Active Learning

Maria-Florina Balcan

10/22/2018
Logistics

- Homework 4 due on Oct 31st
- Project Proposal – Autolab feedback.
Classic Fully Supervised Learning Paradigm Insufficient Nowadays

Modern applications: massive amounts of raw data. Only a tiny fraction can be annotated by human experts.

Protein sequences  Billions of webpages  Images
Modern ML: New Learning Approaches

Modern applications: **massive amounts** of raw data.

Techniques that best utilize data, **minimizing need for expert/human intervention**.

Paradigms where there has been great progress.

• Semi-supervised Learning, (Inter)active Learning.
Semi-Supervised Learning

Learning Algorithm

Data Source

Expert / Oracle

Unlabeled examples

Labeled Examples

Algorithm outputs a classifier

\[ S_l = \{(x_1, y_1), \ldots, (x_{m_l}, y_{m_l})\} \]

\[ x_i \text{ drawn i.i.d from } D, \quad y_i = c^*(x_i) \]

\[ S_u = \{x_1, \ldots, x_{m_u}\} \text{ drawn i.i.d from } D \]

**Goal:** \( h \) has small error over \( D \).

\[ \text{err}_D(h) = \Pr_{x \sim D} (h(x) \neq c^*(x)) \]
Active Learning

Additional resources:
• Two faces of active learning. Sanjoy Dasgupta. 2011.
Batch Active Learning

- Learner can choose specific examples to be labeled.
- **Goal:** use fewer labeled examples [pick informative examples to be labeled].

Data Source: Unlabeled examples

Algorithm outputs a classifier w.r.t $D$
Selective Sampling Active Learning

- Selective sampling AL (Online AL): stream of unlabeled examples, when each arrives make a decision to ask for label or not.
- Goal: use fewer labeled examples [pick informative examples to be labeled].
What Makes a Good Active Learning Algorithm?

- Guaranteed to output a relatively good classifier for most learning problems.

- Doesn’t make too many label requests.
  Hopefully a lot less than passive learning and SSL.

- Need to choose the label requests carefully, to get informative labels.
Can adaptive querying really do better than passive/random sampling?

• YES! (sometimes)

• We often need far fewer labels for active learning than for passive.

• This is predicted by theory and has been observed in practice.
Can adaptive querying help? [CAL92, Dasgupta04]

- Threshold fns on the real line: \( h_w(x) = 1(x \geq w), \ C = \{h_w: w \in \mathbb{R}\} \)
- Exponential improvement.

Active Algorithm

- Get \( N \) unlabeled examples
- How can we recover the correct labels with \( \ll N \) queries?
- Do binary search! Just need \( O(\log N) \) labels!
- Output a classifier consistent with the \( N \) inferred labels.

- \( N = O(1/\epsilon) \) we are guaranteed to get a classifier of error \( \leq \epsilon \).

Passive supervised: \( \Omega(1/\epsilon) \) labels to find an \( \epsilon \)-accurate threshold.
Active: only \( O(\log 1/\epsilon) \) labels. Exponential improvement.
Common Technique in Practice

**Uncertainty sampling** in SVMs common and quite useful in practice. E.g., [Tong & Koller, ICML 2000; Jain, Vijayanarasimhan & Grauman, NIPS 2010; Schohon Cohn, ICML 2000]

**Active SVM Algorithm**

- At any time during the alg., we have a “current guess” $w_t$ of the separator: the max-margin separator of all labeled points so far.
- Request the label of the example closest to the current separator.
Active SVM seems to be quite useful in practice.

[Timon & Koller, ICML 2000; Jain, Vijayanarasimhan & Grauman, NIPS 2010]

**Algorithm (batch version)**

Input $S_u \{x_1, \ldots, x_{m_u}\}$ drawn i.i.d from the underlying source $D$

Start: query for the labels of a few random $x_i$s.

For $t = 1, \ldots,$

- Find $w_t$ the max-margin separator of all labeled points so far.
- Request the label of the example closest to the current separator: minimizing $|x_i \cdot w_t|$.

(highest uncertainty)
Active SVM seems to be quite useful in practice.
E.g., Jain, Vijayanarasimhan & Grauman, NIPS 2010

Newsgroups dataset (20,000 documents from 20 categories)
**Common Technique in Practice**

Active SVM seems to be quite useful in practice.

E.g., Jain, Vijayanarasimhan & Grauman, NIPS 2010

CIFAR-10 image dataset (60,000 images from 10 categories)
Active SVM/Uncertainty Sampling

• Works sometimes....

• However, we need to be very very very very careful!!!
  
  • Myopic, greedy technique can suffer from sampling bias.
  • A bias created because of the querying strategy; as time goes on the sample is less and less representative of the true data source.

[Dasgupta10]
Active SVM/Uncertainty Sampling

- Works sometimes....
- However, we need to be very very very careful!!!
Active SVM/Uncertainty Sampling

- Works sometimes....
- However, we need to be very very careful!!!
  - Myopic, greedy technique can suffer from sampling bias.
  - Bias created because of the querying strategy; as time goes on the sample is less and less representative of the true source.
  - Observed in practice too!!!!
- Main tension: want to choose informative points, but also want to guarantee that the classifier we output does well on true random examples from the underlying distribution.
Safe Active Learning Schemes

Disagreement Based Active Learning

Hypothesis Space Search

[CAL92] [BBL06]

[Hanneke’07, DHM’07, Wang’09, Fridman’09, Kolt10, BHW’08, BHLZ’10, H’10, Ailon’12, ...]
Version Spaces

- \( X \) - feature/instance space; distr. \( D \) over \( X \); \( c^* \) target fnc
- Fix hypothesis space \( H \).

**Definition (Mitchell'82)** Assume realizable case: \( c^* \in H \).

Given a set of labeled examples \((x_1, y_1), \ldots, (x_{m_l}, y_{m_l})\), \( y_i = c^*(x_i) \)

Version space of \( H \): part of \( H \) consistent with labels so far.

I.e., \( h \in VS(H) \) iff \( h(x_i) = c^*(x_i) \ \forall i \in \{1, \ldots, m_l\} \).
Version Spaces

- $X$ - feature/instance space; distr. $D$ over $X$; $c^*$ target fnc
- Fix hypothesis space $H$.

**Definition (Mitchell'82)** Assume realizable case: $c^* \in H$.

Given a set of labeled examples $(x_1, y_1), ..., (x_m, y_m), y_i = c^*(x_i)$

Version space of $H$: part of $H$ consistent with labels so far.

E.g.; data lies on circle in $\mathbb{R}^2$, $H =$ homogeneous linear seps.
Version Spaces. Region of Disagreement

Definition (CAL’92)

- **Version space**: part of $H$ consistent with labels so far.
- **Region of disagreement** = part of data space about which there is still some uncertainty (i.e. disagreement within version space)

\[
x \in X, x \in \text{DIS}(\text{VS}(H)) \iff \exists h_1, h_2 \in \text{VS}(H), h_1(x) \neq h_2(x)
\]

*E.g.*, data lies on circle in $\mathbb{R}^2$, $H =$ homogeneous linear seps.

Region of disagreement in data space

Current version space

Diagram with circle and points indicating regions.
Disagreement Based Active Learning [CAL92]

Algorithm:

Pick a few points at random from the current region of uncertainty and query their labels.

Stop when region of uncertainty is small.

Note: it is active since we do not waste labels by querying in regions of space we are certain about the labels.
Disagreement Based Active Learning [CAL92]

Algorithm:

Query for the labels of a few random $x_i$s.

Let $H_1$ be the current version space.

For $t = 1, \ldots,$

Pick a few points at random from the current region of disagreement $\text{DIS}(H_t)$ and query their labels.

Let $H_{t+1}$ be the new version space.
Region of uncertainty [CAL92]

- **Current version space**: part of $C$ consistent with labels so far.
- "Region of uncertainty" = part of data space about which there is still some uncertainty (i.e. disagreement within version space)
Region of uncertainty [CAL92]

- **Current version space**: part of \( C \) consistent with labels so far.
- “Region of uncertainty” = part of data space about which there is still some uncertainty (i.e. disagreement within version space)
How about the agnostic case where the target might not belong the $H$?
A^2 Agnostic Active Learner [BBL’06]

**Algorithm:**

Let $H_1 = H$.

For $t = 1, \ldots,$

- Pick a few points at random from the current region of disagreement $\text{DIS}(H_t)$ and query their labels.
- Throw out hypothesis if you are statistically confident they are suboptimal.

Careful use of generalization bounds; Avoid the sampling bias!!!
When Active Learning Helps. Agnostic case

\( A^2 \) the first algorithm which is robust to noise.

[Balcan, Beygelzimer, Langford, ICML’06]  [Balcan, Beygelzimer, Langford, JCSS’08]

“Region of disagreement” style: Pick a few points at random from the current region of disagreement, query their labels, throw out hypothesis if you are statistically confident they are suboptimal.

Guarantees for \( A^2 \) [BBL’06,’08]:

- It is safe (never worse than passive learning) & exponential improvements.
  - \( C \) - thresholds, low noise, exponential improvement.
  - \( C \) - homogeneous linear separators in \( \mathbb{R}^d \),
    \( D \) - uniform, low noise, only \( d^2 \log (1/\varepsilon) \) labels.

A lot of subsequent work.

[Hanneke’07, DHM’07, Wang’09 , Fridman’09, Kolt10, BHW’08, BHLZ’10, H’10, Ailon’12, …]
General guarantees for $A^2$ Agnostic Active Learner

“Disagreement based”: Pick a few points at random from the current region of uncertainty, query their labels, throw out hypothesis if you are statistically confident they are suboptimal. [BBL’06]

Guarantees for $A^2$ [Hanneke’07]:

**Disagreement coefficient**

$$\theta_{c^*} = \sup_{r \geq \eta + \epsilon} \frac{\Pr(\text{DIS}(B(c^*, r)))}{r}$$

**Theorem**

$$m = \left(1 + \frac{\eta^2}{\epsilon^2}\right) \VCdim(C) \theta_{c^*}^2 \log\left(\frac{1}{\epsilon}\right)$$

labels are sufficient s.t. with prob. $\geq 1 - \delta$ output $h$ with $\text{err}(h) \leq \eta + \epsilon$.

Realizable case: $$m = \VCdim(C) \theta_{c^*} \log\left(\frac{1}{\epsilon}\right)$$

Linear Separators, uniform distr.: $$\theta_{c^*} = \sqrt{d}$$
General guarantees for $A^2$ Agnostic Active Learner

“Disagreement based”: Pick a few points at random from the current region of uncertainty, query their labels, throw out hypothesis if you are statistically confident they are suboptimal. [BBL’06]

Guarantees for $A^2$ [Hanneke’07]:

**Theorem**

How quickly the region of disagreement collapses as we get closer and closer to optimal classifier

$$m = \left(1 + \frac{\eta}{\epsilon^2}\right) VCdim(C) \theta_{c^*}^2 \log\left(\frac{1}{\epsilon}\right)$$

labels are sufficient s.t. with prob. $\geq 1 - \delta$ output $h$ with $err(h) \leq \eta + \epsilon$.

Realizable case: $m = VCdim(C) \theta_{c^*} \log\left(\frac{1}{\epsilon}\right)$

Linear Separators, uniform distr.: $\theta_{c^*} = \sqrt{d}$

Honorable Mention for Test of Time awards at ICML!
Disagreement Based Active Learning

“Disagreement based” algos: query points from current region of disagreement, throw out hypotheses when statistically confident they are suboptimal.

• Generic (any class), adversarial label noise.
• Computationally efficient for classes of small VC-dimension

Still, could be suboptimal in label complex & computationally inefficient in general.

Lots of subsequent work trying to make it more efficient computationally and more aggressive too: [Hanneke07, DasguptaHsuMontleoni'07, Wang'09, Fridman'09, Koltchinskii10, BHW'08, BeygelzimerHsuLangfordZhang'10, Hsu'10, Ailon'12, ...]
Other Interesting ALTec hniques used in Practice

Interesting open question to analyze under what conditions they are successful.
Density-Based Sampling

Centroid of largest unsampled cluster

[Jaime G. Carbonell]
Uncertainty Sampling

Closest to decision boundary (Active SVM)

[Jaime G. Carbonell]
Maximal Diversity Sampling

Maximally distant from labeled x’s

[Jaime G. Carbonell]
Ensemble-Based Possibilities

Uncertainty + Diversity criteria

Density + uncertainty criteria

[Jaime G. Carbonell]
Graph-based Active and Semi-Supervised Methods
Graph-based Methods

• Assume we are given a pairwise similarity fnc and that very similar examples probably have the same label.

• If we have a lot of labeled data, this suggests a Nearest-Neighbor type of algorithm.

• If you have a lot of unlabeled data, perhaps can use them as “stepping stones”.

<table>
<thead>
<tr>
<th></th>
<th>E.g., handwritten digits [Zhu07]:</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="example1" alt="not similar" /></td>
<td><img src="example2" alt="‘indirectly’ similar with stepping stones" /></td>
</tr>
</tbody>
</table>
Graph-based Methods

Idea: construct a graph with edges between very similar examples.

Unlabeled data can help “glue” the objects of the same class together.
Graph-based Methods

Often, transductive approach. (Given $L + U$, output predictions on $U$). Are allowed to output any labeling of $L \cup U$.

Main Idea:

- Construct graph $G$ with edges between very similar examples.
- Might have also glued together in $G$ examples of different classes.
- Run a graph partitioning algorithm to separate the graph into pieces.

Several methods:
- Minimum/Multiway cut [Blum&Chawla01]
- Minimum “soft-cut” [ZhuGhahramaniLafferty'03]
- Spectral partitioning
- …
SSL using soft cuts

[ZhuGhahramaniLafferty'03]

Solve for label function $f(x) \in [0,1]$ to minimize:

$$J(f) = \sum_{edges \ (i,j)} w_{ij}(f(x_i) - f(x_j))^2 + \sum_{x_i \in L} \lambda(f(x_i) - y_i)^2$$

Similar nodes get similar labels (weighted similarity)

Agreement with labels (agreement not strictly enforces)
Active learning with label propagation

(1) Build neighborhood graph

(2) Query some random points

(3) Propagate labels (using soft-cuts)

(4) Make query and go to (3)

How to choose which node to query?
Active learning with label propagation

One natural idea: query the most uncertain point.

But this has only one edge. Query won’t have much impact!
(even worse: a completely isolated node)

(3) Propagate labels (using soft-cuts)  (4) Make query and go to (3)
Active learning with label propagation

Instead, use a 1-step-lookahead heuristic:

- For a node with label $p$, assume that querying will have prob $p$ of returning answer 1, $1 - p$ of returning answer 0.

- Compute “average confidence” after running soft-cut in each case:
  \[
  p \frac{1}{n} \Sigma x_i \max(f_1(x_i), 1 - f_1(x_i)) + (1 - p) \frac{1}{n} \Sigma x_i \max(f_0(x_i), 1 - f_0(x_i))
  \]

- Query node s.t. this quantity is highest (you want to be more confident on average).

\(\begin{align*}
(3) \text{ Propagate labels (using soft-cuts)} \\
(4) \text{ Make query and go to (3)}
\end{align*}\)
Active Learning with Label Propagation in Practice

• Does well for Video Segmentation (Fathi-Balcan-Ren-Regh, BMVC 11).
What You Should Know

• Active learning could be really helpful, could provide exponential improvements in label complexity (both theoretically and practically)!

• Common heuristics (e.g., those based on uncertainty sampling). Need to be very careful due to sampling bias.

• Safe Disagreement Based Active Learning Schemes.
  • Understand how they operate precisely in noise free scenarios.