控制与决策
Control and Decision

聚合博弈的差分隐私分布式算法：一种Frank-Wolfe方法

杨通清, 莫立坡, 龙飞, 符义昊

引用本文:
杨通清, 莫立坡, 龙飞, 等. 聚合博弈的差分隐私分布式算法：一种Frank-Wolfe方法[J]. 控制与决策, 2025, 40(5): 1677-1686.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2024.0972

聚合博弈的差分隐私分布式算法: 一种 Frank-Wolfe 方法

杨通清[1]，莫立坡[2†]，龙 飞[3]，符义昊[1]

(1. 北京工商大学 数学与统计学院，北京 100048；2. 北京物资学院 系统科学研究院，北京 101149；
3. 贵州理工学院 人工智能与电气工程学院，贵阳 550025)

摘 要: 考虑聚合博弈的隐私保护分布式纳什均衡寻求算法设计. 特别地, 考虑该博弈不存在中心节点, 在这种情况下, 每个玩家无法直接获得用于策略更新所需的聚合策略信息, 采用动态跟踪一致性协议对其进行估计, 其中玩家用于估计聚合策略的状态量被认为是需要保护的敏感信息. 为了保护玩家的隐私, 利用相互独立的高斯噪声对玩家的梯度信息进行干扰. 通过将 Frank-Wolfe 方法与动态跟踪一致性协议相结合, 设计时变通信拓扑下带约束聚合博弈的分布式纳什均衡寻求算法. 进而, 分析算法实现(ϵ,δ)-差分隐私的方差界. 此外, 通过对聚合项估计误差的收敛性分析得到算法收敛的充分条件, 给出算法的收敛性证明. 最后, 通过数值仿真验证了所提出算法的有效性和收敛速度更快的优越性.

关键词: 分布式博弈；差分隐私；聚合博弈；寻找纳什均衡；隐私保护；Frank-Wolfe 方法

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2024.0972

引用格式: 杨通清, 莫立坡, 龙飞, 等. 聚合博弈的差分隐私分布式算法: 一种 Frank-Wolfe 方法 [J]. 控制与决策, 2025, 40(5): 1677-1686.

Differential privacy in aggregative games: A distributed algorithm based on Frank-Wolfe method

YANG Tong-qing[1]，*MO Li-po*[2†]，*LONG Fei*[3]，*FU Yi-hao*[1]

(1. School of Mathematics and Statistics，Beijing Technology and Business University，Beijing 100048，China；
2. Academy of Systems Science，Beijing Wuzi University，Beijing 101149，China；3. School of Artificial Intelligence and Electrical Engineering，Guizhou Institute of Technology，Guiyang 550025，China)

Abstract: This paper considers the design of a privacy-preserving distributed Nash equilibrium seeking algorithm for aggregated games. Specifically, we address scenarios where there is no central node, and in such cases, each player cannot directly obtain the aggregated strategy information required for strategy updates. In this paper, a dynamic tracking consensus protocol is employed to estimate this information. The state variables used by players to estimate the aggregated strategies are regarded as sensitive information that requires protection. To safeguard the players' privacy, independent Gaussian noise is used to perturb the players' gradient information. By combining the Frank-Wolfe method with the dynamic tracking consensus protocol, we design a distributed Nash equilibrium seeking algorithm for constrained aggregated games under time-varying communication topologies. Further, we analyze the variance bounds necessary for the algorithm to achieve (ϵ,δ)-differential privacy. Furthermore, by analyzing the convergence of the estimation error of the aggregated term, we derive sufficient conditions for the convergence of the algorithm and provide a proof of convergence. Finally, the effectiveness and superior convergence speed of the proposed algorithm are validated through numerical simulations.

Keywords: distributed game； differential privacy； aggregated game； Nash equilibrium seeking； privacy protection；Frank-Wolfe method

0 引 言

博弈论是一门研究斗争、竞争以及合作现象的数学理论和方法的学科, 其广泛的应用前景和复杂的技术挑战使得这一理论吸引了大量学者的关注和研究[1]. 聚合博弈中每个玩家的收益取决于其策略和所有玩家的策略总和[2], 聚合博弈在许多领域均有广

收稿日期: 2024-08-15；**录用日期:** 2024-12-12.
基金项目: 国家自然科学基金项目 (62473009).
责任编委: 牛玉刚.
†通信作者. E-mail: beihangmlp@126.com.

泛的应用, 如智能交通[3]、资源分配[4-5] 和智能电网[6] 等. 在聚合博弈中, 所有玩家均以最小化自己的成本函数为目标, 因此, 寻找纳什均衡是聚合博弈的核心问题之一. 在实际应用中, 玩家的策略往往会受到约束, 如厂库的储存总量等, 现有的研究通常利用投影算子来处理约束条件. 起初, 学者们考虑每个玩家均能够直接获取聚合策略, 文献 [7] 首次在图上考虑了玩家无法直接获取聚合策略的情况, 并利用投影算子和分布式跟踪一致性协议提出了分布式算法; 文献 [8] 和文献 [9] 分别在平衡图和耦合约束下提出了连续时间分布式投影算法; 文献 [10] 基于投影算子提出了异步网络中的分布式聚合博弈算法; 文献 [11] 基于投影算子提出了一种具有多轮通信的离散时间分布式算法并实现了线性收敛.

在传统的分布式算法中, 信息交互会带来隐私问题, 如能源管理博弈中的功耗模式, 可能会危及用户隐私和安全性. 因此, 开发隐私保护和通信高效的算法以确保收敛至纳什均衡是至关重要的. 近年来, 学者们提出了一些分布式网络中隐私保护的方法, 对交互的信息进行加密是最常用的方法, 如文献 [12] 在一致性算法中进行同态加密来实现隐私保护. 另一种方法是对交互的信息分解为两个子状态[13]: 一个子状态用来更新自己的状态, 另一个子状态用于传递信息. 然而, 随着迭代次数和玩家数量的增加, 计算量也会大大增加.

差分隐私[14] 是受到广泛关注的隐私保护方法, 其主要思想是在数据中添加噪声来降低对数据集中某条数据的识别能力, 计算量没有同态加密那么大. 差分隐私已在计算机和控制理论等领域被关注, 如分布式学习[15] 等. 在分布式聚合博弈中, 文献 [16] 基于梯度下降法和动态跟踪一致性方法提出了聚合博弈差分隐私分布纳什均衡寻优算法且考虑了带投影算子的情况; 文献 [17] 基于梯度下降法和投影算子提出了随机聚合博弈的差分隐私分布算法; 文献 [18] 提出了能够精确收敛的带投影算子的聚合博弈的差分隐私分布式算法, 解决了差分隐私方法会牺牲收敛精度的问题.

上述算法均用投影算子处理约束, 这意味着玩家需要在每次迭代过程中求解一个二次优化问题来找到约束集中最近的点, 当约束复杂 (如多面体) 时, 求解二次优化问题的计算成本是巨大的, 特别是对于高维优化问题, 同时, 也违背了不使用同态加密而减少计算量的想法. 基于此, 本文想到了著名的 Frank-Wolfe (FW)[19] 方法, 它提供了在保持策略可行性的同时得到有效搜索方向的方法. FW 算法的每步只需要求解一个有约束的线性规划问题, 这个问题对于特定的问题可有一个封闭的形式, 也有有效的解. FW 方法因其无投影特性在在线学习[20] 等大规模问题上的优势而受到关注. 近些年, FW 方法得到了大量的推广, 如文献 [21] 和文献 [22] 分别用 FW 研究了离散时间分布式优化问题和聚合优化问题, 文献 [23] 研究了分布式随机约束优化的 FW 算法等. 为了解决分布式聚合博弈中带投影的算法计算成本太大以及敏感信息可能会泄露的问题, 本文考虑设计一种基于 FW 方法的无投影算法来解决这两个问题.

本文主要设计使用无投影的方法来解决聚合博弈的差分隐私保护, 为聚合博弈网络设计分布式算法求解纳什均衡的同时实现差分隐私. 基于文献 [16] 和文献 [22], 本文提出一种无投影的聚合博弈分布式差分隐私算法. 本文主要内容如下.

1) 设计一种基于策略跟踪和 FW 方法的分布式无投影算法来解决聚合博弈问题, 该算法采用动态平均跟踪方法来估计聚合策略, 再用其估计梯度. 后续的理论分析表明, 估计的聚合策略和梯度项均渐近收敛至真实聚合策略和梯度.

2) 找到使得算法实现差分隐私噪声的方差界, 表明该方差界能够使得所提出算法实现(ϵ,δ)-差分隐私, 由于差分隐私间接访问的鲁棒性, 估计聚合项时状态变量相互传递能够实现差分隐私.

3) 与文献 [16-17] 中使用的方法相比, 所提出算法的收敛速度更快, 能够在更短的时间内达到理想的解, 从而提高计算的效率, 降低计算成本.

符号说明: $\mathbb{R}^m$为m维实向量集合, $\langle x,y\rangle$为向量x与y的内积, $\|x\|$为标准欧几里得范数, $\mathrm{E}[x]$为随机变量x的期望, $[A]_j^i$为矩阵第i行第j列的元素.

1 预备知识和问题描述

1.1 预备知识

首先介绍博弈论的相关基础.

定义 1 一个标准形式的博弈定义为一个三元组$\Gamma=\{\mathcal{V},X,f\}$. 其中: $\mathcal{V}=\{1,2,\ldots,N\}$为玩家集, $X=X_1\times X_2\times\ldots\times X_N(X_i\subseteq\mathbb{R}^m)$为玩家$i$的策略集, $f=(f_1,f_2,\ldots,f_N)$中的f_i是玩家i的成本函数.

定义 2 纳什均衡是一组策略, 假设其他玩家的策略是固定的, 没有玩家可以通过单方面改变自己的策略来减小成本函数, 即策略$x^*=(x_i^*,x_{-i}^*)\in X$为纳什均衡策略, 则$f_i(x_i^*,x_{-i}^*)\leqslant f_i(x_i,x_{-i}^*)(\forall i\in\mathcal{V})$, 其中 $x_i\in X_i$和 $x_{-i}=(x_1^{\mathrm{T}},x_2^{\mathrm{T}},\ldots,x_{i-1}^{\mathrm{T}},x_{i+1}^{\mathrm{T}},\ldots,x_N^{\mathrm{T}})^{\mathrm{T}}$.

定义 3 若存在一个集合函数$\Phi(x):X\to\mathbb{R}$,

它是连续的、可加和、可分离的, 使得函数$f_i(x_i,\Phi(x))$: $X_i\times X\to\mathbb{R}(\forall i\in\mathcal{V})$满足

$$f_i(x_i,\Phi(x))=f_i(x_i,x_{-i}),\ \forall x\in X,$$

则称博弈Γ为一个聚合博弈. 在本文中, 主要考虑$\Phi(x)=\sum_1^N x_i$为聚合项.

1.2　问题描述

在能源消耗、古诺价格竞争和公共物品供给等实际问题中, 与玩家相关的效用不仅依赖于玩家自己的策略, 还依赖于所有玩家策略的加和, 从而产生聚合博弈问题. 本文考虑N个玩家的聚合博弈问题, 所有玩家的策略集受到一定的约束且无法直接获得聚合策略. 本文旨在寻求分布式聚合博弈的纳什均衡并实现玩家的隐私保护, 即玩家i试图求解

$$\min_{x_i\in X_i}\mathrm{E}[f_i(x_i,\Phi(x))]. \tag{1}$$

其中: $X_i(i\in\mathcal{V})$为非空有界闭凸集; $\Phi(x)=\sum_1^N x_i$, 这里$x=(x_1^{\mathrm{T}},x_2^{\mathrm{T}},\dots,x_N^{\mathrm{T}})^{\mathrm{T}}$. 玩家之间通过切换的无向连通图$G(k)=(\mathcal{V},\mathcal{E}(k),A(k))$交互信息, 该图由非空玩家集$\mathcal{V}=\{1,2,\dots,N\}$、$k$时刻的边集$\mathcal{E}(k)\subseteq\mathcal{V}\times\mathcal{V}$和邻接矩阵$A(k)=[a_{ij}(k)]_{N\times N}$构成. 若玩家$i$与$j$间存在边$(j,i)\in\mathcal{E}(k)$, 则表示玩家$i$与玩家$j$可以交互信息, 此时玩家$i$与玩家$j$间的通信权重$a_{ij}(k)>0$; 否则, $a_{ij}(k)=0$. $\mathcal{N}_i(k)=\{j\in\mathcal{V},(j,i)\in\mathcal{E}(k)\}$表示玩家$i$在$k$时刻的邻居玩家集, 本文假设玩家$i$是自己的邻居. 为了方便表示, 本文将成本函数定义为$g_i(x)\triangleq f_i(x_i,\Phi(x))$, 函数$g_i(x)$的梯度定义[22]为

$$\nabla g_i(x)\triangleq$$
$$\mathbf{1}_i(\nabla_{x_i}f_i(x_i,\Phi(x))+\nabla_{\Phi}f_i(x_i,\Phi(x))\nabla_{x_i}\Phi(x)),$$

其中$\mathbf{1}_i$表示第i个元素为 1, 其余均为 0 的列向量, 即$\mathbf{1}_i=(0,\dots,0,1,0,\dots,0)^{\mathrm{T}}$. 下面给出几个必要的假设.

假设 1　1) 每个玩家$i\in\mathcal{V}$的策略集X_i均为非空有界闭凸集, 假设最大直径为d, 即存在正数$d>0$, 使得对于任意$i\in\mathcal{V}$, x_i、$y_i\in X_i$, 有$\max_{i\in\mathcal{V}}\|y_i-x_i\|\leqslant d$, 其中$\|\cdot\|$为标准 2 范数.

2) 每个玩家$i\in\mathcal{V}$的成本函数$g_i(x)$在$x\in X$上为连续可微的μ-强凸函数, 其梯度在$x\in X$上为L-光滑, 即

$$g_i(y)-g_i(x)\geqslant(y-x)^{\mathrm{T}}\nabla g_i(x)+\frac{\mu}{2}\|y-x\|^2,$$
$$\|\nabla g_i(x)-\nabla g_i(y)\|\leqslant L\|x-y\|,\ \forall x,y\in X.$$

L-光滑的表达式等价于下式:

$$g_i(x)-g_i(y)\leqslant(x-y)^{\mathrm{T}}\nabla g_i(y)+\frac{L}{2}\|x-y\|^2,$$

其中$\mu>0$、$L>0$分别为强凸参数和光滑参数.

假设 2　1) $\nabla_{x_i}f_i(x_i,z)(\forall i\in\mathcal{V})$对于任意$x_i\in X_i$关于$z\in\mathbb{R}^m$为$l_1$-Lipschitz 连续的, 即存在一个正常数$l_1$和$z_1$、$z_2\in\mathbb{R}^m$, 有

$$\|\nabla_{x_i}f_i(x_i,z_1)-\nabla_{x_i}f_i(x_i,z_2)\|\leqslant l_1\|z_1-z_2\|.$$

2) $\nabla_z f_i(x_i,z)(\forall i\in\mathcal{V})$关于$(x_i,z)\in X_i\times\mathbb{R}^m$是$l_2$-Lipschitz 连续的, 即存在一个正常数$l_2$和任意的$x_1$、$x_2\in X_i$, z_1、$z_2\in\mathbb{R}^m$, 有

$$\|\nabla_{\Phi}f_i(x_1,z_1)-\nabla_{\Phi}f_i(x_2,z_2)\|\leqslant$$
$$l_2\|x_1-x_2\|+l_2\|z_1-z_2\|.$$

假设 3　1) 邻接矩阵$A(k)=[a_{ij}(k)]_{N\times N}$为双随机矩阵, 即$\sum_{i=1}^N a_{ij}(k)=\sum_{j=1}^N a_{ij}(k)=1$;

2) 存在一个常数$0<\eta<1$, 使得$a_{ii}(k)\geqslant\eta$, $a_{ij}(k)\geqslant\eta\,(\forall j\in\mathcal{N}_i(k),i\in\mathcal{V})$;

3) 存在一个整数$B\geqslant 1$, 玩家j在$k\geqslant 0$的时间中, 每连续B个时隙向相邻玩家i至少发送一次信息.

本文对于任意的$k\geqslant s\geqslant 0$, 定义矩阵

$$\Phi(k,s)=A(k)A(k-1)\dots A(s),$$

其中$\Phi(k,k)=A(k)$.

引理 1[22]　若假设 3 成立, 则存在一个常数$\theta>0,\beta\in(0,1)$, 使得

$$\left\|[\psi(k,s)]_j^i-\frac{1}{N}\right\|\leqslant\theta\beta^{k-s},\ \forall k\geqslant s\geqslant 0,\ \forall i,j\in\mathcal{V}.$$

2　主要内容

2.1　聚合博弈的差分隐私分布式 Frank-Wolfe 算法

为了求解问题 (1), 现在已经提出了一些基于投影算子的分布式算法, 如文献 [7-11, 16-18]. 然而, 在实际计算过程中, 投影的计算是一个繁琐的问题且计算量很大, 本文在文献 [16] 的投影梯度法的基础上采用 FW 方法对算法进行改进, 提出了一种基于 FW 方法和梯度下降法的差分隐私分布式算法. 简单而言, FW 方法使用线性化函数来近似目标函数, 并通过求解线性目标优化来推导可行的下降方向$y_i(k)\in\arg\min_{y\in X_i}\langle\nabla g_i(x(k)),y\rangle$, $x_i(k+1)=x_i(k)+a_k(y_i(k)-x_i(k))$, 显然, x_i的更新为凸约束集X_i内的x_i与y的凸组合, 使得更新的x_i属于约束集X_i. 此外, 聚合博弈中每个玩家有策略x_i和状态v_i两个变量, 因为博弈过程中玩家不能直接获取聚合信息, 状态v_i的引入则是为了估计问题 (1) 中成本函数的聚合项. 在初始化时, 令$x_i(0)=v_i(0)\in X_i$. 在每次迭代开始时, 玩家i从它的邻居$j\in\mathcal{N}_i(k)$接收到状

态信息$v_j(k)$, 利用这些信息估计$\hat{v}_i(k)=\sum\limits_{j=\mathcal{N}_i(k)} v_j(k)$, 得到$\hat{v}_i(k)$后用来更新自己的状态和估计成本函数的梯度. 为了在这个信息交互过程中玩家的隐私信息不被泄露, 本文在每次计算下降方向的梯度添加一个相互独立的高斯噪声, 即$\nabla_{x_i(k)}f(x_i(k),N\hat{v}_i(k))+N\nabla_{x_i(k)}\hat{v}_i(k)\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k))+w_i(k)$, 其中$w_i(k)\sim N(0,\sigma_i(k)^2)$, 该过程被称为高斯机制, 也是后文定义 5 中的随机算法$\mathcal{M}$. 具体算法如下所示:

$$\hat{v}_i(k)=\sum_{j=1}^{N}a_{ij}(k)v_j(k), \tag{2}$$

$$y_i(k)\in\arg\min_{y_i\in X_i}\langle\nabla_{x_i(k)}f(x_i(k),N\hat{v}_i(k))+\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k))+w_i(k),y_i\rangle, \tag{3}$$

$$x_i(k+1)=x_i(k)+\alpha_k(y_i(k)-x_i(k)), \tag{4}$$

$$v_i(k+1)=\hat{v}_i(k)+x_i(k+1)-x_i(k), \tag{5}$$

这里: $x_i(k)\geqslant 0$为玩家i的策略, $v_i(k)$为玩家的状态, $y_i\geqslant 0$为辅助变量, α_k为时变的步长, $w_i(k)\sim N(0,\sigma_i^2(k))$为$k$时刻玩家$i$添加的高斯噪声.

注 1 为方便起见, 本文在分析和后续表述中假设$x_i(k)$和$v_i(k)\in\mathbb{R}$. 利用克罗内克 (Kronecker) 积可将结论推广至$\mathbb{R}^m$中.

定义

$$\begin{aligned}&y(k)=(y_1(k),y_2(k),\dots,y_N(k))^{\mathrm{T}},\\&x(k)=(x_1(k),x_2(k),\dots,x_N(k))^{\mathrm{T}},\\&v(k)=(v_1(k),v_2(k),\dots,v_N(k))^{\mathrm{T}},\\&\hat{v}(k)=(\hat{v}_1(k),\hat{v}_2(k),\dots,\hat{v}_N(k))^{\mathrm{T}},\end{aligned}$$

则式 (4) 和 (5) 的向量形式可写为

$$x(k+1)=x(k)+\alpha_k(y(k)-x(k)), \tag{6}$$

$$v(k+1)=\hat{v}(k)+x_i(k+1)-x(k). \tag{7}$$

注 2 算法中使用动态跟踪方法使得$N\hat{v}_i(k)$跟踪聚合项$\Phi(x(k))=\sum\limits_{1}^{N}x_i(k)$, 使用$\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k))$估计梯度$\nabla_{\Phi}f_i(x_i(k),\Phi(x(k)))$, 收敛性证明表明估计误差均渐近趋于 0. 此外, 第 2 项的梯度为$\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k))\nabla_{x_i(k)}\Phi(x(k))$, 由$\Phi(x(k))=\sum\limits_{1}^{N}x_i(k)$的具体形式可知, $\nabla_{x_i(k)}\Phi(x(k))=1\ (\forall i\in\mathcal{V})$. 将上述算法写为伪代码形式, 如算法 1 所示.

算法 1 聚合博弈的差分隐私分布式 Frank-Wolfe 算法.

初始化: $k=0$, 对于$\forall i\in\mathcal{V}$, $v_i(0)=x_i(0)\in X_i$, 设置初始步长$\alpha_0>0$和足够小的常数$\rho>0$.

一致性: 玩家i发送其状态信息$v_i(k)$给它的邻居, 其中$v_i(k)$为玩家i在k时刻的状态估计. 玩家i从它的邻居$j\in\mathcal{N}_i(k)$接收到估计$v_j(k)$, 并将以下步骤执行一次.

策略更新: 对于任意$i\in\mathcal{V}$, 有

$$\begin{aligned}&\hat{v}_i(k)=\sum_{j=1}^{N}a_{ij}(k)v_j(k),\\&y_i(k)\in\arg\min_{y_i\in X_i}\langle\nabla_{x_i(k)}f(x_i(k),N\hat{v}_i(k))+\\&\qquad\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k))+w_i(k),y_i\rangle,\\&x_i(k+1)=x_i(k)+\alpha_k(y_i(k)-x_i(k)),\\&v_i(k+1)=\hat{v}_i(k)+x_i(k+1)-x_i(k),\\&k=k+1.\end{aligned}$$

终止条件: $|x_i(k+1)-x_i(k)|\leqslant\rho$.

2.2 算法 1 的隐私分析

首先给出邻居数据集和差分隐私的定义.

定 义 4 两组不同的玩家状态信息样本记为$D_k=\{v_i(k),i=1,2,\dots,N\}$和$D_k'=\{v_i'(k),i=1,2,\dots,N\}$, 若只有一个采样点不同, 则称$D_k$与$D_k'$为相邻数据集.

定 义 5 对于随机算法$\mathcal{M}$, 给定ϵ、$\delta\geqslant 0$, 若对于任意相邻数据集D_k和D_k', 以及对于输出的任意子集$\Upsilon\subseteq\mathrm{Range}(\mathcal{M})$, 使得

$$P(\mathcal{M}(D_k)\in\Upsilon)\leqslant\mathrm{e}^{\epsilon}P(\mathcal{M}(D_k')\in\Upsilon)+\delta,$$

则称随机算法$\mathcal{M}$是(ϵ,δ)差分隐私的, 其中$P(\mathcal{M}(D_k)\in\Upsilon)$表示数据集$D_k$添加噪声的输出属于$\Upsilon$的概率.

本文旨在为聚合博弈网络设计分布式算法求解纳什均衡的同时实现差分隐私. 首先, 对查询函数和隐私泄露的可能性进行简单的介绍, 用$o(\cdot)$表示查询函数, 若对手的目的为查询该数据集D_k的平均值, 则有$o(D_k)=\dfrac{1}{N}\sum\limits_{j=1}^{N}v_j(k)$. 在不添加噪声的情况下, 若知道$o(D_k)$和$v_j(k)\ (j\geqslant 2)$, 则很容易推断出$v_1(k)$的值. 添加噪声的干扰会降低对这组数据进行查询时的识别度, 以达到保护隐私信息的目的, 这种保证差分隐私的方法在文献 [14] 中有详细的介绍. 然后, 推导算法 1 满足(ϵ,δ)-差分隐私的噪声方差条件. 在给出定理 1 之前, 先给出灵敏度的定义.

定 义 6 第k次迭代时查询函数$o(\cdot)$的灵敏度定义为

$$\Delta_k=\sup_{D_k,D_k':\mathrm{Adj}(D_k,D_k')}\|o(D_k)-o(D_k')\|.$$

引 理 2 算法 1 在第$k\geqslant 1$次迭代时的灵敏度满足

$$\Delta_k\leqslant\alpha_{k-1}d. \tag{8}$$

证明　首先, 令

$$p_i(k)=\nabla_{x_i(k)}f(x_i(k),N\hat{v}_i(k))+\nabla_{\hat{v}_i(k)}f(x_i(k),N\hat{v}_i(k)),$$
$$\hat{v}'_i(k)=\sum_{j=1}^{N}a_{ij}(k)v'_j(k),$$
$$p'_i(k)=\nabla_{x_i(k)}f(x_i(k),N\hat{v}'_i(k))+\nabla_{\hat{v}'_i(k)}f(x_i(k),N\hat{v}'_i(k)).$$

根据定义 4, D_k与D'_k为相邻数据集, 数据集的数据$v_i(k)$和$D'_i(k)$在算法 1 中仅用到$y_i(k)$估计, 考虑$y_i(k)\in\langle p_i(k)+w_i(k),y\rangle$由数据集$D_k$计算, $y'_i(k)\in\langle p'_i(k)+w_i(k),y\rangle$由数据集$D'_i(k)$计算, 可得到

$$\begin{aligned}&\|x_i(k)-x'_i(k)\|=\\&\|x_i(k-1)+\alpha_{k-1}(y_i(k-1)-x_i(k-1))-\\&x_i(k-1)-\alpha_{k-1}(y'_i(k-1)-x_i(k-1))\|\leqslant\\&\alpha_{k-1}\|y_i(k-1)-y'_i(k-1)\|\leqslant\\&\alpha_{k-1}d.\end{aligned}$$

□

定理 1　设$\epsilon\in(0,1),\delta>0$, $\sigma_i^2(k)$为$w_i(k)$的方差且满足

$$\sigma_i(k)=\frac{d\sqrt{2\ln\left(\frac{1.25}{\delta}\right)}\alpha_{k-1}}{\epsilon},\tag{9}$$

则算法 1 的每次迭代均是(ϵ,δ)差分隐私的. 换言之, 对于任意的相邻数据集D_k、D'_k和任意的输出集Υ, 有

$$P(\mathcal{M}(D_k)\in\Upsilon)\leqslant\mathrm{e}^{\epsilon}P(\mathcal{M}(D'_k)\in\Upsilon)+\delta.$$

证明　设D_k与D'_k是两个邻接数据集, $y_i(k)$为任意输出, 则在输出$y_i(k)$时的隐私损失如下所示:

$$\begin{aligned}&\left|\ln\frac{P(\mathcal{M}(D_k)=y_i(k))}{P(\mathcal{M}(D'_k)=y_i(k))}\right|=\\&\left|\ln\frac{P(o(D_k)+w_i(k)=y_i(k))}{P(o(D'_k)+w_i(k)=y_i(k))}\right|=\\&\left|\ln\frac{P(w_i(k)=y_i(k)-o(D_k))}{P(w_i(k)=y_i(k)-o(D_k)+\Delta_k)}\right|=\\&\left|\ln\frac{\exp\left(-\frac{1}{2\sigma_i^2(k)}(y_i(k)-o(D_k))^2\right)}{\exp\left(-\frac{1}{2\sigma_i^2(k)}(y_i(k)-o(D_k)+\Delta_k)^2\right)}\right|=\\&\left|-\frac{1}{2\sigma_i^2(k)}(w_i^2(k)-(w_i(k)+\Delta_k)^2)\right|=\\&\left|\frac{1}{2\sigma_i^2(k)}(2w_i(k)\Delta_k+\Delta_k^2)\right|\leqslant\\&\left|\frac{1}{2\sigma_i^2(k)}(2w_i(k)\alpha_{k-1}d+(\alpha_{k-1}d)^2)\right|,\end{aligned}\tag{10}$$

其中不等号由引理 2 得到. 将式 (9) 代入 (10), 可得到

$$\left|\ln\frac{P(\mathcal{M}(D_k)=y_i(k))}{P(\mathcal{M}(D'_k)=y_i(k))}\right|\leqslant\frac{\epsilon^2}{4d^2\ln(1.25/\delta)\alpha_{k-1}^2}\times|2w_i(k)\alpha_{k-1}d+(\alpha_{k-1}d)^2|.$$

当$|w_i(k)|\leqslant d\alpha_{k-1}\left(2\epsilon^{-1}\ln\left(\frac{1.25}{\delta}\right)-\frac{1}{2}\right)$时, 有

$$\left|\ln\frac{P(\mathcal{M}(D_k)=y_i(k))}{P(\mathcal{M}(D'_k)=y_i(k))}\right|\leqslant\epsilon.$$

接下来证明

$$P(|w_i(k)|>r)\leqslant\delta,\tag{11}$$

其中$r=d\alpha_{k-1}\left(2\epsilon^{-1}\ln\left(\frac{1.25}{\delta}\right)-\frac{1}{2}\right)$. 因此, 证明$P(w_i(k)>r)\leqslant\frac{\delta}{2}$即可. 利用正态分布的尾界, 有$P(w_i(k)>r)\leqslant\frac{\sigma_i(k)}{\sqrt{2\pi}r}\exp\left(-\frac{r^2}{\sigma_i^2(k)}\right)$, 当$\delta$取很小时$(\leqslant0.01)$和$0<\epsilon<1$时, 可得到

$$\frac{\sigma_i(k)}{r}<1,\quad-\frac{r^2}{\sigma_i^2(k)}\leqslant\ln\left(\sqrt{2\pi}\frac{\delta}{2}\right).$$

由式 (10) 和 (11), 可得到

$$P(\mathcal{M}(D_k)=y_i(k))\leqslant\mathrm{e}^{\epsilon}P(\mathcal{M}(D'_k)=y_i(k))+\delta,$$

又因$y_i(k)\in\Upsilon$, 定理 1 得证. □

注 3　定理 1 表明了在寻找梯度方向时添加噪声可保证差分隐私的方差界, 由文献 [17] 的定理 4 可知, 间接访问差分隐私输出的数据集, 不会削弱差分隐私的隐私保护能力, 因此, 所提出算法 1 在信息交互时可实现差分隐私. 此外, 常数ϵ衡量随机算法$\mathcal{M}$的隐私水平, ϵ越小, 隐私保护水平越高.

2.3　算法 1 的收敛分析

本节验证算法的收敛性, 首先给出必要的假设以及 Frank-Wolfe 方法的终止条件和下降方向.

假设 4　步长α_k满足$\sum_{k=0}^{\infty}\alpha_k=\infty,\sum_{k=0}^{\infty}\alpha_k^2<\infty$, 对于任意$k\geqslant0$, 有$0\leqslant\alpha_{k+1}\leqslant\alpha_k\leqslant1$.

假设 5　问题 (1) 至少存在一个稳定的纳什均衡解$x^*\in X$.

注 4　假设 4 是变步长常见的随机逼近型假设, 也是所提出算法收敛的技术要求, 如$\alpha_k=(k+1)^{-\Gamma}$, 其中$\frac{1}{2}<\Gamma\leqslant1$, 文献 [17] 和文献 [22] 等有所介绍. 假设 5 为问题 (1) 有解的必要条件, 文献 [16] 表明成本函数为强凸函数时, 强凸函数的定义可等价为

$$(y-x)^{\mathrm{T}}(\nabla g_i(y)-\nabla g_i(x))\geqslant\mu\|y-x\|^2,\quad\forall x,y\in X.$$

这是文献 [7] 和文献 [16-17] 等常用的形式. 在强凸条件下, 纳什均衡$x^*=[x_1^*,x_2^*,\ldots,x_N^*]^{\mathrm{T}}$使得$\nabla g_i(x^*)$

$=0\,(\forall i\in\mathcal{V})$.

引理 3[19] 对于式 (3) 求出的$y_i(k)$, 有:

1) $\nabla g_i(x(k))^{\mathrm{T}}(y(k)-x(k))=0$, 则$x(k)$为问题 (1) 的最优点.

2) $\nabla g_i(x(k))^{\mathrm{T}}(y(k)-x(k))\neq 0$, 则

$$\nabla g_i(x(k))^{\mathrm{T}}(y(k)-x(k))<0,$$

此时, $y(k)-x(k)$为$x(k)$处的下降方向.

下文引理 4 表明对聚合项估计的收敛性.

引理 4 若假设 3 成立, $\hat{v}_i(k)$由算法 1 迭代生成, 则

$$\mathrm{E}\Big[\Big\|N\hat{v}_i(k)-\sum_{i=1}^{N}x_i(k)\Big\|\Big]=$$

$$N\mathrm{E}\Big[\Big\|\hat{v}_i(k)-\frac{1}{N}\sum_{i=1}^{N}x_i(k)\Big\|\Big]\leqslant$$

$$N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}.$$

证明 首先, 通过对式 (5) 进行迭代, 可得到

$$\begin{aligned}&v_i(k+1)=\\&\sum_{j=1}^{N}[A(k)]_j^i\Big(\sum_{j=1}^{N}[A(k-1)]_j^iv_j(k-1)+\\&x_i(k)-x_i(k-1)\Big)+x_i(k+1)-x_i(k)=\ldots=\\&\sum_{j=1}^{N}[\psi(k,0)]_j^iv_j(0)+\\&\sum_{s=1}^{k}\sum_{j=1}^{N}[\psi(k,s)]_j^i(x_j(s)-x_j(s-1))+\\&x_i(k+1)-x_i(k).\end{aligned}\tag{12}$$

对式 (12) 进行移项, 可得到

$$\begin{aligned}&v_i(k+1)-x_i(k+1)+x_i(k)=\\&\sum_{j=1}^{N}[\psi(k,0)]_j^iv_j(0)+\\&\sum_{s=1}^{k}\sum_{j=1}^{N}[\psi(k,s)]_j^i(x_j(s)-x_j(s-1)).\end{aligned}\tag{13}$$

由式 (5) 可知, (13) 左边为$\hat{v}_i(k)$, 因此

$$\begin{aligned}&\hat{v}_i(k)=\\&\sum_{j=1}^{N}[\psi(k,0)]_j^iv_j(0)+\sum_{s=1}^{k}\sum_{j=1}^{N}[\psi(k,s)]_j^i(x_j(s)-\\&x_j(s-1)).\end{aligned}\tag{14}$$

记$q(k)=\dfrac{1}{N}\sum_{i=1}^{N}x_i(k)$, 则有

$$\begin{aligned}&q(k)=q(k-1)+(q(k)-q(k-1))=\\&q(k-2)+(q(k-1)-q(k-2))+\\&(q(k)-q(k-1))=\ldots=\\&q(0)+\sum_{s=1}^{k}(q(s)-q(s-1)).\end{aligned}$$

由$q(k)$的定义和$v_i(0)=x_i(0)$, 可得到

$$\begin{aligned}&\frac{1}{N}\sum_{i=1}^{N}x_i(k)=\\&\frac{1}{N}\sum_{i=1}^{N}v_i(0)+\frac{1}{N}\sum_{s=1}^{k}\sum_{i=1}^{N}(x_i(s)-x_i(s-1)).\end{aligned}\tag{15}$$

因此, 由式 (14) 和 (15), 可得到

$$\begin{aligned}&\Big\|\hat{v}_i(k)-\frac{1}{N}\sum_{i=1}^{N}x_i(k)\Big\|=\\&\Big\|\sum_{j=1}^{N}\Big([\psi(k,0)]_j^i-\frac{1}{N}\Big)v_j(0)+\\&\sum_{s=1}^{k}\sum_{j=1}^{N}\Big([\psi(k,s)]_j^i-\frac{1}{N}\Big)(x_j(s)-x_j(s-1))\Big\|\leqslant\\&\sum_{j=1}^{N}\Big\|[\psi(k,0)]_j^i-\frac{1}{N}\Big\|\|v_j(0)\|+\\&\sum_{s=1}^{k}\sum_{j=1}^{N}\Big\|[\psi(k,s)]_j^i-\frac{1}{N}\Big\|\|x_j(s)-x_j(s-1)\|.\end{aligned}\tag{16}$$

由引理 1 和式 (4), 式 (16) 可写为

$$\begin{aligned}&\Big\|\hat{v}_i(k)-\frac{1}{N}\sum_{i=1}^{N}x_i(k)\Big\|\leqslant\\&\theta\beta^k\sum_{j=1}^{N}\|v_j(0)\|+\\&\sum_{s=1}^{k}\theta\beta^{k-s}\alpha_{s-1}\sum_{j=1}^{N}\|y_j(s-1)-x_j(s-1)\|.\end{aligned}\tag{17}$$

又由于$v_i(0)=x_i(0)\in X_i$, 对式 (17) 求期望, 再由假设 1 中的 1), 可得到

$$\begin{aligned}&\mathrm{E}\Big[\Big\|\hat{v}_i(k)-\frac{1}{N}\sum_{i=1}^{N}x_i(k)\Big\|\Big]\leqslant\\&Nd\theta\beta^k+Nd\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}.\end{aligned}\tag{18}$$

将式 (18) 两边乘以N, 引理 4 得证. □

引理 5 若假设 1 ∼ 假设 3、假设 5 成立, x^*为纳什均衡策略, 且每个玩家$i\in\mathcal{V}$的策略和状态由算法 1 给出, 则

$$\mathrm{E}[f_i(x_i(k+1),\Phi(x(k+1)))-f_i(x_i^*,\Phi(x^*))]\leqslant$$
$$(1-\alpha_k)\mathrm{E}[f_i(x_i(k),\Phi(x(k)))-f_i(x_i^*,\Phi(x^*))]+$$
$$\frac{NL}{2}\alpha_k^2d^2+\alpha_k(dl_1+dl_2)\Big(N^2d\theta\beta^k+$$
$$N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big).$$

证明　由式 (6) 可知, $x(k+1)-x(k)=a_k(y(k)-x(k))$. 由$g_i$的$L$-光滑性和$X_i$的有界性可知

$$g_i(x(k+1))-g_i(x(k))\leqslant$$
$$\alpha_k(y(k)-x(k))^{\mathrm{T}}\nabla g_i(x(k))+\frac{NL}{2}\alpha_k^2d^2. \tag{19}$$

又由于

$$\nabla g_i(x)\triangleq$$
$$\mathbf{1}_i(\nabla_{x_i}f_i(x_i,\Phi(x))+\nabla_{\Phi}f_i(x_i,\Phi(x))\nabla_{x_i}\Phi(x)), \tag{20}$$

对于任意的$y=[y_1,y_2,\ldots,y_N]^{\mathrm{T}}\in X$, 有

$$\langle\nabla g_i(x(k)),y\rangle=$$
$$\langle\nabla_{x_i(k)}f_i(x_i(k),\Phi(x(k)))+$$
$$\nabla_{\Phi}f_i(x_i(k),\Phi(x(k)))\nabla_{x_i(k)}\Phi(x(k))+$$
$$\nabla_{x_i(k)}f_i(x_i(k),N\hat{v}_i(k))-$$
$$\nabla_{x_i(k)}f_i(x_i(k),N\hat{v}_i(k))+w_i(k)-$$
$$w_i(k)+\nabla_{\hat{v}_i(k)}f_i(x_i(k),N\hat{v}_i(k))-$$
$$\nabla_{\hat{v}_i(k)}f_i(x_i(k),N\hat{v}_i(k)),y_i\rangle.$$

令$y=y(k)-x^*$, 有

$$\langle\nabla g_i(x(k)),y(k)-x^*\rangle\leqslant$$
$$\langle\nabla_{x_i(k)}f_i(x_i(k),\Phi(x(k)))-$$
$$\nabla_{x_i(k)}f_i(x_i(k),N\hat{v}_i(k)),y_i(k)-x_i^*\rangle+$$
$$\langle\nabla_{\Phi}f_i(x_i(k),\Phi(x(k)))\nabla_{x_i(k)}\Phi(x(k))-$$
$$\nabla_{\hat{v}_i(k)}f_i(x_i(k),N\hat{v}_i(k)),y_i(k)-x_i^*\rangle-$$
$$\langle w_i(k),y_i(k)-x_i^*\rangle\leqslant$$
$$dl_1\|\Phi(x(k))-N\hat{v}_i(k)\|-$$
$$\langle w_i(k),y_i(k)-x_i^*\rangle+$$
$$d\|\nabla_{\Phi}f_i(x_i(k),\Phi(x(k)))\nabla_{x_i(k)}\Phi(x(k))-$$
$$\nabla_{\hat{v}_i(k)}f_i(x_i(k),N\hat{v}_i(k))\|. \tag{21}$$

其中: 第 1 个小于等于号由引理 3 得到, 第 2 个小于等于号由假设 1 中的 1) 和假设 2 中的 1) 得到. 在式 (21) 两边加上$\langle\nabla g_i(x(k)),x^*-x(k)\rangle$, 可得到

$$\langle\nabla g_i(x(k)),y(k)-x(k)\rangle\leqslant$$
$$\langle\nabla g_i(x(k)),x^*-x(k)\rangle+$$
$$dl_1\|\Phi(x(k))-N\hat{v}_i(k)\|+$$
$$d\|\nabla_{\Phi}f_i(x_i(k),\Phi(x(k)))-$$
$$\nabla_{\hat{v}_i(k)}f_i(x_i(k),N\hat{v}_i(k))\|-$$
$$\langle w_i(k),y_i(k)-x_i^*\rangle\leqslant$$
$$\langle\nabla g_i(x_i(k)),x^*-x(k)\rangle-$$
$$\langle w_i(k),y_i(k)-x_i^*\rangle+$$
$$(dl_1+dl_2)\|\Phi(x(k))-N\hat{v}_i(k)\|. \tag{22}$$

这里: 第 1 个不等号由于$\nabla_{x_i(k)}\Phi(x(k))=1$成立, 第 2 个不等号由假设 2 中的 2) 得到. 又因g_i为强凸函数, 由$\langle\nabla g_i(x(k)),x^*-x(k)\rangle\leqslant-(g_i(x(k))-g_i(x^*))$, 式(22) 可写为

$$\langle\nabla g_i(x(k)),y(k)-x(k)\rangle\leqslant$$
$$-(g_i(x(k))-g_i(x^*))+$$
$$dl_1\|\Phi(x(k))-N\hat{v}_i(k)\|-$$
$$\langle w_i(k),y_i(k)-x_i^*\rangle+$$
$$dl_2\|\Phi(x(k))-N\hat{v}_i(k)\|. \tag{23}$$

由于$w_i(k)\sim N(0,\sigma_i^2(k))$, 对式 (23) 求期望, 可得到

$$\mathrm{E}[\langle\nabla g_i(x(k)),y(k)-x(k)\rangle]\leqslant$$
$$-\mathrm{E}[g_i(x_i(k))-g_i(x_i^*)]+$$
$$d(l_1+l_2)\mathrm{E}[\|\Phi(x(k))-N\hat{v}_i(k)\|]. \tag{24}$$

将引理 4 代入式 (24), 可得到

$$\mathrm{E}[\langle\nabla g_i(x(k)),y(k)-x(k)\rangle]\leqslant$$
$$-\mathrm{E}[g_i(x(k))-g_i(x^*)]+d(l_1+l_2)\Big(N^2d\theta\beta^k+$$
$$N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big). \tag{25}$$

对式 (19) 进行移项, 将其两边均减去一个$g_i(x^*)$, 求期望, 可得到

$$\mathrm{E}[g_i(x(k+1))-g_i(x^*)]\leqslant$$
$$\mathrm{E}[g_i(x(k))-g_i(x^*)]+\alpha_k\mathrm{E}[(y(k)-$$
$$x(k))^{\mathrm{T}}\nabla g_i(x)]+\frac{NL}{2}\alpha_k^2d^2. \tag{26}$$

将式 (25) 代入 (26), 可得到

$$\mathrm{E}[g_i(x(k+1))-g_i(x^*)]\leqslant$$
$$\frac{NL}{2}\alpha_k^2d^2+$$
$$d(l_1+l_2)\alpha_k\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big)+$$
$$(1-\alpha_k)\mathrm{E}[g_i(x(k))-g_i(x^*)]. \tag{27}$$

再根据$g_i(x(k))$的定义, 引理 5 得证. □

引理 6[22]　设$\{h(k),k=0,1,\ldots\}$, $\{\tau(k),k=0,1,\ldots\}$和$\{\mu(k),k=0,1,\ldots\}$为实序列, 满足$0<\tau(k)\leqslant1$, $\mu(k)\geqslant0$ $(k=0,1,\ldots)$, $\sum_{k=0}^{\infty}\tau(k)=\infty$, $\frac{\mu(k)}{\tau(k)}\to0$ $(k\to\infty)$, 以及$h(k+1)\leqslant(1-\tau(k))h(k)+\mu(k)$, 则

$\lim\limits_{k\to\infty}\sup h(k)\leqslant 0$. 特别地, 若$h(k)\geqslant 0\,(k=0,1,\ldots)$, 则$k\to\infty$时, $h(k)\to 0$.

定理 2 设假设 1 ~ 假设 5 成立, 每个玩家$i\in\mathcal{V}$的策略$x_i(k)$根据算法 1 迭代生成, 则有

$$\lim_{k\to\infty}\mathrm{E}[f_i(x_i(k+1),\Phi(x(k+1)))-f_i(x_i^*,\Phi(x^*))]=0,$$

其中x_i^*为玩家i的纳什均衡策略.

证明 由引理 5, 可得到

$$\mathrm{E}[g_i(x(k+1))-g_i(x^*)]\leqslant$$
$$(1-\alpha_k)\mathrm{E}[g_i(x(k))-g_i(x^*)]+\frac{NL}{2}\alpha_k^2d^2+$$
$$\alpha_k dl_1\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big)+$$
$$\alpha_k dl_2\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big).$$

由引理 6, 令

$$h(k)=\mathrm{E}[g_i(x(k))-g_i(x^*)],\ \tau(k)=\alpha_k;$$
$$\mu(k)=$$
$$\frac{NL}{2}\alpha_k^2d^2+\alpha_k dl_1\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big)+$$
$$\alpha_k dl_2\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big).$$

由假设 4 可知

$$\sum_{k=0}^{\infty}\alpha_k=\infty,$$
$$\lim_{k\to\infty}\frac{\mu(k)}{\tau(k)}=$$
$$\lim_{k\to\infty}\Big(\frac{NL}{2}\alpha_k d^2+dl_1\Big(N^2d\theta\beta^k+$$
$$N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big)+$$
$$dl_2\Big(N^2d\theta\beta^k+N^2d\theta\sum_{s=1}^{k}\beta^{k-s}\alpha_{s-1}\Big)\Big)=0.$$

由假设 5, 可得到

$$h(k)=\mathrm{E}[g_i(x(k))-g_i(x^*)]\geqslant$$
$$\mathrm{E}[\langle\nabla g_i(x^*),x(k)-x^*\rangle]=0,$$

因此, 有

$$\lim_{k\to\infty}\mathrm{E}(g_i(x(k))-g_i(x^*))=0.$$

再根据$g_i(x(k))$的定义, 定理 2 得证. □

推论 1 设假设 1 ~ 假设 5 成立, $\epsilon\in(0,1)$, $\delta>0$足够小, $w_i(k)\sim N(0,\sigma_i^2(k))$, $\sigma_i(k)=\dfrac{d\sqrt{2\ln\Big(\dfrac{1.25}{\delta}\Big)}\alpha_{k-1}}{\epsilon}$, 每个玩家的策略根据算法 1 迭代生成, 则生成的$x_i(k)\,(i\in\mathcal{V})$能够均方收敛, 即算法 1 可以实现差分隐私保护并在均方意义下找到纳什均衡点.

证明 由定理 1 可知, 算法 1 可实现(ϵ,δ)-差分隐私. 主要证明算法 1 实现均方收敛. 由于函数$g_i(x(k))$为μ强凸函数, 可得到

$$g_i(x(k))-g_i(x^*)\geqslant$$
$$(x(k)-x^*)^{\mathrm{T}}\nabla g_i(x^*)+\frac{\mu}{2}\|x(k)-x^*\|^2.\tag{28}$$

由假设 5 和x^*为纳什均衡点可知$\nabla g_i(x^*)=0$, 式 (28) 可写为

$$\frac{\mu}{2}\|x(k)-x^*\|^2\leqslant g_i(x(k))-g_i(x^*).\tag{29}$$

对式 (29) 两边取期望, 可得到

$$\frac{\mu}{2}\mathrm{E}[\|x(k)-x^*\|^2]\leqslant\mathrm{E}[g_i(x(k))-g_i(x^*)].$$

因此, 由定理 1 可知序列$\{\mathrm{E}[g_i(x(k))-g_i(x^*)],k=1,2,\ldots\}$收敛, 序列$\{\mathrm{E}[\|x(k)-x^*\|^2],k=1,2,\ldots\}$是收敛的, 即算法 1 均方意义下收敛. □

3 数值仿真

在本节中, 考虑 5 个玩家的能耗博弈[16], 它们之间的通信拓扑由图 1 所示的 3 种通信拓扑进行切换. 在能量消耗博弈中, 玩家i的目标函数为

$$f_i(x)=(x_i-\hat{x}_i)^2+\Big(0.04\sum_{i=1}^{5}x_i+5\Big)x_i.$$

其中: $\hat{x}_1=50,\hat{x}_2=55,\hat{x}_3=60,\hat{x}_4=65,\hat{x}_5=70$. 为了进一步表明参与者调节自身能量消耗的能力有限, 假设$x_1\in[40,43],x_2\in[42,50],x_3\in[48,52],x_4\in[54,58],x_5\in[58,63]$. 本文选择初始值$x(0)=(42,45,50,55,60)$, 步长$\alpha_k=\dfrac{1}{k}$, $\epsilon=0.1$, $\delta=0.01$. 通过直接计算, 纳什均衡点为$x^*=(41.5,46.4,51.3,56.2,61.1)$. 显然, 上述情形满足本文的假设. 通过 Matlab 使用算法 1 对上述问题进行仿真实验, 得到如下结果. 图 2 为玩家 1 在对梯度添加噪声和不添加噪声情况下聚合策略平均值的估计, 两者有一定的差别, 即在估计聚合策略时传递信息不是真实信息, 以达到隐私保护的目的. 图 3 为所提出算法下每个玩家对聚合项平均值的估计随时间的变化, 聚合项随迭代的增加是收敛的, 即当所有策略均达到纳什均衡时, 总体能耗是保持不变的. 图 4 为投影梯度下降法聚合策略的平均值随迭代次数的演化. 图 5 为所提出算法下每个玩家策略值随时间的变化, 随着迭代的增加, 所有玩家的策略均会达到一个定值, 即寻找到纳什均衡, 以实现本文的目标. 图 6 为投影梯度下降法下每个玩家策略随迭代次数的演化, 约

束集为一个区间, 当下降过大时会被投影回区间的最小值, 因此, 图 6 中一开始变化幅度会很大. 此外, 图 3 和图 5 在 40 步左右便能够实现收敛, 图 4 和图 6 则是在 60 步左右才能收敛, 进而体现出所提出算法收敛速度更快的优越性.

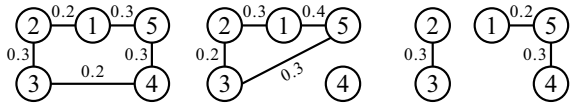

图1　玩家之间的通信拓扑

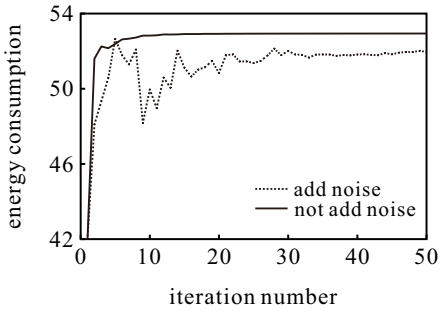

图2　玩家 1 对聚合策略平均值估计的比较

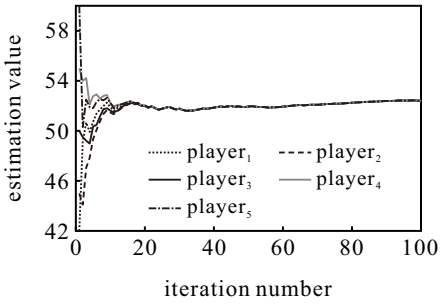

图3　每个玩家对聚合策略平均值的估计

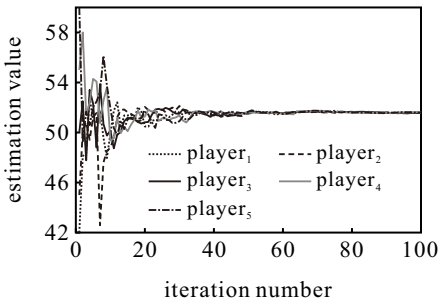

图4　投影梯度法对聚合策略平均值的估计

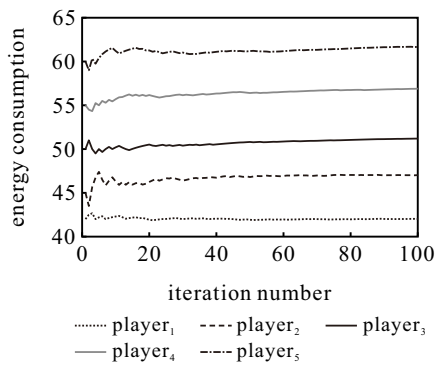

图5　每个玩家策略随时间的变化

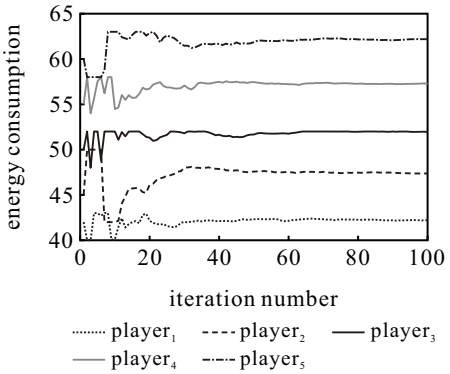

图6　投影梯度法玩家策略随时间的变化

4　结　论

本文深入探讨了分布式聚合博弈中的纳什均衡寻求问题, 并特别关注了在寻求均衡过程中如何有效地保护玩家的隐私. 为了准确地估计玩家的聚合策略, 本文采用了动态跟踪一致性协议估计聚合项; 为了不泄露玩家敏感信息, 通过引入高斯分布的随机噪声对梯度信息进行了干扰, 以实现隐私保护. 本文提出了一种新颖的分布式差分隐私算法, 该算法基于步长递减的 Frank-Wolfe 方法, 旨在解决聚合博弈中的隐私保护和收敛性问题. 通过精心设计的算法框架, 不仅确保了玩家隐私的安全, 还通过实验验证了所提出算法收敛速度更快的优越性.

参考文献 (References)

[1] 王元华, 张秋童, 臧文科. 切换网络演化博弈的同步[J]. 控制与决策, 2024, 39(10): 3313-3318.
(Wang Y H, Zhang Q T, Zang W K. Synchronization of switched networked evolutionary games[J]. Control and Decision, 2024, 39(10): 3313-3318.)

[2] Deng Z H. Distributed Nash equilibrium seeking for aggregative games with second-order nonlinear players[J]. Automatica, 2022, 135: 109980.

[3] 衣鹏, 潘越, 王文远, 等. 基于博弈论的多车智能驾驶交互决策综述[J]. 控制与决策, 2023, 38(5): 1159-1175.
(Yi P, Pan Y, Wang W Y, et al. A review on interactive decision-making of multi-vehicle autonomous driving with a game theoretical perspective[J]. Control and Decision, 2023, 38(5): 1159-1175.)

[4] 刘学达, 何明, 禹明刚, 等. 基于公共物品博弈的无人机集群弹药分配方法[J]. 控制与决策, 2022, 37(10): 2696-2704.
(Liu X D, He M, Yu M G, et al. UAV swarm ammunition distribution method based on public goods game[J]. Control and Decision, 2022, 37(10): 2696-2704.)

[5] 王浩丞, 罗贺, 马滢滢, 等. 基于纳什均衡博弈的多无人机对地攻击目标分配方法[J]. 控制与决策, 2024, 39(4): 1361-1369.
(Wang H C, Luo H, Ma Y Y, et al. A target assignment method based on Nash equilibrium game for multi UAV

ground attack[J]. Control and Decision, 2024, 39(4): 1361-1369.)

[6] 刘敏, 王金环. 基于势博弈的智能电网需求侧管理问题[J]. 控制与决策, 2024, 39(2): 545-550.
(Liu M, Wang J H. Potential game for demand-side management of smart grids[J]. Control and Decision, 2024, 39(2): 545-550.)

[7] Koshal J, Nedić A, Shanbhag U V. Distributed algorithms for aggregative games on graphs[J]. Operations Research, 2016, 64(3): 680-704.

[8] Deng Z H, Nian X H. Distributed generalized Nash equilibrium seeking algorithm design for aggregative games over weight-balanced digraphs[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(3): 695-706.

[9] Liang S, Yi P, Hong Y G. Distributed Nash equilibrium seeking for aggregative games with coupled constraints[J]. Automatica, 2017, 85: 179-185.

[10] Zhu R P, Zhang J Q, You K Y, et al. Asynchronous networked aggregative games[J]. Automatica, 2022, 136: 110054.

[11] Huang S J, Lei J L, Hong Y G. A linearly convergent distributed Nash equilibrium seeking algorithm for aggregative games[J]. IEEE Transactions on Automatic Control, 2023, 68(3): 1753-1759.

[12] Ruan M H, Gao H, Wang Y Q. Secure and privacy-preserving consensus[J]. IEEE Transactions on Automatic Control, 2019, 64(10): 4035-4049.

[13] Wang Y Q. Privacy-preserving average consensus via state decomposition[J]. IEEE Transactions on Automatic Control, 2019, 64(11): 4711-4716.

[14] Dwork C, Roth A. The algorithmic foundations of differential privacy[J]. Foundations and Trends® in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[15] Yan Y P, Wang X L, Ligeti P, et al. DP-FSAEA: Differential privacy for federated surrogate-assisted evolutionary algorithms[J]. IEEE Transactions on Evolutionary Computation, 2024, PP(99): 1.

[16] Ye M J, Hu G Q, Xie L H, et al. Differentially private distributed Nash equilibrium seeking for aggregative games[J]. IEEE Transactions on Automatic Control, 2022, 67(5): 2451-2458.

[17] Wang J M, Zhang J F, He X K. Differentially private distributed algorithms for stochastic aggregative games[J]. Automatica, 2022, 142: 110440.

[18] Wang Y Q, Nedić A. Differentially private distributed algorithms for aggregative games with guaranteed convergence[J]. IEEE Transactions on Automatic Control, 2024, 69(8): 5168-5183.

[19] Frank M, Wolfe P. An algorithm for quadratic programming[J]. Naval Research Logistics Quarterly, 1956, 3(1/2): 95-110.

[20] Hazan E, Minasyan E. Faster projection-free online learning[J/OL]. 2020, arXiv: 2001.11568.

[21] Chen G P, Yi P, Hong Y G, et al. Distributed optimization with projection-free dynamics: A frank-wolfe perspective[J]. IEEE Transactions on Cybernetics, 2024, 54(1): 599-610.

[22] Wang T Y, Yi P. Distributed projection-free algorithm for constrained aggregative optimization[J]. International Journal of Robust and Nonlinear Control, 2023, 33(10): 5273-5288.

[23] Jiang X, Zeng X L, Xie L H, et al. Distributed stochastic projection-free solver for constrained optimization[J/OL]. 2022, arXiv: 2204.10605.

作者简介

杨通清 (1997−), 男, 硕士生, 主要研究方向为分布式控制、优化与博弈, E-mail: yangtongqing08@126.com;

莫立坡 (1980−), 男, 教授, 博士, 博士生导师, 主要研究方向为分布式控制、优化与博弈, E-mail: beihangmlp@126.com;

龙飞 (1972−), 男, 教授, 博士, 主要研究方向为混杂系统控制、神经网络控制, E-mail: feilong@git.edu.cn;

符义昊 (2002−), 男, 硕士生, 主要研究方向为分布式优化与博弈, E-mail: Fyhao_0809@163.com.