

第 10 章：联邦学习贡献度与激励机制

思考题 10.1

根据夏普利值的计算公式：

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

我们需要计算参与方 1 加入所有可能不包含其自身的子集 S 时的边缘贡献及其对应的权重。系统的总参与方数量为 $N = 3$ 。

当子集 $S = \emptyset$ (即 $|S| = 0$) 时, 权重为 $\frac{0!2!}{3!} = \frac{1}{3}$, 此时参与方 1 的边缘贡献为 $v(\{1\}) - v(\emptyset) = 2 - 0 = 2$ 。加权后的值为 $\frac{1}{3} \times 2 = \frac{2}{3}$ 。当子集 $S = \{2\}$ (即 $|S| = 1$) 时, 权重为 $\frac{1!1!}{3!} = \frac{1}{6}$, 此时参与方 1 的边缘贡献为 $v(\{1, 2\}) - v(\{2\}) = 7 - 3 = 4$ 。加权后的值为 $\frac{1}{6} \times 4 = \frac{2}{3}$ 。当子集 $S = \{3\}$ (即 $|S| = 1$) 时, 权重为 $\frac{1!1!}{3!} = \frac{1}{6}$, 此时参与方 1 的边缘贡献为 $v(\{1, 3\}) - v(\{3\}) = 5 - 1 = 4$ 。加权后的值为 $\frac{1}{6} \times 4 = \frac{2}{3}$ 。当子集 $S = \{2, 3\}$ (即 $|S| = 2$) 时, 权重为 $\frac{2!0!}{3!} = \frac{1}{3}$, 此时参与方 1 的边缘贡献为 $v(\{1, 2, 3\}) - v(\{2, 3\}) = 12 - 6 = 6$ 。加权后的值为 $\frac{1}{3} \times 6 = 2$ 。

将所有可能情况下的加权边缘贡献进行求和, 即可得到参与方 1 的夏普利值 $\varphi_1 = \frac{2}{3} + \frac{2}{3} + \frac{2}{3} + 2 = 4$ 。

思考题 10.2

在联邦学习的激励机制中, 奖励函数的目的在于量化并回馈参与方对全局模型带来的性能提升。根据书中边际收益 (Marginal Gain) 分配的思想, 参与方的效用可以通过其加入联邦系统前后全局模型性能的变化来衡量。

由于全局模型的目标是最小化总损失函数 $\mathcal{L}(W)$, 一个有用的模型更新应当能够进一步降低全局损失。我们定义 $W \setminus \{w_i\}$ 为排除了参与方 i 的模型更新后聚合得到的全局模型, 定义 W 为包含所有参与方更新聚合后的全局模型。参与方 i 提供更新 w_i 所带来的边际损失减少量即为 $\mathcal{L}(W \setminus \{w_i\}) - \mathcal{L}(W)$ 。为了鼓励有效的模型更新并防止由于恶意或低质量更新导致损失增加而被奖励, 我们可以通过一个缩放系数和非负截断操作来构建奖励函数。其数学表达式可以设计为:

$$R_i(w_i, W) = \alpha \cdot \max(0, \mathcal{L}(W \setminus \{w_i\}) - \mathcal{L}(W))$$

式中, $\alpha > 0$ 为将损失函数的降低幅度转换为实际奖励份额的缩放超参数。该函数能够确保只有当参与方的更新真正有助于优化全局目标时, 才会获得与之贡献成正比的奖励。

思考题 10.3

为了计算每个客户端的总奖励, 我们需要先将总奖励池按照设定的规则拆分为“数据量奖励池”和“数据质量奖励池”, 然后再分别计算各客户端在两个池中所占的份额并予以加和。已知总奖励为 1000 单位, 根据比例设定, 数据量奖励池的总额为 $1000 \times 70\% = 700$ 单位, 数据质量奖励池的总额为 $1000 \times 30\% = 300$ 单位。

对于数据量部分，四家客户端提供的数据总条数为 $500 + 300 + 200 + 100 = 1100$ 条。各客户端在此部分获取的奖励取决于其数据量占总量的比例。对于数据质量部分，四家客户端的质量总得分为 $8 + 9 + 7 + 10 = 34$ 分。各客户端在此部分获取的奖励取决于其质量得分占总得分的比例。

客户端 A 的总奖励 $= 700 \times \frac{500}{1100} + 300 \times \frac{8}{34} \approx 318.18 + 70.59 = 388.77$ 单位。
 客户端 B 的总奖励 $= 700 \times \frac{300}{1100} + 300 \times \frac{9}{34} \approx 190.91 + 79.41 = 270.32$ 单位。
 客户端 C 的总奖励 $= 700 \times \frac{200}{1100} + 300 \times \frac{7}{34} \approx 127.27 + 61.76 = 189.03$ 单位。
 客户端 D 的总奖励 $= 700 \times \frac{100}{1100} + 300 \times \frac{10}{34} \approx 63.64 + 88.24 = 151.88$ 单位。

加总核算可知， $388.77 + 270.32 + 189.03 + 151.88 = 1000$ ，验证了分配结果的准确性。

思考题 10.4

本题中，各参与方组合的模型性能即代表了组合的收益值 $v(S)$ 。假定未加入任何数据时（即空集 \emptyset ）的模型基础性能为 $v(\emptyset) = 0$ 。我们需要根据夏普利值计算公式对客户端 A、B、C 分别进行遍历核算。

对于客户端 A，当加入空集 \emptyset 时，边缘贡献为 $0.60 - 0 = 0.60$ ，权重为 $1/3$ ；当加入子集 $\{B\}$ 时，边缘贡献为 $0.72 - 0.65 = 0.07$ ，权重为 $1/6$ ；当加入子集 $\{C\}$ 时，边缘贡献为 $0.74 - 0.62 = 0.12$ ，权重为 $1/6$ ；当加入子集 $\{B, C\}$ 时，边缘贡献为 $0.80 - 0.76 = 0.04$ ，权重为 $1/3$ 。将这些加权相加得到客户端 A 的夏普利值为 $\varphi_A = \frac{1}{3} \times 0.60 + \frac{1}{6} \times 0.07 + \frac{1}{6} \times 0.12 + \frac{1}{3} \times 0.04 = 0.20 + 0.011667 + 0.02 + 0.013333 = 0.245$ 。

对于客户端 B，当加入空集 \emptyset 时，边缘贡献为 $0.65 - 0 = 0.65$ ，权重为 $1/3$ ；当加入子集 $\{A\}$ 时，边缘贡献为 $0.72 - 0.60 = 0.12$ ，权重为 $1/6$ ；当加入子集 $\{C\}$ 时，边缘贡献为 $0.76 - 0.62 = 0.14$ ，权重为 $1/6$ ；当加入子集 $\{A, C\}$ 时，边缘贡献为 $0.80 - 0.74 = 0.06$ ，权重为 $1/3$ 。加权求和得到客户端 B 的夏普利值为 $\varphi_B = \frac{1}{3} \times 0.65 + \frac{1}{6} \times 0.12 + \frac{1}{6} \times 0.14 + \frac{1}{3} \times 0.06 = 0.216667 + 0.02 + 0.023333 + 0.02 = 0.280$ 。

对于客户端 C，当加入空集 \emptyset 时，边缘贡献为 $0.62 - 0 = 0.62$ ，权重为 $1/3$ ；当加入子集 $\{A\}$ 时，边缘贡献为 $0.74 - 0.60 = 0.14$ ，权重为 $1/6$ ；当加入子集 $\{B\}$ 时，边缘贡献为 $0.76 - 0.65 = 0.11$ ，权重为 $1/6$ ；当加入子集 $\{A, B\}$ 时，边缘贡献为 $0.80 - 0.72 = 0.08$ ，权重为 $1/3$ 。加权求和得到客户端 C 的夏普利值为 $\varphi_C = \frac{1}{3} \times 0.62 + \frac{1}{6} \times 0.14 + \frac{1}{6} \times 0.11 + \frac{1}{3} \times 0.08 = 0.206667 + 0.023333 + 0.018333 + 0.026667 = 0.275$ 。

我们可以通过效率公理（合理性）来验证上述计算结果： $\varphi_A + \varphi_B + \varphi_C = 0.245 + 0.280 + 0.275 = 0.80$ ，正好等同于全局模型在使用所有数据时的总性能 $v(\{A, B, C\})$ ，证明计算准确无误。