

## 第 7 章：联邦学习的多目标优化

### 思考题 7.1

由于三个目标  $\epsilon_p, \epsilon_u, \epsilon_c$  都是越小越好，因此在多目标优化中，若一个方案在三个目标上都不大于另一个方案，且至少有一个目标严格更小，则称前者支配后者。

首先检查三个方案是否满足约束条件：

$$\epsilon_p \leq 0.3, \quad \epsilon_u \leq 0.5, \quad \epsilon_c \leq 0.45$$

对三种方案分别有：

$$\alpha = (0.25, 0.40, 0.35), \quad \beta = (0.30, 0.35, 0.30), \quad \gamma = (0.20, 0.45, 0.40)$$

可以看出三者都满足约束，因此都是可行解。

(a) 这里不作图，直接用文字说明 Pareto 前沿。比较各方案：

$\alpha$  与  $\beta$ ：

方案  $\alpha$  在隐私泄露上更优：

$$0.25 < 0.30$$

但在效用损失和通信成本上较差：

$$0.40 > 0.35, \quad 0.35 > 0.30$$

因此  $\alpha$  不支配  $\beta$ ， $\beta$  也不支配  $\alpha$ 。

$\alpha$  与  $\gamma$ ：

方案  $\gamma$  在隐私泄露上更优：

$$0.20 < 0.25$$

但在效用损失和通信成本上较差：

$$0.45 > 0.40, \quad 0.40 > 0.35$$

因此  $\alpha$  与  $\gamma$  互不支配。

$\beta$  与  $\gamma$ ：

方案  $\gamma$  在隐私泄露上更优：

$$0.20 < 0.30$$

但方案  $\beta$  在效用损失和通信成本上更优：

$$0.35 < 0.45, \quad 0.30 < 0.40$$

因此  $\beta$  与  $\gamma$  也互不支配。

所以，原来的三个方案都属于非支配解，即 Pareto 前沿为

$$\{\alpha, \beta, \gamma\}$$

(b) 验证方案  $\beta$  是否被其他方案支配。

若  $\beta$  被支配,则必须存在某个方案在三个目标上都不大于  $\beta = (0.30, 0.35, 0.30)$ , 且至少一个更小。

先看  $\alpha = (0.25, 0.40, 0.35)$ :

$$0.25 < 0.30$$

但

$$0.40 > 0.35, \quad 0.35 > 0.30$$

因此  $\alpha$  不支配  $\beta$ 。

再看  $\gamma = (0.20, 0.45, 0.40)$ :

$$0.20 < 0.30$$

但

$$0.45 > 0.35, \quad 0.40 > 0.30$$

因此  $\gamma$  也不支配  $\beta$ 。

故方案  $\beta$  不被其他方案支配, 即

$\beta$  不是被支配解

(c) 引入新方案

$$\delta = (0.28, 0.38, 0.33)$$

先验证其是否满足约束:

$$0.28 \leq 0.3, \quad 0.38 \leq 0.5, \quad 0.33 \leq 0.45$$

因此  $\delta$  也是可行解。

接着比较  $\delta$  与原有方案的支配关系。

与  $\alpha = (0.25, 0.40, 0.35)$  比较:

$\delta$  在  $\epsilon_u, \epsilon_c$  上更优, 即  $0.38 < 0.40, 0.33 < 0.35$

但在  $\epsilon_p$  上较差:

$$0.28 > 0.25$$

所以  $\delta$  与  $\alpha$  互不支配。

与  $\beta = (0.30, 0.35, 0.30)$  比较:

$\delta$  在  $\epsilon_p$  上更优, 即  $0.28 < 0.30$

但在  $\epsilon_u, \epsilon_c$  上较差:

$$0.38 > 0.35, \quad 0.33 > 0.30$$

所以  $\delta$  与  $\beta$  互不支配。

与  $\gamma = (0.20, 0.45, 0.40)$  比较:

$\delta$  在  $\epsilon_u, \epsilon_c$  上更优, 即  $0.38 < 0.45, 0.33 < 0.40$

但在  $\epsilon_p$  上较差:

$$0.28 > 0.20$$

所以  $\delta$  与  $\gamma$  也互不支配。

因此, 新方案  $\delta$  不被原有方案支配, 同时也不支配原有任何方案。引入  $\delta$  后, Pareto 前沿扩展为

$$\{\alpha, \beta, \gamma, \delta\}$$

也就是说, 前沿上的非支配解数量由原来的 3 个增加为 4 个, 说明新方案提供了一个新的折中选择: 它在隐私、效用和通信三者之间取得了较为均衡的表现。

## 思考题 7.2

设高斯过程先验均值函数为 0, 核函数为

$$k(x, x') = \exp\left(-\frac{\|x - x'\|^2}{2l^2}\right)$$

记输入向量为

$$x = (\epsilon_p, \epsilon_u)$$

已有观测点为

$$x_1 = (0.25, 0.40), \quad x_2 = (0.30, 0.35), \quad x_3 = (0.20, 0.45)$$

对应观测值为

$$Y_0 = \begin{bmatrix} 0.35 \\ 0.30 \\ 0.40 \end{bmatrix}$$

要求在测试点

$$x_* = (0.28, 0.38)$$

处进行预测。

(a) 高斯过程回归的预测均值与方差公式分别为

$$\mu(x_*) = k_*^\top K^{-1} Y_0$$

$$\sigma^2(x_*) = k(x_*, x_*) - k_*^\top K^{-1} k_*$$

其中

$$K = \begin{bmatrix} k(x_1, x_1) & k(x_1, x_2) & k(x_1, x_3) \\ k(x_2, x_1) & k(x_2, x_2) & k(x_2, x_3) \\ k(x_3, x_1) & k(x_3, x_2) & k(x_3, x_3) \end{bmatrix}, \quad k_* = \begin{bmatrix} k(x_*, x_1) \\ k(x_*, x_2) \\ k(x_*, x_3) \end{bmatrix}$$

若取长度尺度  $l = 0.5$ , 则首先计算各核值。

由于

$$k(x_i, x_i) = 1$$

故对角元均为 1。

再计算非对角元：

$$\|x_1 - x_2\|^2 = (0.25 - 0.30)^2 + (0.40 - 0.35)^2 = 0.005$$

$$k(x_1, x_2) = \exp\left(-\frac{0.005}{2 \times 0.5^2}\right) = \exp(-0.01) \approx 0.9900$$

同理，

$$\|x_1 - x_3\|^2 = (0.25 - 0.20)^2 + (0.40 - 0.45)^2 = 0.005$$

$$k(x_1, x_3) \approx 0.9900$$

$$\|x_2 - x_3\|^2 = (0.30 - 0.20)^2 + (0.35 - 0.45)^2 = 0.02$$

$$k(x_2, x_3) = \exp\left(-\frac{0.02}{2 \times 0.5^2}\right) = \exp(-0.04) \approx 0.9608$$

因此

$$K \approx \begin{bmatrix} 1 & 0.9900 & 0.9900 \\ 0.9900 & 1 & 0.9608 \\ 0.9900 & 0.9608 & 1 \end{bmatrix}$$

接着计算测试点与各训练点之间的核值：

$$\|x_* - x_1\|^2 = (0.28 - 0.25)^2 + (0.38 - 0.40)^2 = 0.0013$$

$$k(x_*, x_1) = \exp\left(-\frac{0.0013}{2 \times 0.5^2}\right) = \exp(-0.0026) \approx 0.9974$$

$$\|x_* - x_2\|^2 = (0.28 - 0.30)^2 + (0.38 - 0.35)^2 = 0.0013$$

$$k(x_*, x_2) \approx 0.9974$$

$$\|x_* - x_3\|^2 = (0.28 - 0.20)^2 + (0.38 - 0.45)^2 = 0.0113$$

$$k(x_*, x_3) = \exp\left(-\frac{0.0113}{2 \times 0.5^2}\right) = \exp(-0.0226) \approx 0.9777$$

故

$$k_* \approx \begin{bmatrix} 0.9974 \\ 0.9974 \\ 0.9777 \end{bmatrix}$$

代入公式可得预测均值近似为

$$\mu(x_*) \approx 0.3248$$

预测方差近似为

$$\sigma^2(x_*) \approx 2.00 \times 10^{-4}$$

因此，在点  $(\epsilon_p = 0.28, \epsilon_u = 0.38)$  处，

$$\mu \approx 0.3248, \quad \sigma^2 \approx 0.0002$$

(b) 当长度尺度  $l$  从 0.5 增加到 1.0 时, RBF 核函数衰减得更慢, 即距离较远的点之间也会保持较高的相关性。这样会带来以下变化:

首先, 模型会认为更大范围内的样本彼此相似, 预测结果会更加平滑, 对局部波动不再那么敏感。其次, 由于测试点会同时受到更多已有观测点的影响, 预测方差通常会下降, 模型不确定性减小。于是采集函数在选择新点时更倾向于利用当前已经认为较优的区域, 而不是探索那些距离已有样本较远的未知区域。

因此, 从探索-利用权衡的角度看,  $l$  变大后, 模型的**利用性增强, 探索性减弱**。相反, 若  $l$  较小, 则核函数只强调局部相似性, 远处点相关性迅速衰减, 预测方差会相对更大, 更有利于探索未知区域。

(c) 为更好捕捉隐私-效用之间可能存在的非线性关系, 可以对核函数作如下改进。

一种直接方法是采用带自动相关确定 (ARD) 的 RBF 核, 即对不同输入维度使用不同长度尺度:

$$k_{\text{ARD}}(x, x') = \exp \left( -\frac{(\epsilon_p - \epsilon'_p)^2}{2l_p^2} - \frac{(\epsilon_u - \epsilon'_u)^2}{2l_u^2} \right)$$

这样可以分别学习隐私维度与效用维度的影响范围。当两个目标对结果的敏感程度不同, ARD 核通常比标准 RBF 核更合适。

若希望进一步表达更复杂的非线性耦合关系, 可以加入乘积项或非平稳项, 例如构造如下核函数:

$$k_{\text{new}}(x, x') = \exp \left( -\frac{(\epsilon_p - \epsilon'_p)^2}{2l_p^2} - \frac{(\epsilon_u - \epsilon'_u)^2}{2l_u^2} - \frac{\lambda((\epsilon_p \epsilon_u) - (\epsilon'_p \epsilon'_u))^2}{2} \right)$$

其中  $\lambda > 0$  为权重参数。该核函数除了考虑隐私和效用各自的相似性, 还显式建模了它们之间的交互作用, 因此更适合描述“隐私提高会以非线性方式影响效用”这一类关系。

另外, 也可以采用核函数加和或乘积的方式, 例如

$$k(x, x') = k_{\text{RBF}}(x, x') + \alpha k_{\text{Poly}}(x, x')$$

或

$$k(x, x') = k_{\text{RBF}}(x, x') \cdot k_{\text{RQ}}(x, x')$$

其中多项式核可增强对交互项的表达能力, Rational Quadratic 核则可以刻画多尺度变化。这样构造的组合核往往能更好地拟合隐私-效用之间复杂、非线性的目标函数关系。

综上, 若要更好捕捉隐私-效用的非线性关系, 推荐优先采用带不同长度尺度的 ARD-RBF 核; 若需要描述更强的耦合效应, 则可进一步引入交互项或组合核。

### 思考题 7.3

先说明一点：题目中称其为“零和博弈”，但给出的支付矩阵并不满足零和条件，因为每个格子的两个玩家收益之和并不恒为常数。例如，

$$(3, 2) \Rightarrow 3 + 2 = 5, \quad (1, 0) \Rightarrow 1 + 0 = 1$$

因此这里按**一般双人博弈**来求纳什均衡。

根据纳什均衡的定义，需要分别找出两名玩家的最佳响应。

对于玩家 1，固定玩家 2 的动作，比较玩家 1 的收益：

当玩家 2 选  $A$  时，玩家 1 收益分别为

$$X : 3, \quad Y : 2, \quad Z : 1$$

因此玩家 1 的最佳响应为

$$BR_1(A) = \{X\}$$

当玩家 2 选  $B$  时，玩家 1 收益分别为

$$X : 1, \quad Y : 2, \quad Z : 0$$

因此玩家 1 的最佳响应为

$$BR_1(B) = \{Y\}$$

当玩家 2 选  $C$  时，玩家 1 收益分别为

$$X : 2, \quad Y : 0, \quad Z : 2$$

因此玩家 1 的最佳响应为

$$BR_1(C) = \{X, Z\}$$

对于玩家 2，固定玩家 1 的动作，比较玩家 2 的收益：

当玩家 1 选  $X$  时，玩家 2 收益分别为

$$A : 2, \quad B : 0, \quad C : 3$$

因此玩家 2 的最佳响应为

$$BR_2(X) = \{C\}$$

当玩家 1 选  $Y$  时，玩家 2 收益分别为

$$A : 1, \quad B : 2, \quad C : 3$$

因此玩家 2 的最佳响应为

$$BR_2(Y) = \{C\}$$

当玩家 1 选  $Z$  时，玩家 2 收益分别为

$$A : 1, \quad B : 0, \quad C : 2$$

因此玩家 2 的最佳响应为

$$BR_2(Z) = \{C\}$$

纳什均衡是双方策略互为最佳响应的动作组合。由上可知：

$$(X, C)$$

中，玩家 1 在玩家 2 选  $C$  时选择  $X$  是最佳响应，而玩家 2 在玩家 1 选  $X$  时选择  $C$  也是最佳响应，所以

$$(X, C)$$

是一个纳什均衡。

同理，

$$(Z, C)$$

中，玩家 1 在玩家 2 选  $C$  时选择  $Z$  也是最佳响应，而玩家 2 在玩家 1 选  $Z$  时选择  $C$  仍是最佳响应，所以

$$(Z, C)$$

也是一个纳什均衡。

因此，该博弈的纯策略纳什均衡为

$$(X, C) \text{ 和 } (Z, C)$$

其中对应的支付分别为

$$(X, C) \rightarrow (2, 3), \quad (Z, C) \rightarrow (2, 2)$$

## 思考题 7.4

(a) 该多目标优化问题可写为

$$\min_{\mathbf{w} \in \mathcal{W}} (f_1(\mathbf{w}), f_2(\mathbf{w}))$$

其中

$$\mathbf{w} = (w_1, w_2)$$

两个目标函数分别为

$$f_1(\mathbf{w}) = -(3w_1 + 2w_2)$$

$$f_2(\mathbf{w}) = \sqrt{w_1^2 + w_2^2}$$

可行域为

$$\mathcal{W} = \{(w_1, w_2) \mid w_1 \geq 0, w_2 \geq 0\}$$

因此，完整数学表达式为

$$\begin{aligned} \min_{w_1, w_2} \quad & \left( -(3w_1 + 2w_2), \sqrt{w_1^2 + w_2^2} \right) \\ \text{s.t.} \quad & w_1 \geq 0, \\ & w_2 \geq 0 \end{aligned}$$

(b) 若要求模型准确度至少为 10, 由于实际准确度为

$$3w_1 + 2w_2$$

因此约束条件应为

$$3w_1 + 2w_2 \geq 10$$

等价地, 由于

$$f_1(\mathbf{w}) = -(3w_1 + 2w_2)$$

也可写成

$$f_1(\mathbf{w}) \leq -10$$

所以新的约束不等式为

$$3w_1 + 2w_2 \geq 10$$

(c) 现在需要满足以下全部约束:

$$w_1 \geq 0, \quad w_2 \geq 0, \quad 3w_1 + 2w_2 \geq 10$$

取两个不同的可行解。

先取

$$\mathbf{w}^{(1)} = (2, 2)$$

验证可行性:

$$3 \times 2 + 2 \times 2 = 6 + 4 = 10$$

满足约束。此时

$$f_2(\mathbf{w}^{(1)}) = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2}$$

再取

$$\mathbf{w}^{(2)} = (4, 0)$$

验证可行性:

$$3 \times 4 + 2 \times 0 = 12 \geq 10$$

也满足约束。此时

$$f_2(\mathbf{w}^{(2)}) = \sqrt{4^2 + 0^2} = 4$$

因此, 两个可行解及其对应的  $f_2$  值可写为

$$\mathbf{w}^{(1)} = (2, 2), \quad f_2(\mathbf{w}^{(1)}) = 2\sqrt{2}$$

$$\mathbf{w}^{(2)} = (4, 0), \quad f_2(\mathbf{w}^{(2)}) = 4$$