电子科技大学

UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA

专业学位硕士学位论文

MASTER THESIS FOR PROFESSIONAL DEGREE

论文题目 面向数据价值共享的激励技术研究与实现

专业学位类别	工 程 硕 士
学 号	201722060929
作 者 姓 名	罗 通
指 导 教 师	罗光春 教授

分类号 _____ 密级 _____

UDC [注1] _____

学 位 论 文

面向数据价值共享的激励技术研究与实现

（题名和副题名）

罗 通

（作者姓名）

指导教师 罗光春 教授

电子科技大学 成 都

（姓名、职称、单位名称）

申请学位级别 硕士 专业学位类别 工 程 硕 士

工程领域名称 计算机技术

提交论文日期 2020.4.2 论文答辩日期 2020.5.19

学位授予单位和日期 电子科技大学 2020 年 6 月

答辩委员会主席 _____

评阅人 _____

注 1：注明《国际十进分类法 UDC》的类号。

The Study and Implementation of Incentive Techniques for Value-based Data Sharing

A Master Thesis Submitted to

University of Electronic Science and Technology of China

Discipline: **Master of Engineering**

Author: **Tong Luo**

Supervisor: **Guangchun Luo**

School: **School of Computer Science & Engineering**

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名：_____ 日期：　　年　　月　　日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将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、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

作者签名：_____ 导师签名：_____

日期：　　年　　月　　日

摘　要

在科学技术不断发展的今天，人们每天的日常生活都会产生海量数据，而对这些数据资源的分析应用已经创造了大量的经济价值、社会价值。对于中心化的数据资源，可以使用现有的大数据分析技术对其进行价值挖掘。而地理上分布于不同组织及个人的海量数据却难以实现高效联合应用。因为受限于成本，隐私、社会规范等诸多因素，理性的数据拥有者们可能并不愿意将原始数据直接共享。这造成了“数据孤岛”的现象。而数据价值共享的目标是：尽可能利用这些地理上分散的多方数据来创建计算应用，同时避免原始数据直接传递，从而最大限度保证数据使用安全。即共享数据价值，而非共享数据本身。

为此，本文提出了一种多方数据价值共享计算模式，该计算模式能够在传递数据价值的同时，避免原始数据直接共享。在该计算模式下，提供相同或相似内容的数据拥有者之间会产生竞争。为了妥善处理这些竞争，选出参与数据价值共享的胜出者，同时激励理性的参与者尽可能真实地参与数据价值共享，保证该计算模式的有效性，并最大化系统整体收益，本文针对该数据价值共享模式的两种不同具体计算场景设计了性质良好的激励机制。本文的具体工作如下：

1、提出了多方数据价值共享计算模式。针对简单可并行的计算任务提出了多约束价值共享激励模型。本文首先对问题进行建模，分析了数据量约束、指标集约束、机构约束三种具体应用实例，并设计了计算有效、真实、社会福利最大化的 DSIC 激励拍卖机制。模拟实验说明了该模型的有效性及良好性能。

2、针对依赖相关的计算任务，提出了以计算时间作为重要限制指标的时间敏感价值共享激励模型。本文首先以 AOE 网对任务流程进行建模。论证了相应社会福利最大化问题的 NP 困难性。然后对一类朴素贪心思路进行证否，并提出基于另一种贪心思想的启发式算法来确定分配方法。最后，设计了考虑任务方收益的最优拍卖机制。模拟实验说明了该模型的性能和有效性。

3、本文最后设计并实现了数据价值共享拍卖系统，完成了系统的总体设计，子系统及模块化设计。将多约束价值共享激励模型和时间敏感价值共享激励模型部署至具体的应用环境，并对激励拍卖系统的核心流程进行界面展示。系统功能完善，运行良好。

关键词：机制设计，数据价值，多方计算，背包拍卖

ABSTRACT

With the continuous development of science and technology, people's daily life produces massive data, and the analysis and application of these data resources have created a large number of economic and social values. For centralized data resources, the existing big data analysis technology can be applied for value mining easily. However, it's hard to deploy efficient joint application to the massive geographically distributed data owned by different organizations and individuals. Due to many factors such as cost, privacy, and social regulation, rational data owners may not be willing to donate their data directly. This resulted in the phenomenon of "data island". And the goal of value-based data sharing is to exploit these geographically distributed multi-party data as much as possible to construct computing applications while avoiding the direct transfer of the original data so as to ensure data security. That is, to share the value of data instead of data itself.

Therefore, this thesis proposes a value-based data sharing scheme, which avoids sharing original data directly while transferring data values.In the scheme, there will be competitions between data owners who provide equivalent content. For the purpose of breaking the tie, selecting the winners who participate in the scheme, encouraging rational participants to be as truthfully as possible, ensuring the effectiveness of the scheme and maximizing the overall welfare of the system, it designs ideal incentive mechanisms for two specific scenarios. The specific work of this thesis is as follows:

Firstly, a multi-party value-base data sharing scheme is proposed. Aiming at simple and parallelizable computation tasks, a multi-constraint value-based data sharing incentive model follows. Specifically, the formal modeling of the problem is carried out, then three specific application instances (data volume constraint, indicator set constraint, organization constraint) are analysed, after that a DSIC incentive auction mechanism which is computational effective, truthful as well as social welfare maximized is designed. Simulation experiments show the effectiveness and good performance of the model.

Secondly, for dependency-related computation tasks, a time-sensitive value-based data sharing incentive model is proposed, in which execution time is taken as an essential limiting indicator. Specifically, the task flow is modeled by AOE network. After that, the NP hardness of corresponding social welfare maximization problem is demonstrated. Then, the ineffectiveness of some greedy thoughts is proved while another greedy

heuristic algorithm is given which works well to approximate the optimal allocation rule. Finally, the optimal auction mechanism considering the revenue of the task initiator is given. Simulation experiments show the effectiveness of the model.

Eventually, this thesis designs and implements a value-based data sharing auction system. In addition to overall design,the subsystem and modular design is completed correspondingly. The above multi-constraint value-based data sharing incentive model and time-sensitive value-based data sharing incentive model are deployed to specific application environments. The core process of the auction is displayed then, which shows good performance of the system.

Keywords: mechanism design，data value，multiparty computation，knapsack auction

目 录

第一章 绪 论

1.1 研究工作的背景与意义

在科学技术不断发展的今天，人类的活动及其产生的影响都可以被信息化。衣食住行、自然观测、历史记载等领域都不例外。随之产生的海量数据中存在巨大的潜在价值，而现在已经有精彩纷呈的数据挖掘及分析技术 (机器学习、深度学习等) 应用于这些数据上，训练网络、学习知识，从而获取巨大的社会及经济价值。《2019 中国大数据产业发展白皮书》[1] 指出，2015 年以来，随着国家和地方政府的大力推动，大数据产业加速发展。2018 年整体规模达到 4384.5 亿元，预计到 2021 年将达到 8070.6 亿元，持续促进传统产业转型升级，激发经济增长活力，主力新型智慧城市和数字化建设。海量数据早已成为一种重要的资源。然而在数据的使用方法不断革新，前途一片光明的同时，数据使用的合法性、安全性也成为亟待解决的难题。各个数据拥有者，可能出于隐私防护、利益诉求、知识产权、保密责任等各种原因，不愿将数据直接共享，以创造更大的价值。于是，各个“数据孤岛”产生了。而在网络安全事件，隐私泄露事件频发的今天，面对复杂的低信任度网络环境，如何打破这些孤岛之间的共享障碍，促进数据更好地使用，同时限制数据暴露的程度来降低数据安全风险是现有研究努力的方向。

解决以上“数据孤岛”难题的一种方法是将计算模型根据现有的数据分布进行重组拆分，拆分后的子计算任务在相应数据拥有方进行本地计算。这些本地计算仅依赖于本地的隐私敏感数据。最后各个子计算任务的结果由中心节点进行整合。从而实现数据不直接共享，仅共享数据价值的计算模式。在充分利用分布式多方数据创造更多价值的同时，该计算模式可以有力保证数据拥有者的数据隐私安全。

然而，数据价值共享必然不可避免得带给数据拥有者损失 (提供计算、保持通信的资源消耗、数据的获取及维护成本)，这不利于数据拥有者主动参与价值共享生态。因而需要系统对数据拥有者进行补偿，从而鼓励数据拥有者在受限的数据暴露程度下贡献其数据价值。系统中的环境、规则形成了整个数据价值共享的体系机制，好的规则体系能够充分调动所有数据拥有方的积极性，提升整体性能。而坏的机制可能使得数据拥有者罢工，为体系带来一系列不可估量的风险，甚至使整个系统停止运转。所以在打破“数据孤岛”壁垒的同时，针对具体应用场景确定性能优良的价格体系，完善激励机制对数据价值共享生态有着极大的促进和支撑作用。但大数据产业目前仍然处于探索与研究的阶段，满足数据价值共享场景

的激励体系研究极少。针对理想的数据价值共享计算模式设计公平合理、计算高效的价格体系是具有重要意义的。

1.2 国内外研究历史与现状

激励技术是公平合理的资源交换及分配的核心方法，其主体内容是合理的机制设计，长期以来受到学术及工业界的广泛关注。本部分将从发展历史、关键应用、数据直接共享领域、数据价值共享领域这几个方面对相关研究进行概述。

机制设计起源于上世纪 60 年代。占优策略激励相容的概念由 Hurwicz[2] 在 1972 年正式提出。而理想机制的概念起源于 Vickrey[3]，这篇文章也是拍卖理论的奠基之作。搜索引擎的主要收入来源是关键字拍卖，关键字拍卖的广义二价拍卖 (GSP) 模型模型来源于 Edelman[4] 和 Varian[5]。而拍卖者具有指定税收目标的拍卖机制由 Goldberg 等人[6] 讨论及分析。

另一方面，算法机制设计起源于 Nisan[7] 和 Lehmann 等人[8]。单变量环境的概念由 Archer 和 Tardos[9] 于 2001 年提出。而在资源分配领域应用广泛的背包拍卖是由 Mu'Alem 和 Nisan[10] 提出。显示定理来自于 Gibbard[11]。而近年来算法机制设计领域的快速发展得益于其与近似算法领域的紧密连接。Ibarra 和 Kim[12] 于 1975 年给出了背包问题的经典 FPTAS 近似算法。Briest[13] 以此为基础给出了计算可行且性质良好的背包拍卖机制。类似的，Lehmann 等人[8] 以集合覆盖问题为基础，以贪心算法实现了性质良好的机制。

前述的算法大多考虑社会福利最大化，而着重考虑拍卖方收益的最优拍卖机制起源于 Myerson[14] 的研究。Ostrovsky 和 Schwarz[15] 在将此思想应用至雅虎公司的关键字拍卖中。雅虎高层管理者认为设置更高的保留价格是雅虎公司在 2008 年第三季度的搜索引擎获利增加的最主要原因。

机制设计的应用场景还涉及到频谱拍卖领域[16] [17] [18] [19]。在单次频谱拍卖中，可能涉及的金额高达百万美元。因而失败的机制将带来不可挽回的经济损失。Rassenti 等人[20] 早在 1982 年就尝试以组合拍卖来确定机场的时隙分配。Cramon[21] 详细描述了早期频谱拍卖中的出现的共谋和竞标信号问题。美国联邦通信委员会 (FCC)[22] 于 2015 年给出了 FCC 激励拍卖机制的细节。该机制使政府可以以反向拍卖的方式从广播电视台回购频谱，同时保证未被回购的频谱不会产生冲突，然后进行资源整合并重新出售整合后的宽频谱，从而更好得分配频谱资源并带来更多的经济收益。其反向拍卖的核心问题与平面图的点着色问题有关。

前面的机制及算法大都是以货币作为激励手段，另一种无货币的机制也有重要应用场景。Roth 等人[23] 以 TTC 算法来解决肾脏交换的问题。但 TTC 算法的结

果可能包含较长的置换链，这增加了肾脏交换过程中的风险。因此其将原问题建模为无向图，并通过图的匹配来寻找长度仅为 2 的置换链[24]。另外，Roth[23] 还将 TTC 算法及其激励特性应用至所有人亡故的房屋与没有住所的人的匹配问题。而在 [25] 中，Roth 等人进一步考虑置换链长度为 3 的肾脏匹配机制，这意味着同时进行 6 个患者的手术。相比于长度为 2 的置换链，这极大提升了肾脏匹配成功的数量。但是，继续增大置换链的长度，例如 4、5，以至更长，似乎都难以显著提升匹配数量。Sack[26] 在 2012 年实施了一场置换链长度为 30 的肾脏移植，由一名无偿肾源捐献者作为置换链的起点。前述算法的激励层级大多是在患者级别，即每个患者尽表达尽可能多的肾脏交换意愿是其占优策略，这有利于促成更多的成功匹配。然而，若在肾脏交换意愿在医院层面被部分拦截，即医院内部尽可能最优匹配，这可能不利于总体系统的匹配性能。这部分其实与共谋有关。Ashlagi 等人[27] 针对肾脏置换场景下医院层面的激励机制做了一些关于讨论。

另外一个广泛的应用场景是稳定匹配问题。Gale 和 Shapley[28] 形式化了稳定匹配问题，给出了延迟接受算法，并证明了是算法的时间复杂度和部分最优性。Dubins 和 Freedman[29] 研究了上述场景的一个变种：未匹配的参与者希望依次进行匹配而非同时进行。他们还分析证明了延迟接受算法的激励属性：算法对匹配的一方具有真实表达意愿的激励，而对另一方没有。

而在数据直接共享方面，激励机制的应用主要集中在众包领域。*SenseMart*[30] 讨论了在感知数据交付机制中的激励问题并提出了一系列具有挑战的难题。在与众包相近的参与感知领域中也存在一些关于激励机制的研究。Reddy 等人[31] 来设计了一种关于匹配感知任务最优参与者的激励框架。然而，他们仅仅关注于参与者的选择，而并未涉及激励机制的设计。Danezis 等人[32] 设计了一种密封二价拍卖机制来提高参与者的参与度。然而，他们没有在机制设计中进一步考虑众包者本身的效用。Lee 和 Hoh[33] 设计并且评估了一种动态价格激励机制，参与者可以将感知数据以自己的标的价格卖给需求方，但这种机制中的参与者可能会为了最大化自身效用而给出非真实估值。duan 等人[34] 研究了两种应用场景：数据获取和分布式计算。对于数据获取，他们考虑了一种阈值模型来保证数据感知的有效性，并且所有的参与者共享预设的报酬。对于分布式计算的场景，他们设计了一种基于契约理论的机制来适应参与者的多样性。另外 Li 和 Cao[35] 在激励机制设计中考虑了隐私保护的目标。另外，还存在一些特殊目的机制设计。Koutsopoulos[36] 研究了一种随机化的激励机制，在保证能够达到某一阈值的数据感知服务质量级别的情况下，最小化付给参与者的报酬。在参与者估值的概率分布已知的情况下，Luo 等人[37] 设计了一种最大化期望收益同时满足理性人约束的激励体系。这些提

及的机制均为离线机制，即众包者获取所有的信息后再进行参与者选择。而一些在线机制也有被研究与讨论，Zhao 等人[38]就设计了在线的激励机制，每个参与者到达时，众包者必须就现有信息立即给出该参与者的胜出结果。

在与数据直接共享相对的数据价值共享方面，与本文的研究对象 (数据价值共享模式) 最为相近的概念是联邦机器学习。Google 于 2018 年提出联邦机器学习的概念，并设计了名为 Gboard[39] 的虚拟键盘应用。在相似的研究方向上，Yang 等人[40] 进一步讨论了联邦学习的概念、架构以及潜在应用。在优化方向上，Wang 等人[41] 将深度增强学习和联邦学习框架融合进网络边缘的移动设备来实现移动边缘学习、缓存及通信优化。Tran 等人[42] 提出了无线网络联邦学习的优化问题，以获得较优的训练时间、精确度和能量损耗。Samarakoon 等人[43] 使用联邦学习来估计网络队列的尾端概率分布，从而最小化网络负担，同时保证车辆系统之间的可靠低时延通信。在框架安全相关的研究方向上，Shayan[44] 认为移动设备可能会利用泄露的信息对联邦学习的模型进行污染攻击，或者直接破坏其他移动端参与者。针对该问题，他们使用了拒绝负面影响防护模式 (RONI) 来阻止模型的破坏，另外使用差分隐私模式来进行隐私保护。该模型被实现在区块链系统中。类似得，Kim 等人[45] 以区块链来存储验证本地的模型更新，他们还分析了端到端的学习完成时延来优化区块产生的速率。Fung 等人[46] 介绍了女巫攻击，然后以参与者的贡献相似度来识别这些恶意攻击。这些与联邦学习算法相关的研究大多是关于性能优化：模型学习时间或者模型学习安全。他们大多有着相似的假设：参与者总是无条件地为联邦学习提供数据、通信及计算资源[40]。而这样的假设是不符合实际场景的。Nishio and Yonetani[47] 考虑了资源受限和参与者选择的问题，但是其忽略了参与者的可靠性因素。在没有合适激励机制的情况下，资源丰富的数据拥有者往往不愿意参与模型学习。

1.3 本文的研究目标与研究内容

由相关领域的研究历史及现状可知，激励机制已经被应用于科学与应用的诸多方面。在众包领域有大量的激励机制，但他们大都是针对移动场景设计，并且是数据直接共享，与本文数据价值共享场景不符，因而相关激励机制无法直接使用。在与本文的数据价值共享概念极为相似的联邦学习领域，相关研究却主要着眼于联邦学习算法性能和使用安全，对于激励机制的研究极少。另一方面，联邦学习建立在同态加密技术之上，数据会加密后进行传输，并且需要借助第三方做数据交换。若在更加严格的数据使用限制环境内，加密传输也被禁止。那么联邦学习的思想并不完全适用于本文场景。因而本文需要抽象出理想的数据价值共享

模式，以此为基础挖掘数据价值共享流程中的细节信息，并设计不同应用场景中的激励机制。从而鼓励“数据孤岛”之间互联互通，在受限的数据暴露程度下使用数据，充分创造新的价值。确切地说，主要有以下三个研究点：

1. 简述理想的多方数据价值共享计算模式，该计算模式需要完全保证参与者的数据不发生转移。分析该模式中简单可并行计算场景的特点及相关限制，对问题进行建模，应用拍卖理论，求解具体的优化问题，设计具有计算有效、真实、社会福利最大等优秀性质的激励机制，提高数据拥有者的参与度。
2. 从多方数据价值共享计算模式的依赖相关计算场景出发，对问题进行建模，深入剖析该场景的重要限制指标。对核心问题进行优化求解。设计具有计算有效、真实、社会福利最大等优良性质的激励机制，提高数据拥有者的积极性。同时完成该场景下的最优机制的设计，提高任务方的收益。实施模拟实验对算法性能进行论证分析。
3. 实现多方数据价值共享拍卖系统，将上述算法及机制进行实装，验证其性能及有效性。

1.4 本论文的结构安排

本文的章节结构安排如下：

第一章，分析本文的研究背景和研究意义，论述本题相关领域的算法及应用的国内外研究历史和现状。确定本文的研究目标与研究内容，最后对全文章节结构进行梳理。

第二章，介绍本文用到的相关理论。主要是机制设计和拍卖理论。

第三章，介绍理想的数据价值共享计算模式——多方数据价值共享计算。针对简单可并行的具体计算场景做机制设计。对核心最优化问题进行形式化建模、分析求解。其共有三个来自于应用场景的具体约束：1、数据量约束。2、指标集约束。3、机构约束。最后以实验说明机制的性能。

第四章，研究依赖相关计算的激励机制设计问题。考虑计算时间限制在该场景下的重要意义，对问题进行详尽的论述分析。对核心最优化问题进行形式化建模求解。然后给出该场景对应的最优机制。最后，进行模拟实验，论述算法的性能和有效性。

第五章，实现数据价值共享拍卖系统，将上述算法部署至应用环境。给出总体设计、模块设计。最后对应用系统的功能界面进行展示。

第六章，对全文进行总结陈述，分析本文的工作可取之处与不足，并展望后续工作的可能研究方向。

第二章 相关理论基础

本章介绍本文研究涉及的相关理论基础，主要是机制设计与拍卖理论。只有在这些理论基础上才能结合具体场景，设计性质良好的激励机制。

2.1 机制设计

日常生活中会有许多需要策略决策的场景，例如卖出一台二手电视机，但此时其价格难以确定。又或者需要确定在办公室购置一台新的电冰箱，而同事们愿意为这个冰箱各自付出多少经济支持也是未知的。那么确定是否购入冰箱的策略可能是依次去询问他们，并告诉后面的人前面的人的估值。也可以同时询问所有人的估值来判断是否购入冰箱。当然，两种模式产生的效果是不同的。这两种模式都在参与者中引入了一种非合作性的策略博弈。参与者知道博弈的结果不仅取决于自身的选择，也取决于其他人的策略。因而每个参与者自身的最优策略依赖于其他参与者的策略。机制设计理论因此建立于博弈论。博弈论以游戏的规作为输入，对策略玩家的表现进行预测。而机制设计是关于选择游戏的最优规则。更确切得说，机制设计是关于多个参与者的隐藏信息，在二手电视机的问题中，它是各个买家参与者对这台电视机的内心真实估值。而在冰箱问题中，它是同事对新冰箱的真实购买意愿。机制规则一旦被确定后，便不再更改，无论是参与者还是设计者。这是机制有效运行的基础。

2.1.1 简单拍卖及理想机制

本节简要介绍二价拍卖相关的简单拍卖机制及理想机制概念。

2.1.1.1 单物品拍卖

考虑现有一个卖家，仅有一件物品需要卖出。同时有 n 个潜在的买家需要购买该物品。为了对买家的策略进行推断，需要一个模型来描述买家的收益。第一个关键假设是每个买家都有一个非负的估值 v_i，来表征他对该物品的真实购买需求程度。在现实场景中，人的真实购买需求意愿是不断变化的。但在此模型中，对于每个买方，其真实估值 v_i 被认为是不变且私密的，即除了该买家自己，卖方和其它买方都无法获得其真实值。买家的效用函数模型为：$u_i = v_i - p_i$，若买家获得该物品;0，若买家未获得。这被称为准线性效用模型，本文也采用该模型来描述各个参与者的效用。

2.1.1.2 最高价拍卖

对于单物品拍卖，其流程大致是：

1. 买方给出密封标的 b_i
2. 确定胜出者，并将物品分配给胜出者。
3. 买方向卖方支付价格 p_i

其中，第二步的最简单实现是直接将物品分配给标的最高的买方。而第三步价格的确定，可以有多种选择，例如直接向卖方支付胜出者的标的价格 (称为最高价拍卖)，或者次高价格，亦或是直接令支付价格为 0。在不同的价格机制下，买方都会制定相应的标的策略来使自己的效益最大化。因而买方的行为及拍卖的结果都会随着价格机制的变化而变化。

最高价拍卖是常见的拍卖类型，在许多藏品流通、地产交易等市场均有广泛的应用。然而最高价拍卖，尤其是密封拍卖，是一种难以分析推理的拍卖模式。作为一个参与者，在准线性效用下，难以找到使自身收益最大的标的策略。因为在直接显示的机制下，无论参与者是胜出还是失败，其效用均为 0。相应的，作为一个卖方，或者是机制设计者，很难预测系统的整体局面及结果。

2.1.1.3 二价拍卖与占优策略

另一种同样应用广泛且极其重要的拍卖机制是二价拍卖，也称 Vickery 拍卖。其实一种密封拍卖机制：最高标的者作为胜出者获得物品的分配，并向卖方支付除其自身标的以外的最高标的价格。为了描述这种拍卖机制的优良性质，此处给出占优策略的简单定义。

定义 2.1 (占优策略) 无论其他参与者如何投标，该参与者的一种策略 (即标的)，都能够最大化其效用。

于是，二价拍卖的激励特点如下所示。

推论 2.2 (二价拍卖中的激励) 在二价拍卖机制中，每个参与者 i 都有一个占优策略：使标的 bid_i 等于其对物品的真实估值 v_i。

二价拍卖的另一个重要特点是，一个真实表达估值的参与者不会在二价拍卖中受损。这可以鼓励更多的真实表达的参与者加入到拍卖环节中。该特点也被称为个人理性约束。

推论 2.3 (效用非负性) 在二价拍卖机制中，每个真实投标的参与者都能够保证其效用非负。

2.1.1.4 理想机制

从二价拍卖中可以归纳总结出性质良好的机制的特点，应用至更加广泛的机制设计中。首先，给出相关概念的定义。

定义 2.4 (占优策略激励相容 (Dominant-Strategy incentive Compatible)) 在一个机制中，若对每个参与者来说，真实的投标总是其占优策略，并且任意真实投标的参与者总能获得非负的效用。那么这个机制被称为具有占优策略激励相容的特性。

然后是拍卖中关于社会福利的定义。这个概念体现了拍卖机制的有效性及积极意义，若最大化社会福利对应着将物品分配给真正需要的人。

定义 2.5 (社会福利) 单物品拍卖中的社会福利定义为：$\sum_{i=1}^{n} v_i x_i$，若参与者 i 胜出，则 $x_i = 1$, 否则 $x_i = 0$。

由前述的定义可以得出理想机制的特点，这也是本文需要着重研究设计的激励机制特性。

1. **强激励保证**：该机制满足占优策略激励相容 (*DSIC*)
2. **有效性保证**：该机制满足社会福利最大化
3. **计算有效性保证**：该机制可以在多项式时间内实现

这三种性质都是极为重要的。从参与者的角度来说，DSIC 的特性使得其可以很容易的选择标的来参与到机制中。这泯灭了有高级参与者和初级参与者之间的经验差异。从卖方或者是机制设计者的角度来看，DSIC 的机制特性使得推断机制的结果局面变得更为容易可行。值得一提的是，任何机制局面的推断都依赖于对参与者行为的假设。在一个 DSIC 的拍卖机制中，仅有的假设是参与者以占优策略参与到拍卖环节。这是一个关于参与者行为的弱假设。这也符合真实的理性人的一般行为，有利于设计研究的激励机制应用到真实应用场景并取得较优的性能结果。

DSIC 特性是值得采纳和研究的，然而 DSIC 的机制设计空间仍然较大。例如，一个随机赠予的拍卖机制也符合 DSIC 的特性。因为，参与者给出的非真实标的无法增加其获胜的可能性。然而，分配规则一旦不依赖于参与者的标的，会造成机制的有效性丧失，无法提升系统整体性能。此时，社会福利最大的特性就显得尤其重要。二价拍卖机制在解决社会福利最大的同时，保证了 DSIC 的性质，并在线性时间复杂度内求解。因而其是一种性质优秀的理想机制典型。

2.1.2 麦尔森引理

本节介绍麦尔森引理，其是本文工作的重要理论基础。

2.1.2.1 单变量环境

如前文所述，机制设计关注的是参与者自身的隐藏信息。而以隐藏信息做分类，可以将机制设计的情形划分为单变量环境与多变量环境。直观上来讲，单变量环境指的是各个参与者的私密信息是单个值。在单变量环境中，麦尔森引理是确定价格的有力工具，而与多变量环境相对应的是 VCG 机制。

2.1.2.2 引理表述

一个机制以参与者的标的 $\boldsymbol{b}$ 作为输入，然后确定胜出者及相应的分配 $\boldsymbol{x}$，x_i 是分配给参与者 i 的物品数量。最后确定需要支付的价格 $\boldsymbol{p}$,p_i 是参与者 i 的价格。而单变量环境下 DSIC 机制的设计可以简单的归纳为对分配规则 $\boldsymbol{x}(\boldsymbol{b})$ 和价格规则 $\boldsymbol{p}(\boldsymbol{b})$ 的确定，保证激励机制的有效性。麦尔森引理确定了机制的分配函数与价格函数之间的数量关系。然而并非所有分配函数都可以设计为拥有前述优良性质的激励机制。首先给出关于分配函数的两个定义。

定义 2.6 (可实施的分配规则) 一个分配规则 $\boldsymbol{x}$ 是可实施的，当且仅当存在一个价格规则 $\boldsymbol{p}$，使得直接显示机制 (x,p) 满足 DSIC 的性质。

由上述定义可知，可实施的分配规则是那些可以扩展为 DSIC 机制的分配规则。等价地说，DSIC 机制在分配规则上的投影也满足可实施的性质。若机制设计的目标是一个 DSIC 的机制，那么其目标范围需要限制在可实施的分配规则这个集合内。这相当于是机制设计的可行集。

定义 2.7 (单调分配规则) 单变量环境下的一个分配规则 x 被称为是单调的，当且仅当对于任意参与者 i 以及任意 $\boldsymbol{b}_{-\boldsymbol{i}}$（表示除 bid_i 分量以外的总标的向量），分配规则 $x_i(z,\boldsymbol{b}_{-\boldsymbol{i}})$ 是关于 $agent_i$ 的标的 z 的单调不减函数。

单调分配规则的含义是：对于任意参与者 i，增加标的只会使其得到的分配增加。

接下来正式给出麦尔森引理的内涵。

定理 2.8 (麦尔森引理) 在单变量环境中：

1. 一个分配规则 $\boldsymbol{x}$ 是可实施的，当且仅当他是单调的。
2. 若分配规则 $\boldsymbol{x}$ 是单调的，则存在唯一支付规则 $\boldsymbol{p}$，使得直接显示机制 $(\boldsymbol{x},\boldsymbol{p})$ 是 DSIC 的，且 $p_i(\boldsymbol{b})=0$，当 $b_i=0$
3. 上述支付规则可以由以下公式求得。

$$p_i(b_i,\boldsymbol{b}_{-\boldsymbol{i}})=\int_0^{b_i} z\cdot\frac{d}{dz}x_i(z,\boldsymbol{b}_{-\boldsymbol{i}})dz$$

麦尔森引理是后文机制设计的基础。第一条表述了可实施规则和单调规则的

的充要性。这极大方便了对 DSIC 的机制设计流程，同时缩小了设计空间。此时只需考虑满足单调性的设计规则。而通常分析分配规则的单调性是远比分析其可实施性来得容易。第二条的含义是支付规则的唯一性。这与第三条支付规则的具体计算方法结合起来就能得到完整的直接显示 DSIC 机制 (x,p)。因而麦尔森引理完整描述了单变量环境下的 DSIC 机制设计的流程和基本方法，并给出了充要条件下的设计范围，是一个极为有效的理论与实践工具。这也是本文针对具体应用场景进行激励机制设计的重要理论基础。

下面再给出离散条件下支付规则的计算方式。

$$p_i(b_i, \boldsymbol{b}_{-\boldsymbol{i}}) = \sum_{j=1}^{l} z_j \cdot [x_i(\cdot, \boldsymbol{b}_{-\boldsymbol{i}}) \text{在} z_j \text{处的阶跃值}] \tag{2-1}$$

因而，设计理想机制的一般流程是：

1. 假设所有参与者已经真实的给出标的，即 $\boldsymbol{b} = \boldsymbol{v}$
2. 以 $\boldsymbol{b}$ 进行社会福利最大化或者其他目标函数的求解，得到分配规则 $\boldsymbol{x}(\boldsymbol{b})$
3. 验证分配规则 $\boldsymbol{x}(\boldsymbol{b})$ 的单调性
4. 应用麦尔森引理给出支付规则 $\boldsymbol{p}(\boldsymbol{b})$

2.1.3 背包拍卖及算法机制设计

在前述的简单拍卖机制的基础上，机制所面临的场景可能会变得越发复杂。此时，希望在单变量环境中设计的机制仍然具有 DSIC，社会福利最大化，计算有效等优秀的激励性质。一般来说，场景的复杂性增加主要体现在社会福利最大化的问题上。接下来的机制求解过程中就将面临 NP-hard 难度的问题求解。为了保证机制的计算有效性，这些 NP-hard 困难问题往往在可以接受的范围内被近似求解。而社会福利最大化近似求解可能带来分配规则不单调的严重后果。由麦尔森引理可知，这样的近似算法对应的分配规则是无法被扩展为一个有效的直接显示 DSIC 机制的。

背包拍卖是另一种单变量环境的例子，其在资源分配领域有较多应用。在一个背包拍卖中，每个买方 i 拥有尺寸 w_i(公共知识) 以及一个私有秘密估值 v_i。卖方或者平台方拥有容量 W。可行集被定义为 0-1 向量 $(x_1, ..., x_n)$，使得 $\sum_{i=1} nw_i x_i \leq W$。其中，如同前文简单拍卖的场景，$x_i = 1$ 意味着参与者 i 是一个胜出者。由此可知，在资源容量受限且共享的情况下，卖方和买方之间可以很容易的形成背包拍卖模型。例如，每个买方的尺寸 w_i 可以代表商业公司的视频广告时长，而私密估值是其对于该广告在具体的平台或者活动中进行播放所愿意支付的真实价格。而容量

W 可以认为是平台或者活动中可允许的广告总时长。存储硬件共享问题、数据流分配问题、计算时隙分配等一系列与有限资源分配及共享相关的问题均可能被建模为背包拍卖进行求解。

2.1.3.1 分配规则的定义

首先给出背包拍卖中社会福利最大对应分配规则的定义。

定义 2.9 (背包拍卖对应的分配规则)

$$\boldsymbol{x}(\boldsymbol{b}) = argmax_X \sum_{i=1}^{n} b_i x_i$$

由上述定义可知，在参与者真实地给出标的时，社会福利最大化问题等价于一个 0-1 背包问题。可以证明可以精确求解上述社会福利最大对应的分配规则一定满足单调性的需求。

2.1.3.2 临界标的

在背包拍卖中，买方的分配函数被限制于 0-1 向量，因而买方的分配值 x_i 只能是 0 或者 1。由麦尔森引理中支付规则的离散形式2-1可知，每个买方所需支付的价格仅取决于临界标的——该买方由失败者转换为胜出者的下确界标的。这与前文的二价拍卖机制的价格制定是相似的。

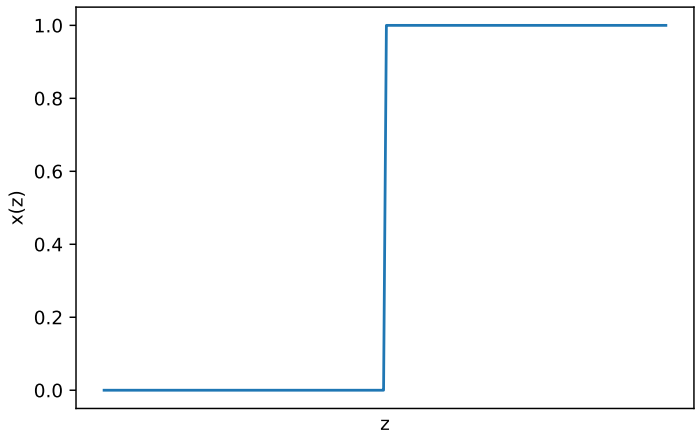

图 2-1 临界标的的示意

2.1.3.3 社会福利最大化带来的问题

前文中提及的理想机制主要满足 DSIC、社会福利最大化、计算有效性特性。然而在背包拍卖中难以完全实现。因为背包问题属于 NP-hard 问题，难以在多项

式时间内准确求解，除非 $P = NP$。所以社会福利最大化特性和计算有效性不可兼得。为了解决两者的冲突性，放松 DSIC 的限制并不能带来任何帮助。若放松社会福利最大化的限制，保证计算有效性，可以通过近似算法在多项式时间内求解社会福利最大问题，但这可能使分配规则单调性被破坏。若放松计算有效性的限制，可以通过动态规划算法在伪多项式时间内对该问题求解。这在问题规模较小或者有较大的算力的条件下是极好的，因为社会福利最大化被精确求解，对应的分配规则一定是单调的，可以被扩展为 DSIC 机制。

2.1.3.4 启发式算法

利用现有的近似算法，可以得到一个背包拍卖的启发式算法，该算法可以在真实投标的情况下，达到最优社会福利的至少 50%。

算法 2-1 基于贪心思想的背包问题启发式算法

1 对买方根据各自 $\frac{b_i}{w_i}$ 指标进行降序排列，使得 $\frac{b_1}{w_1} \geq \frac{b_2}{w_2} \geq \cdots \geq \frac{b_n}{w_n}$;
2 以上述序列依次选择胜出者，直到背包无法继续装下，得到胜出者集合 *Winners*;
3 比较最高标的的买方作为唯一胜出者的社会福利与集合 *Winners* 的社会福利，返回较大的那个作为最终的胜出者。;

2.1.3.5 算法机制设计

算法机制设计是算法博弈论中研究较为广泛的一个分支。背包拍卖也是该领域的研究对象之一。算法机制设计的主要模式是尽可能少地放松理想机制中的社会福利最大化限制条件，同时满足 DSIC 和计算有效性的限制。于单变量环境而言，麦尔森引理将此任务归约至对于具有多项式时间和单调性的分配规则的设计，同时减少社会福利的损失。

算法机制设计与近似算法领域的诸多相似性可能也是其在过去十几年取得较多进展的原因之一。近似算法的主要研究目标是为 NP-hard 问题设计一种尽可能最优的多项式时间算法。算法机制设计往往也有类似的目标，唯一不同之处是额外需要一个单调性的限制条件。那么，算法机制的设计就被限制于一个可计算模型的设计了。

显示定理可以进一步扩大 DSIC 机制的有效应用范围。

定理 2.10 (DSIC **机制的显示定理**) 对于任意机制 M, 若每个参与者总是有一个占优策略，那么一定存在一个与 M 等价的直接显示 DSIC 机制 M'

上述定理中的等价意味着，对任意参与者估值向量 $\boldsymbol{v}$, 直接显示机制 M' 的结果

(价格和分配) 与参与者执行占优策略下的机制 M 的结果是一致的。这也说明若要设计具有占优策略的机制，只需要考虑 DSIC 机制。

如图2-2所示，对于任意一个具有占优策略的机制 M，都可以构建一个以真实估值作为标的输入然后执行各个参与者的占优策略，并最终得到与机制 M 完全一致结果的直接显示 DSIC 机制 M'。

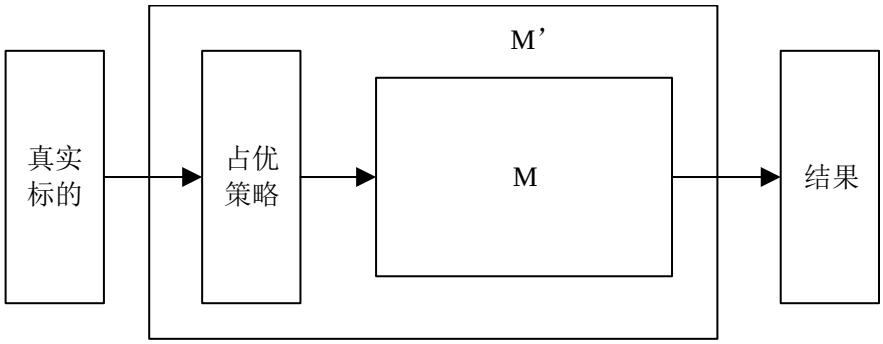

图 2-2 DSIC 机制显示定理的示意

若考虑放松 DSIC 的特性，会损失掉机制的强激励属性。例如在参与者不具有占优策略的机制中，机制设计者需要设定更强的对参与者策略及行为的假设，然后以此判断机制的结果。例如，可以考虑在已知各个参与者私密估值的先验分布的情况下，分析具有贝叶斯纳什均衡的机制。在一些特殊场景需求下，非 DSIC 机制或许能够取得一些额外的性质。而在较一般的场景中，DSIC 的激励特性是极有价值的。

2.1.4 税收最大化拍卖

在前面的机制设计中，社会福利最大化需要求解的目标函数，可以准确求解或者近似求解。卖方的收益在这样的机制中是没有着重考虑的。但是在实际应用中，卖方希望尽可能最大化自身收益是一个极为合理的场景需求。

2.1.4.1 贝叶斯分析

为了比较不同拍卖机制，需要一个模型来衡量这些机制在不同的真实估值向量下的税收和。经典的方法是采用贝叶斯分析。考虑这样一个模型：

- 单变量环境，且对任意 i 及任意可行解 $(x_1, x_2 ..., x_n) \in X$ 存在一个常数 M, 使得 $x_i \leq M$。
- 独立的分布 $F_1 ... F_n$, 以及对应的连续概率密度函数 $f_1 . . f_n$。假设参与者 i 的私有估值 v_i 来自于分布 F_i，且分布 F_i 存在有限一阶矩。

另外，机制设计值知道分布 $F_1, F_2, F_3, ..., F_n$，而参与者不知道。

定义 2.11 **(期望税收)** 对于一个 DSIC 机制 (x,p)，其期望税收为

$$\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\sum_{i}^{n}p_i(\boldsymbol{v})\right] \tag{2-2}$$

其中 $F=F_1\times...\times F_n$。直观来看，直接最大化上式是相对困难的。因而给出虚拟估值的定义。

2.1.4.2 虚拟社会福利

定义 2.12 **(虚拟估值)** 对于参与者 i，其估值及其对应分布分别是 v_i,F_i，则其虚拟估值定义为：

$$\phi_i(v_i)=v_i-\frac{1-F_i(v_i)}{f_i(v_i)} \tag{2-3}$$

由上述定义可知，参与者的虚拟估值仅依赖于他的真实估值与其对应概率分布，而不依赖于其他参与者的信息。然后给出一个引理，该引理是最优拍卖理论的基石。

引理 2.13 对于任意单变量环境、任意概率分布 $F_1,F_2...,F_n$、任意 DSIC 机制 $(\boldsymbol{x},\boldsymbol{p})$、任意参与者 i、任意其他参与者的估值 $\boldsymbol{v_{-i}}$,

$$\boldsymbol{E}_{v_i\sim F_i}[p_i(\boldsymbol{v})]=\boldsymbol{E}_{v_i\sim F_i}[\phi_i(v)\cdot x_i(\boldsymbol{v})] \tag{2-4}$$

上述引理的含义为：任意参与者支付 p_i 的期望等于该参与者所获得的虚拟价值 $\phi_i(v)\cdot x_i(\boldsymbol{v})$ 的期望。

基于引理2.13, 可得如下重要定理。

定理 2.14 **(期望税收等于期望虚拟社会福利)** 对于任意单变量环境、任意估值的概率分布 $F_1,...,F_n$，任意 DSIC 机制 $(\boldsymbol{x},\boldsymbol{p})$，

$$\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\sum_{i}^{n}p_i(\boldsymbol{v})\right]=\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\sum_{i}^{n}\phi_i(v_i)*x_i(\boldsymbol{v})\right] \tag{2-5}$$

上述定理的重要意义在于，其在相同的分配规则可行集内，将难以直接最大化的期望税收转化依赖于分配函数的最大化期望虚拟社会福利。在式2-5中，着重考虑等式右边的部分 $\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}[\sum_i^n\phi_i(v_i)*x_i(\boldsymbol{v})]$。对于概率分布 $\boldsymbol{F}$ 及虚拟估值 $\phi_i(v_i)$，机制设计者是无法控制或者改变的。只有分配规则 $\boldsymbol{x}(\boldsymbol{v})$ 由机制设计者制定。为了最大化期望虚拟社会福利，可以对前式取关于 $\boldsymbol{v}$ 的条件期望，得到

$$\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\boldsymbol{E}\left[\sum_{i}^{n}\phi_i(v_i)*x_i(\boldsymbol{v})\middle|\boldsymbol{v}\right]\right] \tag{2-6}$$

原问题则转化为对相应条件期望的最大化，由上式可知，这等价于选择使虚拟社会福利 $\sum_i^n \phi_i(v_i) * x_i(\boldsymbol{v})$ 最大化对应的分配规则。

值得注意的是，上述分配规则必须满足单调性，否则前述定理的前提条件 $(\boldsymbol{x}, \boldsymbol{p})$ 是 DSIC 机制无法被满足。为了说明虚拟社会福利对应分配规则的单调性，有如下定义。

定义 2.15 (正规分布) 若虚拟估值函数 $v - \frac{1-F(v)}{f(v)}$ 是非单减的函数，则概率分布 F 称为正规分布。

进一步可知，若所有参与者的估值分布 $F_1, F_2, ..., F_n$ 均是正规分布，则虚拟社会福利最大化对应的分配规则一定是单调的。从而上述税收最大化的设计可以完成其闭环流程，如下所示：

算法 2-2 期望税收最大化

1 假设：每个参与者估值的分布 F_i 均为正规分布;
2 将每个参与者的真实估值 v_i 转化为虚拟估值 $\phi_i(v_i)$;
3 在可行集中选择可行解 $\boldsymbol{x}$ 使得虚拟社会福利最大化 $\sum_i^n \phi_i(v_i) * x_i(\boldsymbol{v})$;
4 根据麦尔森引理计算支付向量 $\boldsymbol{p}$;

上述流程为单变量环境下，期望税收最大化即最优拍卖的一般设计流程。

2.1.5 多变量环境

前面的理论以单变量环境为基础，参与者的隐藏信息为单个值。而更一般的是多变量环境，即参与者的隐藏信息为多个值。在一般的多变量机制中有：

1. n 个策略性的参与者
2. 有限的结果集合 Ω
3. 每个参与者 i 具有私密的非负估值函数 $v_i(\omega), \omega \in \Omega$。

此时的社会福利被定义为 $\sum_{i=1}^n v_i(\omega)$。在多变量环境中有重要的结论：

定理 2.16 任意多变量环境都存在一个社会福利最大化的 DSIC 机制。

该 DSIC 机制被称为 VCG 机制，其分配规则和支付规则分别为：

$$\boldsymbol{x}(\boldsymbol{b}) = argmax_{\omega \in \Omega} \sum_{i=1}^{n} b_i(\omega) \tag{2-7}$$

$$p_i(\boldsymbol{b}) = \left(\max_{\omega \in \Omega} \sum_{j \neq i} b_j(\omega) \right) - \sum_{j \neq i} b_j(\omega^\star) \tag{2-8}$$

其中，$\omega^{\star}$ 是上述分配规则选出的结果。在多变量环境下，由于 VCG 机制的存在，似乎优秀激励性质的机制设计变得可行。然而事实并非如此。一方面，其最大化社会福利问题基本都是 NP-hard 问题，难以有效实现。每个参与者标的的长度随问题规模呈指数级增长，存储、传输这些多维的标的也将带来极大的时空花费。另一方面，VCG 机制仅能保证社会福利最大，而在税收等其他方面并不具有更多的优秀性质。

2.2 本章小结

本章介绍了二价拍卖、麦尔森引理、最优拍卖、背包拍卖等算法机制设计中的关键概念, 为后文针对具体场景进行机制设计及分析做准备。

第三章 简单可并行数据价值共享计算的激励机制

本章介绍了理想的多方数据价值共享计算模式，针对简单可并行场景提出多约束价值共享激励模型。主要对数据量约束、指标集约束、机构约束三种问题进行分析，设计社会福利最大化的 DSIC 拍卖机制。

3.1 多方数据价值共享计算模式

现有的大数据应用模式与数据使用安全问题存在不可调和的矛盾。一方面，大数据创造的价值依赖于数据整合并较好地应用相关数据挖掘算法。而整合意味着开放，开放必然引入隐私安全隐患。为此，本节介绍一种理想的多方数据价值共享计算（在后文的分析中可能简称为多方计算）模式。该模式并不直接整合数据，而是对计算任务进行分解拆分，使之能够在各数据中心（本节以数据中心作为数据拥有者的代表）本地完成相应的分布式计算，并将计算结果传输给控制节点。这些计算结果不会引入原始数据的泄露风险。然后由控制节点实现结果的整合。对于复杂的计算问题，该过程可能包含若干次迭代操作。

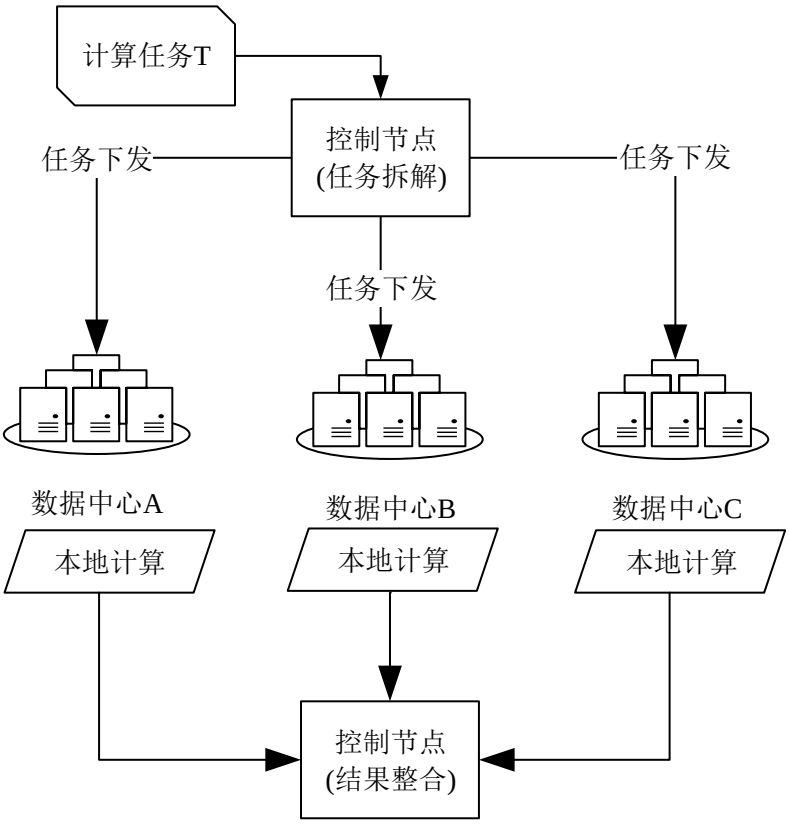

图 3-1 多方数据价值共享计算示意

值得注意的是，该计算模式中，各个数据中心的计算任务仅依赖于本地数据，即数据本身分布于各地且在整个计算过程中不通过网络传输或者转移。这可以有力保证数据的隐私安全性。如何将计算任务 T 根据现有数据分布进行子任务切分是控制节点的问题，本文并不对此进行说明，只是假设控制节点可以有效地完成此任务。

对于各个数据拥有者 (如图3-1中的数据中心) 来说，参与到多方价值计算模式必然给自身带来损失。系统的设计者需要给予经济奖励，来激励更多的数据价值共享。而随着参与者的增多，提供相同计算内容的参与者之间的竞争增加，如何选择胜出者并确定价格体系是一个重要问题。胜出者选择混乱或者价格体系不当会破坏理性参与者的积极性，降低系统的价值共享性能。因而需要设计公平合理的机制来保证系统的有效运行。

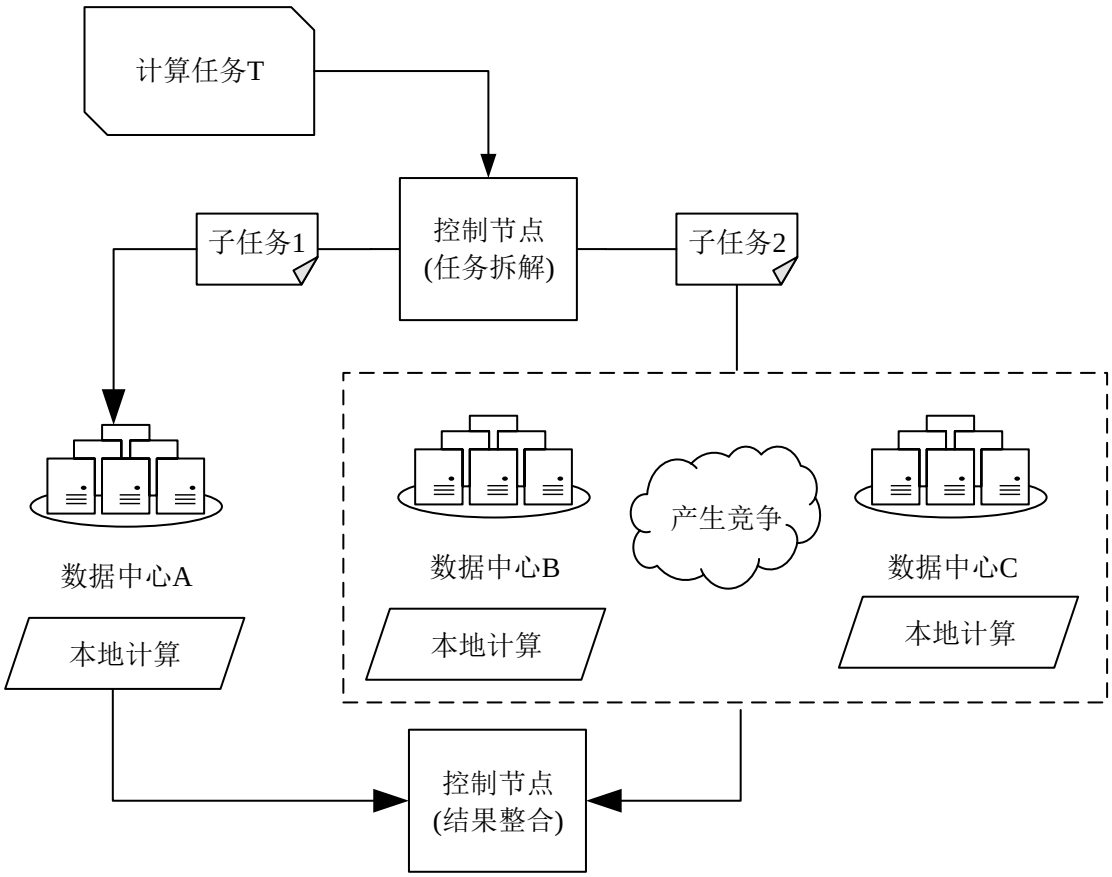

图 3-2 多方数据价值共享中的竞争

如图3-2所示，数据中心 B 和数据中心 C 都可以在依赖于本地数据的情况下提供对子任务 2 的计算，此时两者产生竞争，如何确定最终执行子任务 2 的数据中心并确定支付给该数据中心的报酬是一个核心问题。而本文的后续内容主要是针

对该数据价值共享模式，在不同计算场景下进行相应的机制设计。

3.2 多约束价值共享激励模型

在多方数据价值共享计算模式中，针对简单可并行的计算场景，本节提出多约束价值共享激励模型。

3.2.1 问题描述

在简单可并行数据价值共享计算（后文可能简称为简单可并行计算）场景中，上述多方计算任务 T 可以被控制节点根据现有的数据分布情况划分为一定数量的子计算任务。这些依赖于本地数据的子计算任务可以在各个数据中心完全并行的完成，然后由控制节点对计算结果进行一次整合得到原任务的解。可知，这些子计算任务大多是同构的 (例如，对图片数据进行特征提取)。每个子计算任务称为一个单位 (unit) 的多方计算。

根据场景的复杂性，拍卖模型中需要引入多种限制条件来满足各方实际需求。其最基本的是数据量约束，即任务方表达其对多方计算任务的具体数量需求。

可知数据量约束是本场景下基础而重要的指标，但其不一定能够满足所应用需求。作为数据价值的使用者，任务方可能会对数据价值共享流程提出一些额外的限制约束条件。例如：任务方认为越多的胜出者承担一项多方计算任务，可能带来越大的数据安全风险，并降低数据结果的可靠性。于是，其出于计算来源多样性的需求要求竞拍胜出者的数量不能超过某给定阈值；或者其要求多方计算任务的总体响应时间不能大于给定目标值。在本场景中，参与者会被赋予不同的信誉及可靠性评估等级。而任务方也可以根据自己对计算任务难易程度的估计，制定相应的限制条件。这些限制条件往往由限制指标来进行描述。限制指标的集合 *Limit* 是有限集。本文使用表3-1所示指标集。

表 3-1 限制指标集

指标名称	描述	符号	产生方式
一级参与者的数量阈值	来自信誉系统	$Parti_1$	由平台方或任务方确定
二级参与者的数量阈值	同上	$Parti_2$	由平台方或任务方确定
三级参与者的数量阈值	同上	$Parti_3$	由平台方或任务方确定
总体响应时间和	各个胜出者完成来自任务 *T* 所指派计算花费的时间总和	TIME	由平台方或任务方确定
计算需求量		datademand	任务 *T* 固有属性

上述指标集中，前三项来自于对参与者的信誉及可靠性评估等级。（本文不对

具体的信誉值计算方式做讨论。）它们是同类指标，以第一项为例，它意味着任务方要求任务的竞拍胜出者中一级参与者刚好有 $Parti_1$ 个。第四项指标衡量了多方计算任务的总体完成效率。*TIME* 值越小，意味平台方对于任务的响应要求越高，对于拍卖环节的限制也就更强。第五项 *datademand* 是来自于多方计算任务本身的需求，机制需要尽可能使 *datademand* 被满足，这里也将其视为任务方对计算任务分配过程的限制指标之一。上述限制条件被称为指标集约束。

在进一步具体的场景中，简单可并行计算任务分配的限制条件变得更为复杂。

一方面，简单可并行计算任务竞拍流程中参与者的真实角色是拥有计算资源及相应数据访问权限的计算节点。这些计算节点隶属于不同的部门机构。就相对严格而紧密的组织而言，其部门机构可能存在较为显著的上下级关系。这种关系最典型的案例是树形关系。如图3-3所示。在这种树形关系中，各机构可能会出于成本管理、机构职能、安全性保障等多方面因素对其自身及下属机构参与多方计算任务提出新的要求及限制。例如，表3-1所示的各种限制性指标。这些要求及限制形成每个机构的偏好信息。如图3-3，每个机构都拥有一个偏好信息描述。（图中只画出了机构 2 的偏好信息）

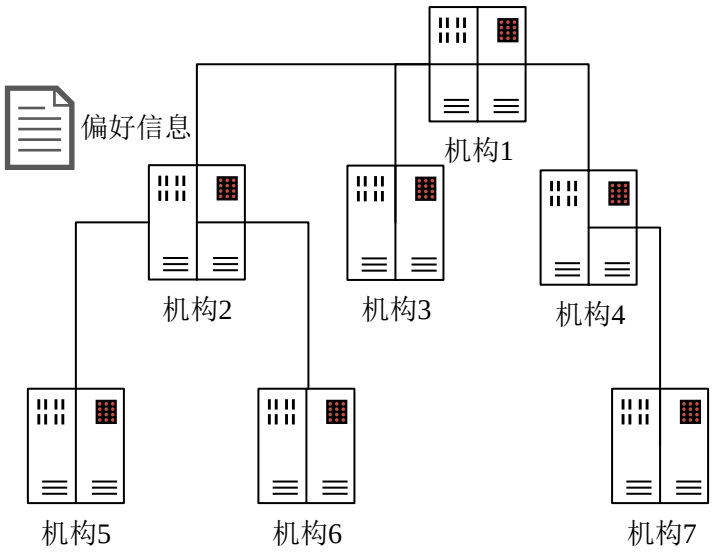

图 3-3 机构部门间的树形关系

另一方面，同一机构内部可能具有多个可提供计算能力的单元，他们具有相同数据源的访问权，但他们的计算能力、服务质量又不尽相同。当同一机构内部的不同计算单元作为参与者进入到简单可并行计算任务 *T* 的竞争环节中时，多个参与者可能提供的是内容相同而质量（响应时间、可靠性等）不同计算服务。相同的计算内容对于简单可并行计算任务 *T* 来说是冗余的。因此在上述场景中，这

些数据同质的参与者之间实质存在互斥关系。即在这些数据同质的参与者中，分配规则最多只能选择 1 个胜出者。同一机构可能拥有多个不同的数据源，因此在一家机构内部也可能存在多组这样的互斥关系。目前本文只考虑在来自一家机构的参与者中存在数据同质的现象。

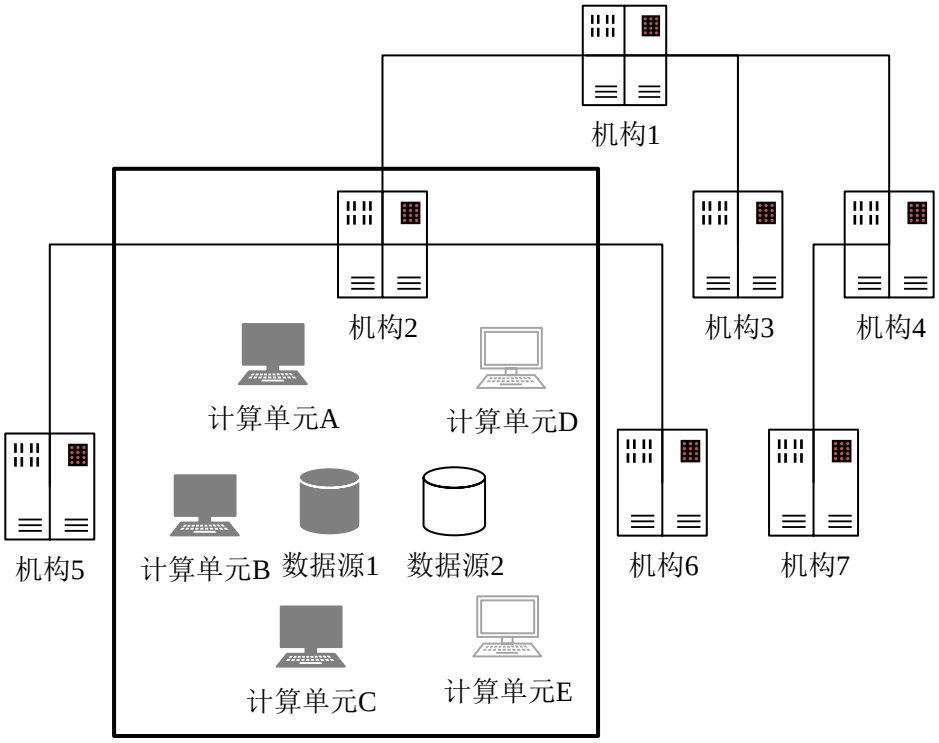

图 3-4 机构内部参与者的互斥关系示例

在图3-4的示例中，机构 2 的计算单元 A, B, C 拥有数据源 1 的访问权，计算单元 D, E 拥有数据源 2 的访问权。当这些计算单元参与至简单可并行计算任务竞争环节时，计算单元 A, B, C 及 D, E 中各自最多只能有一个胜出者。这种引入上下级组织关系及计算单元互斥关系的限制条件被称为机构约束。

而本章的目标是在上述三种具体约束条件下制定 DSIC 拍卖机制的分配算法和价格算法。

3.2.2 问题建模

首先给出相关合理假设：

- 假设 1：参与者是有限理性的个体，总是执行理性条件下最大化各自效用函数的策略，且不存在共谋。
- 假设 2：除参与者对简单可并行计算任务代价的内心估值为私密知识以外，其余均为公共知识，为平台方和其它参与者所知。

机制中以虚拟代币作为货币。机制中有 n 个参与者 ***agent*** 可以进入多方计算任务 T 的竞拍环节。多方计算任务 T 共需要 $datademand$ 单位的计算。对于 $1 \leq i \leq n$, 参与者 $agent_i$ 可以针对任务书 T 提供 $datacount_i$ 单位的多方计算任务。而参与者 $agent_i$ 拥有私密内心估值 $0 \leq val_i = INCENT - cost_i$，$INCENT$ 是平台方给予胜出者的每单位计算任务的固定奖赏，由多方计算任务发起者确定。$cost_i$ 是该参与者认购每单位多方计算任务的真实损失。$0 \leq cost_i \leq INCENT$，否则，参与者 $agent_i$ 应当退出此次竞拍来避免自己受损。于是，val_i 表示 $agent_i$ 对认购每单位多方计算任务带来的真实价值。其 val_i 只对参与者 $agent_i$ 可见，平台方及其余参与者不可见。在机制中，每个参与者会提交自己的标的 bid_i, 形成标的向量 ***bid***。分配函数 ***allocation***$(\boldsymbol{bid})$ 也是一个向量，描述了机制对每个参与者分配的多方计算任务单位数量。$agent_i$ 的效用函数为准线性函数 $utility_i = val_i * allocation_i - payment_i$。总社会福利 SW 定义为 $\sum_{i=1}^{n} val_i * allocation_i$, 其是所有参与者的效用函数与平台方收益的总和。即：$SW = \sum_{i=1}^{n} utility_i + \sum_{i=1}^{n} payment_i$。

本文的目标是设计参与者具有占优策略的拍卖机制。由显示定理可知，对于任意一个参与者具有占优策略的机制 M，总是存在一个等价的直接显示 (direct-revelation) 占优策略激励相容 (DSIC) 机制 M'。因此，本文在 $DSIC$ 机制的范围中寻找合适的解。而在前述定义中，参与者的私密值仅为其对认购多方计算任务收益的真实估值 val_i，且效用函数为准线性函数。这属于单变量环境，需要麦尔森引理来主导机制设计的流程。

对于数据量约束，假设所有参与者已经真实地表达多方计算任务的估值，并给出标的，即 $\boldsymbol{bid} = \boldsymbol{val}$。此时，社会福利最大化问题等价于最优化问题3-1。

$$\begin{aligned} \max_{\vec{allocation}} \quad & \sum_{i=1}^{n} bid_i * allocation_i \\ s.t \quad & 0 \leq allocation_i \leq datacount_i, \quad allocation_i = 0, 1, 2... \\ & \sum_{i=1}^{n} allocation_i = datademand \end{aligned} \tag{3-1}$$

接下来在前述定义的基础上引入指标集约束条件。$level_i \in 1, 2, 3$ 为 $agent_i$ 的信誉及可靠性评估等级。对于 $1 \leq j \leq 3$, 胜出者集合中第 j 级参与者数量 $= parti_j$。$timeperunit_i$ 是 $agent_i$ 关于 T 完成每单位简单可并行计算任务所花费的时间。$transmitcost_i$ 是 $agent_i$ 向平台方提交结果数据所花费的平均时间，主要由网络时延、吞吐量等因素决定。分配规则需要满足时效性要求指标：$\sum_{i=1}^{n} timeperunit_i * allocation_i + \boldsymbol{I}(allocation_i > 0) * transmitcost_i < TIME$。其中

$\boldsymbol{I}$(表达式) $=1$ 当且仅当表达式为真。否则 $\boldsymbol{I}(*)=0$。社会福利 SW 的定义仍然不变。

对于指标集约束，假设所有参与者已经真实地表达简单可并行计算任务的估值，并给出标的，即 $\boldsymbol{bid}=\boldsymbol{val}$，此时，社会福利最大化等价于最优化问题3-2。

$$\max_{\vec{allocation}} \quad \sum_{i=1}^{n} bid_i * allocation_i \tag{3-2}$$

$$\begin{aligned} s.t \quad & 0 \le allocation_i \le datacount_i, \quad allocation_i = 0,1,2... \\ & \sum_{i=1}^{n} allocation_i = datademand \\ & \left(\sum_{i=1}^{n} timeperunit_i * allocation_i + \boldsymbol{I}(allocation_i > 0) * transmitcost_i\right) < TIME \\ & \left(\sum_{i=1}^{n} \boldsymbol{I}(allocation_i > 0, level_i = j)\right) = parti_j, j = 1,2,3 \end{aligned}$$

更进一步，在前面的定义中增加机构的概念。机制中共有 m 个机构 $\boldsymbol{org}$，每个参与者 $agent_i$，$1 \le i \le n$ 隶属于一个机构。每个机构具有参与者偏好 $prefer_i$，描述了其对自身管辖的部门参与多方计算的限制条件。为了简化问题，偏好信息仅考虑如下限制：该机构及其管辖部门的参与者所提供的总计算任务不能超过 $limit_i$ 单位。所得分析结果及结论可以容易地推广至任意限制指标 $\le$ 某一阈值的更一般情况。机构之间形成森林结构，即对于 org_i，其最多仅有一个父亲节点。

$agentpinorg_i = \{agent_k | agent_k$ 属于机构$i\}$ 是隶属于机构 org_i 的参与者（计算单元）集合。该集合可以根据参与者对数据源的依赖关系被划分为 $datasourcenum$ 个子集，每个子集最多产生一名胜出者。

对于机构约束问题，假设所有参与者已经真实地表达多方计算任务的估值，并给出标的，即 $\boldsymbol{bid}=\boldsymbol{val}$。此时，社会福利最大化问题等价于最优化问题3-3。

$$\max_{\vec{allocation}} \quad \sum_{i=1}^{n} bid_i * allocation_i \tag{3-3}$$

$$s.t \quad 0 \le allocation_i \le datacount_i, \quad allocation_i = 0,1,2...$$

$$\sum_{i=1}^{n} allocation_i = datademand$$

$$\left(\sum_{i=1}^{n} timeperunit_i * allocation_i + \boldsymbol{I}(allocation_i > 0) * transmitcost_i\right) < TIME$$

$$\left(\sum_{i=1}^{n} \boldsymbol{I}(allocation_i > 0, level_i = j)\right) = parti_j, j = 1,2,3$$

$$\text{satisfy} \quad perfer_i \quad \text{and mutual exclusion in} \quad agentpinorg_i, 1 \le i \le m$$

3.2.3 分析及求解

现分别对上述三种约束限制问题进行分析及求解，给出相应的分配算法和价格算法。

3.2.3.1 数据量约束

对于数据量约束下社会福利最大化问题3-1，给出分配算法3-1，其时间复杂度$O(n)$。注：本文中数组下标均从 1 开始计数，且可以通过 first 和 second 来分别指代二元组的第一、二关键字。

算法 3-1 贪心求解数据量约束问题

Input: ***datacount***, ***bid***, *datademand*
Output: ***allocation***

$i \leftarrow 1$;
$total \leftarrow datademand$;
对二元组序列 $list = \{(bid_j, j) | 1 \le j \le n\}$ 以第一关键字进行降序排列，第一关键字相同的情况下，以第二关键字升序排列;
while $total > 0$ **do**
    if $i > n$ **then**
        datademand 单位的计算任务无法被分配完毕，返回错误信息。break;
    end
    $temp \leftarrow \min(total, \quad datacount_{list[i].second})$;
    $total \leftarrow total - temp$;
    $allocation_i \leftarrow temp$;
    $i \leftarrow i + 1$;
end

定理 3.1 算法3-1是问题3-1的解。

证明: 算法3-1的思想是在供应 *datademand* 有限的情况下，优先满足代价估值 bid_i 更大的参与者的需求。假设存在一个更优解 $S^1(SW^1 > SW)$ 与该思想相悖。即存在 $1 \leq i \neq j \leq n, bid_i > bid_j$, 使得 $allocation_i < datacount_i, allocation_j > 0$。不妨将分配给参与者 $agent_j$ 的 $temp = min(datacount_i - allocation_i, allocation_j)$ 单位计算任务重新分配给参与者 $agent_i$, 得到解 S^2, 此时新的社会福利 $SW^2 = SW^1 - temp * bid_j + temp * bid_i = SW^1 + temp * (bid_i - bid_j)$，由前述条件可知,$temp > 0$ 且 $bid_i - bid_j > 0$。易得,$SW^1 < SW^2$。继续对 S^2 执行以上流程，直到前提条件不满足。此时，解 S^n 优先满足代价估值更大的参与者的需求。由贪心算法可知 $SW^n = SW$，则 $SW^1 < SW^2 ... < SW^n = SW$, 这与假设不符。故不存在上述更优解。 ■

分配规则已经确定，为了应用麦尔森引理确定价格规则，需要首先分析分配规则关于标的 bid_i 的单调性。

定理 3.2 对于任意参与者 $agent_i$ 以及任意 $\boldsymbol{bid_{-i}}$（表示除 bid_i 分量以外的总标的向量），算法3-1所示分配规则 $allocation_i(z, \boldsymbol{bid_{-i}})$ 是关于 $agent_i$ 的标的 z 的单调不减函数。

证明: 在保持其余标的不变的情况条件下，若 $agent_i$ 的标的 z 变大，则其在算法3-1中 *list* 序列中的排位只会更加靠前，从而获得更高优先级的分配权力。而算法的不确定性已经由第二关键字排序消除。 ■

然后分析该分配规则的特性，并制定相应价格规则。

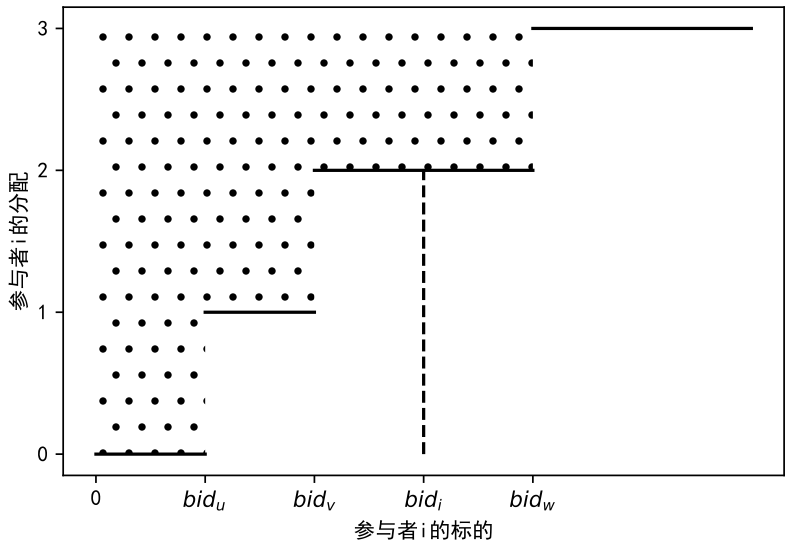

图 3-5 贪心算法分配函数示例

不失一般性，$allocation_i(z, \boldsymbol{bid}_{-i})$ 函数图像如图3-5所示。根据麦尔森引理，阴影部分面积即为 $agent_i$ 向平台方支付的报酬。由图像可知，需要求解出这些阶跃变化值。根据贪心算法的流程，若已知根据 ***bid*** 降序排列的 ***datacount*** 前缀和数组 ***prefix***, 则可以迭代求出这些阶跃值，从而求得阴影部分总面积。其余 *agent* 的代价计算亦然。总体支付算法的具体细节如算法3-2所示，时间复杂度 $O(n^2)$。

算法 3-2 数据量约束模型的支付算法

Input: ***datacount***, ***bid***, *datademand*
Output: ***payment***

运行算法3-1, 获得 *list*;
// 根据标的排序求 *datacount* 的各前缀和
prefix 置为初始值为 0 的数组;
for $i = 1$ **to** n **do**
  if $i > 1$ **then**
    $prefix[i] \leftarrow prefix[i-1]$;
  end
  $prefix[i] += datacount_{list[i].second}$;
end
// 求每个参与者的支付 $payment_i$
for $i = 1$ **to** n **do**
  $payment_{list[i].second} \leftarrow 0$;
  // *ind* 存储遍历下标
  $ind \leftarrow i + 1$ // y 存储当前的分配值
  if $i = 1$ **then**
    $y \leftarrow min(datademand, datacount_{list[i].second})$;
  else
    $y \leftarrow min(max(datademand - prefix[i-1], 0), datacount_{list[i].second})$;
  end
  while $ind \leq n$ *and* $y > 0$ **do**
    $newy \leftarrow min(max(datademand - prefix[ind] + datacount_{list[i].second}, 0), datacount_{list[i].second})$;
    $payment_{list[i].second} += (y - newy) * list[ind].first$;
    $y \leftarrow newy$;
    $ind += 1$;
  end
end

3.2.3.2 指标集约束

考虑指标集约束下的社会福利最大化问题3-2，其是一个 NP-hard 的组合优化问题，此处借用背包问题的思想，尝试以动态规划的方式进行求解。拟定 6 维状态 $dp[i, j, a, b, c, t]$，表示考虑前 i 个参与者，刚好分配 j 单位多方计算任务，其中一

级参与者 a 个，二级参与者 b 个，三级参与者 c 个，最多花费 t 单位总时间，所能够获得的最大收益。通过枚举分配给 $agent_i$ 的计算任务数量，可以得到状态转移方程3-4。

$$dp[i,j,a,b,c,t] = max \begin{cases} 1 \le k \le datacount_i \\ \text{If} \quad level_i = 1, \\ dp[i-1, j-k, a-1, b, c, t - k * timeperunit_i - transmitcost_i] + k * bid_i, \\ \text{If} \quad level_i = 2, \\ dp[i-1, j-k, a, b-1, c, t - k * timeperunit_i - transmitcost_i] + k * bid_i, \\ \text{If} \quad level_i = 3, \\ dp[i-1, j-k, a, b, c-1, t - k * timeperunit_i - transmitcost_i] + k * bid_i, \\ \text{all condition}, \\ dp[i-1, j, a, b, c, t] \end{cases} \tag{3-4}$$

$$dp[0, 0...datademand, 0...parti_1, 0...parti_2, 0...parti_3, 0...TIME] = -\infty$$

$$dp[0, 0, 0, 0, 0, 0...TIME] = 0$$

上述转移方程中，值得一提的是状态的初始化方法。考虑最优化问题3-2的限制条件可知，只有总体响应时间和是不等式限制，其余四项限制指标均为等式。这可以通过设置初始状态的合法性来解决。如转移方程3-4所示，在限制指标张成的五维空间中，仅有关于运行时间的一维子空间 (此处的状态空间是离散的) 被赋予合法性。其余非法状态置 $-\infty$。当限制指标集扩展时，针对不同类型的限制属性也可以按此思路进行初始状态设定。为了减少状态存储，转移方程3-4可以记忆化搜索的方式进行。相关细节如算法3-3所示，时间复杂度约为 $O(\sum_{i=1}^{n} datacount_i * S)$，$S$ 为除了第一维状态以外五维子空间的总状态数量。

算法 3-3 记忆化搜索

Input: ***datacount***, ***timeperunit***, ***level***, ***bid***, *datademand*, 及3.2.2节中定义的限制指标集

Output: ***allocation***

对参与者按照默认优先级进行排序，优先级较高的排位靠前。

$Search(n, datademand, parti_1, parti_2, parti_3, TIME)$;

以最优路径对 ***allocation*** 进行赋值;

;

$Search(i,j,a,b,c,t)$ 定义为：;

检查状态是否访问过，是则直接返回最优解，否则继续向下;

根据方程3-4所示进行状态转移;

for $i \leftarrow 0$ **to** k **do**

  $Search(new\ status) + k * bid_i$

end

记录当前状态最优值，若存在多个最优解，选择 k 值较小的那个，同时记录最优路径。;

定理 3.3 对于任意参与者 $agent_i$ 以及任意 $\boldsymbol{bid}_{-i}$，算法3-3所示分配规则 $allocation_i(z, \boldsymbol{bid}_{-i})$ 是关于 $agent_i$ 的标的 z 的单调不减函数。

证明: 将 $agent_i$ 移至所有参与者的最后一位。由算法3-3及转移方程3-4可知，参与者 $agent_i$ 的分配 $allocation_i$ 依赖于子空间 $dp[n-1,,,,,]$ 中 $datacount_i + 1$ 个状态 (分别对应于分配 012...$datacount_i$ 件计算任务)，以及 bid_i 的值。$dp[i-1,,,,,]$ 中的状态由参与者的许多信息 (包括 $\boldsymbol{bid}_{-i}$) 及所有环境参量 (如3.2.2节中定义的限制指标集) 决定。因此其不受 bid_i 影响。当 bid_i 变化时，这些状态可以看做固定值。

记 $allocation_i(z, \boldsymbol{bid}_{-i})$ 为 $al_i(z)$，$dp[i-1,,,,,]$ 中对应的 $datacount_i + 1$ 个状态分别为 $ndp[0], ndp[1], ...ndp[datacount_i]$。不妨假设 $a < b$, 且当 $bid_i = a$ 时，$al_i(z) = j$。这意味着 $ndp[j] + j * a$ 是 $\{ndp[k] + k * a | 0 \le k \le j\}$ 中的极大值。此时再考虑 $bid_i = b$ 时的情景。对于 $0 \le k \le j$, 对应的状态分别为 $ndp[k] + k*b = ndp[k] + k*a + k*(b-a)$, 由于 $ndp[k] + k * a \le ndp[j] + j * a$(来自于 $bid_i = a$ 的假设)，且 $k*(b-a) \le j*(b-a)$，所以 $ndp[k] + k * b \le ndp[j] + j * b$。那么 $al_i(a) \le al_i(b)$ ■

为了确定指标集约束问题下的价格函数，针对每一个 $agent_i$，需要确定证明10中 $dp[n-1,,,,,]$ 子空间中的 $datacount_i + 1$ 个状态的值。然后根据这些值确定分配函数 $al_i(z)$ 中的那些阶跃点。此时，对于每个阶跃点，其 y 轴的阶跃差仅为 1。那么可以根据麦尔森引理, 求得 $agent_i$ 所需支付的价格。

$$\begin{aligned} ndp[1] + 1 * b_1 &= ndp[0] \\ ndp[2] + 2 * b_2 &= ndp[1] + b_2 \\ ndp[3] + 3 * b_3 &= ndp[2] + 2 * b_3 \\ &\vdots \\ ndp[k] + k * b_k &= ndp[k-1] + (k-1) * b_k \end{aligned} \tag{3-5}$$

解方程组3-5, 可以得到所有阶跃点序列 $b_1, b_2, b_3 ... b_k$。值得注意的是，该序列不一定单调递增。价格规则实现如算法3-4所示，其中 $\boldsymbol{I}$(表达式) $= 1$ 当且仅当表达式为真。价格算法的细节如算法3-4所示，时间复杂度与分配算法类似。

算法 3-4 指标集约束问题的价格算法

Input: ***datacount***, ***timeperunit***, ***level***, ***bid***, *datademand*, 及3.2.2节中定义的限制指标集

Output: ***payment***

运行算法3-3, 得到分配 $allocation_i$;
若 $allocation_i = 0$，则 $payment_i = 0$。;
for 每个 $allocation_i > 0$ 的参与者 $agent_i$ **do**
  $payment_i \leftarrow 0$;
  将 $agent_i$ 移至末位，重新运行算法3-3, 得到:;
  $ndp[0] = dp[n-1, datademand, parti_1, parti_2, parti_3, TIME]$;
  $ndp[k] = dp[n-1, datademand - k, parti_1 - \boldsymbol{I}(level_i = 1), parti_2 - \boldsymbol{I}(level_i = 2), parti_3 - \boldsymbol{I}(level_i = 3), TIME - k * timeperunit_i - transmitcost_i], 1 \leq k \leq datacount_i$;
  $record \leftarrow 0$;
  for $ind \leftarrow 1$**to** $allocation_i$ **do**
    $record \leftarrow max(record, ndp[ind-1] - ndp[ind])$;
    $payment_i \leftarrow payment_i + record$;
  end
end

3.2.3.3 机构约束

对于机构约束下的社会福利最大化问题3-3，为森林状的机构添加虚根，使其转为树形结构。然后将问题抽象成图3-6。其中圆形代表机构，三角形及矩形代表机构中的计算单元，即机制的参与者。形状的不同体现了其数据来源的差异性，从而将他们划分为不同的互斥组。此时的社会福利最大化问题解决思路与前两节相似，不同点在于动态规划需要在整个树形结构上进行。

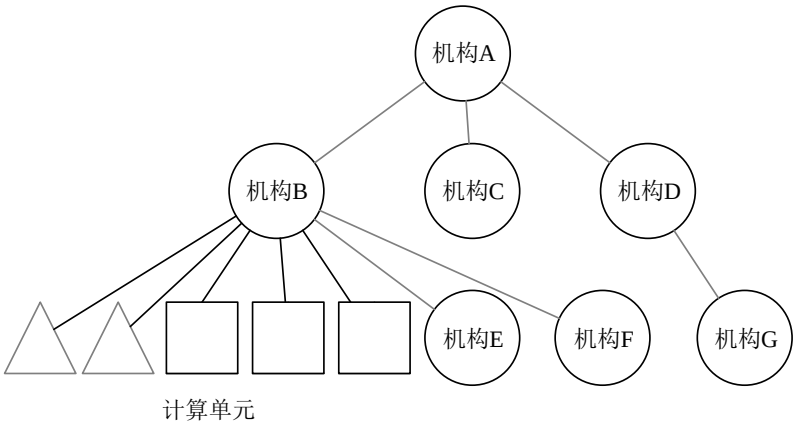

图 3-6 树形结构抽象图

仿照方程3-4拟定 6 维状态 $dp[i,j,a,b,c,t]$，表示考虑第 i 个机构及其下属机构，刚好分配 j 单位多方计算任务，其中一级参与者 a 个，二级参与者 b 个，三级参与者 c 个，最多花费 t 单位总时间，所能够获得的最大收益。由泛化物品的概念可知，每一个状态可以理解为一个泛化物品。那么原状态转移则是这些泛化物品在树上自底向上不断求和的过程。值得注意的是，图3-6中每个机构所属的三角形及矩形(计算单元) 首先要根据其互斥关系，以动态规划的方式合成一个泛化物品，然后再参与到树上的泛化物品合并流程。在此过程中同时记录最优路径。

另一方面，各个机构的偏好 $prefer_i$ 也可以在树上最优化的过程中解决。对于本文考虑的数据量约束 $limit_i$，树上最优化流程进行到机构 i 时，他可以直接将状态 $dp[i, limit_i + 1...datademand, , , ,]$ 全部置为非法状态。然后沿着树形结构继续最优化过程。本场景中的问题求解思想与3.2.3.2节中的思想是一致的。故此处直接给出分配算法3-5。

算法3-5的时间复杂度较高，约为 $O(m * S^2)$，S 为除第一维状态以外的五维子空间的总状态数。其关键步骤在于泛化物品之间的和并，思想是直接枚举费用状态在两者之间的分配。

定理 3.4 算法3-5所示的分配规则仍然单调。

证明: 证明思想与证明10 完全一致 ■

由于互斥组的存在，动态规划的无后效性被破坏，难以像前文一样直接将 $agent_i$ 移至末位，然后算出各个阶跃值。当然，若为每个互斥组增加一维二值状态，仍然可解，但此时的状态空间大小似乎难以接受。接下来直接以二分查找的方式来寻找这些阶跃值，时间复杂度为 $O(allocation_i * log(INCENT) * m * S^2)$。若 bid_i 的范围较小，也可以直接枚举求解。应根据具体数据量做相应调整。支付规则的细节如算法3-6所示。

算法 3-5 机构约束问题的分配算法

Input: ***datacount***, ***timeperunit***, ***level***, ***bid***, *datademand*,3.2.2节中定义的限制指标集, 本节新定义的量

Output: ***allocation***

generalizeditem(虚根, *datademand*, $parti_1$, $parti_2$, $parti_3$, *TIME*);
以最优路径对 ***allocation*** 进行赋值。;
;
generalizeditem(i,j,a,b,c,t) 定义为:;
if i 具有计算单元，即 $agentpinorg_i \neq \emptyset$ **then**
    以其计算单元的信息运行算法思想3-3, 注意同一组内最多选取一个参与者分配计算任务, 得到泛化物品 *init*;
    记录最优路径;
else
    init 是一个不产生任何影响的初始泛化物品。
end
for 机构 i 的每一个下属单位 u **do**
    计算 *generalizeditem* = $(u, 0...datademand, 0...parti_1, 0...parti_3, 0...parti_3, 0...TIME)$，得到泛化物品 u;
    将泛化物品 u 并入 *init*;
    // 按照既定的优先级处理多解的情况
    记录最优路径;
end
将 $init[, limit_i + 1...datademand, , , ,]$ 中的所有状态置为非法状态;
return *init*;

算法 3-6 机构约束问题的支付算法

Input: ***datacount***, ***timeperunit***, ***level***, ***bid***, *datademand*,3.2.2节中定义的限制指标集, 本节新定义的量

Output: ***payment***

运行算法3-5，得到 ***allocation***;
for 每个 $agent_i$ **do**
    $payment_i \leftarrow 0$;
    for $ks \leftarrow 0$ **to** $allocation_i$ **do**
        二分 bid_i，运行算法3-5, 找到 $allocation_i = ks$ 的临界标的 b。
        $payment_i \leftarrow payment_i + b$
    end
end

3.3 实验及分析

本章设计的机制均为 DSIC 机制，即所有参与者的占优策略是真实地投标，这由单变量环境下的麦尔森引理保证。本节实验主要对三种机制在相似的参数设定下做性能比较。参数设定如下：参与者的数量为 $10-500$，v 的设定为 100，$\boldsymbol{level}=(10,10,10)$，$m=10$，$TIME=10$, 互斥关系每个机构一组，每个机构的偏好 $perfer_i$ 也相应设置，以上数值仅意味着尺度范围。在实际应用中可以进行尺度变换。例如，$v=100$，实际数据需求量单位可能为百万，即数据量上限是 10^6。参与者的估值 v_i 服从正态分布 N(50,1)。使用的相关技术工具有：python、pandas、numpy、scipy、matplotlib。

运行本章的三种限制条件下的算法机制，观察其性能。结果如图3-7所示，仅有数据量约束条件下，算法的运行速度是较快的，基本能够在秒级完成。然而，引入指标集约束和机构约束后，由于算法的伪多项式性质，其时间花费大大增加。因此，在这两种情形下，相关环境参数的设置是较为敏感的。若需要求解的问题有较大的数据范围，可能会引入较大的时间花费。幸运的是，伪多项式算法是这些参数的多项式形式，其性能仍然完全优于指数级算法。由于相对尺度的原因，图3-7中数据量限制的算法运行时间并非近似线性，其运行效率的细节如图3-8。

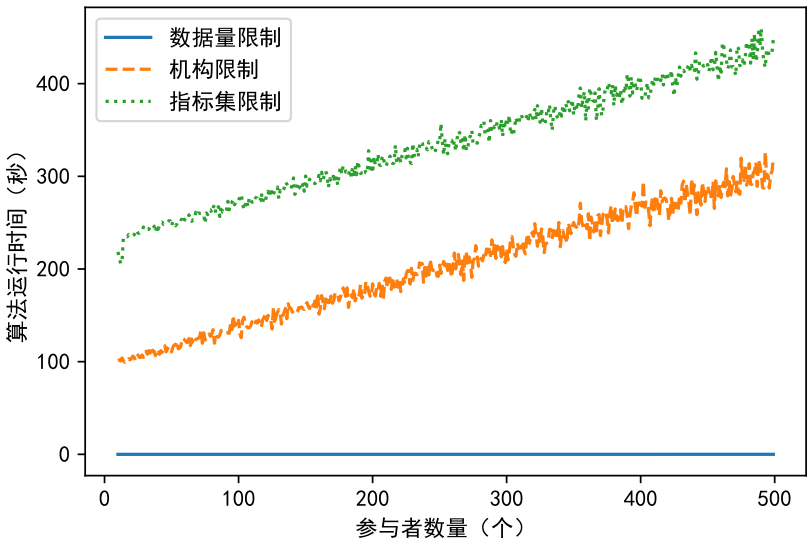

图 3-7 不同限制条件下的运行效率

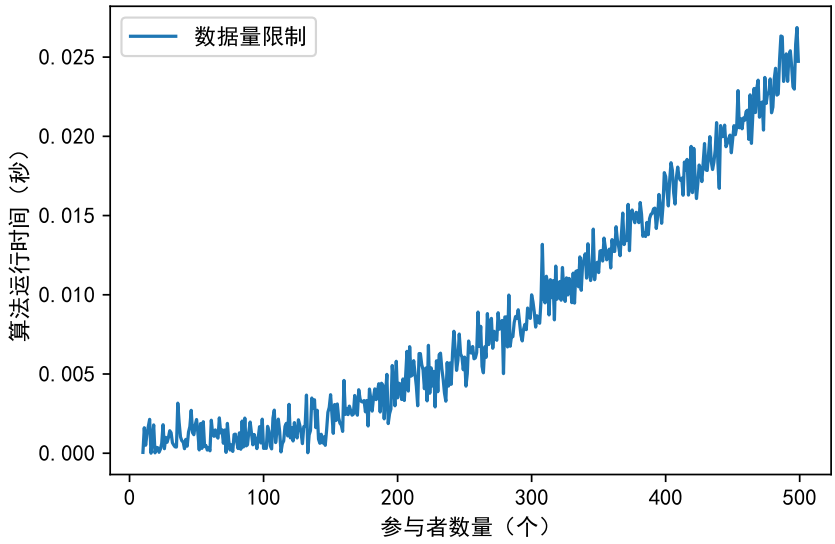

图 3-8 贪心算法的运行效率细节

另一方面，对于每个参与者来说，其效用总是随着人数的增加而不断减少。因为参与者之间的竞争随着人数的增加而愈发激烈。这个结论可以由图3-9所示实验结果得出。在该实验中，以一名参与者 $agent_k$ 作为观察的目标，增加参与者的数量，重新运行机制，计算该参与者的效用。为保证实验效率，只以数据量作为限制条件，即使用算法3-2。

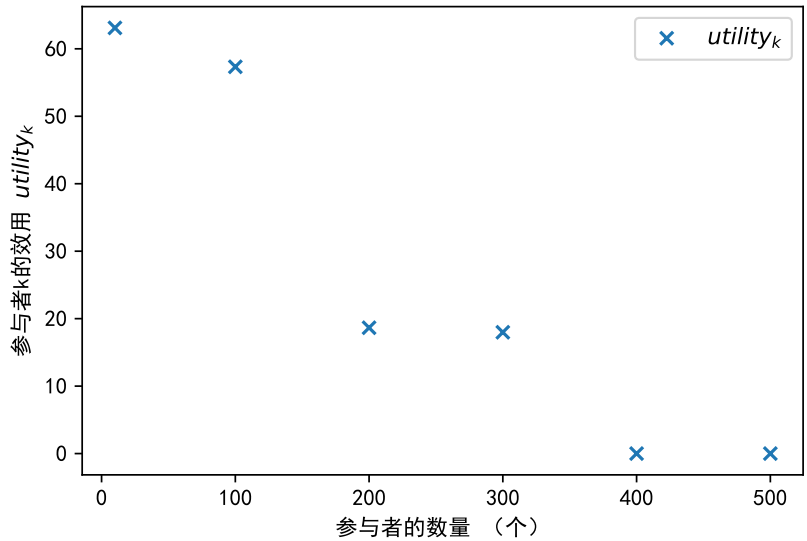

图 3-9 参与者的效用变化

3.4 本章小结

本章在简单可并行数据价值共享计算场景下提出多约束价值共享激励模型，依次讨论了数据量约束、指标集约束、机构约束等应用实例。数据量约束是拍卖机制的基础部分。在有限理性人、准线性效用等假设下，分配规则为满足任务方数据量需求限制条件下的社会福利最大化。指标集约束引入了任务方对多方计算任务执行者的进一步细节要求。例如：时效性，参与者数量，信誉评级等。而机构约束引入了机构组织的概念，更进一步考虑了参与者的上下级关系带来的新的限制，以及数据同质参与者之间的互斥性。以上三种激励机制均满足社会福利最大化、DSIC。数据量约束可以在多项式时间内求解，而指标集约束和机构约束需要在伪多项式时间内求解。

第四章 依赖相关数据价值共享计算的激励机制

本章从依赖相关的数据价值共享计算出发，提出时间敏感价值共享激励模型。主要分析多方数据价值共享计算模式中复杂问题的计算时间限制，分别给出社会福利最大化和期望税收最大化的 DSIC 拍卖机制。

4.1 引言

多方数据价值共享计算环境中，由于任务 T 对数据依赖的内在复杂性，数据分布的差异性等因素，更一般的情形是计算不可简单分布式并行完成。此时，原计算任务 T 被分割算法根据所需数据划分为若干个更小的计算子任务。每个子任务满足多方计算的限制，即其计算仅依赖于本地数据。然后合并算法将这些子任务的计算结果重新合并成原始计算问题 T 的解。而合并的结果的方式并不单一，可能包含了若干次迭代操作。一方面，这些反复的结果传输带来的时延会造成总计算时间增加。这是分布式计算环境不可避免的问题。而另一方面，参与多方计算的各个计算单元的计算能力可能有较大差异。若是将子任务分配给了效率极低的计算单元，多方计算的时效性将会进一步降低。这对于响应时间敏感的计算任务而言是难以接受的。因此，本章主要以计算时间作为依赖相关数据价值共享计算（后文可能简称为依赖相关计算）场景下的限制指标。

4.2 时间敏感价值共享激励模型

对于依赖相关的多方计算，本节提出时间敏感价值共享激励模型，其有两个目标函数：社会福利最大和期望税收最大。研究的主要内容是确定时间限制下的分配算法和价格算法。

4.2.1 问题描述

在依赖相关的计算中，子任务之间存在复杂的同步等待关系，可以形成有向无环图。任务方的主要限制条件可以描述为：每个子计算任务确定其胜出者者后，完成总任务的计算时间需要在给定允许范围内。

如图4-1所示，每个顶点意味着子任务的同步等待。只有当指向该节点的所有边上所示子任务均完成时，该节点的同步等待方结束，继续进行后续子任务计算。

另一方面，在前文的机制设计中，平台方根据定义好的社会福利来确定分配规则及价格规则，对应于社会福利最大化问题。这样的分配规则可以使得系统整

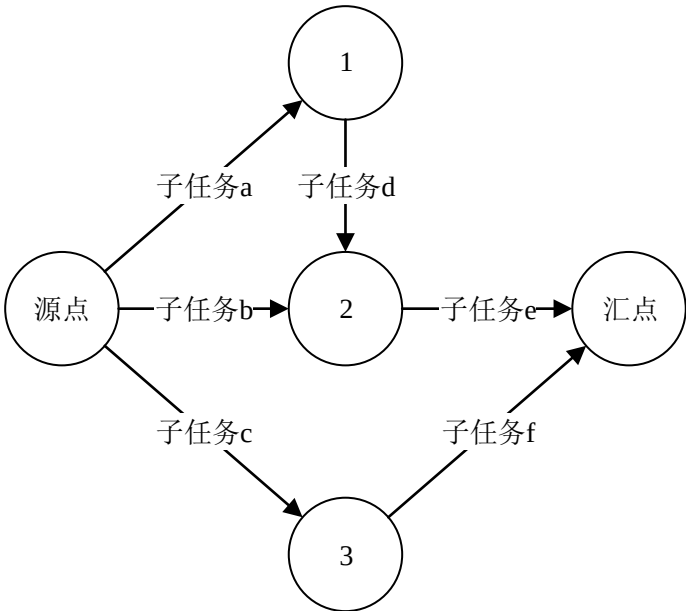

图 4-1 子任务的 AOE 网示例

体收益最优，但此时任务方的收益无法确切保证。若任务方的预算是有限的，则需要设计新的分配规则及价格规则来保证其收益。即，在完成任务方依赖相关计算任务的条件下，尽可能减少任务方的成本。

4.2.2 问题建模

对于计算任务 T，任务分解算法将其划分为子任务集合 $\boldsymbol{SubTask}, |\boldsymbol{SubTask}| = ST$。这些子任务之间的同步等待问题存在拓扑序关系。为了描述这种关系，本文借用 AOE 网的思想。构建有向无环图 $D = (\boldsymbol{V}, \boldsymbol{E})$，集合 $\boldsymbol{V}$ 是所有同步节点的集合。有向边 $< u, v > \in \boldsymbol{E}$ 表示子任务的进行。另有关于有向边的函数 $t(e)$，其值是子任务 e 由该任务的胜出者进行计算所需时长。每个子任务 $SubTask_i$ 拥有竞争该任务的参与者列表 $list_i$，每个参与者 $agent_{ij} \in list_i$ 有关于任务 $SubTask_i$ 的私密估值 val_i 以及其完成该计算任务所需时间 $timefromagent_i$。每个列表中只能产生也必须产生一名胜出者，来完成该子任务的计算。此处假定每个参与者仅参与一项子任务的竞争。最重要的限制条件是：所有子任务的胜出者确定后，总任务的完成时间 $finishedtime \leq$ 某一阈值 $timelimit$。包括效用函数、社会福利等其余定义与假设均与第三章类似，此处不做赘述。

假设所有参与者已经真实地表达对各自计算子任务的估值，并给出标的，即 $\boldsymbol{bid} = \boldsymbol{val}$。此时社会福利最大化可以形式化为问题4-1。

$$\begin{aligned} \max_{\vec{allocation}} \quad & \sum_{i=1}^{n} bid_i * allocation_i \\ s.t \quad & allocation_i = \{0,1\} \\ & \left(\sum_{i=1}^{n} I(agent_i \in list_j) * allocation_i\right) = 1, \text{for every } 1 \le j \le ST \\ & finishedtime(\boldsymbol{allocation}) \le timelimit \end{aligned} \tag{4-1}$$

另一方面，考虑任务方的税收，由3.2.2节可知，平台方的真实收益是 $profit = \sum_i^n payment_i - m * INCENT$，其中 m 是多方计算任务 T 所需单位计算的数量。在简单可并行场景下，$m = datademand$；在依赖相关计算场景中，$m = ST$。$-m * INCENT$ 部分是固有值，不可更改。最大化 $profit$ 等价于最大化 $\sum_i^n payment_i$。面对不同的参与者估值，同一机制的税收可能也是不同的。故本节采用期望税收最大化的机制设计来保证平台方在平均意义下的收益最优。

现有独立的概率分布 $F_1, F_2, F_3, ...F_n$ 及对应的连续概率密度函数 $f_1, f_2, f_3 .. f_n$，且这些分布均存在有限期望。参与者 $agent_i$ 的私密值 val_i 的概率分布是 F_i。

假设所有参与者已经真实地表达对各自计算子任务的估值，并给出标的，即 $\boldsymbol{bid} = \boldsymbol{val}$。由于期望税收等于期望虚拟社会福利，此时期望税收最大化可以形式化为问题4-2，其中 $\phi_i(bid_i)$ 为参与者 i 的虚拟估值。

$$\begin{aligned} max \quad & \boldsymbol{E}_{\boldsymbol{bid} \sim \boldsymbol{F}}\left[\sum_{i}^{n} \phi_i(bid_i) * allocation_i(\boldsymbol{bid})\right] \\ s.t \quad & allocation_i = \{0,1\} \\ & \left(\sum_{i=1}^{n} I(agent_i \in list_j) * allocation_i\right) = 1, \text{for every } 1 \le j \le ST \\ & finishedtime(\boldsymbol{allocation}) \le timelimit \end{aligned} \tag{4-2}$$

4.2.3 分析及求解

现分别针对以上的社会福利最大化问题和期望税收最大化问题进行分析及求解。

4.2.3.1 社会福利最大化

给定 AOE 网，可以利用关键路径算法求出该网络的最少花费时长。对于图4-1中的顶点 i，同步等待结束当且仅当其所有前驱顶点等待结束且对应边上的

子任务完成。而顶点 i 结束等待所需花费的时长是其所有前驱花费时长与对应子任务时长之和的最大值。此时产生明显的最优子结构，而在 DAG 中，这些子结构是会被重复求解的。拟定状态 $dp[i]1 \leq i \leq |V|$，表示同步节点 i 完成等待所需的时间。则有转移方程 $dp[i] = max(dp[k] + t(< k, i >)| < k, i > \in \boldsymbol{E}), dp[源] = 0$。总任务所需时间 *finishedtime* 即为 $dp[汇]$。

考虑 $SubTask_i$ 的胜出者选择过程，对于参与者 i,j，若 $val_i < val_j$，且 $timefromagent_i > timefromagent_j$，则 $agent_i$ 完全劣于 $agent_j$，故可以将 $allocation_i$ 直接置为 0。此时可以认为，*timefromagent* 随着 *val* 单调递增。这意味着选取更大估值的参与者会带来更长的计算时长，在 *AOE* 网中，若该子任务对应的边在关键路径上。那么会引起总的时长增加，可能违反限制条件。若采用暴力枚举，假设每条边共有 a 种选择 (对应于该子任务的 a 个竞争者)，那么 b 条边，总可行集大小就有 a^b 种，似乎难以接受。

定理 4.1 问题4-1属于 NP-hard 问题。

证明: 令 S 表示问题4-1。要证 $S \in NP - hard$，需要存在一个现有 NPC 问题 S' 归约至 S。此处以 0-1 背包作为 S'。

对于 S' 的任意实例 *ins*，共有 n（此处的变量名仅在本证明内有效）个物品，n 维向量 ***size*** 和 ***val*** 分别是物品质量向量和价值向量。B 是背包容量。构建有向图 $D = (\boldsymbol{V}, \boldsymbol{E})$，$\boldsymbol{V} = 1, 2, ..., n, n+1, \boldsymbol{E} = \{(i, i+1)|1 \leq i \leq n\}$。对于 $1 \leq i \leq n$，构建 $list_i$，有两个参与者，$(timefromagent, bid) = \{(size_{i-1}, val_{i-1}), (0, 0)\}$。$timelimit = B$。得到问题4-1的一个实例 *ins*′。

原问题 *ins* 的最优化等价于现问题 *ins*′ 的求解。故任意 0-1 背包问题实例都可以在多项式时间内归约至问题4-1的一个实例。故 $S \in NP - hard$。 ■

由于问题4-1是难以在多项式时间内精确求解的。本文首先尝试以朴素的贪心算法对其近似求解。

其思想是从初始可行解 S 开始，每次寻找一个满足时间限制条件的更优解 S' 取代原可行解，直到时间限制无法满足为止，如算法4-1所示。

算法4-1的思想是从最小社会福利的解开始，每次选择一个子任务 j，该子任务选择更优胜出者的价值收益与时间花费损失的比值最大。然后判断新的解是否满足最长路时间限制条件。若新解是可行解则更新，否则当前解为此贪心算法下的最优解。算法时间复杂度为 $O((|V| + |E|) * n)$，n 为总的参与者数量。

定理 4.2 算法4-1所示分配规则 $allocation_i(z, \boldsymbol{bid}_{-i})$ 不一定关于 $agent_i$ 的标的 z 的单调不减。

证明: 要证上述分配规则不一定单增，可以举一反例说明。一实例如图

所示，共有两个串行的子任务，每个子任务有 3 个竞争的参与者。$list_1 = \{(1,1),(2,3),(3,5)\}, list_2 = \{(1,1),(2,2),(3,9)\}$，二元组 (a,b) 表示 $timefromagent = a, bid = b$，$timelimit = 5$。运行算法4-1, 可知 $(2,2)$ 对应的参与者为胜出者之一。

此时将 $(2,2)$ 对应参与者 $agent_z$ 的标的增加至 4，即用 $(2,4)$ 替代原 $(2,2)$, 再次运行算法4-1。新的胜出者是 $(3,9)$。因而对于 $agent_z$ 来说，其分配函数并非关于其标的 bid_z 单增。 ■

算法 4-1 贪心近似求解依赖相关计算问题

Input: 前文建模定义的所有相关量
Output: ***allocation***

对于任意子任务竞争列表中的任意参与者 i,j，若 $val_i < val_j$，且 $timefromagent_i > timefromagent_j$，置 $allocation_i = 0$，并将参与者 i 从该竞争列表中删除。然后将各个竞争者列表 $list_i$ 中的参与者各自按照 $timefromagent$ 关键字递增排序。;
初始化解 S，其中所有子任务的胜出者为各自竞争列表中时长花费最小的参与者。;
若以 $index_i$ 表示子任务 i 的当前胜出者在 $list_i$ 中的下标。则 $index_i = 1$。;
根据转移方程 $dp[i] = max(dp[k] + t(< k,i >)| < k,i > \in \boldsymbol{E}), dp[源] = 0$ 计算 S 所需时间 $ftime = dp[汇]$。;
if $ftime > finishedtime$ **then**
    任务无法在给定时限内完成，输出错误信息。;
end
while *True* **do**
    选出 $\{bid_{index_i+1} - bid_{index_i} / timefromagent_{index_i+1} - timefromagent_{index_i}\}$ 中的最大值所对应的子任务下标 j。;
    构造新的解 $S' = S$, 除了 $index_j = index_j + 1$;
    根据上述状态转移方程计算解 S' 是否满足时间限制条件。;
    if S' 不是可行解 **then**
        continue;
    end
    $S = S'$;
end
根据最终解 S 中的胜出者确定分配向量 ***allocation***;

更一般的可知，这种从初始状态开始，每一步选取选择下一个参与者的收益增量最大的子任务进行阶段性迭代更新的贪心策略对应的分配函数均不满足单增的性质。因为总是存在前述证明中的参与者 $agent_z$ 的情况。由麦尔森引理及 DSIC 机制的必要条件可知此类贪心策略无法实施。

接下来考虑每次直接选择标的最大的参与者作为胜出者的贪心策略，如算法4-2所示。类似的，其最坏时间复杂度为 $O((|V| + |E|) * n)$，n 为参与者数量。接

下来说明该分配规则的单调性。

定理 4.3 对于任意参与者 $agent_i$ 以及任意 $\boldsymbol{bid}_{-i}$，算法4-2所示分配规则 $allocation_i(z, \boldsymbol{bid}_{-i})$ 是关于 $agent_i$ 的标的 z 的单调不减函数。

证明: 记 $al(z) = allocation_i(z, \boldsymbol{bid}_{-i})$，由前述场景可知，$al(z) \in \{0, 1\}$。不妨假设 $a < b$, 且$al(a) = 1$(对于 $al(a) = 0$ 的情况，$al(a) \leq al(b)$ 一定成立)。

对于 $agent_i$ 并非其竞争列表中 *timefromagent* 值最小的情况, 考虑算法4-2的流程，假设到 $agent_i$ 之前根据标的递减排序的参与者序列为 $p_1p_2p_3...p_k = agent_i$，若增大标的 z 会将 $agent_i$ 的位次提前。在 $z = b$ 的情况下，假设新的参与者序列为 $p_1p_2p_3...p_u = agent_i...p_{k-1}p_{k+1}$。当贪心算法考虑到 p_u 时，由于 $u < k$, 且$al(a) = 1$，$agent_i$ 所属子任务 *SubTask* 一定未曾被访问过。算法4-2中的新解 S' 也一定是可行解。否则，$al(a) = 0$。(因为算法确定序列 $p_{u+1}...p_{k-1}$ 中新的胜出者的过程只会使得 DAG 的总时长不减少)。故 $agent_i$ 会继续成为其所属子任务的胜出者，$al(a) \leq al(b) = 1$。

若 $agent_i$ 是其所属子任务的竞争列表中时长花费最小的参与者，增大 z 可能会使得部分后继参与者直接因绝对次优性被删除。而留下来的参与者的相对标的 $bid_k - z$ 会减少，这导致相应的参与者位次后移。类似于前面的分析，这都不会改变 $agent_i$ 的胜出者事实。故 $al(a) \leq al(b) = 1$ 始终成立。 ■

本场景下的分配向量 ***allocation*** 被限制于 0-1 向量，故对于每个胜出者，只需找出其无法继续胜出的临界标的作为其支付的价格。算法4-3的最坏时间复杂度约为 $O(|E| * (|V| + |E|) * (n + max(|E|, |E| * C)))$，$C \leq n$ 为各个子任务对应参与者数量的最大值。即为 $O(|E|^2 * n * (|V| + |E|))$，$n$ 为总参与者数量。

算法 4-2 贪心近似求解依赖相关计算问题 2

Input: 前文建模定义的所有相关量
Output: ***allocation***

对于任意子任务竞争列表中的任意参与者 i,j，若 $val_i < val_j$，且 $timefromagent_i > timefromagent_j$，置 $allocation_i = 0$，并将参与者 i 从该竞争列表中删除。然后将各个竞争者列表 $list_i$ 中的参与者各自按照 *timefromagent* 关键字递增排序。;
此时每个竞争列表 $list_i$ 首位的参与者称为该子任务的基准参与者;
初始化解 S，其所有子任务的胜出者为各自基准参与者。;
根据转移方程 $dp[i] = max(dp[k] + t(< k,i >)| < k,i > \in \boldsymbol{E}), dp[源] = 0$ 计算 S 所需时间 $ftime = dp[汇]$。;
if $ftime > finishedtime$ **then**
    任务无法在给定时限内完成，输出错误信息。;
end
初始化相对标的列表 $lst = \{(bid_i - base_i, timefromagent_i) | 1 \le i \le n$且参与者 i 并非基准参与者$\}$，$base_i$ 是 $agent_i$ 所属子任务的基准参与者的标的;
将相对标的列表 *lst* 按照二元组的第一关键字进行降序排列。;
置所有子任务为未访问状态。;
while *lst* 不为空 **do**
    选出 *lst* 中当前首位标的所对应的参与者 $agent_k$。;
    然后在 *lst* 中删除该标的;
    if 参与者 k 对应的子任务 $SubTask_u$ 已经被访问过 **then**
        continue;
    end
    构造新的解 $S' = S$，$agent_k$ 是 $SubTask_u$ 的胜出者。;
    根据上述状态转移方程检查解 S' 是否满足时间限制条件。;
    if S' 不是可行解 **then**
        continue;
    end
    $S = S'$;
    置 $SubTask_u$ 为已被访问状态。;
end
根据最终解 S 中的胜出者确定分配向量 ***allocation***;

算法 4-3 贪心近似求解依赖相关计算问题 2 的支付算法

Input: 前文建模定义的所有相关量
Output: ***payment***

运行算法4-2, 得到 ***allocation***;
for 每个 $agent_i$ **do**
  if $allocation_i = 0$ **then**
    $payment_i = 0$;
  else
    将单减的原始相对标的序列 $\boldsymbol{b} = b_1 b_2 b_3 ... b_k$ 中与 $agent_i$ 属于同一竞争列表的所有相对标的 $b_a, b_b, b_c, ..., b_{agent_i}, b_{next}...$ 全部删除，得到新的原始标的序列 $\boldsymbol{b}'$;
    使用 $\boldsymbol{b}'$ 重新运行算法4-2，得到各个胜出者产生时对应的 DAG 序列 $\boldsymbol{GS} = G_1, G_2, G_3 ... G_u$，每个 G_i 是算法4-2中的一个新的可行解 S' 对应的 DAG;
    if $agent_i$ 不是基准参与者 **then**
      假设 $agent_i$ 的相对标的 z 在图序列 ***GS*** 中的位次是 $G_1, G_2, ...z, G_j, G_{j+1}....G_u$;
      for $v = j$ **to** u **do**
        在 G_v 的基础上将 $agent_i$ 置为所属子任务的胜出者，得到新解 S'，以算法4-2中最长路的计算方法检查 S' 的合法性;
        if S' 不合法 **then**
          $payment_i = bid_i +$ max(产生G_v所对应的相对标的, $agent_i$后一位的相对标的b_{next}的第一关键字)$-$ $agent_i$ 的相对标的 z;
          break;
        end
      end
    else
      假设与 $agent_i$ 所属同一子任务的其余相对标的在 DAG 序列 ***GS*** 中的位次是 $G_1, G_2, ..., z_1, ..., z_2, ..., z_k, ...G_u$。不断减少 bid_i，直到 $z_1, ...z_k$ 中首次出现新的胜出者，减少量为 Δb;
      if $\Delta b > bid_i$ **then**
        $payment_i = 0$;
      else
        $payment_i = bid_i - \Delta b$;
      end
    end
  end
end

4.2.3.2 期望税收最大化

虚拟估值定义为 $\phi_i(v_i) = v_i - \frac{1-F_i(v_i)}{f_i(v_i)}$。在参与者真实地给出标的的情况下，期望税收等于期望虚拟社会福利。即

$$\boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\sum_i^n payment_i(\boldsymbol{v})\right] = \boldsymbol{E}_{\boldsymbol{v}\sim\boldsymbol{F}}\left[\sum_i^n \phi_i(v_i) * allocation_i(\boldsymbol{v})\right] \tag{4-3}$$

故期望税收最大化等价于期望虚拟社会福利最大化。

模型4-2的求解思路是在 ***bid*** 的条件下在与4-1相同的可行集上最大化虚拟估值 $\sum_i^n \phi_i(bid_i) * allocation_i(\boldsymbol{bid})$，可知其仍然是 $NP-hard$ 问题，故仍采用算法4-2近似求解。而为了满足参与者真实投标的前提，需要讨论虚拟社会福利最大化对应分配规则 *virtualal* 的单调性。

算法 4-4 最优拍卖机制的分配算法

Input: 建模定义的所有量

Output: ***allocation***

1 将所有参与者的标的 bid_i 以其虚拟估值 $\phi_i(bid_i)$ 替代;

2 其它信息不更改，运行算法4-2，得到 ***allocation***;

定理 4.4 若任意分布的失效率函数 $\frac{f_i(v)}{1-F_i(v)}$ 关于 v 单调不减，则对于任意参与者 $agent_i$ 以及任意 $\boldsymbol{bid}_{-i}$，算法4-4所示分配规则 $allocation_i(z, \boldsymbol{bid}_{-i})$ 是关于 $agent_i$ 的标的 z 的单调不减函数。

证明: 虚拟社会福利可能引入的负数标的不影响原问题求解。算法4-2所示分配规则单调不减，若分布的失效率函数单调不减，则虚拟估值 $\phi_i(v_i)$ 单调不减，则 $allocation_i(z, \boldsymbol{bid}_{-i})$ 也单调不减。 ■

类似地，给出最优拍卖的支付算法。

算法 4-5 最优拍卖机制的支付算法

Input: 建模定义的所有量

Output: ***payment***

1 将所有参与者的标的 bid_i 以其虚拟估值 $\phi_i(bid_i)$ 替代;

2 运行算法4-3，得到 ***payment***;

3 **for** $allocation_i = 1$ 的参与者 **do**

4 　将 $payment_i$ 替换为 $\phi_i^{-1} payment_i$

5 **end**

4.3 实验及分析

本节针对贪心求解依赖相关计算问题的算法4-2进行模拟实验分析。实验环境及工具为 python、numpy、networkx。为了衡量贪心算法的性能，需要知道问题实例的精确解。由于问题4-1是 NP-hard 问题。随着数据范围增大，精确计算该问题的时间花费呈指数级增长，所以本文只在小数据范围内验证该贪心算法的有效性。

如前文形式化所定义，原始计算问题的 aoe 网、参与者的标的信息、参与者的时长信息等可由随机模拟产生，记为随机变量 ***instance***。由算法4-2得到的近似社会福利 ***aSF*** 和真实确切的最大化社会福利 *SF* 均是 ***instance*** 的函数。本节将 $\boldsymbol{ratio} = \frac{\boldsymbol{aSF}}{\boldsymbol{SF}}$ 作为评估性能的指标。$0 < \boldsymbol{ratio} \leq 1$，且 ***ratio*** 越接近 1 意味着近似性能越好。

设置 aoe 网的生成是等可能随机，且 $|E| = constant * |V|$($|E|$ 为边集大小，$|V|$ 为 AOE 网的阶数，*constant* 为一较小常数)。参与者的标的 bid_i 服从 $N(50,1)$。参与者的时长 $1 \leq timefromagent_i \leq 100$ 为整数，且等可能分布。每次实验抽样 1000 次。为了尽可能说明贪心算法的有效性，原始任务无解和单独选择各子任务中价值最高的参与者即为最优的两种情况已被预先排除。因为在这两种情况中，贪心算法一定能够求得精确最优解。这通过限制 *timelimit* 的大小来实现。

表 4-1 实验结果

AOE 网的阶数	$aSF = SF$ 的次数	0.5 分位点	ratio 样本均值	ratio 样本方差
10	961	1.0	0.999962	0.000236
15	943	1.0	0.999968	0.000170
20	952	1.0	0.998137	0.029445

由表4-1可知，在阶数较小的简单图范围内，贪心算法4-2的具有较好的近似性能。

为了验证贪心算法4-2的计算有效性。本文在不同阶数的 AOE 网中利用该算法进行求解。

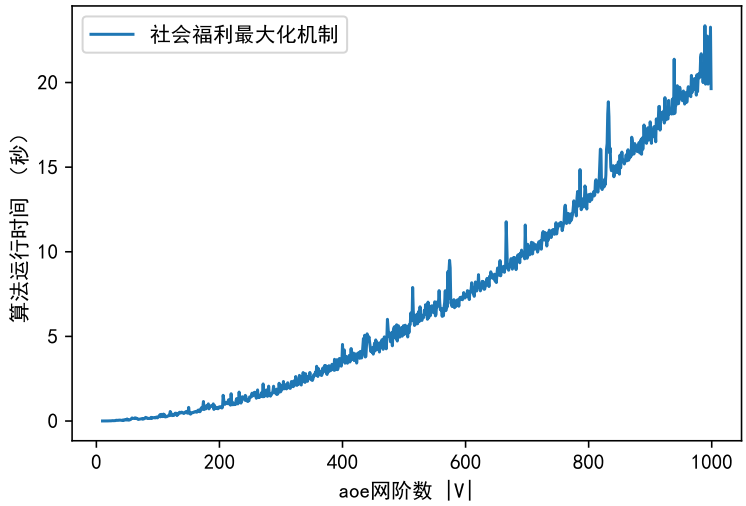

图 4-2 贪心算法关于 AOE 网阶数的执行效率

以上实验对 10 至 1000 阶有向图进行模拟求解。由图4-2可知，贪心算法4-2是计算有效的多项式算法，实验结果与时间复杂度分析吻合。

在本实验环境设定中，相关变量主要有：aoe 网络的阶数、aoe 网络的结构、参与者数量、参与者标的分布。接下来以一系列实验分析这些因素对于税收的影响，此处以社会福利最大化为例。

由于本文用于实验的计算资源有限，设定 aoe 网络的生成核为线性函数 $kernel(x) = x$（核函数的幂指数越高意味着网络结构并行化程度越高），每个子任务的参与者数量上界为 100，参与者标的服从正态分布 $N(50, 1)$。观察 aoe 网络的阶数对任务方税收的影响，结果如图4-3。可知税收近似是网络阶数的线性函数，这与直觉相符合。因为每个子任务必须有一个胜出者，其税收最多为其标的，总税收近似等于 平均标的 $*$ $|E|$。而本实验中 aoe 网的边数 $|E|$ 是阶数 |V| 的同阶线性函数，故总税收应近似为 aoe 网络阶数的线性函数。

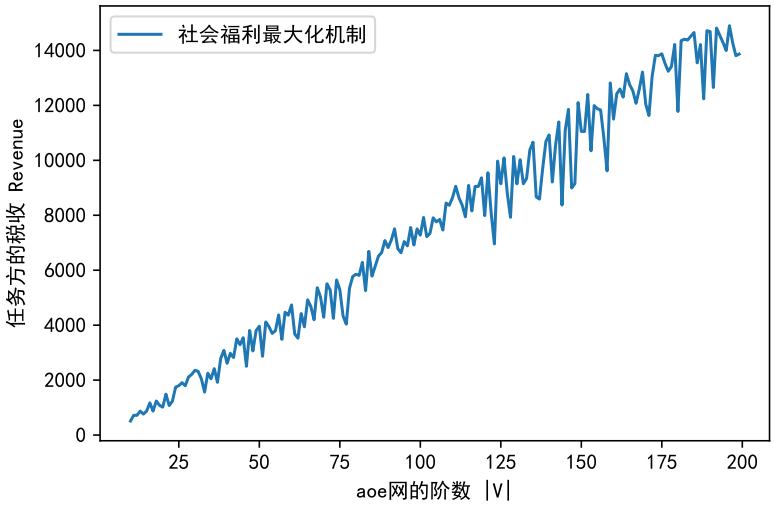

图 4-3 税收关于 aoe 网阶数的变化

然后设定 aoe 网络的阶数为 200，网络生成核为线性函数 $kernel(x) = x$，参与者标的服从正态分布 $N(50, 1)$，观察每个子任务的竞争参与者数量上界 C 对总体税收的影响。结果如图4-4，可知当 $C \in [2, 20]$ 时，此时参与者数量较少，竞争强度较低，为保证可以完成拍卖任务，大部分子任务的税收都是 0。所以总体税收较低，但是从实验数据可以发现，税收随着 C 的增长快速增加。当 $C > 20$ 以后，参与者的竞争已经达到饱和，总税收不再明显上升。此时限制总税收增加的其实是参与者的估值的分布，也就是子任务的带给参与者的实际价值。

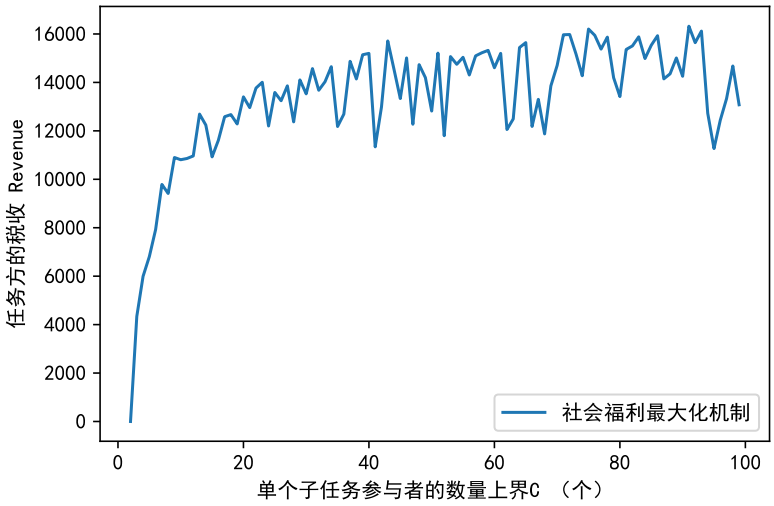

图 4-4 税收关于每个子任务参与者数量上界的变化

接下来设定 aoe 网络的阶数为 200，每个子任务的参与者数量上界为 100，参与者标的服从正态分布 $N(50,1)$，观察 aoe 网络的生成核函数的幂指数 *power* 对总体税收的影响。结果如图4-5, 可知当核函数为线性函数时，税收不高。此时是因为网络结构复杂，并行化程度较低，时间限制极容易被破坏，前文设计的机制会选择计算时间耗费更小的参与者，而这意味着总体税收会降低。另外当 $power > 5$ 左右时，税收快速上升并逐渐稳定，这也一定程度上说明了核函数的有效使用范围。

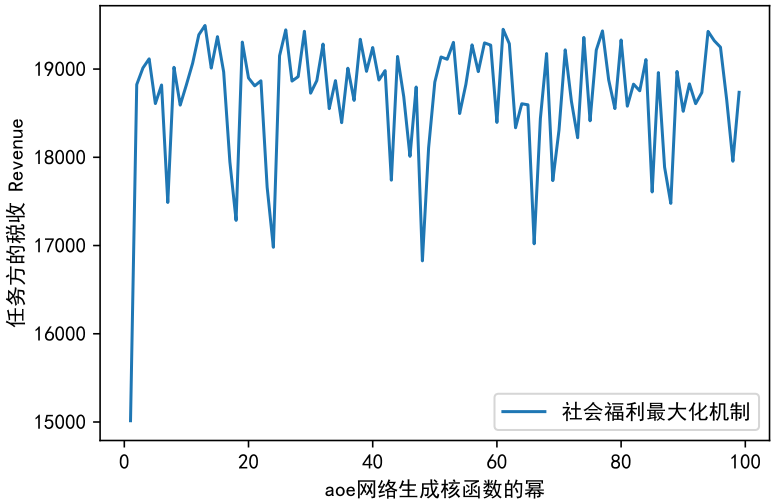

图 4-5 税收关于网络生成核函数幂指数的变化

接下来设定 aoe 网络的阶数为 200，每个子任务的参与者数量上界为 100，网络生成核为线性函数 $kernel(x) = x$，观察参与者标的分布的方差对总体税收的影响。如图4-6所示，当方差增大时，总体税收的方差也增大，而税收期望的缓慢增加。这可能是由于标的的方差在本机制中具有不同的影响。

一方面，由于本章的社会福利求解使用了贪心启发式算法，该算法优先考虑标的较高的参与者，这意味着越大的标的方差会使贪心启发式算法的近似程度增加，使得其税收靠近精确社会福利最大化的税收。

另一方面，方差的增加也会增大总体税收的方差。因而得到了图4-6所示总体税收方差和期望同时增加的情形。

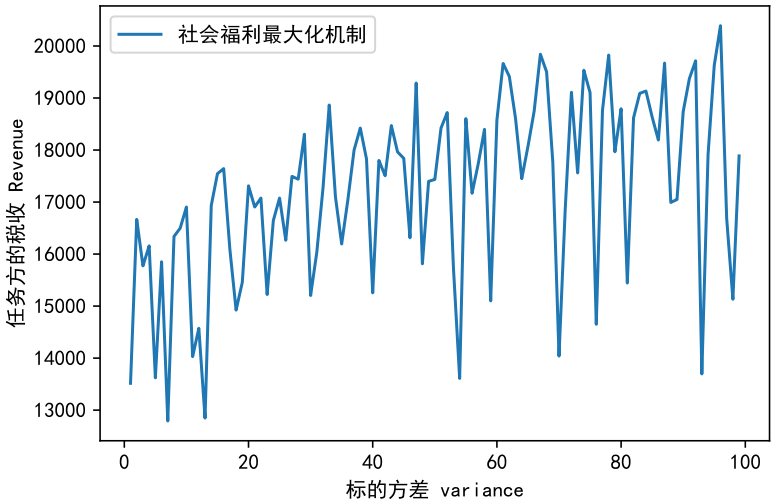

图 4-6 税收关于参与者标的方差的变化

为了验证最优拍卖机制的有效性，将其与社会福利最大化对应机制在 200 阶有向图范围内进行对比试验，以任务方的税收作为参考指标。其中各个参与者估值的先验概率分布均为正态分布，具有相同方差，不同的均值。具体的是，所有参与者的均值服从均值为 50 的正态分布。其余环境设定与前文实验类似。结果如图4-7所示，相比于社会福利最大化的机制，在多数情况下，最优拍卖机制能够有效提升任务方的税收性能。

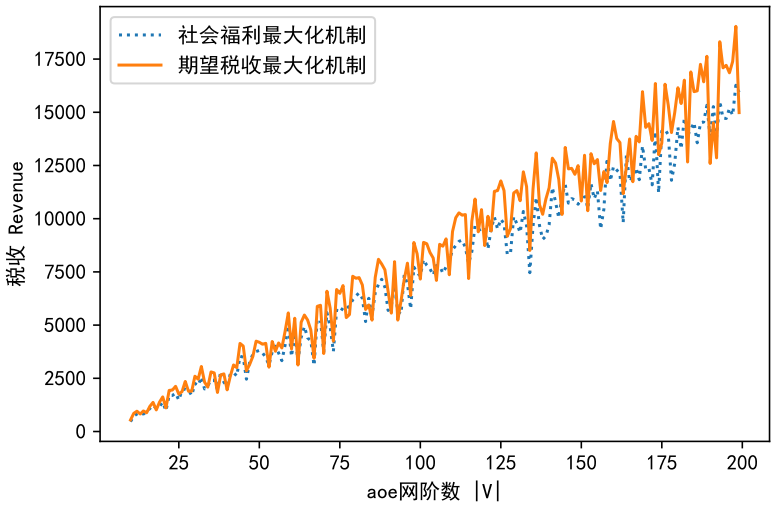

图 4-7 最优拍卖的有效性实验

在上述实验的基础上，在参与者标的向量 $\boldsymbol{v}$ 的维度上做样本均值。由于计算

资源有限，只对部分阶数的 aoe 网络做实验验证。相关实验结果如图4-8所示，当 aoe 网的阶数较低时，最优拍卖总是能够提升税收性能，这与理论分析相符。但当 aoe 网阶数增至 200 时，期望税收并未明显提升。这可能是因为随着阶数增大，税收的方差也随之增大，而需要更多的样本来获得更加稳定的均值。于是，可知最优拍卖的确能够在期望意义下提升拍卖机制的税收性能。

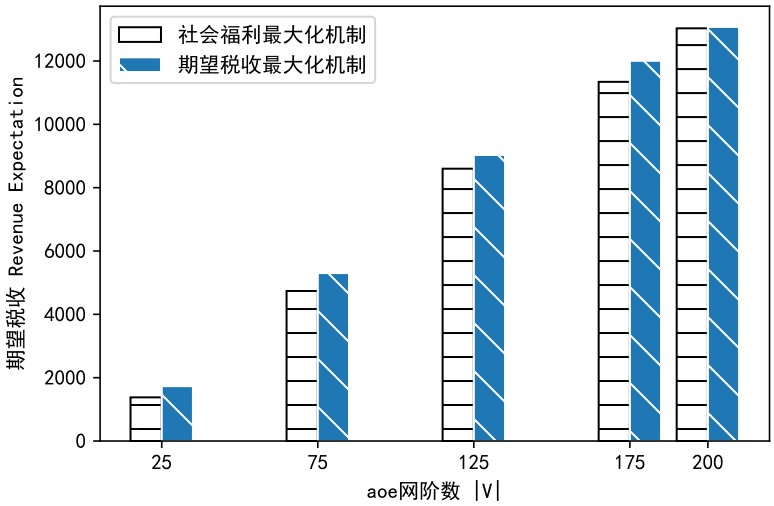

图 4-8 期望税收的比较

4.4 本章小结

针对多方数据价值共享计算任务中子计算任务存在复杂依赖关系的问题提出时间敏感价值共享激励模型。本章以 AOE 网进行建模。将参与者完成子任务的时长作为最关键性能指标，并映射至 AOE 网中。详细分析了总任务在限制时间内完成的条件下的社会福利最优化分配问题。然后证明了其 NP 困难性，并给出一种基于贪心思想的近似求解方案，该方案可以在多项式时间内求解，时间复杂度是 $O(|E|^2 * n * (|V| + |E|))$。另外，分析了基于参与者私密值 Val_i 概率分布的期望税收最大化机制。然后通过模拟实验说明了两种机制的性能和有效性。

第五章 数据价值共享激励拍卖系统设计与实现

本章设计并实现数据价值共享激励拍卖系统，来应用前文的两种拍卖机制。

5.1 概述

本文的第三四章分别设计了两种计算场景下的拍卖激励机制。本章根据这两种拍卖机制，为多方数据价值共享计算模式设计一个拍卖系统。该系统能够帮助平台方完成胜出者决策的流程，妥善处理多方计算中的参与者竞争现象。本系统的硬件环境是：Intel Core i5-7400 3.0GHZ，主存 12GB。实现技术：bootstrap、php、codeigniter、apache2 httpd、mysql。

5.2 总体设计

该拍卖系统的总体结构如下图所示，主要包含用户及资源管理子系统、简单可并行计算拍卖子系统、依赖相关计算拍卖子系统、前端展示系统。

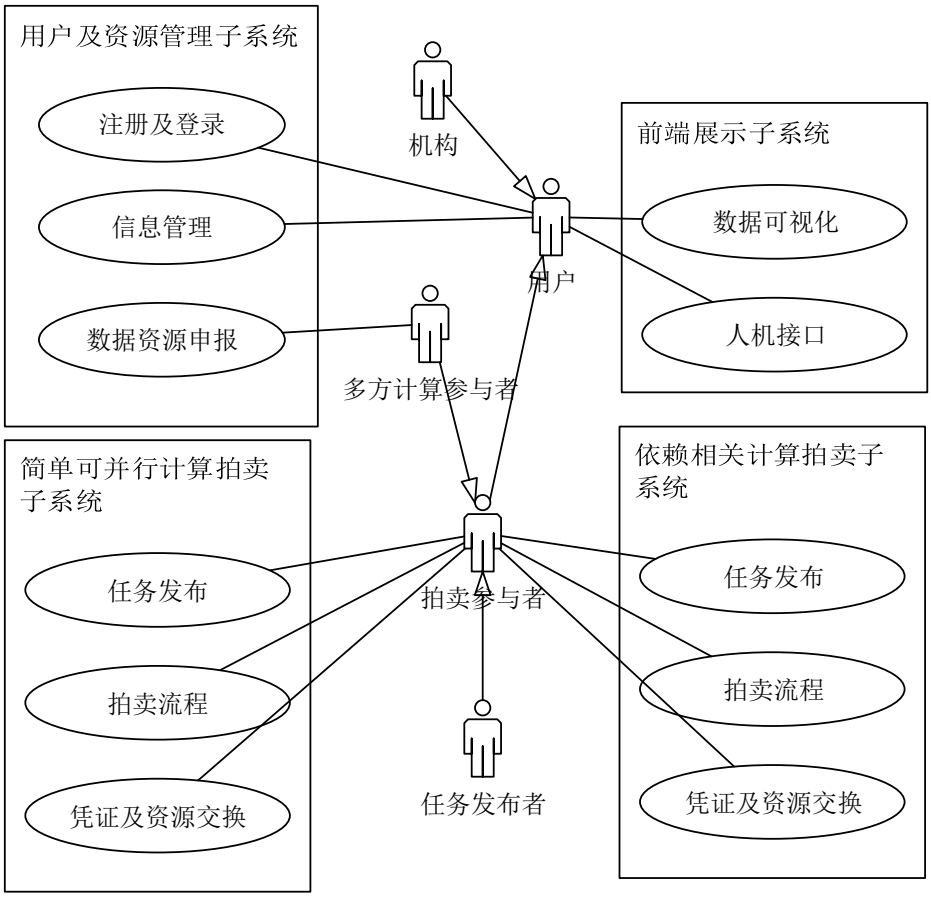

图 5-1 拍卖系统总体结构

用户及资源管理子系统主要维护所有的人员信息及数据资源信息，一切与参与者相关的设置都在这里完成。主要包含了注册登录模块、信息管理模块、数据资源申报模块。前端展示子系统承担了数据可视化及人机接口的功能，这是管理员配置信息、任务发布者发布多方计算任务、参与者进行拍卖等系统重要流程的接口。简单可并行计算拍卖子系统和依赖相关计算拍卖子系统分别对应于第三章和第四章具体场景及对应算法的实现。主要包含任务发布模块、拍卖流程模块、凭证及资源交换模块。

5.3 子系统及模块设计

本节对子系统及其模块进行进一步设计。

5.3.1 用户及资源管理子系统

在用户及资源管理子系统中，主要有注册及登录模块、信息管理模块、数据资源申报模块。注册及登录模块实现用户分类、权限设置、管理员增删查改等功能。在本系统中，用户共有三类：机构，如第三章所定义，是拥有数据资源的组织。多方计算参与者是隶属于机构的计算单元 (unit)，他们是多方计算的真正执行者。任务发布者即多方计算任务的需求方，通过该系统获得相应的数据价值。

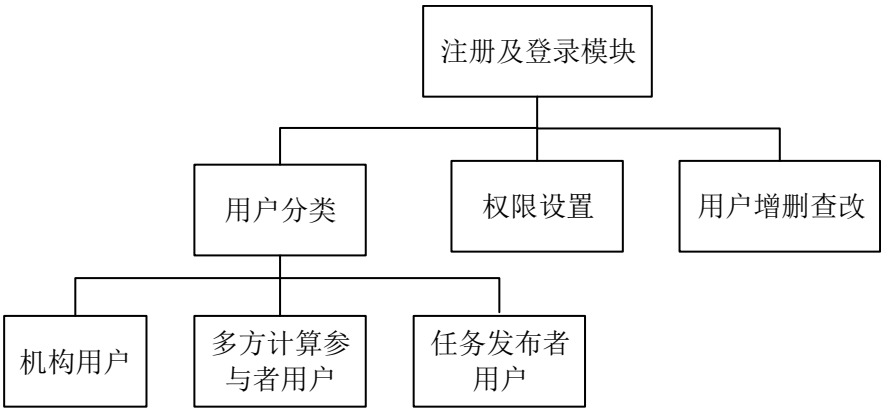

图 5-2 注册及登录模块

信息管理模块对用户相关的重要信息进行管理，包括用户的责任单位、联系方式、隶属关系 (例如第三章所定义的树形关系)、数字证书等基本信息、以及计算参与者的信誉评级、机构的指标集约束等信息（详见第三、四章相关描述与定义）。

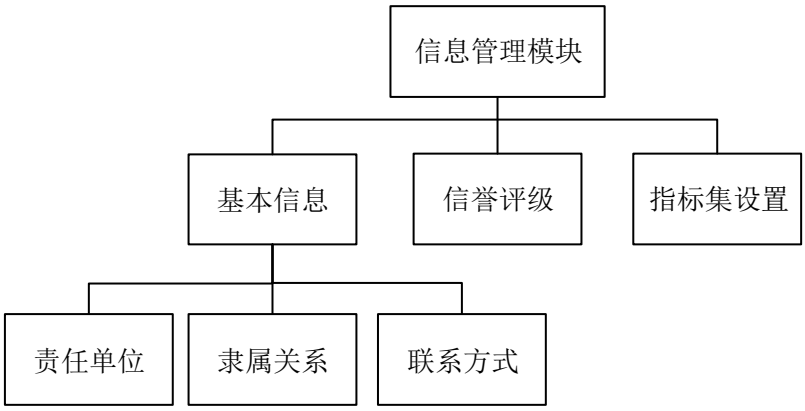

图 5-3 信息管理模块

数据资源申报模块是用户及资源管理子系统中最重要的部分，多方计算参与者在此处申报可提供的本地资源数据，这也是多方计算拆解算法的主要输入之一。基本信息描述了可提供的数据的相关元数据，包括但不限于类型、规模、来源、精度指标等。互斥关系指本文第三章同机构的不同参与者提供同质数据内容的情况，此时需要描述参与者申报的数据资源之间的互斥关系。

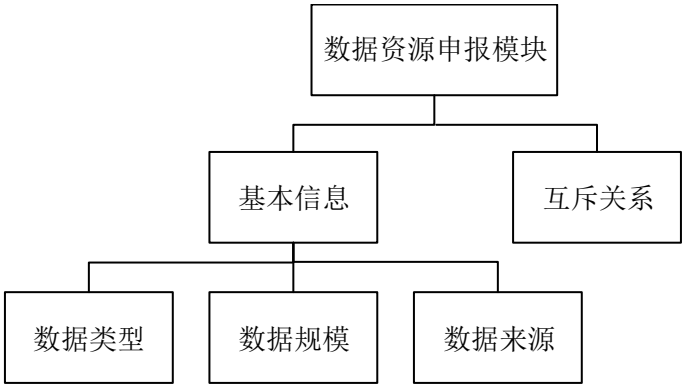

图 5-4 数据资源申报模块

5.3.2 前端展示子系统

前端展示子系统主要包括多方数据可视化模块及用户 UI 模块。多方数据可视化模块可以对现有的数据资源进行可视化展示。用户 UI 模块是用户使用系统的主要接口，所有多方数据价值共享激励拍卖相关的操作均需要在用户 UI 完成。

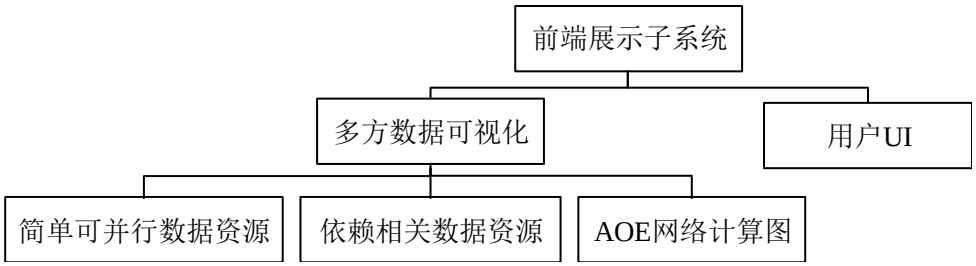

图 5-5 前端展示子系统

5.3.3 简单可并行计算拍卖子系统

本子系统实现简单可并行场景下的拍卖核心流程。首先，任务发布者在本系统中发布简单可并行计算任务，设置任务开始时间、需求数据类型、标的截止时间、指标集约束等一系列任务细节信息。然后，系统以参与者的信息为基础，根据任务需求，筛选符合要求的参与者子集，并将拍卖信息推送给参与者。参与者接受到信息后，根据自身意愿选择是否在截止时间前进行投标，即参与到该任务的竞拍环节。拍卖截止时间到达后，系统综合所有参与者的信息，选择决定胜出者所需的具体算法。对于任务方不存在指标集约束的场景，仅有数量的需求，系统以第三章的简单可并行的数据量约束模型求解，主要是以贪心算法进行快速求解。若任务方存在指标集约束，但参与者的关系是对等的，不存在森林状机构约束，则以指标集约束模型求解。否则，以机构约束模型进行求解。确定了胜出者后，以相应的分配结果向参与者发放多方计算凭证 (也可以签订电子合约)，并以对应价格向参与者支付费用 $allocation_i * INCENT - payment_i$。然后进行多方计算的实际执行，完成后，由平台方或者任务方对信誉系统更新。详细流程信息见图5-6。

5.3.4 依赖相关计算拍卖子系统

本子系统实现依赖相关计算的拍卖核心流程。首先，任务方在系统内发布依赖相关的多方计算任务，设置任务时间限制。任务分解算法根据现有的数据资源申报情况将其拆解为一系列子任务，形成 AOE 网结构。然后，系统依照 AOE 网将拍卖信息发送给各条有向弧上的参与者。参与者仍然需要在拍卖投标的截止时间内设置其标的，否则视为不参与该次多方计算拍卖。接下来，系统根据设置的拍卖偏好选择相应的算法机制。若偏向社会福利最大化，则选择依赖相关计算模型的贪心算法确定胜出者。否则，以历史数据拟合的分布或者预设概率分布作为最优拍卖模型的输入，确定相应的胜出者。若原任务无法完成，则对任务方进行反馈或者指导任务方重新设置时间限制条件。若任务能够完成，则发放凭证并支付报酬。最后实际执行多方计算，并根据结果对信誉系统进行更新。如图5-7。

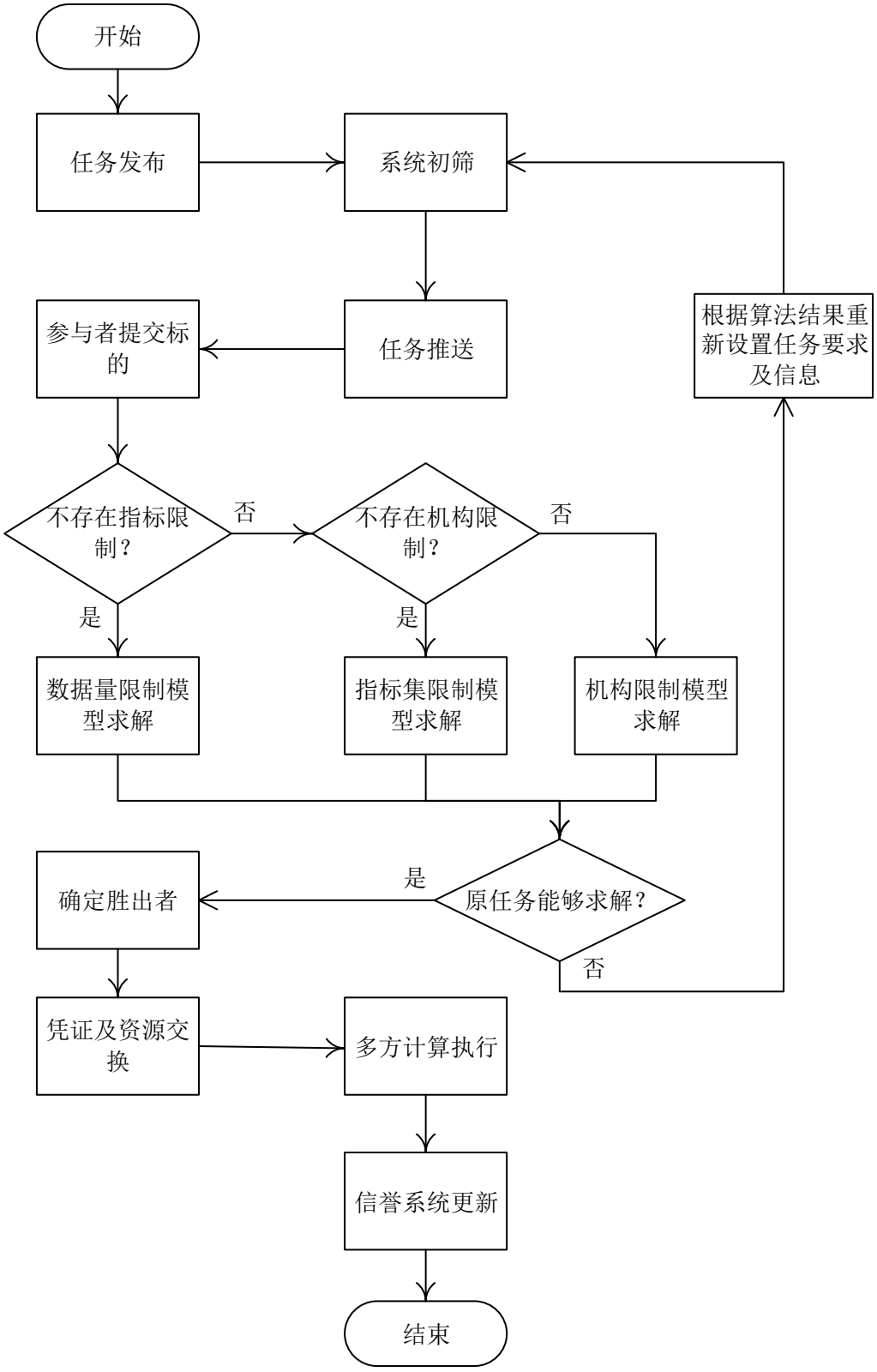

图 5-6 简单可并行计算拍卖流程

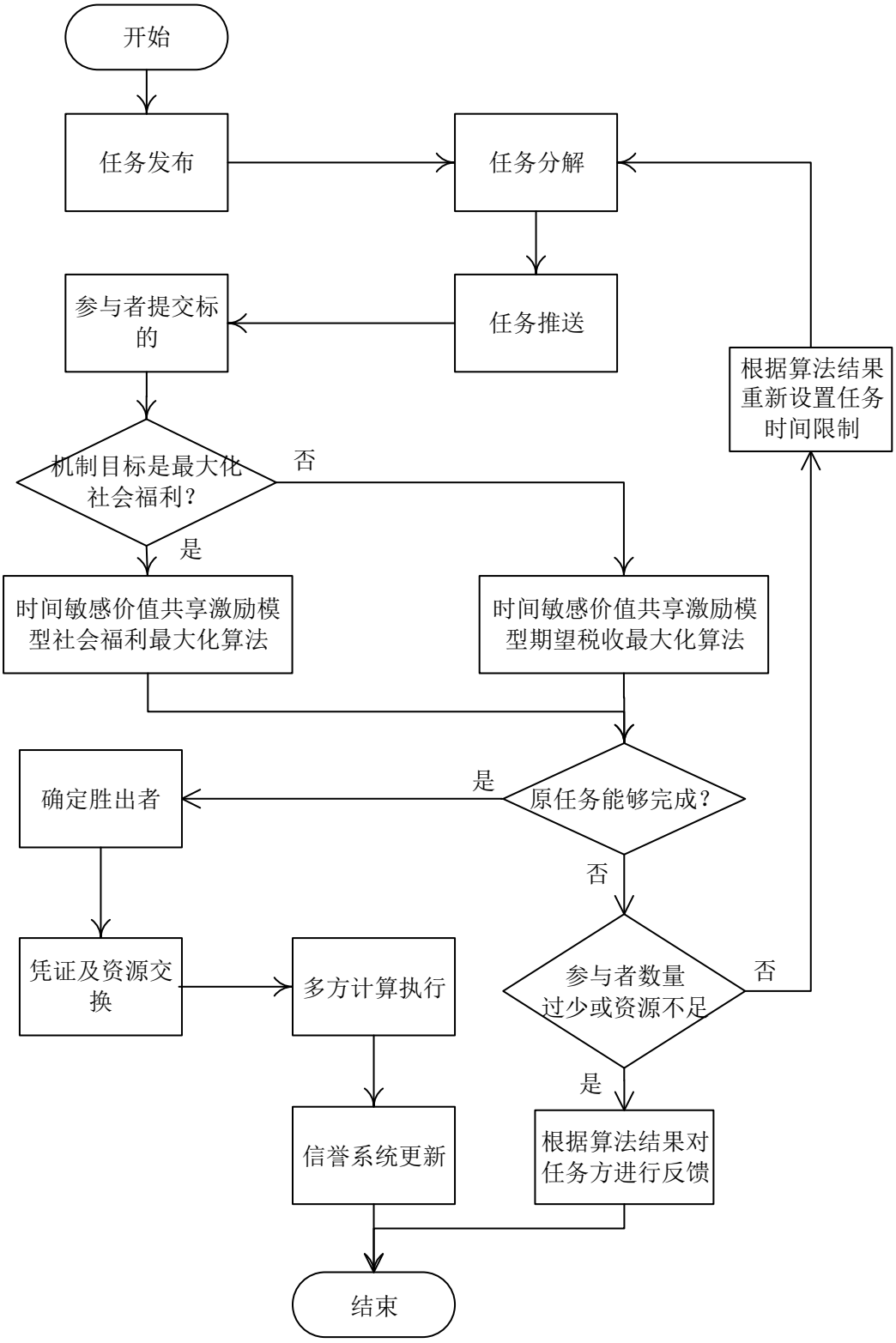

图 5-7 依赖相关计算拍卖流程

5.4 界面展示

在前端展示子系统中，人机接口是最重要的模块。这是用户参与数据价值共享的窗口，友好的界面可以增加用户的使用体验，有利于促进数据价值共享。本节对数据价值共享激励拍卖系统部分核心功能进行界面展示。

图 5-8 个人信息管理

如图5-8所示，用户可以在此对自己的基本信息进行修改、查看信誉评级。机构用户还能够设置自己的指标集约束内容。

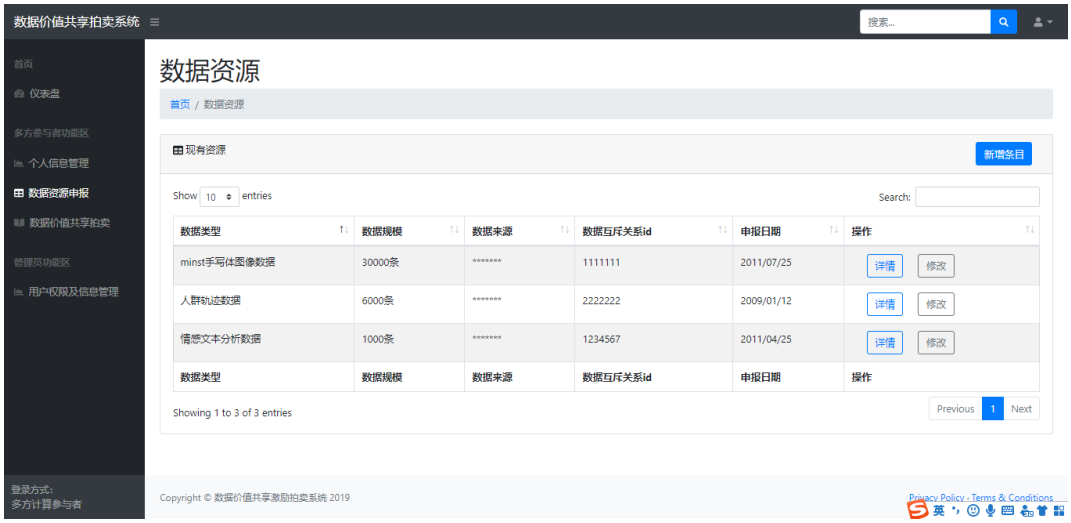

图 5-9 资源申报

如图5-9所示，多方计算的参与者可以在此进行可计算的资源申报，此处的信息也是拍卖机制运行的基础。

图 5-10 用户权限及信息管理

对于管理员而言，可以在界面5-10中对普通参与者的信息、权限进行修改、管理。

然后是本系统的核心部分，数据价值共享拍卖，此处包含了简单可并行和依赖相关两种任务类型。在界面5-11中，任务方可以发布多方计算任务。参与者可以完成浏览拍卖信息、投标、查看结果等一系列参与拍卖的重要流程。详情信息见界面5-12、5-13、5-14、5-15。

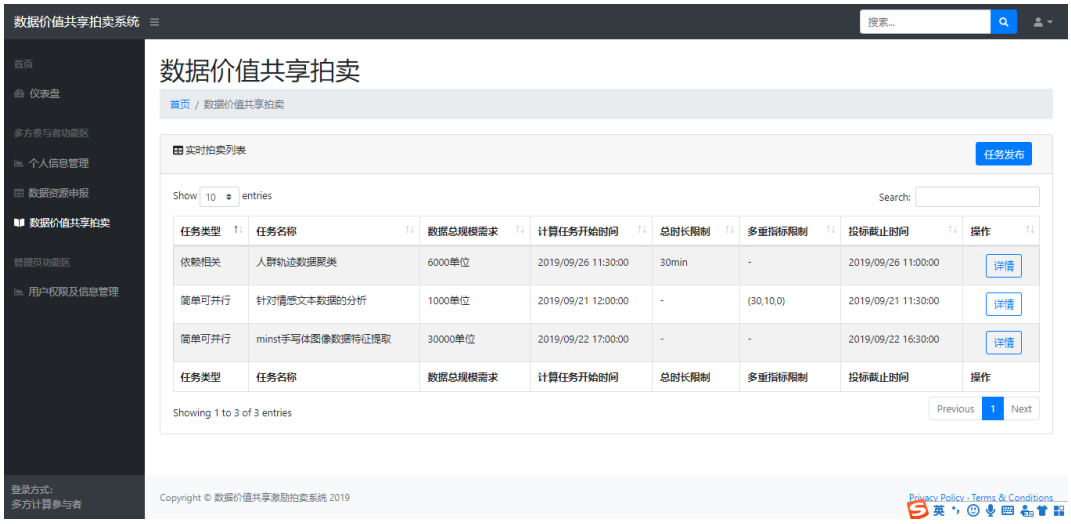

图 5-11 数据价值共享拍卖

如图5-11，参与者可以在实时拍卖列表中选择感兴趣的多方计算任务。该列表仅展示当前用户能够参与的拍卖，即当前用户能够利用其本地数据提供计算，分享数据价值给任务方。

实时拍卖列表会详细展示任务类型、任务名称、数据量需求、计算任务开始时

间、总时长限制、指标集约束、投标截止时间等一系列多方计算任务的细节信息。

用户可以点击任务详情进入投标界面，如图5-12，此处会展示用户标的上限*INCENT*，该上限由任务方设置。为了确保安全性，用户需要以密码对标的进行确认。

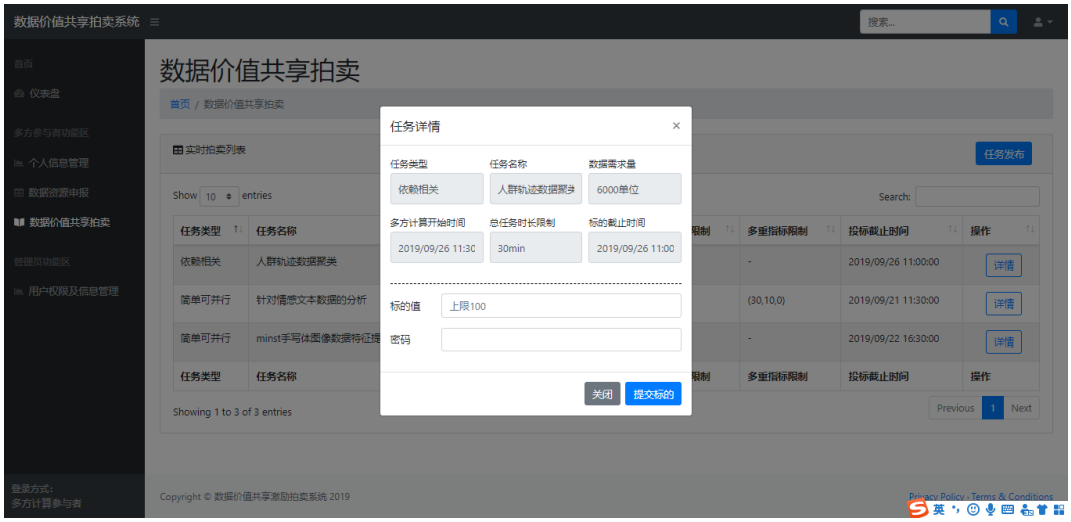

图 5-12 数据价值共享拍卖的投标

当标的截止时间到达后，该多方任务出于不可投标状态。系统综合所有信息开始运行拍卖算法，如图5-13。

图 5-13 数据价值共享拍卖的算法运行

一段时间后，拍卖算法运行完毕。对于参与者来说有两种结果，胜出或者失败。若用户胜出，则系统向其公布报酬。参与者需要再次以密码确认竞拍结果。然后交换数据凭证，并为实际的多方计算任务做准备，如图5-14所示。

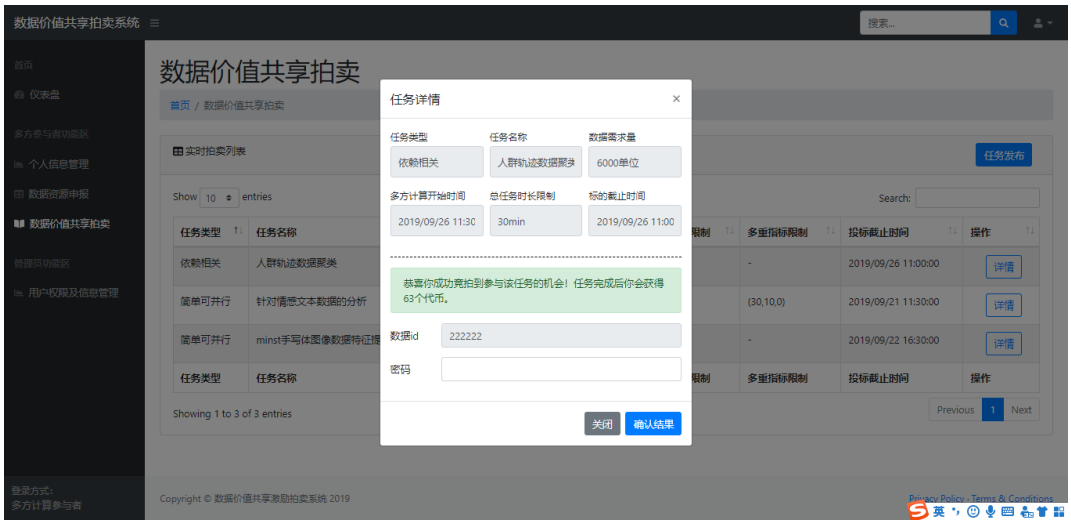

图 5-14 参与者胜出

若参与者失败，则用户的状态并不发生改变。用户可以继续在实时拍卖列表中选择新的多方计算任务, 如图5-15。

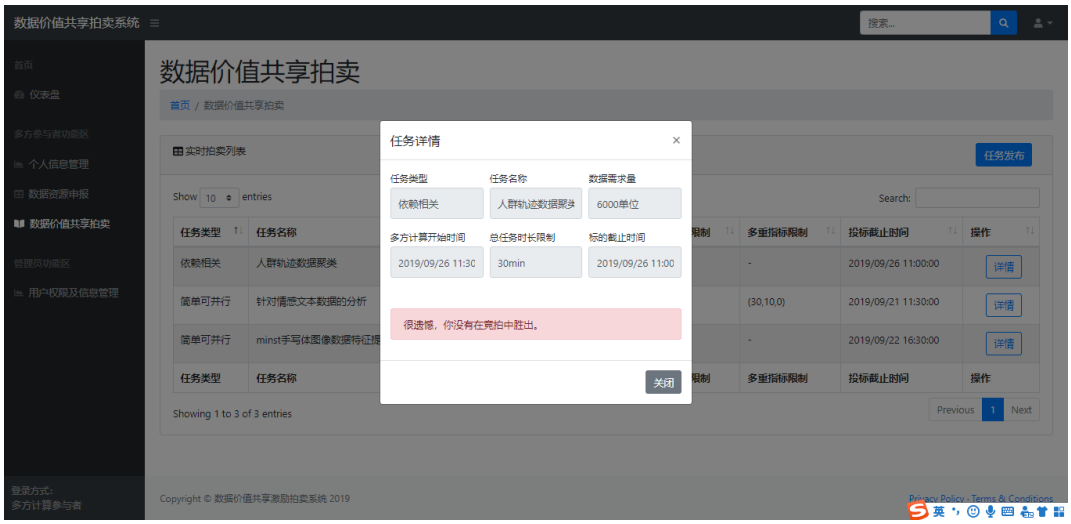

图 5-15 参与者失败

同时，为了及时将拍卖信息传递给不同的用户，系统设计了相应的消息反馈机制。包括推送新的拍卖信息、公布参与者的拍卖结果、向任务方反馈计算任务可行性。详见界面5-16、5-17、5-18、5-19。

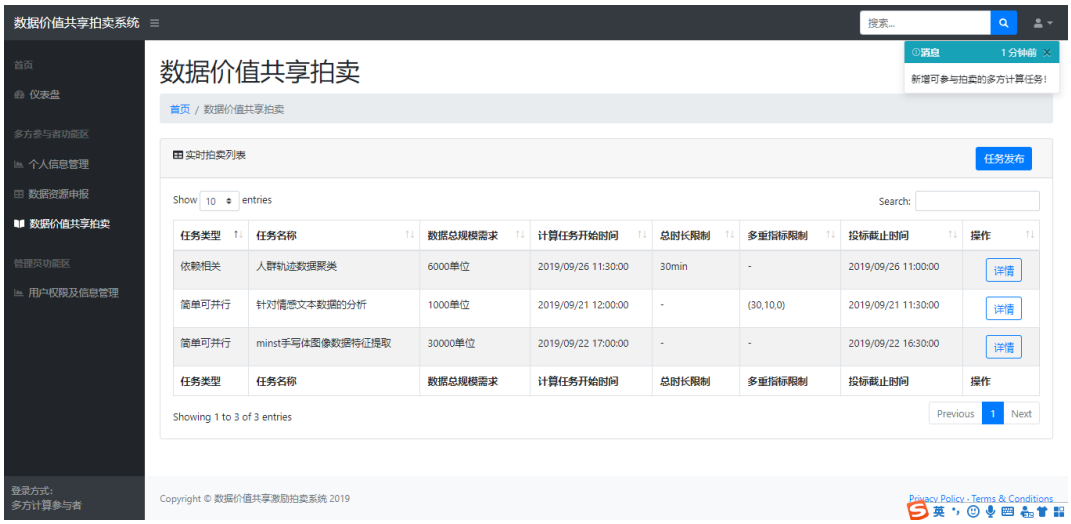

图 5-16 新增可参与的拍卖消息

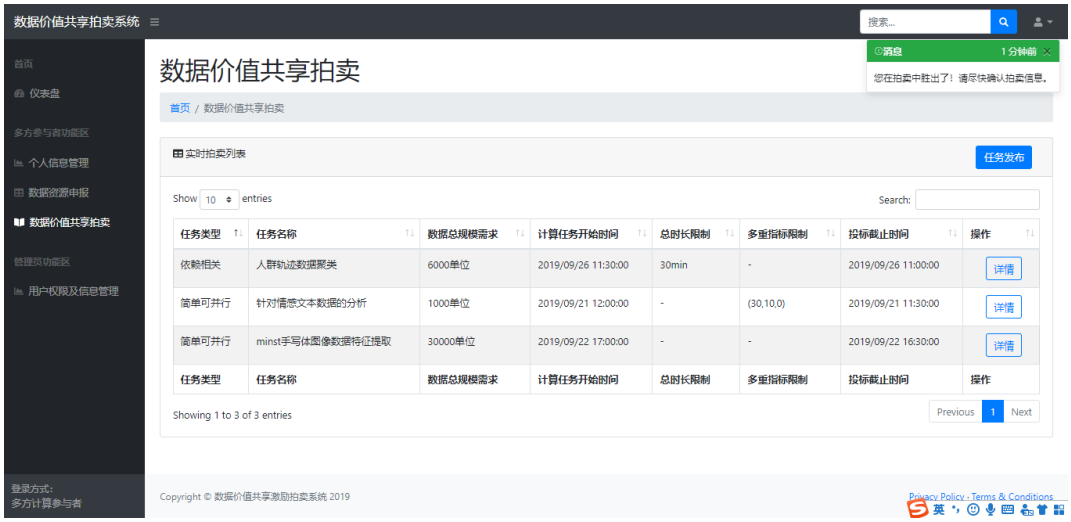

图 5-17 参与者的胜出消息

当用户浏览其他界面时，实时的拍卖信息会传递到用户的前端界面, 图5-16、图5-17、图5-18分别是新的可参与拍卖、参与者胜出、参与者失败的事件消息。

由于现有数据的缺乏、数据分布的复杂性、任务方限制指标过多、多方计算参与者不愿参与等多种不可控因素，任务发布者提交的多方计算任务可能无法成功完成。此时，平台方需要向任务方反馈，引导其调整任务信息，并重新发布。促进系统资源最大化利用，如图5-19。

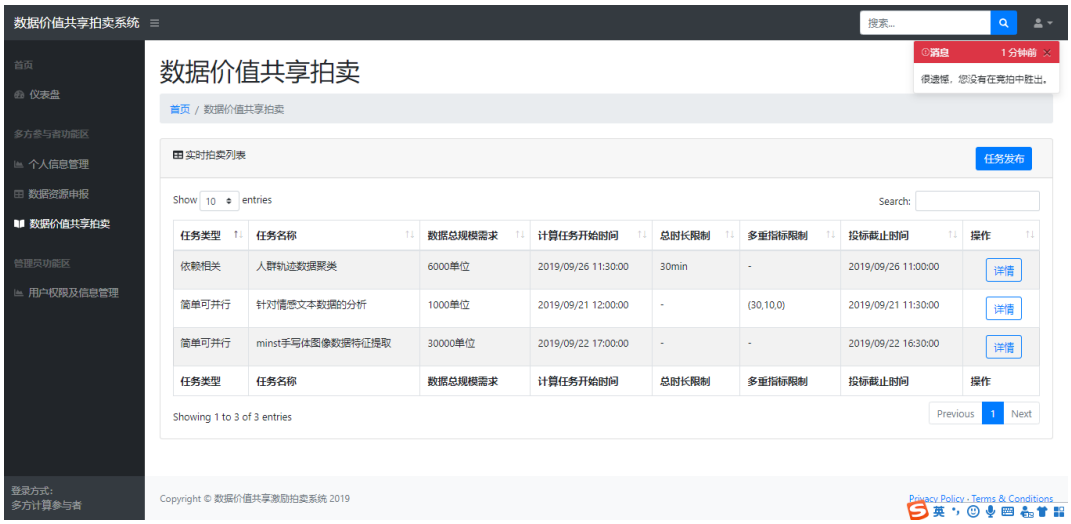

图 5-18 参与者的失败消息

图 5-19 向任务方反馈

5.5 系统功能测试

本系统的核心功能是完成数据资源申报及完成多方数据价值共享激励拍卖。拍卖主要有简单可并行和依赖相关两种不同的计算任务类型。因而本节针对本系统的核心功能点做测试，并测量系统完成相应功能逻辑所需时间，从而估计系统使用者的服务等待时间。主要结果如表5-1所示。

由测试结果可知，系统的功能运转基本正常，能够在可接受的时间范围内给出用户服务响应，可以承担数据价值共享拍卖的任务。

表 5-1 核心功能测试结果表

功能点名称	测试步骤	测试结果	运行时间（秒）
可计算资源申报功能测试	1. 以多方计算参与者的身份登录。 2. 进入数据资源申报。 3. 点击新增条目。 4. 输入详细的数据信息并提交。	通过	2s
简单可并行拍卖任务功能测试	1. 以多方计算参与者的身份登录。 2. 进入数据价值共享拍卖。 3. 选择具体任务并投标。 4. 等待系统公布竞拍结果。	通过	3s
依赖相关拍卖任务功能测试	1. 以多方计算参与者的身份登录系统。 2. 进入数据价值共享拍卖。 3. 选择具体任务并投标。 4. 等待系统公布竞拍结果。	通过	20s
拍卖任务发布功能测试	1. 以任务发布者的身份登录系统。 2. 进入数据价值共享拍卖。 3. 点击任务发布，填写任务详细信息。 4. 提交系统，等待系统更新。	通过	2s

5.6 本章小结

本章对数据价值共享激励拍卖系统进行了实现，将本文三四章的场景及算法应用到具体的系统环境中。首先概述了系统的硬件环境及技术方法，然后依次分析了系统的总体模块设计、子系统的详细模块设计，最后对部分功能界面进行展示分析。由系统的运行情况可知，主体功能运行良好，能够有效实现数据价值共享的主要竞拍流程。

第六章 全文总结与展望

6.1 全文总结

在大数据分析及应用日新月异的今天，医疗、商业、科学等诸多领域的进一步发展都离不开对数据的挖掘利用。同时各方数据拥有者的安全意识不断增强，需要新的数据使用模式来适应更强的数据使用安全需求。而多方数据价值共享计算是这样的一种共享数据价值而非数据本身计算模式。在现有的社会规则、从属关系等限制条件下，其打破“数据孤岛”，联合使用多方数据创造更大的价值，同时尽可能减少原数据传输，保证数据的使用安全。本文在此基础上引入拍卖激励体系，针对不同计算场景设计了 DSIC 拍卖机制，解决多方数据价值共享计算中的参与者竞争问题，促进更多的参与者加入数据价值共享体系，建立积极的数据价值共享生态。具体来讲，本文完成了如下工作：

第三章描述了多方数据价值共享计算模式的流程与特点。针对简单可并行数据价值共享计算提出多约束价值共享激励模型。首先根据实际场景将参与者之间的竞争建立为正向拍卖模型，对参与者效用函数、社会福利等进行定义，分别引入数据量约束、指标集约束和机构约束。然后针对这三种不同的限制条件，分别以朴素的贪心算法、有界背包算法、更一般的动态规划算法，来精确求解社会福利最大化问题，从而确定各限制条件下的分配算法和价格算法。这三种算法的时间复杂度依次递增。最后以模拟实验分析说明了三种算法的有效性。

第四章分析了依赖相关数据价值共享计算的特点，提出以计算时间作为主要限制条件的时间敏感价值共享激励模型。首先根据实际场景以 AOE 网建模，论证了总时间限制下保证社会福利最大化问题的 NP 困难性。然后提出基于贪心的启发式算法对该问题近似求解，从而确定相应的分配算法和价格算法。最后，以此为基础，在考虑任务方期望收益最大化的条件下，设计了依赖于正态分布的最优拍卖机制。模拟实验说明了贪心的启发式算法和最优拍卖机制的性能和有效性。

第五章将三、四章的场景及核心算法进行实现，设计并部署了数据价值共享激励拍卖系统。该系统能够完成数据价值共享拍卖的主体流程。系统的运行结果表现了较好的性能。

总的来说，本文的工作初步解决了数据价值共享模式中的参与者竞争问题，能够较好地激励数据拥有着真实地表达他们对数据价值共享计算任务的估值，降低参与数据价值共享计算的复杂性，促进公平竞争，保证他们参与价值共享的收益。这有利于充分调动数据拥有者的积极性，减少“数据孤岛”现象，促进分布

式多方数据的利用。

6.2 后续工作展望

本文针对简单可并行计算和依赖相关计算两种场景设计了激励机制及算法，能够初步解决一些主要问题。然而仍然存在一些值得继续优化深入的研究工作：

1. 简单可并行场景中，在引入机构约束时，拍卖机制的时间复杂度较高，达到了 $O(m*S^2)$，其中 m 是机构的数量，而 S 是五维限制状态的总数量。在有限的计算资源下，限制指标的尺度范围将会极大受限。可以考虑引入近似的启发式算法。另外，也可以进一步分析更复杂的同质参与者的互斥关系限制。
2. 依赖相关场景中，可以在时间限制的条件下，进一步引入其他指标限制。同样的，这也将极大增加问题的困难性。
3. 本文的两个场景的拍卖机制均为单变量环境下的 DSIC 机制，可以进一步挖掘计算场景的特点，考虑多变量环境下的组合拍卖机制设计，或非 DSIC 机制设计。

致 谢

时间过得很快，三年的研究生生涯就要划上句号。在这三年中，一方面我进一步夯实了基础知识，见识到了更加广阔的学术领域和氛围，坚定了内心的想法与方向。另一方面也结实了更多良师益友，收获很多。

首先感谢我的导师罗光春老师，他扎实的专业知识及严谨的治学风范为我树立了良好的榜样。激励着我在科研学习及日常生活中踏实努力，不断追求新的高度。

感谢陈爱国老师，陈老师在这三年中给予了我许多帮助，无论是在项目工程或是论文撰写，都尽心尽力，耐心地给予督导和指点。在我遇到陌生的研究领域及较大的科研困难时，还常常请求其他老师给予我针对性的帮助。陈老师认真负责的科研工作态度也激励着我进一步的努力学习，钻研探索。

也要感谢田玲老师，尤其是三年前的秋天，我独自来到实验室面试，非常感谢田老师在短短一个小时的面谈中肯定我的学习能力及成绩，并给予在实验室继续攻读硕士学位的机会。在本论文的撰写过程中田老师也给予了指导和帮助。

然后感谢郑旭老师，在过去的两年时光中，郑老师经常参与我们的组会，为我们提供了许多科研项目的新思路和见解，使我们受益匪浅。在论文撰写的过程中，郑老师也给予我非常多的指导和帮助。郑老师的学术能力、处事方式都值得我学习。

还要感谢赵太银老师，赵老师专业知识扎实，为人非常有亲和力，在日常学习生活中也给予我许多帮助，是值得学生敬重与爱戴的好老师。

另外感谢各位同组同门：陈远帆、邵福骏、谢渊、骆佳程、李思宁，以及好朋友刘竹、胡小东。

最后感谢我的父母，生活中给予我无微不至的照顾与关怀。

致　谢

参考文献

[1] 赛迪顾问. 2019 中国大数据产业发展白皮书 [R]. 北京: 赛迪顾问, 2019 年 4 月 1 日

[2] L. Hurwicz. On informationally decentralized systems[J]. Decision and organization: A volume in Honor of J. Marschak, 1972, 1-1

[3] W. Vickrey. Counterspeculation, auctions, and competitive sealed tenders[J]. The Journal of finance, 1961, 16(1): 8-37

[4] B. Edelman, M. Ostrovsky, M. Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords[J]. American economic review, 2007, 97(1): 242-259

[5] H. R. Varian. Position auctions[J]. international Journal of industrial Organization, 2007, 25(6): 1163-1178

[6] A. V. Goldberg, J. D. Hartline, A. R. Karlin, et al. Competitive auctions[J]. Games and Economic Behavior, 2006, 55(2): 242-269

[7] N. Nisan, A. Ronen. Algorithmic mechanism design[J]. Games and Economic behavior, 2001, 35(1-2): 166-196

[8] D. Lehmann, L. I. Oćallaghan, Y. Shoham. Truth revelation in approximately efficient combinatorial auctions[J]. Journal of the ACM (JACM), 2002, 49(5): 577-602

[9] A. Archer, É. Tardos. Truthful mechanisms for one-parameter agents[C]. Proceedings 42nd IEEE Symposium on Foundations of Computer Science, 2001, 482-491

[10] A. Mu'Alem, N. Nisan. Truthful approximation mechanisms for restricted combinatorial auctions[J]. Games and Economic Behavior, 2008, 64(2): 612-631

[11] A. Gibbard. Manipulation of voting schemes: a general result[J]. Econometrica: journal of the Econometric Society, 1973, 587-601

[12] O. H. Ibarra, C. E. Kim. Fast approximation algorithms for the knapsack and sum of subset problems[J]. Journal of the ACM (JACM), 1975, 22(4): 463-468

[13] P. Briest, P. Krysta, B. Vöcking. Approximation techniques for utilitarian mechanism design[C]. Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, 2005, 39-48

[14] R. B. Myerson. Optimal auction design[J]. Mathematics of operations research, 1981, 6(1): 58-73

[15] M. Ostrovsky, M. Schwarz. Reserve prices in internet advertising auctions: A field experiment[C]. Proceedings of the 12th ACM conference on Electronic commerce, 2011, 59-60

[16] L. Gao, Y. Xu, X. Wang. Map: Multiauctioneer progressive auction for dynamic spectrum access[J]. IEEE Transactions on Mobile Computing, 2010, 10(8): 1144-1161

[17] W. Wang, B. Li, B. Liang. District: Embracing local markets in truthful spectrum double auctions[C]. 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2011, 521-529

[18] D. Yang, X. Zhang, G. Xue. Promise: A framework for truthful and profit maximizing spectrum double auctions[C]. IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, 109-117

[19] X. Zhou, S. Gandhi, S. Suri, et al. ebay in the sky: Strategy-proof wireless spectrum auctions[C]. Proceedings of the 14th ACM international conference on Mobile computing and networking, 2008, 2-13

[20] S. J. Rassenti, V. L. Smith, R. L. Bulfin. A combinatorial auction mechanism for airport time slot allocation[J]. The Bell Journal of Economics, 1982, 402-417

[21] P. Cramton, J. A. Schwartz. Collusive bidding: Lessons from the fcc spectrum auctions[J]. Journal of regulatory Economics, 2000, 17(3): 229-252

[22] F. C. Commission, F. C. Commission. Procedures for competitive bidding in auction 1000, including initial clearing target determination, qualifying to bid, and bidding in auctions 1001 (reverse) and 1002 (forward)[J]. Public notice FCC, 2015, 15-78

[23] A. E. Roth, T. Sönmez, M. U. Ünver. Kidney exchange[J]. The Quarterly journal of economics, 2004, 119(2): 457-488

[24] A. E. Roth, T. Sönmez, M. U. Ünver. Pairwise kidney exchange[J]. Journal of Economic theory, 2005, 125(2): 151-188

[25] A. E. Roth, T. Sönmez, M. U. Ünver. Efficient kidney exchange: Coincidence of wants in markets with compatibility-based preferences[J]. American Economic Review, 2007, 97(3): 828-851

[26] K. Sack. 60 lives, 30 kidneys, all linked[J]. New York Times, , 18: 124-124

[27] I. Ashlagi, F. Fischer, I. A. Kash, et al. Mix and match: A strategyproof mechanism for multi-hospital kidney exchange[J]. Games and Economic Behavior, 2015, 91: 284-296

[28] D. Gale, L. S. Shapley. College admissions and the stability of marriage[J]. The American Mathematical Monthly, 1962, 69(1): 9-15

[29] L. E. Dubins, D. A. Freedman. Machiavelli and the gale-shapley algorithm[J]. The American Mathematical Monthly, 1981, 88(7): 485-494

[30] C. T. Chou, N. Bulusu, S. Kanhere, et al. Sensing data market[J]. Proceedings of Poster Papers, 2007, 13-13

[31] S. Reddy, D. Estrin, M. Srivastava. Recruitment framework for participatory sensing data collections[C]. International Conference on Pervasive Computing, 2010, 138-155

[32] G. Danezis, S. Lewis, R. J. Anderson. How much is location privacy worth?[C]. WEIS, 2005, 21-35

[33] J.-S. Lee, B. Hoh. Sell your experiences: a market mechanism based incentive for participatory sensing[C]. 2010 IEEE International Conference on Pervasive Computing and Communications (PerCom), 2010, 60-68

[34] L. Duan, T. Kubo, K. Sugiyama, et al. Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing[C]. 2012 Proceedings IEEE INFOCOM, 2012, 1701-1709

[35] Q. Li, G. Cao. Providing privacy-aware incentives for mobile sensing[C]. 2013 IEEE international conference on pervasive computing and communications (PerCom), 2013, 76-84

[36] I. Koutsopoulos. Optimal incentive-driven design of participatory sensing systems[C]. 2013 Proceedings IEEE INFOCOM, 2013, 1402-1410

[37] T. Luo, H.-P. Tan, L. Xia. Profit-maximizing incentive for participatory sensing[C]. IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, 127-135

[38] D. Zhao, X.-Y. Li, H. Ma. How to crowdsource tasks truthfully without sacrificing utility: Online incentive mechanisms with budget constraint[C]. IEEE INFOCOM 2014-IEEE Conference on Computer Communications, 2014, 1213-1221

[39] A. Hard, K. Rao, R. Mathews, et al. Federated Learning for Mobile Keyboard Prediction[J]. arXiv e-prints, 2018, arXiv:1811.03604

[40] Q. Yang, Y. Liu, T. Chen, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19

[41] X. Wang, Y. Han, C. Wang, et al. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning[J]. IEEE Network, 2019, 33(5): 156-165

[42] N. H. Tran, W. Bao, A. Zomaya, et al. Federated learning over wireless networks: Optimization model design and analysis[C]. IEEE INFOCOM 2019-IEEE Conference on Computer Communications, 2019, 1387-1395

[43] S. Samarakoon, M. Bennis, W. Saad, et al. Federated learning for ultra-reliable low-latency v2v communications[C]. 2018 IEEE Global Communications Conference (GLOBECOM), 2018, 1-7

[44] M. Shayan. Biscotti - a ledger for private and secure peer to peer machine learning[D]. , 2019,

[45] H. Kim, J. Park, M. Bennis, et al. Blockchained on-device federated learning[J]. IEEE Communications Letters, 2019, 1-1

[46] C. Fung, C. J. M. Yoon, I. Beschastnikh. Mitigating Sybils in Federated Learning Poisoning[J]. arXiv e-prints, 2018, arXiv:1808.04866

[47] T. Nishio, R. Yonetani. Client selection for federated learning with heterogeneous resources in mobile edge[C]. ICC 2019-2019 IEEE International Conference on Communications (ICC), 2019, 1-7

[48] S. Zhong, L. E. Li, Y. G. Liu, et al. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks[J]. Wireless networks, 2007, 13(6): 799-816

[49] L. Chen, L. Libman, J. Leneutre. Conflicts and incentives in wireless cooperative relaying: A distributed market pricing framework[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 22(5): 758-772

[50] D. Yang, X. Fang, G. Xue. Truthful auction for cooperative communications[C]. Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2011, 1-10

攻读专业硕士学位期间取得的成果

[1] 学业一等奖学金，2017 年 10 月

[2] 学业一等奖学金，2018 年 10 月

[3] 学业二等奖学金，2019 年 10 月

[4] 参与军口项目：XXX 大数据可信服务关键技术，2019