CONSTRANGED BAYESIAN ACTIVE LEARNING OF A LINEAR CLASSIFIER

Anestis Tsakmalis, Symeon Chatzinotas and Björn Ottersten

SnT - securityandtrust.lu, University of Luxembourg

ABSTRACT

In this paper, an on-line interactive method is proposed for learning a linear classifier. This problem is studied within the Active Learning (AL) framework where the learning algorithm sequentially chooses unlabelled training samples and requests their class labels from an oracle in order to learn the classifier with the least queries to the oracle possible. Additionally, a constraint is introduced into this interactive learning process which limits the percentage of the samples from one "unwanted" class under a certain threshold. An optimal AL solution is derived and implemented with a sophisticated, accurate and fast Bayesian Learning method, the Expectation Propagation (EP) and its performance is demonstrated through numerical simulations.

Index Terms— Active Learning, Constrained Dynamic Programming, Expectation Propagation

1. INTRODUCTION

In many learning scenarios, data are not delivered passively to the learner but they have to be obtained interactively. In this proactive approach, the learner sequentially designs questions and queries an oracle in order to gain consecutively more and more informative answers about a learning problem. In the Machine Learning regime, this special class of learning problems is called Active Learning (AL). One of the first AL pieces of work which had a great impact in the research community and dealt with actively identifying regressors is [1]. Later on, the Cognitive Radio research community managed to connect the AL problem with Cutting Plane Methods (CPMs) which basically tackled active classification problems [2, 3]. The same approach was followed by the authors of [4] who also applied CPMs to compression schemes.

A complementary approach to the AL problem is based on its sequential nature. This iterative rationale is connected to the Bayesian Experimental Design framework [5] which in its turn is related to the theory of optimal Decision Making. Researchers from the Decision Making field have exploited a Dynamic Programming (DP) approach to sequentially design experiments [6]. The same framework has been used in [7] for state tracking with active observation control where a Kalman-Like state estimator is developed and in [8] for designing primary user system power probes for actively learning interference channel gains. In this category, also constrained AL problems were formulated and solved by researchers in various fields which employed Constrained DP [9, 10]. The authors of [11] accomplished to actively identify human body states with biometric device sensing costs and the authors of [12] achieved to manage a sensor network with communication costs.

In this paper, we combine this Constrained DP framework with a sophisticated Bayesian Learning tool, the EP [13], for sequentially designing unlabelled data, basically feature vectors chosen from a continuous high dimensional space, and requesting their labels from an oracle. The purpose of this Constrained Bayesian AL (CBAL) design method is to learn a linear classifier with the minimum number of queries to the oracle while setting a limit on the expected number of class labels from a specific "unwanted" class. Moreover, an analytical implementation of the EP is proposed for the first time by utilizing recent advances in statistics from the econometrics research community [14]. The remainder of this paper is structured as follows: Section II provides the Bayesian Learning formulation and presents the EP. Section III elaborates on the optimal CBAL for a linear classifier. In Section IV, the simulation results obtained from the application of the proposed technique are shown and in Section V conclusions and future work in this topic are given.

2. BAYESIAN LEARNING AND EXPECTATION PROPAGATION

We begin by defining the normalized version of the unknown linear classifier that we wish to learn:

$$ y = \begin{cases} +1 & \text{if } h^T x \leq 1 \\ -1 & \text{if } h^T x > 1 \end{cases} $$(1)

where $x$ is a feature vector in $\mathbb{R}^N$ and $y$ is its corresponding label. In this section, we present a probabilistic way to learn the $N$-dimensional parameter vector, $h$, of the linear classifier. The true value of $h$ will be denoted as $h^*$ from here on. To describe Bayesian Learning in detail, first we need to define the label conditional likelihood as the probability of $y$ conditioned on the unknown parameter $h^*$ and the feature

This work was supported by the European Research Council under the project "AGNOSTIC: Actively Enhanced Cognition based Framework for Design of Complex Systems"
vector $x$:

$$Pr[y|h = h^*, x^T] = \begin{cases} 
1 & \text{if } y = +1 \text{ and } h \cdot x^T \leq 1 \\
0 & \text{if } y = +1 \text{ and } h \cdot x^T > 1 \\
1 & \text{if } y = -1 \text{ and } h \cdot x^T > 1 \\
0 & \text{if } y = -1 \text{ and } h \cdot x^T \leq 1 
\end{cases}$$ (2)

This expression is actually a threshold likelihood metric determined by the label observation, $y$, and the feature vector $x$. According to the version space duality [15], when we deal with learning linear classifiers, feature vectors are hyperplanes in the parameter or version space and vice versa. Hence, when a learning procedure tries to estimate the parameters of a hyperplane, the version, it actually tries to localize a point in the parameter or version space. In addition, by combining a feature vector and its respective label, an inequality is obtained which in the $h$ space, or version space, represents a linear inequality. Therefore, the likelihood function may also be thought of as a halfspace defined by $x$ and $y$ in the version space.

Now, let us assume that following $t$ queries, or unlabelled feature vectors, $x_0:(t-1) = \{x(0), \ldots, x(t-1)\}$, the learner has obtained $t$ responses, or labels, $y_0:(t-1) = \{y(0), \ldots, y(t-1)\}$, which all together constitute the data known until the $(t-1)$ training sample pair, $D_{t-1}$. After a new feature vector $x(t)$ and its label, $y_t$, the $h$ posterior pdf is expressed as:

$$f_{t+1}(h) = \frac{Pr[y_t|h = h^*, x(t)] f_t(h)}{Pr[y_t|x(t), D_{t-1}]}$$ (3)

which indicates the probability of where $h^*$ lies in the $h$ space given $D_t$. Here, we have exploited the fact that the label $y_t$ is conditionally independent of the previous labels $y_0:(t-1)$ and feature vectors $x_0:(t-1)$ given $h = h^*$ and $x(t)$. Moreover, the denominator term is called the marginal likelihood and even though it is difficult to calculate, it is actually a normalization constant which guarantees that the posterior pdf integrates to 1. Alternatively, the posterior pdf expressed in (3) can be written in a non-recursive form:

$$f_{t+1}(h) = \prod_{i=0}^{t} \frac{Pr[y_i|h = h^*, x(i)]}{\prod_{i=0}^{t} Pr[y_i|x(i), D_{i-1}]} f_0(h)$$ (4)

where $f_0(h)$ is the prior pdf and again the denominator term is a normalization factor whose computation will be shown unnecessary.

2.1. The Expectation Propagation algorithm

Now, each likelihood function can be expressed as $l_i(h) = Pr[y_i|h = h^*, x(i)]$ and hence the likelihood function product of (4) is now $\prod_{i=0}^{t} l_i(h)$, which is basically a product of halfspace indicator functions. In this subsection, we show how to approximate $\prod_{i=0}^{t} l_i(h)$ and thus the deriving posterior pdf using EP [13]. The rationale of the EP is to approximate this product by finding an approximation $\tilde{l}_i(h)$ for each $l_i(h)$. This is done by initializing arbitrarily the likelihood function approximations and iteratively filtering each one of them considering the rest approximations stable. This filtration process is based on minimizing the Kullback-Leibler (KL) divergence of $l_i(h) \prod_{i=0,i\neq j}^{t} l_i(h)$ and $\tilde{l}_i(h) \prod_{i=0,i\neq j}^{t} l_i(h)$. A detailed algorithmic description of EP is presented in Algo. 1.

**Algorithm 1 The Expectation Propagation algorithm**

1. Initialize arbitrarily $\{\tilde{l}_0(h), \tilde{l}_1(h), \ldots, \tilde{l}_t(h)\}$
2. for $k = 1 : N_{EP}$ do
   1. for $j = 0 \rightarrow t$ do
      1. $\tilde{l}_j(h) := \arg \min_{\tilde{l}_j(h)} KL(l_j(h), \prod_{i=0,i\neq j}^{t} \tilde{l}_i(h))$ with $l_j(h) = \prod_{i=0}^{t} l_i(h)$
   2. end for
3. end for

Next, we show how to tackle analytically the KL divergence minimization, the critical step of the EP algorithm, without relying on numerical quadratures or independence assumptions between the latent variables. This will lead to greater accuracy and faster implementation of this sophisticated tool. Here, each approximation in the EP algorithm is considered to be a multivariate normal (MVN) pdf. Consequently, the product of MVN pdf’s, which appears in the KL divergence minimization step, based on Gaussian identities is also an MVN pdf. More specifically, if $\tilde{l}_i(h) = N(h; \mu_i, \Sigma_i)$ for $i = 0, \ldots, t$, where $\mu_i$ are the mean row vectors and $\Sigma_i$ are the covariance matrices, then their product, $\prod_{i=0}^{t} \tilde{l}_i(h)$, is an un-normalized MVN pdf proportional to an MVN pdf, $N(h; \mu_{tot}, \Sigma_{tot})$, where $\Sigma_{tot} = \sum_{i=0}^{t} \Sigma_i$, $\mu_{tot} = \sum_{i=0}^{t} \mu_i$, $\Sigma_{tot}$ and all vectors are assumed to be row vectors.

Hence, the second part of the KL divergence in the core stage of the EP method, $\tilde{l}_j(h) \prod_{i=0,i\neq j}^{t} \tilde{l}_i(h)$, and the approximation product in the first part, $\prod_{i=0,i\neq j}^{t} \tilde{l}_i(h)$, are basically un-normalized MVN pdf’s. For notation simplification, $\prod_{i=0,i\neq j}^{t} \tilde{l}_i(h)$ will be symbolized from now on as $\tilde{l}_{-j}(h)$.

Now, as far as the KL divergence minimization is concerned, when approximations within the exponential family are used, then this is achieved by moment matching [16]. Moment matching means that the two functions whose KL divergence needs to be minimized must have the same moments and
since the second function is an un-normalized MVN one, this results to matching the $0_{th}$, $1_{st}$ and $2_{nd}$ moments of the two parts. This basically indicates that the function to be refined in each EP step, $\hat{l}_j(h)$, must be adjusted so that the moments of $\hat{l}_j(h)$ $\hat{l}_{-j}(h)$ are equal to the ones of $l_j(h)$ $\hat{l}_{-j}(h)$.

Now, let us examine the function $l_j(h)$ $\hat{l}_{-j}(h)$. First, we have already shown that $\hat{l}_j(h)$ is an un-normalized MVN function and we have described $\hat{l}_j(h)$ as a halffspace indicator function. Thus, $l_j(h)$ $\hat{l}_{-j}(h)$ is actually a one-side truncated multivariate Gaussian and what we need is to calculate its $0_{th}$, $1_{st}$ and $2_{nd}$ moments, $q$, $q$ and $Q$ which can be found in detail in Appendix A of [17]. Once these moments are computed, $\hat{l}_j(h)$ is defined as an MVN pdf with covariance matrix $\Sigma^{-1}$ $\Sigma^{-1}$ and mean $\mu = \{q \Sigma^{-1} - \mu_j \Sigma^{-1} \} \Sigma_j$. We also need to highlight that matching the $0_{th}$ moments does not offer essentially better approximations, because multiplying $\hat{l}_j(h)$ with a constant may lead to unwanted results in this iterative filtering process. Still, we mentioned this earlier as part of the moment matching process for the sake of completeness.

3. CONSTRANDED BAYESIAN ACTIVE LEARNING OF INTERFERENCE CHANNEL GAINS

The goal of this paper is to sequentially design feature vectors, $x$, whose labels are revealed to the learner one by one in order to learn as fast as possible the parameter vector, $h^*$, and while ensuring that the number of feature vectors of class $y = -1$ for a specific query budget is always below a certain limit. This means that assuming a limited number of $N_T$ queries and thus feature vectors, $\{x(0), ..., x(N_T - 1)\}$ and their corresponding labels, $\{y_0, ..., y_{N_T - 1}\}$, we wish to minimize the uncertainty of our knowledge about $h^*$, formally represented by the entropy of $f_{N_T}(h)$, subject to maintaining the sum of $y_t = -1$, where $t = 0, ..., N_T - 1$, below a threshold and which is equivalent to controlling the sum of $y_t = +1$, where $t = 0, ..., N_T - 1$, above a corresponding limit. In the previous section, we showed the recursive Bayesian update (3) which modifies our knowledge about $h^*$ step by step. This will be our main tool for handling the iterative nature of this proactive feature vector design strategy.

3.1. The DP formulation of the Constrained Bayesian AL problem

Next, we investigate the optimal training sample design policy that should be chosen in each step of this recursive Bayesian estimation process in order to optimally reduce the posterior pdf entropy after $N_T$ feature vectors, $\{x(0), ..., x(N_T - 1)\}$, with their corresponding labels, $y_{0:N_T - 1}$, subject to $\frac{1}{N_T} \sum_{t=0}^{N_T-1} 1_{\{y_t = -1\}} \leq \alpha'$ or $\frac{1}{N_T} \sum_{t=0}^{N_T-1} 1_{\{y_t = +1\}} \geq \alpha$, where $1_{\{\cdot\}}$ is the indicator function, $\alpha'$ is the threshold ratio of class $y = -1$ occurrences, $\alpha$ is the lower limit ratio of class $y = +1$ occurrences and $\alpha = 1 - \alpha'$. From here on, we employ $\alpha$ for the formulation of our problem. The constraint can also be written as $\sum_{t=0}^{N_T-1} y_t \geq (2\alpha - 1)N_T$. This multistage constrained optimization problem can be expressed in the spirit of DP [18] as finding the optimal query rule that maps $\{f_0, ..., f_{N_T - 1}\}$ to $\{x(0), ..., x(N_T - 1)\}$ in order to achieve the maximum average entropy reduction from the $f_0(h)$ to the $f_{N_T}(h)$ pdf subject to the aforementioned constraint. In a formal manner, we seek the optimal query/feature vector design policy $\pi^*_0(N_{T-1}) = \{x(0) = \mu^*(f_0), ..., x(N_T - 1) = \mu^*(f_{N_T - 1})\}$ which solves the following constrained optimization problem over all possible label sequences derived by this query policy:

$$\max_{\pi} \mathbb{E}^{\pi}[\mathcal{H}(f_0) - \mathcal{H}(f_{N_T}) | x(N_T - 1), D_{N_T - 2}]$$

(5a)

s.t. $\mathbb{E}^{\pi} \left[ \sum_{t=0}^{N_T-1} y_t | x(N_T - 1), D_{N_T - 2} \right] \geq (2\alpha - 1)N_T$

(5b)

where $\mathcal{H}$ is the entropy operator of a pdf and $\mathbb{E}^{\pi}[\cdot]$ is the operator of the average value over all possible label sequences derived by an abstract policy $\pi$.

Before we continue though with the DP solution of our constrained multistage problem, let us first redefine the multivariate cumulative distribution function (cdf) in a more "natural" than the usual way. Assuming a hyperplane, $x w^T = 1$, we alternatively determine the cdf $C$ of a multivariate pdf $f$ as:

$$C(w) = Pr[x w^T \leq 1] = \int_{x w^T \leq 1} f(x) \, dV_x.$$  \hspace{1cm} (6)

In our case, this means that the posterior cdf after the $(t - 1)$ step, $C_t(x)$, is expressed as:

$$C_t(x) = Pr[h x^T \leq 1 | h = h^*, D_{t-1}] = \int_{h x^T \leq 1} f_t(h) \, dV_h.$$  \hspace{1cm} (7)

Using this cdf definition, the optimal feature vector design policy of the Constrained DP problem (5) is found to be $\pi^*_0(N_{T-1}) = \{x(0) = C^{-1}_0(\alpha_0), ..., x(N_T - 1) = C^{-1}_{N_T - 1}(\alpha_{N_T - 1})\}$ where $\alpha_0 = \alpha$, $\alpha_k = \frac{2\alpha N_T - k - \sum_{t=0}^{k-1} y_t}{2(N_T - k)}$ for $k = 1, ..., (N_T - 1)$ and $x(k) = C^{-1}_k(\alpha_k)$ is equivalent to $C_k(x(k)) = \alpha_k$. A detailed derivation of this solution can be found in [17].

3.2. The Necessity of Exploration

Reducing the uncertainty of our knowledge about $h^*$ must be performed by approaching this exact value uniformly from all directions. This means that the training samples in an
AL process must be diversified and this can be accomplished by choosing hyperplanes in the version space of random direction uniformly which promotes exploration. Therefore, we need first to define how to uniformly sample a random direction $\theta$, where $\theta$ is a unit vector. This problem is related to the uniform unit hypersphere point picking which has been thoroughly described in [3, 8]. Hence, in order to produce a feature vector which represents a hyperplane of random direction, $x(t)$ must be parallel to a randomly generated $\theta$, $x(t) = \beta \theta$ where $\beta \in \mathbb{R}$, and it must also satisfy $C_t(x(t)) = c_t$ according to our previous analysis. In a formal manner, this is expressed using (6) as:
\[
\int_{\theta^{\beta} \leq 1} f_t(h) \, dV_h = C_t(\beta \theta) = c_t.
\]
At this point, we make use of the Gaussian approximation of each step’s posterior pdf which we developed in Section II with the help of EP. In accordance with that result, $f_t(h)$ can be approximated by the normalized version of $\prod_{i=0}^{t-1} l_i(h)$ which we denote as $\tilde{f}_t(h)$. So, (8) now becomes:
\[
\int_{\theta^{\beta} \leq 1} \tilde{f}_t(h) \, dV_h = c_t.
\]
After some processing, we obtain that $\beta = F^{-1} (\frac{c_t}{c_1 + c_2})$ where $F^{-1}(\cdot)$ is the inverse cdf of the univariate normal pdf with mean $c_1$ and variance $c_2$. Furthermore, $c_1 = \mu(t)$ and $c_2 = \sum_{i=1}^{N} \theta_i \theta^T (\bar{\Sigma}_i(t))^{-1} \theta_i$ where $\bar{\Sigma}_i(t)$ is the $i_{th}$ column of the covariance matrix of $\tilde{f}_t(h)$.

\section{RESULTS}

In this section, we show the $h^*$ estimation error achieved by the proposed CBAL method depending on the number of training samples. The $h^*$ estimation error metric at each time step is defined as the normalized root-square error $\frac{\|\hat{h}(t) - h^*\|}{\|h^*\|}$ and basically demonstrates the learning efficiency of our method. The estimated parameter vector at each step, $\hat{h}(t)$, is considered as the $\mu(t)$ of the EP. The error figure results are obtained as the average of the error metric defined earlier over 100 random draws of parameter vectors $h^*$. The examined scenarios consider $N = 5$ with $\alpha = \{0.7, 0.9\}$ and $N = 10$ with $\alpha = 0.7$ and the “budget” of queries to the oracle is considered to be $N_T = 200$. Additionally, for the EP implementation, the outer loop iterations, $N_{EP}$, are chosen to be 5 and the prior pdf is a MVN of sufficiently vast circular covariance matrix.

Next, in Fig. 1 we examine the performance of the CBAL technique for all the aforementioned scenarios. First, we observe that the number of required training samples to reach a specific error percentage increases as the problem dimensions, $N$, grow. Second, as $\alpha$ increases, the necessary training samples to achieve again a particular estimation error also increase. Furthermore, a metric $\alpha_{sim}$ is provided which examines the simulated “wanted” class label occurrences, $\alpha_{sim} = \frac{\sum_{i=0}^{N_T} l_i}{N_T}$. As far as the resulting $\alpha_{sim}$ metric is concerned, its values are 0.68, 0.87 and 0.67 for $\alpha = 0.7$ and $N = 5$, for $\alpha = 0.9$ and $N = 5$ and for $\alpha = 0.7$ and $N = 10$ respectively.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{Classifier estimation error vs number of training samples using the CBAL method}
\end{figure}

\section{CONCLUSIONS AND FUTURE WORK}

In this paper, we proposed an AL method in order to learn a linear classifier as fast as possible and while limiting the expected ratio of labels from one “unwanted” class under a specific threshold. This problem was formulated within the Constrained DP framework and its optimal feature vector design policy was implemented with the help of an advanced, fast and accurate Bayesian Learning technique, the EP. The performance of this method was demonstrated through numerical simulations and we confirmed that the simulated metric for the label ratio of the “wanted” class, $\alpha_{sim}$, is satisfactorily close to the target, or design, ratio $\alpha$. As part of our future work, the learning convergence rate of the proposed CBAL method will be studied, since theoretical guarantees for the number of iterations needed to approach the learning solution within some error bound are an essential part of the AL setting.
6. REFERENCES


