- Support Vector Machines (SVMs).
- · Semi-Supervised Learning.
 - Semi-Supervised SVMs.

Maria-Florina Balcan 03/25/2015

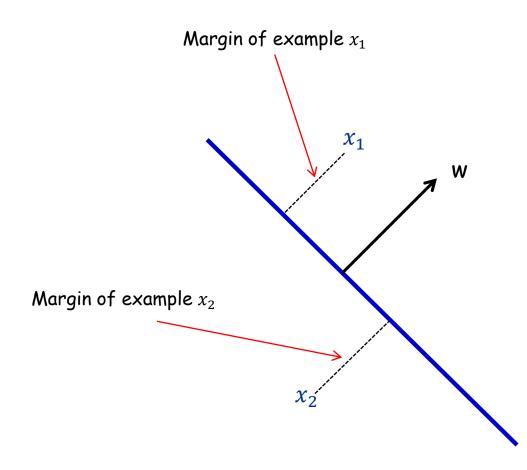
One of the most theoretically well motivated and practically most effective classification algorithms in machine learning.

Directly motivated by Margins and Kernels!

Geometric Margin

WLOG homogeneous linear separators $[w_0 = 0]$.

Definition: The margin of example x w.r.t. a linear sep. w is the distance from x to the plane $w \cdot x = 0$.



If ||w|| = 1, margin of x w.r.t. w is $|x \cdot w|$.

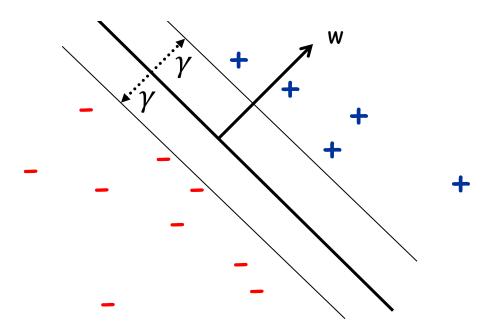
$$Y_i = \frac{y_i w^T x_i}{|w_i|}, \forall x_i \in S$$

Geometric Margin

Definition: The margin of example x w.r.t. a linear sep. w is the distance from x to the plane $w \cdot x = 0$.

Definition: The margin γ_w of a set of examples S wrt a linear separator w is the smallest margin over points $x \in S$.

Definition: The margin γ of a set of examples S is the maximum γ_w over all linear separators w.



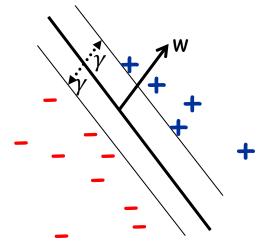
Margin Important Theme in ML

Both sample complexity and algorithmic implications.

Sample/Mistake Bound complexity:

- If large margin, # mistakes Peceptron makes is small (independent on the dim of the space)!
- If large margin γ and if alg. produces a large margin classifier, then amount of data needed depends only on R/γ [Bartlett & Shawe-Taylor '99].

Algorithmic Implications





Suggests searching for a large margin classifier... SVMs

Directly optimize for the maximum margin separator: SVMs

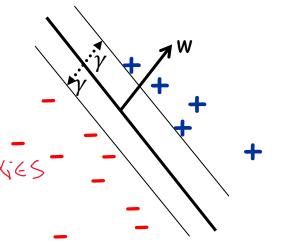
First, assume we know a lower bound on the margin γ

Input: γ , S={(x₁, y₁), ...,(x_m, y_m)};

Find: some w where:

- For all i, $y_i w \cdot x_i \ge \gamma$

JIWI > 7, Y



Output: w, a separator of margin γ over 5

Realizable case, where the data is linearly separable by margin γ

Directly optimize for the maximum margin separator: SVMs

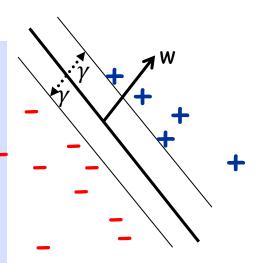
E.g., search for the best possible γ

Input:
$$S=\{(x_1, y_1), ..., (x_m, y_m)\};$$

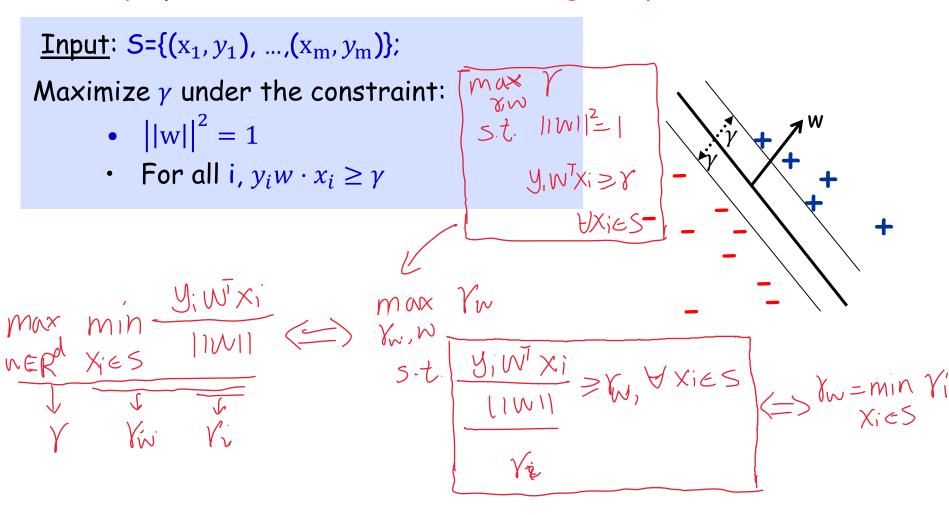
Find: some w and maximum γ where:

- For all i, $y_i w \cdot x_i \ge \gamma$

Output: maximum margin separator over 5



Directly optimize for the maximum margin separator: SVMs



Directly optimize for the maximum margin separator: SVMs

```
Input: S=\{(x_1, y_1), ..., (x_m, y_m)\};

Maximize \gamma under the constraint:

||w||^2 = 1
• For all i, y_i w \cdot x_i \ge \gamma

objective constraints
```

This is a constrained optimization problem.

 Famous example of constrained optimization: linear programming, where objective fn is linear, constraints are linear (in)equalities

Directly optimize for the maximum margin separator: SVMs

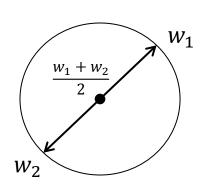
<u>Input</u>: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Maximize y under the constraint:

- $||w||^2 = 1$
- For all i, $y_i w \cdot x_i \ge \gamma$

This constraint is non-linear.

In fact, it's even non-convex



Directly optimize for the maximum margin separator: SVMs

<u>Input</u>: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Maximize γ under the constraint:

- For all i, $y_i w \cdot x_i \ge \gamma$

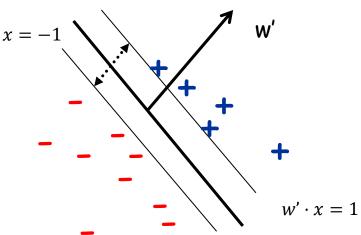
 $||w'|| = ||w|| = \frac{||w||}{||w||}$ $= \frac{1}{||w||}$

 $w' = w/\gamma$, then max γ is equiv. to minimizing $||w'||^2$ (since $||w'||^2 = 1/\gamma^2$). So, dividing both sides by γ and writing in terms of w' we get:

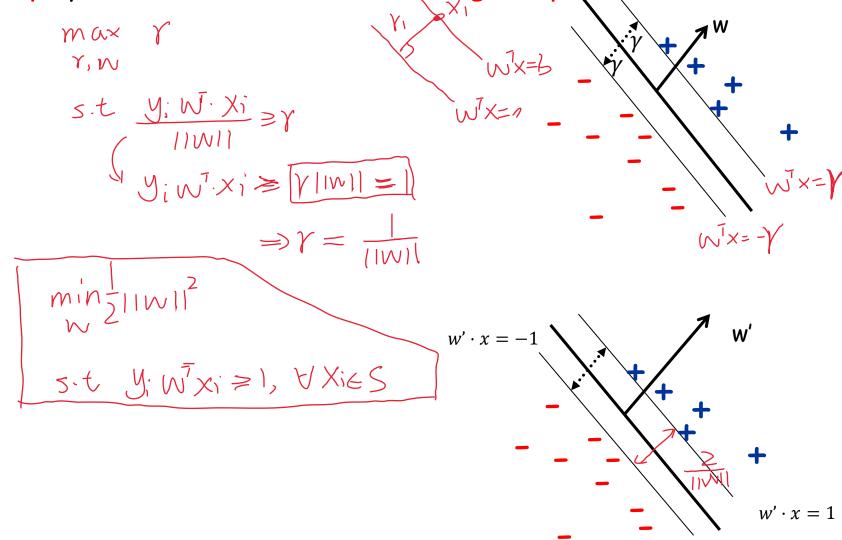
<u>Input</u>: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Minimize $||w'||^2$ under the constraint:

• For all i, $y_i w' \cdot x_i \ge 1$



Directly optimize for the maximum margin separator: SVMs



Directly optimize for the maximum margin separator: SVMs

```
Input: S=\{(x_1, y_1), (x_m, y_m)\};
\operatorname{argmin}_{v} ||w||^2 \text{ s.t.}:
• For all i, y_i w \cdot x_i \ge 1
```

This is a constrained optimization problem.

- The objective is convex (quadratic)
- All constraints are linear
- Can solve efficiently (in poly time) using standard quadratic programing (QP) software

Question: what if data isn't perfectly linearly separable?

<u>Issue 1</u>: now have two objectives

- maximize margin
- minimize # of misclassifications.

Ans 1: Let's optimize their sum: minimize $||w||^2 + C(\# \text{ misclassifications})$

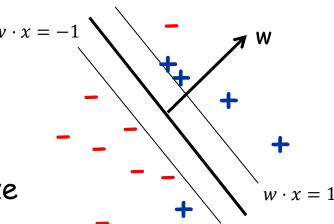
where C is some tradeoff constant.

<u>Issue 2</u>: This is computationally hard (NP-hard).



[even if didn't care about margin and minimized # mistakes]

NP-hard [Guruswami-Raghavendra'06]



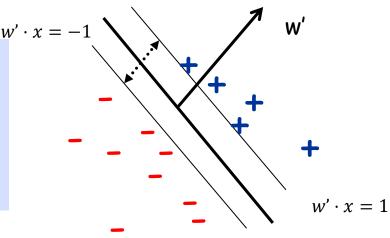
Question: what if data isn't perfectly linearly separable?

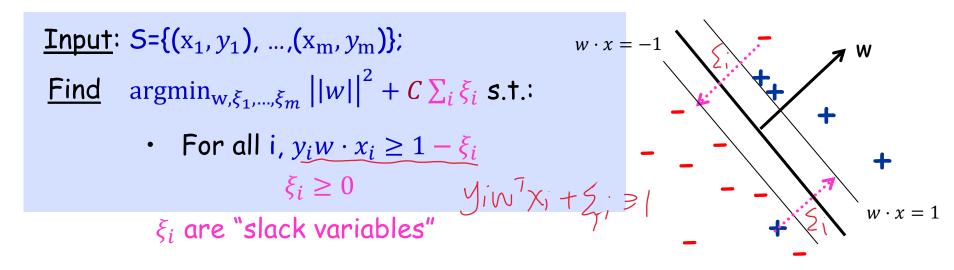
Replace "# mistakes" with upper bound called "hinge loss"

<u>Input</u>: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Minimize $||w'||^2$ under the constraint:

• For all i, $y_i w' \cdot x_i \ge 1$





Question: what if data isn't perfectly linearly separable? Replace "# mistakes" with upper bound called "hinge loss"

```
Input: S=\{(x_1, y_1), ..., (x_m, y_m)\};
  Find \operatorname{argmin}_{W,\xi_1,...,\xi_m} ||w||^2 + C \sum_i \xi_i \text{ s.t.}:
              For all i, y_i w \cdot x_i \ge 1 - \xi_i
                          \xi_i \geq 0
                                             D y; w'x; ≥1, ξ;=0
              \xi_i are "slack variables" y_i y_i y_i^T x_i < 1
C controls the relative weighting between the
twin goals of making the ||w||^2 small (margin is
large) and ensuring that most examples have
functional margin \geq 1.
             hinge loss: [= max (0, 1- ywx)
                                                                 l(w, x, y) = \max(0, 1 - y w \cdot x)
```

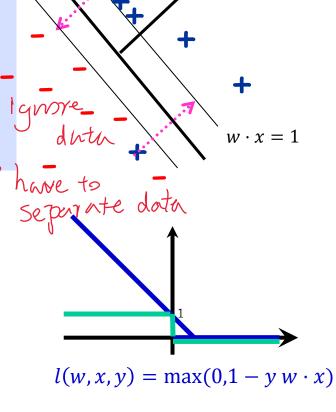
<u>Input</u>: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Find $\operatorname{argmin}_{W,\xi_1,...,\xi_m} \left| |w| \right|^2 + C \sum_i \xi_i \text{ s.t.}$:

• For all i, $y_i w \cdot x_i \ge 1 - \xi_i$ $\zeta = 0$, Ignore— $\xi_i \ge 0$

Replace the number of mistakes with the hinge loss

 $||w||^2 + C$ (# misclassifications)



Question: what if data isn't perfectly linearly separable? Replace "# mistakes" with upper bound called "hinge loss"

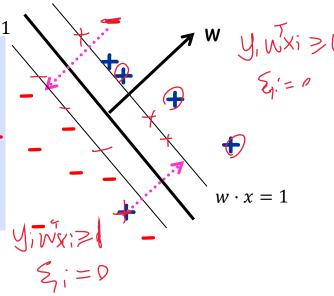
Input:
$$S=\{(x_1, y_1), ..., (x_m, y_m)\};$$

Find
$$\operatorname{argmin}_{w,\xi_1,...,\xi_m} ||w||^2 + C \sum_i \xi_i \text{ s.t.}$$
:

For all i, $y_i w \cdot x_i \ge 1 - \xi_i$

 ξ_i are "slack variables"

min
$$\frac{1}{2}||w||^2 + C = \frac{m}{2}(1 - y_i w^T x_i)_+$$
 = unconstraint optimization regularization $\frac{z_{i-1}}{2}$ = empirical risk groblem.



What if the data is far from being linearly separable?

Example:



٧S



No good linear separator in pixel representation.

SVM philosophy: "use a Kernel"

$$\frac{K(x_i, x_j)}{\langle x_i, x_j \rangle} = \int (x_i) \, \Phi(x_i)$$

SVMs -- Primal Form and Dual Form max = | ||w||^2 - = | \times | $d = \frac{1}{max} \left(\frac{1}{min} + \frac{1}{min} \right) \left(\frac{1}{min} + \frac{1}{min} + \frac{1}{min} \right) \left(\frac{1}{min} + \frac{1}{min} + \frac{1}{min} \right) \left(\frac{1}{min} + \frac{1}{min} + \frac{1}{min} + \frac{1}{min} \right) \left(\frac{1}{min} + \frac{1}{min} + \frac{1}{min} \right) \left(\frac{1}{min} + \frac{1}{mi$ == n, stationary Qi(Y; WXi-1)=0, complementery yiwxi>1, primal S.t. Qi≥0, 1=1,2,..., M Zi≥o, dual

```
Input: S=\{(x_1, y_1), ..., (x_m, y_m)\};
Find \underset{w,\xi_1,...,\xi_m}{\operatorname{Find}} ||w||^2 + C \sum_i \xi_i \text{ s.t.}:
Primal form

• For all i, y_i w \cdot x_i \ge 1 - \xi_i
\xi_i \ge 0
```

Which is equivalent to:

```
\begin{array}{ll} \underline{\text{Input}} \colon \text{S=}\{(x_1,y_1), ..., (x_m,y_m)\}; \\ \underline{\text{Find}} & \operatorname{argmin}_{\alpha} \frac{1}{2} \sum_{i} \sum_{j} y_i y_j \; \alpha_i \alpha_j x_i \cdot x_j - \sum_{i} \alpha_i \; \text{s.t.}; \\ & \cdot & \text{For all i,} \quad 0 \leq \alpha_i \leq \xi_i \; \text{C} \\ & \sum_{i} y_i \alpha_i = 0 \end{array}
```

Lagrangian Dual

Primal: min
$$\frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}i|$$

s.t. $y(w^{x_1}+b) = 1-\frac{1}{2}i$
 $(w,b, \Sigma, \alpha, \lambda)$

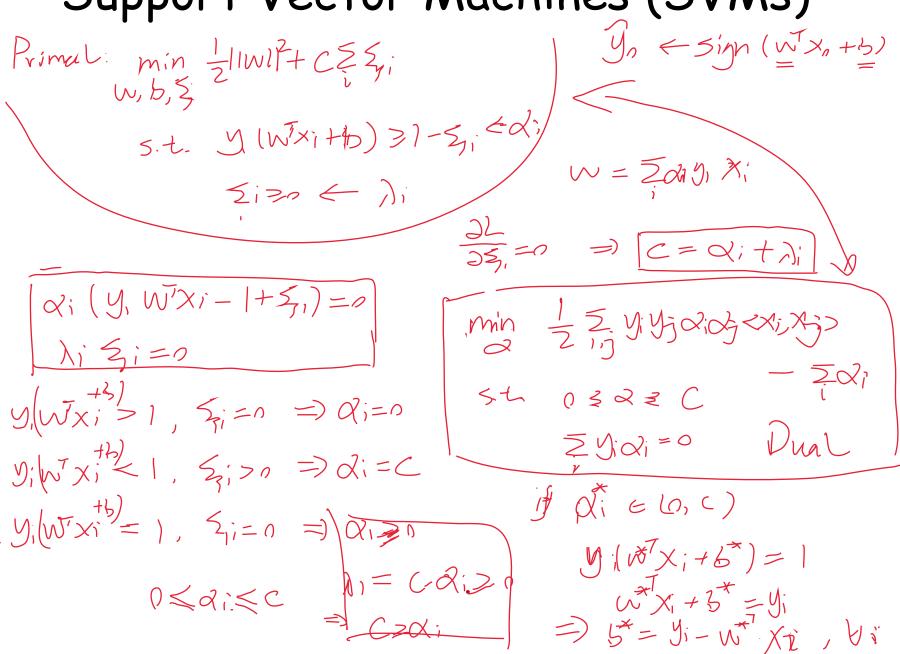
$$= \frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}i|$$
 $(w,b, \Sigma, \alpha, \lambda)$

$$= \frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}i|$$
 $(w,b, \Sigma, \alpha, \lambda)$

$$= \frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}i|$$
 $(w,b, \Sigma, \alpha, \lambda)$

$$= \frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}i|$$

$$= \frac{1}{2}||w||^2 + C_{\frac{1}{2}} \frac{1}{2}$$



SVMs (Lagrangian Dual)

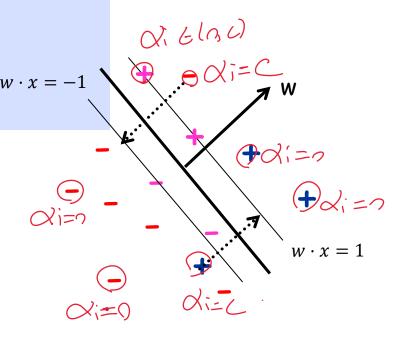
Input: $S=\{(x_1, y_1), ..., (x_m, y_m)\};$

Find
$$\operatorname{argmin}_{\alpha} \frac{1}{2} \sum_{i} \sum_{j} y_{i} y_{j} \alpha_{i} \alpha_{j} x_{i} \cdot x_{j} - \sum_{i} \alpha_{i} \text{ s.t.}$$
:

• For all i, $0 \le \alpha_i \le C_i$ $\sum_i y_i \alpha_i = 0$

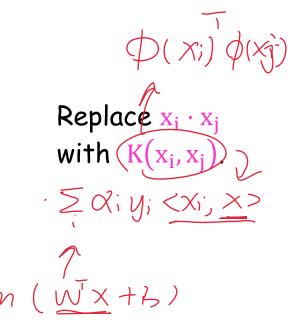
- Final classifier is: $w = \sum_i \alpha_i y_i x_i$
- The points x_i for which $\alpha_i \neq 0$ are called the "support vectors"





Kernelizing the Dual SVMs

```
\begin{split} & \underline{\text{Input}} \colon \text{S=}\{(x_1,y_1), ..., (x_m,y_m)\}; \\ & \underline{\text{Find}} \quad \text{argmin}_{\alpha} \frac{1}{2} \sum_{i} \sum_{j} y_i y_j \; \alpha_i \alpha_j x_i \cdot x_j + \sum_{i} \alpha_i \; \text{s.t.}; \\ & \cdot \quad \text{For all i,} \quad 0 \leq \alpha_i \leq C_i \\ & \sum_{i} y_i \alpha_i = 0 \end{split}
```



- Final classifier is: $w = \sum_i \alpha_i y_i x_i$
- The points x_i for which $\alpha_i \neq 0$ are called the "support vectors"
- With a kernel, classify x using $\sum_i \alpha_i y_i K(x, x_i)$

Lernielized

2. S.V. example spanistry

3. Sano - dual

Support Vector Machines (SVMs).

One of the most theoretically well motivated and practically most effective classification algorithms in machine learning.

Directly motivated by Margins and Kernels!

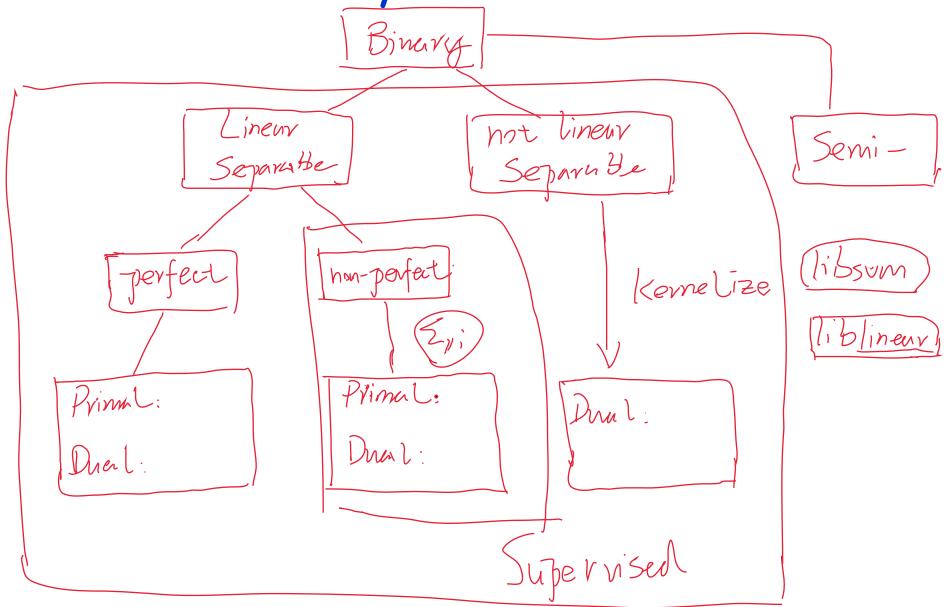
What you should know

- The importance of margins in machine learning.
- The primal form of the SVM optimization problem
- The dual form of the SVM optimization problem.
- Kernelizing SVM.

• Think about how it's related to <u>Regularized Logistic</u> Regression.

$$V = \frac{1}{11001}$$
 SVM: min $(1-ywx)_+ + \lambda 110012$

What you should know



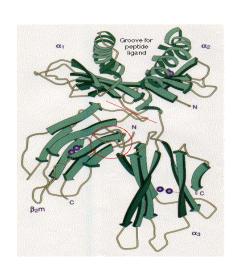
Modern (Partially) Supervised Machine Learning

 Using Unlabeled Data and Interaction for Learning

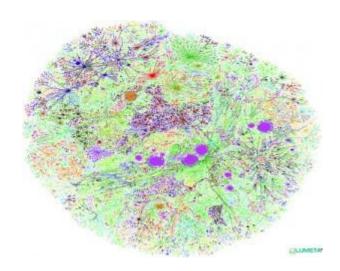
Classic Paradigm Insufficient Nowadays

Modern applications: massive amounts of raw data.

Only a tiny fraction can be annotated by human experts.



Protein sequences

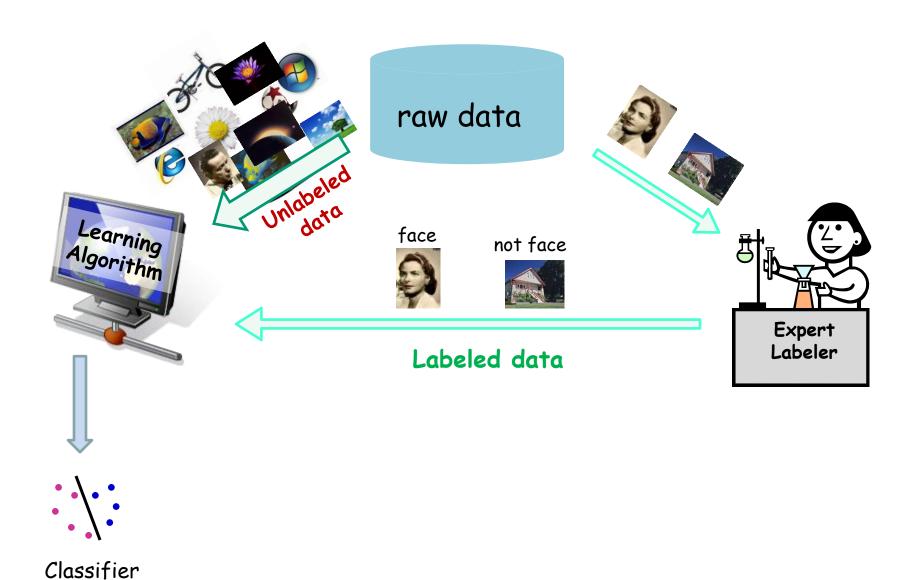


Billions of webpages

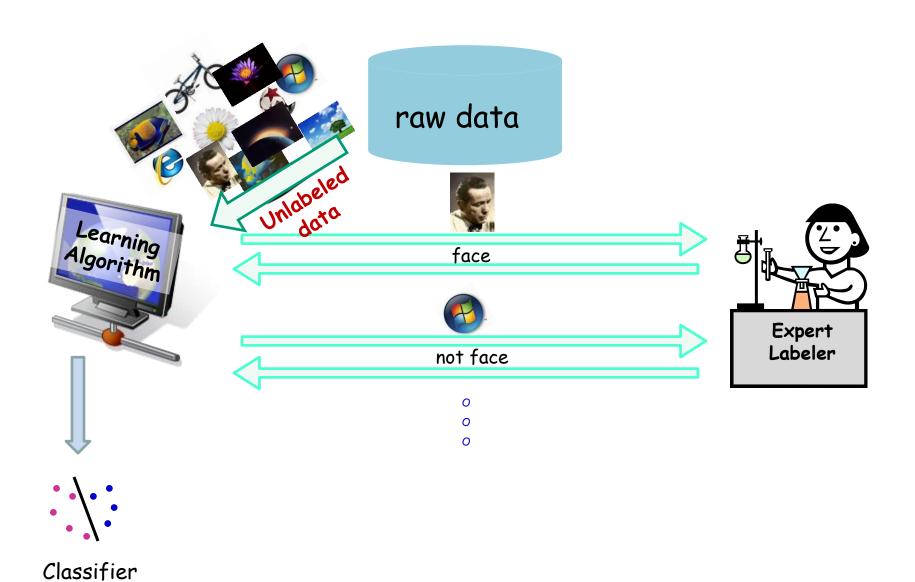


Images

Semi-Supervised Learning



Active Learning



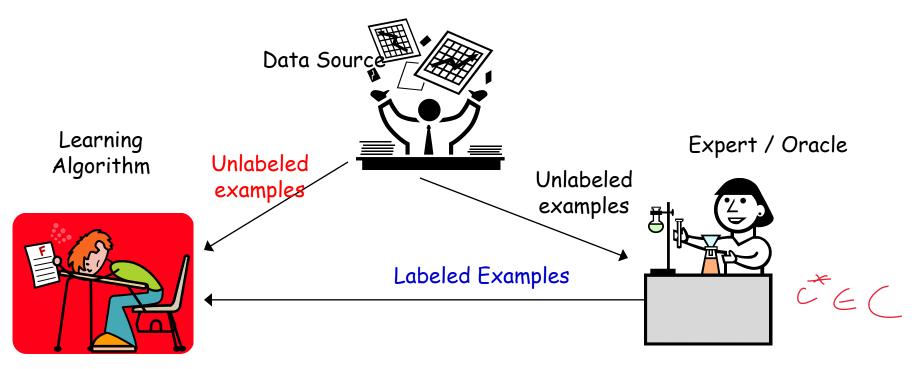
Semi-Supervised Learning

Prominent paradigm in past 15 years in Machine Learning.

- Most applications have lots of unlabeled data, but labeled data is rare or expensive:
 - · Web page, document classification
 - Computer Vision
 - Computational Biology,

•

Semi-Supervised Learning



Algorithm outputs a classifier

$$\begin{split} &S_l \text{=} \{(x_1,y_1), ..., (x_{m_l},y_{m_l})\} \\ &x_i \text{ drawn i.i.d from D, } y_i = c^*(x_i) \\ &S_u \text{=} \{x_1, ..., x_{m_u}\} \text{ drawn i.i.d from D} \end{split}$$

Goal: h has small error over D.

$$\operatorname{err}_{D}(h) = \Pr_{x \sim D}(h(x) \neq c^{*}(x))$$

Semi-supervised learning: no querying. Just have lots additional unlabeled data.

A bit puzzling since unclear what unlabeled data can do for you....

Key Insight

Unlabeled data useful if we have beliefs not only about the form of the target, but also about its relationship with the underlying distribution.

Combining Labeled and Unlabeled Data

- Several methods have been developed to try to use unlabeled data to improve performance, e.g.:
 - Transductive SVM [Joachims '99]
 - Co-training [Blum & Mitchell '98]
 - Graph-based methods [B&C01], [ZGL03]

Test of time awards at ICML!

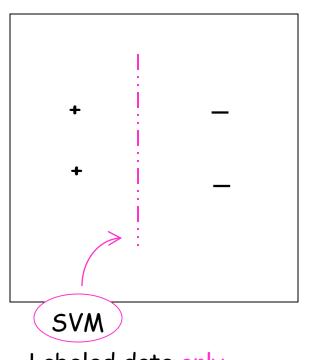
Workshops [ICML '03, ICML' 05, ...]

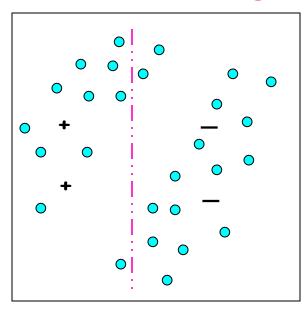
- Books: Semi-Supervised Learning, MIT 2006

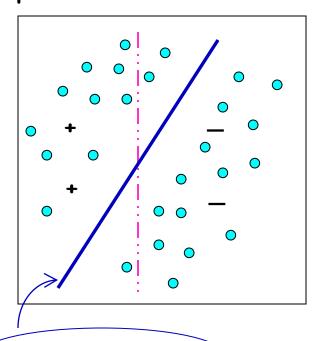
 O. Chapelle, B. Scholkopf and A. Zien (eds)
 - Introduction to Semi-Supervised Learning, Morgan & Claypool, 2009 Zhu & Goldberg

Example of "typical" assumption: Margins

- The separator goes through low density regions of the space/large margin.
 - assume we are looking for linear separator
 - belief: should exist one with large separation







Transductive SVM

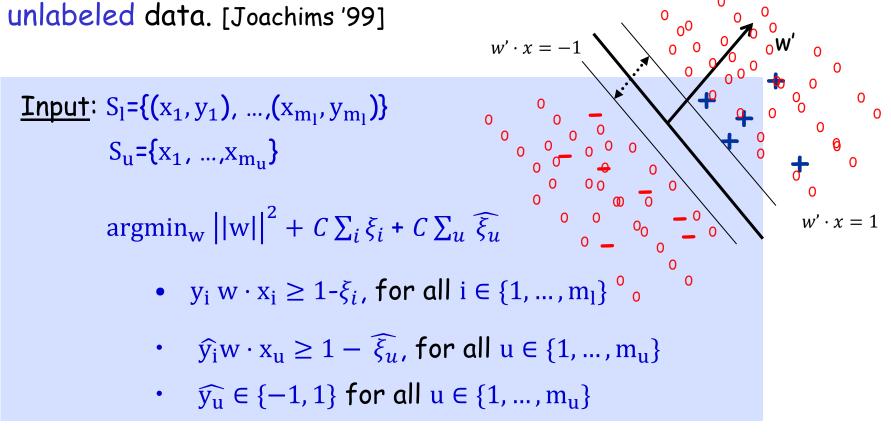
Labeled data only

Optimize for the separator with large margin wrt labeled and

unlabeled data. [Joachims '99] <u>Input</u>: $S_l = \{(x_1, y_1), ..., (x_{m_1}, y_{m_1})\}$ $S_{u} = \{x_{1}, ..., x_{m_{u}}\}$ $\operatorname{argmin}_{w} ||w||^{2} s.t.$ • $y_i w \cdot x_i \ge 1$, for all $i \in \{1, ..., m_l\}$ $\widehat{y_u} w \cdot x_u \ge 1$, for all $u \in \{1, ..., m_u\}$ $\widehat{y_u} \in \{-1, 1\} \text{ for all } u \in \{1, ..., m_u\}$

Find a labeling of the unlabeled sample and w s.t. w separates both labeled and unlabeled data with maximum margin.

Optimize for the separator with large margin wrt labeled and



Find a labeling of the unlabeled sample and w s.t. w separates both labeled and unlabeled data with maximum margin.

Optimize for the separator with large margin wrt labeled and unlabeled data.

```
\begin{split} & \underline{\text{Input}} \colon S_{l} \text{=} \{ (x_{1}, y_{1}), ..., (x_{m_{l}}, y_{m_{l}}) \} \\ & S_{u} \text{=} \{ x_{1}, ..., x_{m_{u}} \} \\ & \text{argmin}_{w} \left| \left| w \right| \right|^{2} + C \sum_{i} \xi_{i} + C \sum_{u} \widehat{\xi_{u}} \\ & \bullet \quad y_{i} \ w \cdot x_{i} \geq 1 \text{-} \xi_{i}, \ \text{for all } i \in \{1, ..., m_{l}\} \\ & \bullet \quad \widehat{y_{i}} w \cdot x_{u} \geq 1 - \widehat{\xi_{u}}, \ \text{for all } u \in \{1, ..., m_{u}\} \\ & \bullet \quad \widehat{y_{u}} \in \{-1, 1\} \ \text{for all } u \in \{1, ..., m_{u}\} \end{split}
```

NP-hard..... Convex only after you guessed the labels... too many possible guesses...

Optimize for the separator with large margin wrt labeled and unlabeled data.

Heuristic (Joachims) high level idea:

- First maximize margin over the labeled points
- Use this to give initial labels to unlabeled points based on this separator.
- Try flipping labels of unlabeled points to see if doing so can increase margin

Keep going until no more improvements. Finds a locally-optimal solution.

Experiments [Joachims99]

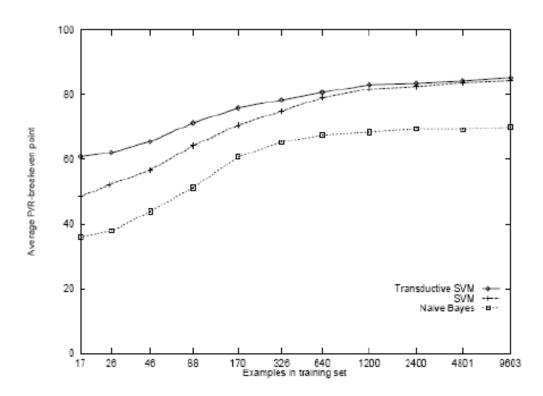
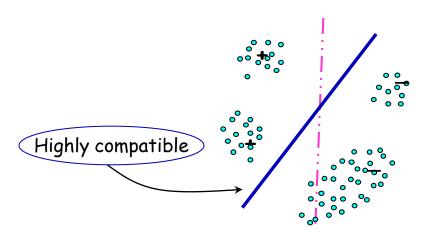


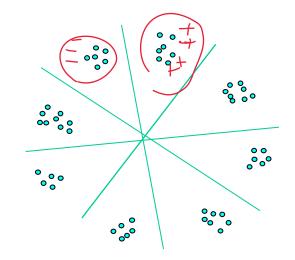
Figure 6: Average P/R-breakeven point on the Reuters dataset for different training set sizes and a test set size of 3,299.

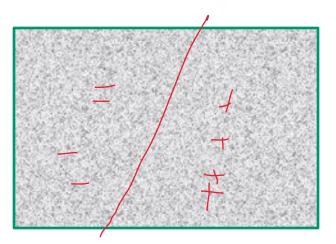
Helpful distribution



Non-helpful distributions

 $1/\gamma^2$ clusters, all partitions separable by large margin





Semi-Supervised Learning

Prominent paradigm in past 15 years in Machine Learning.

Key Insight

Unlabeled data useful if we have beliefs not only about the form of the target, but also about its relationship with the underlying distribution.

Prominent techniques

- Transductive SVM [Joachims '99]
- Co-training [Blum & Mitchell '98]
- Graph-based methods [B&C01], [ZGL03]