

第 9 章：联邦学习公平性

思考题 9.1

计算性能向量的均值：

对于模型 G ：

$$\bar{P}(G) = \frac{0.8 + 1.2 + 1.0}{3} = 1.0$$

对于模型 G' ：

$$\bar{P}(G') = \frac{0.5 + 1.5 + 1.0}{3} = 1.0$$

基于方差计算公平性：方差反映了模型在各个客户端上性能的偏离程度，方差越小，性能分布越均衡，模型越公平。对于模型 G 的方差：

$$Var(P(G)) = \frac{(0.8 - 1.0)^2 + (1.2 - 1.0)^2 + (1.0 - 1.0)^2}{3} = \frac{0.04 + 0.04 + 0}{3} \approx 0.0267$$

对于模型 G' 的方差：

$$Var(P(G')) = \frac{(0.5 - 1.0)^2 + (1.5 - 1.0)^2 + (1.0 - 1.0)^2}{3} = \frac{0.25 + 0.25 + 0}{3} \approx 0.1667$$

由于 $Var(P(G)) < Var(P(G'))$ ，根据基于方差的公平性度量准则，**模型 G 比模型 G' 更公平。**

基于余弦相似度计算公平性：余弦相似度衡量性能向量 P 与理想全 1 向量 $\vec{1}$ 的接近程度，余弦值越大（越接近 1），说明模型在各客户端表现越一致、越公平。对于模型 G ：

$$Cos(P(G), \vec{1}) = \frac{\sum P_k(G)}{\sqrt{3} \cdot \sqrt{\sum P_k(G)^2}} = \frac{3.0}{\sqrt{3} \cdot \sqrt{0.64 + 1.44 + 1.0}} = \frac{3.0}{\sqrt{3} \times 3.08} \approx 0.9868$$

对于模型 G' ：

$$Cos(P(G'), \vec{1}) = \frac{\sum P_k(G')}{\sqrt{3} \cdot \sqrt{\sum P_k(G')^2}} = \frac{3.0}{\sqrt{3} \cdot \sqrt{0.25 + 2.25 + 1.0}} = \frac{3.0}{\sqrt{3} \times 3.5} \approx 0.9258$$

由于 $Cos(P(G), \vec{1}) > Cos(P(G'), \vec{1})$ ，模型 G 更公平。**两种度量方法得出的结论是一致的。**

思考题 9.2

计算参与方 1 的夏普利值 $\varphi(1)$ ：根据夏普利值计算公式

$$\varphi(i) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(N - |S| - 1)!}{N!} [v(S \cup \{i\}) - v(S)]$$

参与方总数 $N = 3$ 列出参与方 1 加入所有可能子集 S 的边缘贡献与权重：

- 当 $S = \emptyset$ 时, 权重为 $\frac{0!2!}{3!} = \frac{1}{3}$, 边缘贡献为 $v(\{1\}) - v(\emptyset) = 6 - 0 = 6$ 。
- 当 $S = \{2\}$ 时, 权重为 $\frac{1!1!}{3!} = \frac{1}{6}$, 边缘贡献为 $v(\{1, 2\}) - v(\{2\}) = 24 - 12 = 12$ 。
- 当 $S = \{3\}$ 时, 权重为 $\frac{1!1!}{3!} = \frac{1}{6}$, 边缘贡献为 $v(\{1, 3\}) - v(\{3\}) = 30 - 18 = 12$ 。
- 当 $S = \{2, 3\}$ 时, 权重为 $\frac{2!0!}{3!} = \frac{1}{3}$, 边缘贡献为 $v(\{1, 2, 3\}) - v(\{2, 3\}) = 48 - 36 = 12$ 。

综合求和:

$$\varphi(1) = \frac{1}{3} \times 6 + \frac{1}{6} \times 12 + \frac{1}{6} \times 12 + \frac{1}{3} \times 12 = 2 + 2 + 2 + 4 = 10$$

因此, 参与方 1 的夏普利值为 **10**。

验证合理性公理 (效率公理): 合理性公理要求所有参与方的夏普利值总和等于全集收益 $v(\{1, 2, 3\}) = 48$ 。我们需要核算 $\varphi(2)$ 与 $\varphi(3)$: 对于参与方 2:

$$\varphi(2) = \frac{1}{3}(12) + \frac{1}{6}(24 - 6) + \frac{1}{6}(36 - 18) + \frac{1}{3}(48 - 30) = 4 + 3 + 3 + 6 = 16$$

对于参与方 3:

$$\varphi(3) = \frac{1}{3}(18) + \frac{1}{6}(30 - 6) + \frac{1}{6}(36 - 12) + \frac{1}{3}(48 - 24) = 6 + 4 + 4 + 8 = 22$$

将三者相加:

$$\varphi(1) + \varphi(2) + \varphi(3) = 10 + 16 + 22 = 48 = v(\{1, 2, 3\})$$

验证通过, 该结果满足合理性公理。

思考题 9.3

计算性能均等性函数 F : 根据题目给定公式, F 的本质即为各个客户端模型准确率的总体标准差。给定准确率向量 (p_1, p_2, \dots, p_N) , 首先计算均值 $\bar{p} = \frac{1}{N} \sum_{i=1}^N p_i$, 随后代入公式:

$$F = \sqrt{\frac{1}{N} \sum_{i=1}^N (p_i - \bar{p})^2}$$

F 的值越小, 代表性能在各个客户端间的分布越集中, 即联邦学习系统的公平性越高。

推导 p_i 关于 α_i 的数学关系: 在联邦学习本地训练阶段, 客户端 i 的准确率 p_i 受到超参数 (如学习率 α_i) 的直接影响。基于梯度下降优化的特性, 在模型并未严重过拟合或发散的前提下, 损失函数 L_i 的下降量与学习率 α_i 呈一定的非线性关系。由于准确率通常与损失函数呈负相关 ($p_i \approx 1 - cL_i$), 在合理的

取值范围内，准确率 p_i 可以利用泰勒展开近似为一个关于学习率 α_i 的凹二次函数：

$$p_i(\alpha_i) \approx p_i^{(0)} + \eta_i \alpha_i - \zeta_i \alpha_i^2$$

其中：

- $p_i^{(0)}$ 为未进行当前轮次更新前的基础准确率。
- $\eta_i > 0$ 表示由梯度下降带来的正向收益系数（一阶项）。
- $\zeta_i > 0$ 表示惩罚过大学习率导致震荡或不收敛的负向系数（二阶项）。

要使总体公平性度量 F 最小化，系统可以通过上述函数关系，为性能落后的客户端分配更优的 α_i （使其准确率趋近最优极值点），以缩小与 \bar{p} 的差距。

思考题 9.4

使指标 D 最小化的全局特征权重 \mathbf{b} 选择策略： 指标 $D = \max p_i - \min p_i$ 表示客户端间性能的最大极差。为了使得 D 最小化，理想情况下所有客户端的准确率应绝对相等，即对于目标常数 C ，有：

$$p_i \approx \mathbf{A}_i \cdot \mathbf{b} = C, \quad \forall i \in \{1, 2, \dots, N\}$$

将其写为矩阵形式，即要求解 $\mathbf{A}\mathbf{b} = C\mathbf{1}$ （其中 $\mathbf{1}$ 为全 1 向量）。在实际应用中（通常是超静定方程），我们可以利用最小二乘法来寻找使误差平方和最小的全局模型权重 \mathbf{b}^* ：

$$\mathbf{b}^* = \arg \min_{\mathbf{b}} \|\mathbf{A}\mathbf{b} - C\mathbf{1}\|_2^2$$

其闭式解为：

$$\mathbf{b}^* = C(\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \mathbf{1}$$

这样选出的 \mathbf{b} 能在各客户端的数据特征分布 \mathbf{A} 之间寻找平衡，有效降低极差 D 。

引入权重向量 \mathbf{w} 后，使 D_w 最小化的策略： 当引入客户端影响力权重 \mathbf{w} 后，指标变为 $D_w = \max(w_i p_i) - \min(w_i p_i)$ 。为了最小化加权极差 D_w ，我们需要使加权后的准确率趋于一致，即要求 $w_i(\mathbf{A}_i \cdot \mathbf{b}) = C'$ 。定义对角权重矩阵 $\mathbf{W} = \text{diag}(w_1, w_2, \dots, w_N)$ ，则矩阵方程变为 $\mathbf{W}\mathbf{A}\mathbf{b} = C'\mathbf{1}$ 。

- **对 \mathbf{w} 的选择：** 权重 w_i 的设定应与该客户端的数据质量或样本量呈反向相关。对于数据质量差、量少的弱势客户端，设置较大的 w_i 值（给予更多关注）；对于数据丰富的强势客户端，设置较小的 w_i 值。这迫使优化过程向弱势群体倾斜，弥补其天然短板。
- **对 \mathbf{b} 的选择：** 在确定了 \mathbf{W} 矩阵后，通过加权最小二乘法求解全局特征权重 \mathbf{b}^* ：

$$\mathbf{b}^* = \arg \min_{\mathbf{b}} \|\mathbf{W}\mathbf{A}\mathbf{b} - C'\mathbf{1}\|_2^2$$

闭式解为：

$$\mathbf{b}^* = C'(\mathbf{A}^T \mathbf{W}^2 \mathbf{A})^{-1} \mathbf{A}^T \mathbf{W} \mathbf{1}$$

通过协同设定非负权重向量 \mathbf{w} 并结合上式求解 \mathbf{b} ，联邦系统可以在充分兼顾数据异构性和质量差异的前提下，最大程度地提升加权公平性指标。