S[2]相同的逻辑语言，LTL（线性时序逻辑，linear temporal logic）、CLT和CTL*能表达的属性都能用μ-演算来表示。μ-演算是模态逻辑的扩展，本文讨论Kozen提出的命题μ-演算[14]。构成μ-演算语言的符号有：

- 原子命题符号的集合：$\mathscr{A}$；
- 变元符号的可数集：$\mathscr{V}$；
- 常量符号：$\bot$和$\top$；
- 布尔联结符号：$\vee$，$\wedge$，和$\neg$;
- 路径量词符号：A和E;

[2]无限完全二叉树下的一元二阶理论（monadic second order theory of the infinite complete binary tree），简称为S2S。

- 时序操作符号：X 用于用于表示“下一个状态”；
- 不动点符号：μ和ν，分别表示“最小不动点”和“最大不动点”。

通常认为AX和EX的优先级比布尔连接符高[15]，为了保证文章的统一性，本文规定各类符号之间的如下优先级：

$$\neg \quad \mathrm{EX} \quad \mathrm{AX} \quad \wedge \quad \vee \quad \mu \quad \nu.$$

此时可如下定义μ-演算的公式：

$$\varphi := \top \mid \bot \mid p \mid \neg p \mid X \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathrm{EX}\varphi \mid \mathrm{AX}\varphi \mid \mu X.\varphi \mid \nu X.\varphi$$

其中$p \in \mathscr{A}$且$X \in \mathscr{V}$。称出现在$\mu X.\varphi$和$\nu X.\varphi$中的变元X是*受约束的*（bound），不受约束的变元称为*自由变元*。原子命题和变元符号及其各自的否定称为*文字*，出现在公式φ中的原子命题的集合记为$Var(\varphi)$。

由上述定义可以看出，“$\neg$”符号只能出现在原子命题符号的前面。但在μ-演算公式的一般定义中，“$\neg$”符号可以出现在变元符号的前面，但是要求变元符号前的“$\neg$”符号的个数为偶数。尽管如此，这两种方式定义的公式具有相同的表达能力。

对于给定的公式φ，若出现在其中的自由变元与受约束变元不同，且每个变元最多被约束一次，则称公式φ是*取名恰当的*（well-named）。此外，若公式$\delta X.\varphi(X)$（$\delta \in \{\mu,\nu\}$）中变元X的每次出现都是在EX或AX的辖域[3]内，则称变元在公式$\delta X.\varphi(X)$中是*受保护的*（guarded）。一个没有自由变元出现的公式称为μ*-句子*（sentence）。在本文中所谈到的公式指的是取名恰当的、受保护的μ-句子。

与CTL公式类似，μ-演算公式（简称为μ-公式或公式）的语义定义在Kripke结构上。但是，与CTL不同的是，这里不要求$\mathscr{M} = (S,R,L,r)$中的r为初始状态，且这里的r称为根（root）。

定义 2.5. *给定μ-演算公式φ、初始结构$\mathscr{M}$和一个赋值函数$v : \mathscr{V} \to 2^S$。公式在$\mathscr{M}$和v上的解释是S的一个子集$\|\varphi\|_v^{\mathscr{M}}$（当$\mathscr{M}$在上下文中是显然的，则可以省去上标）：*

$$\begin{aligned}
&\|p\|_v = \{s \mid p \in L(s)\}\ ,\ \|\top\|_v = S\ ,\ \|\bot\|_v = \emptyset,\\
&\|\neg p\|_v = S - \|p\|_v,\\
&\|X\|_v = v(X),\\
&\|\varphi_1 \vee \varphi_2\|_v = \|\varphi_1\|_v \cup \|\varphi_2\|_v,
\end{aligned}$$

[3]给定公式$*\varphi$（$* \in \{\neg, \mathrm{EX}, \mathrm{AX}, \mu X, \nu X\}$），则称$\varphi$为$*$在公式$*\varphi$中的**辖域**。对于公式$\varphi * \psi$（$* \in \{\vee,\wedge\}$），则分别称$\varphi$和$\psi$为他们之间的$*$在$\varphi * \psi$中的左辖域和右辖域。

$$
\begin{aligned}
&\|\varphi_1 \wedge \varphi_2\|_v = \|\varphi_1\|_v \cap \|\varphi_2\|_v,\\
&\|\mathrm{EX}\varphi\|_v = \{s \mid \exists s'.(s,s') \in R \wedge s' \in \|\varphi\|_v\},\\
&\|\mathrm{AX}\varphi\|_v = \{s \mid \forall s'.(s,s') \in R \Rightarrow s' \in \|\varphi\|_v\},\\
&\|\mu X.\varphi\|_v = \bigcap\{S' \subseteq S \mid \|\varphi\|_{v[X:=S']} \subseteq S'\},\\
&\|\nu X.\varphi\|_v = \bigcup\{S' \subseteq S \mid S' \subseteq \|\varphi\|_{v[X:=S']}\}.
\end{aligned}
$$

其中，$v[X := S']$是一个赋值函数，它除了$v[X := S'](X) = S'$之外，和v完全相同。也即是，对任意的$Y \in \mathscr{V}$：

$$
v[X := S'](Y) = \begin{cases} S', & \text{若} Y = X;\\ v(Y), & \text{否则。}\end{cases}
$$

在下文中，若$s \in \|\varphi\|_v$，则称s“满足”φ，记为$(\mathscr{M},s,v) \models \varphi$。此时，若$(\mathscr{M},r,v) \models \varphi$，则称$(\mathscr{M},r,v)$为$\varphi$的一个模型。当公式$\varphi$为$\mu$-句子时，可以将赋值函数$v$省略，记为$(\mathscr{M},s) \models \varphi$。记$Mod(\varphi)$为$\varphi$的模型的集合。其他记号与CTL情形类似，这里不再赘述。

2.2.5　μ-公式的析取范式

Janin等人首先提出了μ-演算的析取范式[16]，后来被逐步完善，本文使用文章[17]中的析取μ-公式的定义。

在给出该定义之前，事先给出μ-公式的另一种定义，称为覆盖-语法（cover-syntax）。该定义是将上述μ-公式的定义中的EX用覆盖操作（cover operator）的集合来替换得到。在覆盖-语法中，

- $Cover(\emptyset)$；
- 对任意的$n \geq 1$，若$\varphi_1,\ldots,\varphi_n$是公式，则$Cover(\varphi_1,\ldots,\varphi_n)$是公式。

对于给定的初始结构$\mathscr{M} = (S,R,L,r)$和赋值函数v：

- $(\mathscr{M},r,v) \models Cover(\emptyset)$当且仅当$r$没有任何的后继状态；
- $(\mathscr{M},s,v) \models Cover(\varphi_1,\ldots,\varphi_n)$当且仅当
  - 对任意的$i = 1,\ldots,n$，存在$(s,t) \in R$使得$(\mathscr{M},t,v) \models \varphi_i$；
  - 对任意的$(s,t) \in R$，存在$i \in \{1,\ldots,n\}$使得$(\mathscr{M},t,v) \models \varphi_i$。

尽管覆盖-语法在形式上与上一小节中μ-公式的定义大相径庭，但是已经证明这两种定义是等价的[17]。基于此，可以给出析取μ-公式的形式定义如下：

定义 2.6 (析取μ-公式[17]). 析取μ-公式的集合$\mathscr{F}_d$是包含$\top$、$\bot$和不矛盾的文字的合取且封闭于下面几条规则的最小集合:

(1) 吸取式（*disjunctions*）：若$\alpha, \beta \in \mathscr{F}_d$，则$\alpha \vee \beta \in \mathscr{F}_d$；

(2) 特殊合取式（*special conjunctions*）：若$\varphi_1, \ldots, \varphi_n \in \mathscr{F}_d$且$\delta$为不矛盾的文字的合取，则$\delta \wedge Cover(\varphi_1, \ldots, \varphi_n) \in \mathscr{F}_d$；

(3) 固定点操作（*fixpoint operators*）：若$\varphi \in \mathscr{F}_d$，且对任意的公式$\psi$，$\varphi$不含有形如$X \wedge \psi$的子公式，则$\mu X.\varphi$和$\nu X.\varphi$都在$\mathscr{F}_d$中。

2.3 模型检测

2.4 遗忘理论

2.5 本章小结

围绕本文的研究工作，本章首先介绍了隐私以及隐私泄露的定义，明确了本文中隐私保护的研究范畴，随后，介绍了差分隐私模型并给出标准形式的定义。其次，介绍了本文研究需要的Shannon信息论知识，包括基本通信模型、信息熵、条件熵、联合熵、互信息量等概念。在此基础上，对信息论中两个重要的不等式和率失真理论进行了简要的叙述。进一步，介绍了本文将使用的优化理论知识以及在对策博弈模型中的应用。最后，结合本章内容，给定了本文中所研究的差分隐私均衡优化的定义。针对差分隐私模型中隐私保护与数据可用性之间的矛盾问题，利用均衡优化思想研究差分隐私最优化机制是本文研究的核心。本章中所介绍内容为后续章节提供了基本模型与定义，是开展后续研究工作的理论出发点。

第三章　遗忘理论的定义及其语义属性

本章首先通过扩展互模拟的概念，给出*CTL*下遗忘理论的定义。其次，探索遗忘理论的一般通用属性，这些属性包括：模块化（*Modularity*）性质、交换性（*Commutativity*）、齐次性（*Commutativity*）等属性。

3.1　引言

从一个公式中“遗忘”掉一些原子命题得到的结果应该不违背定义在剩余原子命题集合上的公式，也就是说对于剩余原子命题集合上的公式，原始公式能够逻辑蕴涵它当且仅当遗忘得到的结果能过逻辑蕴涵它。从模型的角度来讲，遗忘得到的结果的模型与原始公式的模型在除去被遗忘的那些原子命题之后是能够想互模拟的。*互模拟*描述的是两个在行为上能够相互替代的转换系统[2]。在本文中，转换系统被描述成为Kripke结构。因此为了描述遗忘理论，这部分给出在给定原子命题集合上的Kripke结构（或Ind-结构）上的互模拟的定义及其性质。

基于互模拟的概念，给出了CTL下遗忘理论的定义。与后面章节将要讲述的约束CTL下的遗忘相对应，这部分探索没有约束的遗忘理论的一般属性。

3.2　V-互模拟

这部分给出定义在给定原子命题集合V上的互模拟的概念，本文称之为V-互模拟。尽管在文章[18]中给出了相似的概念，但是如在基础知识部分所述，*S5*的语义是定义在一种特殊的Kripke结构（K-解释）下的，因而不具有一般性。接下来探讨一种更加一般的V-互模拟。

为此，首先给出能够描述一定深度$n \in \mathbb{N}$的计算树之间的V-互模拟关系，记为$\mathscr{B}_n^V$。令$V \subseteq \mathscr{A}$是原子命题的集合，$i \in \{1,2\}$，$\mathscr{M}_i = (S_i, R_i, L_i, s_0^i)$（或$\mathscr{M}_i = (S_i, R_i, L_i, [_]_i, s_0^i)$）是初始结构（Ind-Kripke结构），$\mathscr{K}_i = (\mathscr{M}_i, s_i)$是K-结构（或Ind-结构）。$\mathscr{B}_n^V$被递归定义如下：

- 若$L_1(s_1) - V = L_2(s_2)$，则$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_0^V$；
- 对任意$n \geq 0$，若满足下面几个条件，则$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^V$成立：
  - $(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_0^V$；
  - 对任意$(s_1, s_1') \in R_1$，存在$(s_2, s_2') \in R_2$使得$(\mathscr{K}_1', \mathscr{K}_2') \in \mathscr{B}_n^V$；

– 对任意$(s_2,s_2')\in R_2$，存在$(s_1,s_1')\in R_1$使得$(\mathscr{K}_1',\mathscr{K}_2')\in\mathscr{B}_n^V$。

其中$\mathscr{K}_i'=(\mathscr{M}_i,s_i')$。

当所谈及的原子命题的集合V很显然的时候，上述$\mathscr{B}_n^V$中的V可以省略，记为$\mathscr{B}_n$。此外，当讨论的$\mathscr{M}_i(i=1,2)$是显然的时候，可以使用$(s_1,s_2)\in\mathscr{B}_n$代替$((\mathscr{M}_1,s_1),(\mathscr{M}_2,s_2))\in\mathscr{B}_n$。此时，$V$-互模拟关系就可以定义如下：

定义 3.1 (V-互模拟)**.** 令V是$\mathscr{A}$的一个子集，$i\in\{1,2\}$，$\mathscr{K}_1$和$\mathscr{K}_2$是K-结构（或*Ind*-结构）。

- $\mathscr{K}_1$和$\mathscr{K}_2$是V-互模拟的，当且仅当对所有的$n\geq 0$都有$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_n$。若$\mathscr{K}_1$和$\mathscr{K}_2$是$V$-互模拟的，则记为$\mathscr{K}_1\leftrightarrow_V\mathscr{K}_2$。
- 对$\mathscr{M}_i$上的路径$\pi_i=(s_{i,1},s_{i,2},\dots)$，若对于任意的$j\in\mathbb{N}_{\geq 1}$[1]都有$\mathscr{K}_{1,j}\leftrightarrow\mathscr{K}_{2,j}$，则$\pi_1\leftrightarrow_V\pi_2$。其中$\mathscr{K}_{i,j}=(\mathscr{M}_i,s_{i,j})$。

上述V-互模拟的定义是现有互模拟定义的一般化，这可以从下面几个方面来体现[2]。首先，当给定的V为空集且谈论指定的初始状态时，本文的V-互模拟与定义在Baier等文章里的互模拟等价（定义7.1[2]）的概念一致。其次，在同一文章里的基于状态的互模拟（定义7.7[2]）是定义在给定结构的状态上的，因此与本文的V-互模拟（定义在结构的集合上）也不同。最后，本文的$\mathscr{B}_n$的定义与Browne的论文中的状态等价E_n类似，只是后者是定义在状态上[3]而本文的定义在K-结构（或Ind-结构）上。

下面例子呈现结构之间的V-互模拟。

例 3.1. 令$\mathscr{K}_1$，$\mathscr{K}_2$和$\mathscr{K}_3$为三个K-结构，其图表示分别如图中的$\mathscr{K}_1$，$\mathscr{K}_2$和$\mathscr{K}_3$所示。它们之间的互模拟关系也如图中标记所示，即$\mathscr{K}_1\leftrightarrow_{\{sp\}}\mathscr{K}_2$，$\mathscr{K}_2\leftrightarrow_{\{se\}}\mathscr{K}_3$和$\mathscr{K}_1\leftrightarrow_{\{sp,se\}}\mathscr{K}_3$。此外，可以看出$\mathscr{K}_1$，$\mathscr{K}_2$和$\mathscr{K}_3$之间是互不互模拟[2]的，即不$\emptyset$-互模拟。

为了简化书写和看起来简洁，当从上下文中能明确知道所指的初始结构和Ind-Kripke结构（为了方便，将这两种结构通称为结构），则可以使用状态来表示这些结构之间的V-互模拟，即使用$s_1\leftrightarrow_V s_2$替代$(\mathscr{M}_1,s_1)\leftrightarrow(\mathscr{M}_2,s_2)$。

V-互模拟给出了两个结构之间相互模仿的行为关系，下面的命题给出了这种关系一些关键的性质。

命题 3.1. 令i是属于集合$\{1,2\}$的变量，V_1和V_2是$\mathscr{A}$的子集，s_1'和s_2'是两个状态，π_1'和π_2'是两条路径，$\mathscr{K}_j=(\mathscr{M}_j,s_j)(j=1,2,3)$是K-结构（或*Ind*-结构）。如果$(\mathscr{K}_1\leftrightarrow_{V_1}\mathscr{K}_2)$且$(\mathscr{K}_2\leftrightarrow_{V_2}\mathscr{K}_3)$，则：

[1] $\mathbb{N}_{\geq 1}$是大于等于1的整数的集合。

[2] 在其他领域也有类似的定义，如：定义在数据库相关文献中的概念k-互模拟[19]。k-互模拟概念中涉及与本文$\mathscr{B}_n$类似的定义，只是其关系是从相反的方向（即：从孩子到父节点的方向）来说明的。此外，值得一提的是，本文的V-互模拟的概念是定义在K-结构上的。

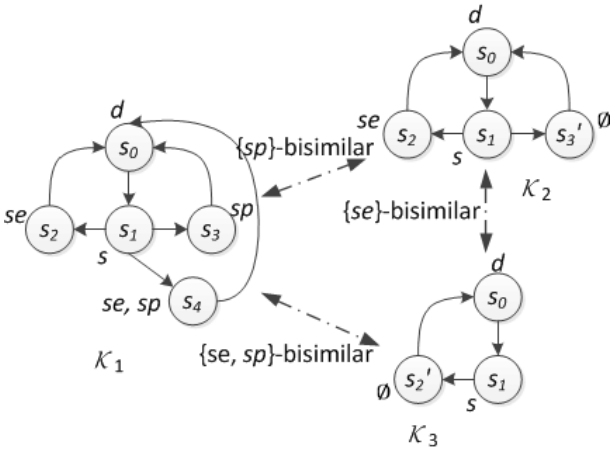

图 3.1: K-结构之间的V-互模拟关系

(i) 若$s_1' \leftrightarrow_{V_i} s_2'$，则$s_1' \leftrightarrow_{V_1 \cup V_2} s_2'$；

(ii) 若$\pi_1' \leftrightarrow_{V_i} \pi_2'$，则$\pi_1' \leftrightarrow_{V_1 \cup V_2} \pi_2'$；

(iii) 对$\mathscr{M}_1$上的任意一条路径π_{s_1}，存在$\mathscr{M}_2$上的一条路径π_{s_2}使得$\pi_{s_1} \leftrightarrow_{V_1} \pi_{s_2}$；反之亦然；

(iv) $\mathscr{K}_1 \leftrightarrow_{V_1 \cup V_2} \mathscr{K}_3$；

(v) 若$V_1 \subseteq V_2$，则$\mathscr{K}_1 \leftrightarrow_{V_2} \mathscr{K}_2$。

证明. 这里给出结构为K-结构的证明，结构为Ind-结构的情形可以类似地证明。

(i) 假设s_1'和s_2'分别来源于$\mathscr{M}_1$和$\mathscr{M}_2$，$\mathscr{K}_1 = (\mathscr{M}_1, s_1)$，$\mathscr{K}_2 = (\mathscr{M}_2, s_2)$。为了证明$s_1' \leftrightarrow_{V_1 \cup V_2} s_2'$，只需证明对于任意的$n \geq 0$，$(s_1', s_2') \in \mathscr{B}_n^{V_1 \cup V_2}$。

基始. 当$n = 0$时显然是成立的。

归纳步骤. 假设对于任意的$0 \leq k \leq n$，若$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_k^{V_1}$且$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_k^{V_2}$，则$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_k^{V_1 \cup V_2}$。这里根据定义 3.1证明对于若$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^{V_1}$且$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^{V_2}$，则$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^{V_1 \cup V_2}$。

（a）$L_1(s_1) - (V_1 \cup V_2) = L_2(s_2) - (V_1 \cup V_2)$是显然成立的。

（b）给定$i \in \{1,2\}$，$0 < k \leq n+1$，$\mathscr{K}_i^k = (\mathscr{M}_i, s_i^k)$。这里将证明对于任意的$(s_1, s_1^1) \in R_1$，存在一个$(s_2, s_2^1) \in R_2$使得$(s_1^1, s_2^1) \in \mathscr{B}_n^{V_1 \cup V_2}$。有归纳假设可知$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_n^{V_1 \cup V_2}$，因而有$(\mathscr{K}_1^1, \mathscr{K}_2^1) \in \mathscr{B}_{n-1}^{V_1 \cup V_2}$。因此，只需证明对于任意的$(s_1^n, s_1^{n+1}) \in R_1$，存在$(s_2^n, s_2^{n+1}) \in R_2$使得$(s_1^{n+1}, s_2^{n+1}) \in \mathscr{B}_0^{V_1 \cup V_2}$。因为$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^{V_1}$且$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_{n+1}^{V_2}$，所以有$L_1(s_1^{n+1}) - (V_1 \cup V_2) = L_1(s_2^{n+1}) - (V_1 \cup V_2)$。

（c）定义中的第三点可以类似（b）证明。

因此，当令s_1和s_2分别为s_1'和s_2'，就可得到$s_1' \leftrightarrow_{V_1\cup V_2} s_2'$。

(ii) 根据定义和(i)很容易证明。

(iii) 为了证明该结论成立，下面给出一个等价的V-互模拟的定义。令V是$\mathscr{A}$的一个子集，$\mathscr{K}_i = (\mathscr{M}_i, s_i)$ $(i = 1,2)$是κ(Ind)-结构，则$\mathscr{K}_1 \leftrightarrow_V \mathscr{K}_2$（也记为$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}$）当且仅当

(a) $L_1(s_1) - V = L_2(s_2) - V$；

(b) 对任意的$(s_1, s_1') \in R_1$，存在一个$(s_2, s_2') \in R_2$使得$\mathscr{K}_1' \leftrightarrow_V \mathscr{K}_2'$；

(c) 对任意的$(s_2, s_2') \in R_2$，存在一个$(s_1, s_1') \in R_1$使得$\mathscr{K}_1' \leftrightarrow_V \mathscr{K}_2'$。

其中$\mathscr{K}_i' = (\mathscr{M}_i, s_i')$。

下面从两个方面证明上述结论成立。

($\Rightarrow$) (a) 显然$L_1(s_1) - V = L_2(s_2) - V$成立。

(b) $\mathscr{K}_1 \leftrightarrow_V \mathscr{K}_2$当且仅当对于所有的$n \geq 0$都有$(\mathscr{K}_1, \mathscr{K}_2) \in \mathscr{B}_n$。因此，对任意的$(s_1, s_1') \in R_1$，存在一个$(s_2, s_2') \in R_2$使得对于任意的$n > 0$都有$(\mathscr{K}_1', \mathscr{K}_2') \in \mathscr{B}_n$且$L_1(s_1') - V = L_2(s_2') - V$。因此，$\mathscr{K}_1' \leftrightarrow_V \mathscr{K}_2'$。

(c) 这点的证明与(b)的证明类似。

($\Leftarrow$) 显然，$L_1(s_1) - V = L_2(s_2) - V$蕴涵$(s_1, s_2) \in \mathscr{B}_0$。(b)蕴涵对于任意的$(s_1, s_1') \in R_1$，存在一个$(s_2, s_2') \in R_2$使得对于任意的$n \geq 0$都有$(s_1', s_2') \in \mathscr{B}_n$。(c) 蕴涵对于任意的$(s_2, s_2') \in R_2$，存在一个$(s_1, s_1') \in R_1$使得对于任意的$n \geq 0$都有$(s_1', s_2') \in \mathscr{B}_n$。因此，对于任意的$n \geq 0$都有$(s_1, s_2) \in \mathscr{B}_n$。如此就可以知道$\mathscr{K}_1 \leftrightarrow_V \mathscr{K}_2$。

(iv) 令$\mathscr{M}_j = (S_j, R_j, L_j, s_j)$ $(j = 1,2,3)$，$\mathscr{B}$是有V_1-互模拟关系的结构的集合（即：$s_1 \leftrightarrow_{V_1} s_2$当且仅当$(s_1, s_2) \in \mathscr{B}$），$\mathscr{B}''$是有$V_2$-互模拟关系的结构的集合。

集合$\mathscr{B}'$是由$\mathscr{B}$和$\mathscr{B}''$共同约束下得到的，即$\mathscr{B}' = \{(w_1, w_3) \mid (w_1, w_2) \in \mathscr{B}$且$(w_2, w_3) \in \mathscr{B}''\}$。显然$(s_1, s_3) \in \mathscr{B}'$成立。为了证明命题中的结论成立，下面从(iii)中的(a)，(b)和(c)三个方面来证明$\mathscr{B}'$是有$(V_1 \cup V_2)$-互模拟关系的结构的集合。

对于所有的$(w_1, w_3) \in \mathscr{B}'$：

(a) 存在S_2中的一个状态w_2使得$(w_1, w_2) \in \mathscr{B}$且$(w_2, w_3) \in \mathscr{B}''$。此外，由$(w_1, w_2) \in \mathscr{B}$可知对于任何不在$V_1$中的原子命题$q$，有$q \in L_1(w_1)$当且仅当$q \in L_2(w_2)$；由$(w_2, w_3) \in \mathscr{B}''$可知对于任何不在$V_2$中的原子命题$q'$，有$q' \in L_2(w_2)$当且仅当$q' \in L_3(w_3)$。因此可以得知，对于任意不在$V_1 \cup V_2$中的原子命题$r$，有$r \in L_1(w_1)$当且仅当$r \in L_3(w_3)$，即：$L_1(s_1) - (V_1 \cup V_2) = L_3(s_3) - (V_1 \cup V_2)$。

(b) 若$(w_1,u_1)\in R_1$，根据$\mathscr{B}'$的定义可知存在$w_2\in S_2$使得$(w_1,w_2)\in\mathscr{B}$和$(w_2,w_3)\in\mathscr{B}''$，则存在$u_2\in S_2$使得$(w_2,u_2)\in R_2$和$(u_1,u_2)\in\mathscr{B}$成立。因此，存在一个$u_3\in S_3$使得$(w_3,u_3)\in R_3$和$(u_2,u_3)\in\mathscr{B}''$成立。因此，有$(u_1,u_3)\in\mathscr{B}'$成立。

(c) 与(b)的证明类似，可以证明对于任意$(w_3,u_3)\in R_3$，存在$(w_1,u_1)\in R_1$使得$(u_1,u_3)\in\mathscr{B}'$。

因此有$\mathscr{K}_1\leftrightarrow_{V_1\cup V_2}\mathscr{K}_3$成立。

(v) 为了证明此结论，这里假定x和k是大于等于0的整数，$\mathscr{K}_{i,x}=(\mathscr{M}_i,s_{i,x})$是结构。为了方便，用$(s_{i,k},s_{i,k+1})\in R_i$表示路径$(s_i=s_{i,0},s_{i,1},s_{i,2},\ldots,s_{i,k},s_{i,k+1},\ldots)$上的第$k+2$个节点。接下来将展示对任意的$n\geq 0$都有$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_n^{V_2}$。

基始. $L_1(s_1)-V_1=L_2(s_2)-V_1$　　（已知）
$\Rightarrow$ 对任意的$q\in(\mathscr{A}-V_1)$，有$q\in L_1(s_1)$当且仅当$q\in L_2(s_2)$
$\Rightarrow$ 对任意的$q\in(\mathscr{A}-V_2)$，有$q\in L_1(s_1)$当且仅当$q\in L_2(s_2)$　　（$V_1\subseteq V_2$）
$\Rightarrow L_1(s_1)-V_2=L_2(s_2)-V_2$，即：$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_0^{V_2}$。

归纳步骤. 假定对于任意的$0\leq n\leq k$ $(k>0)$，若$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_n^{V_1}$则$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_n^{V_2}$成立，接下来证明若$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_k^{V_1}$则$(\mathscr{K}_1,\mathscr{K}_2)\in\mathscr{B}_{k+1}^{V_2}$。

(a) 显然$L_1(s_1)-V_2=L_2(s_2)-V_2$成立。

(b) 对于任意的$(s_1,s_{1,1})\in R_1$，下面证明存在一个$(s_2,s_{2,1})\in R_2$使得$(\mathscr{K}_{1,1},\mathscr{K}_{2,1})\in\mathscr{B}_k^{V_2}$。由归纳假设可知$(\mathscr{K}_{1,1},\mathscr{K}_{2,1})\in\mathscr{B}_{k-1}^{V_2}$，因而只需要证明：① 对于所有的$(s_{1,k},s_{1,k+1})\in R_1$存在一个$(s_{2,k},s_{2,k+1})\in R_2$使得$(\mathscr{K}_{1,k+1},\mathscr{K}_{2,k+1})\in\mathscr{B}_0^{V_2}$由于$(\mathscr{K}_{1,1},\mathscr{K}_{2,1})\in\mathscr{B}_k^{V_1}$。因此，类似与基始里的证明方法，可得$L_1(s_{1,k+1})-V_2=L_2(s_{2,k+1})-V_2$成立，即：$(\mathscr{K}_{1,k+1},\mathscr{K}_{2,k+1})\in\mathscr{B}_0^{V_2}$。② 可以类似①证明对任意的$(s_{2,k},s_{2,k+1})\in R_1$存在一个$(s_{1,k},s_{1,k+1})\in R_2$使得$(\mathscr{K}_{1,k+1},\mathscr{K}_{2,k+1})\in\mathscr{B}_0^{V_2}$。

(c) 对于任意的$(s_2,s_{2,1})\in R_2$，类似(b)可以证明存在$(s_1,s_{1,1})\in R_1$使得$(\mathscr{K}_{1,1},\mathscr{K}_{2,1})\in\mathscr{B}_k^{V_2}$。　□

在命题 3.1中，性质(i)-(iii)是V-互模拟的标准属性，含义比较直观。性质(iv)表示如果一个结构分别与另外的两个结构具有V_1和V_2-互模拟关系，则这两个结构是$V_1\cup V_2$-互模拟的（如图 4.1所示）。如后文所示，这一性质对遗忘理论性质的探索至关重要。性质(v)表示若两个结构是V_1-互模拟的，则对于任意的V_2，若$V_1\subseteq V_2$则这两个结构是V_2-互模拟的。

从互模拟的定义上来看，如果两个结构是V-互模拟的，那么对于与V中的原子命题无关的公式φ来说，这两个结构同时满足或不满足φ。这一性质可以形式化地描述如下：

定理 3.1. 令$V \subseteq \mathscr{A}$是原子命题的集合，$\mathscr{K}_i\ (i=1,2)$是两个具有V-互模拟的K-结构，即：$\mathscr{K}_1 \leftrightarrow_V \mathscr{K}_2$，$\Phi$是一个*CTL*公式且$IR(\Phi,V)$。则有$\mathscr{K}_1 \models \Phi$当且仅当$\mathscr{K}_2 \models \Phi$。

证明. 这一结论可以从CTL公式的结构归纳地来证明。此外，不失一般性地可以假设$Var(\Phi)\cap V=\emptyset$，$\mathscr{K}_1=(\mathscr{M},s)$和$\mathscr{K}_1=(\mathscr{M}',s')$。

情形1：$\Phi = p$ （$p \in \mathscr{A}-V$）.

$(\mathscr{M},s)\models\Phi$当且仅当$p\in L(s)$ （可满足关系的定义）

$\Leftrightarrow p\in L'(s')$ （$s\leftrightarrow_v s'$）

$\Leftrightarrow (\mathscr{M}',s')\models\Phi$。

情形2：$\Phi=\neg\psi$.

$(\mathscr{M},s)\models\Phi$当且仅当$(\mathscr{M},s)\not\models\psi$

$\Leftrightarrow (\mathscr{M}',s')\not\models\psi$ （归纳假设）

$\Leftrightarrow (\mathscr{M}',s')\models\Phi$。

情形3：$\Phi=\psi_1\vee\psi_2$.

$(\mathscr{M},s)\models\Phi$

$\Leftrightarrow (\mathscr{M},s)\models\psi_1$或$(\mathscr{M},s)\models\psi_2$

$\Leftrightarrow (\mathscr{M}',s')\models\psi_1$或$(\mathscr{M}',s')\models\psi_2$ （归纳假设）

$\Leftrightarrow (\mathscr{M}',s')\models\Phi$。

情形4：$\Phi=\mathrm{EX}\psi$.

$(\mathscr{M},s)\models\Phi$

$\Leftrightarrow$ 存在一条路径$\pi=(s,s_1,\ldots)$使得$(\mathscr{M},s_1)\models\psi$

$\Leftrightarrow$ 存在一条路径$\pi'=(s',s'_1,\ldots)$使得$\pi\leftrightarrow_V\pi'$ ($s\leftrightarrow_V s'$，Proposition 3.1)

$\Leftrightarrow s_1\leftrightarrow_V s'_1$ ($\pi\leftrightarrow_V\pi'$)

$\Leftrightarrow (\mathscr{M}',s'_1)\models\psi$ （归纳假设）

$\Leftrightarrow (\mathscr{M}',s')\models\Phi$。

情形5：$\Phi=\mathrm{EG}\psi$.

$(\mathscr{M},s)\models\Phi$

$\Leftrightarrow$ 存在一条路径$\pi=(s=s_0,s_1,\ldots)$使得对于任意的$i\geq 0$都有$(\mathscr{M},s_i)\models\psi$

$\Leftrightarrow$ 存在一条路径$\pi'=(s'=s'_0,s'_1,\ldots)$使得$\pi\leftrightarrow_V\pi'$ ($s\leftrightarrow_V s'$，Proposition 3.1)

$\Leftrightarrow$ 对于任意的$i\geq 0$都有$s_i\leftrightarrow_V s'_i$ ($\pi\leftrightarrow_V\pi'$)

$\Leftrightarrow$ 对于任意的$i\geq 0$都有$(\mathscr{M},s'_i)\models\psi$ （归纳假设）

$\Leftrightarrow (\mathscr{M}',s')\models\Phi$。

情形6：$\Phi=\mathrm{E}(\psi_1\mathrm{U}\psi_2)$.

$(\mathscr{M},s)\models\Phi$

$\Leftrightarrow$ 存在一条路径$\pi=(s=s_0,s_1,\ldots)$和$i\geq 0$使得$(\mathscr{M},s_i)\models\psi_2$，且对所有的$0\leq j<i$都

有$(\mathscr{M},s_j)\models\psi_1$
$\Leftrightarrow$ 存在一条路径$\pi'=(s'=s'_0,s'_1,\ldots)$使得$\pi\leftrightarrow_V\pi'$　　($s\leftrightarrow_V s'$，Proposition 3.1)
$\Leftrightarrow(\mathscr{M}',s'_i)\models\psi_2$，且对于所有的$0\leq j<i$都有$(\mathscr{M}',s'_j)\models\psi_1$　　（归纳假设）
$\Leftrightarrow(\mathscr{M}',s')\models\Phi$。　　□

例 3.2. 令$\varphi_1=d\wedge\mathrm{EF}se\wedge\mathrm{AG}(se\rightarrow\mathrm{AX}d)$和$\varphi_2=d\wedge\mathrm{AX}se$是两个CTL公式，且$\mathrm{IR}(\varphi_1,\{sp\})$和$\mathrm{IR}(\varphi_2,\{sp\})$成立。因此可以验证图 4.1中的$\mathscr{K}_1$和$\mathscr{K}_2$都满足$\varphi_1$，但是都不满足$\varphi_2$。

3.3　遗忘理论及其语义属性

这部分将给出CTL下的遗忘理论的定义及其相关属性。

定义 3.2 (遗忘理论). 令V是$\mathscr{A}$的一个子集，Φ是一个公式。如果一个公式ψ满足下面条件，则称ψ为从Φ中遗忘掉V后得到结果，记为$\mathrm{F}_{\mathrm{CTL}}(\Phi,V)$：

- ψ与V中原子命题无关（即：$Var(\psi)\cap V=\emptyset$）；
- $Mod(\psi)=\{\mathscr{K}\mid\mathscr{K}$是一个初始K-结构$,\exists\mathscr{K}'\in Mod(\phi)\ \ s.t.\ \ \mathscr{K}'\leftrightarrow_V\mathscr{K}\}$

从定义 3.2可以看出，如果有两个公式ψ和ψ'都是从Φ中遗忘掉V中元素后得到的结果，则有$\psi\equiv\psi'$。从这个角度来看，可以说从Φ中遗忘掉V中元素后得到的结果之间是语义等价的。此外，当V中只包含一个元素的时候，可以省略掉集合符号，即：$\mathrm{F}_{\mathrm{CTL}}(\Phi,\{p\})\equiv\mathrm{F}_{\mathrm{CTL}}(\Phi,p)$。值得指出的是，遗忘理论的定义与均匀插值的语义定义等价，也即是遗忘理论与均匀插值是一对对偶概念，这与其他逻辑（包括模态逻辑S4、S5和经典命题逻辑）中的说法一致[?]。

从命题公式φ中遗忘掉原子命题p得到的结果记为：$Forget(\varphi,\{p\})\equiv\varphi[p/\bot]\vee\varphi[p/\top]$。值得注意的是，本文的遗忘理论的定义与Lin等人于1994提出命题逻辑下的遗忘理论一致。换句话说，本文将命题逻辑下的遗忘理论扩展到了CTL下。下面命题展示了上述结论：

定理 3.2. 给定一个命题公式φ和原子命题的集合$V\subseteq\mathscr{A}$，则下面逻辑等式成立。

$$\mathrm{F}_{\mathrm{CTL}}(\varphi,V)\equiv Forget(\varphi,V).$$

证明. 为了证明上述结论成立，只需要证明$Mod(\mathrm{F}_{\mathrm{CTL}}(\varphi,V))=Mod(Forget(\varphi,V))$。

一方面，对于$\mathrm{F}_{\mathrm{CTL}}(\varphi,V)$的任意一个模型$(\mathscr{M},s)$，由遗忘理论的定义可知存在一个$\varphi$的模型$(\mathscr{M}',s')$使得$(\mathscr{M},s)\leftrightarrow_V(\mathscr{M}',s')$。因而有$(s,s')\in\mathscr{B}_0$，这意味着$(\mathscr{M},s)\models Forget(\varphi,V)$。

另一方面，对于$Forget(\varphi,V)$的任意一个模型$(\mathscr{M},s)$（$\mathscr{M}=(S,R,L,s)$），存在一个φ的模型$(\mathscr{M}',s')$（$\mathscr{M}'=(S',R',L',s')$）使得$(s,s')\in\mathscr{B}_0$。此时可以构建一个初始K-结构$(\mathscr{M}_1,s_1)$使得$\mathscr{M}_1=(S_1,R_1,L_1,s_1)$，其中：

- $S_1=(S-\{s\})\cup\{s_1\}$；
- R_1由将R出现的s替换为s_1得到；
- 对于S_1中的任意的一个状态s^*：

$$L_1(s^*)=\begin{cases} L'(s'), & \text{如果}s^*=s_1;\\ L(s^*), & \text{否则。}\end{cases}$$

显然，$(\mathscr{M}_1,s_1)$是φ的一个模型且$s_1\leftrightarrow_V s$。因此，$(\mathscr{M},s)$是$\mathrm{F}_{\mathrm{CTL}}(\varphi,V)$的一个模型。□

遗忘理论的另一个重要的属性与V-无关性密切相关。直观地说，对于给定的公式$\psi=\varphi\wedge(q\leftrightarrow\alpha)$，如果$\mathrm{IR}(\varphi\wedge\alpha,\{q\})$，那么从$\psi$中遗忘掉$q$后得到的结果为$\varphi$。这一性质与后文中将要介绍的*SNC*（*WSC*）的计算密切相关。但是由于其也是遗忘理论的性质，因而本文将其放在此处来探讨。

引理 3.1. 给定两个公式φ和α，且$q\in\overline{Var(\varphi)\cup Var(\alpha)}$。则$\mathrm{F}_{\mathrm{CTL}}(\varphi\wedge(q\leftrightarrow\alpha),q)\equiv\varphi$。

证明. 令$\varphi'=\varphi\wedge(q\leftrightarrow\alpha)$。对于任意$\mathrm{F}_{\mathrm{CTL}}(\varphi',q)$的模型$(\mathscr{M},s)$，有遗忘理论的定义可知存在一个初始K-结构$(\mathscr{M}',s')$使得$(\mathscr{M},s)\leftrightarrow_{\{q\}}(\mathscr{M}',s')$且$(\mathscr{M}',s')\models\varphi'$。$(\mathscr{M}',s')\models\varphi$显然成立。此外，由于$\mathrm{IR}(\varphi,\{q\})$且$(\mathscr{M},s)\leftrightarrow_{\{q\}}(\mathscr{M}',s')$，由定理 3.1可知$(\mathscr{M},s)\models\varphi$。

为了证明另一个方向，令$\mathscr{M}=(S,R,L,s)$且$(\mathscr{M},s)\in Mod(\varphi)$。下面初始K-结构构造$(\mathscr{M}',s)$使得$\mathscr{M}'=(S,R,L',s)$，其中：

$L':S\to\mathscr{A}$ 和 $\forall s^*\in S$, 若 $(\mathscr{M},s^*)\not\models\alpha$, 则$L'(s^*)=L(s^*)-\{q\}$ 否则 $L'(s^*)=L(s^*)\cup\{q\}$,
若 $(\mathscr{M},s)\models\alpha$, 则$L'(s)=L(s)\cup\{q\}$, 否则 $L'(s)=L(s)-\{q\}$.

可以看出$(\mathscr{M}',s)\models\varphi$，$(\mathscr{M}',s)\models q\leftrightarrow\alpha$且$(\mathscr{M}',s)\leftrightarrow_{\{q\}}(\mathscr{M},s)$。因此，$(\mathscr{M}',s)\models\varphi\wedge(q\leftrightarrow\alpha)$。所以，由$(\mathscr{M}',s)\leftrightarrow_{\{q\}}(\mathscr{M},s)$可知$(\mathscr{M},s)\models\mathrm{F}_{\mathrm{CTL}}(\varphi\wedge(q\leftrightarrow\alpha),q)$。□

除了上述性质，遗忘理论还有其他一些一般属性。下面将详细介绍这些属性。

根据遗忘理论的定义可以看出，从一个公式里遗忘掉某个原子命题集合中的元素是将该集合看作一个整体来遗忘的。下面的结论说明，遗忘可以将原子命题中的元素拿出来一个一个的遗忘，而不是作为一个整体。

命题 3.2 (Modularity). 对于给定的公式φ，原子命题集合V，和原子命题p（$p \notin V$），下面的结论成立：

$$\mathrm{F}_{\mathrm{CTL}}(\varphi, \{p\} \cup V) \equiv \mathrm{F}_{\mathrm{CTL}}(\mathrm{F}_{\mathrm{CTL}}(\varphi, p), V).$$

证明. 要证明上述结论成立，只需证明等式左右两边的公式有相同的模型。

一方面，令$\mathscr{M}_1 = (S_1, R_1, L_1, s_1)$是一个初始结构，$(\mathscr{M}_1, s_1)$是$\mathrm{F}_{\mathrm{CTL}}(\varphi, \{p\} \cup V)$的一个模型。由遗忘理论的定义可知，存在$\varphi$的一个模型$(Hm, s)$（$\mathscr{M} = (S, R, L, s)$）使得$(\mathscr{M}_1, s_1) \leftrightarrow_{\{p\} \cup V} (\mathscr{M}, s)$。此时，可以如下构建一个初始K-结构$(\mathscr{M}_2, s_2)$使得$\mathscr{M}_2 = (S_2, R_2, L_2, s_2)$且：

(1) 对于s_2情形：令s_2是满足下面条件的状态：

- $p \in L_2(s_2)$当且仅当$p \in L_1(s_1)$，
- 对于任意的$q \in V$，$q \in L_2(s_2)$当且仅当$q \in L(s)$，
- 对于其他的原子命题q'，$q' \in L_2(s_2)$当且仅当$q' \in L_1(s_1)$当且仅当$q' \in L(s)$。

(2) 其他情形：

- 对于所有的满足$w \in S$，$w_1 \in S_1$且$w \leftrightarrow_{\{p\} \cup V} w_1$的状态对$(w, w_1)$，如下构造$w_2 \in S_2$：
  - $p \in L_2(w_2)$当且仅当$p \in L_1(w_1)$，
  - 对于任意的$q \in V$，$q \in L_2(w_2)$当且仅当$q \in L(w)$，
  - 对于其他的原子命题q'，$q' \in L_2(w_2)$当且仅当$q' \in L_1(w_1)$当且仅当$q' \in L(w)$。
- 对于$(w_1', w_1) \in R_1$，若w_2是基于w_1构造而成，且w_2'是基于w_1'构造而成，则令$(w_2', w_2) \in R_2$。

(3) 删除掉S_2和R_2中重复的元素。

□

不难看出，从公式中遗忘掉原子命题的集合中的元素，可以将该集合拆成两个集合后遗忘。

推论 3.1. 对于给定的公式φ，原子命题集合V_1和V_2，下面的结论成立：

$$\mathrm{F}_{\mathrm{CTL}}(\varphi, V_1 \cup V_2) \equiv \mathrm{F}_{\mathrm{CTL}}(\mathrm{F}_{\mathrm{CTL}}(\varphi, V_1), V_2).$$

如同被遗忘的原子命题的集合能被拆成两个集合的遗忘一样，下面将介绍有些情况下从带路径时序词的公式中遗忘掉一些原子命题可以将这些时许词提到遗忘操作的前面。

命题 3.3. 令$V \subseteq \mathscr{A}$为原子命题的集合，ϕ为*CTL*公式，则下面等式成立：

(i) $\mathrm{F}_{\mathrm{CTL}}(\mathrm{AX}\phi, V) \equiv \mathrm{AXF}_{\mathrm{CTL}}(\phi, V)$；

(ii) $\mathrm{F}_{\mathrm{CTL}}(\mathrm{EX}\phi, V) \equiv \mathrm{EXF}_{\mathrm{CTL}}(\phi, V)$；

(iii) $\mathrm{F}_{\mathrm{CTL}}(\mathrm{AF}\phi, V) \equiv \mathrm{AFF}_{\mathrm{CTL}}(\phi, V)$；

(iv) $\mathrm{F}_{\mathrm{CTL}}(\mathrm{EF}\phi, V) \equiv \mathrm{EFF}_{\mathrm{CTL}}(\phi, V)$。

证明. 为了证明上述结论成立，这里新引入一个叫做“子结构”的概念。对于给定的初始结构$\mathscr{M} = (S, R, L, s_0)$，称满足下面约束的初始K-结构$(\mathscr{M}', s_0')$为$(\mathscr{M}, s_0)$的一个子结构：

- $S' \subseteq S$且$S' = \{s' \mid s'$ 从s_0'是可达的$\}$，
- $R' = \{(s_1, s_2) \mid s_1, s_2 \in S'$ 和$(s_1, s_2) \in R\}$，
- $L' : S' \to 2^{\mathscr{A}}$且对于所有的$s_1 \in S'$有$L'(s_1) = L(s_1)$，且
- s_0'要么是s_0本身，要么是从s_0可达的某一个状态。

(i) 要证明$\mathrm{F}_{\mathrm{CTL}}(\mathrm{AX}\phi, V) \equiv \mathrm{AXF}_{\mathrm{CTL}}(\phi, V)$，只需证明：

$$Mod(\mathrm{F}_{\mathrm{CTL}}(\mathrm{AX}\phi, V)) = Mod(\mathrm{AXF}_{\mathrm{CTL}}(\phi, V)).$$

($\Rightarrow$) 对于任意$\mathrm{F}_{\mathrm{CTL}}(\mathrm{AX}\phi, V)$的模型$(\mathscr{M}', s')$，存在一个初始K-结构$(\mathscr{M}, s)$使得$(\mathscr{M}, s) \models \mathrm{AX}\phi$且$(\mathscr{M}, s) \leftrightarrow_V (\mathscr{M}', s')$
$\Rightarrow$ 对任意$(\mathscr{M}, s)$的子结构$(\mathscr{M}_1, s_1)$（其中$(s, s_1) \in R$），$(\mathscr{M}_1, s_1) \models \phi$
$\Rightarrow$ 存在一个初始K-结构$(\mathscr{M}_2, s_2)$使得$(\mathscr{M}_2, s_2) \models \mathrm{F}_{\mathrm{CTL}}(\phi, V)$且$(\mathscr{M}_2, s_2) \leftrightarrow_V (\mathscr{M}_1, s_1)$
$\Rightarrow$ 由这些$(\mathscr{M}_2, s_2)$容易构造出一个初始K-结构$(\mathscr{M}_3, s_3)$，使得s_2是s_3的直接后继状态，$(\mathscr{M}_2, s_2)$是$(\mathscr{M}_3, s_3)$的子结构且$(\mathscr{M}_3, s_3) \leftrightarrow_V (\mathscr{M}, s)$
$\Rightarrow (\mathscr{M}_3, s_3) \models \mathrm{AX}(\mathrm{F}_{\mathrm{CTL}}(\phi, V))$且$(\mathscr{M}_3, s_3) \leftrightarrow_V (\mathscr{M}', s')$
$\Rightarrow (\mathscr{M}', s') \models \mathrm{AX}(\mathrm{F}_{\mathrm{CTL}}(\phi, V))$（由定理 3.1）

($\Leftarrow$) 令$(\mathscr{M}_3, s_3)$是$\mathrm{AX}(\mathrm{F}_{\mathrm{CTL}}(\phi, V))$的模型，则对于任意$(\mathscr{M}_3, s_3)$的子结构$(\mathscr{M}_2, s_2)$（其中$(s_3, s_2) \in R_3$）有$(\mathscr{M}_2, s_2) \models \mathrm{F}_{\mathrm{CTL}}(\phi, V)$

$\Rightarrow$ 对任意上述的$(\mathscr{M}_2,s_2)$，存在一个初始K-结构$(\mathscr{M}_1,s_1)$使得$(\mathscr{M}_1,s_1)\models\phi$且$(\mathscr{M}_1,s_1)\leftrightarrow_V(\mathscr{M}_2,s_2)$
$\Rightarrow$ 由这些$(\mathscr{M}_1,s_1)$容易构造出一个初始K-结构$(\mathscr{M},s)$，使得s_1是s的直接后继状态，$(\mathscr{M}_1,s_1)$是$(\mathscr{M},s)$的子结构且$(\mathscr{M}_3,s_3)\leftrightarrow_V(\mathscr{M},s)$
$\Rightarrow(\mathscr{M},s)\models \mathrm{AX}\phi$且$(\mathscr{M}_3,s_3)\models \mathrm{F}_{\mathrm{CTL}}(\mathrm{AX}\phi,V)$。

(ii) 为了证明$\mathrm{F}_{\mathrm{CTL}}(\mathrm{EX}\phi,V)\equiv\mathrm{EXF}_{\mathrm{CTL}}(\phi,V)$，只需证明：

$$Mod(\mathrm{F}_{\mathrm{CTL}}(\mathrm{EX}\phi,V))=Mod(\mathrm{EXF}_{\mathrm{CTL}}(\phi,V)).$$

($\Rightarrow$) 对于任意$\mathrm{F}_{\mathrm{CTL}}(\mathrm{EX}\phi,V)$的模型$(\mathscr{M}',s')$，存在一个初始K-结构$(\mathscr{M},s)$使得$(\mathscr{M},s)\models\mathrm{AX}\phi$且$(\mathscr{M},s)\leftrightarrow_V(\mathscr{M}',s')$
$\Rightarrow$ 存在$(\mathscr{M},s)$的子结构$(\mathscr{M}_1,s_1)$（其中$(s,s_1)\in R$），$(\mathscr{M}_1,s_1)\models\phi$
$\Rightarrow$ 存在一个初始K-结构$(\mathscr{M}_2,s_2)$使得$(\mathscr{M}_2,s_2)\models\mathrm{F}_{\mathrm{CTL}}(\phi,V)$且$(\mathscr{M}_2,s_2)\leftrightarrow_V(\mathscr{M}_1,s_1)$
$\Rightarrow$ 由$(\mathscr{M}_2,s_2)$和$(\mathscr{M},s)$的其他子结构容易构$(\mathscr{M},s_x)$（$(s,s_x)\in S$）造出一个初始K-结构$(\mathscr{M}_3,s_3)$，使得s_2是s_3的直接后继状态，$(\mathscr{M}_2,s_2)$是$(\mathscr{M}_3,s_3)$的子结构且$(\mathscr{M}_3,s_3)\leftrightarrow_V(\mathscr{M},s)$
$\Rightarrow(\mathscr{M}_3,s_3)\models\mathrm{EX}(\mathrm{F}_{\mathrm{CTL}}(\phi,V))$且$(\mathscr{M}_3,s_3)\leftrightarrow_V(\mathscr{M}',s')$
$\Rightarrow(\mathscr{M}',s')\models\mathrm{EX}(\mathrm{F}_{\mathrm{CTL}}(\phi,V))$（由定理 3.1）

($\Leftarrow$) 令$(\mathscr{M}_3,s_3)$是$\mathrm{EX}(\mathrm{F}_{\mathrm{CTL}}(\phi,V))$的模型，则存在一个$(\mathscr{M}_3,s_3)$的子结构$(\mathscr{M}_2,s_2)$（其中$(s_3,s_2)\in R_3$）有$(\mathscr{M}_2,s_2)\models\mathrm{F}_{\mathrm{CTL}}(\phi,V)$
$\Rightarrow$ 对任意上述的$(\mathscr{M}_2,s_2)$，存在一个初始K-结构$(\mathscr{M}_1,s_1)$使得$(\mathscr{M}_1,s_1)\models\phi$且$(\mathscr{M}_1,s_1)\leftrightarrow_V(\mathscr{M}_2,s_2)$
$\Rightarrow$ 由$(\mathscr{M}_1,s_1)$和$(\mathscr{M}_3,s_3)$的其他子结构$(\mathscr{M}_3,s_x)$（$(s_3,s_x)\in S$）容易构造出一个初始K-结构$(\mathscr{M},s)$，使得s_1是s的直接后继状态，$(\mathscr{M}_1,s_1)$是$(\mathscr{M},s)$的子结构且$(\mathscr{M}_3,s_3)\leftrightarrow_V(\mathscr{M},s)$
$\Rightarrow(\mathscr{M},s)\models\mathrm{EX}\phi$且$(\mathscr{M}_3,s_3)\models\mathrm{F}_{\mathrm{CTL}}(\mathrm{EX}\phi,V)$。

同理可证(iii)和(iv)成立。　□

3.4　本章小结

本章基于现有不同环境下的互模拟，给出了扩展的Kripke结构下的V-互模拟的定义。结构间的V-互模拟描述的是两个结构除了V中的元素之外，它们的状态转换行为是能够互相模拟的。这与遗忘理论所描述的“遗忘掉不想考虑的原子命题应该不影响剩余原子命题上的结论”一致。因此，我们使用V-互模拟刻画了原始公式与遗忘结果的模型之间的关系，从而得到了遗忘理论的定义。遗忘理论作为本主要探讨的对象，本章通过研究V-互模拟的一些基本性质，探索了遗忘理论应有的一般属性，这些属性包括：模块化性质、交换性、同质性和命题罗也满足的属性。除了这些基本性质，本

章还说明了本文所给出的遗忘理论的定义是命题逻辑下遗忘理论定义的扩展。这些都为后文探索如何使用遗忘理论计算最强必要条件和最弱充分条件奠定了坚实的基础。

第四章　计算CTL下的遗忘：基于归结的方法

已有结果显示，任意的*CTL*公式可以转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合。归结是一种以子句为计算对象的判断可满足性的方法，本章提出一种基于归结的计算遗忘理论的方法。其主要思想是：首先将给定的*CTL*公式转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合，其次在相应的原子命题上使用归结规则得到归结结果，最后“消除”之前引入的索引和***start***，最终得到遗忘的结果。其主要流程图如图 *4.1*所示。正如本章所要说明的那样，*CTL*不具有均匀插值这一属性，基于归结的方法在有的情况下是不能计算出遗忘结果的。然而，在有些*CTL*子类下，本章提出的方法能够计算出其遗忘结果。

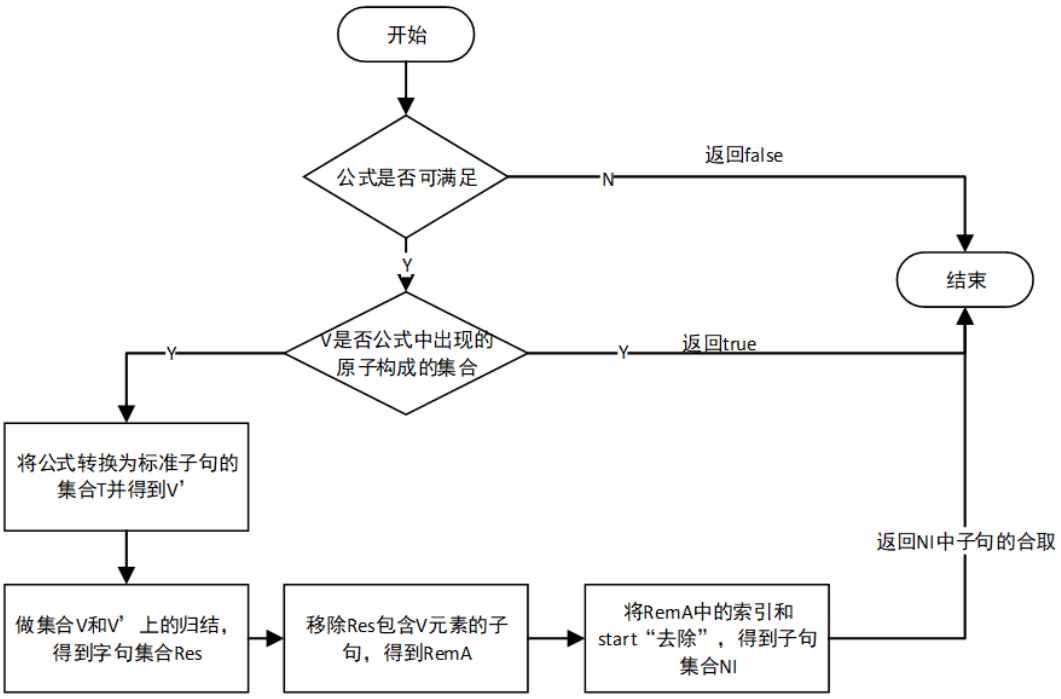

图 4.1: 基于归结的遗忘的主要流程图

4.1　引言

本章展示如何使用表 2.3中的归结规则来计算CTL下的遗忘理论。在本章给定如下约定的记号。令$V \subseteq \mathscr{A}$是要遗忘的原子命题的集合，$I \subseteq \mathrm{Ind}$是索引的集合，V'表示计算过程所引入的原子命题的集合且满足$V' \cap V = \emptyset$。此外，φ是CTL公式，且T_{φ}是在φ上使用表 2.1中的转换规则得到的$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合。显然可以知道，$V' =$

$Var(T_\varphi) - Var(\varphi)$。在不另加说明的情况下$\mathscr{M}$表示五元组$(S,R,L,[_],s_0)$。此时，本章所设计的算法的伪代码如算法 4.1所示。

算法 4.1 $ERes(\varphi,V)$

输入:

φ :CTL公式

V :需要遗忘的原子命题的集合

输出:

$ERes(\varphi,V)$:公式的合取

1: **if** φ 是不可满足的 **then**
2: **return** $\bot$;
3: **end if**
4: **if** $V = Var(\varphi)$ **then**
5: **return** $\bot$;
6: **end if**
7: $T_\varphi, V', I \leftarrow Transform(\varphi)$;
8: $Res \leftarrow Resolution(T_\varphi, V \cup V')$;
9: $RemA \leftarrow Removing\_atoms(Res, V)$;
10: NI $\leftarrow Removing\_index(RemA)$;
11: **return** $\bigwedge_{\psi \in \mathrm{NI}_{\mathrm{CTL}}} \psi$;

算法 4.1对于输入φ和V，输出结果记为$ERes(\varphi,V)$。为了实现这一目标，需要解决如下两个主要问题：

(1) 如何表示CTL公式和带索引的CTL公式之间的关系？如在第三章中所展示的那样，将一个CTL公式转换为$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合会引入新的原子命题和索引。虽然已有的研究说明了CTL公式可以转换为带索引的公式的集合并保证其可满足性，然而并没有表明这两种形式的公式之间的模型具有怎样的联系。本章给出一种扩展的互模拟定义，以描述两种公式的模型之间的关系。

(2) 如何“移除”无关的原子命题（包括需要遗忘的原子命题和转换过程中引入的新的原子命题），以及如何“消除”索引？为此，本章给出“移除”原子命题的一般操作，对应算法 4.1中的$Removing_atoms(Res,V)$过程，并提出一种一般化的Ackermann引理。为了“消除”索引，探索几个几个逻辑等价关系，对应算法 4.1中的$Removing_index(RemA)$过程。

本章其余部分组织如下：首先，第4.2节给出二元互模拟的定义及其相关性质。其次，第节从分节详细地介绍算法 4.1如何使用基于归结的方法计算遗忘。第三，第4.4节分析算法 4.1的可终止性及其时间和空间复杂性。最后总结本章的主要工作。

4.2　二元互模拟

对于给定的初始Ind-结构，这里定义一种$\langle V,I\rangle$-互模拟关系。为了与一元的（只考虑原子命题的集合）V-互模拟对应，称$\langle V,I\rangle$-互模拟为二元互模拟。其在V-互模拟的基础上又考虑了索引的集合在结构间关系。

定义 4.1 (二元互模拟). 令$V \subseteq \mathscr{A}$、$I \subseteq Ind$分别是原子命题和索引的集合，$\mathscr{K}_i = (\mathscr{M}_i, s^i)$是初始*Ind*-结构，其中$\mathscr{M}_i = (S_i, R_i, L_i, [_], s_0^i)$ $(i = 1,2)$。称$\mathscr{K}_1$和$\mathscr{K}_2$是$\langle V,I\rangle$-互模拟的（记为$\mathscr{K}_1 \leftrightarrow_{\langle V,I\rangle} \mathscr{K}_2$），当且仅当$\mathscr{K}_1 \leftrightarrow_V \mathscr{K}_2$且$\forall j \in (Ind - I)$有：

- 对任意的$(s,s_1) \in [j]_1$，存在$(s',s_1') \in [j]_2$使得$s \leftrightarrow_V s'$且$s_1 \leftrightarrow_V s_1'$；
- 对任意的$(s',s_1') \in [j]_2$，存在$(s,s_1) \in [j]_1$使得$s \leftrightarrow_V s'$且$s_1 \leftrightarrow_V s_1'$。

由定义 4.1可知，当探讨的公式为CTL公式时，因为不用考虑索引，$\leftrightarrow_{\langle V,I\rangle}$“降维”为$\leftrightarrow_V$。与$\leftrightarrow_V$类似，$\leftrightarrow_{\langle V,I\rangle}$在本文中至关重要的两个性质如下。

命题 4.1. 令$V_1, V_2 \subseteq \mathscr{A}$为原子命题的集合，$I_1, I_2 \subseteq Ind$为索引的集合，$\mathscr{K}_i = (\mathscr{M}_i, s_0^i)$ $(i = 1,2,3)$为初始*Ind*-结构。若$\mathscr{K}_1 \leftrightarrow_{\langle V_1,I_1\rangle} \mathscr{K}_2$、$\mathscr{K}_2 \leftrightarrow_{\langle V_2,I_2\rangle} \mathscr{K}_3$，则：

(i) $\mathscr{K}_1 \leftrightarrow_{\langle V_1 \cup V_2, I_1 \cup I_2\rangle} \mathscr{K}_3$；

(ii) 如果$V_1 \subseteq V_2$且$I_1 \subseteq I_2$，则$\mathscr{K}_1 \leftrightarrow_{\langle V_2,I_2\rangle} \mathscr{K}_2$。

证明. (i) 由定义 4.1可知$\mathscr{K}_1 \leftrightarrow_{V_1} \mathscr{K}_2$、$\mathscr{K}_2 \leftrightarrow_{V_2} \mathscr{K}_3$，因此由命题 3.1可知$\mathscr{K}_1 \leftrightarrow_{V_1 \cup V_2} \mathscr{K}_3$。

$\mathscr{K}_1 \leftrightarrow_{\langle V_1,I_1\rangle} \mathscr{K}_2$

$\Rightarrow \forall j \in (\mathrm{Ind} - (I_1 \cup I_2))$有：$\forall (s,s_1) \in [j]_1$，$\exists (s',s_1') \in [j]_2$使得$s \leftrightarrow_{V_1} s'$，$s_1 \leftrightarrow_{V_1} s_1'$

$\Rightarrow$ 又因为$\mathscr{K}_2 \leftrightarrow_{\langle V_2,I_2\rangle} \mathscr{K}_3$，所以$\exists (s'',s_1'') \in [j]_3$使得$s' \leftrightarrow_{V_2} s''$，$s_1' \leftrightarrow_{V_2} s_1''$

$\Rightarrow s \leftrightarrow_{V_1 \cup V_2} s''$且$s_1 \leftrightarrow_{V_1 \cup V_2} s_1''$

同理可证，$\forall (s'',s_1'') \in [j]_3$，$\exists (s,s_1) \in [j]_1$使得$s \leftrightarrow_{V_1 \cup V_2} s''$且$s_1 \leftrightarrow_{V_1 \cup V_2} s_1''$。因此，由定义 4.1可知$\mathscr{K}_1 \leftrightarrow_{\langle V_1 \cup V_2, I_1 \cup I_2\rangle} \mathscr{K}_3$。

(ii)可以由命题 3.1中的(ii)可得。 □

对于给定的Ind-Kripke结构$\mathscr{M} = (S,R,L,[_],s_0)$和$\mathscr{M}' = (S',R',L',[_],s_0')$，$\mathscr{M}$和$\mathscr{M}'$之间的二元互模拟关系$\leftrightarrow_{\langle V,I\rangle}$给描述公式间在二元组$\langle V,I\rangle$上的等价关系提供了前提条件。这同时也为解决本章引言部分提出的问题(1)奠定了基础。

定义 4.2. 给定两个公式（或公式的集合）T_1和T_2，$I \subseteq Ind$是索引的集合，$V'' \subseteq \mathscr{A}$是原子命题的集合。如果下面条件被满足，则称$T_1$和$T_2$在二元组$\langle V,I\rangle$上逻辑等价（记为$T_1 \equiv_{\langle V,I\rangle} T_2$）：

- $\forall (\mathscr{M},s_0) \in Mod(T_1)$，$\exists (\mathscr{M}',s_0') \in Mod(T_2)$使得$(\mathscr{M},s_0) \leftrightarrow_{\langle V,I\rangle} (\mathscr{M}',s_0')$，且
- $\forall (\mathscr{M}',s_0') \in Mod(T_2)$，$\exists (\mathscr{M},s_0) \in Mod(T_1)$使得$(\mathscr{M},s_0) \leftrightarrow_{\langle V,I\rangle} (\mathscr{M}',s_0')$。

4.3 基于归结的方法计算遗忘

在本节中，将围绕之前提出的两个问题和算法 4.1中的几个关键步骤（第7到第11行）来证明$ERes(\varphi,V) \equiv_{\langle V',\emptyset\rangle} \mathrm{F}_{\mathrm{CTL}}(\varphi,V)$。在这个等价关系中$\varphi$为CTL公式，$V$为需要遗忘的原子命题的集合，$V'$是将$\varphi$转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句集合过程中引入的新的原子命题的集合。这个结论表明，如果$ERes(\varphi,V)$公式中不包含V'中的元素，或者$\mathrm{IR}(ERes(\varphi,V),V')$，则$ERes(\varphi,V)$就是从$\varphi$中遗忘掉$V$中的原子命题之后得到的结果。

4.3.1 将CTL公式转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合

将CTL公式φ转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合这一过程（记为$Trangsform(\varphi)$）对应算法 4.1中的第7行所代表的过程。对于输入φ，该过程事先将φ转换为其否定范式（记为$\mathbf{nnf}(\varphi)$），然后通过下面的等价关系[7,20]将出现在公式中的$\top$和$\bot$“去掉”（记为$\mathbf{simp}(\mathbf{nnf}(\varphi))$）。

$$
\begin{array}{llll}
(\varphi \wedge \top) \equiv \varphi & (\varphi \wedge \bot) \equiv \bot & (\varphi \vee \top) \equiv \top & (\varphi \vee \bot) \equiv \varphi \\
\neg\top \equiv \bot & \neg\bot \equiv \top & QT\bot \equiv \bot & QT\top \equiv \top \\
Q(\varphi \mathrm{U} \bot) \equiv \bot & Q(\varphi \mathrm{U} \top) \equiv \top & Q(\bot \mathrm{U} \varphi) \equiv \varphi & Q(\top \mathrm{U} \varphi) \equiv Q\mathrm{F}\varphi \\
Q(\varphi \mathrm{W} \bot) \equiv Q\mathrm{G}\varphi & Q(\varphi \mathrm{W} \top) \equiv \top & Q(\bot \mathrm{W} \varphi) \equiv \varphi & Q(\top \mathrm{W} \varphi) \equiv \top
\end{array}
$$

在上述等价关系中，$Q \in \{\mathrm{A},\mathrm{E}\}$是路径量词，$T \in \{\mathrm{F},\mathrm{G},\mathrm{X}\}$是时序操作符。

在得到$\mathbf{simp}(\mathbf{nnf}(\varphi))$后，将$T_\varphi$初始化为$\{\mathrm{AG}(\mathbf{start} \rightarrow p), \mathrm{AG}(p \rightarrow \mathbf{simp}(\mathbf{nnf}(\varphi)))\}$，然后转换过程从表 2.1中找到匹配的规则来将$T_\varphi$中的非$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句形式的公式转换为$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句，并将得到的结果更新$T_\varphi$直到$T_\varphi$中不存在非$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句形式的公式。这个转换过程被写为算法 4.2。

在算法 4.2中，$Trans(\psi)$表示使用表 2.1中的某一条规则来转换ψ（规则中长横线上面的部分），并返回规则的结果（规则中长横线下面的部分）、引入的新原子命题和索引。这里使用规则**Trans(6)**为例来描述这一过程。令$\psi = q \rightarrow \mathrm{AX}\phi$，可以看出当$\phi$不是经典子句的时候$\psi$不是$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句，且规则**Trans(6)**是能使用的（匹配的）规则，则$Trans(\psi)$对ψ使用规则**Trans(6)**并返回结果$\{q \rightarrow \mathrm{AX}q', q' \rightarrow \phi\}$（在这里，引入了新的原子命题$q'$，但是没有引入新的索引）。

命题 4.2. 令φ是一个*CTL*公式，$(T_\varphi, V', I) = Transform(\varphi)$，则$\varphi \equiv_{\langle V',I\rangle} T_\varphi$。

证明. 为了讨论方便，令$Transform(\varphi)$过程产生了一个公式集合的序列，$T_0, T_1, \ldots, T_n = T_\varphi$，其中$p$是不出现在$\varphi$中的原子命题，$T_0 = \{\mathrm{AG}(\mathbf{start} \rightarrow p), \mathrm{AG}(p \rightarrow \mathbf{simp}(\mathbf{nnf}(\varphi)))\}$且

算法 4.2 *Transform*(φ)

输入：

φ　　:CTL公式

输出：

T_φ　　: $\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合

V'　　: 新引入的原子命题的集合

I　　: 引入的索引的集合

1: $T_\varphi \leftarrow \{\mathrm{AG}(\mathbf{start} \rightarrow p), \mathrm{AG}(p \rightarrow \mathbf{simp}(\mathbf{nnf}(\varphi)))\}$;（其中$p \in \mathscr{A} - var(\varphi)$）
2: $V' \leftarrow \{p\}$;
3: $I \leftarrow \emptyset$;
4: **while** $\exists \psi \in T_\varphi$使得$\psi$不是$\mathrm{SNF}^g_{\mathrm{CTL}}$子句 **do**
5:　$T_\varphi \leftarrow T_\varphi - \{\psi\}$;
6:　$T_\varphi \leftarrow Trans(\psi) \cup T_\varphi$;
7:　**if** $Trans(\psi)$引入了一个新原子命题q **then**
8:　　$V' \leftarrow V' \cup \{q\}$;
9:　**end if**
10:　**if** $Trans(\psi)$引入了一个新的索引ind **then**
11:　　$I \leftarrow I \cup \{ind\}$;
12:　**end if**
13: **end while**
14: **return** T_φ, V', I;

对任意的i（$0 \leq i < n$）有$T_{i+1} = (T_i - \{\psi\}) \cup R_i$（$Trans(\psi)$返回的结果为$R_i$）。此外，在这一过程中，所有的公式都是其否定范式的形式。

为了证明命题中的结论成立，只需证明，对任意的i（$0 \leq i < n$）有$T_i \equiv_{\langle V', I\rangle} T_{i+1}$成立。由于$T_{i+1}$是由$T_i$通过表 2.1中的规则作用于$T_i$中的某一个公式得到，因此证明过程分为两个部分：（1）从φ到T_0部分；（2）对表 2.1中的规则做归纳的部分。为了方便，下面假设$\mathscr{M}_1 = (S_1, R_1, L_1, [_], s_1)$和$\mathscr{M}_2 = (S_2, R_2, L_2, [_]_2, s_2)$。

（1）这里将证明$\varphi \equiv_{\langle\{p\},\emptyset\rangle} T_0$。

($\Rightarrow$) $\forall(\mathscr{M}_1, s_1) \in Mod(\varphi)$，可以构造一个Ind-Kripke结构$\mathscr{M}_2 = (S_2, R_2, L_2, [_], s_2)$使得$\mathscr{M}_2$除了$L_2(s_2) = L_1(s_1) \cup \{p\}$（默认不出现在$\varphi$中的原子命题都不出现在状态的标签中），其他的元素都与$\mathscr{M}_1$中元素相同。显然，$(\mathscr{M}_2, s_2) \models T_0$且$(\mathscr{M}_1, s_1) \leftrightarrow_{\langle\{p\},\emptyset\rangle} (\mathscr{M}_2, s_2)$。

($\Leftarrow$) $\forall(\mathscr{M}_1, s_1) \in Mod(T_0)$，由**start**的语义可以知道$(\mathscr{M}_1, s_1) \models \varphi$。

（2）这里将证明对任意的i（$0 \leq i < n$）有$T_i \equiv_{\langle V', I\rangle} T_{i+1}$成立，其中$T_{i+1} = (T_i - \{\psi\}) \cup R_i$。为了方便，用$\psi \rightarrow_t R_i$表示$R_i$是使用规则$t$在公式$\psi$上得到的结果，且$T_i = X \cup \{\psi\}$（显然，$T_{i+1} = X \cup R_i$）。下面证明规则$t \in \{$**Trans(1), Trans(4), Trans(6)**$\}$的情形，其他情形可以类似地证明。

（a）$t =$ **Trans(1)**。

$(\Rightarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_i)$，即$(\mathscr{M}_1,s_1)\models X\wedge \mathrm{AG}(q\rightarrow \mathrm{EX}\varphi)$
$\Rightarrow (\mathscr{M}_1,s_1)\models X$，且对任意路径$\pi$上的状态$s_{1,j}$ $(j\geq 1)$有：$(\mathscr{M},s_{1,j})\not\models \neg q$或存在一个状态$s_{1,j+1}$使得$(s_{1,j},s_{1,j+1})\in R_1$且$(\mathscr{M},s_{1,j+1})\models \varphi$。

由此可以构造一个Ind-Kripke结构$\mathscr{M}_2$使得$\mathscr{M}_2$与$\mathscr{M}_1$相同，除了对使用规则**Trans(1)**在公式$\mathrm{AG}(q\rightarrow \mathrm{EX}\varphi)$上面引入的新索引$ind$有$[ind]_2=\bigcup_{s\in S}R_s\cup R_y$。其中：

- $R_{s_{1,j}}=\{(s_{1,j},s_{1,j+1}),(s_{1,j+1},s_{1,j+2}),\dots\}$ $(j\geq 1)$，其满足“若$(\mathscr{M}_1,s_{1,j})\models q$，则$(\mathscr{M}_1,s_{1,j+1})\models\varphi$”且“对于任意的$i\geq j$，若$(s_{1,i},s')\in R_s$ $(s\neq s_{1,j})$，则$s'=s_{1,i+1}$”；
- $R_y=\{(s_x,s_y)\mid s_x\in S$，若$\forall(s'_1,s'_2)\in\bigcup_{s\in S}R_s$，$s'_1\neq s_x$，则找一个状态$s_y\in S_2$使得$(s_x,s_y)\in R_2\}$。

显然，$(\mathscr{M}_1,s_1)\leftrightarrow_{\langle\emptyset,\{ind\}\rangle}(\mathscr{M}_2,s_2)$
$\Rightarrow$对任意从s_2开始的路径$\pi=(s_2=s_{2,1},s_{2,2},\dots)$，如果$s_{2,j}\in\pi$，则$(\mathscr{M}_2,s_{2,j})\models\neg q$或者$(\mathscr{M}_2,s_{2,j})\models \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi$
$\Rightarrow (\mathscr{M}_2,s_2)\models \mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$
$\Rightarrow (\mathscr{M}_2,s_1)\models X\wedge\mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$

$(\Leftarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_{i+1})$，即$(\mathscr{M}_1,s_1)\models X\wedge\mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$
$\Rightarrow (\mathscr{M}_1,s_1)\models X$且$(\mathscr{M}_1,s_1)\models \mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$
$\Rightarrow$对任意的以s_1为始点的路径上的任意状态$s_{1,j}$，$(\mathscr{M}_1,s_{1,j})\models\neg q$或$(\mathscr{M}_1,s_{1,j})\models\mathrm{EX}\varphi$
$\Rightarrow (\mathscr{M}_1,s_1)\models\mathrm{AG}(q\rightarrow\mathrm{EX}\varphi)$
$\Rightarrow (\mathscr{M}_1,s_1)\models X\wedge\mathrm{AG}(q\rightarrow\mathrm{EX}\varphi)$。

（b）$t=$**Trans(4)**。

$(\Rightarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_i)$，即$(\mathscr{M}_1,s_1)\models X\wedge\mathrm{AG}(q\rightarrow\varphi_1\vee\varphi_2)$
$\Rightarrow (\mathscr{M}_1,s_1)\models X$且$\forall s'_1\in S_1$，$(\mathscr{M}_1,s'_1)\models q\rightarrow\varphi_1\vee\varphi_2$
$\Rightarrow (\mathscr{M}_1,s'_1)\models\neg q$或$(\mathscr{M}_1,s'_1)\models\varphi_1\vee\varphi_2$。

可以如下构造Ind-Kripke结构$\mathscr{M}_2$：

- $S_2=S_1$，$R_2=R_1$，$[_]_2$与$[_]_1$一样且$s_2=s_1$；
- L_2与L_1类似，除了：若$(\mathscr{M}_1,s'_1)\models\neg q$则$L_2(s'_1)=L_1(s'_1)$，否则“若$(\mathscr{M}_1,s'_1)\models\varphi_1$则$L_2(s'_1)=L_1(s'_1)$，否则$L_2(s'_1)=L_1(s'_1)\cup\{p\}$”。

显然，$(\mathscr{M}_2,s'_1)\models(q\rightarrow\varphi_1\vee p)\wedge(p\rightarrow\varphi_2)$且$(\mathscr{M}_1,s_1)\leftrightarrow_{\langle\{p\},\emptyset\rangle}(\mathscr{M}_2,s_2)$，因而$(\mathscr{M}_2,s_1)\models T_{i+1}$。

$(\Leftarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_{i+1})$，即$(\mathscr{M}_1,s_1)\models X\wedge\mathrm{AG}(q\rightarrow\varphi_1\vee p)\wedge\mathrm{AG}(p\rightarrow\varphi_2)$。显然，$(\mathscr{M}_1,s_1)\models T_i$。

（c）t=**Trans(6)**。

这里证明$\mathrm{E}_{\langle ind\rangle}\mathrm{X}$的情形，AX情形可以类似地证明。

$(\Rightarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_i)$，即$(\mathscr{M}_1,s_1)\models X\wedge \mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi)$
$\Rightarrow (\mathscr{M}_1,s_1)\models X$且对任意的$s_1'\in S,(\mathscr{M}_1,s_1')\models q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi$
$\Rightarrow (\mathscr{M}_1,s_1')\models \neg q$或者存在一个状态$s'$使得$(s_1',s')\in[ind]$且$(\mathscr{M}_1,s')\models\varphi$

可以如下构造Ind-Kripke结构$\mathscr{M}_2$：

- $S_2=S_1$，$R_2=R_1$，$[_]_2$与$[_]_1$一样且$s_2=s_1$；
- L_2与L_1类似，除了：若$(\mathscr{M}_1,s_1')\models\neg q$则$L_2(s_1')=L_1(s_1')$，否则“若$(\mathscr{M}_1,s_1')\models q$则$L_2(s')=L_1(s')\cup\{p\}\ ((s_1',s')\in R_2)$”。

显然，$(\mathscr{M}_2,s_2)\models \mathrm{AG}(q\rightarrow \mathrm{E}_{\langle ind\rangle}\mathrm{X}p)\wedge\mathrm{AG}(p\rightarrow\varphi),(\mathscr{M}_2,s_2)\models T_{i+1}$且$(\mathscr{M}_1,s_1)\leftrightarrow_{\langle\{p\},\emptyset\rangle}(\mathscr{M}_2,s_2)$ $(s_2=s_1)$。

$(\Leftarrow)\ \forall(\mathscr{M}_1,s_1)\in Mod(T_{i+1})$，即$(\mathscr{M}_1,s_1)\models X\wedge\mathrm{AG}(q\rightarrow\mathrm{E}_{\langle ind\rangle}\mathrm{X}p)\wedge\mathrm{AG}(p\rightarrow\varphi)$。显然，$(\mathscr{M}_1,s_1)\models T_i$。 □

命题 4.2表示，对于给定的CTL公式φ，通过上述的转换过程得到的$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合$T_\varphi$与$\varphi$在二元组$\langle V',I\rangle$上逻辑等价。下面给出本章的运行示例来展示每一个过程。

例 4.1 (运行示例)**.** 给定公式$\varphi=\mathrm{A}((p\wedge q)\mathrm{U}(f\vee m))\wedge r$和原子命题的集合$V=\{p,r\}$。$(T_\varphi,V',I)=Transform(\varphi)$，其中$V'=\{x,y,z,w\}$（$w$是与子句$z\rightarrow\mathrm{AF}x$对应的新引入的原子命题[1]），$I=\emptyset$且$T_\varphi$中的元素如下：

1.$\mathbf{start}\rightarrow z$　2.$\top\rightarrow\neg z\vee r$　3.$\top\rightarrow\neg x\vee f\vee m$　4.$\top\rightarrow\neg z\vee x\vee y$
5.$\top\rightarrow\neg y\vee p$　6.$\top\rightarrow\neg y\vee q$　7.$z\rightarrow\mathrm{AF}x$　8.$y\rightarrow\mathrm{AX}(x\vee y)$.

4.3.2 归结过程

本节的归结过程在转换过程之后执行。给定的公式φ和原子命题的集合V，令$(T_\varphi,V',I)=Transform(\varphi)$。在$T_\varphi$和$V\cup V'$上的归结过程（记为$Resolution(T_\varphi,V\cup V')$）产生一个子句集合的序列$T_0=T_\varphi,T_1,T_2,\ldots,T_n=Res$并返回$Res$。在这个序列中，对所有的$0\le i\le n$都有$T_{i+1}=T_i\cup R_i$（$R_i$是由表 2.3中的某条归结规则作用到$T_i$中的某些子句上得到的结果），且在$Res$中不能再由任何的归结规则产生新的子句（或者产生了矛盾，即子句$\mathbf{start}\rightarrow\bot$和子句$\top\rightarrow\bot$，因为在此情况下可以得出$\mathrm{F}_{\mathrm{CTL}}(\varphi,V)\equiv\bot$）。值得注意的是，在这一过程中产生的$T_i$（$0\le i\le n$）是$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合。

下面的命题表示T_φ与归结过程得到的结果在二元组$\langle V\cup V',\emptyset\rangle$上逻辑等价。

[1]注意：本文中对每个Q-某时子句（$Q\in\{\mathrm{E},\mathrm{A}\}$）都产生一个新的原子变量$w$与之对应。

命题 4.3. 给定公式φ和原子命题的集合V。若$(T_\varphi, V', I) = Transform(\varphi)$，则$T_\varphi \equiv_{\langle V\cup V',\emptyset\rangle} Resolution(T_\varphi, V\cup V')$。

证明. 这一结论可以通过证明$T_i \equiv_{\langle V\cup V',\emptyset\rangle} T_{i+1}$（$0 \le i < n$），其中$T_{i+1} = T_i \cup R_i$。记$\Pi \to_r R_i$为通过对$\Pi \subseteq T_i$和原子命题$p \in (V \cap Var(\Pi))$使用表 2.3中的归结规则$r$得到$R_i$。

（1）这里证明若$r \in \{$**(SRES1)**, …, **(SRES8)**, (**RW1**), (**RW2**)$\}$，则$T_i \equiv_{\langle\{p\},\emptyset\rangle} T_{i+1}$。

一方面可以证明$\Pi \models R_i$，因而$T_{i+1} \models T_i$。另一方面，由于$T_i \subseteq T_{i+1}$，所以$T_{i+1} \models T_i$。显然$T_i \equiv T_{i+1}$，又$\emptyset \subseteq (V\cup V')$且$\emptyset \subseteq \emptyset$，由命题 4.1可知$T_i \equiv_{\langle V\cup V',\emptyset\rangle} T_{i+1}$。

（2）这里证明若$r =$**(ERES1)**，则$T_i \equiv_{\langle\{l, w^{\mathrm{A}}_{\neg l}\},\emptyset\rangle} T_{i+1}$，其中$w^{\mathrm{A}}_{\neg l} \in V'$是与子句$Q \to \mathrm{AF}\neg l$相关的新的原子命题，$l$是文字（即：$p$或者$\neg p$）。

在文章[21]中已经证明$\Pi \models R_i$，因此有$T_{i+1} = T_i \cup \Lambda^{\mathrm{A}}_{\neg l}$，其中$\Lambda^{\mathrm{A}}_{\neg l}$是通过使用表 2.1中的转换规则作用到$R_i$上得到的$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合（请查看文章[22]获取更加详细的描述）。显然，对所有的$(\mathscr{M}_1, s_1) \in Mod(T_i = X \cup \Pi)$都存在一个$(\mathscr{M}_2, s_2) \in Mod(T_{i+1} = T_i \cup \Lambda^{\mathrm{A}}_{\neg l})$使得$(\mathscr{M}_1, s_1) \leftrightarrow_{\langle\{p, w^{\mathrm{A}}_{\neg l}\},\emptyset\rangle} (\mathscr{M}_2, s_2)$，且对任意的$(\mathscr{M}_2, s_2) \in Mod(T_{i+1} = T_i \cup \Lambda^{\mathrm{A}}_{\neg l})$也存在一个$(\mathscr{M}_1, s_1) \in Mod(T_i = X \cup \Pi)$使得$(\mathscr{M}_1, s_1) \leftrightarrow_{\langle\{p, w^{\mathrm{A}}_{\neg l}\},\emptyset\rangle} (\mathscr{M}_2, s_2)$。又$\{p, w^{\mathrm{A}}_{\neg l}\} \subseteq (V \cup V')$且$\emptyset \subseteq \emptyset$，由命题 4.1可知$T_i \equiv_{\langle V\cup V',\emptyset\rangle} T_{i+1}$。

当规则为**(ERES2)**时可以类似地证明。 □

命题 4.3和命题 4.2表明$\varphi \equiv_{\langle V'',\emptyset\rangle} Resolution(T_\varphi, V'')$，即对任意的公式$\psi$，$\mathrm{IR}(\psi, V'')$蕴涵“$\varphi \models \psi$当且仅当$Resolution(T_\varphi, V'') \models \psi$”，其中$V'' = V \cup V'$。

例 4.2 (例 4.1的延续)**.** 对例 4.1中的T_φ和$V \cup V'$使用上述归结过程，除了例 4.1中的子句，还得到如下子句:

(1) **start** $\to r$	(1,2,**SRES5**)	(2) **start** $\to x \vee y$	(1,4,**SRES5**)
(3) $\top \to \neg z \vee y \vee f \vee m$	(3,4,**SRES8**)	(4) $y \to \mathrm{AX}(f \vee m \vee y)$	(3,8,**SRES6**)
(5) $\top \to \neg z \vee x \vee p$	(4,5,**SRES8**)	(6) $\top \to \neg z \vee x \vee q$	(4,6,**SRES8**)
(7) $y \to \mathrm{AX}(x \vee p)$	(5,8,**SRES6**)	(8) $y \to \mathrm{AX}(x \vee q)$	(6,8,**SRES6**)
(9) **start** $\to f \vee m \vee y$	(3,(2),**SRES5**)	(10) **start** $\to x \vee p$	(5,(2),**SRES5**)
(11) **start** $\to x \vee q$	(6,(2),**SRES5**)	(12) $\top \to p \vee \neg z \vee f \vee m$	(5,(3),**SRES8**)
(13) $\top \to q \vee \neg z \vee f \vee m$	(6,(3),**SRES8**)	(14) $y \to \mathrm{AX}(p \vee f \vee m)$	(5,(4),**SRES6**)
(15) $y \to \mathrm{AX}(q \vee f \vee m)$	(6,(4),**SRES6**)	(16) **start** $\to f \vee m \vee p$	(5,(9),**SRES5**)
(17) **start** $\to f \vee m \vee q$	(6,(9),**SRES5**)		

4.3.3 “移除”过程

本节意在“移除”如何将归结过程得到的结果中含有V中原子命题的子句，而保证其在二元组$\langle V\cup V,I\rangle$上的逻辑等价关系，这一过程对应算法 4.1中的第9行。给定$\mathrm{SNF}^g_{\mathrm{CTL}}$子句$C$和原子命题的集合$V$：

$$Removing\_atoms(C,V)\equiv\begin{cases}\top, & Var(C)\cap V\neq\emptyset;\\ C, & \text{otherwise.}\end{cases}$$

此外，对于$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的集合$\Pi$，

$$Removing\_atoms(\Pi,V)=\{Removing\_atoms(r,V)\mid r\in\Pi\}.$$

可以看出，通过这一过程后得到的子句集合里的子句不再包含V中的原子命题的集合且与原集合满足下面关系。

命题 4.4. *对于给定的公式φ和原子命题的集合，有：*

$$Resolution(T_\varphi,V\cup V')\equiv_{\langle V\cup V',\emptyset\rangle} Removing\_atoms(Resolution(T_\varphi,V\cup V'),V).$$

证明. 因为要考虑的索引集合为空集，所以只需证明：

$$Resolution(T_\varphi,V\cup V')\equiv_{V\cup V'} Removing\_atoms(Resolution(T_\varphi,V\cup V'),V)$$

其中$\equiv_V$与$\equiv_{\langle V,I\rangle}$的定义类似，只是不考虑索引部分。为了证明这一过程，下面给出两个事实：

- **(GNA)** 对任意的$p\in Var(\varphi)$，p都不出现在$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的左边；
- **(PI)** 对任意的$p\in V'$，如果p出现在$\mathrm{SNF}^g_{\mathrm{CTL}}$子句的左边，那么$p$为负出现，即该子句关于$p$是负的。

不失一般性地，假设$V=\{p\}$，且规定$Res=Resolution(T_\varphi,V\cup V')$、$V''=V\cup V'$、$C_i$是经典子句、$l$是$p$或者$\neg p$。显然，$Res\models Removing\_atoms(Res,V)$，这里将证明对任意的$\mathscr{K}=(\mathscr{M},s)$（$\mathscr{K}\in Mod(Removing_atoms(Res,V))$且$\mathscr{M}=(S,R,L,s)$），存在一个初始结构$\mathscr{K}'=(\mathscr{M}',s')$使得$\mathscr{K}\leftrightarrow_{V''}\mathscr{K}'$且$\mathscr{K}'\models Res$。接下来从两个大点证明这一结论。

（1）假设全局子句$C=\top\rightarrow C_1\vee l\in Res$，其中$Var(l)=\{p\}$。

(a) 如果不存在子句$C'\in Res$使得C和C'在p上是可归结的[2]，这意味着在Res中不存

[2]如果能在表 2.3中找到一条规则使得子句C和C'为该规则的横线上面部分，且相应的文字是p，则称C和C'在p上是可归结。

在其他非Pt-某时子句包含有文字$\neg l$，其中$Pt \in \{\mathrm{A},\mathrm{E}\}$。则有两种情况需要讨论：

(i) $p \notin Var(C')$。$\forall \mathscr{K} = (\mathscr{M},s) \in Mod(Removing_atoms(Res,V))$可以如下构造$(\mathscr{M}',s')$：令$\mathscr{M}' = (S,R,L',s)$（即$s' = s$），其中$L'$与$L$一样，除了对于$s_1 \in S$，如果$(\mathscr{M},s_1) \not\models C_1 \vee l$则“若$l = p$，则令$L'(s_1) = L(s_1) \cup \{p\}$，否则令$L'(s_1) = L(s_1) - \{p\}$”。

(ii) 如果$C' = Q \to Pt\mathrm{F}\neg l$。不失一般性地，假设$l = p$且$Q$为文字（$Q$为文字的合取的情形可以类似证明）。$\forall \mathscr{K} = (\mathscr{M},s) \in Mod(Removing\_atoms(Res,V))$，如下构造$(\mathscr{M}',s')$：令$\mathscr{M}' = (S',R',L',s')$，其中$S' = S$，$R' = R$，$s' = s$，且$L' = L$，除了$\forall s \in S'$，“如果$Q$为正文字，则令$L'(s) = L(s) - \{Q\}$，且若$(\mathscr{M},s) \not\models C_1$，则$L'(s) = L(s) \cup \{p\}$”，否则令$L'(s) = L(s)$。

因此，有$\mathscr{K} \leftrightarrow_{V''} \mathscr{K}'$且$\mathscr{K}' \models Res$。

(b) 如果存在子句$C' \in Res$使得C和C'在p上是可归结的。

(i) 若$C' = Q \to Pt\mathrm{X}(C_2 \vee \neg l)$（这里令$Pt = \mathrm{G}$，当$Pt = \mathrm{E}$时可以类似地证明），因此有$Q \to \mathrm{GX}(C_1 \vee C_2) \in Res$。$\forall \mathscr{K} = (\mathscr{M},s) \in Mod(Removing\_atoms(Res,V))$，如下构造$(\mathscr{M}',s')$：令$\mathscr{M}' = (S,R,L',s)$（即：$s' = s$），其中$L'$与$L$类似，除了$\forall s_1 \in S$，若$(\mathscr{M},s_1) \not\models Q$，则“$\forall (s_1,s_2) \in R$，若“$(\mathscr{M},s_2) \not\models C_1$，则“若$l = p$，则令$L'(s_2) = L(s_2) \cup \{p\}$，否则$L'(s_2) = L(s_2) - \{p\}$””，否则，若$(\mathscr{M},s_2) \models C_1 \wedge \neg C_2$，则“若$l = p$，则$L'(s_2) = L(s_2) - \{p\}$，否则$L'(s_2) = L(s_2) \cup \{p\}$””；否则若$(\mathscr{M},s_2) \models \neg C_1 \wedge C_2$，则“若$l = p$，则令$L'(s_2) = L(s_2) \cup \{p\}$，否则$L'(s_2) = L(s_2) - \{p\}$”。显然，$\mathscr{K} \leftrightarrow_{V''} \mathscr{K}'$且$\mathscr{K}' \models C' \wedge C$。

(ii) 若$C' = Q \to Pt\mathrm{F}\neg l$。不失一般性地，假设$l = p$。由于$C$和$C'$在$p$上可归结，则存在$\mathrm{SNF}^g_{\mathrm{CTL}}$子句集合$\Pi = \{P^1_1 \to *C^1_1, \ldots, P^1_{m_1} \to *C^1_{m_1}, P^n_1 \to *C^n_1, \ldots, P^1_{m_n} \to *C^1_{m_n}\}$使得$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} P^i_j \to \mathrm{EXEG}l$，其中$*$要么为空字符要么为集合$\{\mathrm{GX}, \mathrm{E}\langle ind\rangle\mathrm{X}\}$中的某个元素。此外，$\neg C_1 \to l \in \Pi$。因此，通过规则**ERES1**可以得到子句$C'' = \top \to \neg Q \vee \neg p \vee C_1$（对规则**ERES2**类似）。因此，在子句$C$和$C''$上使用规则**SRES8**可得$\top \to \neg Q \vee C_1$。$\forall \mathscr{K} = (\mathscr{M},s) \in Mod(Removing\_atoms(Res,V))$，可以如下构造$(\mathscr{M}',s')$：令$\mathscr{M}' = (S,R,L',s)$（即：$s' = s$），其中$L'$与$L$类似，除了$\forall s_1 \in S$，“若$(\mathscr{M},s_1) \models Q$，则令$L'(s_1) = L(s_1) - \{p\}$，否则令$L'(s_1) = L(s_1) \cup \{p\}$”。显然，$\mathscr{K} \leftrightarrow_{V''} \mathscr{K}'$且$\mathscr{K}' \models C' \wedge C$。

（2）这里考虑Pt-步子句，令$C \in Res$为子句$Q \to \mathrm{AX}(C_1 \vee \neg l)$。不失一般性地，假设存在子句$C' \in Res$使得$C$和$C'$在$p$上可归结，且$l = p$.

若$C' = Q_1 \to Pt\mathrm{X}(C_2 \vee l)$（$Pt = \mathrm{E}_{ind}$，$Pt = \mathrm{A}$可以类似地证明），则有$Q \wedge Q_1 \to \mathrm{E}_{ind}\mathrm{X}(C_1 \vee C_2) \in Res$。因此，$\forall \mathscr{K} = (\mathscr{M}, s) \in Mod(Removing\_atoms(Res, V))$，构造$(\mathscr{M}', s')$：$\mathscr{M}' = (S, R, L', s)$（令$s' = s$），其中$L'$与$L$类似，除了$\forall s_1 \in S$：

(i) 若$(\mathscr{M}, s_1) \not\models Q \wedge Q_1$则“若$(\mathscr{M}, s_1) \models \neg Q \wedge Q_1$，则（对于$(s_1, s_2') \in \pi_s^{\langle ind \rangle}$，若$(\mathscr{M}, s_2') \not\models C_2$，则令$L'(s_2') = L(s_2') - \{p\}$，否则令$L'(s_2') = L(s_2')$），否则，若$(\mathscr{M}, s_1) \models Q \wedge \neg Q_1$，则$\forall (s_1, s_2) \in R$（若$(\mathscr{M}, s_2) \not\models C_1$，则令$L'(s_2) = L(s_2) \cup \{p\}$，否则令$L'(s_2') = L(s_2')$），否则令$L'(s_2') = L(s_2')$”。

(ii) 否则，若$(\mathscr{M}, s_1) \models Q \wedge Q_1$，则对$(s_1, s_2) \in \pi_s^{\langle ind \rangle}$，有$(\mathscr{M}, s_2') \models C_1 \vee C_2$。因此，若$(\mathscr{M}, s_2') \models C_1 \wedge \neg C_2$，则$L'(s_2') = L(s_2') - \{p\}$，否则，若$(\mathscr{M}, s_2') \models \neg C_1 \wedge C_2$，则令$L'(s_2) = L(s_2) \cup \{p\}$，否则$L'(s_2') = L(s_2')$。对于其他状态$s_2$（$(s_1, s_2) \in R$且$s_2 \neq s_2'$），若$(\mathscr{M}, s_1) \models Q$且$(\mathscr{M}, s_2) \models \neg C_1$，则令$L'(s_2) = L(s_2) \cup \{p\}$，否则令$L'(s_2') = L(s_2')$。

显然，$\mathscr{K} \leftrightarrow_{V''} \mathscr{K}'$且$\mathscr{K}' \models C' \wedge C$，其中$\mathscr{K}' = (\mathscr{M}', s')$。

其他情形的组合都可以从上述描述中找到或者类似，因此不在这里赘述。　□

例 4.3 (例 4.2的延续)**.** 在移除掉$Resolution(T_\varphi, V'')$中包含$V$中元素的子句后，得到如下子句的集合：

$\mathbf{start} \to z$,	$\top \to \neg x \vee f \vee m$,	$\top \to q \vee \neg z \vee f \vee m$,	$y \to \mathrm{AX}(x \vee y)$,
$\mathbf{start} \to f \vee m \vee q$,	$\top \to \neg z \vee x \vee q$,	$z \to \mathrm{AF}x$,	$\top \to \neg z \vee x \vee y$,
$y \to \mathrm{AX}(q \vee f \vee m)$,	$\mathbf{start} \to x \vee y$,	$y \to \mathrm{AX}(x \vee q)$,	$\top \to \neg z \vee y \vee f \vee m$,
$\top \to \neg y \vee q$,	$\mathbf{start} \to f \vee m \vee y$,	$y \to \mathrm{AX}(f \vee m \vee y)$,	$\mathbf{start} \to x \vee q$.

4.3.4　索引和“start”的“消除”

算法 4.1中的一个关键的步骤就是将转换过程中引入的索引和**start**“消除”。通过表 2.1里的规则可知，没有两个E-某时子句有相同的索引，且在归结过程中没有E-某时子句产生。因而可以通过等价关系“$\mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi \equiv \varphi \vee \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{F}\varphi$”事先将“$\mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi$”转换为“$\varphi \vee \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{F}\varphi$”。

引理 4.1. 给定$\mathrm{SNF}^g_{\mathrm{CTL}}$公式$\mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi$，下面等价关系成立：

$$\mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi \equiv \varphi \vee \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{F}\varphi.$$

证明. ($\Rightarrow$) 令$(\mathscr{M}, s_0) \in Mod(\mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi)$，存在一条路径$\pi_{s_0}^{\langle ind \rangle} = (s_0, s_1, \ldots)$使得对于某些$s_j \in \pi_s^{\langle ind \rangle}$（$j \geq 0$）有$(\mathscr{M}, s_j) \models \varphi$。因此，$j = 0$或者$j > 0$，所以有$(\mathscr{M}, s_0) \models \varphi \vee \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{F}\varphi$。

($\Leftarrow$) 令$(\mathscr{M}, s_0) \in Mod(\varphi \vee \mathrm{E}_{\langle ind \rangle}\mathrm{XE}_{\langle ind \rangle}\mathrm{F}\varphi)$，因此有$(\mathscr{M}, s_0) \models \varphi$或者存在一条索引号为$ind$的路径$\pi_{s_0}^{\langle ind \rangle} = (s_0, s_1, \ldots)$使得$(\mathscr{M}, s_1) \models \mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi$。因此，有$(\mathscr{M}, s_0) \models \mathrm{E}_{\langle ind \rangle}\mathrm{F}\varphi$。　□

此外，要消除索引，还需要引入以下等价关系。

引理 4.2. 令P，P_i和φ_i为*CTL*公式，则：

(i) $\bigwedge_{i=1}^{n}(P \to \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_i) \equiv_{\langle\emptyset,\{ind\}\rangle} P \to \mathrm{EX}\bigwedge_{i=1}^{n}\varphi_i$；

(ii) $\bigwedge_{i=1}^{n}(P_i \to \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_i) \equiv_{\langle\emptyset,\{ind\}\rangle} \bigwedge_{e\in 2^{\{1,\ldots,n\}}\setminus\{\emptyset\}}(\bigwedge_{i\in e}P_i \to \mathrm{EX}(\bigwedge_{i\in e}\varphi_i))$；

(iii) $\bigwedge_{i=1}^{n}(P \to \mathrm{E}_{\langle ind\rangle}\mathrm{F}\varphi_i) \equiv_{\langle\emptyset,\{ind\}\rangle} P \to \bigvee \mathrm{EF}(\varphi_{j_1}\wedge\mathrm{EF}(\varphi_{j_2}\wedge\mathrm{EF}(\cdots\wedge\mathrm{EF}\varphi_{j_n})))$，其中$(j_1,\ldots,j_n)$为集合$\{1,\ldots,n\}$中的所有元素构成的序列；

(iv) $(P \to (C \vee \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_1)) \wedge (P \to \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_2) \equiv_{\langle\emptyset,\{ind\}\rangle} P \to ((C\wedge\mathrm{EX}\varphi_2)\vee\mathrm{EX}(\varphi_1\wedge\varphi_2))$；

(v) $(P_1 \to \varphi \vee \mathrm{E}_{\langle ind\rangle}\mathrm{XE}_{\langle ind\rangle}\mathrm{F}\varphi_1)\wedge(P_2 \to \mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_2) \equiv_{\langle\emptyset,\{ind\}\rangle} (P_1 \to \varphi\vee\mathrm{EXEF}\varphi_1)\wedge(P_2\to\mathrm{EX}\varphi_2)$ $\wedge(P_1\wedge P_2 \to ((\varphi\wedge\mathrm{EX}\varphi_2)\vee\mathrm{EX}(\varphi_2\wedge\mathrm{EF}\varphi_1)))$。

证明. (i) $\forall(\mathscr{M},s_0)\in Mod(\bigwedge_{i=1}^{n}(P\to\mathrm{E}_{\langle ind\rangle}\mathrm{X}\varphi_i))$，若$(\mathscr{M},s_0)\models P$，则存在$(s_0,s_1)\in[ind]$使得$(\mathscr{M},s_1)\models\varphi_1,\ldots,(\mathscr{M},s_1)\models\varphi_n$。因此存在$(s_0,s_1)\in R$使得$(\mathscr{M},s_1)\models\bigwedge_{i=1}^{n}\varphi_i$，即$(\mathscr{M},s_0)\models P\to\mathrm{EX}\bigwedge_{i=1}^{n}\varphi_i$。

$\forall(\mathscr{M},s_0)\in Mod(P\to\mathrm{EX}\bigwedge_{i=1}^{n}\varphi_i)$，假定存在$(s_0,s_1)\in R$使得$(\mathscr{M},s_1)\models\bigwedge_{i=1}^{n}\varphi_i$。容易构造一个初始Ind-结构$(\mathscr{M}',s_0)$使得$(\mathscr{M}',s_0)$与$(\mathscr{M},s_0)$相同，除了$(s_0,s_1)\in[ind]$，即：$(\mathscr{M},s_0)\leftrightarrow_{\langle\emptyset,\{ind\}\rangle}(\mathscr{M}',s_0)$。

(ii) ($\Rightarrow$) 对等式左手边公式的任意模型$(\mathscr{M},s_0)$，若$(\mathscr{M},s_0)\models\bigwedge_{i=1}^{m}P_{j_i}$（$j_i\in\{1,\ldots,n\}$且$1\le m\le n$），则存在$s_0$的下一个状态$s_1$（即：$(s_0,s_1)\in[ind]$）使得$(\mathscr{M},s_1)\models\bigwedge_{i=1}^{m}\varphi_{j_i}$。通过$[ind]$的定义，有$(s_0,s_1)\in R$，因此$(\mathscr{M},s_0)\models\bigwedge_{i=1}^{m}P_{j_i}\to\mathrm{EX}(\bigwedge_{i=1}^{m}\varphi_{j_i})$。另一边类似(i)的证明。

(iii) ($\Leftarrow$) 对等式右手边公式的任意模型$(\mathscr{M},s_0)$，如果$(\mathscr{M},s_0)\models P$，则存在一条路径$\pi_{s_0}=(s_0,s_1,\ldots)$使得$(\mathscr{M},s_{j_i})\models\varphi_{j_i}$（$1\le i\le n$）。构造一个初始Ind-结构$(\mathscr{M}',s_0)$使得$(\mathscr{M}',s_0)$与$(\mathscr{M},s_0)$相同，除了对$\pi_{s_0}$上的任意$(s_j,s_{j+1})$，存在$(s_j,s_{j+1})\in[ind]$ $(0\le j)$。显然，$(\mathscr{M}',s_0)\models\bigwedge_{i=1}^{n}(P\to\mathrm{E}_{\langle ind\rangle}\mathrm{F}\varphi_i)$且$(\mathscr{M},s_0)\leftrightarrow_{\langle\emptyset,\{ind\}\rangle}(\mathscr{M}',s_0)$。另一个方向与(ii)中的证明类似。

其他结果显然是成立的，类似上面的证明。 □

给定子句集合Π，*Removing_index*(Π)这一过程使用引理 4.2中的等价关系将出现在Π中的子句中的索引“去掉”，并返回不具有索引的公式的集合。

命题 4.5. 令Π是$\mathrm{SNF}^{g}_{\mathrm{CTL}}$子句的集合，且对于任意的索引$i$，至多包含一个索引为$i$的E-某时子句。因此，

$$\Pi \equiv_{\langle\emptyset,I\rangle} Removing\_index(\Pi)$$

其中I是出现在Π中的索引的集合.

证明. 由于Π没有两个E-某时子句有相同的索引，所以事先使用引理 4.1中的等价关系将显示出$\mathrm{E}_{ind}\mathrm{X}$时序算子，然后使用引理 4.2中的等价关系“消除”掉$\mathrm{E}_{ind}\mathrm{X}$中的索引。□

需要指出的是，例 4.3中没有索引需要消除。

给定公式φ，下面定义从φ中“消除”**start**的操作，结果记为φ_{CTL}：

$$\varphi_{\mathrm{CTL}} \equiv \begin{cases} D, & \text{如果}\varphi\text{是}\mathrm{AG}(\mathbf{start} \rightarrow D)\text{这种形式;} \\ \varphi, & \text{否则。} \end{cases}$$

此外，对于给定的公式的集合Π，$\Pi_{\mathrm{CTL}} = \{\varphi_{CTL} \mid \varphi \in \Pi\}$。因此，由$\varphi \equiv \mathrm{AG}(\mathbf{start} \rightarrow \varphi)$[21]可知$\Pi \equiv \Pi_{\mathrm{CTL}}$。

到此为止，已经介绍完了算法 4.1中的每个步骤。综上所述，通过算法 4.1得到的结果$ERes(\varphi, V)$与原公式φ在二元组$\langle V \cup V', \emptyset\rangle$上逻辑等价。在接下来的小节中将着重探讨本章开头提出的算法的一些相关计算属性，并提出一种一般的Ackermann引理来尽可能地使$ERes(\varphi, V)$逼近从φ中遗忘掉原子命题集合V的结果。

4.3.5　替换V'中的原子

尽管在 4.3.3节中已经定义了“移除”与V中元素相关的子句的操作，但是由转换过程可知新的原子命题（即V'中的原子命题）被引入而还没被处理过。为了尽可能多地替换这些原子命题，这部分扩展Szalas提出的Ackermann引理[23]如下。在此之前，先约定一些记号：对于给定的公式（或公式的集合）Γ，用$\Gamma[x/\varphi]$表示将Γ中的所有x的出现用φ替换得到的结果；在公式$Qt\mathscr{T}C$中，Qt（$\mathscr{T}$）为空字符或者$Qt \in \{\mathrm{A}, \mathrm{E}\}$且$\mathscr{T} \in \{\mathrm{X}, \mathrm{F}\}$。

定理 4.1 (一般化的Ackermann引理)**.** 令$\Delta = \{\top \rightarrow \neg x \vee C_1, \ldots, \top \rightarrow \neg x \vee C_n, x \rightarrow B_1, \ldots, x \rightarrow B_m\}$、$\Gamma'$是算法 *4.1*中*NI*的子集，$\Gamma = \Delta \cup \Gamma'$。其中，$x \in V'$、$C_i$ $(1 \leq i \leq n)$是不包含原子命题x的经典子句、B_j $(1 \leq j \leq m)$是形如$Qt\mathscr{T}C$形式的公式的吸取或者合取（其中C为不包含原子命题x的*CTL*公式）。令$\varphi = \bigwedge_{i=1}^{n} C_i \wedge \bigwedge_{j=1}^{m} B_j$，那么如果$\Gamma'$关于$x$是正的，则$\Gamma'[x/\varphi] \equiv_{\langle\{x\},\emptyset\rangle} \Gamma$。

证明. ($\Rightarrow$) 对任意Γ的模型$(\mathscr{M}, s_0)$，由于Γ'关于x是正的（即：Γ'关于x是单调的）且$x \rightarrow \varphi$，因而有$(\mathscr{M}, s_0) \models \Gamma'[x/\varphi]$。

($\Leftarrow$) 对任意$\Gamma'[x/\varphi]$的模型$(\mathscr{M}, s_0)$（$\mathscr{M} = (S, R, L, [_], s_0)$），构造一个Ind-初始结构$\mathscr{M}' = (S', R', L', [_]', s_0')$使得$S' = S$、$R' = R$、$s_0' = s_0$、$[\_] = [\_]'$、且$L'$与$L$相同，除了对任意的$s' \in S'$，若$(\mathscr{M}', s') \models \varphi$，则令$L'(s') = L(s) \cup \{x\}$，否则令$L'(s') = L(s) - \{x\}$（即：$x \leftrightarrow \varphi$）。

显然，$(\mathscr{M},s_0)\leftrightarrow_{\langle\{x\},\emptyset\rangle}(\mathscr{M}',s_0')$且$(\mathscr{M}',s_0')\models\Gamma$。 □

这一结论尽量“去掉”了V'中的原子命题。在算法 4.1中并没有把这一过程写入，但是为了使算法的结果更加接近遗忘的结果，这一过程被加到消除**start**之前，消除索引之后。下面的例子展示了这一过程。

例 4.4 (例 4.3的延续)**.** 假定例 4.3中的子句的集合为Γ。显然，$\Delta=\{\top\rightarrow\neg x\vee f\vee m\}$且$\Gamma'=\Gamma-\Delta$。则使用定理 4.1在$\Delta$上（关于$x$），然后再使用定理 4.1在$\{\top\rightarrow\neg z\vee f\vee m\vee y,\top\rightarrow\neg z\vee f\vee m\vee q,\top\rightarrow\neg z\vee \mathrm{AF}(f\vee m)\}$上（关于$z$）得到下面的公式的集合：

$\mathbf{start}\rightarrow(f\vee m\vee y)\wedge(f\vee m\vee q)\wedge\mathrm{AF}(f\vee m)$, $\mathbf{start}\rightarrow f\vee m\vee q$, $\top\rightarrow\neg y\vee q$,
$y\rightarrow\mathrm{AX}(f\vee m\vee y)$, $\mathbf{start}\rightarrow f\vee m\vee y$, $y\rightarrow\mathrm{AX}(f\vee m\vee q)$.

此外，在上面例子的结果中使用“消除”**start**过程得到下面的公式的集合:

$(f\vee m\vee y)\wedge(f\vee m\vee q)\wedge\mathrm{AF}(f\vee m)$, $f\vee m\vee q$, $\mathrm{AG}(\top\rightarrow\neg y\vee q)$,
$\mathrm{AG}(y\rightarrow\mathrm{AX}(f\vee m\vee y))$, $f\vee m\vee y$, $\mathrm{AG}(y\rightarrow\mathrm{AX}(f\vee m\vee q))$.

从上面的几个结论可以得出，对对给定的CTL公式φ和原子命题集合V，当包含V'（转换构成引入的原子命题的集合）中的原子命题的子句能够从NI中移除，则得到的结果为从φ中遗忘掉V后得到的结果。

定理 4.2. *给定CTL公式φ和原子命题集合V。则$\mathrm{ERes}(\varphi,V)\equiv_{\langle V',\emptyset\rangle}\mathrm{F_{CTL}}(\varphi,V)$，其中$V'$是由$Transform$过程引入并存留在$\mathrm{ERes}(\varphi,V)$的原子命题的集合。*

证明. 由命题4.2-4.5和定理4.1可知$\varphi\equiv_{\langle V'\cup V,\emptyset\rangle}ERes(\varphi,V)$。又$\varphi\equiv_{\langle V,\emptyset\rangle}\mathrm{F_{CTL}}(\varphi,V)$（由遗忘理论的定义）、$\mathrm{IR}(ERes(\varphi,V),V)$ 和$\mathrm{IR}(\mathrm{F_{CTL}}(\varphi,V),V)$，因此有$ERes(\varphi,V)\equiv_{\langle V',\emptyset\rangle}\mathrm{F_{CTL}}(\varphi,V)$。 □

这里需要说明的是，有的情况下算法 4.1不能完全替换掉V'中的原子命题，这与CTL不具有均匀插值性[24]一致。否则，若对于任意的CTL公式φ和原子命题集合V，存在一个CTL公式ψ使得$\mathrm{IR}(\psi,V\cup V')$且$\psi\equiv ERes(\varphi,V)$，则通过定理 4.2可知$\mathrm{F_{CTL}}(\varphi,V)$总是存在。这与CTL不具有均匀插值性形成矛盾。

尽管如此，有的CTL公式的遗忘结果总是存在的，如下面的结论所示。

命题 4.6. *给定CTL公式φ，若φ满足下面约束：φ中不包括操作符$Pt\mathscr{T}$（其中$Pt\in\{\mathrm{A},\mathrm{E}\}$且$\mathscr{T}\in\{\mathrm{U},\mathrm{G}\}$），且对于任意的原子命题$p\in V$，若$p$和$\neg p$出现在同一时序算子的范围内；则$\mathrm{ERes}(\varphi,V)\equiv\mathrm{F_{CTL}}(\varphi,V)$。*

证明. 不失一般性地假设$V=\{p\}$。对任意上述所说形式的CTL公式φ，假定$\varphi=\varphi_1\wedge\mathrm{AXEF}\varphi_2$，其中$p\notin Var(\varphi_1)$且$\varphi_2$是一个包含子句$C_1=\neg p\vee\psi_1$和$C_2=p\vee\psi_2$的CNF(conjunctive normal form)公式。φ可以被转换为包含集合$\Pi=\{\top\rightarrow\neg x\vee p\vee\psi_1,\top\rightarrow\neg x\vee\neg p\vee\psi_2\}$的

子句的集合Σ，其中x为新引入的原子命题，ψ_i（$i=1,2$）为经典子句。除此之外，Σ中不包含其他含有p的公式。

由归结过程可产生子句$\top \rightarrow \neg \vee \psi_1 \vee \psi_2$，由定理 4.1可知，$x$可以被$\psi_1 \vee \psi_2$替换。又因为公式$\varphi$中不包含$Pt\mathscr{T}$时序算子，因而不会产生引入嵌套原子命题（同时出现在$\rightarrow$两边的原子命题），此时对新引入的其余的原子命题都可使用定理 4.1。因此，由定理 4.2可知$ERes(\varphi,V) \equiv \mathrm{F}_{\mathrm{CTL}}(\varphi,V)$。 □

4.4　算法的可终止性和计算复杂性

已有结果表明，转换过程和归结过程会终止[7]。此外，*Remove_atoms*、*Remove_index*、替换V'中的原子命题和T_{CTL}过程都会终止，因此算法 4.1会终止。其具体的时间和空间复杂性如下面的结论所示。

命题 4.7. *给定CTL公式φ和原子命题集合$V \subseteq \mathscr{A}$，令$(T_\varphi,V',I)=Transform(\varphi)$. 算法 4.1的时间和空间复杂性为$O((m+1)2^{4(n+n')})$，其中$n=|Var(\varphi)|$、$n'=|V'|$且$m=|I|$。*

证明. 由于*Transform*过程在多项时间内完成，*Remove_atoms*、*Remove_index*、T_{CTL}过程和替换V'中的原子命题最多都只需要扫描$Resolution(\varphi)$集合就能完成。因此，算法的复杂性主要依赖于归结过程。

对于给定的公式φ、V、V'和Ind，归结过程产生的子句个数为$(m+1)2^{4(n+n')}+(m*(n+n')+n+n'+1)2^{2(n+n')+1})$。 □

在上述结论中值得注意的是m的大小不会大于公式φ中出现的时序算子的个数，因此可以得出算法 4.1的计算复杂性仅与出现在φ的原子命题个数和时序算子的个数相关。

4.5　本章小结

kdjfskdfjwiequroewqrjklsef

本章针对差分隐私数据发布中的隐私保护问题，借鉴Shannon信息论基本通信模型，在隐私与数据效用的度量基础上，利用率失真理论构建了隐私与失真的最优化模型，研究了满足数据质量损失约束条件的互信息隐私最优化机制问题，给出差分隐私数据发布的互信息隐私优化模型。随后，在数据发布的隐私通信模型中，考虑了隐私攻击者可能具有的关联辅助背景知识对互信息隐私泄露的影响，提出了基于联合事件的最小化互信息隐私泄露的优化模型。对于模型求解计算信道条件概率分布的问题，利用拉格朗日乘子法和凸问题的KKT最优性条件，给出解的参量表达式。在迭代算法计算方面，基于率失真函数求解的Blahut-Arimoto算法设计了最优化信道条件概率的迭

代求解算法。最后，通过真实数据集上的实验结果，阐述了本章理论部分的研究成果，分析了所提出模型及算法的有效性及优势。

第五章　基于模型的方法计算CTL下的遗忘

遗忘理论与均匀插值是一对对偶概念，已有研究表明*CTL*不具有均匀插值性质[24]，这就表明*CTL*中的遗忘理论不是封闭的[1]。此时，探索*CTL*下遗忘理论封闭的情形对深入引用遗忘理论有重要意义。为此，本章首先提出有限初始K-结构的特征公式；其次，表明*CTL*公式的遗忘结果在此情形下可以表示成其模型的特征公式的吸取；最后，提出一种基于模型的方法计算遗忘，且探索了如何使用遗忘计算最弱充分条件和知识更新。

5.1　引言

计算树逻辑是由Clarke和Emerson提出的一种分支时间时序逻辑，它能很好的描述并发系统的一些性质。Emerson和Halpern证明CTL具有小模型属性：如果一个公式是可满足的，那么它在一个小的有限模型下是可满足的[25]。具体说来，对于给定的CTL公式φ，如果公式的长度[2]为n（记为：$|\varphi| = n$），则存在一个状态数为$n8^n$的初始K-结构$(\mathscr{M}, s_0)$使得$(\mathscr{M}, s_0) \models \varphi$。

此外，现实情况下能处理的系统都是有限的，且在某一固定环境下所涉及到的原子命题是有限的。因此，在这部分讨论一种约束的CTL，即：（1）出现在CTL公式中的原子命题的个数是有限的（即$\mathscr{A}$是有限的）；（2）初始结构的状态空间S是一个有限的固定状态空间$\mathscr{S} = \{b_1, \ldots, b_m\}$的子集（即$S \subseteq \mathscr{S}$），且使得对于任意约束长度的CTL公式$\varphi$，若$\varphi$是可满足的，则存在一个初始K-结构$(\mathscr{M}, s_0)$使得$(\mathscr{M}, s_0) \models \varphi$且其状态空间是$\mathscr{S}$的子集。由此可见，在这种情形下只有有限个初始结构应该被考虑。

下文将表明在这一约束条件下CTL中的遗忘是封闭的。

本章其余部分组织如下：首先，第**??**节介绍本章的基本定义、系统模型，提出研究问题。其次，第**??**节阐述本章中提出的优化模型和ORRP方案。进一步，第**??**节给出所提方案在理论上的性能分析。随后，第**??**节给出真实数据集上的实验结果。最后，在第5.5节中进行本章工作总结。

5.2　描述初始K-结构

本节介绍与一个初始K-结构相关的CTL公式——特征公式是如何得到的。对于一个给定的初始K-结构，其特征公式其计算树的特征公式密切相关。为此，本节首先

[1]对于给定的逻辑语言$\mathscr{L}$和该语言上的操作$\mathscr{O}$，若$\mathscr{O}$作用到$\mathscr{L}$中的元素后得到的结果仍然在$\mathscr{L}$中，则称$\mathscr{O}$在$\mathscr{L}$下是封闭的。

[2]给定公式φ，出现在该公式里的符号的个数为公式的长度，记为$|\varphi|$。

介绍计算树之间的V-互模拟关系，然后给出计算树的特征公式的定义，最后给出初始K-结构的特征公式。

5.2.1 计算树的V-互模拟

****

引理 5.1. 给定原子命题集合$V \subseteq \mathscr{A}$和K-结构，其中$i = 1,2$且$\mathscr{M}_i = (S_i, R_i, L_i, s_0^i)$为有限初始结构。$(s_1, s_2) \in \mathscr{B}$当且仅当$s_1 \leftrightarrow_V s_2$。

证明. 值得注意的是对任意的$n \geq 0$，都有$\mathscr{B}_{n+1} \subseteq \mathscr{B}_n$。又因为$\mathscr{B}_0 \subseteq S_1 \times S_2$ 是有限的，因而存在一个数k使得$\mathscr{B}_{k+1} = \mathscr{B}_k = \mathscr{B}$。

（1）证明若$(s_1, s_2) \in \mathscr{B}$则$s_1 \leftrightarrow_V s_2$。显然，$(s_1, s_2) \in \mathscr{B}$。所以，只需要证明$\mathscr{B}$是$\mathscr{M}_1$和$\mathscr{M}_1$之间的一个$V$-互模拟关系。下面证明对任意的$r_1 \in S_1$和$r_2 \in S_2$，$(r_1, r_2) \in \mathscr{B}$当且仅当

(a) $L_1(r_1) - V = L_2(r_2) - V$;

(b) $\forall w_1 \in S_1$, if $(r_1, w_1) \in R_1$, then $\exists w_2 \in S_2$ s.t. $(r_2, w_2) \in R_2$ and $(w_1, w_2) \in \mathscr{B}$; and

(c) $\forall w_2 \in S_2$, if $(r_2, w_2) \in R_2$, then $\exists w_1 \in S_1$ s.t. $(r_1, w_1) \in R_1$ and $(w_1, w_2) \in \mathscr{B}$.

$(\Rightarrow)$ $(r_1, r_2) \in \mathscr{B}$
$\Rightarrow \forall n \geq 0$，$(r_1, r_2) \in \mathscr{B}_n$
$\Rightarrow (r_1, r_2) \in \mathscr{B}_0$且$\forall n > 0$，$(r_1, r_2) \in \mathscr{B}_n$
$\Rightarrow L_1(r_1) - V = L_2(r_2) - V$ （因此，(a)成立），

且$\forall n \geq 0$，$(r_1, r_2) \in \mathscr{B}_{n+1}$意味着下面几点成立：

- $L_1(r_1) - V = L_2(r_2) - V$;
- $\forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$(w_1, w_2) \in \mathscr{B}_n$；且
- $\forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$(w_1, w_2) \in \mathscr{B}_n$。

因为存在一个数k使得$\mathscr{B}_{k+1} = \mathscr{B}_k = \mathscr{B}$，所以对这样的$k$有$(r_1, r_2) \in \mathscr{B}_{k+1}$使得：

- $L_1(r_1) - V = L_2(r_2) - V$;
- $\forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$(w_1, w_2) \in \mathscr{B}_k$
  $\Rightarrow \forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$(w_1, w_2) \in \mathscr{B}$ （因此，(b)成立）。

- $\forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$(w_1, w_2) \in \mathscr{B}_k$
  $\Rightarrow \forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$(w_1, w_2) \in \mathscr{B}$（因此，(c)成立）。

因此，$\mathscr{B}$是$\mathscr{M}_1$和$\mathscr{M}_1$之间的一个V-互模拟关系。又因为$(s_1, s_2) \in \mathscr{B}$，所以$s_1 \leftrightarrow_V s_2$。

($\Leftarrow$) 假定(a)、(b)和(c)成立，这里证明$(r_1, r_2) \in \mathscr{B}$，即：对于任意的$n \geq 0$都有$(r_1, r_2) \in \mathscr{B}_n$。

(1) 由(a)可知$(r_1, r_2) \in \mathscr{B}_0$，即：$L_1(r_1) - V = L_2(r_2) - V$。

(2) 由(b)可知：$\forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$\forall n \geq 0$都有$(w_1, w_2) \in \mathscr{B}_n$
$\Rightarrow \forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$\forall n > 0$都有$(w_1, w_2) \in \mathscr{B}_{n-1}$
$\Rightarrow \forall n > 0$，$\forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$(w_1, w_2) \in \mathscr{B}_{n-1}$。

(3) 由(c)可知：$\forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$\forall n \geq 0$都有$(w_1, w_2) \in \mathscr{B}_n$
$\Rightarrow \forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$\forall n > 0$都有$(w_1, w_2) \in \mathscr{B}_{n-1}$
$\Rightarrow \forall n > 0$，$\forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$(w_1, w_2) \in \mathscr{B}_{n-1}$。

因此，$\forall n > 0$有：

- $(r_1, r_2) \in \mathscr{B}_0$;
- $\forall w_1 \in S_1$，若$(r_1, w_1) \in R_1$，则$\exists w_2 \in S_2$使得$(r_2, w_2) \in R_2$且$(w_1, w_2) \in \mathscr{B}_{n-1}$；且
- $\forall w_2 \in S_2$，若$(r_2, w_2) \in R_2$，则$\exists w_1 \in S_1$使得$(r_1, w_1) \in R_1$且$(w_1, w_2) \in \mathscr{B}_{n-1}$。

所以对于任意的$n \geq 0$都有$(r_1, r_2) \in \mathscr{B}$，即：$(r_1, r_2) \in \mathscr{B}$。

（ii）由$s_1 \leftrightarrow_V s_2$可知存在$\mathscr{M}_1$和$\mathscr{M}_1$之间的一个$V$-互模拟关系$\mathscr{R}$使得$(s_1, s_2) \in \mathscr{R}$。令$\mathscr{B} = \mathscr{R}$，显然对任意的$n \geq 0$有$(s_1, s_2) \in \mathscr{B}_n$。

□

给定原子命题集合$V \subseteq \mathscr{A}$和初始结构$\mathscr{M}_i$（$i = 1, 2$）。如果下面条件同时被满足，则称$\mathscr{M}_1$的计算树$\mathrm{Tr}_n(s_1)$和$\mathscr{M}_2$的计算树$\mathrm{Tr}_n(s_2)$是V-互模拟的（记为$(\mathscr{M}_1, \mathrm{Tr}_n(s_1)) \leftrightarrow_V (\mathscr{M}_2, \mathrm{Tr}_n(s_2))$，简写为$\mathrm{Tr}_n(s_1) \leftrightarrow_V \mathrm{Tr}_n(s_2)$）：

- $L_1(s_1)-V=L_2(s_2)-V$,
- 对$\mathrm{Tr}_n(s_1)$的任意子树$\mathrm{Tr}_{n-1}(s_1')$，都存在$\mathrm{Tr}_n(s_2)$的一棵子树$\mathrm{Tr}_{n-1}(s_2')$使得$\mathrm{Tr}_{n-1}(s_1')\leftrightarrow_V \mathrm{Tr}_{n-1}(s_2')$，且
- 对任意$\mathrm{Tr}_n(s_2)$的子树$\mathrm{Tr}_{n-1}(s_2')$，都存在$\mathrm{Tr}_n(s_1)$的一棵子树$\mathrm{Tr}_{n-1}(s_1')$使得$\mathrm{Tr}_{n-1}(s_1')\leftrightarrow_V \mathrm{Tr}_{n-1}(s_2')$。

在上述定义中，当$n=0$时，只需考虑第一个条件。

命题 5.1. *给定原子命题集合$V\subseteq\mathscr{A}$和K结构$(\mathscr{M}_i,s_i)$（$i=1,2$）。则：*

$$(s_1,s_2)\in\mathscr{B}_n \text{当且仅当对任意的} 0\leq j\leq n \text{有} Tr_j(s_1)\leftrightarrow_V Tr_j(s_2)。$$

证明. 这里从下面两个方面来证明这一结论：

($\Rightarrow$) 这里证明“如果$(s_1,s_2)\in\mathscr{B}_n$，则对于任意的$0\leq j\leq n$有$Tr_j(s_1)\leftrightarrow_V Tr_j(s_2)$”成立。$(s_1,s_2)\in\mathscr{B}_n$意味着$Tr_n(s_1)$和$Tr_n(s_2)$的根有同样的标签（除了$V$里的元素之外）。此外，对任意的$(s_1,s_{1,1})\in R_1$，存在一个$(s_2,s_{2,1})\in R_2$使得$(s_{1,1},s_{2,1})\in\mathscr{B}_{n-1}$；且对任意的$(s_2,s_{2,1})\in R_2$，存在一个$(s_1,s_{1,1})\in R_1$使得$(s_{1,1},s_{2,1})\in\mathscr{B}_{n-1}$。因此，由定义可知$Tr_1(s_1)\leftrightarrow_V Tr_1(s_2)$。递归地使用上述方法可得对任意的$0\leq j\leq n$都有$Tr_j(s_1)\leftrightarrow_V Tr_j(s_2)$。

($\Leftarrow$)这里证明“如果对于任意的$0\leq j\leq n$有$Tr_j(s_1)\leftrightarrow_V Tr_j(s_2)$，则$Tr_j(s_1)\leftrightarrow_V Tr_j(s_2)$”成立。由$Tr_0(s_1)\leftrightarrow_V Tr_0(s_2)$可知$L(s_1)-V=L'(s_2)-V$，因而$(s_1,s_2)\in\mathscr{B}_0$。由$Tr_1(s_1)\leftrightarrow_V Tr_1(s_2)$可知$L(s_1)-V=L'(s_2)-V$，且对于一棵树根的任意后继状态$s$，都能找到另一棵树根的一个后继状态$s'$使得$(s,s')\in\mathscr{B}_0$。因此有$(s_1,s_2)\in\mathscr{B}_1$。同理可证$(s_1,s_2)\in\mathscr{B}_2,\ldots,(s_1,s_2)\in\mathscr{B}_n$。 □

命题 5.1表明如果任意两个初始结构中的两个状态s_1和s_2能够在$\mathscr{A}-V$上相互模拟对方直到n步，当且仅当分别以s_1和s_2为根的计算树能在$\mathscr{A}-V$上相互模拟直到深度为n。由此可知，如果同一初始结构的两个状态s和s'不是V-互模拟的，则存在一个数$k\in\mathbb{N}$使得分别以s和s'为根的计算树$\mathrm{Tr}_k(s)$和$\mathrm{Tr}_k(s')$不是V-互模拟的。

命题 5.2. *给定原子命题集合$V\subseteq\mathscr{A}$、初始结构$\mathscr{M}$和两个状态$s,s'\in S$。若$s\not\leftrightarrow_V s'$，则存在一个最小整数$k$使得$Tr_k(s)$和$Tr_k(s')$不是$V$-互模拟的。*

证明. 若$s\not\leftrightarrow_V s'$，则存在一个最小的数$c$使得$(s_i,s_j)\notin\mathscr{B}_c$。因此，由命题 5.1可知，存在一个最小整数$m$（$m\leq c$）使得$\mathrm{Tr}_m(s_i)$和$\mathrm{Tr}_m(s_j)$不是$V$-互模拟的。令$k=m$可得上述结论。 □

5.2.2　计算树的特征公式

由上面小节的讨论可知，V-互模拟可以将计算树分别开来[3]。本节讨论如何使用CTL公式描述一棵计算树，且表明具有（或没有）V-互模拟关系之间的计算树的特征公式又有怎么样的关系。为此，首先给出计算树的特征公式的定义。

定义 5.1. 给定原子命题集合$V \subseteq \mathscr{A}$、初始结构$\mathscr{M} = (S,R,L,s_0)$和状态$s \in S$。定义在$V$上的计算树$Tr_n(s)$的特征公式（记为$\mathscr{F}_V(Tr_n(s))$，$n \geq 0$）被递归定义如下：

$$\mathscr{F}_V(Tr_0(s)) = \bigwedge_{p \in V \cap L(s)} p \wedge \bigwedge_{q \in V - L(s)} \neg q,$$

$$\mathscr{F}_V(Tr_{k+1}(s)) = \bigwedge_{(s,s') \in R} \mathrm{EX}\mathscr{F}_V(Tr_k(s')) \wedge \mathrm{AX}\left(\bigvee_{(s,s') \in R} \mathscr{F}_V(Tr_k(s')) \right) \wedge \mathscr{F}_V(Tr_0(s)) \quad (k \geq 0)。$$

由定义 5.1可知，计算树的特征公式从三个方面展示了计算树的信息：（1）只考虑V中的原子命题；（2）突出了树节点的内容，即：对于任意原子命题$p \in V$，若p在节点的标签中，则其正出现在特征公式中，否则负出现在特征公式中；（3）公式中的时序算子表示了状态之间的转换关系。通俗地讲，$\mathscr{F}_V(\mathrm{Tr}_0(s))$表明了节点$s$的在$V$上的内容；EX的合取部分和AX部分保证以$s$的每个直接后继状态$s'$为根深度为$k$的计算树都有一个CTL公式来描述。

下面的结论表明，若两个计算树是V-互模拟的，则他们在V上的特征公式是逻辑等价的。

引理 5.2. 给定原子命题集合$V \subseteq \mathscr{A}$、初始结构$\mathscr{M} = (S,R,L,s_0)$和$\mathscr{M}' = (S',R',L',s'_0)$、$s \in S$、$s' \in S'$且$n \geq 0$。若$Tr_n(s) \leftrightarrow_{\overline{V}} Tr_n(s')$，则$\mathscr{F}_V(Tr_n(s)) \equiv \mathscr{F}_V(Tr_n(s'))$。

证明. 通过归纳计算树的深度n来证明。

基始（$n = 0$）：对任意的$s_x \in S$和$s'_x \in S'$，若$\mathrm{Tr}_0(s_x) \leftrightarrow_{\overline{V}} \mathrm{Tr}_0(s'_x)$，则由$L(s_x) - \overline{V} = L'(s'_x) - \overline{V}$可知$\mathscr{F}_V(\mathrm{Tr}_0(s_x)) \equiv \mathscr{F}_V(\mathrm{Tr}_0(s'_x))$。

归纳步（$n > 0$）：假设对任意的$0 \leq m \leq n$若$\mathrm{Tr}_m(s) \leftrightarrow_{\overline{V}} \mathrm{Tr}_m(s')$，则$\mathscr{F}_V(\mathrm{Tr}_m(s)) \equiv \mathscr{F}_V(\mathrm{Tr}_m(s'))$。这里要证明若$\mathrm{Tr}_{n+1}(s) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n+1}(s')$，则$\mathscr{F}_V(\mathrm{Tr}_{n+1}(s)) \equiv \mathscr{F}_V(\mathrm{Tr}_{n+1}(s'))$。

由归纳假设可知，对任意的$k = m$、$s_k \in S$ 和$s'_k \in S'$，若$\mathrm{Tr}_{n-k}(s_k) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n-k}(s'_k)$，则$\mathscr{F}_V(\mathrm{Tr}_{n-k}(s_k)) \equiv \mathscr{F}_V(\mathrm{Tr}_{n-k}(s'_k))$。因此，要证原结论成立，只需要证明若$\mathrm{Tr}_{n-k+1}(s_{k-1}) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n-k+1}(s'_{k-1})$，则$\mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s_{k-1})) \equiv \mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s'_{k-1}))$。其中，$(s_{k-1},s_k) \in R$且$(s'_{k-1},s'_k) \in$

[3] Similar approaches has been taken in the literature e.g., in [26], a class (namely, $\equiv_{\overline{k}}$-class) of structures of monadic formulas has been characterized by Hintikka formulas [27]. Another example is Yankov-Fine construction in [28].

R'。显然，由计算树的特征公式可知：

$$\mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s_{k-1})) = \left(\bigwedge_{(s_{k-1},s_k)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_{n-k}(s_k))\right) \wedge \mathrm{AX}\left(\bigvee_{(s_{k-1},s_k)\in R} \mathscr{F}_V(\mathrm{Tr}_{n-k}(s_k))\right) \wedge \mathscr{F}_V(\mathrm{Tr}_0(s_{k-1}))$$

and

$$\mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s'_{k-1})) = \left(\bigwedge_{(s'_{k-1},s'_k)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_{n-k}(s'_k))\right) \wedge \mathrm{AX}\left(\bigvee_{(s'_{k-1},s'_k)\in R} \mathscr{F}_V(\mathrm{Tr}_{n-k}(s'_k))\right) \wedge \mathscr{F}_V(\mathrm{Tr}_0(s'_{k-1})).$$

又因为$\mathrm{Tr}_{n-k+1}(s_{k-1}) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n-k+1}(s'_{k-1})$，所以对任意的$(s_{k-1},s_k)\in R$存在$(s'_{k-1},s'_k)\in R'$使得$\mathrm{Tr}_{n-k}(s_k) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n-k}(s'_k)$，且对任意的$(s'_{k-1},s'_k)\in R'$存在$(s_{k-1},s_k)\in R$使得$\mathrm{Tr}_{n-k}(s_k) \leftrightarrow_{\overline{V}} \mathrm{Tr}_{n-k}(s'_k)$。因此，由归纳假设可知$\mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s_{k-1})) \equiv \mathscr{F}_V(\mathrm{Tr}_{n-k+1}(s'_{k-1}))$。 □

此外，对于初始结构$\mathscr{M}$上的状态s和s'，若$(\mathscr{M},s)$是定义在V上的根为s'深度为n的计算树的特征公式，则s和s'至少属于$\mathscr{B}_n$，即：s和s'能想互模拟至少到第n层深度。

引理 5.3. 令$V\subseteq\mathscr{A}$、$\mathscr{M}=(S,R,L,s_0)$、$\mathscr{M}'=(S',R',L',s'_0)$、$s\in S$、$s'\in S'$且$n\geq 0$，则：

(i) $(\mathscr{M},s)\models\mathscr{F}_V(Tr_n(s))$；

(ii) 若$(\mathscr{M},s)\models\mathscr{F}_V(Tr_n(s'))$，则$Tr_n(s)\leftrightarrow_{\overline{V}} Tr_n(s')$。

证明. (i) **基始**（$n=0$）：从树的特征公式定义可知$\mathscr{F}_V(\mathrm{Tr}_0(s))$是显然的。

归纳步（$n>0$）：假设对任意的$k\geq 0$，$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_k(s))$，下面证明$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_{k+1}(s))$，即：

$$(\mathscr{M},s)\models\left(\bigwedge_{(s,s')\in R}\mathrm{EX}T(s')\right)\wedge\mathrm{AX}\left(\bigvee_{(s,s')\in R}T(s')\right)\wedge\mathscr{F}_V(\mathrm{Tr}_0(s)).$$

其中$T(s')=\mathscr{F}_V(\mathrm{Tr}_k(s'))$。由基始可知$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_0(s))$。由归纳假设可知，对任意的$(s,s')\in R$有$(\mathscr{M},s')\models\mathscr{F}_V(\mathrm{Tr}_k(s'))$。因此有$(\mathscr{M},s)\models\mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_k(s')$，从而$(\mathscr{M},s)\models\bigwedge_{(s,s')\in R}\mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_k(s'))$。

同理，对任意的$(s,s')\in R$都有$(\mathscr{M},s')\models\bigvee_{(s,s')\in R}\mathscr{F}_V(\mathrm{Tr}_k(s'))$。因此，

$$(\mathscr{M},s)\models \mathrm{AX}\left(\bigvee_{(s,s')\in R}\mathscr{F}_V(\mathrm{Tr}_k(s'))\right)$$

从而可知对任意的$n\geq 0$，$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_n(s))$。

(ii) **基始**（$n=0$）：若$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_0(s'))$，则$L(s)-\overline{V}=L'(s')-\overline{V}$。因此$\mathrm{Tr}_0(s)\leftrightarrow_{\overline{V}}\mathrm{Tr}_0(s')$。

归纳步（$n>0$）：假定若$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_{n-1}(s'))$，则$\mathrm{Tr}_{n-1}(s)\leftrightarrow_{\overline{V}}\mathrm{Tr}_{n-1}(s')$。下面证明若$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_n(s'))$，则$\mathrm{Tr}_n(s)\leftrightarrow_{\overline{V}}\mathrm{Tr}_n(s')$。

(a) 由基始知$L(s)-\overline{V}=L'(s')-\overline{V}$；

(b) 因为$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_n(s'))$，所以$(\mathscr{M},s)\models\mathrm{AX}\left(\bigvee_{(s',s'_1)\in R}\mathscr{F}_V(\mathrm{Tr}_{n-1}(s'_1))\right)$。由此，对于任意的$(s,s_1)\in R$，存在$(s',s'_1)\in R'$使得$(\mathscr{M},s_1)\models\mathscr{F}_V(\mathrm{Tr}_{n-1}(s'_1))$。由归纳假设可知$\mathrm{Tr}_{n-1}(s_1)\leftrightarrow_{\overline{V}}\mathrm{Tr}_{n-1}(s'_1)$。即：$\forall(s,s_1)\in R$，$\exists(s',s'_1)\in R'$使得$\mathrm{Tr}_{n-1}(s_1)\leftrightarrow_{\overline{V}}\mathrm{Tr}_{n-1}(s'_1)$。

(c) 因为$(\mathscr{M},s)\models\mathscr{F}_V(\mathrm{Tr}_n(s'))$，所以$(\mathscr{M},s)\models\bigwedge_{(s',s'_1)\in R'}\mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_{n-1}(s'_1))$。由此，对于任意的$(s',s'_1)\in R'$，存在$(s,s_1)\in R$使得$(\mathscr{M},s_1)\models\mathscr{F}_V(\mathrm{Tr}_{n-1}(s'_1)$。由归纳假设可知$\mathrm{Tr}_{n-1}(s_1)\leftrightarrow_{\overline{V}}\mathrm{Tr}_{n-1}(s'_1)$。即：$\forall(s',s'_1)\in R'$，$\exists(s,s_1)\in R$使得$\mathrm{Tr}_{n-1}(s_1)\leftrightarrow_{\overline{V}}\mathrm{Tr}_{n-1}(s'_1)$。

□

5.2.3　初始κ-结构的特征公式

由V-互模拟的定义和命题 5.2可以自然地得到一个V-互模拟的补概念——V-可区分的。特别地，在命题 5.2中，若初始结构$\mathscr{M}$的两个状态s和s'不是$\overline{V}$-互模拟的（即：$s\not\leftrightarrow_{\overline{V}}s'$），则称$s$和$s'$是$V$-可区分的。且用$\mathrm{dis}_V(\mathscr{M},s,s',k)$表示状态$s$和$s'$在命题 5.2中所说的最小数$k$下是$V$-可区分的。正如下文所说，$V$-可区分这一概念是定义初始κ-结构的特征公式重要概念。

此外，对于给定的初始结构$\mathscr{M}$和原子命题集合V，若在$\mathscr{M}$中存在两个状态s和s'是V-可区分的，则称$\mathscr{M}$是V-可区分的。而对于一个V-可区分的初始结构$\mathscr{M}$，存在一个一个最小的数k使得对于该结构上的任意两个状态s和s'，若s和s'是可区分的，则$(s,s')\notin\mathscr{B}_k$。本文称这样的数为$\mathscr{M}$关于$V$的特征数，记为$ch(\mathscr{M},V)$，其定义如下：

$$ch(\mathscr{M},V)=\begin{cases}\max\{k\mid s,s'\in S\text{ 且}\mathrm{dis}_V(\mathscr{M},s,s',k)\}, & \mathscr{M}\text{ 是}V\text{-可区分的；}\\ \min\{k\mid \mathscr{B}_k=\mathscr{B}_{k+1},k\geq 0\}, & \text{否则。}\end{cases}$$

由$ch(\mathscr{M},V)$定义可知，对于任意的$\mathscr{M}$和V，$ch(\mathscr{M},V)$总是存在的，这体现在两个方面：（1）若$\mathscr{M}$是V-可区分的，存在两个状态s和s'是V-可区分的，由命题 5.2可知，存在一个数k使得$\mathrm{dis}_V(\mathscr{M},s,s',k)$成立；（2）若对于任意$k \geq 0$和$\mathscr{M}$上的两个状态$s$和$s'$都有$(s,s') \in \mathscr{B}_k$且$\mathscr{B}_k = \mathscr{B}_{k+1}$，则$ch(\mathscr{M},V) = 0$。

非形式化地说，特征数$c = ch(\mathscr{M},V)$将$\mathscr{M}$上的状态分为两大类：第一类中的任意两个状态s和s'是V-可区分的，且$(s,s') \notin \mathscr{B}_c$；第二类中状态都是$V$-不可区分的。这也在计算树的特征公式上：

引理 5.4. 令$V \subseteq \mathscr{A}$、$\mathscr{M} = (S,R,L,s_0)$、$k = ch(\mathscr{M},V)$且$s \in S$，则

(i) $(\mathscr{M},s) \models \mathscr{F}_V(Tr_k(s))$；

(ii) 对任意的$s' \in S$，$(\mathscr{M},s) \leftrightarrow_{\overline{V}} (\mathscr{M},s')$当且仅当$(\mathscr{M},s') \models \mathscr{F}_V(Tr_k(s))$。

证明. (i) 这由引理 5.3易知。

(ii) 令$\phi = \mathscr{F}_V(\mathrm{Tr}_k(s))$（$k$为$\mathscr{M}$关于$V$的特征数）。由(i)知$(\mathscr{M},s) \models \phi$，从而对任意的$s' \in S$，若$s \leftrightarrow_{\overline{V}} s'$，由定理 3.1和$\mathrm{IR}(\phi, \mathscr{A} - V)$知$(\mathscr{M},s') \models \phi$。

假定$(\mathscr{M},s') \models \phi$。若$s \nleftrightarrow_{\overline{V}} s'$，则$\mathrm{Tr}_k(s) \not\leftrightarrow_{\overline{V}} \mathrm{Tr}_k(s')$，因而由引理 5.3可知$(\mathscr{M},s') \not\models \phi$，这与假定矛盾。 □

由此，可定义初始K-结构的特征公式如下。

定义 5.2 (特征公式). 给定原子命题集合$V \subseteq \mathscr{A}he$和初始K-结构$\mathscr{K} = (\mathscr{M},s_0)$，其中$c = ch(\mathscr{M},V)$。对任意$\mathscr{M}$上得状态$s' \in S$，记$T(s') = \mathscr{F}_V(Tr_c(s'))$。则$\mathscr{K}$关于$V$的特征公式$\mathscr{F}_V(\mathscr{K})$为：

$$T(s_0) \wedge \bigwedge_{s \in S} \mathrm{AG}\left(T(s) \rightarrow \bigwedge_{(s,s') \in R} \mathrm{EX}T(s') \wedge \mathrm{AX}\left(\bigvee_{(s,s') \in R} T(s')\right)\right)$$

有时为了凸显出初始结构及其初始状态，也把特征公式写为$\mathscr{F}_V(\mathscr{M},s_0)$。显然，$\mathrm{IR}(\mathscr{F}_V(\mathscr{M},s_0),\overline{V})$。此外，在特征公式的定义中，使用了深度为$c$（即：特征数）的计算树的特征公式意在表明对任意$\mathscr{M}$上的两个状态$s$和$s'$，$s$和$s'$是$V$-可区分的当且仅当$\mathscr{F}_V(\mathrm{Tr}_c(s)) \neq \mathscr{F}_V(\mathrm{Tr}_c(s'))$。特别地，$T(s_0)$确保了初始K-结构的初始状态被CTL公式描述；其余部分表明了结构$\mathscr{M}$上状态之间的转换关系。下面的例子给出了计算特征公式的一般步骤：

例 5.1 (Continued from Example **??**). 考虑图 5.1中左边的初始K-结构$\mathscr{K}_2 = (\mathscr{M},s_0)$（其最初出现在图 **??**中）。左边的为$\mathscr{M}$上的四棵计算树：从左到右表示以$s_0$为根、深度分别

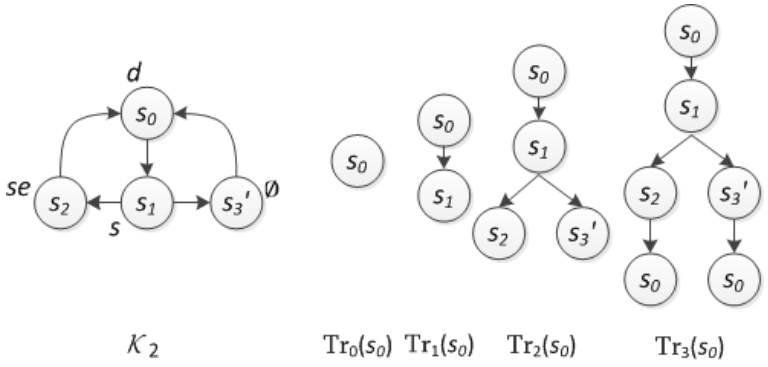

图 5.1: 左图为初始K-结构$\mathscr{K}_2$ (源于图 **??**)；右图：从左到右表示以s_0为根、深度分别为0、1、2和3的计算树（为简化图，计算树的标签没有给出，但是每个树节点的标签可从$\mathscr{K}_2$找到。）

为0、1、2和3的计算树（为简化图，计算树的标签没有给出，但是每个树节点的标签可从$\mathscr{K}_2$找到。）。令$V=\{d\}$，则$\overline{V}=\{s,se\}$。

因为$L(s_1)-\overline{V}=L(s_2)-\overline{V}$，所以有$\mathrm{Tr}_0(s_1)\leftrightarrow_{\overline{V}}\mathrm{Tr}_0(s_2)$。由于存在$(s_1,s_2)\in R$使得对任意的$(s_2,s')\in R$都有$L(s_2)-\overline{V}\neq L(s')-\overline{V}$，所以$\mathrm{Tr}_1(s_1)\not\leftrightarrow_{\overline{V}}\mathrm{Tr}_1(s_2)$。由此可知$s_1$和$s_2$是$V$-可区分的，且$\mathrm{dis}_V(\mathscr{M},s_1,s_2,1)$。

同样，我们可得到：$\mathrm{dis}_V(\mathscr{M},s_0,s_1,0)$、$\mathrm{dis}_V(\mathscr{M},s_1,s_3',1)$、$\mathrm{dis}_V(\mathscr{M},s_0,s_2,0)$和$\mathrm{dis}_V(\mathscr{M},s_0,s_3',0)$。此外，$s_2\leftrightarrow_{\overline{V}}s_3'$。因此可以计算$\mathscr{M}$关于$V$的特征数为：

$$ch(\mathscr{M},V)=\max\{k\mid s,s'\in S \text{ and } \mathrm{dis}_V(\mathscr{M},s,s',k)\}=1.$$

所以，可以由以下步骤计算$\mathscr{K}_2$关于V的特征公式：

$$\begin{aligned}
&\mathscr{F}_V(\mathrm{Tr}_0(s_0))=d, \qquad \mathscr{F}_V(\mathrm{Tr}_0(s_1))=\neg d,\\
&\mathscr{F}_V(\mathrm{Tr}_0(s_2))=\neg d, \qquad \mathscr{F}_V(\mathrm{Tr}_0(s_3'))=\neg d,\\
&\mathscr{F}_V(\mathrm{Tr}_1(s_0))=\mathrm{EX}\neg d\wedge\mathrm{AX}\neg d\wedge d\equiv\mathrm{AX}\neg d\wedge d,\\
&\mathscr{F}_V(\mathrm{Tr}_1(s_1))=\mathrm{EX}\neg d\wedge\mathrm{EX}\neg d\wedge\mathrm{AX}(\neg d\vee\neg d)\wedge\neg d\equiv\mathrm{AX}\neg d\wedge\neg d,\\
&\mathscr{F}_V(\mathrm{Tr}_1(s_2))=\mathrm{EX}d\wedge\mathrm{AX}d\wedge\neg d\equiv\mathrm{AX}d\wedge\neg d,\\
&\mathscr{F}_V(\mathrm{Tr}_1(s_3'))\equiv\mathscr{F}_V(\mathrm{Tr}_1(s_2)),\\
&\mathscr{F}_V(\mathscr{M},s_0)\equiv\mathrm{AX}\neg d\wedge d\wedge\\
&\qquad\mathrm{AG}(\mathrm{AX}\neg d\wedge d\rightarrow\mathrm{AX}(\mathrm{AX}\neg d\wedge\neg d))\wedge\\
&\qquad\mathrm{AG}(\mathrm{AX}\neg d\wedge\neg d\rightarrow\mathrm{AX}(\mathrm{AX}d\wedge\neg d))\wedge\\
&\qquad\mathrm{AG}(\mathrm{AX}d\wedge\neg d\rightarrow\mathrm{AX}(\mathrm{AX}\neg d\wedge d)).
\end{aligned}$$

下面的定理表示上述定义的特征公式确实描述了一个初始K-结构，此时对系统结构的操作就可转换为对其特征公式的操作，如下文将要讲的给定系统下的最弱充分条件计算。更直观地说，特征公式保持了给定初始K-结构在原子命题集合V上的所有特性，即：具有$\overline{V}$-互模拟的两个初始K-结构关于V的特征公式逻辑等价。

定理 5.1. 令$V \subseteq \mathscr{A}$、$\mathscr{M} = (S,R,L,s_0)$且$\mathscr{M}' = (S',R',L',s_0')$，则：

(i) $(\mathscr{M}',s_0') \models \mathscr{F}_V(\mathscr{M},s_0)$ 当且仅当$(\mathscr{M},s_0) \leftrightarrow_{\overline{V}} (\mathscr{M}',s_0')$；

(ii) 若$s_0 \leftrightarrow_{\overline{V}} s_0'$则$\mathscr{F}_V(\mathscr{M},s_0) \equiv \mathscr{F}_V(\mathscr{M}',s_0')$。

证明. (i) 令$\mathscr{F}_V(\mathscr{M},s_0)$为$(\mathscr{M},s_0)$关于$V$的特征公式。显然，$\mathrm{IR}(\mathscr{F}_V(\mathscr{M},s_0),\overline{V})$。为了证明上述结论成立，下面证明首先证明$(\mathscr{M},s_0) \models \mathscr{F}_V(\mathscr{M},s_0)$。

令$c = ch(\mathscr{M},V)$，由引理 5.3可知$(\mathscr{M},s_0) \models \mathscr{F}_V(\mathrm{Tr}_c(s_0))$。下面证明特征公式里的另一部分，即：$(\mathscr{M},s_0) \models \bigwedge_{s\in S} \mathrm{AG}\ G(\mathscr{M},s)$，其中

$$G(\mathscr{M},s) = \mathscr{F}_V(\mathrm{Tr}_c(s)) \rightarrow \left(\bigwedge_{(s,s_1)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_c(s_1)) \right) \wedge \mathrm{AX} \left(\bigvee_{(s,s_1)\in R} \mathscr{F}_V(\mathrm{Tr}_c(s_1)) \right).$$

为此，下面证明$(\mathscr{M},s_0) \models \mathrm{AG}\ G(\mathscr{M},s)$。考虑下面两种情况：

- 若$(\mathscr{M},s_0) \not\models \mathscr{F}_V(\mathrm{Tr}_c(s))$，显然$(\mathscr{M},s_0) \models G(\mathscr{M},s)$；
- 若$(\mathscr{M},s_0) \models \mathscr{F}_V(\mathrm{Tr}_c(s))$：

  $(\mathscr{M},s_0) \models \mathscr{F}_V(\mathrm{Tr}_c(s))$

  $\Rightarrow s_0 \leftrightarrow_{\overline{V}} s$ （引理 5.4）

  $\forall (s,s_1) \in R$：

  $(\mathscr{M},s_1) \models \mathscr{F}_V(\mathrm{Tr}_c(s_1))$ （$s_1 \leftrightarrow_{\overline{V}} s_1$）

  $\Rightarrow (\mathscr{M},s) \models \bigwedge_{(s,s_1)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_c(s_1))$

  $\Rightarrow (\mathscr{M},s_0) \models \bigwedge_{(s,s_1)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_c(s_1))$ （$\mathrm{IR}(\bigwedge_{(s,s_1)\in R} \mathrm{EX}\mathscr{F}_V(\mathrm{Tr}_c(s_1)),\overline{V})$, $s_0 \leftrightarrow_{\overline{V}} s$）

  $\forall (s,s_1) \in R$：

  $(\mathscr{M},s_1) \models \bigvee_{(s,s_2)\in R} \mathscr{F}_V(\mathrm{Tr}_c(s_2))$

  $\Rightarrow (\mathscr{M},s) \models \mathrm{AX}\left(\bigvee_{(s,s_2)\in R} \mathscr{F}_V(\mathrm{Tr}_c(s_2))\right)$

  $\Rightarrow (\mathscr{M},s_0) \models \mathrm{AX}\left(\bigvee_{(s,s_2)\in R} \mathscr{F}_V(\mathrm{Tr}_c(s_2))\right)$ （$\mathrm{IR}(\mathrm{AX}\left(\bigvee_{(s,s_2)\in R} \mathscr{F}_V(\mathrm{Tr}_c(s_2))\right),\overline{V})$, $s_0 \leftrightarrow_{\overline{V}} s$）

  $\Rightarrow (\mathscr{M},s_0) \models G(\mathscr{M},s)$。

对任意其他能从s_0可达的状态s'，都可以类似地证明$(\mathscr{M},s') \models G(\mathscr{M},s)$。因此，对任意的$s \in S$，$(\mathscr{M},s_0) \models \text{AG}\, G(\mathscr{M},s)$，从而$(\mathscr{M},s_0) \models \mathscr{F}_V(\mathscr{M},s_0)$。

下面从两个方面证明(i)成立：

($\Leftarrow$) 证明：若$s_0 \leftrightarrow_{\overline{V}} s'_0$，则$(\mathscr{M}',s'_0) \models \mathscr{F}_V(M,s_0)$。因为$(\mathscr{M},s_0) \models \mathscr{F}_V(\mathscr{M},s_0)$且$\text{IR}(\mathscr{F}_V(\mathscr{M},s_0),\overline{V})$，由定理 3.1可知$(\mathscr{M}',s'_0) \models \mathscr{F}_V(M,s_0)$。

($\Rightarrow$) 证明：若$(\mathscr{M}',s'_0) \models \mathscr{F}_V(M,s_0)$，则$s_0 \leftrightarrow_{\overline{V}} s'_0$。为此，下面证明对任意的$n \geq 0$，$Tr_n(s_0) \leftrightarrow_{\overline{V}} Tr_n(s'_0)$。

基始（$n=0$）：由特征公式的定义，显然$Tr_0(s_0) \equiv Tr_0(s'_0)$成立。

归纳步骤（$n>0$）：假定对任意的$k>0$都有$\text{Tr}_k(s_0) \leftrightarrow_{\overline{V}} \text{Tr}_k(s'_0)$，下面证明$\text{Tr}_{k+1}(s_0) \leftrightarrow_{\overline{V}} \text{Tr}_{k+1}(s'_0)$。令$(s_0,s_1),(s_1,s_2),\ldots,(s_{k-1},s_k) \in R$且$(s'_0,s'_1),(s'_1,s'_2),\ldots,(s'_{k-1},s'_k) \in R'$，即对于任意的$0 \leq i \leq k-1$，$s_{i+1}$（$s'_{i+1}$）是$s_i$ (s'_i)的直接后继状态。由归纳假设可知，只需证明$\text{Tr}_1(s_k) \leftrightarrow_{\overline{V}} \text{Tr}_1(s'_k)$。

(a) 由归纳假设可知$L(s_k)-\overline{V} = L'(s'_k)-\overline{V}$。

在讨论其他点时，首先考虑下面事实（**fact**）：

$(\mathscr{M}',s'_0) \models \mathscr{F}_V(\mathscr{M},s_0)$

$\Rightarrow \forall s' \in S'$，$\forall s \in S$，

$(\mathscr{M}',s') \models \mathscr{F}_V(\text{Tr}_c(s)) \rightarrow \left(\bigwedge_{(s,s_1)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_1))\right) \wedge \text{AX}\left(\bigvee_{(s,s_1)\in R} \mathscr{F}_V(\text{Tr}_c(s_1))\right)$

(I) $(\mathscr{M}',s'_0) \models \mathscr{F}_V(\text{Tr}_c(s_0)) \rightarrow \left(\bigwedge_{(s_0,s_1)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_1))\right) \wedge \text{AX}\left(\bigvee_{(s_0,s_1)\in R} \mathscr{F}_V(\text{Tr}_c(s_1))\right)$

(II) $(\mathscr{M}',s'_0) \models \mathscr{F}_V(\text{Tr}_c(s_0)))$ (已知)

(III) $(\mathscr{M}',s'_0) \models \left(\bigwedge_{(s_0,s_1)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_1))\right) \wedge \text{AX}\left(\bigvee_{(s_0,s_1)\in R} \mathscr{F}_V(\text{Tr}_c(s_1))\right)$ ((I),(II))

(b) 这里证明$\forall(s_k,s_{k+1}) \in R$，存在$(s'_k,s'_{k+1}) \in R'$使得$L(s_{k+1})-\overline{V} = L'(s'_{k+1})-\overline{V}$。

(1) $(\mathscr{M}',s'_0) \models \bigwedge_{(s_0,s_1)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_1))$ (III)

(2) $\forall(s_0,s_1) \in R$，$\exists(s'_0,s'_1) \in R'$ 使得$(\mathscr{M}',s'_1) \models \mathscr{F}_V(\text{Tr}_c(s_1))$ (1)

(3) $\text{Tr}_c(s_1) \leftrightarrow_{\overline{V}} \text{Tr}_c(s'_1)$ ((2), 引理 5.3)

(4) $L(s_1)-\overline{V} = L'(s'_1)-\overline{V}$ ((3), $c \geq 0$)

(5) $(\mathscr{M}',s'_1) \models \mathscr{F}_V(\text{Tr}_c(s_1)) \rightarrow \left(\bigwedge_{(s_1,s_2)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_2))\right) \wedge \text{AX}\left(\bigvee_{(s_1,s_2)\in R} \mathscr{F}_V(\text{Tr}_c(s_2))\right)$ **(fact)**

(6) $(\mathscr{M}',s'_1) \models \left(\bigwedge_{(s_1,s_2)\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_2))\right) \wedge \text{AX}\left(\bigvee_{(s_1,s_2)\in R} \mathscr{F}_V(\text{Tr}_c(s_2))\right)$ ((2), (5))

(7) ……

(8) $(\mathscr{M}',s'_k) \models \left(\bigwedge_{(s_k,s_{k+1})\in R} \text{EX}\mathscr{F}_V(\text{Tr}_c(s_{k+1}))\right) \wedge \text{AX}\left(\bigvee_{(s_k,s_{k+1})\in R} \mathscr{F}_V(\text{Tr}_c(s_{k+1}))\right)$ (与(6)类似)

(9) $\forall(s_k,s_{k+1}) \in R$，$\exists(s'_k,s'_{k+1}) \in R'$ 使得$(\mathscr{M}',s'_{k+1}) \models \mathscr{F}_V(\text{Tr}_c(s_{k+1}))$ (8)

(10) $\text{Tr}_c(s_{k+1}) \leftrightarrow_{\overline{V}} \text{Tr}_c(s'_{k+1})$ ((9), 引理 5.3)

(11) $L(s_{k+1})-\overline{V} = L'(s'_{k+1})-\overline{V}$ ((10), $c \geq 0$)

(c) 这里证明$\forall(s'_k,s'_{k+1})\in R'$，存在$(s_k,s_{k+1})\in R$使得$L(s_{k+1})-\overline{V}=L'(s'_{k+1})-\overline{V}$。

(1) $(\mathscr{M}',s'_k)\models \mathrm{AX}\left(\bigvee_{(s_k,s_{k+1})\in R}\mathscr{F}_V(\mathrm{Tr}_c(s_{k+1}))\right)$ (上面的(8))

(2) $\forall(s'_k,s'_{k+1})\in R'$，$\exists(s_k,s_{k+1})\in R$使得$(\mathscr{M}',s'_{k+1})\models\mathscr{F}_V(\mathrm{Tr}_c(s'_{k+1}))$ (1)

(3) $\mathrm{Tr}_c(s_{k+1})\leftrightarrow_{\overline{V}}\mathrm{Tr}_c(s'_{k+1})$ ((2), 引理 5.3)

(4) $L(s_{k+1})-\overline{V}=L'(s'_{k+1})-\overline{V}$ ((3), $c\geq 0$)

(ii) 由引理 5.2和5.4易知。

□

5.3 遗忘理论的封闭性

当给定的CTL公式的长度（字符的个数）为n，由小模型理论可知定义在状态个数为$k=n8^n$的状态空间$\mathscr{S}=\{s_1,s_2,\ldots,s_k\}$上的初始结构就能保证公式的可满足性[25]。对于其他拥有同样大小的状态空间上的任意初始K-结构，都能在$\mathscr{S}$状态空间上找到一个初始K-结构与之互模拟，且由定理 5.1可知他们有相同的特征公式。因此，只有有限个初始K-结构作为该公式的候选模型。因此下面结论成立。

引理 5.5. *给定CTL公式φ，下面等式成立：*

$$\varphi\equiv\bigvee_{(\mathscr{M},s_0)\in Mod(\varphi)}\mathscr{F}_{\mathscr{A}}(\mathscr{M},s_0).$$

证明. 令$(\mathscr{M}',s'_0)$为φ的模型。由定理 5.1可知$(\mathscr{M}',s'_0)\models\mathscr{F}_{\mathscr{A}}(\mathscr{M}',s'_0)$，则：

$$(\mathscr{M}',s'_0)\models\bigvee_{(\mathscr{M},s_0)\in Mod(\varphi)}\mathscr{F}_{\mathscr{A}}(\mathscr{M},s_0).$$

另一方面，假定$(\mathscr{M}',s'_0)$为$\bigvee_{(\mathscr{M},s_0)\in Mod(\varphi)}\mathscr{F}_{\mathscr{A}}(\mathscr{M},s_0)$的模型。则存在$(\mathscr{M},s_0)\in Mod(\varphi)$使得$(\mathscr{M}',s'_0)\models\mathscr{F}_{\mathscr{A}}(\mathscr{M},s_0)$。由定理 5.1可知$(\mathscr{M},s_0)\leftrightarrow_{\emptyset}(\mathscr{M}',s'_0)$，从而由定理 3.1可知$(\mathscr{M},s_0)$是$\varphi$的一个模型。 □

这一结论表明：任意的CTL公式都与其模型的特征公式的吸取逻辑等价。这对遗忘理论的封闭性提供了重要的理论支撑，也即是从公式里遗忘掉原子命题集合V中的元素只需找到与给定公式的模型V-互模拟的那些模型就能确定遗忘的结果。形式化地，对于给定的公式φ和原子命题集合V，从φ中遗忘掉V中的元素得到的结果为：

$$\bigvee_{\mathscr{K}\in\{\mathscr{K}'\mid\exists\mathscr{K}''\in Mod(\phi)\ \text{and}\ \mathscr{K}''\leftrightarrow_V\mathscr{K}'\}}\mathscr{F}_{\overline{V}}(\mathscr{K}).$$

在上述的遗忘理论的定义中说明了如果公式ψ的任意一个模型$\mathscr{K}$都能找到φ的一个模型$\mathscr{K}'$使得$\mathscr{K} \leftrightarrow_V \mathscr{K}'$，则称$\psi$为从$\varphi$中遗忘掉$V$中原子命题后得到的结果。为刻画S5逻辑下该概念的直观含义，Zhang等人提出了如下遗忘理论特性——这些特性被称为*遗忘理论公设*（forgetting postulates）[18]。给定CTL公式φ、$\varphi' = \mathrm{F}_{\mathrm{CTL}}(\varphi, V)$和原子命题集合$V \subseteq \mathscr{A}$和$\varphi' = \mathrm{F}_{\mathrm{CTL}}(\varphi, V)$，遗忘理论公设如下：

(**W**) 弱（Weakening）属性：$\varphi \models \varphi'$；

(**PP**) 正支持性（Positive Persistence）：对任意与V无关的公式η，若$\varphi \models \eta$则$\varphi' \models \eta$；

(**NP**) 负支持性（Negative Persistence）：对任意与V无关的公式η，若$\varphi \not\models \eta$则$\varphi' \not\models \eta$；

(**IR**) 无关性（Irrelevance）：$\mathrm{IR}(\varphi', V)$

直观地说，(**W**)和(**IR**)表明“遗忘”削弱了公式φ且得到的结果与V无关，(**PP**)和(**NP**)表明对任意与V无关的公式η，$\varphi \models \eta$当且仅当$\varphi' \models \eta$。总而言之，遗忘得到的结果能推出所有与V无关且能被φ推出的结果，且不能推出所有与V无关且不能被φ推出的结果。从数据库和安全的层面讲，遗忘相当于从已有的关系表中构建出一个视图，达到了隐私保护的作用。下面的定理表明CTL中的遗忘理论与上述公设也具有当且仅当的关系。

定理 5.2 (Representation Theorem)**.** *给定CTL公式φ和φ'，$V \subseteq \mathscr{A}$为原子命题的集合。下面的陈述是等价的：*

(i) $\varphi' \equiv \mathrm{F}_{\mathrm{CTL}}(\varphi, V)$,

(ii) $\varphi' \equiv \{\phi \mid \varphi \models \phi \ and \ IR(\phi, V)\}$,

*(iii) 若φ、φ'和V为(i)和(ii)中提到的符号，则公设(**W**)、(**PP**)、(**NP**)和(**IR**)成立.*

证明. $(i) \Leftrightarrow (ii)$. 为了证明这个结论，只需证明如下等式成立：

$$Mod(\mathrm{F}_{\mathrm{CTL}}(\varphi, V)) = Mod(\{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi, V)\}).$$

($\Rightarrow$) 对任意$\mathrm{F}_{\mathrm{CTL}}(\varphi, V)$的模型$\mathscr{K}'$
$\Rightarrow \exists \mathscr{K}$使得$\mathscr{K} \models \varphi$且$\mathscr{K} \leftrightarrow_V \mathscr{K}'$ (定义 3.2)
$\Rightarrow \forall \phi$，若$\varphi \models \phi$且$\mathrm{IR}(\phi, V)$则$\mathscr{K}' \models \phi$ (定理 3.1)
$\Rightarrow \mathscr{K}' \models \{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi, V)\}$

($\Leftarrow$) 因为$\mathrm{IR}(\mathrm{F}_{\mathrm{CTL}}(\varphi,V),V)$且$\varphi \models \mathrm{F}_{\mathrm{CTL}}(\varphi,V)$，由定义 3.2可知$\{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi,V)\} \models \mathrm{F}_{\mathrm{CTL}}(\varphi,V)$。

$(ii) \Rightarrow (iii)$.令$A = \{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi,V)\}$。首先，由于对任意的$\phi' \in A$都有$\varphi \models \phi'$，所以$\varphi \models \varphi'$。其次，对任意的公式$\phi$，若$\mathrm{IR}(\phi,V)$且$\varphi \models \phi$则$\phi \in A$，因此$\varphi' \models \phi$. 第三，对任意的公式$\phi$，若$\mathrm{IR}(\phi,V)$且$\varphi \not\models \phi$则$\phi \notin A$。因此$\varphi' \not\models \phi$。最后，因为对任意的$\phi' \in A$都有$\mathrm{IR}(\varphi',V)$ ，所以$\mathrm{IR}(\phi',V)$。

$(iii) \Rightarrow (ii)$.一方面，由(**PP**) 和(**NP**)可知，对任意的公式ϕ'且$\mathrm{IR}(\phi',V)$，$\varphi \models \phi'$当且仅当$\varphi' \models \phi'$。所以对任意的$\phi' \in \{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi,V)\}$都有$\varphi' \models \phi'$，因而$\varphi' \models \{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi,V)\}$。另一方面，由(**W**) 和(**IR**)可知$\{\phi \mid \varphi \models \phi, \mathrm{IR}(\phi,V)\} \models \varphi'$。因此，$\varphi' \equiv \{\phi \mid \varphi \models \phi \text{ and } \mathrm{IR}(\phi,V)\}$。 □

5.4 基于模型的遗忘理论计算方法

5.5 本章小结

本章针对差分隐私数据收集中多维数据处理的隐私脆弱性和有效性问题，为了权衡隐私泄露与数据质量损失，利用信息论的方法提出了有序随机响应扰动(ORRP)方案。首先，对于元组的多维属性使用分治策略思想分解元组属性，构建本地扰动的独立并联信道模型。其次，针对单属性分量的隐私保护问题，基于信息论的度量方法形式化数据质量损失约束前提下最小化隐私信息泄露的最优化模型，用于计算最优概率密度函数(PDF)。然后，以B-A为基本构建模块设计ORRP，利用上述PDF实现有序随机响应，并给出算法描述。最后，给出理论分析和真实数据集上的实验结果。

第六章　μ-演算中的遗忘理论

本章探索μ-演算中的遗忘理论。μ-演算是描述转换系统性质重要逻辑语言，其具有表达能力强的优点：μ-演算是一种表达能力与*S2S*[1]相同的逻辑语言，*LTL*（线性时序逻辑，*linear temporal logic*）、*CLT*和*CTL**能表达的属性都能用μ-演算来表示。

已有研究表明μ-演算具有均匀插值性质，这体现了μ-演算下的遗忘理论研究本质上与*CTL*下的不同。本章首先给出μ-演算下的遗忘理论的定义。其次，表明μ-演算下的遗忘理论是封闭的，这是其与*CTL*下的遗忘理论的最大的不同。最后，模型检测问题作为形式化验证的重要方法，本章给出μ-演算下遗忘理论的模型检测和推理问题的复杂性结果。

6.1　引言

然而，尽管μ-演算下存在均匀插值这一性质，但是有两个方面的不足：首先，现有研究对μ-演算的均匀插值没有直观的表现，也即是对其基本性质缺乏更加形象的探讨；其次，对其应用讳莫如深。

本章就上述提到的两个问题进行深入的研究。本章通过研究μ-演算下的遗忘理论性质的角度探索均匀插值的一般属性，

近年来，私有敏感信息泄露问题引起了社会和学术研究领域的广泛关注，正在成为大数据时代的一个主要挑战。如医疗数据、在线社交活动、基于位置的服务等网络应用中对个人数据的使用，使得个人的隐私遭受到了潜在的风险，由此产生了用户隐私泄露问题。隐私泄露逐渐成为数据收集、发布、分析、感知等隐私计算[?]任务中迫切需要解决的问题，技术层面上亟需有效的隐私保护模型与算法。围绕隐私保护的核心任务，学术研究已提出诸多的隐私保护模型及解决方案。其中，差分隐私[? ? ?]是广泛被接受的隐私保护模型。为了克服基本假设中存在可信实体的局限性，本地模型的差分隐私[? ?](Local Differential Privacy，LDP)被提出，并主要应用于解决数据收集阶段的隐私保护问题。在差分隐私的本地模型中，每一个用户独立的扰动自己的原始数据，然后报告扰动后的数据给数据聚合者(收集者)。由于本地模型的显著特性，一经提出就受到学术研究和产业应用的关注。学术界围绕本地模型的应用，先后提出诸如RAPPOR[? ?]、*k*-RR[?]、OUE[?]等众多著名先进的隐私机制。产业界如Google Chrome 浏览器[?]、Apple公司操作系统[?]等将其应用于隐私保护数据收集、分析场景。纵观研究工作，数据聚合者通常是半诚实的敌手模型，隐私性与数据质量依然是核心

[1]无限完全二叉树下的一元二阶理论（monadic second order theory of the infinite complete binary tree），简称为S2S。

的关注问题，隐私保护难以实现完美无泄露，相对的寻找隐私保护策略均衡成为较为理想的权衡折中解决方案。

实际的应用中，随机化响应[?]技术是有效实现LDP的方法[????]，其已成为LDP方案设计的基本构建模块。本质上，随机化响应是从原始数据到扰动输出数据的一个概率性映射。基于此，隐私机制的随机性与隐私保护的隐私和数据质量密切相关，这就是权衡隐私与效用课题的研究内容。目前，这仍然是差分隐私保护中学术研究的重点。在差分隐私本地模型的数据收集应用中，数据聚合者收集、存储、分析用户报告的扰动数据[?]，扰动后的数据与原始数据之间的关联决定了隐私保护的隐私性与数据的可用性。为了解决权衡的问题，在寻找有效的折中方案过程中，隐私与数据质量的度量是基本的前提工作。当前，隐私预算参数ε是一个量化差分隐私不可区分等级的事实标准。但是，这个度量是分布独立的，其存在着一些不足之处。例如，一个确定性的隐私协议$Q(x) = x \bmod 2$提供$\varepsilon = \infty$的隐私保障，但是该隐私协议仍然可以阻止部分的隐私泄露[?]。除了上面提到的，这样的隐私度量无法在等价的ε-隐私机制集合中区分那个隐私机制的性能更好，因为集合中的隐私机制都提供相同的ε-不可区分等级。受这些问题的激励，度量也亟需新的评价方法。

针对上述问题，从隐私信息流的角度，基于信息论的方法可以得到有效的解决[?]。首先，上述有关LDP机制的数据处理过程，可以被建模为一个原始数据与扰动数据之间的噪声信道模型[??](参见**??**节内容)。然后，利用熵与互信息量定义隐私泄露度量，且已在诸多研究工作中得到了应用[????]。重要的，信息论的模型中考虑了数据分布和隐私机制对隐私泄露的影响，互信息隐私测量扰动数据包含原始数据的信息量，它捕捉住了隐私攻击者有关数据分布的先验知识。此外，隐私保护系统中仅有两方的参与者[?]，用户本地执行隐私协议旨在减少隐私泄露，其类似于隐私防护者。相似的，聚合者试图最大化隐私泄露，以至于推断用户的个人信息，类似于隐私攻击者。鉴于上述分析，本章中关注的问题演变为了有关隐私的攻防对抗问题。自然的，以博弈均衡的思想解决这个问题不失为一个理想的选择。现有存在的工作中，二人零和对策博弈[????]、斯坦伯格博弈[?]、贝叶斯博弈[?]等在差分隐私框架下都有一定的应用。重要的，从量化信息流的角度构建的信息泄露博弈[??]、量化信息流博弈[?]是有效的隐私分析方法。

鉴于上述的分析，本章中考虑在理性的框架下使用信息论的方法解决隐私与效用的均衡问题，通过分析隐私保护者与攻击者的隐私目标，首先将其形式化表述为隐私的极大极小问题。然后，基于差分隐私通信模型(**??**节)，提出隐私保护的攻防博弈模型，也即是一个二人的零和博弈模型。进一步，提出一个交替最优化算法计算提出的攻防博弈的鞍点，利用鞍点策略实现差分隐私的均衡优化。理论上的均衡分析和实验结果表明，提出的均衡思想是一种稳定的状态，可用于预测评估隐私泄露风险。本章的主要贡献可以总结如下：

(1) 通过使用信息论的方法量化隐私攻击者的信息增益，提出了隐私保护的攻防博弈模型(PPAD)，用于分析用户和聚合者的理性策略行为。

(2) 在隐私与效用的原则下，分析隐私防护者与攻击者的隐私目标，形式化表述互信息隐私的极大极小问题，构建二人零和对策博弈求解形式化表述的极大极小问题，并利用交替最优响应策略，设计交替最优的策略优化选择算法。

(3) 对于等价的ε-隐私机制，提出一种有效的比较分析方法，并进一步验证了互信息隐私泄露在最差情况下可以达到隐私泄露的上界，为隐私泄露风险评估提供了量化分析的方法。

本章其余部分组织如下：首先，第8.2节阐述本章的系统模型、敌手模型，提出研究问题。其次，第8.3节提出隐私保护的攻防博弈模型(PPAD)，并给出均衡分析。进一步，第8.4节介绍均衡求解的策略优化选择算法。最后，第8.5节给出实验与分析，并在第8.6节总结本章的研究工作。

6.2　系统模型与问题提出

6.3　本章小结

本章针对差分隐私数据收集应用中存在的策略型攻击问题，利用信息论、博弈均衡理论研究了隐私防护者与隐私攻击者的理性策略选择，提出了隐私保护的攻防博弈(PPAD)模型，以实现隐私与数据效用均衡。首先，基于信息论度量方法分析差分隐私保护系统中隐私保护者和攻击者的隐私目标，形式化表述为互信息隐私的极大极小问题。其次，针对上述提出的问题，考虑策略型的隐私攻击者和防护者，提出隐私保护的攻防博弈模型，并具体为二人的零和博弈模型。随后，给出博弈的凹凸性以及均衡分析。进一步，为了求解博弈模型鞍点，设计了策略优化选择算法。最后，通过实验阐述了所提出的方案可以用于比较等价的隐私机制，并阐述了隐私量化是最坏情况下的隐私泄露，也即是，隐私防护者的最大隐私泄露。

第七章　遗忘理论的应用

本章针对差分隐私存在策略型攻击问题，基于差分隐私通信模型，提出隐私保护的攻防博弈模型，以实现隐私保护的隐私与数据效用均衡。首先，定义差分隐私保护系统中隐私保护者与攻击者(敌手)的隐私目标，并将其表述为隐私泄露的极大极小问题。针对该问题，以隐私度量为效用函数，构建两方零和对策博弈模型，并基于极大极小定理、凹凸博弈给出相应的博弈均衡分析。理论分析表明鞍点的存在，并进一步给出鞍点的内涵。其次，对于等价的ε-隐私机制，提出等价类隐私机制可比较的方法，解决ε-隐私度量存在的不足。最后，基于交替最优响应设计鞍点计算的策略优化选择算法。理论分析及实验结果表明提出的方法可辅助隐私保护者评估隐私泄露风险。

7.1　引言

近年来，私有敏感信息泄露问题引起了社会和学术研究领域的广泛关注，正在成为大数据时代的一个主要挑战。如医疗数据、在线社交活动、基于位置的服务等网络应用中对个人数据的使用，使得个人的隐私遭受到了潜在的风险，由此产生了用户隐私泄露问题。隐私泄露逐渐成为数据收集、发布、分析、感知等隐私计算[?]任务中迫切需要解决的问题，技术层面上亟需有效的隐私保护模型与算法。围绕隐私保护的核心任务，学术研究已提出诸多的隐私保护模型及解决方案。其中，差分隐私[???]是广泛被接受的隐私保护模型。为了克服基本假设中存在可信实体的局限性，本地模型的差分隐私[??](Local Differential Privacy，LDP)被提出，并主要应用于解决数据收集阶段的隐私保护问题。在差分隐私的本地模型中，每一个用户独立的扰动自己的原始数据，然后报告扰动后的数据给数据聚合者(收集者)。由于本地模型的显著特性，一经提出就受到学术研究和产业应用的关注。学术界围绕本地模型的应用，先后提出诸如RAPPOR[??]、k-RR[?]、OUE[?]等众多著名先进的隐私机制。产业界如Google Chrome 浏览器[?]、Apple公司操作系统[?]等将其应用于隐私保护数据收集、分析场景。纵观研究工作，数据聚合者通常是半诚实的敌手模型，隐私性与数据质量依然是核心的关注问题，隐私保护难以实现完美无泄露，相对的寻找隐私保护策略均衡成为较为理想的权衡折中解决方案。

实际的应用中，随机化响应[?]技术是有效实现LDP的方法[????]，其已成为LDP方案设计的基本构建模块。本质上，随机化响应是从原始数据到扰动输出数据的一个概率性映射。基于此，隐私机制的随机性与隐私保护的隐私和数据质量密切相关，这就是权衡隐私与效用课题的研究内容。目前，这仍然是差分隐私保护中学术研究的重点。在差分隐私本地模型的数据收集应用中，数据聚合者收集、存储、分析用户报告的扰

动数据[?]，扰动后的数据与原始数据之间的关联决定了隐私保护的隐私性与数据的可用性。为了解决权衡的问题，在寻找有效的折中方案过程中，隐私与数据质量的度量是基本的前提工作。当前，隐私预算参数ε是一个量化差分隐私不可区分等级的事实标准。但是，这个度量是分布独立的，其存在着一些不足之处。例如，一个确定性的隐私协议$Q(x) = x \bmod 2$提供$\varepsilon = \infty$的隐私保障，但是该隐私协议仍然可以阻止部分的隐私泄露[?]。除了上面提到的，这样的隐私度量无法在等价的ε-隐私机制集合中区分那个隐私机制的性能更好，因为集合中的隐私机制都提供相同的ε-不可区分等级。受这些问题的激励，度量也亟需新的评价方法。

针对上述问题，从隐私信息流的角度，基于信息论的方法可以得到有效的解决[?]。首先，上述有关LDP机制的数据处理过程，可以被建模为一个原始数据与扰动数据之间的噪声信道模型[??](参见**??**节内容)。然后，利用熵与互信息量定义隐私泄露度量，且已在诸多研究工作中得到了应用[????]。重要的，信息论的模型中考虑了数据分布和隐私机制对隐私泄露的影响，互信息隐私测量扰动数据包含原始数据的信息量，它捕捉住了隐私攻击者有关数据分布的先验知识。此外，隐私保护系统中仅有两方的参与者[?]，用户本地执行隐私协议旨在减少隐私泄露，其类似于隐私防护者。相似的，聚合者试图最大化隐私泄露，以至于推断用户的个人信息，类似于隐私攻击者。鉴于上述分析，本章中关注的问题演变为了有关隐私的攻防对抗问题。自然的，以博弈均衡的思想解决这个问题不失为一个理想的选择。现有存在的工作中，二人零和对策博弈[????]、斯坦伯格博弈[?]、贝叶斯博弈[?]等在差分隐私框架下都有一定的应用。重要的，从量化信息流的角度构建的信息泄露博弈[??]、量化信息流博弈[?]是有效的隐私分析方法。

鉴于上述的分析，本章中考虑在理性的框架下使用信息论的方法解决隐私与效用的均衡问题，通过分析隐私保护者与攻击者的隐私目标，首先将其形式化表述为隐私的极大极小问题。然后，基于差分隐私通信模型(**??**节)，提出隐私保护的攻防博弈模型，也即是一个二人的零和博弈模型。进一步，提出一个交替最优化算法计算提出的攻防博弈的鞍点，利用鞍点策略实现差分隐私的均衡优化。理论上的均衡分析和实验结果表明，提出的均衡思想是一种稳定的状态，可用于预测评估隐私泄露风险。本章的主要贡献可以总结如下：

(1) 通过使用信息论的方法量化隐私攻击者的信息增益，提出了隐私保护的攻防博弈模型(PPAD)，用于分析用户和聚合者的理性策略行为。

(2) 在隐私与效用的原则下，分析隐私防护者与攻击者的隐私目标，形式化表述互信息隐私的极大极小问题，构建二人零和对策博弈求解形式化表述的极大极小问题，并利用交替最优响应策略，设计交替最优的策略优化选择算法。

(3) 对于等价的ε-隐私机制，提出一种有效的比较分析方法，并进一步验证了互信息隐私泄露在最差情况下可以达到隐私泄露的上界，为隐私泄露风险评估提供了量化

分析的方法。

本章其余部分组织如下：首先，第8.2节阐述本章的系统模型、敌手模型，提出研究问题。其次，第8.3节提出隐私保护的攻防博弈模型(PPAD)，并给出均衡分析。进一步，第8.4节介绍均衡求解的策略优化选择算法。最后，第8.5节给出实验与分析，并在第8.6节总结本章的研究工作。

7.2 最强必要条件和最弱充分条件

这部分介绍如何使用遗忘理论计算最强必要条件和最弱充分条件。直观地说，最强必要条件指最一般的结果（the most general consequence），最弱充分条件指最特殊的诱因（the most specific abduction）。下面给出其形式化定义，本章所说的公式指的是μ-句子或CTL公式。

定义 7.1 (充分和必要条件). 给定两个公式ϕ和ψ，$V \subseteq Var(\phi)$，$q \in Var(\phi) - V$ 和$Var(\psi) \subseteq V$。

- 若$\phi \models q \to \psi$，则称ψ是q在V和ϕ上的必要条件（necessary condition，NC）；
- 若$\phi \models \psi \to q$，则称ψ是q在V和ϕ上的充分条件（sufficient condition，SC）；
- 若ψ是q在V和ϕ上的必要条件，且对于任意的q在V和ϕ上的必要条件ψ'都有$\phi \models \psi \to \psi'$，则称$\psi$是$q$在$V$和$\phi$上的最强必要条件（strongest necessary condition，SNC）；
- 若ψ是q在V和ϕ上的充分条件，且对于任意的q在V和ϕ上的充分条件ψ'都有$\phi \models \psi' \to \psi$，则称$\psi$是$q$在$V$和$\phi$上的最弱充分条件（weakest sufficient condition，WSC）；

从上述定义可以看出，SNC（WSC）是q在V和ϕ上的NC（SC）中最强（最弱）的一个，即：对任意的（或SC）ψ'，$\phi \models \text{SNC} \to \psi'$（$\phi \models \psi' \to \text{WSC}$）。此外，如果公式$\psi$和$\psi'$都是$q$在$V$和$\phi$上的SNC（WSC），则$\psi \equiv \psi'$。下面的命题表明SNC和WSC是一对对偶概念。

命题 7.1 (对偶性). 令V、q、φ和ψ为定义 *7.1*出现的符号。则ψ是q在V和ϕ上的*SNC*（*WSC*）当且仅当$\neg\psi$是$\neg q$在V和ϕ上的*WSC*（*SNC*）。

证明. （i）假设ψ是q在V和ϕ上的SNC。则$\varphi \models q \to \psi$，因而$\varphi \models \neg\psi \to \neg q$，即$\neg\psi$是$\neg q$ 在V 和ϕ上的SC. 设ψ' 是$\neg q$ 在V 和ϕ 上的SC：$\varphi \models \psi' \to \neg q$。则$\varphi \models q \to \neg\psi'$，即$\neg\psi'$是$q$ 在V 和ϕ 上NC。因此，由假设可知$\varphi \models \psi \to \neg\psi'$，所以$\varphi \models \psi' \to \neg\psi$。这证明了$\neg\psi$是$\neg q$ 在V 和ϕ上的WSC。可以类似地证明另一部分。

（ii）WSC的情形可以类似SNC的情形给出证明。 □

在定义 7.1中将q替换为任意的公式α，$V \subseteq Var(\alpha) \cup Var(\phi)$，则定义 7.1被推广到任意公式的最强必要条件和最弱充分条件的定义。下面的命题表示了原子命题的充分（必要）条件与公式的充分（必要）条件之间的关系：通过计算原子命题的充分（必要）条件来计算公式的充分（必要）条件。

命题 7.2. *给定公式Γ和α，$V \subseteq Var(\alpha) \cup Var(\Gamma)$，$q$是不出现在$\Gamma$和$\alpha$中的原子命题。集合$V$上的公式$\varphi$是$\alpha$在$V$和$\Gamma$上的SNC（WSC）当且仅当$\varphi$是$q$在$V$和$\Gamma'$上的SNC（WSC），其中$\Gamma' = \Gamma \cup \{q \leftrightarrow \alpha\}$。*

证明. 这里给出SNC部分的证明，WSC部分的证明与其类似。

对于任意的公式β，记$SNC(\varphi,\beta,V,\Gamma)$为“$\varphi$是$\beta$在$V$和$\Gamma$上的SNC”，$NC(\varphi,\beta,V,\Gamma)$为“$\varphi$是$\beta$在$V$和$\Gamma$上的NC”。

($\Rightarrow$) 证明“若$SNC(\varphi,\alpha,V,\Gamma)$，则$SNC(\varphi,q,V,\Gamma')$”。由$SNC(\varphi,\alpha,V,\Gamma)$和$\alpha \equiv q$可知$\Gamma' \models q \rightarrow \varphi$，即：$\varphi$是$q$在$V$和$\Gamma'$上的NC。假设$\varphi'$是$q$在$V$和$\Gamma'$上的任意NC，由于$\alpha \equiv q$和$IR(\alpha \rightarrow \varphi', \{q\})$，因此，$\mathrm{F}_{\mathrm{CTL}}(\Gamma', q) \models \alpha \rightarrow \varphi'$。由引理3.1可知$\Gamma \models \alpha \rightarrow \varphi'$，即：$NC(\varphi',\alpha,V,\Gamma)$。

($\Leftarrow$) 证明“若$SNC(\varphi,q,V,\Gamma')$，则$SNC(\varphi,\alpha,V,\Gamma)$”。由$SNC(\varphi,q,V,\Gamma')$、$IR(\alpha \rightarrow \varphi, \{q\})$和(**PP**) 可知$\mathrm{F}_{\mathrm{CTL}}(\Gamma', \{q\}) \models \alpha \rightarrow \varphi$，又由引理3.1可知$\Gamma \models \alpha \rightarrow \varphi$，即：$NC(\varphi,\alpha,V,\Gamma)$。设$\varphi'$是$\alpha$在$V$和$\Gamma$上的任意NC。由$\alpha \equiv q$和$\Gamma' = \Gamma \cup \{q \equiv \alpha\}$可知$\Gamma' \models q \rightarrow \varphi'$，即：$NC(\varphi',q,V,\Gamma')$。又因为$SNC(\varphi,q,V,\Gamma')$、$IR(\varphi \rightarrow \varphi', \{q\})$和(**PP**)，所以$\mathrm{F}_{\mathrm{CTL}}(\Gamma', \{q\}) \models \varphi \rightarrow \varphi'$。由引理3.1可知$\Gamma \models \varphi \rightarrow \varphi'$，因此$SNC(\varphi,\alpha,V,\Gamma)$成立。 □

为了对给定原子命题集合下的公式的最弱充分条件有个直观的认识，下面给出一个简单的例子。

例 7.1 (Continued from Example **??**). 本例来源于图 **??**中的初始结构$\mathscr{K}_2$。令$\psi = \mathrm{EX}(s \wedge (\mathrm{EX}se \vee \mathrm{EX}\neg d))$、$\varphi = \mathrm{EX}(s \wedge \mathrm{EX}\neg d)$、$\mathscr{A} = \{d,s,se\}$和$V = \{s,d\}$。下面证明$\varphi$是$\psi$在$V$和$\mathscr{K}_2$上的WSC：

(i) 由已知有$\varphi \models \psi$和$Var(\varphi) \subseteq V$。此外，$(\mathscr{M}, s_0) \models \varphi \wedge \psi$，因此$\mathscr{K}_2 \models \varphi \rightarrow \psi$，即：$\varphi$是$\psi$在$V$和$\mathscr{K}_2$上的SC;

(ii) 这里证明“对任意的ψ在V和$\mathscr{K}_2$上的SC φ'都有$\mathscr{K}_2 \models \varphi' \rightarrow \varphi$”。易知若$\mathscr{K}_2 \not\models \varphi'$，则$\mathscr{K}_2 \models \varphi' \rightarrow \varphi$。假设$\mathscr{K}_2 \models \varphi'$。由$\varphi'$是$\psi$在$V$和$\mathscr{K}_2$上的SC可知$\varphi' \models \mathrm{EX}(s \wedge \phi)$，其中$\phi$是使得$\phi \models \mathrm{EX}se \vee \mathrm{EX}\neg d$成立的公式。又$\mathrm{IR}(\varphi', \overline{V})$，所以$\phi \models \mathrm{EX}\neg d$。因此，$\varphi' \models \varphi$且$\mathscr{K}_2 \models \varphi' \rightarrow \varphi$。

如何使用遗忘理论计算SNC（WSC）是本章讨论的关键问题。下面首先给出其理论基础，然后再做直观的解释。

定理 7.1. 给定公式φ、原子命题的集合$V \subseteq Var(\varphi)$和原子命题$q \in Var(\varphi) - V$。

(i) $\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q, (Var(\varphi) \cup \{q\}) - V)$ 是q在V和φ上的*SNC*;

(ii) $\neg\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge \neg q, (Var(\varphi) \cup \{q\}) - V)$是$q$在$V$和$\varphi$上的*WSC*。

证明. (i) 令$\mathscr{F} = \mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q, (Var(\varphi) \cup \{q\}) - V)$。

“NC”部分：由遗忘理论的定义可知$\varphi \wedge q \models \mathscr{F}$。因此，$\varphi \models q \rightarrow \mathscr{F}$，即：$\mathscr{F}$ 是q在V 和φ上的NC。

“SNC”部分：假设ψ'为q在V和φ上的任意NC，即：$\varphi \models q \rightarrow \psi'$。由定理 3.1和$IR(\psi', (Var(\varphi) \cup \{q\}) - V)$可知，若$\varphi \wedge q \models \psi'$，则$\mathscr{F} \models \psi'$。由假设可知$\varphi \models q \rightarrow \psi'$，所以$\varphi \wedge \mathscr{F} \models \psi'$，因此$\varphi \models \mathscr{F} \rightarrow \psi'$。

由上面两部分可知，$\mathscr{F}$是q在V和φ上的SNC。

(ii) 令$\mathscr{F} = \neg\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge \neg q, (Var(\varphi) \cup \{q\}) - V)$。由命题 7.1可知，对任意的命题$q'$，$\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q', (Var(\varphi) \cup \{q'\}) - V)$是$q'$在$V$和$\varphi$上的SNC，当且仅当$\neg\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q', (Var(\varphi) \cup \{q'\}) - V)$是$\neg q'$在$V$和$\varphi$上的WSC。由(i)可知$\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q', (Var(\varphi) \cup \{q'\}) - V)$是$q'$在$V$和$\varphi$上的SNC，所以$\neg\mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q', (Var(\varphi) \cup \{q'\}) - V)$是$\neg q'$在$V$和$\varphi$上的WSC。令$q = \neg q'$，可得$\mathscr{F}$ 是q 在V 和φ上的WSC。 □

令$\mathscr{F} = \mathrm{F}_{\mathrm{CTL}}(\varphi \wedge q, (Var(\varphi) \cup \{q\}) - V)$。上面的定理可以直观地解释如下：由遗忘理论的定义可知$\varphi \wedge q \models \beta$，这说明$\mathscr{F}$ 是q 在V 和φ上的NC；对任意的与$(Var(\varphi) \cup \{q\}) - V$无关的公式$\psi$，若$\varphi \wedge q \models \psi$，则由定理 **??**可知$\beta \models \psi$。

由第五章可知，任意的有限的初始K-结构都能由一个CTL公式表示，所以由上面的定理自然地就能得到给定有限初始K-结构下的SNC和WSC。

推论 7.1. 令$\mathscr{K} = (\mathscr{M}, s)$为初始K-结构，其中$\mathscr{M} = (S, R, L, s_0)$ 为有限原子命题集合$\mathscr{A}$上的初始-*Kripke*结构，$V \subseteq \mathscr{A}$且$q \in V' = \mathscr{A} - V$。则：

(i) $\mathrm{F}_{\mathrm{CTL}}(\mathscr{F}_{\mathscr{A}}(\mathscr{K}) \wedge q, V')$是$q'$在$V$和$\mathscr{K}$上的*SNC*;

(ii) $\neg\mathrm{F}_{\mathrm{CTL}}(\mathscr{F}_{\mathscr{A}}(\mathscr{K}) \wedge \neg q, V')$是$q'$在$V$和$\mathscr{K}$上的*WSC*。

7.3 μ-演算下的知识更新

本小节介绍遗忘理论的另一个应用：知识更新（Knowledge update）。具体说来，本节将使用遗忘理论定义知识更新，使得用这种方式定义的知识更新满足下面由Katsuno和Mendelzon的基本条件：

- (U1) $\Gamma \diamond \phi \models \phi$;

- (U2) 若$\Gamma \models \phi$，则$\Gamma \diamond \phi \equiv \Gamma$；
- (U3) 若Γ和ϕ都是可满足的，则$\Gamma \diamond \phi$是可满足的；
- (U4) 若$\Gamma_1 \equiv \Gamma_2$且$\phi_1 \equiv \phi_2$，则$\Gamma_1 \diamond \phi_1 \equiv \Gamma_2 \diamond \phi_2$；
- (U5) $(\Gamma \diamond \phi) \wedge \psi \models \Gamma \diamond (\phi \wedge \psi)$；
- (U6) 若$\Gamma \diamond \phi \models \psi$且$\Gamma \diamond \psi \models \phi$，则$\Gamma \diamond \phi \equiv \Gamma \diamond \psi$；
- (U7) 若Γ有唯一一个模型，则$(\Gamma \diamond \phi) \wedge (\Gamma \diamond \psi) \models \Gamma \diamond (\phi \vee \psi)$；
- (U8) $(\Gamma_1 \vee \Gamma_2) \diamond \phi / (\Gamma_1 \diamond \phi) \vee (\Gamma_2 \diamond \phi)$。

其中，$\diamond$为知识更新操作，$\varphi \diamond \psi$表示用ψ更新φ得到的结果。

本小节假设所有的初始K-结构都是有限的，即：状态来源于有限的状态空间且$\mathscr{A}$为有限的原子命题的集合。下面定理显然成立：

定理 7.2. *给定μ-句子ϕ和原子命题的集合$V \subseteq \mathscr{A}$。存在一个μ-句子ψ使得：*

$$\mathscr{M} \models \psi \text{ 当且仅当存在} \mathscr{M}' \in Mod(\phi) \text{ 使得} \mathscr{M} \leftrightarrow_V \mathscr{M}'$$

其中$\mathscr{M}$和$\mathscr{M}'$都是有限的初始结构。

证明. 令$\psi = \mathrm{F}_\mu(\phi, V)$。由定理 **??**和遗忘理论的定义可知，对任意的$\mathscr{M} \models \psi$存在一个$\mathscr{M}' \models \phi$使得$\mathscr{M} \leftrightarrow_V \mathscr{M}'$，且对每一个$\mathscr{M}' \in Mod(\phi)$都有$\mathscr{M}' \models \psi$。此时，容易证明对任意的有限初始结构$\mathscr{M}$，若$\mathscr{M} \models \psi$，则存在一个$\mathscr{M}'$使得$\mathscr{M}' \models \phi$且$\mathscr{M} \leftrightarrow_V \mathscr{M}'$。

此外，对任意的$\mathscr{M}' \in Mod(\phi)$，由(**W**)可知存在$\mathscr{M}' \models \psi$。又$\mathscr{M} \leftrightarrow_V \mathscr{M}'$，所以由定理 **??**可知$\mathscr{M} \models \psi$。 □

定理 7.2表明模型结构被限制到有限初始结构下的μ-演算下遗忘理论也是封闭的。此外，由?? 可知，任意$\mathscr{A}$上的有限初始K-结构$\mathscr{K}$都能用一个CTL公式——特征公式$\mathscr{F}_{\mathscr{A}}(\mathscr{K})$来表示，此公式也是$\mu$-句子。

对于给给定的$\mathscr{A}$和$V_{min} \subseteq \mathscr{A}$，记$\varphi = \mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{K}), V_{min})$，其中$V_{min} \subseteq \mathscr{A}$是使得$\varphi$可满足的极小子集。此外，公式

$$\bigcup_{V_{min} \subseteq \mathscr{A}} Mod(\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{K}), V_{min}))$$

表示所有$\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{K}), V_{min})$的模型集合的并集。此时，可如下定义$\mu$-演算下的知识更新操作$V_{min}$：

定义 7.2. 给定μ-句子Γ和ϕ。知识更新操作$\diamond_\mu$定义如下：

$$Mod(\Gamma \diamond_\mu \phi) = \bigcup_{\mathscr{K} \in Mod(\Gamma)} \bigcup_{V_{min} \subseteq \mathscr{A}} Mod(\mathrm{F}_\mu(\mathscr{F}_\mathscr{A}(\mathscr{K}), V_{min}) \wedge \phi),$$

其中，$\mathscr{F}_\mathscr{A}(\mathscr{K})$是$\mathscr{K}$在$\mathscr{A}$上的特征公式，$V_{min} \subseteq \mathscr{A}$是使得$\mathrm{F}_\mu(\mathscr{F}_\mathscr{A}(\mathscr{K})$可满足的极小子集。

从直观上来说，$\Gamma \diamond_\mu \phi$表示通过极小化改变Γ的模型到ϕ的模型来更新Γ。换句话说，定义 7.2通过极小化改变Γ的每个模型，使得该模型能够满足ϕ来更新原有的知识Γ。从这个角度看，这样定义的知识更新是一种基于模型的知识更新方法。

此外，μ-演算下的知识更新也可以通过像命题逻辑里的那样来定义：令I，J_1和J_2为三个赋值，即：原子命题的集合；则J_1比J_2更接近I（记为：$J_1 \leq_{I,pam} J_2$）当且仅当$\mathrm{Diff}(I,J_1) \subseteq \mathrm{Diff}(I,J_2)$，其中$\mathrm{Diff}(X,Y) = \{p \in \mathscr{A} \mid X(p) \neq Y(p)\}$。那么命题逻辑里的知识更新——用$\psi$更新$\Gamma$，即为$\psi$的关于偏序关系$\leq_{I,pam}$的所有极小模型的集合（$I$是$\Gamma$的模型），即：

$$Mod(\Gamma \diamond_{pam} \psi) = \bigcup_{I \in Mod(\Gamma)} Min(Mod(\psi), \leq_{I,pam}).$$

其中，$Min(Mod(\psi), \leq_{I,pam})$是$\psi$的关于偏序关系$\leq_{I,pam}$的极小模型的集合。

类似地，这里定理有限初始结构之间关于另一个初始结构的偏序关系。

定义 7.3. 给定三个有限初始结构$\mathscr{M}$、$\mathscr{M}_1$和$\mathscr{M}_2$，$\mathscr{M}_1$比$\mathscr{M}_2$更接近$\mathscr{M}$（记为$\mathscr{M}_1 \leq_\mathscr{M} \mathscr{M}_2$）当且仅当对任意使得$\mathscr{M}_2 \leftrightarrow_{V_2} \mathscr{M}$成立的$V_2 \subseteq \mathscr{A}$都存在一个$V_1 \subseteq V_2$使得$\mathscr{M}_1 \leftrightarrow_{V_1} \mathscr{M}$。$\mathscr{M}_1 <_\mathscr{M} \mathscr{M}_2$当且仅当$\mathscr{M}_1 \leq_\mathscr{M} \mathscr{M}_2$且$\mathscr{M}_2 \not\leq_\mathscr{M} \mathscr{M}_1$。

给定有限初始结构的集合M和有限初始结构$\mathscr{M}$，用$Min(M, \leq_\mathscr{M})$表示M中关于偏序关系$\leq_\mathscr{M}$的极小有限初始结构的集合。则$\leq_\mathscr{M}$与知识更新操作$\diamond_\mu$有如下关系。

定理 7.3. 给定μ-句子Γ和ϕ，则：

$$Mod(\Gamma \diamond_\mu \phi) = \bigcup_{\mathscr{M} \in Mod(\Gamma)} Min(Mod(\phi), \leq_\mathscr{M}).$$

证明. 对每一个初始结构$\mathscr{M}' \in Mod(\Gamma \diamond_\mu \phi)$，这里证明存在一个$\mathscr{M} \in Mod(\Gamma)$使得$\mathscr{M}' \in Min(Mod(\phi), \leq_\mathscr{M})$。由定义 7.2可知，存在$\mathscr{M} \in Mod(\Gamma)$使得$\mathscr{M}' \in Mod(\mathrm{F}_\mu(\mathscr{F}_\mathscr{A}(\mathscr{M}), V_{min}) \wedge \phi)$。此外，存在一个特殊的$V' \subseteq \mathscr{A}$（即：$V' = V_{min}$）使得$\mathscr{M}' \leftrightarrow_{V'} \mathscr{M}$和$\mathscr{M}' \in Mod(\phi)$。因为$V'$是使得$\mathscr{M}' \leftrightarrow_{V'} \mathscr{M}$成立的极小子集，因此对任意使得$\mathscr{M}'' \leftrightarrow_{V_{min}} \mathscr{M}$成

立的ϕ的模型$\mathscr{M}''$，由遗忘理和特征公式论的定义可知$\mathscr{M}' \leq_{\mathscr{M}} \mathscr{M}''$。因此，$\mathscr{M}' \in Min(Mod(\phi), \leq_{\mathscr{M}})$。

对每一个初始结构$\mathscr{M}' \in \bigcup_{\mathscr{M}\in Mod(\Gamma)} Min(Mod(\phi), \leq_{\mathscr{M}})$，存在$\mathscr{M} \in Mod(\Gamma)$使得$\mathscr{M}' \in Min(Mod(\phi), \leq_{\mathscr{M}})$。设$V_{min}$是使得$\mathscr{M}' \leftrightarrow_{V_{min}} \mathscr{M}$成立的极小子集。根据$\leq_{\mathscr{M}}$的定义可知，不存在其他$\mathscr{M}'' \in Mod(\phi)$使得$\mathscr{M}'' \leftrightarrow_{V'} \mathscr{M}$ 且$V' \subset V_{min}$。因而$\mathscr{M}' \in Mod(\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_{min}) \wedge \phi)$，所以$\mathscr{M}' \in Mod(\Gamma \diamond_\mu \phi)$。 □

从定理 7.3可以看出，通过遗忘理论定义的知识更新操作与通过有限初始结构间的偏序关系定义的知识更新一致，且通过遗忘理论定义的知识更新操作满足Katsuno和Mendelzon提出的八条基本条件。

定理 7.4. *知识更新操作$\diamond_\mu$满足Katsuno和Mendelzon提出的基本条件(U1)-(U8)。*

证明. For (U1), we know that $Mod(\Gamma \diamond_\mu \phi) \subseteq Mod(\phi)$ by Theorem 7.3, hence $\Gamma \diamond_\mu \phi \models \phi$.

For (U2), we will prove $\Gamma \diamond_\mu \phi \models \Gamma$ at first. For each model $\mathscr{M}$ of $\Gamma \diamond_\mu \phi$, there is a $\mathscr{M}_1 \in Mod(\Gamma)$ and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. Then we have $V_{min} = \emptyset$ due to $\Gamma \models \phi$. Similarly, for each model $\mathscr{M}$ of Γ, there is a $\mathscr{M}_1 \in Mod(\Gamma \diamond_\mu \phi)$ and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. We have $V_{min} = \emptyset$ due to $\Gamma \models \phi$. Hence $\Gamma \models \Gamma \diamond_\mu \phi$.

It is easy to show that $\diamond_\mu$ satisfies (U3) and (U4). We now prove (U5). For each model $\mathscr{M}$ of $(\Gamma \diamond_\mu \phi) \wedge \psi$, there is a $\mathscr{M}_1 \in Mod(\Gamma)$ and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. Besides, we can see that $\mathscr{M} \models \phi \wedge \psi$. Therefore, we have $\mathscr{M} \models \Gamma \diamond_\mu (\phi \wedge \psi)$.

For (U6), we will prove $\Gamma \diamond_\mu \phi \models \Gamma \diamond_\mu \psi$, and the other direction can be proved in a similar way. For each model $\mathscr{M}$ of $\Gamma \diamond_\mu \phi$, $\mathscr{M}$ is also a model of ψ. There is a $\mathscr{M}_1 \in Mod(\Gamma)$ and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. Therefore $\mathscr{M}$ is a model of $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V_{min}) \wedge \psi$. This shows that $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V_{min}) \wedge \psi$ is consistent. Moreover, V_{min} is also the minimal set s.t. $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V_{min}) \wedge \psi$ is consistent. Otherwise, suppose that $V \subset V_{min}$ s.t. $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V) \wedge \psi$ is consistent as well. Then, $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V) \wedge \phi$ should also be consistent by $\Gamma \diamond_\mu \phi \models \psi$, which contradicts to the fact that V_{min} is the minimal set of atoms s.t. $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}_1), V_{min}) \wedge \phi$ is consistent. Hence, $\mathscr{M}$ is also a model of $\Gamma \diamond_\mu \psi$.

Now we prove (U7). Suppose that Γ has the unique model $\mathscr{M}$. For each $\mathscr{M}_1 \in Mod((\Gamma \diamond_\mu \phi) \wedge (\Gamma \diamond_\mu \psi))$ there exists V_1 and V_2 which are minimal s.t. $\mathscr{M} \leftrightarrow_{V_1} \mathscr{M}_1$ and $\mathscr{M} \leftrightarrow_{V_2} \mathscr{M}_1$, i.e., $\mathscr{M}_1$ is a model of both $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_1) \wedge \phi$ and $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_2) \wedge \psi$. Therefore $\mathscr{M}_1 \leftrightarrow_{V_1 \cap V_2} \mathscr{M}$. Thus, $\mathscr{M}_1$ is a model of $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_1 \cap V_2)$. Then we have $V_1 = V_2$, otherwise V_1 (or V_2) is not the minimal set. $\mathscr{M}_1$ is a model of $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_1) \wedge (\phi \vee \psi)$ as well. Moreover, V_1 is the minimal set s.t. $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_1) \wedge (\phi \vee \psi)$ is satisfiable. Otherwise, suppose that $V_3 \subset V_1$ s.t. $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_3) \wedge (\phi \vee \psi)$ is satisfiable. Then $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_3) \wedge \phi$ or $\mathrm{F}_\mu(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_3) \wedge \psi$

is satisfiable. Without loss of generality, suppose that $\mathrm{F}_{\mu}(\mathscr{F}_{\mathscr{A}}(\mathscr{M}), V_3) \wedge \phi$ is satisfiable, V_1 is not the minimal set, a contradiction. Therefore $\mathscr{M}_1$ is also a model of $\Gamma \diamond_{\mu} (\phi \vee \psi)$.

For (U8), we will prove $(\Gamma_1 \vee \Gamma_2) \diamond_{\mu} \phi \models (\Gamma_1 \diamond_{\mu} \phi) \vee (\Gamma_2 \diamond_{\mu} \phi)$ at first. For each $\mathscr{M} \in Mod((\Gamma_1 \vee \Gamma_2) \diamond_{\mu} \phi)$, there is a $\mathscr{M}_1 \in Mod(\Gamma_1)$ (or $\mathscr{M}_1 \in Mod(\Gamma_2)$) and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. Therefore, we have $\mathscr{M} \models (\Gamma_1 \diamond_{\mu} \phi) \vee (\Gamma_2 \diamond_{\mu} \phi)$. Similarly, for each $\mathscr{M} \in Mod((\Gamma_1 \diamond_{\mu} \phi) \vee (\Gamma_2 \diamond_{\mu} \phi))$, there is a $\mathscr{M}_1 \in Mod(\Gamma_1)$ (or $\mathscr{M}_1 \in Mod(\Gamma_2)$) and V_{min} s.t. $\mathscr{M} \leftrightarrow_{V_{min}} \mathscr{M}_1$. Hence, $\mathscr{M} \models (\Gamma_1 \vee \Gamma_2) \diamond_{\mu} \phi$. □

7.4 本章小结

本章针对差分隐私数据收集应用中存在的策略型攻击问题，利用信息论、博弈均衡理论研究了隐私防护者与隐私攻击者的理性策略选择，提出了隐私保护的攻防博弈(PPAD)模型，以实现隐私与数据效用均衡。首先，基于信息论度量方法分析差分隐私保护系统中隐私保护者和攻击者的隐私目标，形式化表述为互信息隐私的极大极小问题。其次，针对上述提出的问题，考虑策略型的隐私攻击者和防护者，提出隐私保护的攻防博弈模型，并具体为二人的零和博弈模型。随后，给出博弈的凹凸性以及均衡分析。进一步，为了求解博弈模型鞍点，设计了策略优化选择算法。最后，通过实验阐述了所提出的方案可以用于比较等价的隐私机制，并阐述了隐私量化是最坏情况下的隐私泄露，也即是，隐私防护者的最大隐私泄露。

第八章　差分隐私策略机制的均衡优化模型

本章针对差分隐私存在策略型攻击问题，基于差分隐私通信模型，提出隐私保护的攻防博弈模型，以实现隐私保护的隐私与数据效用均衡。首先，定义差分隐私保护系统中隐私保护者与攻击者(敌手)的隐私目标，并将其表述为隐私泄露的极大极小问题。针对该问题，以隐私度量为效用函数，构建两方零和对策博弈模型，并基于极大极小定理、凹凸博弈给出相应的博弈均衡分析。理论分析表明鞍点的存在，并进一步给出鞍点的内涵。其次，对于等价的ε-隐私机制，提出等价类隐私机制可比较的方法，解决ε-隐私度量存在的不足。最后，基于交替最优响应设计鞍点计算的策略优化选择算法。理论分析及实验结果表明提出的方法可辅助隐私保护者评估隐私泄露风险。

8.1　引言

近年来，私有敏感信息泄露问题引起了社会和学术研究领域的广泛关注，正在成为大数据时代的一个主要挑战。如医疗数据、在线社交活动、基于位置的服务等网络应用中对个人数据的使用，使得个人的隐私遭受到了潜在的风险，由此产生了用户隐私泄露问题。隐私泄露逐渐成为数据收集、发布、分析、感知等隐私计算[?]任务中迫切需要解决的问题，技术层面上亟需有效的隐私保护模型与算法。围绕隐私保护的核心任务，学术研究已提出诸多的隐私保护模型及解决方案。其中，差分隐私[???]是广泛被接受的隐私保护模型。为了克服基本假设中存在可信实体的局限性，本地模型的差分隐私[??](Local Differential Privacy，LDP)被提出，并主要应用于解决数据收集阶段的隐私保护问题。在差分隐私的本地模型中，每一个用户独立的扰动自己的原始数据，然后报告扰动后的数据给数据聚合者(收集者)。由于本地模型的显著特性，一经提出就受到学术研究和产业应用的关注。学术界围绕本地模型的应用，先后提出诸如RAPPOR[??]、k-RR[?]、OUE[?]等众多著名先进的隐私机制。产业界如Google Chrome 浏览器[?]、Apple公司操作系统[?]等将其应用于隐私保护数据收集、分析场景。纵观研究工作，数据聚合者通常是半诚实的敌手模型，隐私性与数据质量依然是核心的关注问题，隐私保护难以实现完美无泄露，相对的寻找隐私保护策略均衡成为较为理想的权衡折中解决方案。

实际的应用中，随机化响应[?]技术是有效实现LDP的方法[????]，其已成为LDP方案设计的基本构建模块。本质上，随机化响应是从原始数据到扰动输出数据的一个概率性映射。基于此，隐私机制的随机性与隐私保护的隐私和数据质量密切相关，这就是权衡隐私与效用课题的研究内容。目前，这仍然是差分隐私保护中学术研究的重点。在差分隐私本地模型的数据收集应用中，数据聚合者收集、存储、分析用户报告的扰

动数据[?]，扰动后的数据与原始数据之间的关联决定了隐私保护的隐私性与数据的可用性。为了解决权衡的问题，在寻找有效的折中方案过程中，隐私与数据质量的度量是基本的前提工作。当前，隐私预算参数ε是一个量化差分隐私不可区分等级的事实标准。但是，这个度量是分布独立的，其存在着一些不足之处。例如，一个确定性的隐私协议$Q(x) = x \bmod 2$提供$\varepsilon = \infty$的隐私保障，但是该隐私协议仍然可以阻止部分的隐私泄露[?]。除了上面提到的，这样的隐私度量无法在等价的ε-隐私机制集合中区分那个隐私机制的性能更好，因为集合中的隐私机制都提供相同的ε-不可区分等级。受这些问题的激励，度量也亟需新的评价方法。

针对上述问题，从隐私信息流的角度，基于信息论的方法可以得到有效的解决[?]。首先，上述有关LDP机制的数据处理过程，可以被建模为一个原始数据与扰动数据之间的噪声信道模型[??](参见**??**节内容)。然后，利用熵与互信息量定义隐私泄露度量，且已在诸多研究工作中得到了应用[????]。重要的，信息论的模型中考虑了数据分布和隐私机制对隐私泄露的影响，互信息隐私测量扰动数据包含原始数据的信息量，它捕捉住了隐私攻击者有关数据分布的先验知识。此外，隐私保护系统中仅有两方的参与者[?]，用户本地执行隐私协议旨在减少隐私泄露，其类似于隐私防护者。相似的，聚合者试图最大化隐私泄露，以至于推断用户的个人信息，类似于隐私攻击者。鉴于上述分析，本章中关注的问题演变为了有关隐私的攻防对抗问题。自然的，以博弈均衡的思想解决这个问题不失为一个理想的选择。现有存在的工作中，二人零和对策博弈[????]、斯坦伯格博弈[?]、贝叶斯博弈[?]等在差分隐私框架下都有一定的应用。重要的，从量化信息流的角度构建的信息泄露博弈[??]、量化信息流博弈[?]是有效的隐私分析方法。

鉴于上述的分析，本章中考虑在理性的框架下使用信息论的方法解决隐私与效用的均衡问题，通过分析隐私保护者与攻击者的隐私目标，首先将其形式化表述为隐私的极大极小问题。然后，基于差分隐私通信模型(**??**节)，提出隐私保护的攻防博弈模型，也即是一个二人的零和博弈模型。进一步，提出一个交替最优化算法计算提出的攻防博弈的鞍点，利用鞍点策略实现差分隐私的均衡优化。理论上的均衡分析和实验结果表明，提出的均衡思想是一种稳定的状态，可用于预测评估隐私泄露风险。本章的主要贡献可以总结如下：

(1) 通过使用信息论的方法量化隐私攻击者的信息增益，提出了隐私保护的攻防博弈模型(PPAD)，用于分析用户和聚合者的理性策略行为。

(2) 在隐私与效用的原则下，分析隐私防护者与攻击者的隐私目标，形式化表述互信息隐私的极大极小问题，构建二人零和对策博弈求解形式化表述的极大极小问题，并利用交替最优响应策略，设计交替最优的策略优化选择算法。

(3) 对于等价的ε-隐私机制，提出一种有效的比较分析方法，并进一步验证了互信息隐私泄露在最差情况下可以达到隐私泄露的上界，为隐私泄露风险评估提供了量化

分析的方法。

本章其余部分组织如下：首先，第8.2节阐述本章的系统模型、敌手模型，提出研究问题。其次，第8.3节提出隐私保护的攻防博弈模型(PPAD)，并给出均衡分析。进一步，第8.4节介绍均衡求解的策略优化选择算法。最后，第8.5节给出实验与分析，并在第8.6节总结本章的研究工作。

8.2　系统模型与问题提出

本节首先介绍本章的系统模型与符号表示，随后，阐述敌手攻击模型并给出问题描述及形式化表述。

8.2.1　系统模型

如图 8.1描绘了本章的系统模型，其中包含一个不可信数据聚合者和诸多的用户参与到系统数据处理流程中，并通过网络实现互联。本章中重点关注于系统中的隐私保护问题，因此忽略具体的内部网络连接细节。为了保护用户的隐私，每个用户独立的执行隐私保护协议扰动其自己的私密数据。本章中假设用户执行相同的隐私协议，并且隐私协议由用户和聚合者共同协商决定。在这样的情景下，隐私保护的数据处理遵循以下的三个步骤。

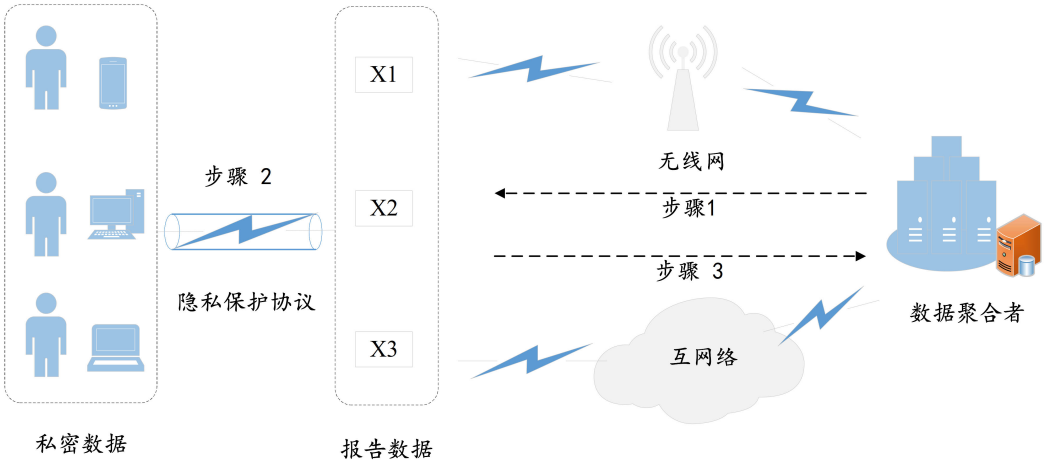

图 8.1: 隐私保护数据收集的系统模型

步骤1: 数据聚合者发布一个数据收集的信号，并决定收集数据的具体细节。这些将要被收集的数据可能包含个人的数据，如家庭地址、婚姻状态、性别、年龄等。然后，数据聚合者招募用户去上报她们自己的私密数据。

步骤2: 系统中的用户可以决定是否上报他们的数据给数据聚合者。如果一个用户同意参与到当前的数据收集任务，她将执行隐私保护协议得到伪装的数据，然后将得到的伪装数据上报给数据聚合者。

步骤3: 基于上述步骤1和步骤2，数据聚合者收集、存储用户的上报数据，然后分析这些上报的数据。

针对图 8.1描述的隐私保护数据收集系统模型，假设有n个用户参与，$[n]=\{1,2,\cdots,n\}$。有限集合$\mathscr{X}$和$\hat{\mathscr{X}}$分别表示用户数据和伪装数据的所有可能取值域，进一步，$|\mathscr{X}|$表示有限集合$\mathscr{X}$的不同原子数量，使用从1到$|\mathscr{X}|$的整数几个表示$\mathscr{X}$中真实字母表的序数。离散随机变量X和$\hat{X}$分别表示个人的原始数据和伪装数据。由此，LDP形成一个概率性函数，映射$x\in\mathscr{X}$到$\hat{x}\in\hat{\mathscr{X}}$的概率为$Q(\hat{x}|x)$，记作，$Q:\mathscr{X}\to\hat{\mathscr{X}}$。除此之外，本章中有时使用下标的$x_i$和$\hat{x}_i$表示第$i$个用户的数据和伪装数据。

为了保护用户个体的隐私信息，每个用户独立的扰动自己的原始数据得到扰动的数据，然后将扰动数据发送给数据聚合者。不失一般性，混淆机制与噪声信道相关，因为差分隐私的定义是基于一个随机的概率性函数。通过这种方式，LDP与信息论建立了基本的联系。为了更好的说明这种关系，以下给出一个具体的例子。

例 8.1. 对于“是”和“否”的选择型问题，它可以被$\{0,1\}$二进制的候选集表示。对于这类问题，差分隐私的混淆机制可以被视为一个二元对称信道。例如，$Q_{0|0}=Q_{(1|1)}=0.7$和$Q_{010}=Q_{(0|1)}=0.3$，则其满足$\varepsilon=\ln\frac{7}{3}$的$\varepsilon$-差分隐私。

令P是支撑集$\mathscr{X}$上的任意一个概率分布，有限集合$\mathscr{P}$包含$\mathscr{X}$上所有可能的概率分布，则有$P\in\mathscr{P}$。假设每一个用户的个人私密数据独立地抽样于的一个分布$P\in\mathscr{P}$，数据聚合者不知道这个分布P，仅知道它是集合$\mathscr{P}$的元素。基于这样的模型假定，本章中考虑策略型的敌手和数据聚合者知道彼此的策略空间。在这种情况下，聚合者旨在最大化隐私推断的成功概率。

8.2.2 敌手模型

本章中，攻击模型是一个半诚实但好奇的(Semi-honest-but curious)敌手模型，也就是，数据聚合者诚实的执行隐私保护协议，但是试图从用户报告的扰动数据中去推断用户的个人隐私信息。事实上，聚合者可能是一个消息灵通的策略型敌手，他可能知道一些有关数据分布的先验知识帮助推断用户隐私。为了捕捉这个先验，假设聚合者仅知道数据分布属于一个确定的集合，$P\in\mathscr{P}$，但是不知道确切的数据分布P。在此情况下，本章中考虑一个策略型的敌手A，他知道用户的隐私保护策略集$\mathscr{Q}$，并有一些数据分布的先验知识$\mathscr{P}$，目标是获取最大的隐私信息量以保证能够推断、识别用户的真实隐私信息。

8.2.3 问题提出

差分隐私的预算参数ε是量化隐私保护不可区分等级的事实标准，但是，ε-度量提供了最差情况下的隐私保证，那也就是说，这个度量是对隐私攻击者有一个较强的假

设。因为ε-度量仅依赖于概率性映射函数，如引言中所述的这个度量存在着一些不足之处[?]。如果存在一个隐私保护机制集合$\mathscr{Q}$，集合中的每个元素$Q \in \mathscr{Q}$都提供ε-隐私保障，则ε-度量无法区分哪一个机制具有较好的隐私保护效果。然而，在很多的应用中，这些隐私保护机制的质量又迫切需要评估。针对这个问题，信息论方法提供了一种有效的解决途径，以下从定义开始介绍其方法的具体细节。

定义 8.1. *离散有限集合$\mathscr{Q}$表示一个含有k个隐私保护机制的集合。如果$\mathscr{Q}$中的每一个机制$Q^i : \mathscr{X} \to \hat{\mathscr{X}} (s.t. 1 \le i \le k)$是一个$\varepsilon$-隐私机制，则这些机制$\{Q^i\}_{i=1}^k$称为一个等价$\varepsilon$-隐私机制。*

注 8.1. *上述定义8.1可以被放松获得一个宽松的LDP机制集合，也就是，一个任意的隐私机制$Q^i \in \mathscr{Q}$是ε_i-LDP机制。*

事实上，隐私保护机制$Q^i : \mathscr{X} \to \hat{\mathscr{X}}$是一个损失压缩机制，它控制着从原始数据到伪装数据的隐私信息比特流动。为了量化信息的流动量，使用信息论的方法定义聚合者的信息增益为

定义 8.2. *对于给定的隐私信息x_i，概率分布$P(X = x_i)$和$P(X = x_i | \hat{X} = \hat{x}_i)$分别表示先验分布和观察到$\hat{x}_i$后的后验概率分布。概率分布的比值$\log\left(\frac{P(X=x_i|\hat{X}=\hat{x}_i)}{P(X=x_i)}\right)$定义为聚合者的信息增益。*

基于上述定义8.2，可以在观察到扰动数据之后，测量有关原始数据的不确定度减少量。本质上，这个度量是关于原始数据的先验和后验概率分布的比较。此外，注意到这个度量和信息论中著名的互信息具有相同的形式。重要地，期望形式的互信息测量一个用户的平均信息损失量，可以用来测量隐私机制的隐私泄露量，也就是互信息泄露

$$I(X;\hat{X}) = \sum_{x \in \mathscr{X}} \sum_{y \in \hat{\mathscr{X}}} P(x) Q(\hat{x}|x) \log\left(\frac{Q(\hat{x}|x)}{P(y)}\right) \tag{8.1}$$

基于互信息隐私泄露的概念，等价的ε隐私机制之间是彼此可以比较的。为了阐述一个偏序关系，首先给出以下定义

定义 8.3. *对于一个给定的先验概率分布P，和任意的两个隐私机制$Q^i, Q^j \in \mathscr{Q} (s.t. 1 \le i, j \le k)$。如果$I(P;Q^i) \le I(P;Q^j)$，则有$Q^i \succcurlyeq Q^j$；否则，$Q^i \prec Q^j$。*

具体的来说，这种偏序关系是可以传递的，它可以用来比较不同机制的隐私保护强度。接下来，考虑互信息测量隐私泄露。首先，互信息测量的隐私泄露聚焦在测量给定伪装数据时，原始数据的不确定度。其次，伪装数据在满足差分隐私的同时应该保持有关原始数据的信息内容尽可能的多。进一步，伪装数据包含的信息量由著名的互信息测量。基于这些理论上的支撑，本章考虑理性的用户旨在减少原始数据与伪装

数据之间的互信息量，以至于聚合者不能拥有足够的信息完全识别一个用户的个人数据。然而，理性的聚合者想要去最大化隐私泄露去得到更多的隐私信息。基于这样的分析，用户的隐私目标可以形式化表述为下列的极小极大问题，则有

$$\inf_{Q\in\mathscr{Q}}\sup_{P\in\mathscr{P}} I(P;Q) \tag{8.2}$$

另外，聚合者想要估计一个分布最大化互信息泄露，因为一个先验的概率分布集合对聚合者是可见的。在这种情况下，隐私机制在最差情况下的互信息泄露将会是

$$\sup_{P\in\mathscr{P}}\inf_{Q\in\mathscr{Q}} I(P;Q) \tag{8.3}$$

事实上，上面的问题被建模成为一个极小极大的问题，它变成了一个凸优化问题[?]。极小极大的问题捕捉到一个基本的场景，参与者的目标是相对立的。在实践中，聚合者可能是一个策略型的参与者而不仅仅受限于仅能观察伪装数据，他可以适应性的改变他自己的策略根据用户的保护策略。在这样的情况下，本章中考虑互信息泄露作为聚合者的信息增益。

8.3 隐私保护攻防博弈

本节中针对上述8.2.3小节提出的极大极小隐私问题，给出隐私保护的攻防博弈模型(PPAD)，并进行相应的均衡分析。

8.3.1 博弈模型

上述隐私保护数据收集的系统模型中，每一个用户使用隐私保护机制扰动自己的原始数据，类似于隐私防护者。同样地，不可信的数据聚合者试图推断用户隐私信息类似于一个隐私攻击者。基于这样的类比，上述8.2.3小节的极小极大隐私问题自然地演变为一个隐私攻击和防御的对策博弈问题。为了有一个较好的阐述，下面首先给出隐私攻防博弈的定义。

定义 8.4. 隐私保护的攻防博弈*(PPAD)*框架是一个元组$(D,A,\mathscr{D},\mathscr{A},U)$，其中，有限集合$\mathscr{D}$和$\mathscr{A}$分别是隐私保护者$D$和隐私攻击者$A$的策略空间，$U:\mathscr{D}\times\mathscr{A}\to\mathbb{R}$是冯诺依曼·摩根斯坦*(von Neumann-Morgenstern)*效用函数。由此，隐私防护者和攻击者的理性行为可以被定义为

$$\begin{cases} s_d^* \overset{def}{=} \arg\min_{s_d\in\mathscr{D}} U_D(s_d,s_a^*) \\ s_a^* \overset{def}{=} \arg\max_{s_a\in\mathscr{A}} U_A(s_d^*,s_a). \end{cases} \tag{8.4}$$

为了阐述更多的细节，以下给出隐私保护的攻防博弈$(D,A,\mathscr{D},\mathscr{A},U)$的标准形式描述，包括博弈参与者、参与者策略空间和效用函数。具体如下：

- 攻防博弈的参与者包括防护者*(Defender)*和攻击者*(Attacker)*，则有，参与者$=\{D,A\}$；
- 有限集合$\mathscr{D}$和$\mathscr{A}$分别为D和A的策略空间，其中，所有可行的隐私机制集合$\mathscr{Q}$是防护者的策略空间，即$\mathscr{D} \triangleq \mathscr{Q}$; 此外，所有可能的概率分布集合$\mathscr{P}$是攻击者的策略空间，即$\mathscr{A} \triangleq \mathscr{P}$;
- 博弈参与者D和A的收益函数$U(P,Q)$采用互信息度量，对于任意的$P \in \mathscr{P}$和$Q \in \mathscr{Q}$，参与者的收益计算依据下式效用函数$U(P,Q)$

$$U(P,Q) = \sum_{\mathscr{X}} \sum_{\mathscr{Y}} P^T Q \log\left(\frac{Q}{\sum_{\mathscr{X}} P^T Q}\right) \tag{8.5}$$

例 8.2. 假设信源概率分布集合$\mathscr{P}$包含3个不同的分布，字母表$|\mathscr{X}|=3$，记作$P^i \in \mathscr{P}, i \in \{1,2,3\}$。具体的实例如下表8.1所示。

表 8.1: 数据概率分布示例

	$p_{(1)}$	$p_{(2)}$	$p_{(3)}$
P^1	0.25	0.35	0.4
P^2	0.35	0.5	0.15
P^3	0.6	0.2	0.2

更多的，一个隐私机制的集合$\mathscr{Q}$包含有3个不同隐私机制，记作$\mathscr{Q}=\{Q^1,Q^2,Q^3\}$，更多的细节如表8.2所示。如此以来，本例表述的隐私保护攻防博弈是一个二人矩阵博弈的实例。

表 8.2: $\varepsilon = \ln 2$的隐私机制

$\mathscr{Q}$	$Q^1_{(y\|x)}$			$Q^2_{(y\|x)}$			$Q^3_{(y\|x)}$		
	1	2	3	1	2	3	1	2	3
1	0.4	0.3	0.3	0.4	0.2	0.4	0.3	0.2	0.5
2	0.25	0.15	0.6	0.3	0.3	0.4	0.2	0.4	0.4
3	0.2	0.2	0.6	0.2	0.4	0.4	0.15	0.35	0.5

本章中所提出的隐私攻防博弈是一个有限策略的完全信息静态博弈*(Simultaneous Games)*，意味着参与者D和A做出决策时不知道其它参与者的策略选择。此外，在攻防博弈*PPAD*中，参与者的策略行动$\mathscr{D},\mathscr{A}$和效用函数$U(\cdot,\cdot)$是隐私防护者D和攻击者A的

共同知识*(Common Knowledge)*。在这种情况下，参与者被假设为理性的决策者，趋向于选择最大化自身收益的策略，基于此给出攻防博弈中参与者的理性行为分析。事实上，如果隐私攻击者收益等于防护者损失，则上述是二人零和博弈*(Two-Person Zero-Sum，TPZS)*，其解是对策博弈的鞍点*(Saddle Point，SD)*。接下来，对所提出的攻防博弈*PPAD*进行均衡分析。

8.3.2 均衡分析

针对本章中8.2.3小节形式化的极大极小问题，8.3.1小节提出了隐私保护的攻防博弈PPAD模型。针对上述博弈，本节中分析了博弈模型的效用函数性质、博弈的均衡，为在8.4节给出了博弈均衡的策略优化选择算法奠定理论基础。

首先，本文**??**节介绍的凹凸对策博弈拥有一个特殊的效用函数形式，它是一个参与者策略的凸函数，同时也是另外一个参与者策略的凹函数[?]。在这样的博弈模型中，博弈的解是每个参与者的纯策略组合。本章中隐私攻防博弈的参与者策略集和效用函数满足凹凸性，为此给出以下分析。

引理 8.1. 对于任意的ε-差分隐私$Q^1, Q^2 \in \mathcal{Q}$，一个实数$\alpha \in \mathbb{R}^+, 0 < \alpha < 1$，它们的凸组合$Q^\alpha = \alpha Q^1 + (1-\alpha)Q^2$仍然满足$\varepsilon$-差分隐私。

证明：令x_1, x_2是两个任意的差分隐私输入数据，$\hat{x}$是一个任意的输出数据。则依据差分的定义，有下式成立

$$Q^\alpha(\hat{x}|x_1) = \alpha Q^1(\hat{x}|x_1) + (1-\alpha)Q^2(\hat{x}|x^2) \tag{8.6}$$

$$\leq \alpha Q^1(\hat{x}|x_2) \cdot \exp(\varepsilon) + (1-\alpha)Q^2(\hat{x}|x^2) \cdot \exp(\varepsilon) \tag{8.7}$$

$$= \exp(\varepsilon) \cdot Q^\alpha(\hat{x}|x_2) \tag{8.8}$$

上述公式*8.8*满足差分隐私定义，故有Q^α仍然是ε-差分隐私。

上述ε-隐私机制的性质已在相关研究工作中使用[?]。对于本章中所提出的隐私保护攻防博弈模型，攻击者和防护者的策略都是概率分布集合，假设它们是凸集。基于文献[?]中的定理2.7.4，则有，对于任意的Q，收益函数$U(P,Q)$满足一个封闭凸集的凹函数，同时，对于每一个P，收益函数$U(P,Q)$是Q的凸函数。这是由于互信息函数的凹凸性(定理2.7.4[?]的证明)，基于这个理论分析的结果，所提出的隐私保护攻防博弈(PPAD)模型是一个凹凸博弈。

其次，均衡分析是对策博弈论中的一个重要研究课题，它的目标是寻找对策博弈模型的解。博弈均衡[?]是一种稳定的状态，该状态下没有参与者有动机改变他当前的策略以获得更大的收益。对于所提出的隐私攻防博弈PPAD模型，结合凹凸博弈的性质给出以下具体的博弈均衡分析。

引理 8.2. 如果$U:\mathscr{P}\times\mathscr{Q}\to\mathbb{R}$是$P$的一个凹函数，则攻击者有最佳的响应策略满足$\max_{P\in\mathscr{P}}\min_{Q\in\mathscr{Q}}U(P,Q)$。相似的，如果它是$Q$的一个凸函数，则防护者有最佳响应策略满足$\min_{Q\in\mathscr{Q}}\max_{P\in\mathscr{P}}U(P,Q)$。

上述引理8.2的证明过程类似于文献[?]中对于定理5.2的证明，此处省略去其具体证明过程。

注 8.2. 如果隐私防护者首先选择行动策略，攻击者随后选择策略行动。则有，防护者希望极小化支付量$U(P,Q)$，因此选择$Q\in\mathscr{Q}$极小化$U(P,Q)$，获得$\inf_{Q\in\mathscr{Q}}U(P,Q)$。攻击者选择$P\in\mathscr{P}$使得最坏情况下的支付最大化，攻击者选择$\arg\max_{P\in\mathscr{P}}U(P,Q)$，期望获得支付量$\sup_{P\in\mathscr{P}}\inf_{Q\in\mathscr{Q}}U(P,Q)$。如果和上述策略选择行动顺序相反，防护者可以获得$\inf_{Q\in\mathscr{Q}}\sup_{P\in\mathscr{P}}U(P,Q)$。

除了上面提到的，所提出的隐私保护攻防博弈PPAD模型属于完全信息的静态博弈研究范畴，每一个参与者可以预测其它参与者的最佳响应策略，也就是最优策略。作为一个结果，无论一个攻击者还是防护者都会对其它参与者的策略选择有一个最佳响应策略。基于这个结果，则有下面的定理。

定理 8.1. 对于有限概率分布集合$\mathscr{P}$和$\mathscr{Q}$，隐私保护的攻防博弈存在一个鞍点(P^*,Q^*)满足$U(P,Q^*)\le U(P^*,Q^*)\le U(P^*,Q)$ 对所有的$P\in\mathscr{P}$和$Q\in\mathscr{Q}$。

证明：对于任意的$Q^1,Q^2\in\mathscr{Q}$，和一个参数$\alpha\in\mathscr{R}^+(0<\alpha<1)$，它们的凸组合$Q^\alpha=\alpha Q^1+(1-\alpha)Q^2$仍然是$\varepsilon$-差分隐私。因为$\mathscr{P}$和$\mathscr{Q}$都是概率分布集合，是欧几里德空间的凸子集。进一步，$U(P,Q)$是一个有关P和Q的二元函数，关于P的凹函数，关于Q的凸函数。更重要的是有限集合$\mathscr{P}$和$\mathscr{Q}$是紧致的，即封闭有界集合。然后，基于著名的极大极小定理**??** ，隐私保护的攻防博弈$PPAD$存在鞍点(P^*,Q^*)满足$U(P,Q^*)\le U(P^*,Q^*)\le U(P^*,Q)$。

推论 8.1. 对所有的$P\in\mathscr{P}$和$Q\in\mathscr{Q}$，策略组合(P^*,Q^*)满足

$$\begin{cases}U(P^*,Q^*)=\sup_{P\in\mathscr{P}}U(P,Q^*)\\ U(P^*,Q^*)=\inf_{Q\in\mathscr{Q}}U(P^*,Q).\end{cases}\tag{8.9}$$

则(P^*,Q^*)称为函数$U(P,Q)$ 在乘积空间$\mathscr{P}\times\mathscr{Q}$的鞍点。

从上述定理8.1可以看出，隐私保护攻防博弈PPAD的鞍点(P^*,Q^*)是隐私保护系统模型中隐私信息泄露的一个极端状态，从隐私泄露量的角度对于隐私防护者的隐私信息保护是一种最差的情况。此外，推论中公式8.9表明鞍点(P^*,Q^*)的支付量$U(P^*,Q^*)$是隐私攻击者可以从原始数据中获取的最小隐私信息增益。同时，这个支付量是防护者最大可能的信息损失。基于鞍点的内涵，隐私保护攻防博弈的鞍点支付量可以用来评估互信息隐私泄露。事实上，这个支付量是互信息隐私泄露的上界。

8.4 策略优化选择算法

上述8.3.2小节针对提出的隐私攻防博弈给出了均衡分析，接下来，介绍隐私保护策略优化选择算法。首先，基于上述引理8.2，鞍点策略(P^*,Q^*)是每一个参与者的最佳响应策略。事实上，提出的隐私保护攻防博弈是一个有限策略的二人零和对策博弈，并结合参与者效用函数的凹凸性，基于定理8.1分析了鞍点的存在性。其次，在解博弈模型的过程中，对于鞍点的计算是两个凸集之间的一个交替最优化问题。基于最优响应策略思想，设计一个计算攻防博弈鞍点的策略优化选择算法，用于解决最初给出的隐私泄露极小极大问题。最后，算法计算是一个交替最优化的过程，该过程类似于两个凸集之间最小化距离的解决方法。具体的，策略优化选择算法的计算过程主要包含有以下三个步骤。

步骤1：初始化选择一个任意防护者策略$Q \in \mathscr{Q}$，攻击者计算一个最优的响应策略P，即是$\arg\max_{P\in\mathscr{P}} U(P,Q)$。

步骤2：防护者预测攻击者的策略偏好，由此，防护者将会采用使得收益最大化的策略，也即是$\arg\min_{Q\in\mathscr{Q}}\max_{P\in\mathscr{P}} U(P,Q)$。

步骤3：交替最优化处理、更新参与者的策略选择，并重复上述步骤直到一个策略组合(P^*,Q^*)对隐私攻击者和防护者都是最优的。

算法 8.1 隐私攻防博弈的策略优化选择算法

输入:

$\mathscr{P}$:攻击者A的可行策略空间

$\mathscr{Q}$:防护者D的可行策略集合

$U(P,Q)$:效用函数

输出:

(P^*,Q^*):鞍点策略

SD :鞍点策略的支付量

初始化集合$S_1 \leftarrow Q^0$使用一个任意的策略$Q^0 \in \mathscr{Q}$
计算攻击者的一个最优响应策略$P^* = \arg\max_{P\in\mathscr{P}} U(P,Q^0)$
计算防护者的最优反应策略$Q^* = \arg\min_{Q\in\mathscr{Q}} U(P^*,Q)$
while (P^*,Q^*)不是博弈鞍点 **do**
    计算攻击者最优响应策略$P^* = \arg\max_{P\in\mathscr{P}} U(P,Q^*)$ 并更新P^* 重新计算$U(P^*,Q^*)$ 利用公式8.5
    if (P^*,Q^*) 是博弈鞍点 **then**
        return (P^*,Q^*) 和$SD \leftarrow U(P^*,Q^*)$
    else
        计算防护者最优响应策略$Q^* = \arg\min_{Q\in\mathscr{Q}\setminus S_1} U(P^*,Q)$
        和$U(P^*,Q^*)$ 使用公式8.5
        更新集合$S_1 \leftarrow S_1 \bigcup Q^*$
    end if
end while

上述算法8.1描述了策略优化选择的具体计算过程，算法接受输入攻防博弈的结

构，也即是博弈规则，包括参与者的策略空间$\mathscr{P},\mathscr{Q}$和效用函数$U(P,Q)$。然后，算法执行计算过程并输出博弈鞍点(P^*,Q^*)和支付量SD。首先，算法初始化一个任意的策略$Q^0 \in \mathscr{Q}$，并为Q^0计算一个最优的响应策略P^*(算法的1 ~ 2行)。其次，算法计算隐私防护者的一个最优响应策略Q^*，用来防护攻击者的策略P^*(算法的第3行)。进一步，算法重复执行上面的这些交替最优化的步骤，直到一个稳定的状态(P^*,Q^*)对于攻击者和防护者都是最优的响应策略(算法的4 ~ 12行)。最后，算法返回博弈的鞍点策略及其对应的支付量。

为了直观地理解上述算法的过程，利用例子8.2给出具体的解释说明，支付矩阵如表8.3所示。为了说明算法8.1的计算步骤，假设防护者首先选择策略Q^1，然后攻击者偏好于采取P^3策略，目的是为了获得一个最大的支付量0.0662，也就是说，P^3是攻击者对Q^1的最优响应策略。进一步，防护者可以预测攻击者的行动P^3，并使用策略Q^2去最小化隐私损失，即是，防护者期望获得0.0315的收益。因此，Q^2是防护者对攻击策略P^3的最优响应。同时，P^3也是攻击者对防护者策略Q^2的最优响应。所以，策略组合(P^3,Q^2)是隐私攻防博弈的鞍点，具有支付量0.0315。而且，鞍点策略提供$\varepsilon = \ln 2$的ε-差分隐私。对此，图8.2清晰的描绘了参与者的理性决策过程。

表 8.3: 对策博弈的支付矩阵

	Q^1	Q^2	Q^3	
P^1	0.0531	0.0308	0.0299	.0299
P^2	0.0627	0.0226	0.0339	.0226
P^3	0.0662	0.0315	0.0345	.0315
	.0662	.0315	.0345	

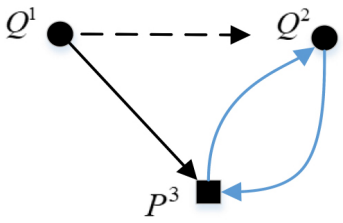

图 8.2: 理性决策过程的描述说明

通过分析算法8.1的一些基本操作，给出计算博弈鞍点的计算复杂度。首先，算法在第一轮迭代中搜索攻击者的策略空间$\mathscr{P}$，寻找一个最优的响应策略P。其次，针对攻击者策略算法计算一个最优响应策略Q，需要搜索防护者的策略空间$\mathscr{Q}$。最后，算法的终止条件保证了极大极小问题的解。鉴于上述分析可知，计算开销随着$\mathscr{P}$和$\mathscr{Q}$的大小而变化。只要策略集合$\mathscr{P}$和$\mathscr{Q}$是有限的，算法计算过程是有效的。

8.5 实验与分析

本节中给出所提出隐私保护策略选择方案的实验结果，并给出实验结果的分析。基于Java实现本章中伪代码描述的算法，并部署在安装Windows 10操作系统的个人PC上执行实验程序。实验分析有两个部分组成，首先，8.5.1节给出一个具体的实例分析，随后，8.5.2节给出数值实验分析结果。

8.5.1 实例分析

对于字母表$|\mathscr{X}|=|\hat{\mathscr{X}}|=6$的情况，本章假设数据先验分布属于一个确定的概率分布集合，但是不能精确的知道真实的数据分布。为了有一个直观的说明，本章借用文献[?]中的分布数据，并在表8.4中给出它们的分布律。

表 8.4: $|\mathscr{X}|=6$的概率分布

	$p_{(1)}$	$p_{(2)}$	$p_{(3)}$	$p_{(4)}$	$p_{(5)}$	$p_{(6)}$
P^1	0.7	0.15	0.06	0.04	0.03	0.02
P^2	0.15	0.7	0.06	0.04	0.03	0.02
P^3	0.06	0.15	0.7	0.04	0.03	0.02
P^4	0.04	0.15	0.06	0.7	0.03	0.02

更多的，考虑两个等价可替换的$\varepsilon=\ln 2$隐私机制，表8.5给出两个隐私机制的条件概率分布，其中，Q^1是截断$\frac{1}{2}$- 几何机制[?]，Q^2是文献[?]提出的隐私机制。进一步，考虑文献[?]中提出的著名k-RR机制，满足对角线概率$e^{\varepsilon}/(|\mathscr{X}|-1+e^{\varepsilon})$。基于此，$k$-RR提供$\varepsilon=\ln 2$差分隐私保护，当且仅当概率密度函数$Q^3$满足

$$Q^3_{(y|x)}=\begin{cases}\frac{e^{\varepsilon}}{|\mathscr{X}|-1+e^{\varepsilon}} & \hat{x}=x\\ \frac{1}{|\mathscr{X}|-1+e^{\varepsilon}} & \hat{x}\neq x\end{cases}\Rightarrow Q^3_{(y|x)}=\begin{cases}2/7 & \hat{x}=x\\ 1/7 & \hat{x}\neq x\end{cases}$$

表 8.5: $|\mathscr{X}|=6$时提供$\varepsilon=\ln 2$的等价隐私机制

In/Out	$Q^1_{(y\|x)}$						$Q^2_{(y\|x)}$					
	1	2	3	4	5	6	1	2	3	4	5	6
1	2/3	1/6	1/12	1/24	1/48	1/48	4/11	2/11	1/11	1/11	1/11	2/11
2	1/3	1/3	1/6	1/12	1/24	1/24	2/11	4/11	2/11	1/11	1/11	1/11
3	1/6	1/6	1/3	1/6	1/12	1/12	1/11	2/11	4/11	2/11	1/11	1/11
4	1/12	1/12	1/6	1/3	1/6	1/6	1/11	1/11	2/11	4/11	2/11	1/11
5	1/24	1/24	1/12	1/6	1/3	1/3	1/11	1/11	1/11	2/11	4/11	2/11
6	1/48	1/48	1/24	1/12	1/6	2/3	2/11	1/11	1/11	1/11	2/11	4/11

上述隐私机制$\{Q^1,Q^2,Q^3\}$是等价的$\ln 2$-隐私机制。为了对这些隐私机制进行比较，假设它们是隐私防护者的所有可能策略。基于这个假设，在此给出以下分析。

基于上述的这些参与者可选行动策略，分析隐私攻击者和防护者的理性策略行为。通过算法8.1求解所对应的博弈模型。作为博弈的解，算法输出一个鞍点P^1, Q^3 和支付量0.0351，这个结果意味着互信息隐私泄露将不会超过一个界(0.0351)。在其它策略组合情况下，隐私防护者将会有动机改变他当前的隐私保护策略。例如，当考虑均匀的先验概率分布，对策博弈的支付量将会是0.0633。综合上述情况，这些情况意味着最佳的隐私保护机制和先验分布密切相关。

此外，本章还利用信息论度量方法解决了等价隐私保护机制之间无法比较的问题。例如，考虑均匀的先验概率分布情景，这些隐私机制的互信息隐私泄露是严格有序的，即$Q^1 = 0.5074 > Q^2 = 0.2164 > Q^3 = 0.0633$。事实上，互信息隐私泄露的这些数值表达出了隐私防护者对于不同博弈产出的偏好。由此，则可以得到$Q^3 \succ Q^2 \succ Q^1$。这种严格的偏序关系对等价的隐私保护机制提供了一种有效的评估方法。

8.5.2　数值分析

为了获得数值实验结果，本文中分别对$|\mathscr{X}| = 6$和$|\mathscr{X} = 12|$随机的生成10个不同的分布。然后，利用随机化响应技术实现隐私保护机制。参考文献[?]，实验中设置ε参数在0到10的区间变化，如此可以获得一个隐私保护机制的集合。基于这些随机的数值数据，给出下面的实验分析。

数据先验概率分布和随机生成的不同隐私机制分别为隐私攻击者和隐私防护者的可用策略行动，并在这些数据上执行实验，利用所提出的策略优化选择算法8.1计算隐私保护攻防博弈的鞍点。为了克服随机性的影响，实验中通过归一化的互信息$I(X;\hat{X}/H(X))$比较所有隐私机制的平均性能，也即是隐私支付量。在所提出的隐私攻防博弈模型中，理性的隐私攻击者和隐私防护者偏好于采用获得最大化(最小化)博弈支付的策略。事实上，互信息隐私泄露是隐私预算ε的严格单调函数，由此，随着ε的增加，归一化的互信息隐私泄露曲线可以被描绘出来。

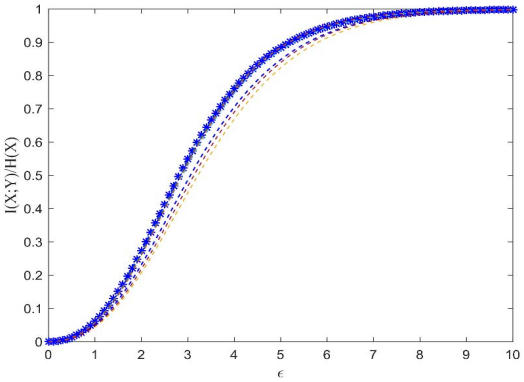

图 8.3: $|\mathscr{X}| = 6$时$I(X;\hat{X})/H(X)$

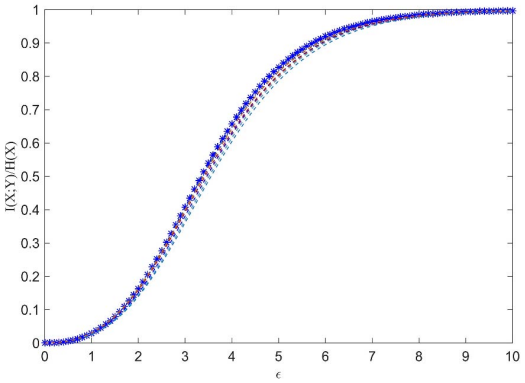

图 8.4: $|\mathscr{X}| = 12$时$I(X;\hat{X})/H(X)$

图 8.3和图 8.4给出了数值实验结果。从图中可以看出，鞍点策略的互信息隐私泄

露对于隐私防护者是最差情况的隐私泄露。另外，图 8.3和图 8.4还表明了上述结论对于字母表基数$|\mathcal{X}|$是不敏感的，因为两组实验具有相同的趋势。最差情况下的互信息隐私泄露可以帮助评估隐私泄露风险，选择适当的ε参数在隐私容忍的范围内。

8.6 本章小结

本章针对差分隐私数据收集应用中存在的策略型攻击问题，利用信息论、博弈均衡理论研究了隐私防护者与隐私攻击者的理性策略选择，提出了隐私保护的攻防博弈(PPAD)模型，以实现隐私与数据效用均衡。首先，基于信息论度量方法分析差分隐私保护系统中隐私保护者和攻击者的隐私目标，形式化表述为互信息隐私的极大极小问题。其次，针对上述提出的问题，考虑策略型的隐私攻击者和防护者，提出隐私保护的攻防博弈模型，并具体为二人的零和博弈模型。随后，给出博弈的凹凸性以及均衡分析。进一步，为了求解博弈模型鞍点，设计了策略优化选择算法。最后，通过实验阐述了所提出的方案可以用于比较等价的隐私机制，并阐述了隐私量化是最坏情况下的隐私泄露，也即是，隐私防护者的最大隐私泄露。

第九章　总结与展望

本章首先总结文中针对差分隐私保护模型的隐私与效用权衡问题做出的研究工作，概括文中使用的研究方法以及取得的研究成果。其次，讨论分析本文工作中存在的不足之处，并基于此对本文的后续研究内容进行了展望。

9.1　工作总结

大数据时代的在线网络数据(如在线社交网络数据、医疗数据、移动轨迹数据等)促使个人隐私遭受潜在的隐私泄露风险，使得隐私泄露成为数据科学与工程的一个主要关注问题，迫切需要有效的数据隐私保护模型及方法。在诸多的隐私保护模型中，差分隐私逐渐成为数据隐私保护研究与应用中的一个事实上的隐私标准，在隐私保护数据发布、隐私保护数据收集、隐私保护数据分析等场景中得到了广泛的应用。差分隐私主要是利用随机性遏制个人隐私推断问题，其随机性涉及的隐私性与数据效用是研究差分隐私机制设计的核心。依据隐私与效用原则，隐私与效用仅能达到较为理想的平衡折中，这就是学术研究中备受关注的隐私与效用权衡问题。当前的研究工作在面向多维数据处理、属性关联以及关联数据隐私攻击等方面还存在一些不足之处，尚需要深入的研究。为此，本文围绕差分隐私应用中存在的隐私与数据效用的权衡问题，提炼出隐私与效用的度量、权衡隐私与效用的优化模型、隐私保护机制的设计及隐私保护机制的评价方法四个关键的问题。针对此，本文利用信息论、优化理论、对策博弈论方法从均衡优化的角度，研究了差分隐私通信模型及其度量方法、差分隐私的均衡优化模型和差分隐私均衡优化模型的算法，提出了面向关联属性的信息熵度量模型、数据关联的差分隐私优化模型、多维数据有序随机响应扰动方案(ORRP)和隐私保护的攻防博弈模型(PPAD)及其对应的算法。旨在借助信息论的基础方法，通过最优化和均衡的手段，探讨差分隐私的均衡优化方法，实现保护个人隐私的同时维持数据质量。具体的，本文的主要工作总结如下：

(1) 基于Shannon基本通信模型，结合差分隐私随机扰动，构建了差分隐私的基本通信模型，并给出形式化的描述。以此为基础，首先抽象差分隐私数据扰动为有损压缩信道机制。进一步，考虑含关联背景知识的敌手模型，提出了差分隐私含敌手背景知识的通信模型。其次，在通信模型的基础上，引入信息熵、联合熵、条件熵、互信息量以及失真等概念，建立了以信息论方法为核心的差分隐私度量模型，逐步形成差分隐私的信息熵度量体系。随后，以基本的度量为基础，针对多维关联属性的隐私度量问题，利用关联分析、图模型以及马尔可夫隐私链，提出了面向关联属性的差分隐私信息熵度量模型及方法。最后，利用数据处理和费诺不等式提供了相应的分析。

(2) 针对差分隐私数据发布中存在的隐私泄露问题，以所建立的差分隐私通信模型为基础，基于隐私与效用的度量方法，形式化表述了隐私与效用权衡问题，给出互信息隐私优化模型。进一步，针对差分隐私发布中存在先验知识的数据关联问题，考虑了含背景知识的敌手模型。通过引入条件互信息量，针对隐私攻击者完全背景知识、数据管理者拥有统计知识的情景，提出了条件互信息优化模型，用于求解最小化隐私泄露的最优隐私机制。最后，针对所提出的优化模型求解问题，设计了最小化的迭代算法，实验结果表明所提出的方法有效提高了数据质量。

(3) 针对差分隐私在处理多维数据时面临的隐私脆弱性和效率低的问题，利用信息论方法，研究了面向多维数据收集的最优机制问题，提出了有序随机响应扰动方案(ORRP)，有效弥补现有隐私机制忽略考虑先验分布的影响，提供相同属性级隐私保护强度的不足。首先，基于独立并联信道模型，使用分治策略思想分解元组分量。其次，基于隐私与效用度量为基础，针对单属性分量，将满足数据质量损失约束最小化规避隐私风险的隐私机制，形式化表述为一个计算单属性的最优输出概率密度函数的优化问题。然后，将上述推广到多维数据情景，提出了ORRP方案，利用模型计算的概率密度函数实现随机扰动，并给出了对应算法。最后，分析了所提出方案的隐私、效用及相关度损失，并在真实数据集上进行实验，分析所提出方案的优势。

(4) 针对差分隐私中存在策略型的敌手模型，在已构建的差分隐私基本通信模型和基本的度量基础上，分析隐私保护系统参与者的隐私目标，提出了隐私保护的攻防博弈模型(PPAD)，旨在于利用博弈均衡理论实现隐私保护系统中隐私与数据效用的均衡。首先，基于所建立的差分隐私度量模型，定义了隐私保护系统中隐私保护者和隐私攻击者(敌手)的隐私目标，形式化表述为有关隐私泄露的极大极小问题。其次，从参与者、策略空间、效用函数的角度给出了隐私攻防博弈的标准形式描述，构建了两方零和对策博弈模型。进一步，利用极大极小定理、凹凸博弈的理论提供了所建立博弈模型的均衡分析，即鞍点的分析。理论上的分析表明鞍点的存在性，并解释了鞍点在隐私保护中的涵义。对于等价的ε-隐私机制，提出了等价类隐私机制可比较的方法，解决了ε-隐私度量存在的不足。此外，基于交替最优响应策略设计了博弈均衡计算的策略优化选择算法，并给出了实验分析。

9.2 研究展望

当前，差分隐私在数据隐私保护中发挥重要的作用，应用范围涉及数据发布、数据收集、数据分析、机器学习等领域，对其应用的研究仍需要积极的推进。虽然本文基于信息论和对策博弈论的基础理论方法，从均衡优化的角度做出了一些有意义的探索工作，但是本文的研究中尚存在一些值得深入研究的问题。具体包括有：

(1) 在隐私度量方面，研究表达用户隐私敏感偏好强度的度量方法，建立差分隐私ε-度量、用户个性化隐私需求和信息熵度量的联系，为个性化的差分隐私研究奠定

基础。进一步，在面向多维关联数据情景研究并提出个性化的差分隐私方案是一个值得深入研究的重要方向。

(2) 在权衡隐私与效用的优化模型研究方面，研究最大化数据效用的优化模型，并设计具体的隐私机制是非常有价值的方向。其次，基于所建立的差分隐私通信模型，从信道容量的角度考虑差分隐私的最大信息传输率，对差分隐私保护系统中隐私信息率的定量化研究也是一个值得探索的方向。

(3) 在隐私与效用的均衡优化方面，基于博弈均衡理论的指导，利用非完全信息的动态博弈、静态博弈，建立两方或多方的攻防博弈模型探讨差分隐私保护的最优策略问题仍然是值得研究的方向。此外，基于量化信息流思想，构建差分隐私的信息泄露博弈仍然是值得关注的研究点。

参考文献

[1] GABBAY D M, SCHMIDT R, SZALAS A. Second order quantifier elimination: Foundations, computational aspects and applications[M]. [S.l.]: College Publications, 2008.

[2] BAIER C, KATOEN J P. Principles of model checking[M]. [S.l.]: The MIT Press, 2008.

[3] BROWNE M C, CLARKE E M, GRÜMBERG O. Characterizing finite Kripke structures in propositional temporal logic[J]. Theoretical Computer Science, 1988, 59(1-2):115-131.

[4] CLARKE E M, EMERSON E A, SISTLA A P. Automatic verification of finite-state concurrent systems using temporal logic specifications[J/OL]. ACM Trans. Program. Lang. Syst., 1986, 8(2):244-263. https://doi.org/10.1145/5397.5399.

[5] BOLOTOV A. A clausal resolution method for CTL branching-time temporal logic [J/OL]. Journal of Experimental & Theoretical Artificial Intelligence, 1999, 11(1):77-93. DOI: 10.1080/095281399146625.

[6] ZHANG L, HUSTADT U, DIXON C. First-order resolution for CTL[R]. [S.l.]: Citeseer, 2008.

[7] ZHANG L, HUSTADT U, DIXON C. A resolution calculus for the branching-time temporal logic CTL[J]. ACM Transactions on Computational Logic (TOCL), 2014, 15(1): 1-38.

[8] ZHANG L, HUSTADT U, DIXON C. CTL-RP: A computation tree logic resolution prover[J/OL]. AI Commun., 2010, 23(2-3):111-136. https://doi.org/10.3233/AIC-2010-0463.

[9] DAVIS M, PUTNAM H. A computing procedure for quantification theory[J/OL]. J. ACM, 1960, 7(3):201-215. http://doi.acm.org/10.1145/321033.321034.

[10] ROBINSON J A. A machine-oriented logic based on the resolution principle[J/OL]. Journal of the ACM (JACM), 1965, 12(1):23-41. http://doi.acm.org/10.1145/321250.321253.

[11] ENJALBERT P, DEL CERRO L F. Modal resolution in clausal form[J/OL]. Theoretical Computer Science, 1989, 65(1):1-33. https://doi.org/10.1016/0304-3975(89)90137-0.

[12] CAVALLI A R, DEL CERRO L F. A decision method for linear temporal logic[C/OL]// SHOSTAK R E. Lecture Notes in Computer Science: volume 170 7th International Conference on Automated Deduction, Napa, California, USA, May 14-16, 1984, Proceedings. Springer, 1984: 113-127. https://doi.org/10.1007/978-0-387-34768-4_7.

[13] BOLOTOV A, FISHER M. A clausal resolution method for CTL branching-time temporal logic[J/OL]. Journal of Experimental & Theoretical Artificial Intelligence, 1999, 11 (1):77-93. https://doi.org/10.1080/095281399146625.

[14] KOZEN D. Results on the propositional mu-calculus[J/OL]. Theor. Comput. Sci., 1983, 27:333-354. https://doi.org/10.1016/0304-3975(82)90125-6.

[15] BRADFIELD J C, WALUKIEWICZ I. The μ-calculus and model checking[M/OL]// CLARKE E M, HENZINGER T A, VEITH H, et al. Handbook of Model Checking. 2018: 871-919. https://doi.org/10.1007/978-3-319-10575-8_26.

[16] JANIN D, WALUKIEWICZ I. Automata for the modal μ-calculus and related results [C/OL]//WIEDERMANN J, HÁJEK P. Lecture Notes in Computer Science: volume 969 Mathematical Foundations of Computer Science 1995, 20th International Symposium, MFCS'95, Prague, Czech Republic, August 28 - September 1, 1995, Proceedings. 1995: 552-562. https://doi.org/10.1007/3-540-60246-1_160.

[17] D'AGOSTINO G, LENZI G. On modal mu-calculus with explicit interpolants[J/OL]. J. Appl. Log., 2006, 4(3):256-278. https://doi.org/10.1016/j.jal.2005.06.008.

[18] ZHANG Y, ZHOU Y. Knowledge forgetting: Properties and applications[J]. Artificial Intelligence, 2009, 173(16-17):1525-1537.

[19] KAUSHIK R, NAUGHTON J F, BOHANNON P, et al. Updates for structure indexes [C]//Proceedings of VLDB'02. [S.l.]: Elsevier, 2002: 239-250.

[20] EMERSON E A. Temporal and modal logic[M/OL]//VAN LEEUWEN J. Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics. Elsevier and MIT Press, 1990: 995-1072. https://doi.org/10.1016/b978-0-444-88074-1.50021-4.

[21] BOLOTOV A. Clausal resolution for branching-time temporal logic.[D]. [S.l.]: Manchester Metropolitan University, 2000.

[22] ZHANG L, HUSTADT U, DIXON C. A refined resolution calculus for CTL[C]// International Conference on Automated Deduction. [S.l.]: Springer, 2009: 245-260.

[23] SZALAS A. Second-order quantifier elimination in modal contexts[C]//European Workshop on Logics in Artificial Intelligence. [S.l.]: Springer, 2002: 223-232.

[24] MAKSIMOVA L. Temporal logics of "the next" do not have the beth property[J]. Journal of Applied Non-Classical Logics, 1991, 1:73-76.

[25] EMERSON E A, HALPERN J Y. Decision procedures and expressiveness in the temporal logic of branching time[J/OL]. Journal of computer and system sciences, 1985, 30(1): 1-24. https://doi.org/10.1016/0022-0000(85)90001-7.

[26] MYCIELSKI J, ROZENBERG G, SALOMAA A. Lecture notes in computer science: volume 1261 structures in logic and computer science, A selection of essays in honor of andrzej ehrenfeucht[C/OL]. Springer, 1997. https://doi.org/10.1007/3-540-63246-8.

[27] HINTIKKA J. Distributive normal forms in the calculus of predicates[J]. Cambridge University Press, 1953, 20(2).

[28] YANKOV V A. Three sequences of formulas with two variables in the positive propositional logic[J]. Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 1968, 32 (4):880-883.

致　　谢

“立身以立学为先，立学以读书为本。”读书是韶华之年提高修养、塑造人格、提升能力的基石，厚积薄发的源泉，时至而立之年当以立身、立业、立家。求学之路，始于黄口，而立之年，学有所成。即将毕业之时，学位论文完稿之际，我衷心的感谢在贵州大学计算机科学与技术学院攻读博士学位期间对我关心、支持、鼓励和帮助的老师、同学和家人。

“古之学者必有师。师者，所以传道受业解惑也。”导师彭长根教授在我攻读博士学位期间，给予我了学术科研的悉心指导和帮助，带我走入了密码学与信息安全、数据安全与隐私保护的研究领域。在论文研究的选题、研究过程、论文写作等环节提出了诸多建设性意见和建议，使我很受启发。惑之不解时，彭老师学识渊博给出了启发式的建议，帮助我解决了研究过程中所面临的关键性困难问题。几年来，受彭老师严谨的学术熏陶、谆谆教诲，日渐培养和提高了我的科研学术能力。生活中，彭老师无微不至的关怀和关爱，以及彭老师温馨的学术团队使我感到了幸福和温暖。在此，我要感谢彭老师，感恩彭老师的指导和帮助才有了本文的学术研究成果。在未来的学习和工作中，我会进一步深入的从事该方向的研究。

感谢团队田有亮教授，感谢田老师在论文研究、撰写的过程中所提出的意见，以及生活上所给予的帮助。此外，感谢实验室团队谭伟杰博士、刘惠篮博士、丁红发博士、刘海博士等在日常科研及生活中所给予的帮助。同时，感谢实验室的师兄弟姐妹在日常生活中给予我的帮助，读书期间的温馨和睦相处和茶余饭后时的谈笑风生都让我感受到家的温暖。

感谢贵州大学计算机学院的老师为本文工作所提供的支持和帮助；感谢秦永彬教授、王以松教授等为本文的选题和研究方案的设计所提出的宝贵意见和建议。

感谢我的父母和妻子在学习和生活上给予我的支持和鼓励。在我攻读博士学位期间，父母对我无私地爱，默默的付出和承担着家庭生活的压力；面对学习困境和压力时，父母给我支持和关心；妻子在我他乡求学期间独自抚养、教育年幼的儿子，给我创造一个安心求学的条件，陪伴我这一段人生路走来，付出和努力了很多。

最后，感谢参与该博士学位论文评审、答辩的诸位专家学者，感谢您们为提高我的博士学位论文质量所提出的宝贵修改意见和建议。

攻读博士学位期间科研和论文情况

一、主持或参与科研项目

主持科研项目

1. 贵州省研究生科研基金立项课题：开放数据发布的隐私保护关键技术及隐私量化评估，合同编号KYJJ2017005

参与科研项目

1. 国家自然科学基金重点项目：数据共享应用的块数据融合分析理论与安全管控模型研究，项目基金号U1836205
2. 国家自然科学基金地区项目：理性隐私计算及隐私风险可控技术研究，项目基金号61662009
3. 贵州省科技计划重大专项：大数据安全与隐私保护关键技术研究，合同编号黔科合重大专项字[2018]3001)

二、发表论文

[1] **Ningbo Wu**, Changgen Peng (Corresponding author). An information theoretic approach to local differential privacy data collection [J] IEEE Transaction on Knowledge and Data Engineering (TKDE) SCI 2区，CCF推荐数据挖掘A类期刊，IF 3.856 (Major Revision, Under Review)

[2] **Ningbo Wu**, Changgen Peng (Corresponding author), Kun Niu. A privacy-preserving game model for local differential privacy by using information-theoretic approach[J]. IEEE ACCESS,2020,8:216741-216751. DOI:10.1109/ACCESS.2020.3041854. SCI 2区，IF 3.8

[3] **吴宁博**,彭长根(通信作者),田有亮,牛坤,丁红发.基于率失真的差分隐私效用优化模型[J]. 计算机学报,2020,43(8):1463-1478. DOI:10.11897/SP.J.1016.2020.01463, CCF推荐中文科技期刊A类，贵州大学(一级学术期刊)

[4] **吴宁博**,彭长根(通信作者),牟其林. 面向关联属性的差分隐私信息熵度量方法[J]. 电子学报,2019,47(11):2337-2343. DOI:10.3969/j.issn.0372-2112.2019.11.015, CCF推荐中文科技期刊A类，贵州大学(一级学术期刊)

附：学位论文原创性声明和关于学位论文使用授权的声明

原 创 性 声 明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的科研成果。对本文的研究在做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律责任由本人承担。

论文作者签名：_____ 日 期：_____年 月

关于学位论文使用授权的声明

本人完全了解贵州大学有关保留、使用学位论文的规定，同意学校保留或向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅；本人授权贵州大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其他复制手段保存论文和汇编本学位论文。

（保密论文在解密后应遵守此规定）

论文作者签名：_____导师签名：_____日 期：_____年 月