分布偏移下伪校准共形预测的覆盖率保证

Farbod Sia hkali，*IEEE*会员，Ashwin Verma，*IEEE*会员，Vijay Gupta，*IEEE*会士

arXiv:2602.14913v1 [cs.LG] 16 Feb 2026

摘要——**保形预测（CP）在可交换性假设下提供无分布假设的边际覆盖率保证，但若数据分布发生偏移，这些保证可能失效。我们分析了在有界标签条件协变量偏移模型下，使用伪校准来弥补这一性能损失的效果。借助域适应工具，我们推导出目标覆盖率的下界，该下界由分类器的源域损失和衡量分布偏移的Wasserstein度量共同确定。基于这一结果，我们提出一种设计伪校准预测集的方法：通过松弛参数增大保形阈值，使目标覆盖率保持在预设水平以上。最后，我们提出一种源域调优伪校准算法，该算法根据分类器不确定性，在硬伪标签与随机化标签之间进行插值。数值实验表明，我们的界限在定性上能够反映伪校准的行为；同时，源域调优方案在保持预测集大小非平凡的情况下，减轻了分布偏移造成的覆盖率下降。**

I. 引言

CONFORMAL预测（CP）提供了一个严格的框架，用于在校准数据与测试数据之间的可交换性假设下构建具有边际覆盖率保证的预测集 [1], [2]。CP已被应用于多种场景 [3], [4], [5]。然而，CP的有限样本、分布无关保证依赖于可交换性 [6]，而由于源域（校准）与目标域（测试）之间的分布偏移，该假设常常被违反 [7], [8], [9]–[10]。若可获得目标域标签，一种纠正此类覆盖不足的方法是采用加权共形预测，即利用源域与目标域在输入空间上的边缘分布之间的估计密度比，对校准分数进行重要性加权 [2], [9]。或者，稳健分布方法围绕分数分布构造模糊集（如L´evy-Prokhorov球），并将最坏情况下的扰动通过分数空间中的共形分位数进行传播 [11]。

当目标域标签不可用时，一种可能的做法是利用源分类器的伪标签。然而，伪标签会引入额外的不确定性，从而可能降低覆盖率。近期一些工作试图通过利用预测熵或重构损失 [12], [13]对分数进行启发式重缩放来缓解这一问题；然而，这些方法并不能给出解析的覆盖率保证。另一种做法是， [14]利用分数分布距离为带伪标签的目标提供界。然而，由于这些界并不依赖于底层分类器或分布偏移特性，它们并不能为设计分类器或伪校准方案以权衡覆盖率与集合大小提供洞见。

这些局限性指向一个更广泛的缺口：现有的分布偏移下的保形预测方法并未考虑源域误差如何转化到目标域。领域自适应理论为这一问题提供了一个自然视角，即通过源域损失和分布偏移度量来界定目标误差 [15], [16]。然而，这些思想尚未被纳入分布偏移下的保形预测，使得分布偏移下无标签多分类保形预测的分析性理解仍不充分。

我们的工作通过借鉴领域自适应理论来弥合这一缺口，推导出明确依赖于分类器性质和分布偏移度量的覆盖率保证。我们将这些工具扩展到多分类，并根据源分类器的损失以及源分布与目标分布之间的Wasserstein距离，得到目标域上伪校准的界。受 [17], 启发，我们进一步提出一种源域调优的伪校准算法，该算法基于分类器不确定性在硬伪标签与随机化标签之间进行插值，从而在保持源域覆盖率的同时降低标准伪校准的保守性。

据我们所知，这是首次将分布自适应理论与分布偏移下的保形覆盖率分析相结合。我们的贡献总结如下。首先，我们根据分类器的源域损失、分类器的利普希茨性质以及分布偏移的 Wasserstein 度量，推导出目标域上伪校准预测集的覆盖率下界。其次，我们提出宽松伪校准集合，通过松弛参数增大保形阈值，并给出简单的设计规则，用于选择该松弛参数以保证所需的目标覆盖率。最后，我们提出一种源域调优伪校准算法，根据分类器不确定性，在硬伪标签和随机化标签之间进行插值。实验表明，我们的理论界与经验行为一致，且所提出的算法在维持非平凡期望集合大小的同时，减轻了目标域上的覆盖下降。

II. 背景与问题公式TION

a) 保形预测：保形预测构造预测集，并提供有限样本边际覆盖率保证 [18]。给定校准数据 $\{(X_i, Y_i)\}_{i=1}^{n}$ 独立同分布$\sim$ P_{XY}以及一个测试点 (X_{n+1}, Y_{n+1})，目标是确保

$$\Pr\{Y_{n+1} \in C_P^{1-\alpha}(X_{n+1})\} \geq 1 - \alpha, \tag{1}$$

对于任意 $\alpha \in (0,1)$，在校准与测试点之间的可交换性假设下，即它们的联合分-

本研究部分得到美国陆军研究办公室资助，资助编号为13001664。作者任职于普渡大学埃尔莫尔电气与计算机工程学院，地址为美国印第安纳州西拉法叶47907（电子邮件： {siahkali,verma240,gupta869}@purdue.edu）。

布在置换下不变 [18, 第 3] 节。设 $s:\ \mathcal{X}\times\mathcal{Y}\to\mathbb{R}$ 为非一致性分数。对于 $\mathcal{X}\times\mathcal{Y}$, 上的分布 P，将推前分数分布记为 $s\#P$，其累积分布函数为 $F_{s\#P}$。对于 $\alpha\in(0,1),$，将 $(1-\alpha)$-分位数定义为 $\inf\{t\in\mathbb{R}:\ F_{s\#P}(t)\ \geq 1-\alpha\}$。利用经验分布 $\hat{P}_n=\frac{1}{n}\sum_{i=1}^{n}\delta_{(X_i,Y_i)}$，在 α 处的分割保形阈值为

$$q_{P,\alpha}:=\mathrm{Quantile}\left(\frac{\lceil(1-\alpha)(n+1)\rceil}{n};s\#\hat{P}_n\right),\qquad(2)$$

且保形预测集定义为

$$C_P^{1-\alpha}(x)=\{y\in\mathcal{Y}:s(x,y)\leq q_{P,\alpha}\}.$$

在可交换性假设下，这一构造保证 (1) [19,定理 1.1]。然而，当测试数据来自一个不同于校准分布 P_{XY} 的联合分布 Q_{XY} 时，如果阈值是根据 $s\#P_{XY}$ 计算的，而测试分数服从 $s\#Q_{XY}$，覆盖率可能会下降。

b) 分布偏移度量：为量化输入分布的偏移，我们使用 Wasserstein距离。本文假设所考虑的所有概率测度都支撑在度量空间 $(\mathbb{R}^d,\|\cdot\|_2)$ 上。

定义 *1*：对于 $p\geq1$ 以及定义在 $\mathcal{X}$ 上的概率测度 P 和 Q, p-Wasserstein距离为

$$W_p(P,Q):=\left(\inf_{\pi\in\Pi(P,Q)}\mathbb{E}_{(X,X')\sim\pi}\left[\|X-X'\|_2^p\right]\right)^{1/p},$$

其中 $\Pi(P,Q)$ 是 P,Q 的所有耦合集合。对于 $p=\infty$，我们定义 $W_\infty(P,Q)=\inf_{\pi\in\Pi(P,Q)}\operatorname{ess\,sup}_{(X,X')\sim\pi}\|X-X'\|_2$.

c) 所考虑的问题：我们考虑一个多类分类问题，其输入空间为 $\mathcal{X}=\mathbb{R}^d$，标签空间为$\mathcal{Y}=[K]:=\{1,\ldots,K\}$。源域和目标域分别由定义在$\mathcal{X}\times\mathcal{Y}$上的联合分布 P_{XY} 和 Q_{XY} 表示。分类器 $f:\ \mathcal{X}\to\mathcal{Y}$ 由逻辑值映射$M_f:\ \mathcal{X}\to\mathbb{R}^K$诱导，该映射返回类别逻辑值向量。预测标签定义为

$$f(x):=\arg\max_{k\in[K]}M_f(x)_k.\qquad(3)$$

对于带标签样本 (x,y)，定义多类间隔，用以衡量真实类别的逻辑值超过最大竞争类别逻辑值的幅度：$\gamma_f(x,y):=M_f(x)_y-\max_{k\neq y}M_f(x)_k$. 为界定分布偏移下的错误，我们采用如下定义的坡形损失：$\ell_r((x,y);f):=r(\gamma_f(x,y))$，其中 $r(t):=\min\{\max(1-t,0),1\}$ 是斜坡函数，它将替代损失截断至区间$[0,1]$。分布 P_{XY} 下的总体斜坡损失为$L_r(f,P):=\mathbb{E}_{P_{XY}}[\ell_r((X,Y);f)]$.。我们还将使用合页损失 $\ell_h((x,y);f):=\max\{1-\gamma_f(x,y),0\}$，其在 P_{XY}下的总体合页损失定义为 $L_h(f,P):=\mathbb{E}_{(X,Y)\sim P_{XY}}[\ell_h((X,Y);f)]$。

假设*1*：对所有 $x,\ x'\in\mathcal{X}$和 $y\in[K],\ \gamma_f(\cdot,\cdot)$ 满足

$$|\gamma_f(x,y)-\gamma_f(x',y)|\leq L_\gamma\|x-x'\|_2.$$

在我们的设定中，f 是一个预训练分类器，其在留出的源域验证数据上的 $L_r(f,\ P)$已知或可估计。一旦 f 固定后，L_γ 可利用谱范数界给出上界，也可通过观测到的源域样本附近的数据依赖型局部梯度范数界进行估计。我们仅能获得无标签目标域输入 $X\sim Q_X$。因此，我们构造确定性的伪标签$\tilde{}$：$Y=f(X)$，由此得到伪标签标注的$\tilde{}$联合分布 Q_{XY} 及相应的分数分布$\tilde{}s\#Q_{XY}$。本文中，我们始终使用非一致性分数 $s(x,y):=-\gamma_f(x,y)$。根据式 (3) 中 f的定义，对于任意 $x\in\mathcal{X}$和 $y\neq f(x)$，有 $\gamma_f(x,f(x))\geq0$且$\gamma_f(x,y)\leq0$.因此，$s(x,f(x))\leq s(x,y)$。由此可见，在伪标签标注下，预测标签的分数始终小于或等于同一x下任意其他标签的分数。这进而意味着，对于$(X,Y)\sim Q_{XY}$，几乎必然有$s(X,f(X))\leq s(X,Y)$。因此，

$$F_{s\#\tilde{Q}}(t)\geq F_{s\#Q}(t),\qquad(4)$$

对所有 $t\in\mathbb{R}$ 均成立。等价地，对每个$\alpha\in(0,\ 1)$，$q_{\tilde{Q},\ \alpha}\leq q_{Q,\ \alpha}$。因此，与使用真实标签的预言机校准相比，伪校准往往采用更小的阈值，因而在目标域上生成更小的预测集。我们还将作出以下假设。

假设*2*：分布 P_{XY}和 Q_{XY} 满足：

(*i*) 边缘分布相同：$P_Y=Q_Y$。(*ii*) 有界条件偏移：对于某个 $\rho>0$，我们有 $\sup_{y\in\mathcal{Y}}W_\infty(P_{X|y},\ Q_{X|y})<\rho.$

假设2(i)是域适应分析中用于隔离标签条件协变量偏移的标准假设（例如 [15]）。假设2(ii)在扰动受到物理约束的感知/控制流程中是自然的；在此类情形下，ρ 被视为先验规格参数（例如，依据已知的环境/传感器动力学，如有界漂移/噪声）。在假设2下，对于所有，我们还有 $W_1(P_{X|y},Q_{X|y})\leq\rho$ y $W_1(P_X,Q_X)\leq(,)$，$\rho_{\mathrm{mix}}=\sum_{y=1}^{K}P_Y\ y\ W_1(P_{X|y},Q_{X|y})\leq\rho$ 因此 $(,):()(,)$。

III. 分析结果

现在，我们给出分布偏移下覆盖率差距的上界；所有证明均推迟至补充材料中。请注意，ρ 和 L_γ 仅出现在以下界中，所提出的程序并不需要它们。根据假设1，对于任意 $y\in[K]$，分数函数 $s(x,\ y)$关于 x是 L_γ-利普希茨的。对于给定的水平 $\alpha\in(0,\ 1)$，令$q_{P,\ \alpha}$ 表示根据式(2)中 $s\#P_n$计算得到的经验分割保形阈值。使用该阈值，目标分布 Q下的实际覆盖率为 $F_{s\#Q}(q_{P,\ \alpha})$，而P下的覆盖率为 $F_{s\#P}(q_{P,\ \alpha})\approx1-\alpha$。定义逐点覆盖率差距

$$\Delta_{P,Q}(\alpha):=\left|F_{s\#P}(q_{P,\alpha})-F_{s\#Q}(q_{P,\alpha})\right|.$$

根据 [10],，我们可以通过$\Delta_{P,\ Q}:=\int_0^1\Delta_{P,\ Q}(\alpha)\,d\alpha$ 汇总所有名义水平上的这些差异，以衡量在P 上进行校准、但在 Q上部署时产生的平均覆盖率失配。

A. 分布偏移下的覆盖率差距上界

我们的第一个结果给出了原始分数分布与分布偏移后的分数分布之间的 Wasserstein距离上界。

引理 *1*：在假设 1 和 2 下，我们有

$$W_1(s\#P, s\#Q) \le L_\gamma \rho.$$

对于使用来自 P_{XY} 的带标签数据进行源校准的情形，我们采用 [10,定理 3.2]给出的通用覆盖差距界：

$$\Delta_{P,Q} \le \Big(\sup_{t\in\mathbb{R}} p_{s\#P}(t)\Big) W_1(s\#P, s\#Q), \tag{5}$$

其中 $p_{s\#P}$ 表示 $s\#P$ 的概率密度函数（若存在）。结合式 (5) 与引理 1，可得 $\Delta_{P,\ Q} \le (\sup_{t\in\mathbb{R}} p_{s\#P}(t)) L_\gamma \rho$，该式根据分数密度、间隔的 Lipschitz 常数和偏移幅度，量化了使用源数据计算保形阈值时覆盖率可能出现的最坏情况退化。

~对于在 Q 上进行伪校准，分数服从 $s\#Q_{XY}$，而测试分数服从 $s\#Q_{XY}$。我们有如下结果。

.定理 *1*：设假设 1 和 2 成立。令 $X_1, \ldots, X_n$ $\overset{\text{i.i.d.}}{\sim}$ Q_X，并定义伪标签 $\tilde{Y}_i = f(X_i)$，$(X_i, \tilde{Y}_i) \sim \tilde{Q}_{XY}$，$(X_{n+1}, Y_{n+1}) \sim Q_{XY}$，$\alpha \in (0,1)$，$(X_{n+1}, Y_{n+1})$ 独立同分布于 $(X_i, Y_i)_{i=1}^n$，并定义伪标签 $\tilde{Y}_i = f(X_i)$，使得 $(X_i, \tilde{Y}_i) \sim \tilde{Q}_{XY}$。令 $q_{\tilde{Q},\alpha}$ 为根据伪分数 $\{s(X_i, Y_i)\}_{i=1}^n$ 计算得到的 $(1-\alpha)$ 分制保形阈值，并定义伪校准预测集

$$C^{1-\alpha}_{\tilde{Q}}(X_{n+1}) := \big\{y \in [K] : s(X_{n+1}, y) \le q_{\tilde{Q},\alpha}\big\}.$$

则目标域上的边际覆盖率满足

$$Q_{XY}\big(Y_{n+1} \in C^{1-\alpha}_{\tilde{Q}}(X_{n+1})\big) \ge 1 - \alpha - L_r(f,P) - L_\gamma \rho_{\text{mix}}, \tag{6}$$

当右侧变为负数时，将其截断为 0。换言之，$\Delta_{\tilde{Q},Q} \le L_r(f, Q) \le L_r(f,P) + L_\gamma \rho_{\text{mix}}$.

注意，当 $P_Y \ne Q_Y$ 时，该结果可通过在边缘分布之间增加一项全变差距离来放宽。该结果表明，硬伪校准保形集仍保留有意义的覆盖率保证，该保证由源坡道损失和分布偏移的幅度所控制。以下推论为放宽的保形集 $(C^{1-\alpha}_{\tilde{Q}}$ 给出了一个显式的依赖于 (τ) 的下界 $_{,\tau})$，该下界通过合页损失得到。

推论*1*：设假设 1 和 2 成立。对任意 $\tau \ge 0$，定义放宽的预测集

$$C^{1-\alpha}_{\tilde{Q},\tau}(X_{n+1}) := \big\{y \in [K] : s(X_{n+1}, y) \le q_{\tilde{Q},\alpha} + \tau\big\}.$$

则目标域上的边际覆盖率满足

$$Q_{XY}\big(Y_{n+1} \in C^{1-\alpha}_{\tilde{Q},\tau}(X_{n+1})\big) \ge 1 - \alpha - \min\left\{L_r(f,Q), \frac{L_h(f,Q)}{1+\tau/2}\right\}. \tag{7}$$

B. 源调优伪校准

由 (4) 可知，伪标签标注在分数空间中具有悲观性。具体而言，它倾向于产生较小的分位数阈值，因而得到较小的预测集，这往往会导致相较于使用真实标签进行校准时出现欠覆盖。为缓解这种悲观性，我们以依赖于数据的方式在伪标签和随机标签之间进行插值。

给定一个函数 $H : \mathcal{X} \to \mathbb{R}_{\ge 0}$，用于度量某种不确定性概念（例如预测熵），当 $H(x)$ 较小时，我们依赖伪标签，否则进行随机化。给定阈值 $u \in \mathcal{U}$，对 $x \in \mathcal{X}$ 定义如下量

$$\tilde{Y}_u(x) = f(x)\mathbb{1}\{H(x) \le u\} + U\mathbb{1}\{H(x) > u\}, \tag{8}$$

算法 1 源调优伪校准

要求： 源数据 $\{(X_i^P, Y_i^P)\}_{i=1}^m$ $\sim$ P_{XY}；无标签目标数据 $\{X_j^Q\}_{j=1}^n \sim Q_X$；分类器 f；不确定性 H： $\mathcal{X} \to \mathbb{R}_{\ge 0}$；分数 s： $\mathcal{X} \times \mathcal{Y} \to \mathbb{R}$；水平 α。

1：对于每个 X_i^P，按式 (8) 计算 $\tilde{Y}_u(X_i^P)$，并相应地——得到伪分数 $S_i^u := s(X_i^P, \tilde{Y}_u(X_i^P))$。

2：令 $q_{\tilde{P}^u,\alpha}$ 为经验（$1-\alpha$）分位数 e of $\{S_i^u\}_{i=1}^m$，并定义经验源覆盖率和阈值

$$\hat{c}(u) := \frac{1}{m}\sum_{i=1}^m \mathbb{1}\{s(X_i^P, Y_i^P) \le q_{\tilde{P}^u,\alpha}\}.$$

$$u^\star = \max\big\{u \in \mathcal{U} : \hat{c}(u) \ge 1-\alpha\big\}.$$

3：对目标点伪标签 $\{\tilde{Y}_{u^\star}(X_j^Q)\}_{j=1}^n$，然后计算目标分数 $\{S_j^{Q,u^\star} := s(X_j^Q, \tilde{Y}_{u^\star}(X_j^Q))\}_{j=1}^n$。4：令 $q_{\tilde{Q}^{u^\star},\alpha}$ 为 $\{S_j^{Q,u^\star}\}_{j=1}^n$ 的 $(1-\alpha)$ 分位数。5：**返回** 阈值 $q_{\tilde{Q}^{u^\star},\alpha}$。

其中 $U \sim$ 服从均匀分布 Unif($[K]$)， $\mathbb{1}\{\cdot\}$ 是指示函数。~令 P^u_{XY} 和 Q^u_{XY} 分别表示由 Y_u 诱导的随机化伪标记~源联合分布和目标联合分布，并令~ ~$s\#P^u$ 和 $s\#Q^u$ 分别表示它们对应的分数分布。由于 $f(x)$使 $s(x,\ y)$ 在 $y \in [K]$上达到最小值，随机化只会增大分数。因此，对于每个 x 以及 $Y_u(x)$ 的每种~ ~实现，都有 $s(x,\ Y_u(x)) \ge s(x,\ f(x))$。因此，对于名义水平 $1-\alpha$，由 Q^u_{XY} 计算得到的保形阈值~ ~绝不会小于在 Q_{XY}下得到的阈值，且预测集绝不会更保守程度更低。

我们通过遍历网格$\mathcal{U}$.，在带标签源数据上调节 u。对于每个 $u \in \mathcal{U}$，我们使用混合伪标记分数 $\{s(X_i^P,\ \tilde{Y}_u(X_i^P))\}_{i=1}^m$计算分割保形阈值。接着，我们选择使经验源覆盖率 $\hat{}$ $c(u)$保持在 $1-\alpha$以上的 $u^\star$ 。固定该 $u^\star$ 后，我们对目标校准样本 $\{X_j^Q\}_{j=1}^n$ 进行伪标记，并根据分数 $\{s(X_j^Q,\ \tilde{Y}_{u^\star}(X_j^Q))\}_{j=1}^n$计算最终阈值。整体流程总结于算法 1。以下结果表明，对于任意固定的 u，与硬伪校准相比，该方案不会降低目标覆盖率。

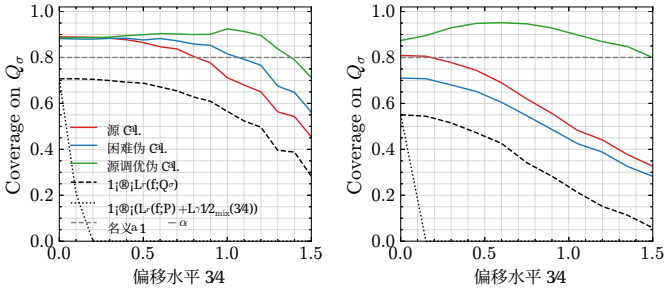
定理 *2*：对于任意具有边缘分布 Q_X的联合分布 Q_{XY} ，基于分数~$s(X, Y_u(X))$的分割共形预测器所达到的目标覆盖率至少与同一水平 $1-\alpha$下的硬伪校准一样大。

IV. 数值实验

我们在 MNIST、CIFAR-10 和 CIFAR-100 上评估所提出的界限和校准方案。原始数据集分布作为 P。目标分布 Q_σ 是通过对输入应用随机图像变换 T_σ 得到的，该变换包括外观变化以及强度为 σ 的截断高斯噪声，符合假设 2(ii)中的有界偏移假设。对于每个数据集，我们在源训练集划分上训练一个固定分类器 f ，并构建校准集和测试集划分 $\mathcal{D}^P_{\text{cal}}$ 和 $\mathcal{D}^P_{\text{tst}}$。相应的目标数据集划分 $\mathcal{D}^{Q_\sigma}$校准集 和 $\mathcal{D}^{Q_\sigma}$测试集 则通过对 $\mathcal{D}^P_{\text{cal}}$ 和 $\mathcal{D}^P_{\text{tst}}$ 中的输入应用 T_σ 得到。我们采用分割共形预测，

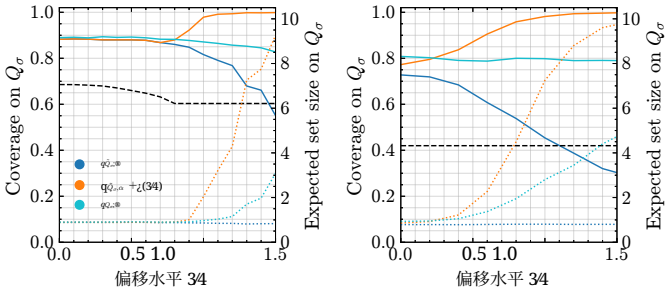
表I：覆盖率和期望集合大小（ESS）随偏移水平 σ （名义值 $1-\alpha=0.8$）的变化。粗体表示每行中最佳的非预言机方法：在覆盖率 $\geq 1-\alpha$ 的方法中，ESS 最小者；若不存在满足条件的方法，则为覆盖率最高者。

数据集	σ	源校准		硬伪校准		源调优伪校准		目标校准（预言机）	
		Cov	ESS	Cov	ESS	Cov	ESS	Cov	ESS
MNIST	0.70	**0.837**	**0.84**	0.871	0.88	0.903	0.93	0.892	0.91
	1.60	0.440	0.55	0.539	0.83	**0.718**	**1.87**	0.834	3.32
	2.00	0.276	0.50	0.347	0.82	**0.437**	**1.22**	0.813	5.45
CIFAR-10	0.45	0.727	0.97	0.647	0.80	**0.935**	**2.12**	0.801	1.18
	1.05	0.481	0.95	0.437	0.80	**0.879**	**4.32**	0.794	3.05
	1.50	0.329	0.94	0.299	0.80	**0.777**	**4.83**	0.808	5.03
CIFAR-100	0.30	0.755	2.46	0.533	0.79	**0.954**	**18.80**	0.813	3.54
	0.50	0.680	2.79	0.458	0.81	**0.937**	**31.95**	0.809	6.16
	0.70	0.596	2.92	0.381	0.81	**0.901**	**39.22**	0.797	9.83



(a) MNIST (b) CIFAR-10

图 1：源校准、硬伪校准和源调优伪校准的覆盖率随 Q_σ 和分布偏移 σ 的变化。虚线表示定理 1 的覆盖率下界。



(a) MNIST (b) CIFAR-10

图 2： Q_σ 的覆盖率（实线，左轴）和 ESS（虚线，右轴）随分布偏移的变化。颜色表示不同方法：硬伪校准 $\tilde{q}_{Q_\sigma,\ \alpha}$、 τ 调整后的 $\tilde{q}_{Q_\sigma,\ \alpha}+\tau(\sigma)$ 以及预言机 $q_{Q_\sigma,\ \alpha}$。黑色曲线表示合页损失下界。增加 τ可维持覆盖率下界，但代价是 ESS 增大。

名义失覆盖率为 $\alpha=0.2$ ，并将预测熵作为不确定性函数 H。我们比较了 Q_σ 上的三种校准策略：**源校准**（使用真实标签对来自 P 的样本进行校准）、**硬伪校准**（使用 Y 对来自 Q_σ 的样本进行伪校准），以及**源调优伪校准**（算法 1）。

表I报告了所有数据集和偏移级别下的经验覆盖率与期望集合大小（ESS）。在所有数据集上，随着 σ 增加，源校准和硬伪校准的欠覆盖现象日益严重。然而，与源校准/硬伪校准相比，源域调优方案提高了覆盖率，并且通常接近预言机，尤其是在中等分布偏移下（特别是在 CIFAR-10 上）。在 CIFAR-100 上，源校准和硬伪校准在大幅分布偏移下都存在严重欠覆盖，而源域调优方法则以增大 ESS 为代价恢复了覆盖率。目标域校准（预言机）使用目标域标签，并作为性能上界报告。

为将这些观察与我们的理论结果联系起来，我们评估定理1所蕴含的覆盖率下界。对于 MNIST 和 CIFAR-10，我们利用来自 Q_σ 的样本的预言机标签估计坡形损失$L_\tau(f, Q_\sigma)$，并计算相应的下界（使用 $\tau=0$）。图1绘出了源校准、硬伪校准和源调优伪校准在 Q_σ 上的经验覆盖率随 σ变化的情况，同时展示了理论界和名义水平。尽管这些界较为保守，但它们反映了分布偏移增大时覆盖率下降的定性趋势，并且在整个 σ范围内始终低于硬伪校准的经验覆盖率。

我们使用源域校准的覆盖不足修正来选择 $\tau(\sigma)$。首先，我们通过使用伪标签Y而非 Y进行校准，量化 P 上的硬伪校准欠覆盖差距。我们得到硬伪校准预测集 $C_{P0}^{1-\alpha}$，(x)，并定义 $\Delta_P:=(1-\alpha)-P\left(Y\in C_{P,0}^{1-\alpha}(X)\right)$。接下来，对于每个偏移水平 σ，在给定 $L_h(f,P)$ 和 $L_h(f,Q_\sigma)$ 的情况下（不揭示目标标签，例如通过 DA 得到一个界，或使用代理估计量），根据推论1，我们通过令式（7）匹配源域下界加上该差距，求解 $\tau(\sigma)$：$\tau(\sigma)=2\left(\frac{L_h}{L_h}(f,Q_\sigma)\,(f,P)-\Delta_P-1\right)\cdot$。随后，我们使用放宽后的阈值 $q_{\tilde{Q}_\sigma,\alpha}+\tau(\sigma)$ 在 Q_σ上构造预测集，并报告覆盖率和 ESS。如图2所示，未经调整的伪校准会随着分布偏移增大而下降，而调整方案能够维持覆盖率，但代价是 ESS 增大。

V. 结论

我们研究了目标域标签不可用时分布偏移下的共形预测。借鉴域适应的思想，我们推导出覆盖率下界，明确揭示了目标域覆盖率与分类器属性及分布偏移度量之间的联系。在此基础上，我们提出了一种源域调优伪校准方案，利用不确定性度量在硬伪标签和随机化标签之间进行插值，从而减轻标准伪校准固有的悲观性。实验表明，所提出的源域调优方案在保持集合大小非平凡的同时，降低了覆盖下降。

参考文献

[1] A. N. Angelopoulos, R. F. Barber, and S. Bates, “共形预测的理论基础,” arXiv preprint arXiv:2411.11824, 2024. [2] R. J. Tibshirani, R. Foygel Barber, E. Candes, and A. Ramdas, “协变量偏移下的共形预测,” 神经信息处理系统进展, vol. 32, 2019. [3] W. Deng, S. Park, M. Li, and O. Simeone, “优化上下文学习以实现高效的完全共形预测,” IEEE信号处理快报, pp. 1–5, 2025. [4] B. Wang, M. Zecchin, and O. Simeone, “具有间歇反馈的镜像在线共形预测,” IEEE信号处理快报, vol. 32, pp. 2888–2892, 2025. [5] I. Alon, D. Arnon, and A. Wiesel, “学习最小体积不确定性椭球,” IEEE信号处理快报, vol. 31, 1659, 2024 1655pp. – .[6] R. F. Barber, E. J. Candes, A. Ramdas, and R. J. Tibshirani, “超越可交换性的共形预测,” 统计年刊, vol. 51, no. 2, pp. 816–845, 2023. [7] J. G. Moreno-Torres, T. Raeder, R. Alaiz-Rodr´ıguez, N. V. Chawla, and F. Herrera, “分类中数据集偏移的统一视角,” 模式识别, vol. 45, no. 1, pp. 521–530, 2012. [8] A. Podkopaev and A. Ramdas, “标签偏移下分类的分布无关不确定性量化,” 收录于第三十七届人工智能不确定性会议论文集，机器学习研究论文集系列，C. de Campos and M. H. Maathuis 编, vol. 161. PMLR, 27–30 Jul 2021, pp. 844–853. [在线]。可访问：https://proceedings.mlr.press/v161/podkopaev21a.html [9] R. Xu, C. Chen, Y. Sun, P. Venkitasubramaniam, and S. Xie, “一般分布偏移下的Wasserstein正则化共形预测,” 收录于第十三届国际学习表征会议, 2025. [在线]。可访问：https://openreview.net/ forum?id=aJ3tiX1Tu4[10]A. H. C. Correia and C. Louizos, “利用最优传输进行非可交换共形预测：借助无标签数据应对分布偏移,” 2025. [在线]。可访问：https://arxiv.org/abs/2507. 10425[11] L. Aolaritei, Z. O. Wang, J. Z hu, M. I. Jordan, and Y. Marzouk, “Levy-Prokhorov分布偏移下的共形预测：对局部和全局扰动的稳健性,” arXiv preprint arXiv:2502.14105, 2025. [12] K. Kasa, Z. Zhang, H. Yang, and G. W. Taylor, “在无标签条件下使预测集适应分布偏移,” 2025. [在线]。可访问：https://arxiv.org/abs/ 2406 01416 . S. Alijani [13] and H. Najjaran, “Wqlcp：用于分布偏移下稳健不确定性量化的加权自适应共形预测,” 收录于IEEE/CVF计算机视觉与模式识别会议（CVPR）研讨会论文集，2025年6月，pp. 1732–1741. [14] S. Angelman, R. Nizhar, and J. Goldberger, “无标签校准：利用伪标签实现无源共形预测,” 收录于第十四届共形与概率预测及其应用研讨会论文集，机器学习研究论文集系列，K. A. Nguyen, Z. Luo, H. Papadopoulos, T. L¨ofstr¨om, L. Carlsson, and H. Bostr¨om 编，vol. 266. PMLR, 10–12 Sep 2025, pp. 63–81. [在线]。可访问：https: // proceedings.mlr.press/v266/angelman25a.html [15] A. Kumar, T. Ma, and P. Liang, “理解渐进式领域适应中的自训练,” 收录于国际机器学习会议. PMLR, 2020, pp. 5468–5479. [16] Y. He, H. Wang, B. Li, and H. Zhao, “渐进式领域适应：理论与算法,” 机器学习研究期刊, vol. 25, no. 361, pp. 1–40, 2024. [17] E. J. Cand`es, A. Ilyas, and T. Zrnic, “可能近似正确标签,” arXiv preprint arXiv:2506.10908, 2025. [18] G. S hafer and V. Vovk, “共形预测教程.” 机器学习研究期刊, vol. 9, no. 3, 2008. [19] A. N. Angelopoulos and S. Bates, “共形预测与分布无关不确定性量化浅介,” 2022. [在线]。可访问：https://arxiv.org/abs/2107.07511

补充材料（附录）

A. 引理 1 的证明

固定 $\epsilon>0$。对于每个 y，选取 $\pi_y\in\Pi(P_{X|y},Q_{X|y})$，使得

$$\operatorname*{ess\,sup}_{(X,X')\sim\pi_y}\|X-X'\|_2\le\rho+\epsilon. \tag{9}$$

设 $Y\sim P_Y$，并在给定 $Y=y$ 的条件下抽取样本 $(X,X')\sim\pi_y$。则 $(X,Y)\sim P_{XY}$且 $(X',Y)\sim Q_{XY}$，并且 $|s(X,Y)-s(X',Y)|\le L_\gamma\|X-X'\|_2$ 几乎处处成立。因此 $W_1(s\#P,s\#Q)\le L_\gamma\,\mathbb{E}\|X-X'\|_2\le L_\gamma(\rho+\epsilon)$。设 $\epsilon\to0$。

B. Kantorovich-Rubinstein 不等式

引理2：设 $(\mathcal{X},d)$ 是一个度量空间，设 P,Q 是定义在 $\mathcal{X}$ 上的概率测度，且 $f\colon\mathcal{X}\to\mathbb{R}$ 是 L-利普希茨函数。则 $\left|\mathbb{E}_P[f(X)]-\mathbb{E}_Q[f(X')]\right|\le L\,W_1(P,Q)$。

证明：对于任意耦合 $\pi\in\Pi(P,Q)$，其中 $(X,X')\sim\pi$，$|\mathbb{E}[f(X)-f(X')]|\le\mathbb{E}|f(X)-f(X')|\le L\,\mathbb{E}[d(X,X')]$。取 $\inf_{\pi\in\Pi(P,Q)}$ 即可得到所述结论。∎

C. 定理 1 的证明

定义 $S:=-\gamma_f(X,Y)$，$\tilde S:=-\gamma_f(X,\tilde Y)$，其中 $(X,Y)\sim Q_{XY}$。对于任意固定的分类器 f，伪-分数 $S_i=s(X_i,f(X_i))$ 在 Q 下具有可交换性。因此，根据分割保形有效性，$\tilde Q\big(\tilde S\le q_{\tilde Q,\alpha}\big)\ge1-\alpha$。由于 $S=s(X,f(X))$ 仅取决于 X，且 $X\sim Q_X$在下同时满足 Q 和 $\tilde Q$，这也等于 $Q(S\le q_{\tilde Q,\alpha})\ge1-\alpha$。因此，在 Q_{XY} 下，

$$Q\big(S>q_{\tilde Q,\alpha}+\tau\big)\le\alpha+Q\big(S-\tilde S>\tau\big). \tag{10}$$

若 $Y=f(X)$ 则 $S=\tilde S$，因此 $S-\tilde S=0$。于是 $\{S-\tilde S>\tau\}\subseteq\{Y\ne f(X)\}$。在事件 $\{Y\ne f(X)\}$ 上，$S-\tilde S=-\gamma_f(X,Y)+\gamma_f(X,f(X))$。因此 $0\le\gamma_f(X,f(X))-\gamma_f(X,Y)$，在事件 $\{S-\tilde S>\tau\}$ 上，$S-\tilde S\le2(-\gamma_f(X,Y))$。因此，

$$\{S-\tilde S>\tau\}\subseteq\Big\{2(-\gamma_f(X,Y))>\tau\Big\}=\Big\{\gamma_f(X,Y)<-\tfrac{\tau}{2}\Big\},$$

因此，

$$Q\big(S-\tilde S>\tau\big)\le Q\Big(\gamma_f(X,Y)\le-\tfrac{\tau}{2}\Big). \tag{11}$$

接下来，我们通过坡形损失控制 $Q(\gamma_f(X,Y)\le-\frac{\tau}{2})$。回顾坡形损失 $\ell_r((x,y);f)=r(\gamma_f(x,y))$。对于任意 $\gamma\le0$，我们有 $1-\gamma\ge1$，因此 $r(\gamma)=\min\{(1-\gamma)^+,1\}=1$. 因此，在事件 $\{\gamma_f(X,Y)\le-\frac{\tau}{2}\}$ 上，我们有 $r(\gamma_f(X,Y))=1\{\gamma_f(X,Y)\le-\frac{\tau}{2}\}\le1$。对其取期望可得

$$Q\big(\gamma_f(X,Y)\le-\tfrac{\tau}{2}\big)\le\mathbb{E}_Q\big[r\big(\gamma_f(X,Y)\big)\big]=L_r(f,Q).$$

由于我们可以针对任意 $\tau\ge0$ 给出结果，因此有

$$Q\big(\gamma_f(X,Y)\le-\tfrac{\tau}{2}\big)\le Q(\gamma_f(X,Y)\le0)\le L_r(f,Q).$$

对于每个 $y\in[K]$，定义 $\ell_y(x):=r(\gamma_f(x,y))$。根据假设1，并且由于 $r(\cdot)$是1-利普希茨的，ℓ_y在 x上是 L_γ-利普希茨的。我们可以写出 $L_r(f,P)=\sum_{y=1}^K P_Y(y)\,\mathbb{E}_{P_{X|y}}[\ell_y(X)]$，，类似地，$L_r(f,Q)=\sum_{y=1}^K Q_Y(y)\,\mathbb{E}_{Q_{X|y}}[\ell_y(X)]$。根据假设2(i)，

$$L_r(f,Q)-L_r(f,P)=\sum_{y=1}^K P_Y(y)\big(\mathbb{E}_{Q_{X|y}}[\ell_y(X)]-\mathbb{E}_{P_{X|y}}[\ell_y(X)]\big).$$

根据引理2，$\big|\mathbb{E}_{Q_{X|y}}[\ell_y(X)]-\mathbb{E}_{P_{X|y}}[\ell_y(X)]\big|\le L_\gamma W_1(P_{X|y},Q_{X|y})$，对于每个 y。因此，

$$\big|L_r(f,Q)-L_r(f,P)\big|\le L_\gamma\sum_{y=1}^K P_Y(y)\,W_1(P_{X|y},Q_{X|y})=L_\gamma\rho_{\mathrm{mix}},$$

特别地，$L_r(f,Q)\le L_r(f,P)+L_\gamma\rho_{\mathrm{mix}}$。结合前面的公式可得 $Q(S>q_{\tilde Q,\alpha}+\tau)\le\alpha+Q(S-\tilde S>\tau)\le\alpha+Q(\gamma_f(X,Y)\le-\frac{\tau}{2})$。因此，

$$L_r(f,P)+L_\gamma\rho_{\mathrm{mix}}.$$

$$Q(S>q_{\tilde Q,\alpha}+\tau)\le\alpha+Q(\gamma_f(X,Y)\le-\tfrac{\tau}{2}).$$

最后，

$$L_r(f,P)+L_\gamma\rho_{\mathrm{mix}}$$

$$Q(Y_{n+1}\in C^{1-\alpha}_{\tilde Q,\tau}(X_{n+1}))=1-\alpha+\tau,$$

由此得到。

$$Q(S\le q_{\tilde Q,\alpha})\ge1-\alpha.$$

D. 推论1的证明

任取 $\tau\ge0$。令 $(X,Y):=(X_{n+1},Y_{n+1})\sim Q_{XY}$表示测试点，并定义 $Y:=f(X)$，$S:=s(X,Y)$，$\tilde S:=s(X,\tilde Y)$。对于松弛集合 $C^{1-\alpha}_{\tilde Q,\tau}(X)=\{y:s(X,y)\le q_{\tilde Q,\alpha}+\tau\}$ 有 $\{Y\notin C^{1-\alpha}_{\tilde Q,\tau}(X)\}=\{S>q_{\tilde Q,\alpha}+\tau\}$。利用 (10) 和 (11)，

$$Q(S>q_{\tilde Q,\alpha}+\tau)\le\alpha+Q(S-\tilde S>\tau)\le\alpha+Q\big(\gamma_f(X,Y)\le-\tfrac{\tau}{2}\big).$$

在事件 $\{\gamma_f(X,Y)\le-\frac{\tau}{2}\}$ 上，我们有 $1-\gamma_f(X,Y)\ge1+\frac{\tau}{2}$，因此 $\ell_h((X,Y);f)=\max\{1-\gamma_f(X,Y),0\}\ge1+\frac{\tau}{2}$。因此，$\mathbb{1}\{\gamma_f(X,Y)\le-\frac{\tau}{2}\}\le\frac{\ell_h((X,Y);f)}{1+\frac{\tau}{2}}$。在 Q_{XY} 下取期望可得 $Q\big(\gamma_f(X,Y)\le-\frac{\tau}{2}\big)\le\frac{L_h}{(f,Q)\,1+\frac{\tau}{2}}$。结合上述各式可得 $Q(S>q_{\tilde Q,\alpha}+\tau)\le\alpha+\frac{L_h}{(f,Q)\,1+\frac{\tau}{2}}$。重新整理即得 (7)。

E. 定理 2 的证明

设 $X_1,\dots,X_{n+1}$ 独立同分布$\sim Q_X$，以及 $\tilde Y_i=f(X_i)$及其相应伪分数 $S_i:=s(X_i,Y_i)$。令$q_{\tilde Q}$、$_\alpha$为 $\{S_i\}_{i=1}^n$的分割保形（$1-\alpha$）阈值。定义$C^{1-\alpha}_{\tilde Q}(x):=\{y:s(x,y)\le q_{\tilde Q,\alpha}\}$。令 $\tilde Y_u(X_i)$按（8）定义，且 $S_i^u:=s(X_i,Y_u(X_i))$。令$q_{\tilde Q^u}$、$_\alpha$为来自 $\{S_i^u\}_{i=1}^n$的分割保形（$1-\alpha$）阈值。令 $C^{1-\alpha}_{\tilde Q^u}(x)=\{y\in[K]:s(x,y)\le q_{\tilde Q^u,\alpha}\}$。

若 $H(X_i)\le u$，则 $S_i^u=S_i$，则标签 $Y_u(X_i)$从 $[K]$中均匀抽取；并且由于 $f(X_i)$在 $y\in[K]$ 上最小化 $s(X_i,y)$，我们有 $s(X_i,Y_u(X_i))\ge s(X_i,f(X_i))=S_i$对每一次实现均成立。因此，$S_i^u\ge S_i$。从而，对任意 $t\in\mathbb{R}$，我们有 $\{S_i^u\le t\}\subseteq\{S_i\le t\}$，这意味着 $\frac{1}{n}\sum_{i=1}^n\mathbb{1}\{S_i^u\le t\}\le\frac{1}{n}\sum_{i=1}^n\mathbb{1}\{\tilde S_i\le t\}$。

根据经验分位数的定义，可得 $q_{\tilde Q^u,\alpha}\ge q_{\tilde Q,\alpha}$。在事件 $\{H(X_i)>u\}$ 上，令 $U_i\sim$服从 Unif($[K]$)。对于测试点 $(X_{n+1},Y_{n+1})\sim Q_{XY}$，指示函数 $\mathbb{1}\{s(X_{n+1},Y_{n+1})\le t\}$ 关于 t 单调不减，因此对于 $\mathcal{C}=(X_1,\dots,X_n,U_1,\dots,U_n)$ 和 (X_{n+1},Y_{n+1}) 的每一种取值，我们都有

$$\mathbb{1}\{s(X_{n+1},Y_{n+1})\le q_{\tilde Q^u,\alpha}\}\ge\mathbb{1}\{s(X_{n+1},Y_{n+1})\le q_{\tilde Q,\alpha}\}.$$

在给定 $\mathcal{C}$ 的条件下取条件期望，得到

$$\mathbb{E}\left[\mathbb{1}\{Y_{n+1}\in C^{1-\alpha}_{\tilde Q^u}(X_{n+1})\}\mid\mathcal{C}\right]\ge\mathbb{E}\left[\mathbb{1}\{Y_{n+1}\in C^{1-\alpha}_{\tilde Q}(X_{n+1})\}\mid\mathcal{C}\right].$$

最后，对 $\mathcal{C}$ 取期望，$Q(Y_{n+1}\in C^{1-\alpha}_{\tilde Q^u}(X_{n+1}))\ge Q(Y_{n+1}\in C^{1-\alpha}_{\tilde Q}(X_{n+1}))$ 得到。