



QG中期考核详细报告书

题  目 《Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design》

学  院 计算机学院

专 业 计算机类

年级班别 24 7班

学 号 3124004280

学生姓名 何晨洋

2025年 4月 3日

目录

[目录 - 1 -](#_Toc194700172)

[1、 文摘 - 1 -](#_Toc194700173)

[2、 文献简介 - 1 -](#_Toc194700174)

[2.1 文献研究的核心与面临的问题 - 1 -](#_Toc194700175)

[3、 文献提出的理论及其核心算法介绍 - 1 -](#_Toc194700176)

[3.1 基本理论与方法 - 1 -](#_Toc194700177)

[3.2 核心算法与公式 - 1 -](#_Toc194700178)

[4、 复现实验结果与流程 - 1 -](#_Toc194700179)

[4.1 公式与参数设置 - 1 -](#_Toc194700180)

1. [启示与思考 - 1 -](#_Toc194700182)

**1、文摘**

**本文献主要讲述了在对数据进行充分保护的情况下，多智能体系统的平均共识问题，即实现了保护隐私与智能体状态对初始状态平均值的共识。主要贡献有：**

**1. 理论结果：证明了在保护差分隐私的前提下智能体无法实现（0，0）精确收敛到初始平均值.**

**2. 算法设计：提出了基于拉普拉斯算法的新的差分隐私共识算法。该算法通过线性状态变化和消息生成函数中加入一个呈指数衰减的拉普拉斯噪声用于保护隐私。并证明了该算法几乎必然收敛到智能体初始状态平均值的无偏估计.**

**3. 性能优化：分析了算法中参数的最优选择，保证了收敛点的方差最小值，并将其与其他方法进行比较，证明最有设计应是对初始状态的一次性扰动.**

**4. 模拟验证：通过模拟实验验证了理论结果，展示了算法在不同隐私保护水平下的性能表现.**

1. **文献简介**
   1. **文献研究的核心与面临的问题**

Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design

Erfan Nozari, Pavankumar Tallapragada, Jorge Cortés

文献基于多智能体系统的差分隐私保护下的平均共识问题开展研究，即如何在保护每个智能体初始状态的数据隐私的前提下，使得智能体们能达成对其初始状态平均值的共识。

在解决该问题过程中，需要解决隐私与共识的矛盾。基于差分隐私的要求，智能体的初始状态信息不能被准确推断，这恰好与达成平均共识的目标，即精确收敛到初始状态平均值存在矛盾。而就此矛盾而建立的算法需要同时兼顾二者，即需要能够充分保护智能体初始状态的隐私，又要保证模型最终收敛到接近初始状态平均值，即初始状态平均值的无偏估计。

提出算法过后还需建立实验来验证算法的性能足够优秀.

1. **文献提出的理论及其核心算法介绍**
   1. **基本理论与方法**

差分隐私：差分隐私是一种隐私保护技术，通过在数据分析过程中人为设置可控的噪声，用于平衡数据的可用性与个体隐私之间的关系。它是一种数学框架，在确保数据集中个人的隐私同时允许对数据进行分析而不泄露任何的个人敏感信息。通常来说，满足（1）的算法可认为满足差分隐私，其中ε为隐私预算.

（1）

拉普拉斯噪声机制：一种常用的差分隐私保护方法，其概率密度函数为（2），其中b是噪声的尺度参数，和ε相关。通过向数据中添加拉普拉斯噪声可以有效保护隐私.

（2）

* 1. **核心算法与公式**

状态更新方程：

（3）

其中θ（k）是智能体在时间k的状态，h是学习率，L是损失函数的梯度，表示边权（各个智能体之间的连系关系），X（k）是时间k智能体传输的消息，S是噪声缩放因子，η（k）表示第k次迭代添加的噪声.

噪声生成算法：

（4）

其中k是迭代次数，c\_i表示第i个样本的敏感度，q\_i表示第i个样本的噪声比例.

收敛点方差公式.

（5）

其中θ表示参数值，无穷表示θ迭代无穷多次后，var表示方差，s\_i表示第i个样本的缩放因子.

收敛点表达公式：

（6）

ave表示均值，n表示样本数量，`η\_i(j)`表示第i个样本的噪声.

参数设置公式：

（7）

α是一个属于[0,1]中的参数，用于调整噪声比例q\_i.

收敛时间公式：

（8）

小于号左边表示第k次迭代的参数值与最终收敛值的距离，tol表示容忍度，即认为算法收敛的阈值.

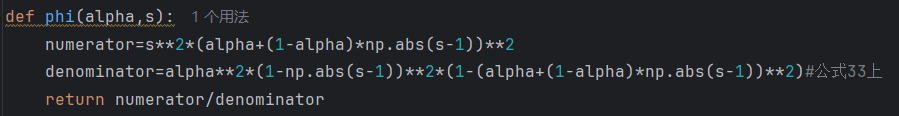
局部目标公式：

（9）

s 是噪声-状态增益参数，α是与噪声衰减率 q 相关的参数，且α=（1−∣s−1∣）/（q−∣s−1∣），q是噪声衰减率，且q∈(∣s−1∣,1).

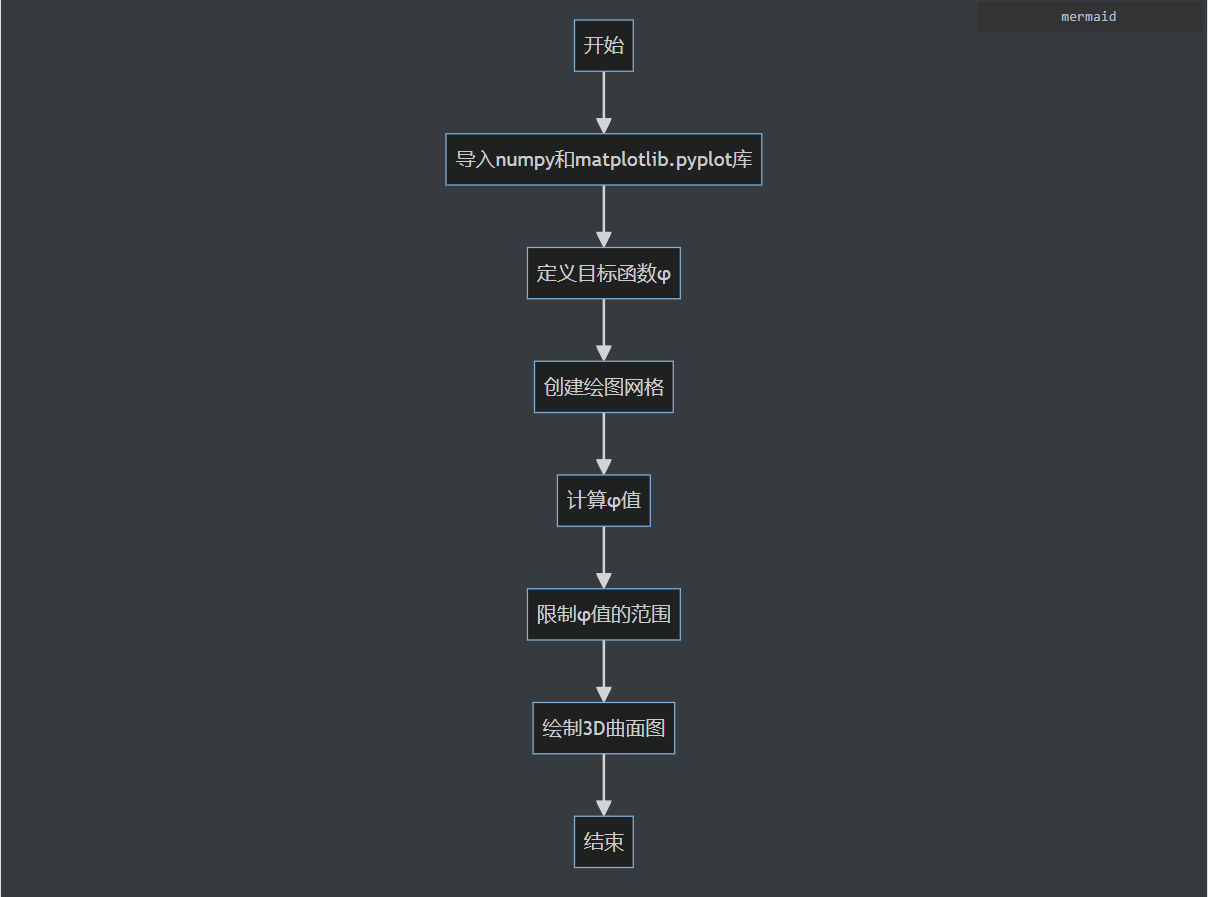
**4、复现实验结果与流程**

**4.1 公式与参数设置**

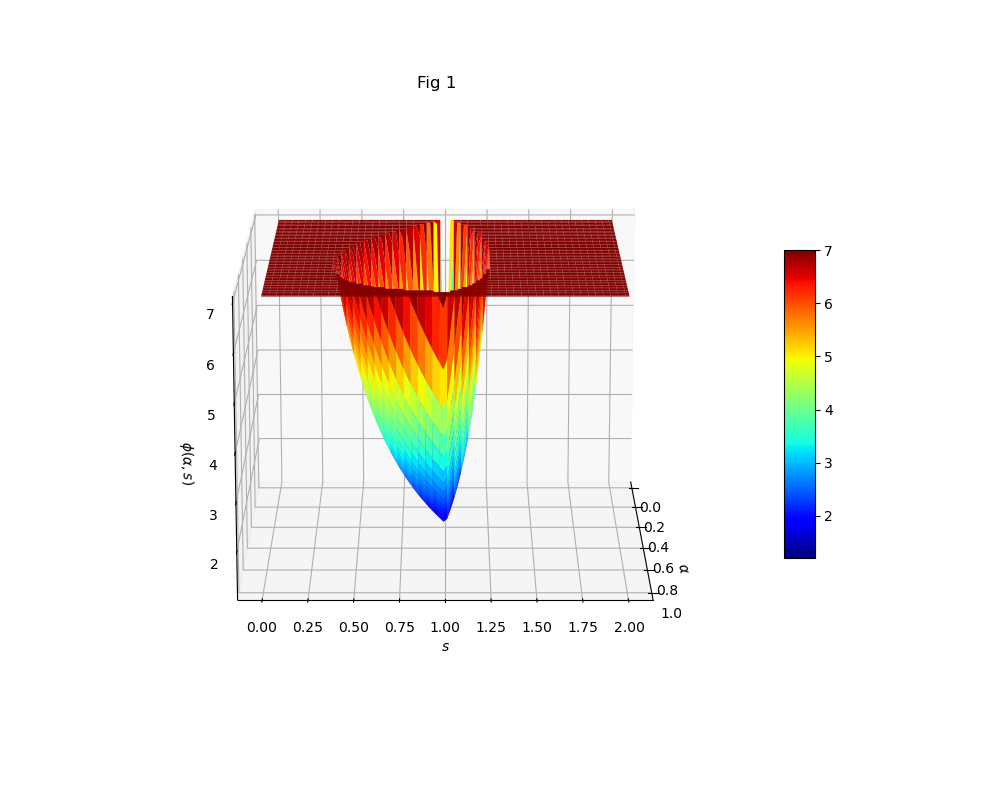
图1的复现运用了公式（9），关键公式如图

参数设置为α是在(0,2)之间均匀取100个点，s在(0,2)均匀取100个点，对应计算后取得的值进行统一绘图

图3的实验流程图如下

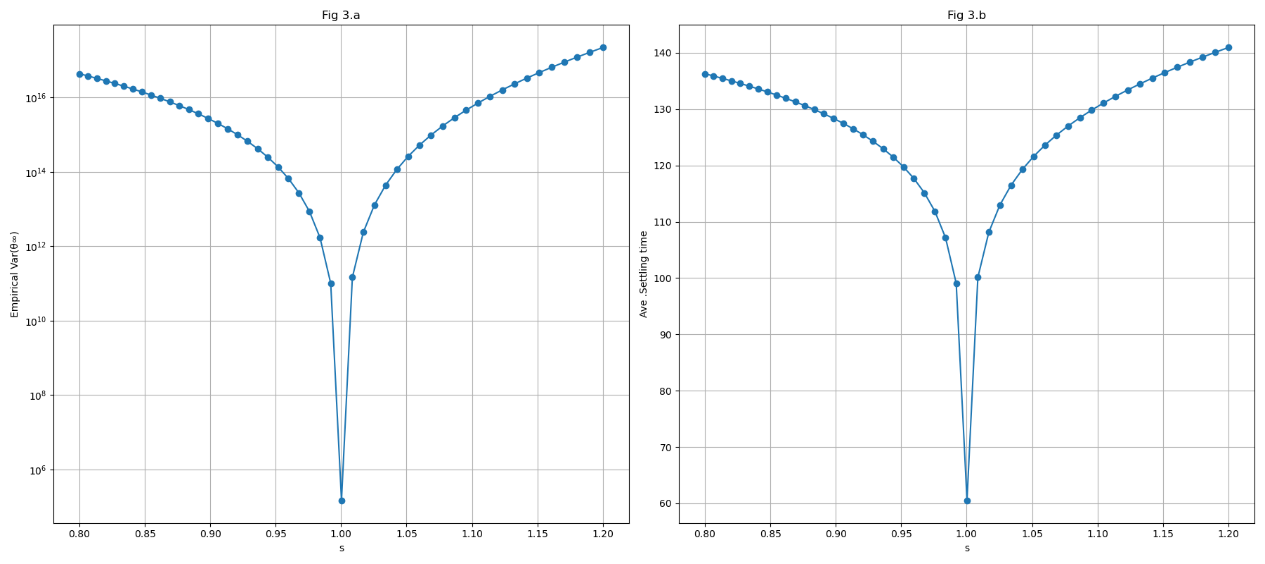
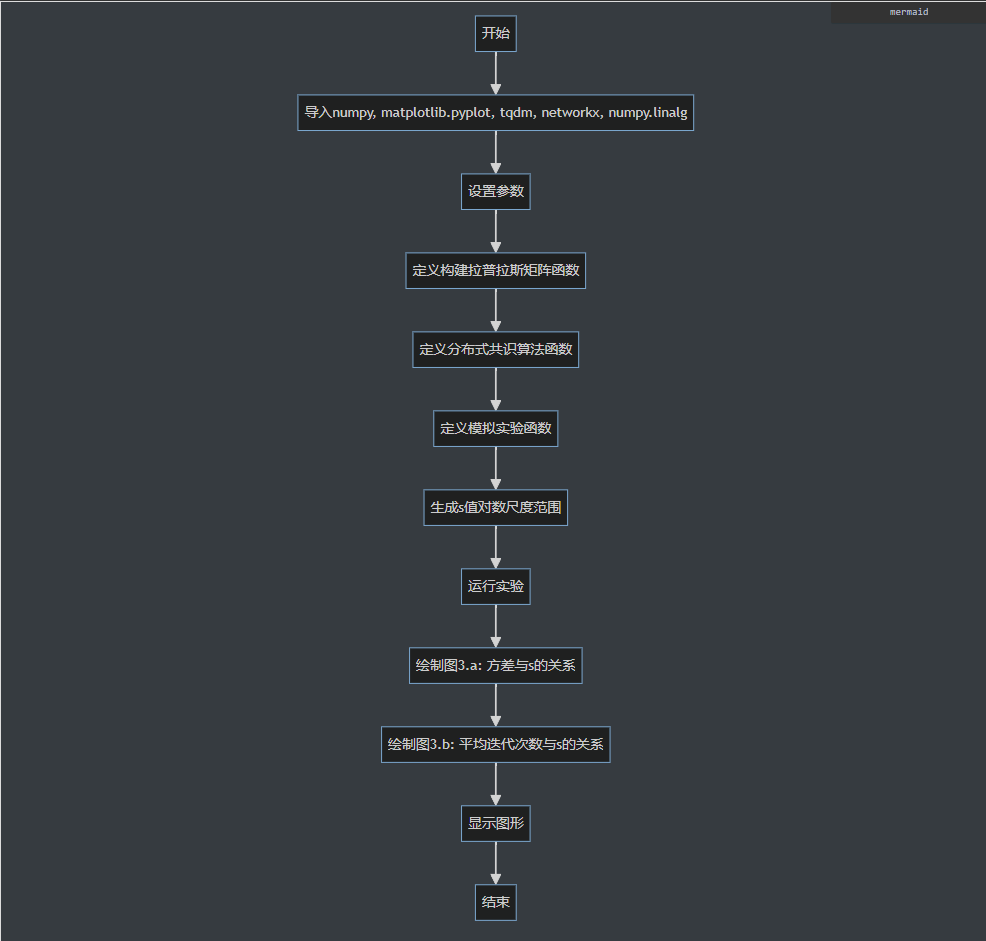


最终实验图如下

图3的复现用了公式（5），关键公式如图



参数设置是δ=1，ε=0.1，tol=1e-2，模拟次数为10000，s为(0.8,1.2)按对数取50个数，流程图如下

最终实现图如下

1. **启示与思考**

对于差分隐私与平均共识算法的首次接触，我对于多智能体与数据的隐私保护有了一个新阶段的认识，无论是对于”噪声“的理解，还是对于”平均共识“的理解，我对这两个论文的绝对关键词进行了一定程度的深挖，同时对其拓展，例如拉普拉斯噪声、收敛速度等常用知识进行了学习。同时第一次进行的文献阅读，给了我新奇的体验，对于英文文献的中英对照查看，对文献的结构的理解，以及对数学推导过程的深思，甚至尝试手推了部分较为简单的公式。同时对于后续实验的阅读与理解，让我又不停的反复理解公式，尝试真正复现实验图，但或许是能力有限，对于图3的复现并没有如此成功，甚至完全没能复现出图4。