# Learning Not to Try Too Hard

**Anonymous Author(s)**
Affiliation
Address
email

[IT SEEMS LIKE A LOT OF OTHER PAPERS REFER TO 'COST' AS 'LOSS'... IS THERE SOMEWHERE WHERE PEOPLE CALL IT 'COST' LIKE WE ARE? –BM] [WILL ADDRESS THIS –NAS]

[NOAH, I PUT YOUR NAME SECOND BECAUSE YOUR NAME SEEMS TO BE LAST ON ALL OF YOUR RECENT PAPERS. I DON'T CARE WHICH OUR NAMES IS FIRST THOUGH, SO FEEL FREE TO SWAP IF YOU WANT. –BM] [I USUALLY GO LAST –NAS]

## Abstract

[DO LAST –NAS]

## 1 Introduction

Discriminative learning algorithms are often motivated by their ability to trade off among different kinds of prediction mistakes with different costs. The cost of a mistake is usually taken to be fully defined by the task, i.e., human system designers are trusted to encode this knowledge prior to learning. Information about the inherent ease of avoiding some errors vs. others is generally not taken into account. Closely related to this, and critically important in domains where the data is constructed by humans, is the problem that the outputs in the training data may be unreliable. For example, if training data is produced by asking humans to label instances, and two labels are insufficiently well defined for human labelers to distinguish them, then a learner might be forgiven for conflating them.

We consider situations where human intuition about relative costs of different errors is insufficient. In a margin-based linear modeling framework, we propose a method for incorporating **learning of the cost function** alongside learning of the model. Our approach introduces explicit estimates of the "ease" of avoiding each type of error (for a particular model family). For error types that are "just too hard," our model is offered the possibility of giving up in favor of making other, less challenging predictions more accurately

[MIGHT WANT TO GIVE SOME MOTIVATING EXAMPLES? NOT SURE IF THAT'S NECESSARY OR NOT. ONE EXAMPLE OF MULTICLASS DOMAIN, AND ONE EXAMPLE WHERE COST FUNCTIONS ARE USED IN STRUCTURED DOMAINS –BM]

[MENTION EXAMPLES OF MEASURES OF 'DIFFICULTY'? CITE. –BM]

Our experiments with text classification show scenarios where the method achieves performance improvements over a strong baseline.

## 2 Background and Notation

In a prediction problem, let $\mathcal{X}$ denote the input space, $\mathcal{Y}$ denote the output space, and assume $N$ training instances $\{(x_1, y_1), \ldots, (x_N, y_N)\}$. We assume a linear model and prediction function:

$$\hat{y} = \operatorname*{argmax}_{y \in \mathcal{Y}} \Big( f(x, y; \mathbf{w}) \triangleq \mathbf{w}^\top \mathbf{g}(x, y) \Big) \tag{1}$$

where $\mathbf{w} \in \mathbb{R}^D$ are the parameters to be learned and $\mathbf{g} : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}^D$ is the feature vector function. We will let $\mathcal{M} = \{f(\cdot, \cdot; \mathbf{w}) \mid \mathbf{w} \in \mathbb{R}^D\}$ denote the model family under consideration, given a fixed choice of $\mathbf{g}$.

Our approach, which assumes $\mathcal{Y}$ is categorical, is based on the soft margin formulation of multi-class support vector machines [1–3]. Tsochantaridis et al. [4] and Taskar et al. **??** generalized this framework to allow for differences in costs between different kinds of mistakes, as found when $\mathcal{Y}$ is structured. Let the cost function $\Delta : \mathcal{Y} \times \mathcal{Y} \to \mathbb{R}$ be such that $\Delta(y, y')$ is the cost of predicting $y$ when the correct label is $y'$. We use the "margin rescaling" variant the multiclass SVM:

$$\min_{\boldsymbol{\xi} \geq 0, \mathbf{w}} \frac{\lambda}{2}\|\mathbf{w}\|_2^2 + \frac{1}{m}\sum_{i=1}^{N} \xi_i \quad \text{s.t.} \quad \forall i, \forall y \in \mathcal{Y} \setminus \{y_i\}, f(x_i, y_i; \mathbf{w}) - f(x, y, \mathbf{w}) \geq \Delta(y, y_i) - \xi_i \tag{2}$$

This objective seeks $\mathbf{w}$ that minimizes misclassifications while maximizing the margin between correct and incorrect instances. Further, the more incorrect an $(x, y)$ pair is, the greater the margin should be. This problem is often transformed into an unconstrained one corresponding to direct minimization of the regularized average hinge loss:

$$\min_{\mathbf{w}} \frac{\lambda}{2}\|\mathbf{w}\|_2^2 + \sum_{i=1}^{N} -f(x_i, y_i; \mathbf{w}) + \max_{y \in \mathcal{Y}} f(x_i, y; \mathbf{w} + \Delta(y, y_i) \tag{3}$$

We introduce some notation for errors. We let $\mathcal{S} \subseteq 2^{\mathcal{Y} \times \mathcal{Y}}$ be a collection of prediction error classes that exhausts $\mathcal{Y}^2$ (i.e., $\bigcup_{S \in \mathcal{S}} S = \mathcal{Y}^2$); the error classes need not be mutually exclusive. We let $e_S \in \mathbb{R}$ denote an estimate of the "ease" with which a learner searching in $\mathcal{M}$ can successfully avoid errors in class $S$. Then we let:

$$\Delta(y, y') = \sum_{S \in \mathcal{S} : (y, y') \in S} e_S = \mathbf{e}^\top \mathbf{s}(y, y') \tag{4}$$

where $\mathbf{e}$ is a vector of the $e_S$ and $\mathbf{s}$ is a binary vector of length $\mathcal{S}$ indicating which error class(es) each possible confusion in $\mathcal{Y} \times \mathcal{Y}$ belongs to.

In this paper, we consider two prediction error classes, corresponding to unordered and ordered pairs of outputs. We denote them $\mathcal{S}^{\mathrm{u}}$ and $\mathcal{S}^{\mathrm{o}}$, respectively.

## 3 Cost Learning Model

Previous work assumes $\Delta$ follows intuitively from the prediction task. For example, in natural language dependency parsing, the number of words attached to the wrong parent (Hamming distance for the parse tree) is a sensible choice. We propose to parameterize $\Delta$ and learn its parameters jointly with $\mathbf{w}$. This learned cost function should encode distances between outputs from the perspective of the ease with which a model in the family $\mathcal{M}$ can distinguish between them. This joint learning setup is expected to be particularly useful when some classes of errors are difficult or impossible for a model in the class to resolve, due to unreliable annotations or an insufficient choice of features $\mathbf{g}$.

### 3.1 Ease

We desire a model that estimates prediction ease $\mathbf{e}$ while estimating predictive model parameters $\mathbf{w}$. We have used the term "ease" with respect to an arbitrary model in the family $\mathcal{M}$, but it is more sensible to consider the particular model we seek to estimate. We propose that, for error class $S$ and a model with parameters $\mathbf{w}$, ease $e_S$ should be inversely related to the number of of margin violations involving $S$ that $f(\cdot, \cdot; \mathbf{w})$ makes in the training data:

$$v_S(\mathbf{w}, \mathbf{e}) \triangleq \left|\left\{i \in \{1, \ldots, D\} \mid \left(y_i, \mathrm{argmax}_{y \in \mathcal{Y}} f(x_i, y; \mathbf{w}) + \mathbf{e}^\top \mathbf{s}(y, y_i)\right) \in S\right\}\right| \tag{5}$$

The intuition is that, when this set is large, it is because it is not easy for the model to shrink. Of course, we should also take into account that the distribution of the data may make some errors more frequent, inflating the size of the set in Eq. 5 even if $S$ is "easy." Further, *infrequently* observed

labels are generally expected to be harder to predict. Yet for an $S$ that includes errors on a rarely occurring class, the set in Eq. 5 will necessarily be small, regardless of how easy it is. We therefore propose the following condition for $e_S$:

$$e_S = \max\left(0, 1 - \frac{v_S(\mathbf{w}, \mathbf{e})}{n_S}\right) \tag{6}$$

where $n_S$ is a fixed, *a priori* upper bound on the count of $S$ errors, $v_S$. This has the desirable property that if $v_S \geq n_S$, i.e., $S$ is too difficult to shrink, then ease $e_S$ goes to zero and the model is allowed to give up on $S$. It also keeps $e_S \in [0, 1]$, giving it an intuitive interpretation that undifferentiated errors (i.e., $\mathbf{e} = \mathbf{1}$).

### 3.2 Objective

Our approach is a modification to the SVM objective in Eq. 3; it is a joint optimization of $\mathbf{w}$ and $\mathbf{e}$:

$$\min_{\mathbf{e}\geq 0, \mathbf{w}} \frac{\lambda}{2}\|\mathbf{w}\|_2^2 + \frac{1}{2}\|\mathbf{e}\|_{\mathbf{n}}^2 - \mathbf{e}^\top \mathbf{n} + \sum_{i=1}^{N} -f(x_i, y_i; \mathbf{w}) + \max_{y \in \mathcal{Y}} f(x_i, y; \mathbf{w}) + \mathbf{e}^\top \mathbf{s}(y, y_i) \tag{7}$$

where $\mathbf{n}$ is the vector of upper bounds on prediction error frequencies and $\|\mathbf{e}\|_{\mathbf{n}}^2 = \sum_{S \in \mathcal{S}} n_S e_S^2$. The changes amount to (1) including $\mathbf{e}$ as a free variable and (2) regualrizing it with a quadratic penalty (second term in Eq. 7) and a linear penalty (third term in Eq. 7). The linear penalty selects which $e_S$ should be nonzero—equivalently, are not impossibly difficult. Setting $e_S = 0$ amounts to giving up on $S$ errors.

**[CITE SELF-PACED LEARNING FOR INSPIRATION FOR NEW OBJECTIVE FUNCTION? –BM] [NOT SURE –NAS]**

**[ADD FOOTNOTE ABOUT RELATIONSHIP BETWEEN NORM IN OBJECTIVE AND MAHALANOBIS NORM –BM] [NOT SURE THIS IS CRITICAL –NAS]**

At points of the objective in Eq. 7 that are differentiable with respect to $e_S$, then it is straightforward to show that Eq. 6 holds. At non-differentiable points, which occur due to ties among $y$, $e_S$ will lie between the values given by Eq. 6 for these tied $y$.

**[IS THIS NON-DIFFERENTIABLE PART UNDERSTANDABLE? IS IT ENOUGH, OR DO I NEED TO GIVE THE PROOF? I STILL HAVEN'T ACTUALLY GONE THROUGH THE PROOF COMPLETELY, SO MAYBE WE SHOULD AT LEAST GO OVER THE REASONING TO MAKE SURE I'M NOT CRAZY. –BM] [I THINK WE SHOULD ADD THE PROOF. THE PAPER IS SHORT, SO THERE IS ROOM, AT LEAST RIGHT NOW. MIGHT BE OKAY JUST TO GIVE THE PROOF FOR DIFFERENTIABLE CASE. –NAS]**

### 3.3 Constants $\mathbf{n}$

The appropriate choice for the normalization vector $\mathbf{n}$ in Eq. 7 depends on the prediction classes in $\mathcal{S}$ and the types of bias we seek to avoid in estimating $\mathbf{e}$. For $\mathcal{S}^{\text{u}}$ and $\mathcal{S}^{\text{o}}$, we are most concerned with unbalanced marginal distributions over labels. Let $c_y$ be the frequency of the label $y$ in the training data, $|\{i \mid y_i = y\}|$. We propose two choices of $\mathbf{n}$, both based on the training data:

1. **Logical** $\mathbf{n}$: an upper bound on $v_S(\cdot, \cdot)$ based on frequencies in the training data. For $\mathcal{S}^{\text{u}}$, let $n_{S_{\{y,y'\}}} = \max(c_y, c_{y'})$. For $\mathcal{S}^{\text{o}}$, let $n_{S_{y,y'}} = c_y$ where $S_{y,y'}$ corresponds to an erroneous label of $y'$ in place of the correct $y$.
2. **Expected** $\mathbf{n}$: an upper bound calculated by assuming that our learner can perform better than a random classifier that uses label proportions observed in the training data. For $\mathcal{S}^{\text{u}}$, let $n_{S_{\{y,y'\}}} = 2c_y c_{y'}/N$. For $\mathcal{S}^{\text{o}}$, let $n_{S_{y,y'}} = c_y c_{y'}/N$.

The **Logical** choice will tend to dramatically overestimate the maximum count of each prediction error, but we might choose it over **Expected** if we have reason to believe that it is difficult to estimate the baseline rate at which the model is biased to predict certain labels by the label distribution independent of the inputs. A third option, not explored here, might use a more sophisticated model to estimate bounds on error counts.

**[MORE DETAIL ON WHY EXPECTED MIGHT BE A BETTER CHOICE THAN LOGICAL –BM]**

## 4 Experiments

We implemented the multiclass SVM (Eq. 3) and variations of our method, which we refer to as normalized cost learning (NCL; Eq. 7), using stochastic gradient descent (SGD) [6]. The learning rate at timestep $t$ is $\frac{1}{\lambda_2 t}$ [7]. We ran SGD for 150 passes over the data [CHECK THAT –NAS], using a random permutation each time. We observed that, during the last ten iterations, accuracy varied by $< 0.001$ and fewer than 5% of predictions changed.

We ran several experiments to compare these models on standard text classification datasets/tasks, using conventional training/test splits. 10% of the training set is used in each case to perform a grid search for $\lambda$ over 16 values in $[10^{-6}, 50]$, choosing the one that gives the best [ACCURACY? –NAS], then fixing $\lambda$ and training on the whole training set.

We consider six variations of NCL, varying the prediction error sets ($\mathcal{S}^{\mathrm{u}}$; $\mathcal{S}^{\mathrm{o}}$) and normalization constants ($\mathbf{1}$, i.e., none; logical; expected). [I THINK THAT'S WHAT "NONE" MEANS – PLEASE CHECK –NAS]

### 4.1 Datasets

We considered two datasets with relatively large output label sets: 20 Newsgroups (20NG; 20 category labels corresponding to newsgroups)[1] and Reuters-21578 (R52; 52 topic labels).[2] We followed [**?** ] in preprocessing the text corpora (including downcasing, removing symbols, etc.) and let features in $\mathbf{g}$ correspond to $\log(1 + tf)$ (log transformed term frequencies) for unigrams. Though alternative feature representations (e.g., tfidf; [**?** ]) may perform better, we do not expect their effect to interact with the choice of learning algorithm.

[CITE HTTP://WWW.AAAI.ORG/PAPERS/AAAI/2006/AAAI06-121.PDF ON RELATIVELY LOW DIFFERENCE IN PERFORMANCE BETWEEN LOG(TF) AND TFIDF –BM]

[CITE HTTP://QWONE.COM/~JASON/WRITING/LOOCV.PDF FOR EXAMPLE USE OF LOG(TF) –BM]

[PREPROCESSED USING METHOD FROM HTTP://WEB.IST.UTL.PT/ACARDOSO/DOCS/2007-PHD-THESIS.PDF –BM]

The 20NG dataset consists of 18,846 documents, sorted by date, with 60% used for training. Though the categories are roughly uniformly distributed, the topics vary greatly in their relatedness, following a hierarchical labeling scheme (e.g., *rec.autos* and *rec.motorcycles* are likely more closely related than either to *sci.space*). This offers a way to measure the effectiveness of NCL at learning "ease": the less closely related two categories are, the greater the ease in learning to distinguish them.

The R52 dataset contains 9,100 documents; we use the ModApte split (70% training). The label distribution is skewed, with 43% of documents assigned to [NAME THE TOPIC HERE –NAS] and 37 topics receiving fewer than 50 examples. [MAYBE SAY SOMETHING HERE ABOUT WHY WE THINK NCL WON'T DO AS WELL HERE? –NAS]

### 4.2 Results

[ALL 20NEWS TABLE NUMBERS ARE WRONG. NEED TO FIX THEM AFTER EXPERIMENTS RERUN. –BM]

Table 1 shows the micro-averaged accuracies on the Reuters and 20 newsgroups tasks for the SVM baseline model and versions of NCL with different choices of normalization constants $\mathbf{n}$ and incorrect prediction classes $\mathcal{S}$.

On 20NG, every variant of NCL outperforms the baseline SVM. Logical and expected variants of $\mathbf{n}$ outperform the naïve version. $\mathcal{S}^{\mathrm{u}}$ usually has a slight advantage over $\mathcal{S}^{\mathrm{o}}$ [PLEASE CHECK CAREFULLY AND THAT I MARKED THESE RIGHT IN THE TABLE; YOU HAD THEM REVERSED –NAS]. This makes sense, given that we do not expect any asymmetry in the ease of resolving confusions between two labels, and $\mathcal{S}^{\mathrm{o}}$ introduces extra $\mathbf{e}$ parameters to be estimated.

[1] http://qwone.com/~jason/20Newsgroups

[2] http://www.csmining.org/index.php/r52-and-r8-of-reuters-21578.html.

Table 1: Micro-averaged accuracies of different learners. [HELPFUL IF YOU BOLDFACE THE BEST RESULT(S) IN EACH COLUMN –NAS]

| Learner | 20NG full | 20NG level 2 | 20NG level 1 | R52 |
|---|---|---|---|---|
| SVM | 0.7760 | 0.8008 | 0.8654 | 0.9213 |
| NCL: $\mathcal{S}^{\text{o}}$, none | 0.8008 | 0.8259 | 0.8752 | 0.9213 |
| NCL: $\mathcal{S}^{\text{u}}$, none | 0.8011 | 0.8257 | 0.8751 | 0.9194 |
| NCL: $\mathcal{S}^{\text{o}}$, logical | 0.8024 | 0.8271 | 0.8769 | 0.9210 |
| NCL: $\mathcal{S}^{\text{u}}$, logical | 0.8376 | 0.8631 | 0.9142 | 0.9159 |
| NCL: $\mathcal{S}^{\text{o}}$, expected | 0.8303 | 0.8557 | 0.9092 | 0.9159 |
| NCL: $\mathcal{S}^{\text{u}}$, expected | 0.8307 | 0.8558 | 0.9084 | 0.9171 |

On R52, NCL performs slightly worse than the SVM. Inspecting the errors, we find that 53% of the SVMs mistakes were on examples whose topics had ten or fewer test [YOU MEAN TRAINING? –NAS] examples. [I DIDN'T UNDERSTAND THIS AT ALL: THERE IS NO NON-DIAGONAL ELEMENT IN THE CONFUSION MATRIX WITH MORE THAN 10 MISTAKES. –NAS] These observations suggest that many of the SVM baseline's mistakes come from infrequent labels rather than systematic conflations between certain label pairs, and further that all of the prediction error sets in the cost learning model will be small. As a result, it is unlikely that rescaling costs, as done by NCL, will have much benefit. Fortunately, NCL does not harm performance by more than 0.5%.

### 4.3 Hierarchy and Ease

The hierarchical structure of the 20 Newsgroups topics encodes a notion of distance between topics as distance within the hierarchy. As noted above, we expect that more distant topics (in the hierarchy) should correspond to greater ease in distinguishing between them. Note that NCL does not take advantage of any information about the hierarchy.

Table 1 includes accuracies computed when nearby topics in the hierarchy are are collapsed into single topics, either at the second level (i.e., into [?? –NAS] categories) or the first (i.e., into [?? –NAS] categories). The advantages of NCL are nearly as great for these collapsed tasks as for the primary one, meaning that it is better than the SVM at distinguishing topics that are farther apart in the hierarchy, and therefore has learned a notion of ease that relates to hierarchy distance.

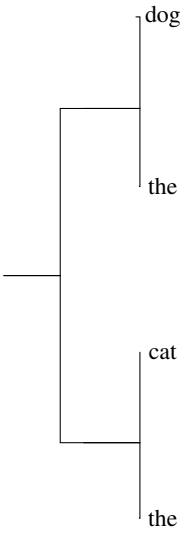
[FIX THE ABOVE PARAGRAPH WHEN GET NEW NUMBERS –BM]

We checked this directly by using $\mathbf{e}$ to reconstruct the hierarchy by applying a hierarchical clustering algorithm.

[CITE HIERARCHICAL CLUSTERING. BE SPECIFIC ABOUT WHICH TYPE OF HIERARCHICAL CLUSTERING IS USED. –BM]

[ADD HIERARCHY FIGURE. –BM]

[ADD MEASUREMENTS OF SIMILARITY BETWEEN HIERARCHIES –BM]




## 5 Related Work

**[HERE ARE SOME THINGS TO POSSIBLY WRITE ABOUT: –BM]**

Self-paced learning [8].

Curriculum Learning [9].

Confidence weighted learning [10].

Ed Hovy inter-annotator agreement cost [11]

Hidden variable learning by state splitting mentioned in `http://www.cs.cmu.edu/~nasmith/papers/career-proposal-2010.pdf` [12].

Finite state output encodings mentioned in `http://www.cs.cmu.edu/~nasmith/papers/career-proposal-2010.pdf` [13]

### 5.1 Future Work and Conclusions

**[IS THERE ANYTHING ELSE THAT I FORGOT? –BM]**

In future work, richer representations of prediction error types ($\mathcal{S}$) might be pursued. For example, classes might be constructed based on frequencies of classes, with the rarest labels forming a group. For structured output spaces such as natural language parsing, the domain might suggest groups of errors; post hoc analysis of $\mathbf{e}$ might, in turn, suggest ways to improve the model through feature engineering.[3] Our framework is easily extended to let these classes depend on the input or metadata as well, allowing very rich parameterizations of learnable cost functions. Recall that these classes need not be mutually exclusive.

Alternative ways to estimate $\mathbf{n}$ might also be considered, such as using a more sophisticated model to estimate bounds on error frequencies in the training set. More generally, characterizations of ease might be developed through alternate means, such as the stability measure from learning theory [14], which might offer insight into the generalizability of predictions involving a particular label.

We concede that our notion of "ease" merges several concepts that might be treated separately. These include the reliability of the labels in training data, the distinctiveness of the labels given the model family (choice of features), the learnability of each label given the number of instances it has in the training set, and the overall similarity of the training distribution to the "true" one. We believe it is an open theoretical question how these various notions might relate to learning guarantees.

[3] We note an interesting parallel to the *ceteris paribus* reasoning suggested by inspection of linear model weights $\mathbf{w}$; inspecting $\mathbf{e}$ shows, "all other things equal," a scaling of error types by ease-of-avoidance.

[THE 'REFERENCES' HEADING GIVEN BY THE BIBLIOGRAPHY COMMAND IS THE WRONG SIZE FONT. NEEDS TO BE THE SIZE OF A 'THIRD LEVEL HEADING'. HOW TO CHANGE THIS? –BM] [MAYBE THE PROBLEM COMES FROM USING NATBIB? –NAS]

## References


[1] Vladimir N Vapnik. Statistical learning theory (adaptive and learning systems for signal processing, communications and control series), 1998.

[2] Koby Crammer and Yoram Singer. On the algorithmic implementation of multiclass kernel-based vector machines. *The Journal of Machine Learning Research*, 2:265–292, 2002.

[3] Jason Weston and Chris Watkins. Multi-class support vector machines. Technical report, Citeseer, 1998.

[4] Ioannis Tsochantaridis, Thomas Hofmann, Thorsten Joachims, and Yasemin Altun. Support vector machine learning for interdependent and structured output spaces. In *Proceedings of the twenty-first international conference on Machine learning*, page 104. ACM, 2004.

[5] Ben Taskar Carlos Guestrin Daphne Koller. Max-margin markov networks. 2003.

[6] G George Yin and Harold Joseph Kushner. *Stochastic approximation and recursive algorithms and applications*. Springer, 2003.

[7] Shai Shalev-Shwartz, Yoram Singer, Nathan Srebro, and Andrew Cotter. Pegasos: Primal estimated sub-gradient solver for svm. *Mathematical programming*, 127(1):3–30, 2011.

[8] M Pawan Kumar, Benjamin Packer, and Daphne Koller. Self-paced learning for latent variable models. In *NIPS*, volume 1, page 3, 2010.

[9] Yoshua Bengio, Jérôme Louradour, Ronan Collobert, and Jason Weston. Curriculum learning. In *Proceedings of the 26th annual international conference on machine learning*, pages 41–48. ACM, 2009.

[10] Mark Dredze, Koby Crammer, and Fernando Pereira. Confidence-weighted linear classification. In *Proceedings of the 25th international conference on Machine learning*, pages 264–271. ACM, 2008.

[11] Barbara Plank, Dirk Hovy, and Anders Søgaard. Learning part-of-speech taggers with inter-annotator agreement loss. In *Proceedings of EACL*, 2014.

[12] Slav Petrov. *Coarse-to-fine natural language processing*. Springer, 2011.

[13] Edward Loper. *Encoding structured output values*. PhD thesis, University of Pennsylvania, 2008.

[14] Sayan Mukherjee, Partha Niyogi, Tomaso Poggio, and Ryan Rifkin. Learning theory: stability is sufficient for generalization and necessary and sufficient for consistency of empirical risk minimization. *Advances in Computational Mathematics*, 25(1-3):161–193, 2006.