Max-Margin Markov Networks

Ben Taskar Carlos Guestrin Daphne Koller
{*btaskar,guestrin,koller*}@*cs.stanford.edu*
Stanford University

Abstract

In typical classification tasks, we seek a function which assigns a label to a single object. Kernel-based approaches, such as support vector machines (SVMs), which maximize the margin of confidence of the classifier, are the method of choice for many such tasks. Their popularity stems both from the ability to use high-dimensional feature spaces, and from their strong theoretical guarantees. However, many real-world tasks involve sequential, spatial, or structured data, where multiple labels must be assigned. Existing kernel-based methods ignore structure in the problem, assigning labels independently to each object, losing much useful information. Conversely, probabilistic graphical models, such as Markov networks, can represent correlations between labels, by exploiting problem structure, but cannot handle high-dimensional feature spaces, and lack strong theoretical generalization guarantees. In this paper, we present a new framework that combines the advantages of both approaches: *Maximum margin Markov (M^3) networks* incorporate both kernels, which efficiently deal with high-dimensional features, and the ability to capture correlations in structured data. We present an efficient algorithm for learning M^3 networks based on a compact quadratic program formulation. We provide a new theoretical bound for generalization in structured domains. Experiments on the task of handwritten character recognition and collective hypertext classification demonstrate very significant gains over previous approaches.

1 Introduction

In supervised classification, our goal is to classify instances into some set of discrete categories. Recently, support vector machines (SVMs) have demonstrated impressive successes on a broad range of tasks, including document categorization, character recognition, image classification, and many more. SVMs owe a great part of their success to their ability to use kernels, allowing the classifier to exploit a very high-dimensional (possibly even infinite-dimensional) feature space. In addition to their empirical success, SVMs are also appealing due to the existence of strong generalization guarantees, derived from the margin-maximizing properties of the learning algorithm.

However, many supervised learning tasks exhibit much richer structure than a simple categorization of instances into one of a small number of classes. In some cases, we might need to label a set of inter-related instances. For example: optical character recognition (OCR) or part-of-speech tagging both involve labeling an entire sequence of elements into some number of classes; image segmentation involves labeling all of the pixels in an image; and collective webpage classification involves labeling an entire set of interlinked webpages. In other cases, we might want to label an instance (e.g., a news article) with multiple non-exclusive labels. In both of these cases, we need to assign multiple labels simultaneously, leading to a classification problem that has an exponentially large set of joint labels. A common solution is to treat such problems as a set of independent classification tasks, dealing with each instance in isolation. However, it is well-known that this approach fails to exploit significant amounts of correlation information [7].

An alternative approach is offered by the probabilistic framework, and specifically by probabilistic graphical models. In this case, we can define and learn a joint probabilistic model over the set of label variables. For example, we can learn a hidden Markov model, or a conditional random field (CRF) [7] over the labels and features of a sequence, and then use a probabilistic inference algorithm (such as the Viterbi algorithm) to classify these instances *collectively*, finding the most likely joint assignment to all of the labels simultaneously. This approach has the advantage of exploiting the correlations between the different labels, often resulting in significant improvements in accuracy over approaches that classify instances independently [7, 10]. The use of graphical models also allows problem structure to be exploited very effectively. Unfortunately, even probabilistic graphical models that are trained discriminatively do not usually achieve the same level of generalization accuracy as SVMs, especially when kernel features are used. Moreover, they are not (yet) associated with generalization bounds comparable to those of margin-based classifiers.

Clearly, the frameworks of kernel-based and probabilistic classifiers offer complementary strengths and weaknesses. In this paper, we present *maximum margin Markov (M^3) networks*, which unify the two frameworks, and combine the advantages of both. Our approach defines a log-linear Markov network over a set of label variables (e.g., the labels of the letters in an OCR problem); this network allows us to represent the correlations between these label variables. We then define a margin-based optimization problem for the parameters of this model. For Markov networks that can be triangulated tractably, the resulting quadratic program (QP) has an equivalent *polynomial*-size formulation (e.g., linear for sequences) that allows a very effective solution. By contrast, previous margin-based formulations for sequence labeling [3, 1] require an *exponential* number of constraints. For non-triangulated networks, we provide an approximate reformulation based on the relaxation used by belief propagation algorithms [8, 12]. Importantly, the resulting QP supports the same kernel trick as do SVMs, allowing probabilistic graphical models to inherit the important benefits of kernels. We also show a generalization bound for such margin-based classifiers. Unlike previous results [3], our bound grows logarithmically rather than linearly with the number of label variables. Our experimental results on character recognition and on hypertext classification, demonstrate dramatic improvements in accuracy over both kernel-based instance-by-instance classification and probabilistic models.

2 Structure in classification problems

In supervised classification, the task is to learn a function $h : \mathcal{X} \mapsto \mathcal{Y}$ from a set of m i.i.d. instances $S = \{(\mathbf{x}^{(i)}, \mathbf{y}^{(i)} = \mathbf{t}(\mathbf{x}^{(i)}))\}_{i=1}^{m}$, drawn from a fixed distribution $D_{\mathcal{X}\times\mathcal{Y}}$. The classification function h is typically selected from some parametric family $\mathcal{H}$. A common choice is the *linear family*: Given n real-valued basis functions $f_j : \mathcal{X} \times \mathcal{Y} \mapsto \mathbb{R}$, a hypothesis $h_{\mathbf{w}} \in \mathcal{H}$ is defined by a set of n coefficients w_j such that:

$$h_{\mathbf{w}}(\mathbf{x}) = \arg\max_{\mathbf{y}} \sum_{i=1}^{n} w_j f_j(\mathbf{x}, \mathbf{y}) = \arg\max_{\mathbf{y}} \mathbf{w}^\top \mathbf{f}(\mathbf{x}, \mathbf{y}) \ , \tag{1}$$

where the $\mathbf{f}(\mathbf{x}, \mathbf{y})$ are *features* or *basis functions*.

The most common classification setting — single-label classification — takes $\mathcal{Y} = \{y_1, \ldots, y_k\}$. In this paper, we consider the much more general setting of multi-label classification, where $\mathcal{Y} = \mathcal{Y}_1 \times \ldots \times \mathcal{Y}_l$ with $\mathcal{Y}_i = \{y_1, \ldots, y_k\}$. In an OCR task, for example, each $\mathcal{Y}_i$ is a character, while $\mathcal{Y}$ is a full word. In a webpage collective classification task [10], each $\mathcal{Y}_i$ is a webpage label, whereas $\mathcal{Y}$ is a joint label for an entire website. In these cases, the number of possible assignments to $\mathcal{Y}$ is exponential in the number of labels l. Thus, both representing the basis functions $f_j(\mathbf{x}, \mathbf{y})$ in (1) and computing the maximization $\arg\max_{\mathbf{y}}$ are infeasible.

An alternative approach is based on the framework of probabilistic graphical models. In this case, the model defines (directly or indirectly) a conditional distribution $P(\mathcal{Y} \mid \mathcal{X})$. We can then select the label $\arg\max_{\mathbf{y}} P(\mathbf{y} \mid \mathbf{x})$. The advantage of the probabilistic framework is that it can exploit sparseness in the correlations between labels $\mathcal{Y}_i$. For example, in the OCR task, we might use a Markov model, where $\mathcal{Y}_i$ is conditionally independent of the rest of the labels given $\mathcal{Y}_{i-1}, \mathcal{Y}_{i+1}$.

We can encode this structure using a *Markov network*. In this paper, purely for simplicity of presentation, we focus on the case of pairwise interactions between labels. We emphasize that our results extend easily to the general case. A *pairwise Markov network* is defined as a graph $\mathcal{G} = (\mathcal{Y}, E)$, where each edge (i,j) is associated with a potential function $\psi_{ij}(\mathbf{x}, y_i, y_j)$. The network encodes a joint conditional probability distribution as $P(\mathbf{y} \mid \mathbf{x}) \propto \prod_{(i,j)\in E} \psi_{ij}(\mathbf{x}, y_i, y_j)$. These networks exploit the interaction structure to parameterize a classifier very compactly. In many cases (e.g., tree-structured networks), we can use effective dynamic programming algorithms (such as the Viterbi algorithm) to find the highest probability label $\mathbf{y}$; in others, we can use approximate inference algorithms that also exploit the structure [12].

The Markov network distribution is simply a log-linear model, with the pairwise potential $\psi_{ij}(\mathbf{x}, y_i, y_j)$ representing (in log-space) a sum of basis functions over $\mathbf{x}, y_i, y_j$. We can therefore parameterize such a model using a set of pairwise basis functions $f(\mathbf{x}, y_i, y_j)$ for $(i,j) \in E$. We assume for simplicity of notation that all edges in the graph denote the same type of interaction, so that we can define a set of features

$$f_k(\mathbf{x}, \mathbf{y}) = \sum_{(i,j)\in E} f_k(\mathbf{x}, y_i, y_j). \tag{2}$$

The network potentials are then $\psi_{ij}(\mathbf{x}, y_i, y_j) = \exp\left[\sum_{k=1}^{n} w_k f_k(\mathbf{x}, y_i, y_j)\right] = \exp\left[\mathbf{w}^\top \mathbf{f}(\mathbf{x}, y_i, y_j)\right]$.

The parameters $\mathbf{w}$ in a log-linear model can be trained to fit the data, typically by maximizing the likelihood or conditional likelihood (e.g., [7, 10]). This paper presents an algorithm for selecting $\mathbf{w}$ that maximize the margin, gaining all of the advantages of SVMs.

3 Margin-based structured classification

For a single-label binary classification problem, support vector machines (SVMs) [11] provide an effective method of learning a maximum-margin decision boundary. For single-label multi-class classification, Crammer and Singer [5] provide a natural extension of this framework by maximizing the margin γ subject to constraints:

$$\text{maximize} \quad \gamma \quad \text{s.t.} \quad ||\mathbf{w}|| \le 1; \quad \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) \ge \gamma, \quad \forall\, \mathbf{x} \in S, \quad \forall \mathbf{y} \neq \mathbf{t}(\mathbf{x}); \tag{3}$$

where $\Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) = \mathbf{f}(\mathbf{x}, \mathbf{t}(\mathbf{x})) - \mathbf{f}(\mathbf{x}, \mathbf{y})$. The constraints in this formulation ensure that $\arg\max_{\mathbf{y}} \mathbf{w}^\top \mathbf{f}(\mathbf{x}, \mathbf{y}) = \mathbf{t}(\mathbf{x})$. Maximizing γ magnifies the difference between the value of the true label and the best runner-up, increasing the "confidence" of the classification.

In structured problems, where we are predicting multiple labels, the loss function is usually not simple 0-1 loss $I(\arg\max_{\mathbf{y}} \mathbf{w}^\top \mathbf{f}_{\mathbf{x}}(\mathbf{y}) = \mathbf{t}(\mathbf{x}))$, but per-label loss, such as the proportion of incorrect labels predicted. In order to extend the margin-based framework to the multi-label setting, we must generalize the notion of margin to take into account the number of labels in $\mathbf{y}$ that are misclassified. In particular, we would like the margin between $\mathbf{t}(\mathbf{x})$ and $\mathbf{y}$ to scale linearly with the number of wrong labels in $\mathbf{y}$, $\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y})$:

$$\text{maximize} \quad \gamma \quad \text{s.t.} \quad ||\mathbf{w}|| \le 1; \quad \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) \ge \gamma\, \Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}), \quad \forall \mathbf{x} \in S, \ \ \forall\, \mathbf{y}; \tag{4}$$

where $\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}) = \sum_{i=1}^{l} \Delta\mathbf{t}_{\mathbf{x}}(y_i)$ and $\Delta\mathbf{t}_{\mathbf{x}}(y_i) \equiv I(y_i \neq (\mathbf{t}(\mathbf{x}))_i)$. Now, using a standard transformation to eliminate γ, we get a quadratic program (QP):

$$\text{minimize} \ \ \frac{1}{2}||\mathbf{w}||^2 \quad \text{s.t.} \ \ \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) \ge \Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}), \ \ \forall \mathbf{x} \in S, \ \forall\, \mathbf{y}. \tag{5}$$

Unfortunately, the data is often not separable by a hyperplane defined over the space of the given set of features. In such cases, we need to introduce slack variables $\xi_{\mathbf{x}}$ to allow some constraints to be violated. We can now present the complete form of our optimization problem, as well as the equivalent dual problem [2]:

Primal formulation (6)

$$\min \quad \frac{1}{2}||\mathbf{w}||^2 + C\sum_{\mathbf{x}} \xi_{\mathbf{x}}\ ;$$
$$\text{s.t.}\ \ \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) \geq \Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}) - \xi_{\mathbf{x}},\ \forall \mathbf{x}, \mathbf{y}.$$

Dual formulation (7)

$$\max \ \sum_{\mathbf{x},\mathbf{y}} \alpha_{\mathbf{x}}(\mathbf{y})\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}) - \frac{1}{2}\left|\left|\sum_{\mathbf{x},\mathbf{y}} \alpha_{\mathbf{x}}(\mathbf{y})\Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y})\right|\right|^2;$$
$$\text{s.t.} \ \sum_{\mathbf{y}} \alpha_{\mathbf{x}}(\mathbf{y}) = C, \forall \mathbf{x}; \quad \alpha_{\mathbf{x}}(\mathbf{y}) \geq 0\ , \forall \mathbf{x}, \mathbf{y}.$$

(Note: for each $\mathbf{x}$, we add an extra dual variable $\alpha_{\mathbf{x}}(\mathbf{t}(\mathbf{x}))$, with no effect on the solution.)

4 Exploiting structure in M^3 networks

Unfortunately, both the number of constraints in the primal QP in (6), and the number of variables in the dual QP in (7) are exponential in the number of labels l. In this section, we present an equivalent, polynomially-sized, formulation.

Our main insight is that the variables $\alpha_{\mathbf{x}}(\mathbf{y})$ in the dual formulation (7) can be interpreted as a density function over $\mathbf{y}$ conditional on $\mathbf{x}$, as $\sum_{\mathbf{y}} \alpha_{\mathbf{x}}(\mathbf{y}) = C$ and $\alpha_{\mathbf{x}}(\mathbf{y}) \geq 0$. The dual objective is a function of expectations of $\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y})$ and $\Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y})$ with respect to $\alpha_{\mathbf{x}}(\mathbf{y})$. Since both $\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}) = \sum_i \Delta\mathbf{t}_{\mathbf{x}}(y_i)$ and $\Delta\mathbf{f}_{\mathbf{x}}(\mathbf{y}) = \sum_{(i,j)} \Delta\mathbf{f}_{\mathbf{x}}(y_i, y_j)$ are sums of functions over nodes and edges, we only need node and edge marginals of the measure $\alpha_{\mathbf{x}}(\mathbf{y})$ to compute their expectations. We define the marginal dual variables as follows:

$$\begin{array}{lcll} \mu_{\mathbf{x}}(y_i, y_j) & = & \sum_{\mathbf{y}\sim[y_i,y_j]} \alpha_{\mathbf{x}}(\mathbf{y}), & \forall\ (i,j) \in E, \forall y_i, y_j,\ \ \forall\ \mathbf{x}; \\ \mu_{\mathbf{x}}(y_i) & = & \sum_{\mathbf{y}\sim[y_i]} \alpha_{\mathbf{x}}(\mathbf{y}), & \quad \forall\ i,\ \forall y_i,\ \ \forall\ \mathbf{x}; \end{array} \tag{8}$$

where $\mathbf{y} \sim [y_i, y_j]$ denotes a full assignment $\mathbf{y}$ consistent with partial assignment y_i, y_j.

Now we can reformulate our entire QP (7) in terms of these dual variables. Consider, for example, the first term in the objective function:

$$\sum_{\mathbf{y}} \alpha_{\mathbf{x}}(\mathbf{y})\Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y}) = \sum_{\mathbf{y}}\sum_{i} \alpha_{\mathbf{x}}(\mathbf{y})\Delta\mathbf{t}_{\mathbf{x}}(y_i) = \sum_{i,y_i} \Delta\mathbf{t}_{\mathbf{x}}(y_i) \sum_{\mathbf{y}\sim[y_i]} \alpha_{\mathbf{x}}(\mathbf{y}) = \sum_{i,y_i} \mu_{\mathbf{x}}(y_i)\Delta\mathbf{t}_{\mathbf{x}}(y_i).$$

The decomposition of the second term in the objective uses edge marginals $\mu_{\mathbf{x}}(y_i, y_j)$.

In order to produce an equivalent QP, however, we must also ensure that the dual variables $\mu_{\mathbf{x}}(y_i, y_j), \mu_{\mathbf{x}}(y_i)$ are the marginals resulting from a legal density $\alpha(\mathbf{y})$; that is, that they belong to the *marginal polytope* [4]. In particular, we must enforce consistency between the pairwise and singleton marginals (and hence between overlapping pairwise marginals):

$$\sum_{y_i} \mu_{\mathbf{x}}(y_i, y_j) = \mu_{\mathbf{x}}(y_j),\ \forall y_j, \quad \forall (i,j) \in E,\ \forall \mathbf{x}. \tag{9}$$

If the Markov network for our basis functions is a forest (singly connected), these constraints are equivalent to the requirement that the μ variables arise from a density. Therefore, the following factored dual QP is equivalent to the original dual QP:

$$\max \quad \sum_{\mathbf{x}}\sum_{i,y_i} \mu_{\mathbf{x}}(y_i)\Delta\mathbf{t}_{\mathbf{x}}(y_i) - \frac{1}{2}\sum_{\mathbf{x},\hat{\mathbf{x}}}\sum_{\substack{(i,j)\\ y_i,y_j}}\sum_{\substack{(r,s)\\ y_r,y_s}} \mu_{\mathbf{x}}(y_i, y_j)\mu_{\hat{\mathbf{x}}}(y_r, y_s)\mathbf{f}_{\mathbf{x}}(y_i, y_j)^\top \mathbf{f}_{\hat{\mathbf{x}}}(y_r, y_s);$$
$$\text{s.t.} \quad \sum_{y_i} \mu_{\mathbf{x}}(y_i, y_j) = \mu_{\mathbf{x}}(y_j); \quad \sum_{y_i} \mu_{\mathbf{x}}(y_i) = C; \quad \mu_{\mathbf{x}}(y_i, y_j) \geq 0. \tag{10}$$

Similarly, the original primal can be factored as follows:

$$\begin{aligned} \min \quad & \frac{1}{2}||\mathbf{w}||^2 + C\sum_{\mathbf{x}}\sum_{i} \xi_{\mathbf{x},i} + C\sum_{\mathbf{x}}\sum_{(i,j)} \xi_{\mathbf{x},ij}; \\ \text{s.t.} \quad & \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}}(y_i, y_j) + \sum_{(i',j):i'\neq i} m_{\mathbf{x},i'}(y_j) + \sum_{(j',i):j'\neq j} m_{\mathbf{x},j'}(y_i) \geq -\xi_{\mathbf{x},ij}; \\ & \sum_{(i,j)} m_{\mathbf{x},j}(y_i) \geq \Delta\mathbf{t}_{\mathbf{x}}(y_i) - \xi_{\mathbf{x},i}; \qquad \xi_{\mathbf{x},ij} \geq 0, \xi_{\mathbf{x},i} \geq 0. \end{aligned} \tag{11}$$

The solution to the factored dual gives us: $\mathbf{w} = \sum_{\mathbf{x}}\sum_{(i,j)}\sum_{y_i,y_j} \mu_{\mathbf{x}}(y_i, y_j)\Delta\mathbf{f}_{\mathbf{x}}(y_i, y_j)$.

Theorem 4.1 *If for each* $\mathbf{x}$ *the edges* E *form a forest, then a set of weights* $\mathbf{w}$ *will be optimal for the QP in (6) if and only if it is optimal for the factored QP in (11).* ∎

If the underlying Markov net is not a forest, then the constraints in (9) are not sufficient to enforce the fact that the μ's are in the marginal polytope. We can address this problem by triangulating the graph, and introducing new η LP variables that now span larger subsets of Y_i's. For example, if our graph is a 4-cycle Y_1—Y_2—Y_3—Y_4—Y_1, we might triangulate the graph by adding an arc Y_1—Y_3, and introducing η variables over joint instantiations of the cliques Y_1, Y_2, Y_3 and Y_1, Y_3, Y_4. These new η variables are used in linear equalities that constrain the original μ variables to be consistent with a density. The η variables appear only in the constraints; they do not add any new basis functions nor change the objective function. The number of constraints introduced is exponential in the number of variables in the new cliques. Nevertheless, in many classification problems, such as sequences and other graphs with low tree-width [4], the extended QP can be solved efficiently.

Unfortunately, triangulation is not feasible in highly connected problems. However, we can still solve the QP in (10) defined by an untriangulated graph with loops. Such a procedure, which enforces only local consistency of marginals, optimizes our objective only over a relaxation of the marginal polytope. In this way, our approximation is analogous to the approximate belief propagation (BP) algorithm for inference in graphical models [8]. In fact, BP makes an additional approximation, using not only the relaxed marginal polytope but also an approximate objective (Bethe free-energy) [12]. Although the approximate QP does not offer the theoretical guarantee in Theorem 4.1, the solutions are often very accurate in practice, as we demonstrate below.

As with SVMs [11], the factored dual formulation in (10) uses only dot products between basis functions. This allows us to use a kernel to define very large (and even infinite) set of features. In particular, we define our basis functions by $\mathbf{f}_\mathbf{x}(y_i, y_j) = \rho(y_i, y_j)\phi^{ij}(\mathbf{x})$, i.e., the product of a selector function $\rho(y_i, y_j)$ with a possibly infinite feature vector $\phi^{ij}(\mathbf{x})$. For example, in the OCR task, $\rho(y_i, y_j)$ could be an indicator function over the class of two adjacent characters i and j, and $\phi^{ij}(\mathbf{x})$ could be an RBF kernel on the images of these two characters. The operation $\mathbf{f}_\mathbf{x}(y_i, y_j)^\top \mathbf{f}_{\hat{\mathbf{x}}}(y_r, y_s)$ used in the objective function of the factored dual QP is now $\rho(y_i, y_j)\rho(y_r, y_s)K_\phi(\mathbf{x}, i, j, \hat{\mathbf{x}}, r, s)$, where $K_\phi(\mathbf{x}, i, j, \hat{\mathbf{x}}, r, s) = \phi^{ij}(\mathbf{x}) \cdot \phi^{rs}(\mathbf{x})$ is the kernel function for the feature ϕ. Even for some very complex functions ϕ, the dot-product required to compute K_ϕ can be executed efficiently [11].

5 SMO learning of M^3 networks

Although the number of variables and constraints in the factored dual in (10) is polynomial in the size of the data, the number of coefficients in the quadratic term (kernel matrix) in the objective is quadratic in the number of examples and edges in the network. Unfortunately, this matrix is often too large for standard QP solvers. Instead, we use a coordinate descent method analogous to the sequential minimal optimization (SMO) used for SVMs [9].

Let us begin by considering the original dual problem (7). The SMO approach solves this QP by analytically optimizing two-variable subproblems. Recall that $\sum_\mathbf{y} \alpha_\mathbf{x}(\mathbf{y}) = C$. We can therefore take any two variables $\alpha_\mathbf{x}(\mathbf{y}^1)$, $\alpha_\mathbf{x}(\mathbf{y}^2)$ and "move weight" from one to the other, keeping the values of all other variables fixed. More precisely, we optimize for $\alpha'_\mathbf{x}(\mathbf{y}^1), \alpha'_\mathbf{x}(\mathbf{y}^2)$ such that $\alpha'_\mathbf{x}(\mathbf{y}^1) + \alpha'_\mathbf{x}(\mathbf{y}^2) = \alpha_\mathbf{x}(\mathbf{y}^1) + \alpha_\mathbf{x}(\mathbf{y}^2)$.

Clearly, however, we cannot perform this optimization in terms of the original dual, which is exponentially large. Fortunately, we can perform precisely the same optimization in terms of the marginal dual variables. Let $\lambda = \alpha'_\mathbf{x}(\mathbf{y}^1) - \alpha_\mathbf{x}(\mathbf{y}^1) = \alpha_\mathbf{x}(\mathbf{y}^2) - \alpha'_\mathbf{x}(\mathbf{y}^2)$. Consider a dual variable $\mu_\mathbf{x}(y_i, y_j)$. It is easy to see that a change from $\alpha_\mathbf{x}(\mathbf{y}^1), \alpha_\mathbf{x}(\mathbf{y}^2)$ to $\alpha'_\mathbf{x}(\mathbf{y}^1), \alpha'_\mathbf{x}(\mathbf{y}^2)$ has the following effect on $\mu_\mathbf{x}(y_i, y_j)$:

$$\mu'_\mathbf{x}(y_i, y_j) = \mu_\mathbf{x}(y_i, y_j) + \lambda I(y_i = y_i^1, y_j = y_j^1) - \lambda I(y_i = y_i^2, y_j = y_j^2). \quad (12)$$

We can solve the one-variable quadratic subproblem in λ analytically and update the appropriate μ variables. We use inference in the network to test for optimality of the current solution (the KKT conditions [2]) and use violations from optimality as a heuristic to select the next pair $\mathbf{y}^1, \mathbf{y}^2$. We omit details for lack of space.

6 Generalization bound

In this section, we show a generalization bound for the task of multi-label classification that allows us to relate the error rate on the training set to the generalization error. As we shall see, this bound is significantly stronger than previous bounds for this problem.

Our goal in multi-label classification is to maximize the number of correctly classified labels. Thus an appropriate error function is the *average per-label loss* $\mathcal{L}(\mathbf{w}, \mathbf{x}) = \frac{1}{l}\Delta\mathbf{t}_{\mathbf{x}}(\arg\max_{\mathbf{y}} \mathbf{w}^\top \mathbf{f}_{\mathbf{x}}(\mathbf{y}))$. As in other generalization bounds for margin-based classifiers, we relate the generalization error to the margin of the classifier. In Sec. 3, we define the notion of per-label margin, which grows with the number of mistakes between the correct assignment and the best runner-up. We can now define a γ-*margin per-label loss*:

$$\mathcal{L}^\gamma(\mathbf{w}, \mathbf{x}) = \sup_{\mathbf{v}:\ |\mathbf{v}(\mathbf{y}) - \mathbf{w}^\top \mathbf{f}_{\mathbf{x}}(\mathbf{y})| \leq \gamma \Delta\mathbf{t}_{\mathbf{x}}(\mathbf{y});\ \forall \mathbf{y}} \frac{1}{l}\Delta\mathbf{t}_{\mathbf{x}}(\arg\max_{\mathbf{y}} \mathbf{v}(\mathbf{y})).$$

This loss function measures the worst per-label loss on $\mathbf{x}$ made by any classifier z which is perturbed from $\mathbf{w}^\top \mathbf{f}_{\mathbf{x}}$ by at most a γ-margin per-label. We can now prove that the generalization accuracy of any classifier is bounded by its expected γ-margin per-label loss on the training data, plus a term that grows inversely with the margin.Intuitively, the first term corresponds to the "bias", as margin γ decreases the complexity of our hypothesis class by considering a γ-per-label margin ball around $\mathbf{w}^\top \mathbf{f}_{\mathbf{x}}$ and selecting one (the worst) classifier within this ball. As γ shrinks, our hypothesis class becomes more complex, and the first term becomes smaller, but at the cost of increasing the second term, which intuitively corresponds to the "variance". Thus, the result provides a bound to the generalization error that trades off the *effective* complexity of the hypothesis space with the training error.

Theorem 6.1 *If the edge features have bounded 2-norm,* $\max_{(i,j),y_i,y_j} \|\mathbf{f}_{\mathbf{x}}(y_i, y_j)\|_2 \leq R_{edge}$*, then for a family of hyperplanes parameterized by* $\mathbf{w}$*, and any* $\delta > 0$*, there exists a constant* K *such that for any* $\gamma > 0$ *per-label margin, and* $m > 1$ *samples, the per-label loss is bounded by:*

$$E_{\mathbf{x}}\mathcal{L}(\mathbf{w}, \mathbf{x}) \quad \leq \quad E_S\mathcal{L}^\gamma(\mathbf{w}, \mathbf{x}) + \sqrt{\frac{K}{m}\left[\frac{R_{edge}^2 \|\mathbf{w}\|_2^2 q^2}{\gamma^2}\left[\ln m + \ln l + \ln q + \ln k\right] + \ln\frac{1}{\delta}\right]}\ ;$$

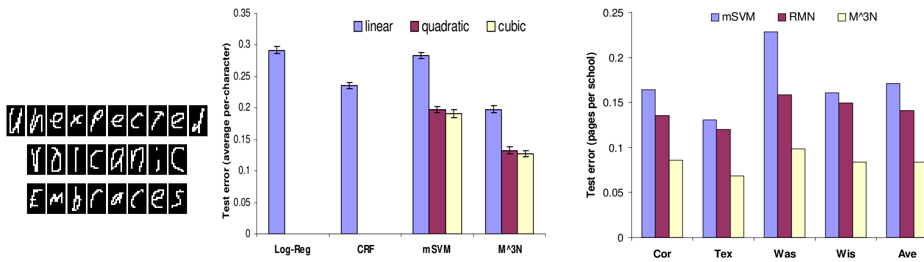
with probability at least $1-\delta$*, where* $q = \max_i |\{(i,j) \in E\}|$ *is the maximum edge degree in the network,* k *is the number of classes in a label, and* l *is the number of labels.* ∎

Proof: See Appendix. ∎

The proof uses a covering number argument analogous to previous results in SVMs [13]. However we propose a novel method for covering structured problems by constructing a cover to the loss function from a cover of the individual edge basis function differences $\Delta\mathbf{f}_{\mathbf{x}}(y_i, y_j)$. This new type of cover is polynomial in the number of edges, yielding significant improvements in the bound. Specifically, our bound has a logarithmic dependence on the number of labels ($\ln l$) and depends only on the 2-norm of the basis functions per-edge (R_{edge}). This is a significant gain over the previous result of Collins [3] which has linear dependence on the number of labels (l), and depends on the joint 2-norm of all of the features (which is $\sim lR_{edge}$, unless each sequence is normalized separately, which is often ineffective in practice). Finally, note that if $\frac{l}{m} = \mathcal{O}(1)$ (for example, in OCR, if the number of instances is at least a constant times the length of a word), then our bound is independent of the number of labels l. Such a result was, until now, an open problem for margin-based sequence classification [3].

7 Experiments

We evaluate our approach on two very different tasks: a sequence model for handwriting recognition and an arbitrary topology Markov network for hypertext classification.



(a) (b) (c)

Figure 1: (a) 3 example words from the OCR data set; (b) OCR: Average per-character test error for logistic regression, CRFs, multiclass SVMs, and M^{3}Ns, using linear, quadratic, and cubic kernels; (c) Hypertext: Test error for multiclass SVMs, RMNs and M^{3}Ns, by school and average.

Handwriting Recognition. We selected a subset of ~ 6100 handwritten words, with average length of ~ 8 characters, from 150 human subjects, from the data set collected by Kassel [6]. Each word was divided into characters, each character was rasterized into an image of 16 by 8 binary pixels. (See Fig. 1(a).) In our framework, the image for each word corresponds to $\mathbf{x}$, a label of an individual character to $\mathcal{Y}_i$, and a labeling for a complete word to $\mathcal{Y}$. Each label $\mathcal{Y}_i$ takes values from one of 26 classes $\{a, \ldots, z\}$.

The data set is divided into 10 folds of ~ 600 training and ~ 5500 testing examples. The accuracy results, summarized in Fig. 1(b), are averages over the 10 folds. We implemented a selection of state-of-the-art classification algorithms: *independent label approaches*, which do not consider the correlation between neighboring characters — logistic regression, multi-class SVMs as described in (3), and one-against-all SVMs (whose performance was slightly lower than multi-class SVMs); and *sequence approaches* — CRFs, and our proposed M^3 networks. Logistic regression and CRFs are both trained by maximizing the conditional likelihood of the labels given the features, using a zero-mean diagonal Gaussian prior over the parameters, with a standard deviation between 0.1 and 1. The other methods are trained by margin maximization. Our features for each label $\mathcal{Y}_i$ are the corresponding image of ith character. For the sequence approaches (CRFs and M^3), we used an indicator basis function to represent the correlation between $\mathcal{Y}_i$ and $\mathcal{Y}_{i+1}$. For margin-based methods (SVMs and M^3), we were able to use kernels (both quadratic and cubic were evaluated) to increase the dimensionality of the feature space. Using these high-dimensional feature spaces in CRFs is not feasible because of the enormous number of parameters.

Fig. 1(b) shows two types of gains in accuracy: First, by using kernels, margin-based methods achieve a very significant gain over the respective likelihood maximizing methods. Second, by using sequences, we obtain another significant gain in accuracy. Interestingly, the error rate of our method using linear features is 16% lower than that of CRFs, and about the same as multi-class SVMs with cubic kernels. Once we use cubic kernels our error rate is 45% lower than CRFs and about 33% lower than the best previous approach. For comparison, the previously published results, although using a different setup (e.g., a larger training set), are about comparable to those of multiclass SVMs.

Hypertext. We also tested our approach on collective hypertext classification, using the data set in [10], which contains web pages from four different Computer Science departments. Each page is labeled as one of course, faculty, student, project, other. In all of our experiments, we learn a model from three schools, and test on the remaining school. The text content of the web page and anchor text of incoming links is represented using a set of binary attributes that indicate the presence of different words. The baseline model is a simple linear multi-class SVM that uses only words to predict the category of the page. The second model is a *relational* Markov network (RMN) of Taskar *et al.* [10], which in addition to word-label dependence, has an edge with a potential over the labels of two pages that are hyper-linked to each other. This model defines a Markov network over each web site that was trained to maximize the conditional probability of the labels given the words and the links. The third model is a M^3 net with the same features but trained by maximizing the margin using the relaxed dual formulation and loopy BP for inference.

Fig. 1(c) shows a gain in accuracy from SVMs to RMNs by using the correlations between labels of linked web pages, and a very significant additional gain by using maximum margin training. The error rate of M3Ns is 40% lower than that of RMNs, and 51% lower than multi-class SVMs.

8 Discussion

We present a discriminative framework for labeling and segmentation of structured data such as sequences, images, etc. Our approach seamlessly integrates state-of-the-art kernel methods developed for classification of independent instances with the rich language of graphical models that can exploit the structure of complex data. In our experiments with the OCR task, for example, our sequence model significantly outperforms other approaches by incorporating high-dimensional decision boundaries of polynomial kernels over character images while capturing correlations between consecutive characters. We construct our models by solving a convex quadratic program that maximizes the *per-label margin*. Although the number of variables and constraints of our QP formulation is polynomial in the example size (e.g., sequence length), we also address its quadratic growth using an effective optimization procedure inspired by SMO. We provide theoretical guarantees on the average *per-label* generalization error of our models in terms of the training set margin. Our generalization bound significantly tightens previous results of Collins [3] and suggests possibilities for analyzing per-label generalization properties of graphical models.

For brevity, we simplified our presentation of graphical models to only pairwise Markov networks. Our formulation and generalization bound easily extend to interaction patterns involving more than two labels (e.g., higher-order Markov models). Overall, we believe that M^3 networks will significantly further the applicability of high accuracy margin-based methods to real-world structured data.

Acknowledgments. This work was supported by ONR Contract F3060-01-2-0564-P00002 under DARPA's EELD program.

References

[1] Y. Altun, I. Tsochantaridis, and T. Hofmann. Hidden markov support vector machines. In *Proc. ICML*, 2003.

[2] D. Bertsekas. *Nonlinear Programming*. Athena Scientific, Belmont, MA, 1999.

[3] M. Collins. Parameter estimation for statistical parsing models: Theory and practice of distribution-free methods. In *IWPT*, 2001.

[4] R.G. Cowell, A.P. Dawid, S.L. Lauritzen, and D.J. Spiegelhalter. *Probabilistic Networks and Expert Systems*. Springer, New York, 1999.

[5] K. Crammer and Y. Singer. On the algorithmic implementation of multiclass kernelbased vector machines. *Journal of Machine Learning Research*, 2(5):265–292, 2001.

[6] R. Kassel. *A Comparison of Approaches to On-line Handwritten Character Recognition*. PhD thesis, MIT Spoken Language Systems Group, 1995.

[7] J. Lafferty, A. McCallum, and F. Pereira. Conditional random fields: Probabilistic models for segmenting and labeling sequence data. In *Proc. ICML01*, 2001.

[8] J. Pearl. *Probabilistic Reasoning in Intelligent Systems*. Morgan Kaufmann, 1988.

[9] J. Platt. Using sparseness and analytic QP to speed training of support vector machines. In *NIPS*, 1999.

[10] B. Taskar, P. Abbeel, and D. Koller. Discriminative probabilistic models for relational data. In *Proc. UAI02*, Edmonton, Canada, 2002.

[11] V.N. Vapnik. *The Nature of Statistical Learning Theory*. Springer-Verlag, New York, 1995.

[12] J. Yedidia, W. Freeman, and Y. Weiss. Generalized belief propagation. In *NIPS*, 2000.

[13] T. Zhang. Covering number bounds of certain regularized linear function classes. *Journal of Machine Learning Research*, 2:527–550, 2002.

A Proof of Theorem 6.1

The proof of Theorem 6.1 uses the covering number bounds of Zhang [13] (in the Data-Dependent Structural Risk Minimization framework.)[1] Zhang provides generalization guarantees for linear binary classifiers of the form $h_{\mathbf{w}}(\mathbf{x}) = \operatorname{sgn}(\mathbf{w}^\top \mathbf{x})$. His analysis is based on the upper bounds on the covering number for the class of linear functions $\mathcal{F}_L(\mathbf{w}, \mathbf{z}) = \mathbf{w}^\top \mathbf{z}$ where the norms of the vectors $\mathbf{w}$ and $\mathbf{z}$ are bounded. We reproduce the relevant definitions and theorems from [13] here to highlight the necessary extensions for structured classification.

The covering number is a key quantity in measuring function complexity. Intuitively, the covering number of an infinite class of functions (e.g. parameterized by a set of weights $\mathbf{w}$) is the number of vectors necessary to approximate the values of any function in the class on a sample. Margin-based analysis of generalization error uses the margin achieved by a classifier on the training set to approximate the original function class of the classifier by a finite covering with precision that depends on the margin. Here, we will only define the ∞-norm covering number.

A.1 Binary classification

In binary classification, we are given a sample $S = \{\mathbf{x}^{(i)}, t(\mathbf{x}^{(i)})\}_{i=1}^m$, where $\mathbf{x} \in \mathbb{R}^n$, $t(\mathbf{x}) = \pm 1$, so we can fold $\mathbf{x}$ and $t(\mathbf{x})$ into $\mathbf{z} = \mathbf{x} \cdot t(\mathbf{x})$.

Definition A.1 (Covering Number) *Let $\mathcal{V} = \{\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(r)}\}$, where $\mathbf{v}^{(j)} \in \mathbb{R}^m$, be a* covering *of a function class $\mathcal{F}(\mathbf{w}, S)$ with ϵ-precision under the metric ρ, if for all $\mathbf{w}$ there exists a $\mathbf{v}^{(j)}$ such that that for each data sample $\mathbf{z}^{(i)} \in S$:*

$$\rho(\mathbf{v}_i^{(j)}, \mathcal{F}(\mathbf{w}, \mathbf{z}^{(i)}) \leq \epsilon.$$

The covering number of a sample S *is the size of the smallest covering: $\mathcal{N}_\infty(\mathcal{F}, \rho, \epsilon, S) = \inf |\mathcal{V}|$ s.t. $\mathcal{V}$ is a covering of $\mathcal{F}(\mathbf{w}, S)$. We also define the* covering number for any sample of size m*: $\mathcal{N}_\infty(\mathcal{F}, \rho, \epsilon, m) = \sup_{S:\, |S|=m} \mathcal{N}_\infty(\mathcal{F}, \rho, \epsilon, S)$.* ∎

When the norms of $\mathbf{w}$ and $\mathbf{z}$ are bounded, we have the following upper bound on the covering number of linear functions under the linear metric $\rho_L(v, v') = |v - v'|$.

Theorem A.2 (Theorem 4 from [13]) *If $\|\mathbf{w}\|_2 \leq a$ and $\|\mathbf{z}\|_2 \leq b$, then $\forall\, \epsilon > 0$,*

$$\log_2 \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, m) \leq 36 \frac{a^2 b^2}{\epsilon^2} \log_2 \left(2 \left\lceil 4ab/\epsilon + 2 \right\rceil m + 1\right). \quad ∎$$

In order to use the the classifier's margin to bound its expected loss, the bounds below use a stricter, margin-based loss on the training sample that measures the worst loss achieved by the approximate covering based on this margin. Let $f : \mathbb{R} \mapsto [0, 1]$ be a loss function. In binary classification, we let $f(z) = I(v \leq 0)$ be the step function, so that 0-1 loss of $\operatorname{sgn}(\mathbf{w}^\top \mathbf{x})$ is $f(\mathcal{F}_L(\mathbf{w}, \mathbf{z}))$. The next theorem bounds the expected f loss in terms of the γ-margin loss, $f^\gamma(z) = \sup_{\rho(z,z') < 2\gamma} f(z')$, on the training sample. For 0-1 loss and linear metric ρ_L, the corresponding γ-margin loss is $f^\gamma(z) = I(z \leq 2\gamma)$.

Theorem A.3 (Corollary 1 from [13]) *Let $f : \mathbb{R} \mapsto [0, 1]$ be a loss function and $f^\gamma(z) = \sup_{\rho(z,z') < 2\gamma} f(z')$ be the γ-margin loss for a metric ρ. Let $\gamma_1 > \gamma_2 > \ldots$ be a decreasing sequence of parameters, and p_i be a sequence of positive numbers such that $\sum_{i=1}^\infty p_i = 1$, then for all $\delta > 0$, with probability of at least $1 - \delta$ over data:*

$$E_{\mathbf{z}} f(\mathcal{F}(\mathbf{w}, \mathbf{z})) \quad \leq \quad E_S f^\gamma(\mathcal{F}(\mathbf{w}, \mathbf{z})) + \sqrt{\frac{32}{m} \left[\ln 4\mathcal{N}_\infty(\mathcal{F}, \rho, \gamma_i, S) + \ln \frac{1}{p_i \delta}\right]}$$

for all $\mathbf{w}$ and γ, where for each fixed γ, we use i to denote the smallest index s.t. $\gamma_i \leq \gamma$.

[1] J. Shawe-Taylor, P. L. Bartlett, R. C. Williamson, and M. Anthony. Structural risk minimization over data-dependent hierarchies. *IEEE Trans. on Information Theory*, 44(5):1926–1940, 1998.

A.2 Structured classification

We will extend this framework to bound the average per-label loss for structured classification by defining an appropriate loss f and a function class $\mathcal{F}$ (as well as a metric ρ) such that $f(\mathcal{F})$ computes average per-label loss and $f^\gamma(\mathcal{F})$ provides a suitable γ-margin loss. We will bound the corresponding covering number by building on the bound in Theorem A.2.

We can no longer simply fold $\mathbf{x}$ and $\mathbf{t}(\mathbf{x})$, since $\mathbf{t}(\mathbf{x})$ is a vector, so we let $\mathbf{z} = (\mathbf{x}, \mathbf{t}(\mathbf{x}))$. In order for our loss function to compute average per-label loss, it is convenient to make our function class *vector-valued* (instead of scalar-valued as above). We define a new function class $\mathcal{F}_M(\mathbf{w}, \mathbf{z})$, which is a vector of minimum values of $\mathbf{w}^\top \Delta\mathbf{f}_\mathbf{x}(\mathbf{y})$ for each error level $\Delta\mathbf{t}_\mathbf{x}(\mathbf{y})$ from 1 to l as described below.

Definition A.4 (dth-error-level function) *The* dth-error-level function $M_d(\mathbf{w}, \mathbf{z})$ *for* $d \in \{1, \ldots, l\}$ *is given by:*

$$M_d(\mathbf{w}, \mathbf{z}) = \min_{\mathbf{y}:\Delta\mathbf{t}_\mathbf{x}(\mathbf{y})=d} \mathbf{w}^\top \Delta\mathbf{f}_\mathbf{x}(\mathbf{y}). \quad \blacksquare$$

Definition A.5 (Multi-error-level function class) *The* multi-error-level function class $\mathcal{F}_M(\mathbf{w}, \mathbf{z})$ *is given by:*

$$\mathcal{F}_M(\mathbf{w}, \mathbf{z}) = \left(M_1(\mathbf{w}, \mathbf{z}), \ldots, M_d(\mathbf{w}, \mathbf{z}), \ldots, M_l(\mathbf{w}, \mathbf{z})\right). \quad \blacksquare$$

We can now compute the average per-label loss from $\mathcal{F}_M(\mathbf{w}, \mathbf{z})$ by defining an appropriate loss function f.

Definition A.6 (Average per-label loss) *The* average per-label loss $f : I\!R^{\,l} \mapsto [0, 1]$ *is given by:*

$$f(\mathbf{z}) = \frac{1}{l} \arg \min_{d:z_d \le 0} z_d,$$

where in case $\forall d, \quad z_d > 0$*, we define* $\arg\min_{d:z_d\le 0} z_d \equiv 0$. $\blacksquare$

With the above definitions, the average per-label loss

$$f(\mathcal{F}_M(\mathbf{w}, \mathbf{z})) = \frac{1}{l} \arg \min_{d, M_d(\mathbf{w},\mathbf{z}) \le 0} M_d(\mathbf{w}, \mathbf{z}) = \frac{1}{l} \Delta\mathbf{t}_\mathbf{x}\big(\arg\min_{\mathbf{y}} \mathbf{w}^\top \Delta\mathbf{f}_\mathbf{x}(\mathbf{y})\big),$$

as desired. Note that the case $\forall d, \quad M_d(\mathbf{w}, \mathbf{z}) > 0$ corresponds to the classifier making no mistakes: $\arg\max_\mathbf{y} \mathbf{w}^\top \mathbf{f}_\mathbf{x}(\mathbf{y}) = \mathbf{t}(\mathbf{x})$.

We now need to define an appropriate metric ρ that in turn defines γ-margin loss for structured classification. Since our margin in (4) grows with the number of mistakes, our metric can become "looser" with the number of mistakes, as there is more room for error.

Definition A.7 (Multi-error-level metric) *Let the* multi-error-level metric $\rho_M : I\!R^l \times I\!R^l \mapsto I\!R$ *for a vector in* $I\!R^{\,l}$ *be given by:*

$$\rho_M(\mathbf{z}, \mathbf{z}') = \max_d \frac{|z_d - z'_d|}{d}. \quad \blacksquare$$

We now define the corresponding γ-margin loss using the new metric:

Definition A.8 (γ-margin average per-label loss) *The* γ-margin average per-label loss $f^\gamma : I\!R^{\,l} \mapsto [0, 1]$ *is given by:*

$$f^\gamma(\mathbf{z}) = \sup_{\rho_M(\mathbf{z},\mathbf{z}') \le 2\gamma} f(\mathbf{z}'). \quad \blacksquare$$

Combining the two definitions, we get:

$$f^\gamma(\mathcal{F}_M(\mathbf{w}, \mathbf{z})) \quad = \quad \sup_{\mathbf{z}:|z_d - M_d(\mathbf{w},\mathbf{z})| \le 2d\gamma} \frac{1}{l} \arg \min_{d:z_d \le 0} z_d.$$

We also define the corresponding covering number for our vector-valued function class:

Definition A.9 (Multi-error-level covering number) *Let $\mathcal{V} = \{\mathbf{V}^{(1)}, \ldots, \mathbf{V}^{(r)}\}$, where $\mathbf{V}^{(j)} = (\mathbf{V}_1^{(j)}, \ldots, \mathbf{V}_i^{(j)}, \ldots, \mathbf{V}_m^{(j)})$ and $\mathbf{V}_i^{(j)} \in I\!\!R^l$, be a* covering *of $\mathcal{F}_M(\mathbf{w}, S)$, with ϵ-precision under the metric ρ_M, if for all $\mathbf{w}$ there exists a $\mathbf{V}^{(j)}$ such that for each data sample $\mathbf{z}^{(i)} \in S$:*

$$\rho_M(\mathbf{V}_i^{(j)}, \mathcal{F}_M(\mathbf{w}, \mathbf{z}^{(i)})) \leq \epsilon.$$

The covering number *of a sample S is the size of the smallest covering: $\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon, S) = \inf |\mathcal{V}|$ s.t. $\mathcal{V}$ is a covering of $\mathcal{F}_M(\mathbf{w}, S)$. We also define $\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon, m) = \sup_{S:\, |S|=m} \mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon, S)$.* ∎

We provide a bound on the covering number of our new function class in terms of a covering number for the linear function class.

Lemma A.10 (Bound on multi-error-level covering number)

$$\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon q, m) \leq \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, mlq(k^2 - 1)),$$

where $q = \max_i |\{(i,j) \in E\}|$ is the maximum edge degree in any sample, k is the number of classes in a label. ∎

Proof: *We will show that $\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon q, S) \leq \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, S')$ for any sample S of size m, where we construct the sample S' of size $mlq(k^2 - 1)$ in order to cover the edge potentials as described below. Note that this is sufficient since $\mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, S') \leq \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, mlq(k^2 - 1))$, by definition, so $\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon q, m) = sup_{S:|S|=m}\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon q, S) \leq \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, mlq(k^2 - 1))$.*

The construction of S' below is inspired by the proof technique in Collins [3], but the key difference is that our construction is linear in the number of labels and edge degree lq while his is exponential in the number of labels. This reduction in size comes about because our covering approximates the values of edge potentials $\mathbf{w}^\top \Delta\mathbf{f}_\mathbf{x}(y_r, y_s)$ for each edge (r, s) and edge assignment (y_r, y_s) as opposed to the values of entire assignments $\mathbf{w}^\top \Delta\mathbf{f}_\mathbf{x}(\mathbf{y})$.

For each sample $\mathbf{z} \in S$, we create $lq(k^2 - 1)$ samples $\Delta\mathbf{f}_\mathbf{x}(y_r, y_s)$, one for each edge (r, s) and each assignment $(y_r, y_s) \neq ((\mathbf{t}(\mathbf{x}))_r, (\mathbf{t}(\mathbf{x}))_s)$. We construct a set of vectors $\nu = \{\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(r)}\}$, where $\mathbf{v}^{(j)} \in I\!\!R^{mlq(k^2-1)}$. The component of $\mathbf{v}^{(j)}$ corresponding to the sample $\mathbf{z}^{(i)}$ and the assignment (y_r, y_s) to the labels of the edge (r, s) will be denoted by $\mathbf{v}_i^{(j)}(y_r, y_s)$. For convenience, we define $\mathbf{v}_i^{(j)}((\mathbf{t}(\mathbf{x}^{(i)}))_r, (\mathbf{t}(\mathbf{x}^{(i)}))_s) = 0$ for correct label assignments, as $\Delta\mathbf{f}_{\mathbf{x}^{(i)}}((\mathbf{t}(\mathbf{x}^{(i)}))_r, (\mathbf{t}(\mathbf{x}^{(i)}))_s) = 0$. To make ν an ∞-norm covering of $\mathcal{F}_L(\mathbf{w}, S')$ under ρ_L, we require that for any $\mathbf{w}$ there exists a $\mathbf{v}^{(j)} \in \nu$ such that for each sample $\mathbf{z}^{(i)}$:

$$|\mathbf{v}_i^{(j)}(y_r, y_s) - \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(i)}}(y_r, y_s))| \leq \epsilon; \ \ \forall(r, s),\ \forall(y_r, y_s). \tag{13}$$

By Definition A.1, the number of vectors in ν is given by $r = \mathcal{N}_\infty(\mathcal{F}_L, \rho_L, \epsilon, mlq(k^2 - 1))$.

We can now use ν to construct a covering $\mathcal{V} = \{\mathbf{V}^{(1)}, \ldots, \mathbf{V}^{(r)}\}$, where $\mathbf{V}^{(j)} = (\mathbf{V}_1^{(j)}, \ldots, \mathbf{V}_i^{(j)}, \ldots, \mathbf{V}_m^{(j)})$ and $\mathbf{V}_i^{(j)} \in I\!\!R^l$, for our multi-error-level function $\mathcal{F}_M$. Let $\mathbf{v}_i^{(j)}(\mathbf{y}) = \sum_{(r,s)} \mathbf{v}_i^{(j)}(y_r, y_s)$, and $M_d(\mathbf{v}_i^{(j)}, \mathbf{z}^{(i)}) = \min_{\mathbf{y}:\Delta\mathbf{t}_{\mathbf{x}^{(i)}}(\mathbf{y})=d} \mathbf{v}_i^{(j)}(\mathbf{y})$, then

$$\mathbf{V}_i^{(j)} = (M_1(\mathbf{v}^{(j)}, \mathbf{z}^{(i)}), \ldots, M_d(\mathbf{v}^{(j)}, \mathbf{z}^{(i)}), \ldots, M_l(\mathbf{v}^{(j)}, \mathbf{z}^{(i)}))\ . \tag{14}$$

Note that $\mathbf{v}_i^{(j)}(y_r, y_s)$ is zero for all edges (r, s) for which the assignment to $(y_r, y_s) = (\mathbf{t}(\mathbf{x}^{(i)}))_r, (\mathbf{t}(\mathbf{x}^{(i)}))_s)$ is correct. Thus for an assignment to $\mathbf{y}$ with k mistakes, at most dq $\mathbf{v}_i^{(j)}(y_r, y_s)$ will be non-zero, as each label can appear in at most q edges. By combining this fact with Eq. (13), we obtain:

$$\forall\mathbf{x}^{(i)}\ \ \forall\mathbf{y} : \Delta\mathbf{t}_{\mathbf{x}^{(i)}}(\mathbf{y}) = d,\ \left|\mathbf{v}_i^{(j)}(\mathbf{y}) - \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(i)}}(\mathbf{y})\right| \leq dq\epsilon\ . \tag{15}$$

We conclude the proof by showing that $\mathcal{V}$ is a covering of $\mathcal{F}_M$ under ρ_M: For each $\mathbf{w}$, pick $\mathbf{V}^{(j)} \in \mathcal{V}$ such that the corresponding $\mathbf{v}^{(j)} \in \nu$ satisfies the condition in Eq. (13). We must now bound:

$$\rho_M(\mathbf{V}_i^{(j)}, \mathcal{F}_M(\mathbf{w}, \mathbf{z}^{(i)})) = \max_d \frac{|\min_{\mathbf{y}:\Delta\mathbf{t}_{\mathbf{x}^{(i)}}(\mathbf{y})=d} \mathbf{v}_i^{(j)}(\mathbf{y}) - \min_{\mathbf{y}:\Delta\mathbf{t}_{\mathbf{x}^{(i)}}(\mathbf{y})=d} \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(j)}}(\mathbf{y})|}{d}.$$

Let $\mathbf{y}_d^{\mathbf{v}} = \arg\min_{\mathbf{y}:\Delta\mathbf{t}_{\mathbf{x}^{(i)}}(\mathbf{y})=d} \mathbf{v}_i^{(j)}(\mathbf{y})$ and $\mathbf{y}_d^{\mathbf{w}} = \arg\min_{\mathbf{y}:\Delta\mathbf{t}_{\mathbf{x}^{(j)}}(\mathbf{y})=d} \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(j)}}(\mathbf{y})$. Consider the case where $\mathbf{v}_i^{(j)}(\mathbf{y}_d^{\mathbf{v}}) \geq \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(i)}}(\mathbf{y}_d^{\mathbf{w}})$ (the reverse case is analogous), we must prove that:

$$\mathbf{v}_i^{(j)}(\mathbf{y}_d^{\mathbf{v}}) - \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(i)}}(\mathbf{y}_s^{\mathbf{w}}) \leq \mathbf{v}_i^{(j)}(\mathbf{y}_s^{\mathbf{w}}) - \mathbf{w}^\top \Delta\mathbf{f}_{\mathbf{x}^{(j)}}(\mathbf{y}_s^{\mathbf{w}}) \leq dq\epsilon\,; \tag{16}$$

where the first step follows from definition of $\mathbf{y}_d^{\mathbf{v}}$, since $\mathbf{v}_i^{(j)}(\mathbf{y}_d^{\mathbf{v}}) \leq \mathbf{v}_i^{(j)}(\mathbf{y}_s^{\mathbf{w}})$. The last step is a direct consequence of Eq. (15). Hence $\rho_M(\mathbf{V}_i^{(j)}, \mathcal{F}_M(\mathbf{w}, \mathbf{z}^{(i)})) \leq q\epsilon$. ∎

Lemma A.11 (Numeric bound on multi-error-level covering number)

$$\log_2 \mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \epsilon, m) \leq 36 \frac{R_{edge}^2 \left\|\mathbf{w}\right\|_2^2 q^2}{\epsilon^2} \log_2 \left(1 + 2\left\lceil 4\frac{R_{edge}\left\|\mathbf{w}\right\|_2 q}{\epsilon} + 2\right\rceil mlq(k^2-1)\right)\;;$$

where $R_{edge} = \max_{(r,s)} \max_{y_r,y_s} \|\mathbf{f}_{\mathbf{x}}(y_r, y_s)\|_2$.

Proof: *Substitute Theorem A.2 into Lemma A.10.* ∎

Theorem A.12 (Multi-label analog of Theorem A.3) *Let f and $f^\gamma(z)$ be as defined above. Let $\gamma_1 > \gamma_2 > \ldots$ be a decreasing sequence of parameters, and p_i be a sequence of positive numbers such that $\sum_{i=1}^\infty p_i = 1$, then for all $\delta > 0$, with probability of at least $1-\delta$ over data:*

$$E_{\mathbf{z}} f(\mathcal{F}_M(\mathbf{w},\mathbf{z})) \quad \leq \quad E_S f^\gamma(\mathcal{F}_M(\mathbf{w},\mathbf{z})) + \sqrt{\frac{32}{m}\left[\ln 4\mathcal{N}_\infty(\mathcal{F}_M, \rho_M, \gamma_i, S) + \ln\frac{1}{p_i\delta}\right]}$$

for all $\mathbf{w}$ and γ, where for each fixed γ, we use i to denote the smallest index s.t. $\gamma_i \leq \gamma$.

Proof: *Similar to the proof of Zhang's Theorem 2 and Corollary 1 [13] where in Step 3 (derandomization) we substitute the vector-valued $\mathcal{F}_M$ and the metric ρ_M.* ∎

Theorem 6.1 follows from above theorem with $\gamma_i = R_{edge}\left\|\mathbf{w}\right\|_2 / 2^i$ and $p_i = 1/2^i$ using an argument identical to the proof of Theorem 6 in Zhang [13].