

第 6 章：无免费午餐定理

思考题 6.1

由题意，隐私泄露风险下界为

$$\epsilon_p \geq 0.35 - \frac{0.75}{100} \cdot \min \left(1, \sigma_\epsilon^2 \sqrt{\sum_{i=1}^2 \frac{1}{\sigma_i^4}} \right)$$

其中 σ_i^2 为第 i 个维度的参数方差。下面分别计算。

(a) 对于客户端 B，其参数方差为

$$\sigma_1^2 = 0.16^2, \quad \sigma_2^2 = 0.13^2$$

因此

$$\sqrt{\sum_{i=1}^2 \frac{1}{\sigma_i^4}} = \sqrt{\frac{1}{(0.16^2)^2} + \frac{1}{(0.13^2)^2}} \approx 70.90$$

当 $\sigma_\epsilon^2 = 0.06$ 时，

$$0.06 \times 70.90 \approx 4.25 > 1$$

所以

$$\min(1, 4.25) = 1$$

从而

$$\epsilon_p \geq 0.35 - \frac{0.75}{100} = 0.35 - 0.0075 = 0.3425$$

因此，客户端 B 对应的隐私泄露风险下界为

$$\epsilon_p \geq 0.3425$$

(b) 对于客户端 A，其参数方差为

$$\sigma_1^2 = 0.11^2, \quad \sigma_2^2 = 0.17^2$$

因此

$$\sqrt{\sum_{i=1}^2 \frac{1}{\sigma_i^4}} = \sqrt{\frac{1}{(0.11^2)^2} + \frac{1}{(0.17^2)^2}} \approx 89.60$$

当 $\sigma_\epsilon^2 = 0.08$ 时，

$$0.08 \times 89.60 \approx 7.17 > 1$$

所以

$$\min(1, 7.17) = 1$$

于是

$$\epsilon_p \geq 0.35 - \frac{0.75}{100} = 0.3425$$

因此，客户端 A 在 $\sigma_\epsilon^2 = 0.08$ 时的隐私泄露风险下界也是

$$\epsilon_p \geq 0.3425$$

与 (a) 比较可知，两者结果相同，均达到该公式下能够取得的最小下界。因此在该公式下，噪声从上一问的设置增大后，并未进一步降低该下界，隐私保护提升幅度为

$$0.3425 - 0.3425 = 0$$

即

提升幅度为0

(c) 对于客户端 C，其两个维度对应的标准差分别为 0.09 和 0.19，因此

$$\frac{1}{(0.09^2)^2} = \frac{1}{0.09^4} \approx 15241.58, \quad \frac{1}{(0.19^2)^2} = \frac{1}{0.19^4} \approx 766.84$$

可以看到，第二个维度由于方差较大，对

$$\sum_{i=1}^2 \frac{1}{\sigma_i^4}$$

的贡献明显更小。由于公式中的修正项为

$$\frac{0.75}{100} \cdot \min \left(1, \sigma_\epsilon^2 \sqrt{\sum_{i=1}^2 \frac{1}{\sigma_i^4}} \right),$$

当某一维度方差变大时， $\frac{1}{\sigma_i^4}$ 会减小，从而使整个根号项变小，最终使被减去的修正项变小，于是隐私泄露风险下界 ϵ_p 反而变大。

也就是说，参数方差越大，会使该公式中的“隐私保护补偿项”越弱，从而导致泄露风险下界更高。因此，客户端 C 第二个维度较大的方差会提高系统的隐私泄露风险。

思考题 6.2

给定效率损失下界：

$$\epsilon_e \geq 0.45 \times 2.1 \times \left(1 - \prod_{i=1}^{10} \rho_i \right) = 0.945 \left(1 - \prod_{i=1}^{10} \rho_i \right)$$

(a) 当所有维度 $\rho_i = 0.7$ 时,

$$\prod_{i=1}^{10} \rho_i = 0.7^{10} \approx 0.02825$$

因此

$$\epsilon_e \geq 0.945 \times (1 - 0.02825) = 0.945 \times 0.97175 \approx 0.918$$

故当前配置下

$$\epsilon_e \approx 0.918 > 0.4$$

不满足监管要求。

(b) 若所有维度取相同保留概率 ρ , 则

$$\prod_{i=1}^{10} \rho_i = \rho^{10}$$

监管要求

$$0.945(1 - \rho^{10}) \leq 0.4$$

化简得

$$1 - \rho^{10} \leq \frac{0.4}{0.945} \approx 0.4233$$
$$\rho^{10} \geq 0.5767$$

两边取 10 次方根:

$$\rho \geq (0.5767)^{1/10} \approx 0.946$$

因此最小保留概率为

$$\rho_{\min} \approx 0.946$$

(c) 新配置为: 前 3 维 $\rho = 0.8$, 后 7 维 $\rho = 0.6$, 则

$$\prod_{i=1}^{10} \rho_i = 0.8^3 \times 0.6^7$$

计算:

$$0.8^3 = 0.512, \quad 0.6^7 \approx 0.02799$$

$$\prod_{i=1}^{10} \rho_i \approx 0.512 \times 0.02799 \approx 0.0143$$

因此

$$\epsilon_e \geq 0.945(1 - 0.0143) = 0.945 \times 0.9857 \approx 0.931$$

由于

$$0.931 > 0.4$$

故该配置

不满足监管要求

原因在于: 后 7 个维度采用较低保留概率 0.6, 使整体乘积 $\prod \rho_i$ 非常小, 从而显著增大 $1 - \prod \rho_i$, 最终导致效率损失过高。

思考题 6.3

已知噪声方差函数为

$$\sigma_{\epsilon}^2(t) = 0.05 + 0.004t$$

隐私泄露下界为

$$\epsilon_p(t) \geq 0.32 - 0.007 \cdot \min \left(1, \sigma_{\epsilon}^2(t) \sqrt{\sum_{i=1}^3 \frac{1}{\sigma_i^4}} \right)$$

并要求满足隐私约束

$$\epsilon_p(t) \leq 0.25e^{-0.05t}$$

其中

$$\sigma_1 = 0.15, \quad \sigma_2 = 0.12, \quad \sigma_3 = 0.18$$

(a) 先计算常数项

$$\sum_{i=1}^3 \frac{1}{\sigma_i^4} = \frac{1}{0.15^4} + \frac{1}{0.12^4} + \frac{1}{0.18^4}$$

分别有

$$\frac{1}{0.15^4} = \frac{1}{0.00050625} \approx 1975.31$$

$$\frac{1}{0.12^4} = \frac{1}{0.00020736} \approx 4822.53$$

$$\frac{1}{0.18^4} = \frac{1}{0.00104976} \approx 952.60$$

因此

$$\sum_{i=1}^3 \frac{1}{\sigma_i^4} \approx 1975.31 + 4822.53 + 952.60 = 7750.44$$

从而

$$\sqrt{\sum_{i=1}^3 \frac{1}{\sigma_i^4}} \approx \sqrt{7750.44} \approx 88.04$$

于是

$$\sigma_{\epsilon}^2(t) \sqrt{\sum_{i=1}^3 \frac{1}{\sigma_i^4}} = (0.05 + 0.004t) \times 88.04$$

当

$$t = 0$$

时,

$$0.05 \times 88.04 = 4.402 > 1$$

因此对任意

$$t \geq 0$$

都有

$$(0.05 + 0.004t) \times 88.04 > 1$$

故

$$\min(1, (0.05 + 0.004t) \times 88.04) = 1$$

所以隐私泄露下界恒为

$$\epsilon_p(t) \geq 0.32 - 0.007 = 0.313$$

而隐私约束要求

$$\epsilon_p(t) \leq 0.25e^{-0.05t}$$

注意到

$$0.25e^{-0.05t} \leq 0.25, \quad \forall t \geq 0$$

但

$$\epsilon_p(t) \geq 0.313 > 0.25$$

因此从初始时刻开始就无法满足隐私约束，即不存在非负整数轮次满足要求。

故最大训练轮次为

$$t_{\max} = -1$$

即在当前噪声函数下，系统从第 0 轮开始就不满足隐私约束；若只考虑非负训练轮次个数，也可表述为

不存在满足约束的训练轮次

(b) 现在设计新的噪声增长函数 $\sigma_\epsilon^{2*}(t)$ ，使得

$$t_{\max} \geq 20$$

要使前 20 轮都满足约束，至少应保证在

$$t = 20$$

时仍有

$$\epsilon_p(20) \leq 0.25e^{-0.05 \cdot 20}$$

即

$$\epsilon_p(20) \leq \frac{0.25}{e} \approx 0.09197$$

但根据原公式，

$$\epsilon_p(t) \geq 0.32 - 0.007 \cdot \min(1, \dots)$$

又由于

$$\min(1, \dots) \leq 1$$

故可得到该下界的最小可能值为

$$0.32 - 0.007 = 0.313$$

也就是说，无论如何设计噪声函数，只要仍使用题目给出的这条隐私泄露公式，就总有

$$\epsilon_p(t) \geq 0.313$$

这显然不可能满足

$$\epsilon_p(20) \leq 0.09197$$

因此，仅通过修改噪声增长函数，无法实现

$$t_{\max} \geq 20$$

所以结论是：

在当前隐私泄露公式不变的情况下，不存在任何 $\sigma_\epsilon^{2*}(t)$ 可使 $t_{\max} \geq 20$

若希望达到

$$t_{\max} \geq 20$$

则必须同时修改隐私泄露公式中的常数项或噪声系数，例如将

$$\epsilon_p(t) \geq 0.32 - 0.007 \cdot \min(\dots)$$

改为更强的抑制形式，如

$$\epsilon_p^*(t) \geq 0.32 - \alpha \cdot \min \left(1, \sigma_\epsilon^{2*}(t) \sqrt{\sum_{i=1}^3 \frac{1}{\sigma_i^4}} \right)$$

并取更大的 α ，或者降低基准常数 0.32，否则单独增大噪声函数无法满足题目要求。

思考题 6.4

解：

已知逆频率加权策略为

$$w_k = \frac{1/p_k}{\sum_{i=1}^3 1/p_i}$$

其中

$$p_1 = 0.15, \quad p_2 = 0.25, \quad p_3 = 0.10$$

(a) 先计算各客户端的倒数频率：

$$\frac{1}{p_1} = \frac{1}{0.15} = 6.6667, \quad \frac{1}{p_2} = \frac{1}{0.25} = 4, \quad \frac{1}{p_3} = \frac{1}{0.10} = 10$$

因此分母为

$$\sum_{i=1}^3 \frac{1}{p_i} = 6.6667 + 4 + 10 = 20.6667$$

于是各客户端的归一化权重为

$$w_1 = \frac{6.6667}{20.6667} \approx 0.3226$$

$$w_2 = \frac{4}{20.6667} \approx 0.1935$$

$$w_3 = \frac{10}{20.6667} \approx 0.4839$$

故三者权重分别为

$$w_1 = 0.3226, \quad w_2 = 0.1935, \quad w_3 = 0.4839$$

(b) 当客户端 2 增加 500 个合成样本后，题目给定其目标类别占比变为

$$p'_2 = 0.18$$

此时新的倒数频率为

$$\frac{1}{p_1} = 6.6667, \quad \frac{1}{p'_2} = \frac{1}{0.18} \approx 5.5556, \quad \frac{1}{p_3} = 10$$

新的分母为

$$6.6667 + 5.5556 + 10 = 22.2223$$

因此更新后的权重为

$$w'_1 = \frac{6.6667}{22.2223} \approx 0.3000$$

$$w'_2 = \frac{5.5556}{22.2223} \approx 0.2500$$

$$w'_3 = \frac{10}{22.2223} \approx 0.4500$$

所以新权重分布为

$$w'_1 = 0.3000, \quad w'_2 = 0.2500, \quad w'_3 = 0.4500$$

与原来相比：

$$w_1 : 0.3226 \rightarrow 0.3000, \quad w_2 : 0.1935 \rightarrow 0.2500, \quad w_3 : 0.4839 \rightarrow 0.4500$$

可见，客户端 2 的权重明显上升，而客户端 1 和客户端 3 的权重有所下降。这是因为 p_2 从 0.25 降到 0.18 后， $\frac{1}{p_2}$ 变大，说明客户端 2 中目标类别变得更稀缺，因此逆频率加权机制会为其分配更大的聚合权重，以增强对少数类信息的补偿。

- (c) 下面说明该加权策略为何能够降低全局模型经验风险的上界。
 设客户端 k 上的经验风险为

$$\hat{R}_k(h) = \frac{1}{n_k} \sum_{j=1}^{n_k} \ell(h(x_{k,j}), y_{k,j})$$

其中 $\ell(\cdot, \cdot)$ 为损失函数。采用加权聚合后，全局经验风险可写为

$$\hat{R}_w(h) = \sum_{k=1}^3 w_k \hat{R}_k(h)$$

在类别不平衡场景下，若直接采用均匀加权或按样本量加权，则目标类别占比较低的客户端在全局目标中贡献偏小，导致模型更偏向多数类，从而使少数类误差较大。设少数类相关误差项与类别比例近似成反比，则可用如下形式刻画其上界：

$$\hat{R}(h) \leq \sum_{k=1}^3 \alpha_k \hat{R}_k(h), \quad \alpha_k \propto \frac{1}{p_k}$$

也就是说，当某客户端的目标类别越稀缺时，其对整体风险上界的影响实际上越大。如果仍然不给它足够权重，则全局经验风险会低估少数类带来的真实误差。

逆频率加权恰好取

$$w_k = \frac{1/p_k}{\sum_{i=1}^3 1/p_i}$$

因此

$$\hat{R}_w(h) = \sum_{k=1}^3 \frac{1/p_k}{\sum_{i=1}^3 1/p_i} \hat{R}_k(h)$$

它提高了少数类占比较低客户端的贡献，使加权后的经验风险对少数类误差更敏感，从而减弱了由类别不平衡造成的风险估计偏差。

进一步地，设每个客户端中目标类别的误差为 e_k^+ ，非目标类别误差为 e_k^- ，则客户端总体误差可写成

$$\hat{R}_k(h) = p_k e_k^+ + (1 - p_k) e_k^-$$

采用逆频率加权后，

$$w_k \hat{R}_k(h) = \frac{1/p_k}{\sum_{i=1}^3 1/p_i} (p_k e_k^+ + (1 - p_k) e_k^-)$$

即

$$w_k \hat{R}_k(h) = \frac{1}{\sum_{i=1}^3 1/p_i} \left(e_k^+ + \frac{1 - p_k}{p_k} e_k^- \right)$$

可以看到，少数类误差项 e_k^+ 得到了更直接的保留，而不是像普通平均那样被小的 p_k 稀释掉。因此，全局目标会更关注目标类别样本的错误，从而有助于压低由类别不平衡引起的经验风险上界。

因此，可以得出结论：**逆频率加权通过提升少数类占比较低客户端在聚合中的作用，减小了类别不平衡导致的风险估计偏差，从而能够降低全局模型经验风险的上界。**

不过更严格地说，这一结论成立依赖于一个合理前提：**全局风险上界中少数类误差确实是主要项，且其影响与 $1/p_k$ 同阶相关。**在这一常见不平衡学习假设下，逆频率加权是有效的。