

第 3 章：联邦大模型

思考题 3.1

(a) 上传方向采用 Top- k 压缩，仅传输 $k = 200$ 个非零元素的值与其索引：

$$\text{上传量} = \underbrace{200 \times 4}_{\text{元素值 (32 位)}} + \underbrace{200 \times 2}_{\text{索引 (16 位)}} = 800 + 400 = 1200 \text{ 字节}.$$

下载方向服务器返回完整梯度 ∇H ：

$$\text{下载量} = 1024 \times 4 = 4096 \text{ 字节}.$$

每轮双向通信总量为：

$$1200 + 4096 = 5296 \text{ 字节} \approx 5.17 \text{ KB}.$$

相比未压缩时的 8 KB，通信量降低了约 35%。

(b) 500 轮的上传总数据量为：

$$1200 \times 500 = 600,000 \text{ 字节} = 4.8 \times 10^6 \text{ bit} = 4.8 \text{ Mbit}.$$

网络带宽为 10 Mbps，因此上传总耗时为：

$$t = \frac{4.8 \text{ Mbit}}{10 \text{ Mbps}} = 0.48 \text{ 秒}.$$

这一结果直观地说明了稀疏压缩的优势：仅保留约 19.5% 的原始维度，便将上传通信开销压缩至不足半秒。

(c) 添加拉普拉斯噪声本身不改变向量维度，因此若直接在完整 H 上加噪后再进行 Top- k 压缩，通信格式不变，通信开销理论上维持不变。

然而实践中会出现以下两种情形，可能间接影响通信成本：

- **压缩效率下降。** 噪声会打乱原始元素的幅值分布，使得 Top- k 所筛选的元素不再集中于真正重要的梯度方向，导致相同压缩率下信息损失更大，需要适当增大 k 以维持模型精度，从而提高上传量。
- **迭代轮次增加。** 噪声引入额外扰动，模型收敛速度通常变慢，训练所需总轮数增加，进而推高整体通信总量。

综上，添加拉普拉斯噪声**不会直接增加单轮通信量**，但会通过压缩效率与收敛速度两条路径**间接提高整体训练的通信开销**，隐私保护与通信效率之间存在一定的权衡关系。

思考题 3.2

各客户端样本数依次为 $n_1 = 500, n_2 = 1000, n_3 = 250, n_4 = 750, n_5 = 1500$ ，总样本数：

$$N = 500 + 1000 + 250 + 750 + 1500 = 4000.$$

每个样本的 logits 向量双向传输（上传本地 logits + 下载教师 logits）的单条通信量为：

$$2 \times 10 \times 4 = 80 \text{ 字节}.$$

(a) 每轮各客户端上传 20% 样本的 logits，总参与样本数为：

$$0.2 \times N = 0.2 \times 4000 = 800 \text{ 条}.$$

服务器每轮双向（收发）总传输量为：

$$800 \times 80 = 64,000 \text{ 字节} = 62.5 \text{ KB}.$$

(b) 若全样本蒸馏，每轮传输量为：

$$4000 \times 80 = 320,000 \text{ 字节} = 312.5 \text{ KB}.$$

采用 20% 采样后，传输量恰好减少为原来的 20%，即**减少了** 80%：

$$1 - \frac{62.5}{312.5} = 1 - 0.2 = 80\%.$$

(c) 按数据量比例分配聚合权重，客户端 3 的权重为：

$$w_3 = \frac{n_3}{N} = \frac{250}{4000} = 0.0625.$$

客户端 3 的数据量仅占全局的 6.25%，在模型聚合中影响力较弱。

(d) 从**蒸馏效果**来看，数据量大的客户端（如客户端 5，占比 37.5%）在聚合时主导全局模型更新方向，而数据量少的客户端（如客户端 3，占比 6.25%）贡献的知识被显著稀释。若各客户端数据分布存在差异（Non-IID），全局模型可能对少数数据客户端的任务表现欠佳，带来公平性问题。

从**通信开销**来看，每轮按固定比例（20%）采样时，大客户端上传的 logits 绝对数量更多（如客户端 5 每轮上传 300 条，客户端 3 仅上传 50 条），网络负载集中于少数大客户端，可能成为训练速度的瓶颈。一种缓解方法是对各客户端设置绝对上限，或根据数据量反向调整采样率，适当增加小客户端的参与比例以改善公平性。

思考题 3.3

(a) 对于 FedAvg 的单轮通信开销，每个客户端需上传并下载完整参数向量 (共 $2d$ 个浮点数)：

$$\text{单客户端} = 2d \times 4 = 2 \times 10^6 \times 4 = 8 \times 10^6 \text{ 字节} = 8 \text{ MB.}$$

$n = 10$ 个客户端合计：

$$C_{\text{FedAvg}} = 10 \times 8 \text{ MB} = 80 \text{ MB.}$$

(b) 对于 DeComFL 的单轮通信开销，每个客户端仅上传 $c = 2$ 个标量，并下载 $c = 2$ 个标量：

$$\text{单客户端} = 2c \times 4 = 2 \times 2 \times 4 = 16 \text{ 字节.}$$

$n = 10$ 个客户端合计：

$$C_{\text{DeComFL}} = 10 \times 16 = 160 \text{ 字节} \approx 0.000153 \text{ MB.}$$

则通信节省倍数为

$$\frac{C_{\text{FedAvg}}}{C_{\text{DeComFL}}} = \frac{80 \times 10^6 \text{ 字节}}{160 \text{ 字节}} = 5 \times 10^5 \text{ 倍.}$$

DeComFL 相较于 FedAvg 每轮节省了约 **50 万倍** 的通信量。这一巨大差距来源于零阶优化的核心思想：通过随机扰动方向上的损失差分来估计梯度方向，无需传输高维参数向量，将通信复杂度从 $\mathcal{O}(d)$ 压缩至 $\mathcal{O}(1)$ 。其代价是梯度估计的方差较大，通常需要更多的本地迭代或更精细的扰动设计来保证收敛。

思考题 3.4

激活向量维度 $h = 4096$ ，32 位浮点（4 字节/元素），梯度稀疏化保留比例 $k = 10\%$ ，即保留 $\lfloor 0.1 \times 4096 \rfloor = 410$ 个条目，索引用 16 位整数（2 字节）表示。

(a) 前向传输激活 H 与反向传输梯度 ∇H 各占 $h \times 4$ 字节：

$$C_{\text{原始}} = 2 \times 4096 \times 4 = 32,768 \text{ 字节} = 32 \text{ KB.}$$

(b) 前向激活 H 仍完整传输（未压缩），反向梯度 ∇H 采用稀疏化传输：

$$\begin{aligned} \text{前向（完整）} &= 4096 \times 4 = 16,384 \text{ 字节,} \\ \text{反向值（} k = 410 \text{ 项）} &= 410 \times 4 = 1,640 \text{ 字节,} \\ \text{反向索引（} k = 410 \text{ 项）} &= 410 \times 2 = 820 \text{ 字节.} \end{aligned}$$

单样本总通信量：

$$C_{\text{GS}} = 16,384 + 1,640 + 820 = 18,844 \text{ 字节} \approx 18.4 \text{ KB.}$$

(c) 原始批次总量：

$$256 \times 32,768 = 8,388,608 \text{ 字节} = 8,192 \text{ KB.}$$

稀疏化后批次总量：

$$256 \times 18,844 = 4,824,064 \text{ 字节} \approx 4,711 \text{ KB.}$$

通信量减少比例：

$$1 - \frac{4,824,064}{8,388,608} = 1 - \frac{18,844}{32,768} \approx 1 - 0.575 = 42.5\%.$$

减少幅度约为 42.5%，主要节省来自反向梯度的稀疏化传输。值得注意的是，前向激活 H 若同样进行压缩（如结合 Top- k 或量化），通信量还可进一步降低；但在本题设定中前向激活为完整传输，这也是实际系统中常见的非对称压缩策略——重点压缩噪声较多的梯度方向，保留前向激活的完整性以维持预测精度。