Lifting Weak Supervision To Structured Prediction

Harit Vishwakarma  
hvishwakarma@wisc.edu

Frederic Sala  
fredsala@cs.wisc.edu

Department of Computer Sciences,  
University of Wisconsin-Madison, WI, USA.

Abstract

Weak supervision (WS) is a rich set of techniques that produce pseudolabels by aggregating easily obtained but potentially noisy label estimates from a variety of sources. WS is theoretically well understood for binary classification, where simple approaches enable consistent estimation of pseudolabel noise rates. Using this result, it has been shown that downstream models trained on the pseudolabels have generalization guarantees nearly identical to those trained on clean labels. While this is exciting, users often wish to use WS for structured prediction, where the output space consists of more than a binary or multi-class label set: e.g. rankings, graphs, manifolds, and more. Do the favorable theoretical properties of WS for binary classification lift to this setting? We answer this question in the affirmative for a wide range of scenarios. For labels taking values in a finite metric space, we introduce techniques new to weak supervision based on pseudo-Euclidean embeddings and tensor decompositions, providing a nearly-consistent noise rate estimator. For labels in constant-curvature Riemannian manifolds, we introduce new invariants that also yield consistent noise rate estimation. In both cases, when using the resulting pseudolabels in concert with a flexible downstream model, we obtain generalization guarantees nearly identical to those for models trained on clean data. Several of our results, which can be viewed as robustness guarantees in structured prediction with noisy labels, may be of independent interest. Empirical evaluation validates our claims and shows the merits of the proposed method.

1 Introduction

Weak supervision (WS) is an array of methods used to construct pseudolabels for training supervised models in label-constrained settings. The standard workflow [RSW+16, RBE+18, FCS+20] is to assemble a set of cheaply-acquired labeling functions—simple heuristics, small programs, pretrained models, knowledge base lookups—that produce multiple noisy estimates of what the true label is for each unlabeled point in a training set. These noisy outputs are modeled and aggregated into a single higher-quality pseudolabel. Any conventional supervised end model can be trained on these pseudolabels. This pattern has been used to deliver excellent performance in a range of domains in both research and industry settings [DRS+20, RNGS20, SLB20], bypassing the need to invest in large-scale manual labeling. Importantly, these successes are usually found in binary or small-cardinality classification settings.

While exciting, users often wish to use weak supervision in structured prediction (SP) settings, where the output space consists of more than a binary or multiclass label set [BHS+07, KL15]. In such cases, there exists meaningful algebraic or geometric structure to exploit. Structured prediction includes, for example, learning rankings used for recommendation systems [KAG18], regression in metric spaces [PM19], learning on manifolds [RCMR18], graph-based learning [GS19], and more.


An important advantage of WS in the standard setting of binary classification is that it sometimes yields models with nearly the same generalization guarantees as their fully-supervised counterparts. Indeed, the penalty for using pseudolabels instead of clean labels is only a multiplicative constant. This is a highly favorable tradeoff since acquiring more unlabeled data is easy. This property leads us to ask the key question for this work: does weak supervision for structured prediction preserve generalization guarantees? We answer this question in the affirmative, justifying the application of WS to settings far from its current use.

Generalization results in WS rely on two steps [RHD + 19, FCS + 20]: (i) showing that the estimator used to learn the model of the labeling functions is consistent, thus recovering the noise rates for these noisy voters, and (ii) using a noise-aware loss to de-bias end-model training [NDRT13]. Lifting these two results to structured prediction is challenging. The only available weak supervision technique suitable for SP is that of [SLV + 22]. It suffers from several limitations. First, it relies on the availability of isometric embeddings of metric spaces into $\mathbb{R}^d$—but does not explain how to find these. Second, it does not tackle downstream generalization at all. We resolve these two challenges.

We introduce results for a wide variety of structured prediction problems, requiring only that the labels live in some metric space. We consider both finite and continuous (manifold-valued) settings. For finite spaces, we apply two tools that are new to weak supervision. The approach we propose combines isometric pseudo-Euclidean embeddings with tensor decomposition algorithms—resulting in a nearly-consistent noise rate estimator. In the continuous case, we introduce a label model suitable for the so-called model spaces—Riemannian manifolds of constant curvature—along with extensions to even more general spaces. In both cases, we show generalization results when using the resulting pseudolabels in concert with a flexible end model from [CRR16, RCMR18].

Contributions:

- New techniques for performing weak supervision in finite metric spaces based on isometric pseudo-Euclidean embeddings and tensor decomposition algorithms,
- Generalizations to manifold-valued regression in constant-curvature manifolds,
- Finite-sample error bounds for noise rate estimation in each scenario,
- Generalization error guarantees for training downstream models on pseudolabels,
- Experiments confirming the theoretical results and showing improvements over [SLV + 22].

2 Background and Problem Setup

Our goal is to theoretically characterize how well learning with pseudolabels (built with weak supervision techniques) performs in structured prediction. We seek to understand the interplay between the noise in WS sources and the generalization performance of the downstream structured prediction model. We provide brief background and introduce our problem and some useful notation.

2.1 Structured Prediction

Structured prediction (SP) involves predicting labels in spaces with rich structure. Denote the label space by $\mathcal{Y}$. Conventionally $\mathcal{Y}$ is a set, e.g., $\mathcal{Y} = \{-1, +1\}$ for binary classification. In the SP setting, $\mathcal{Y}$ has some additional algebraic or geometric structure. In this work we assume that $\mathcal{Y}$ is a metric space with metric (distance) $d_Y$. This covers many types of problems, including

- Rankings, where $\mathcal{Y} = S_{\rho}$, the symmetric group on $\{1, \ldots, \rho\}$, i.e., labels are permutations,
- Graphs, where $\mathcal{Y} = \mathcal{G}_\rho$, the space of graphs with vertex set $V = \{1, \ldots, \rho\}$,
- Riemannian manifolds, including $\mathcal{Y} = S_d$, the sphere, or $\mathbb{H}_d$, the hyperboloid.

Learning and Generalization in Structured Prediction In conventional supervised learning we have a dataset $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ of i.i.d. samples drawn from distribution $\rho$ over $\mathcal{X} \times \mathcal{Y}$. As usual, we seek to learn a model that generalizes well to points not seen during training. Let $\mathcal{F} = \{f : \mathcal{X} \mapsto \mathcal{Y}\}$ be a family of functions from $\mathcal{X}$ to $\mathcal{Y}$. Define the risk $R(f)$ for $f \in \mathcal{F}$ and $f^*$ as

$$R(f) = \int_{\mathcal{X} \times \mathcal{Y}} d_Y^2(f(x), y) d\rho(x,y) \quad f^* \in \arg\min_{f \in \mathcal{F}} R(f). \quad (1)$$
We are now in a position to state the main research question for this work: We adopt the noise model from [SLV] where

\[ \theta \]

An exciting contribution of [CRR16, RCMR18] is the generalization bound where \( \alpha \) valued) spaces. We first discuss learning the noise parameters \( \theta \) is, we must learn \( \alpha \) and then to perform the optimization in (2) to make a prediction.

An exciting contribution of [CRR16, RCMR18] is the generalization bound

\[ R(\hat{f}) \leq R(f^*) + O(n^{-\frac{1}{2}}), \]

that holds with high probability, as long as there is no label noise. The key question we tackle is does the use of pseudolabels instead of true labels \( y_i \) affect the generalization rate?

### 2.2 Weak Supervision

In WS, we cannot access any of the ground-truth labels \( y_i \). Instead we observe for each \( x_i \) the noisy votes \( \lambda_{1,i}, \ldots, \lambda_{m,i} \). These are \( m \) weak supervision outputs provided by labeling functions (LFS) \( s_a \), where \( s_a : X \rightarrow Y \) and \( \lambda_{a,i} = s_a(x_i) \). A two step process is used to construct pseudolabels. First, we learn a noise model (also called a label model) that determines how reliable each source \( s_a \) is. That is, we must learn \( \theta \) for \( P_\theta(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{m} | y) \) - without having access to any samples of \( y \). Second, the noise model is used to infer a distribution (or its mode) for each point: \( \hat{P}_\theta(y_i | \lambda_{1,i}, \ldots, \lambda_{m,i}) \).

We adopt the noise model from [SLV+22], which is suitable for our SP setting:

\[
P_\theta(\lambda_{1}, \ldots, \lambda_{m} | y) = \frac{1}{Z} \exp \left( - \sum_{a=1}^{m} \theta_a d_{\lambda_{a}}^2(\lambda_{a}, y) - \sum_{(a,b) \in E} \theta_{a,b} d_{\lambda_{a}}^2(\lambda_{a}, \lambda_{b}) \right).
\]

\( Z \) is the normalizing partition function, \( \theta = [\theta_1, \ldots, \theta_m]^T > 0 \) are canonical parameters, and \( E \) is a set of correlations. The model can be described in terms of the mean parameters \( \mathbb{E}[d_{\lambda_{a}}^2(\lambda_{a}, y)] \). Intuitively, if \( \theta_a \) is large, the typical distance from \( \lambda_{a} \) to \( y \) is small and the LF is reliable; if \( \theta_a \) is small, the LF is unreliable. This model is appropriate for several reasons. It is an exponential family model with useful theoretical properties. It subsumes popular special cases of noise, including, for regression, zero-mean multivariate Gaussian noise; for permutations, a generalization of the popular Mallows model; for the binary case, it produces a close relative of the Ising model.

Our goal is to form estimates \( \hat{\theta} \) in order to construct pseudolabels. One way to build such pseudolabels is to compute \( \hat{y} = \arg\min_{z \in Y} \frac{1}{m} \sum_{a=1}^{m} \hat{\theta}_a d_{\lambda_{a}}^2(z, \lambda_{a}). \) Observe how the estimated parameters \( \hat{\theta}_a \) are used to weight the labeling functions, ensuring that more reliable votes receive a larger weight.

We are now in a position to state the main research question for this work:

**Do there exist estimation approaches yielding \( \hat{\theta} \) that produce pseudolabels \( \hat{y} \) that maintain the same generalization error rate \( O(n^{-1/4}) \) when used in (2), or a modified version of (2)?**

### 3 Noise Rate Recovery in Finite Metric Spaces

In the next two sections we handle finite metric spaces. Afterwards we tackle continuous (manifold-valued) spaces. We first discuss learning the noise parameters \( \theta \), then the use of pseudolabels.

**Roadmap** For finite metric spaces with \( |Y| = r \), we apply two tools new to weak supervision. First, we embed \( Y \) into a pseudo-Euclidean space [Gol85]. These spaces generalize Euclidean space, enabling isometric (distance-preserving) embeddings for any metric. Using pseudo-Euclidean spaces make our analysis slightly more complex, but we gain the isometry property, which is critical.

Second, we form three-way tensors from embeddings of observed labeling functions. Applying tensor product decomposition algorithms [AGH+14], we can recover estimates of the mean parameters \( \mathbb{E}[d_{\lambda_{a}}^2(\lambda_{a}, y)] \) and ultimately \( \hat{\theta}_a \). Finally, we reweight the model (2) to preserve generalization.
The intuition behind this approach is the following. First, we need a technique that can provide consistent or nearly-consistent estimates of the parameters in the noise model. Second, we need to handle any finite metric space. Techniques like the one introduced in [FCS+20] handle the first—but do not work for generic finite metric spaces, only binary labels and certain sequences. Techniques like the one in [SLV+22] handle any metric space—but only have consistency guarantees in highly restrictive settings (e.g., it requires an isometric embedding, that the distribution over the resulting embeddings is isomorphic to certain distributions, the true label only takes on two values). Pseudo-Euclidean embeddings used with tensor decomposition algorithms meet both requirements.

### 3.1 Pseudo-Euclidean Embeddings

Our first task is to embed the metric space into a continuous space—enabling easier computation and potential dimensionality reduction. A standard approach is multi-dimensional scaling (MDS) [KW78], which embeds $\mathcal{Y}$ into $\mathbb{R}^d$. A downside of MDS is that not all metric spaces embed (isometrically) into Euclidean space, as the square distance matrix $D$ must be positive semi-definite.

A simple and elegant way to overcome this difficulty is to instead use pseudo-Euclidean spaces for embeddings. These pseudo-spaces do not require a p.s.d. inner product. As an outcome, any finite metric space can be embedded into a pseudo-Euclidean space with no distortion [Go85]—so that distances are exactly preserved. Such spaces have been applied to similarity-based learning methods [PPD01, LRB06, PHD+06]. A vector $u$ in a pseudo-Euclidean space $\mathbb{R}^{d^+}, \mathbb{R}^{d^-}$ has two parts: $u^+ \in \mathbb{R}^{d^+}$ and $u^- \in \mathbb{R}^{d^-}$. The dot product and the squared distance between any two vectors $u, v$ are $\langle u, v \rangle_\phi = \langle u^+, v^+ \rangle + \langle u^-, v^- \rangle$, and $d_\phi^2(u, v) = ||u^+ - v^+||_2^2 + ||u^- - v^-||_2^2$. These properties enable isometric embeddings: the distance can be decomposed into two components that are individually induced from p.s.d. inner products—and can thus be embedded via MDS. Indeed, pseudo-Euclidean embeddings effectively run MDS for each component (see Algorithm 1 steps 4-9).

To recover the original distance, we obtain $||u^+ - v^+||_2^2$ and $||u^- - v^-||_2^2$ and subtract.

**Example:** To see why such embeddings are advantageous, we compare with a one-hot vector representation (whose dimension is $|\mathcal{Y}|$). Consider a tree with a root node and three branches, each of which is a path with $t$ nodes. Let $\mathcal{Y}$ be the nodes in the tree with the shortest-hops distance as the metric. The pseudo-Euclidean embedding dimension is just $d = 3$; see Appendix for more details. The one-hot embedding dimension is $d = |\mathcal{Y}| = 3t + 1$—arbitrarily larger!

Now we are ready to apply these embeddings to our problem. Abusing notation, we write $\lambda_a$ and $y$ for the pseudo-Euclidean embeddings of $\lambda_a, y$, respectively. We have that $d_\phi^2(\lambda_a, y) = d_\phi^2(\lambda_a, y)$, so that there is no loss of information from working with these spaces. In addition, we write the mean as $\mu_{a,y} = \mathbb{E}[\lambda_a | y]$ and the covariance as $\Sigma_{a,y}$. Our goal is to obtain an accurate estimate $\mu_{a,y} = \mathbb{E}[\lambda_a | y]$, which we will use to estimate the mean parameters $\mathbb{E}[d_\phi^2(\lambda_a, y)]$. If we could observe $y$, it would be easy to empirically estimate $\mu_{a,y}$—but we do not have access to it. Our approach will be to apply tensor decomposition for multi-view mixtures [AGJ14].

### 3.2 Multi-View Mixtures and Tensor Decompositions

In a multi-view mixture model, multiple views $\{\lambda_a\}_{a=1}^m$ of a latent variable $Y$ are observed. These views are independent when conditioned on $Y$. We treat the positive and negative components $\lambda_a^+ \in \mathbb{R}^{d^+}$ and $\lambda_a^- \in \mathbb{R}^{d^-}$ of our pseudo-Euclidean embedding as separate multi-view mixtures:

$$
\lambda_a^+ | y \sim \mu_{a,y}^+ + \sigma d^{+1} \cdot \epsilon_a^+ \quad \text{and} \quad \lambda_a^- | y \sim \mu_{a,y}^- + \sigma d^{-1} \cdot \epsilon_a^- \quad \forall a \in [m],
$$

where $\mu_{a,y}^+, \mu_{a,y}^- = \mathbb{E}[\lambda_a^+ | y], \mu_{a,y}^- = \mathbb{E}[\lambda_a^- | y]$ and $\epsilon_a^+, \epsilon_a^-$ are mean zero random vectors with covariances $\frac{1}{d^+} I_{d^+}, \frac{1}{d^-} I_{d^-}$ respectively. Here $\sigma^2$ is a proxy variance whose use is described in Assumption 3.
We cannot directly estimate these parameters from observations of \( \sigma \), due to the fact that \( y \) is not observed. However, we can observe various moments of the outputs of the LFs such as tensors of outer products of LF triplets. We require that for each \( a \) such a triplet exists. Then,

\[
T^+ := \mathbb{E}[\lambda_a \otimes \lambda_b \otimes \lambda_c] = \sum_{y \in Y} w_y \mu_{a,y} \mu_{b,y} \mu_{c,y} \quad \text{and} \quad T^- := \frac{1}{n} \sum_{i=1}^{n} \lambda_{a,i} \lambda_{b,i} \lambda_{c,i}. \tag{5}
\]

Here \( w_y \) are the mixture probabilities (prior probabilities of \( Y \)) and \( Y_s = \{ y : w_y > 0 \} \). We similarly define \( T^- \) and \( \mathcal{T}^- \). We then obtain estimates \( \hat{\mu}_{a,y}^+, \hat{\mu}_{a,y}^- \) using an algorithm from [AGH+14] with minor modifications to handle pseudo-Euclidean rather than Euclidean space. The overall approach is shown in Algorithm 1. We have three key assumptions for our analysis,

**Assumption 1.** The support of \( P_Y \), i.e., \( k = |\{ y : w_y > 0 \}| \) and the label space \( \mathcal{Y} \) is such that \( \min(d^+, d^-) \geq k, ||\mu_{a,y}^+||_2 = 1, ||\mu_{a,y}^-||_2 = 1 \) for \( a \in [m], y \in \mathcal{Y} \).

**Assumption 2.** (Bounded angle between \( \mu \) and \( y \)) Let \( \phi(u, v) \) denote the angle between any two vectors \( u, v \) in a Euclidean space. We assume that \( \phi(\mu_{a,y}^+, y^-) \in [0, \pi/2 - c], \phi(\mu_{a,y}^+, y^+) \in [0, \pi/2 - c] \) \( \forall a \in [m] \), and \( y \in \mathcal{Y}_s \), for some sufficiently small \( c \in (0, \pi/4] \) such that \( \sin(c) \geq \max(c_0(d^+), c_0(d^-)) \), where \( c_0(d) \) is defined for some \( n > n_0 \) samples in [6].

**Assumption 3.** \( \sigma \) is such that the recovery error with model [4] is at least as large as with [3].

These enable providing guarantees on recovering the mean vector magnitudes [1] and signs [2] and simplify the analysis [1, 3]; all three can be relaxed at the expense of a more complex analysis.

Our first theoretical result shows that we have near-consistency in estimating the mean parameters in [4]. We use standard notation \( \tilde{O} \) ignoring logarithmic factors.
Theorem 1. Let $\hat{\mu}_{a,y}^+, \hat{\mu}_{a,y}^-$ be the estimates of $\mu_{a,y}^+, \mu_{a,y}^-$ returned by Algorithm I with input $\hat{T}^+, \hat{T}^-$ constructed using isometric pseudo-Euclidean embeddings (in $\mathbb{R}^{d^+, d^-}$). Suppose Assumptions 1 and 2 are met, a sufficiently large number of samples $n$ are drawn from the model in (3), and $k = |\mathcal{Y}_s|$. Then there exists a constant $C_0 > 0$ such that with high probability $\forall \alpha \in [m]$ and $y \in \mathcal{Y}_s$,

$$|\theta_a - \hat{\theta}_a| \leq C_0 \left| \mathbb{E}[d^2_Y(\lambda_a, y)] - \mathbb{E}[d^2_Y(\hat{\lambda}_a, y)] \right| \leq \epsilon(d^+) + \epsilon(d^-),$$

where

$$\epsilon(d) := \begin{cases} \tilde{O} \left( k \sqrt{\frac{n}{d}} \right) + \tilde{O} \left( \frac{\sigma^2}{d} \right) & \text{if } \sigma^2 = \Theta(1), \\ \tilde{O} \left( \sqrt{\frac{n}{d}} \right) + \tilde{O} \left( \frac{\sigma^2}{\epsilon} \right) & \text{if } \sigma^2 = \Theta \left( \frac{1}{d} \right). \end{cases} \quad (6)$$

We interpret Theorem 1. It is a nearly direct application of [AGJ14]. There are two noise cases for $\sigma$. In the high-noise case, $\sigma$ is independent of dimension $d$ (and thus $|\mathcal{Y}|$). Intuitively, this means the average distance balls around each LF begin to overlap as the number of points grows—explaining the multiplicative $k$ term. If the noise scales down as we add more embedded points, this problem is removed, as in the low-noise case. In both cases, the second error term comes from using the algorithm of [AGH14] and is independent of the sampling error. Since $k = \Theta(d)$, this term goes down with $d$. The first error term is due to sampling noise and goes to zero in the number of samples $n$. Note the tradeoffs of using the embeddings. If we used one-hot encoding, $d = |\mathcal{Y}|$, and in the high-noise case, we would pay a very heavy cost for $\sqrt{d/n}$. However, while sampling error is minimized when using a very small $d$, we pay a cost in the second error term. This leads to a tradeoff in selecting the appropriate embedding dimension.

4 Generalization Error for Structured Prediction in Finite Metric Spaces

We have access to labeling function outputs $\lambda_{a,i}, \ldots, \lambda_{m,i}$ for points $x_i$ and noise rate estimates $\hat{\theta}_a, \ldots, \hat{\theta}_m$. How can we use these to infer unobserved labels $y$ in (2)? Our approach is based on [NDRT13, vRW18], where the underlying loss function is modified to deal with noise. Analogously, we modify (2) in such a way that the generalization guarantee is nearly preserved.

4.1 Prediction with Pseudolabels

First, we construct the posterior distribution $P_\theta(Y = y|\lambda)$. We use our estimated noise model $P_\theta(\lambda|Y)$ and the prior $P(Y = y)$. We create pseudo-labels for each data point by drawing a random sample from the posterior distribution conditioned on the output of labeling functions: $\hat{Z}(i) = \hat{z}_i \sim Y|\lambda = \lambda^{(i)}_a, \ldots, \lambda = \lambda^{(i)}_m, \theta$. We thus observe $(x_1, \hat{z}_1), \ldots, (x_n, \hat{z}_n)$ where $\hat{z}_i$ is sampled as above. To overcome the effect of noise we create a perturbed version of the distance function using the noise rates, generalizing [NDRT13]. This requires us to characterize the noise distribution induced by our inference procedure. In particular we seek the probability that $\hat{Z} = y_j$ when the true label is $y_j$. This can be expressed as follows. Let $\mathcal{Y}^m$ denote the $m$-fold Cartesian product of $\mathcal{Y}$ and let $\Lambda_u = (\lambda^{(u)}_1, \ldots, \lambda^{(u)}_m)$ denote its $u^{th}$ entry. We write

$$P_{ij} = P_\theta(\hat{Z} = y_j|Y = y_i) = \sum_{u=1}^{m^{|\mathcal{Y}|}} P_\theta(Y = y_j|\Lambda = \Lambda^{(u)}) \cdot P_\theta(\Lambda = \Lambda^{(u)}|Y = y_i). \quad (7)$$

We define $Q_{ij} = P_\theta(\hat{Z} = y_j|Y = y_i)$ using $\hat{\theta}$. $P$ is the noise distribution induced by the true parameters $\theta$ and $Q$ is an approximation obtained from inference with the estimated parameters $\hat{\theta}$. With this terminology, we can define the perturbed version of the distance function and a corresponding replacement of (2):

$$\hat{d}_q(T, \hat{Y} = y_j) := \sum_{i=1}^{k} (Q^{-1})_{ji} d^2_{\mathcal{Y}}(T, Y = y_i) \quad \forall y_j \in \mathcal{Y}, \quad (8)$$

$$\hat{F}_q(x, y) := \frac{1}{n} \sum_{i=1}^{n} \alpha_i(x) \hat{d}_q(y, \hat{z}_i) \quad \hat{f}_q(x) = \arg \min_{y \in \mathcal{Y}} \hat{F}_q(x, y). \quad (9)$$
We similarly define $\tilde{d}_p, \tilde{F}_p, \hat{f}_p$ using the true noise distribution $P$. The perturbed distance $\tilde{d}_p$ is an unbiased estimator of the true distance. However we do not know the true noise distribution $P$ hence we cannot use it for prediction. Instead we use $d_q$. Note that $d_q$ is no longer an unbiased estimator—its bias can be expressed as function of the parameter recovery error bound in Theorem 1.

### 4.2 Bounding the Generalization Error

What can we say about the excess risk $R(\hat{f}_q) - R(f^*)$? Note that compared to the prediction based on clean labels, there are two additional sources of error. One is the noise in the labels (i.e., even if we know the true $P$, the quality of the pseudolabels is imperfect). The other is our estimation procedure for the noise distribution. We must address both sources of error.

Our analysis uses the following assumptions on the minimum and maximum singular values $\sigma_{\min}(P)$, $\sigma_{\max}(P)$ and the condition number $\kappa(P)$ of true noise matrix $P$ and the function $F$. Additional detail is provided in the Appendix.

**Assumption 4.** (Noise model is not arbitrary) The true parameters $\theta$ are such that $\sigma_{\min}(P) > 0$, and the condition number $\kappa(P)$ is sufficiently small.

**Assumption 5.** (Normalized features) $|\alpha(x)| \leq 1$, for all $x \in \mathcal{X}$.

**Assumption 6.** (Proxy strong convexity) The function $F$ in (2) satisfies the following property with some $\beta > 0$. As we move away from the minimizer of $F$, the function increases and the rate of increase is proportional to the distance between the points:

$$F(x, f(x)) \geq F(x, \hat{f}(x)) + \beta \cdot d_{\Sigma}(f(x), \hat{f}(x)) \quad \forall x \in \mathcal{X}, \forall f \in \mathcal{F}.$$  

(10)

With these assumptions, we provide a generalization result for prediction with pseudolabels,

**Theorem 2.** (Generalization Error) Let $\hat{f}$ be the minimizer as defined in (2) over the clean labels and let $\hat{f}_q$ (defined in (9)) be the minimizer over the noisy labels obtained from inference in Algorithm 1. Suppose Assumptions 4, 5, 6 hold. Then for $c_2 = k^{3/2} \cdot \hat{O}(\epsilon(\alpha^+)) \cdot (1 + \frac{n(P)}{\sigma_{\min}(P)^2})$ and $c_1 = 1 + \frac{\sqrt{\kappa}}{\sigma_{\min}(P)}$, with high probability,

$$R(\hat{f}_q) \leq R(f^*) + \hat{O}(n^{-\frac{1}{2}}) + \hat{O}(\frac{c_1}{\beta} n^{-\frac{1}{2}}) + \hat{O}\left(\frac{3c_2}{\beta^2} n^{-\frac{1}{2}}\right).$$  

(11)

**Implications and Tradeoffs:** We interpret each term in the bound. The first term is present even with access to the clean labels and hence unavoidable. The second term is the additional error we incur if we learn with the knowledge of the true noise distribution. The third term is due to the use of the estimated noise model. It is dominated by the noise rate recovery result in Theorem 1. If the third term goes to 0 (perfect recovery) then we obtain the rate $\hat{O}(n^{-1/4})$, the same as in the case of access to clean labels. The third term is introduced by our noise rate recovery algorithm and has two terms: one dominated by $\hat{O}(n^{-1/2})$ and the other on $\hat{O}(\sqrt{\kappa}/d)$ (see discussion of Theorem 1). Thus we only pay an extra additive factor $\hat{O}(\sqrt{\kappa}/d)$ in the excess risk when using pseudolabels.

### 5 Manifold-Valued Label Spaces: Noise Recovery and Generalization

We introduce a simple recovery method for weak supervision in constant-curvature Riemannian manifolds. First we briefly introduce some background notation on these spaces, then provide our estimator and consistency result, then the downstream generalization result. Finally, we discuss extensions to symmetric Riemannian manifolds, an even more general class of spaces.

**Background on Riemannian manifolds.** The following is necessarily a very abridged background; more detail can be found in [Lee00, Tu11]. A smooth manifold $M$ is a space where each point is located in a neighborhood diffeomorphic to $\mathbb{R}^d$. Attached to each point $p \in M$ is a tangent space $T_pM$; each such tangent space is a $d$-dimensional vector space enabling the use of calculus.
A Riemannian manifold equips a smooth manifold with a Riemannian metric: a smoothly-varying inner product $\langle \cdot , \cdot \rangle_p$ at each point $p$. This tool allows us to compute angles, lengths, and ultimately, distances $d_M(p, q)$ between points on the manifold as shortest-path distances. These shortest paths are called geodesics and can be parametrized as curves $\gamma(t)$, where $\gamma(0) = p$, or by tangent vectors $v \in T_pM$. The exponential map operation $\exp : T_pM \to M$ takes tangent vectors to manifold points. It enables switching between these tangent vectors: $\exp_p(v) = q$ implies that $d_M(p, q) = \| v \|$. The logarithmic map operation $\log : M \to T_pM$ takes manifold points to tangent vectors. Further, $\exp_p(v) = q$ is equivalent to $\log_p(q) = v$.

**Invariant**  Our first contribution is a simple invariant that enables us to recover the error parameters. Note that we cannot rely on the finite metric-space technique, since the manifolds we consider have an infinite number of points. Nor do we need an embedding—we have a continuous representation as-is. This means it can be characterized by the (Riemannian) version of the Pythagorean theorem:

**Lemma 1.** For $\mathcal{Y} = M$, a hyperbolic manifold, $y \sim P$ for some distribution $P$ on $M$ and labeling functions $\lambda_a, \lambda_b$ drawn from $\{\}$, $\mathbb{E} \cosh d_M(\lambda_a, \lambda_b) = \mathbb{E} \cosh d_\mathcal{Y}(\lambda_a, y)\mathbb{E} \cosh d_\mathcal{Y}(\lambda_b, y)$, while for $\mathcal{Y} = M$ a spherical manifold, $\mathbb{E} \cos d_M(\lambda_a, \lambda_b) = \mathbb{E} \cos d_\mathcal{Y}(\lambda_a, y)\mathbb{E} \cos d_\mathcal{Y}(\lambda_b, y)$.

These invariants enable us to easily learn by forming a triplet system. Suppose we construct the equation in Lemma 1 for three pairs of labeling functions. The resulting system can be solved to express $\mathbb{E} \cosh(d_M(\lambda_a, y))$ in terms of $\mathbb{E} \cosh(d_M(\lambda_a, \lambda_b)), \mathbb{E} \cosh(d_M(\lambda_a, \lambda_c)), \mathbb{E} \cosh(d_M(\lambda_b, \lambda_c))$. Specifically,

$$
\mathbb{E} \cosh(d_M(\lambda_a, y)) = \sqrt{\frac{\mathbb{E} \cosh d_M(\lambda_a, \lambda_b)\mathbb{E} \cosh d_M(\lambda_a, \lambda_c)}{\mathbb{E} \cosh(d_M(\lambda_b, \lambda_c))}}.
$$

Note that we can estimate $\hat{\mathbb{E}}$ via the empirical versions of terms on the right, as these are based on observable quantities. This is a generalization of the binary case in [FCS-22] to hyperbolic manifolds. A similar estimator can be obtained for spherical manifolds by replacing $\cosh$ with $\log$.

Using this tool, we can obtain a consistent estimator for $\theta_a$ for each of $a = 1, \ldots, m$. Let $C_0$ satisfy $\mathbb{E}[\hat{\mathbb{E}} \cosh(d_M(\lambda_a, \lambda_b)) - \mathbb{E} \cosh(d_M(\lambda_a, \lambda_b))] \geq C_0\mathbb{E}[\hat{\mathbb{E}} d_M^2(\lambda_a, \lambda_b)] - d_M^2(\lambda_a, \lambda_b)$; that is, $C_0$ reflects the preservation of concentration when moving from distribution $\cosh(d)$ to $d^2$. Then,

**Theorem 3.** Let $M$ be a hyperbolic manifold. Fix $0 < \delta < 1$ and let $\Delta(\delta) = \min_p \Pr[\forall i, d_\mathcal{Y}(\lambda_a, i, \lambda_b, i) \leq \rho] \geq 1 - \delta$. Then, there exists a constant $C_1$ so that with probability at least $1 - \delta$, $\mathbb{E}[\hat{\mathbb{E}} d_M^2(\lambda_a, y)) - d_M^2(\lambda_a, y)] \leq C_1 \cosh(\Delta(\delta))^{3/2}/C_0\sqrt{2n}$.

As we hoped, our estimator is consistent. Note that we pay a price for a tighter bound: $\Delta(\delta)$ is large for smaller probability $\delta$. It is possible to estimate the size of $\Delta(\delta)$ (more generally, it is a function of the curvature). In addition, it is possible to replace the $\Delta(\delta)$ term by applying a version of McDiarmid’s inequality for unbounded spaces as in [Kon14].

Next, we adapt the downstream model predictor [2] in the following way. Let $\hat{\mu}_a^2 = \hat{\mathbb{E}}[d_M^2(\lambda_a, y)]$. Let $\beta = [\beta_1, \ldots, \beta_m]^T$ be such that $\sum_a \beta_a = 1$ and $\beta$ minimizes $\sum_a \beta_a^2 \hat{\mu}_a^2$. Then, we set

$$
\hat{f}(x) = \arg\min_{y \in \mathcal{Y}} \frac{1}{n} \sum_{i=1}^n \alpha_i(x) \sum_{a=1}^m \beta_a^2 d_M^2(y, \lambda_a, i).
$$

We simply replace each of the true labels with a combination of the labeling functions. With this, we can state our nal result. First, we introduce our assumptions.

Let $q = \arg\min_{y \in \mathcal{Y}} \mathbb{E}[\alpha(x)(y)d_\mathcal{Y}^2(z, y)]$, where the expression is taken over the population level distribution and $\alpha(x)(y)$ denotes the kernel at $y$.

**Assumption 7.**(Bounded Hugging Function c.f. [Str22]) Let $q$ be defined as above. For all $a, b \in M$, the hugging function at $q$ is given by $k_q^a(b) = 1 - (\| \log_q(a) - \log_q(b) \|^2 - d_\mathcal{Y}^2(a, b))/d_\mathcal{Y}^2(q, b)$. We assume that $k_q^a(a)$ is lower bounded by $k_{\min}$. 


Assumption 8. *(Kernel Symmetry)* We assume that for all \( x \) and all \( v \in T_q \mathcal{M} \), \( \alpha(x)(\exp_q(v)) = \alpha(x)(\exp_q(-v)) \).

The first condition provides control on how geodesic triangles behave; it relates to the curvature. We provide more details on this in the Appendix. The second assumption restricts us to kernels symmetric about the minimizers of the objective \( F \). Finally, suppose we draw \((x, y)\) and \((x', y')\) independently from \( P_{XY} \). Set \( \sigma^2_\alpha = \alpha(x)(y)\mathbb{E}d^2_{\alpha}(y, y') \).

**Theorem 4.** Let \( \mathcal{M} \) be a complete manifold and suppose the assumptions above hold. Then, there exist constants \( C_3, C_4 \) such that,

\[
\mathbb{E}[d^2_\alpha(\hat{f}(x), \hat{f}(x))] \leq \frac{C_3\sigma^2_\alpha + C_4 \sum_{a=1}^m \beta^2_a(\bar{\mu}^2_a + \sigma^2_\alpha)}{n(1 - k_{\min})^2}.
\]

Note that as \( n \) grows, as long as our worst-quality LF has bounded variance, our estimator of the true predictor is consistent. Moreover, we also have favorable dependence on the noise rate. This is because the only error we incur is in computing suboptimal \( \beta \) coefficients. We comment on this suboptimality in the Appendix.

A simple corollary of Theorem 4 provides the generalization guarantees we sought,

**Corollary 1.** Let \( \mathcal{M} \) be a complete manifold and suppose the assumptions above hold. Then, with high probability, \( R(\hat{f}) \leq R(f^*) + O(n^{-\frac{1}{2}}) \).

**Extensions to Other Manifolds** First, we note that all of our approaches almost immediately lift to products of constant-curvature spaces. For example, we have that \( \mathcal{M}_1 \times \mathcal{M}_2 \) has metric \( d^2_\mathcal{M}(p, q) = d^2_{\mathcal{M}_1}(p_1, q_1) + d^2_{\mathcal{M}_2}(p_2, q_2) \), where \( p_i, q_i \) are the projections of \( p, q \) onto the \( i \)th component.
Figure 3: Continuous case. Parameter estimation improves with more samples in the hyperbolic regression problem. Our estimator outperforms [SLV+22]. Here, we use different randomly sampled values of $\theta$ for each run. We report medians along with upper and lower quartiles across 10 trials.

We can go beyond products of constant-curvature spaces as well. To do so, we can build generalizations of the law of cosines (as needed for the invariance in Lemma[1]). For example, it is possible to do so for symmetric Riemannian manifolds using the tools in [AH91].

6 Experiments

Finally, we validate our theoretical claims with experimental results demonstrating improved parameter recovery and end model generalization using our techniques over that of prior work [SLV+22]. We illustrate both the finite metric space and continuous space cases by targeting rankings (i.e., permutations) and hyperbolic spaces. In the case of rankings we show that our pseudo-Euclidean embeddings with tensor decomposition estimator yields stronger parameter recovery and downstream generalization than [SLV+22]. In the case of hyperbolic regression (an example of a Riemannian manifold), we show that our estimator yields improved parameter recovery over [SLV+22].

Finite metric spaces: Learning to rank To experimentally evaluate our tensor decomposition estimator for finite metric spaces, we consider the problem of learning to rank. We construct a synthetic dataset whose ground truth comprises $n$ samples of two distinct rankings among the finite metric space of all length-four permutations. We construct three labeling functions by sampling rankings according to a Mallows model, for which we obtain pseudo-Euclidean embeddings to use with our tensor decomposition estimator.

In Figure 2 (top left), we show that as we increase the number of samples, we can obtain an increasingly accurate estimate of $T$—exhibiting the nearly-consistent behavior predicted by our theoretical claims. This leads to downstream improvements in parameter estimates, which also become more accurate as $n$ increases. In contrast, we find that the estimates of the same parameters given by [SLV+22] do not improve substantially as $n$ increases, and are ultimately worse (see Figure 2, top right). Finally, this leads to improvements in the label model accuracy as compared to that of [SLV+22], and translates to improved accuracy of an end model trained using synthetic samples (see Figure 2 bottom).

Riemannian manifolds: Hyperbolic regression We similarly evaluate our estimator using synthetic labels from a hyperbolic manifold, matching the setting of Section 5. As shown in Figure 3, we find that our estimator consistently outperforms that of [SLV+22], often by an order of magnitude.

7 Conclusion

We studied the theoretical properties of weak supervision applied to structured prediction in two general scenarios: label spaces that are finite metric spaces or constant-curvature manifolds. We introduced ways to estimate the noise rates of labeling functions, achieving consistency or near-consistency. Using these tools, we established that with suitable modifications downstream structured prediction models maintain generalization guarantees. Future directions include extending these results to even more general manifolds and removing some of the assumptions needed in our analysis.
Acknowledgments

We are grateful for the support of the NSF (CCF2106707), the American Family Funding Initiative and the Wisconsin Alumni Research Foundation (WARF). We are thankful to Changho Shin and Harshavardhan Adepu for the discussions and feedback.

References


Checklist

1. Do the main claims made in the abstract and introduction accurately reflect the paper’s contributions and scope? [Yes]
2. Did you describe the limitations of your work? [Yes]
3. Did you discuss any potential negative societal impacts of your work? [N/A]
4. Have you read the ethics review guidelines and ensured that your paper conforms to them? [Yes]
5. Did you state the full set of assumptions of all theoretical results? [Yes]
6. Did you include complete proofs of all theoretical results? [Yes] See appendix