SVMs, Kernelized SVMs

Sriram Sankararaman

The instructor gratefully acknowledges Fei Sha, Ameet Talwalkar, Kai-Wei Chang, Eric Eaton, and Jessica Wu whose slides are heavily used, and the many others who made their course material freely available online.

Outline

- Review of last lecture
- 2 SVM Hinge loss
- 3 Kernelized SVMs
- 4 Evaluating ML algorithms

Support Vector Machine

- A linear classifier (hyperplane) that maximizes the margin.
- An alternative view of SVMs.

Outline

- 1 Review of last lecture
- SVM Hinge loss
- 3 Kernelized SVMs
- 4 Evaluating ML algorithms

A general view of supervised learning

Definition Assume $y \in \{-1, 1\}$ and the decision rule is

$$h(\boldsymbol{x}) = \text{SIGN}(a(\boldsymbol{x}))$$
 with $a(\boldsymbol{x}) = \boldsymbol{w}^{T} \boldsymbol{\phi}(\boldsymbol{x}) + \boldsymbol{b}$

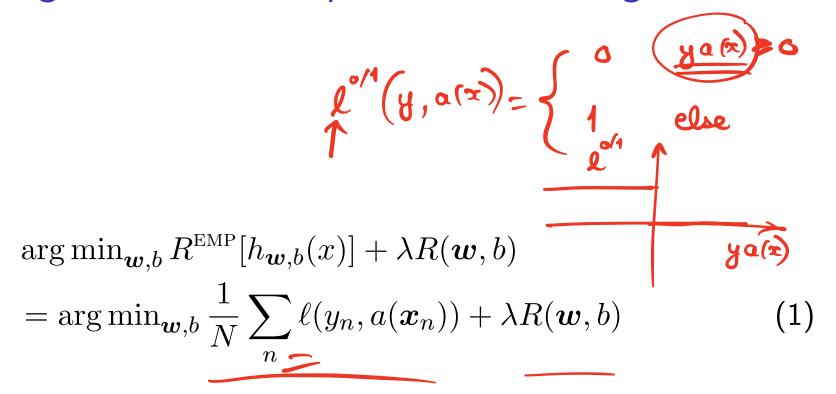
For classification: 0/1 loss

$$\ell^{0/1}(y, a(\boldsymbol{x})) = \begin{cases} 0 & \text{if } \underline{ya(\boldsymbol{x})} \ge 0\\ 1 & \text{otherwise} \end{cases}$$

Minimize weighted sum of empirical risk and regularizer

$$\operatorname{arg\,min}_{\boldsymbol{w},b} \underbrace{R^{\text{EMP}}[h_{\boldsymbol{w},b}(\boldsymbol{x})] + \lambda R(\boldsymbol{w},b)}_{R} = \operatorname{arg\,min}_{\boldsymbol{w},b} \frac{1}{N} \sum_{n} \ell(y_n, a(\boldsymbol{x}_n)) + \lambda R(\boldsymbol{w},b) \tag{1}$$

Minimize weighted sum of empirical risk and regularizer



• Problem with minimizing the 0/1 loss ?

Hinge loss

Definition Assume $y \in \{-1, 1\}$ and the decision rule is $h(\boldsymbol{x}) = \text{SIGN}(a(\boldsymbol{x}))$ with $a(\boldsymbol{x}) = \boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}) + b$,

$$\ell^{\text{HINGE}}(\underline{y}, a(\underline{x})) = \left\{ \begin{array}{c} 0 & \text{if } \underline{ya(x)} \geq 1 \\ 1 - \underline{ya(x)} & \text{otherwise} \end{array} \right.$$

Intuition

$$ya(x) \ge 0$$

 $ya(x) < 1$

Hinge loss

Definition Assume $y \in \{-1,1\}$ and the decision rule is $h(\boldsymbol{x}) = \text{SIGN}(a(\boldsymbol{x}))$ with $a(\boldsymbol{x}) = \boldsymbol{w}^{T} \boldsymbol{\phi}(\boldsymbol{x}) + b$,

$$\ell^{\text{HINGE}}(y, a(\boldsymbol{x})) = \left\{ \begin{array}{c} 0 & \text{if } ya(\boldsymbol{x}) \geq 1 \\ 1 - ya(\boldsymbol{x}) & \text{otherwise} \end{array} \right\}$$

Intuition

- No penalty if raw output, a(x), has same sign and is far enough from decision boundary (i.e., if 'margin' is large enough)
- Otherwise pay a growing penalty, between 0 and 1 if signs match, and greater than one otherwise

Hinge loss

Definition Assume $y \in \{-1,1\}$ and the decision rule is $h(\boldsymbol{x}) = \text{SIGN}(a(\boldsymbol{x}))$ with $a(\boldsymbol{x}) = \boldsymbol{w}^{T} \boldsymbol{\phi}(\boldsymbol{x}) + b$,

$$\ell^{\text{HINGE}}(y, a(\boldsymbol{x})) = \left\{ \begin{array}{cc} \underline{0} & \text{if } ya(\boldsymbol{x}) \geq 1 \\ 1 - ya(\boldsymbol{x}) & \text{otherwise} \end{array} \right.$$

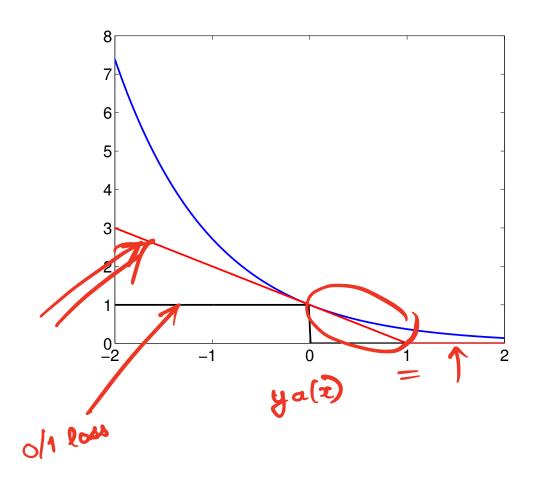
Intuition

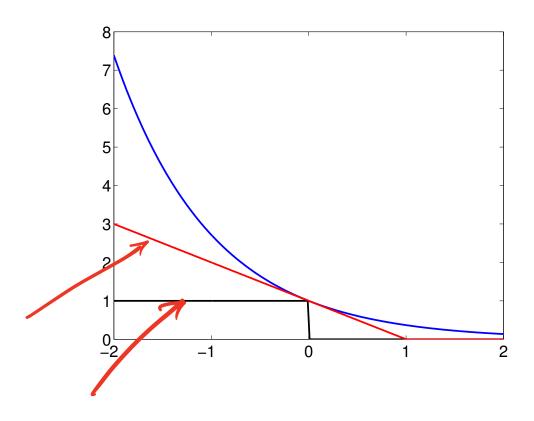
- No penalty if raw output, a(x), has same sign and is far enough from decision boundary (i.e., if 'margin' is large enough)
- Otherwise pay a growing penalty, between 0 and 1 if signs match, and greater than one otherwise

Convenient shorthand

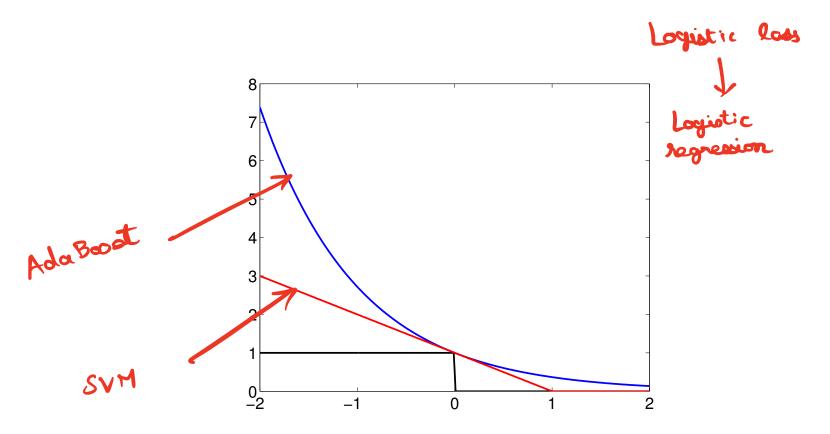
$$\ell^{\text{HINGE}}(y, a(\boldsymbol{x})) = \max(0, 1 - ya(\boldsymbol{x})) = (1 - ya(\boldsymbol{x})) + (1 - ya$$



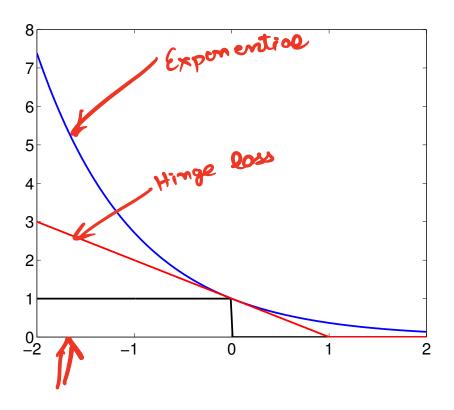




- Upper-bound for 0/1 loss function (black line)
- We use hinge loss as a *surrogate* to 0/1 loss Why?



- Upper-bound for 0/1 loss function (black line)
- We use hinge loss as a *surrogate* to 0/1 loss Why?
- Hinge loss is convex, and thus easier to work with.



- Other surrogate losses can be used, e.g., exponential loss for Adaboost (in blue), logistic loss (not shown) for logistic regression
- Hinge loss less sensitive to outliers than exponential (or logistic) loss

Primal formulation of support vector machines (SVM)

Minimizing the total hinge loss on all the training data with l_2 regularization

$$\min_{\boldsymbol{w},b} \sum_{n} \max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_n) + b]) + \sum_{n=1}^{\lambda} \|\boldsymbol{w}\|_2^2$$

Analogous to l_2 regularized least squares, as we balance between two terms (the loss and the regularizer).

Hinge loss

$$a(x) = \left[w^{T} \phi(x) + b \right]$$

Primal formulation of support vector machines (SVM)

Minimizing the total hinge loss on all the training data with l_2 regularization

Analogous to l_2 regularized least squares, as we balance between two terms (the loss and the regularizer).

Previously, we used geometric arguments to derive:

$$\lim_{\substack{\boldsymbol{w},b,\boldsymbol{\xi}\\ \boldsymbol{w},b,\boldsymbol{\xi}}} \frac{1}{2} \|\boldsymbol{w}\|_2^2 + C \sum_{n} \xi_n$$
 s.t. $y_n[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_n) + b] \geq 1 - \xi_n$ and $\xi_n \geq 0, \quad n \in \{1,\dots,N\}$ Do these yield the same solution?

Recovering our previous SVM formulation

Minimizing the total hinge loss on all the training data

$$\min_{\boldsymbol{w},b} \sum_{n} \max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_n) + b]) + \lambda \boldsymbol{w}_{2}^{\lambda} \boldsymbol{w}_{2}^{2}$$

Define $C = 1/\lambda$:

$$\min_{\boldsymbol{w},b} \sum_{\boldsymbol{x}} \max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_n) + b]) + \frac{1}{2} \|\boldsymbol{w}\|_2^2$$

Recovering our previous SVM formulation

Minimizing the total hinge loss on all the training data

$$\min_{\boldsymbol{w},b} \sum_{n} \max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_n) + b]) + \frac{\lambda}{2} ||\boldsymbol{w}||_2^2$$

Define $C = 1/\lambda$:

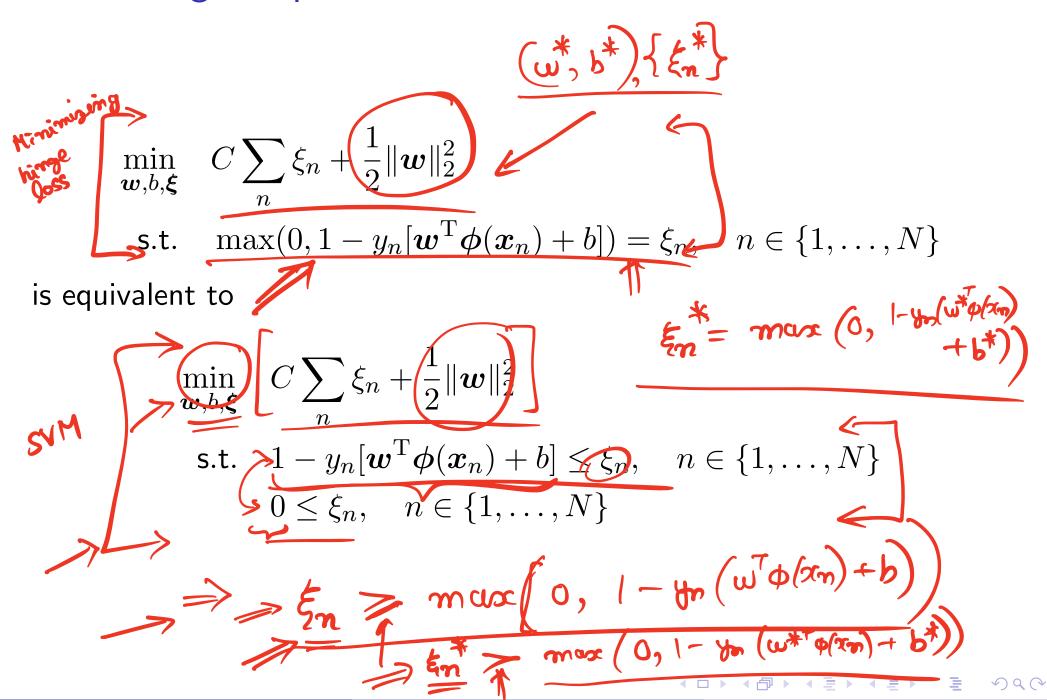
$$\min_{\boldsymbol{w},b} C \sum_{n} \max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_n) + b]) + \frac{1}{2} \|\boldsymbol{w}\|_2^2$$

Define
$$\xi_n = \max(0, 1 - y_n[\boldsymbol{w^T\phi(x_n)} + b])$$

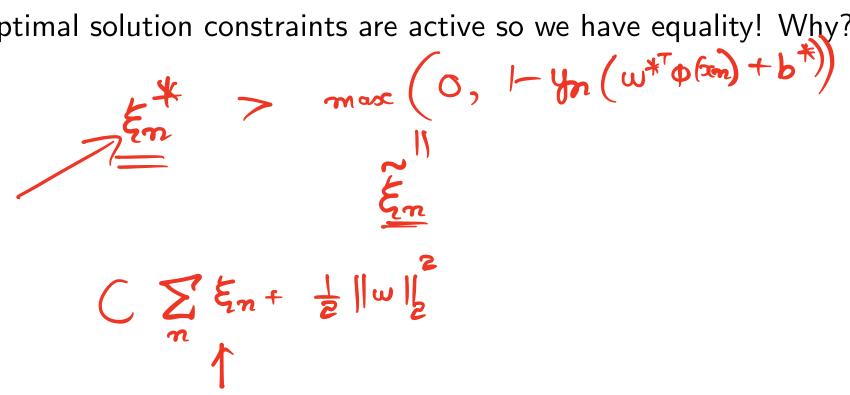
$$\min_{\boldsymbol{w},\boldsymbol{k},\boldsymbol{\xi}} C \sum_{n} \xi_{n} + \frac{1}{2} \|\boldsymbol{w}\|_{2}^{2}$$

s.t.
$$\max(0, 1 - y_n[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_n) + b]) = \xi_n, \quad n \in \{1, \dots, N\}$$

Recovering our previous SVM formulation



At optimal solution constraints are active so we have equality! Why?



At optimal solution constraints are active so we have equality! Why?

- If $\xi_n^* > \max(0, 1 y_n f(\boldsymbol{x}_n))$, we could choose $\bar{\xi}_n < \xi_n^*$ and still satisfy the constraint while reducing our objective function!
- Since $c \ge \max(a, b) \iff c \ge a, c \ge b$, we recover previous formulation

Outline

- 1 Review of last lecture
- 2 SVM Hinge loss
- Kernelized SVMs
- 4 Evaluating ML algorithms

Goal: Kernelize SVMs



- Rewrite the SVM optimization problem so that it no longer depends on $\phi(x_n)$ but instead depends only on inner products $\phi(x_n)^{\mathrm{T}}\phi(x_m)$.
- If we can do this, we can then replace $\phi(x_n)^{\mathrm{T}}\phi(x_m)$ with a kernel function $k(x_n,x_m)$.

Primal formulation of support vector machines (SVM)

$$\min_{\boldsymbol{w},b,\boldsymbol{\xi}} \quad \frac{1}{2} \|\boldsymbol{w}\|_2^2 + C \sum_n \xi_n$$
 s.t. $\widehat{y_n[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_n) + b]} \geq 1 - \xi_n$ and $\xi_n \geq 0, \quad n \in \{1,\dots,N\}$

This can be converted to its dual form.

Dual formulation of SVM

Let $\underline{\underline{w}}_*$ be the minimizer of the SVM problem for training data: $\{(x_n, y_n)\}.$

Then $w_* = \sum_n \alpha_n y_n \phi(x_n)$ for a new set of dual variables: $\alpha_n \geq 0$.

Dual formulation of SVM

Dual is also a convex program

$$\max_{\boldsymbol{\alpha}} \left(\sum_{n} \alpha_{n} - \frac{1}{2} \sum_{\underline{m,n}} \underline{y_{m} y_{n}} \alpha_{m} \alpha_{n} \boldsymbol{\phi}(\boldsymbol{x}_{m})^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_{n}) \right)$$
s.t. $0 \le \alpha_{n} \le \underline{C}, \quad n \in 1, \dots, N$

$$\sum_{n} \alpha_{n} y_{n} = 0$$

There are N dual variable $\underline{\underline{\alpha}}_n$, one for each constraint in the primal formulation

Kernel SVM

We replace the inner products $\phi(x_m)^{\mathrm{T}}\phi(x_n)$ with a kernel function

$$\sum_{\alpha} \sum_{n} \alpha_{n} - \frac{1}{2} \sum_{m,n} y_{m} y_{n} \alpha_{m} \alpha_{n} k(\boldsymbol{x}_{m}, \boldsymbol{x}_{n})$$
s.t. $0 \le \alpha_{n} \le C, \quad n \in 1, \dots, N$

$$\sum_{n} \alpha_{n} y_{n} = 0$$

We can define a kernel function to work with nonlinear features and learn a nonlinear decision surface

Recovering solution to the primal formulation



Weights \underline{w} (primal variables) relation to $\underline{\alpha}$ (dual variables)

$$w = \sum_{n} y_{n} (x_{n}) \phi(x_{n}) \leftarrow \text{Linear combination of the input features}$$

Prediction on a test point \boldsymbol{x}

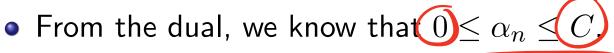
$$h(\boldsymbol{x}) = \operatorname{SIGN}(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}) + b) = \operatorname{SIGN}(\sum_{n} y_{n}\alpha_{n}k(\boldsymbol{x}_{n}, \boldsymbol{x}) + b)$$

At test time it suffices to know the kernel function!

Recovering solution to the primal formulation

We already identified the primal variable $oldsymbol{w}$ as

$$\underline{\boldsymbol{w}} = \sum_{n} \alpha_{n} y_{n} \boldsymbol{\phi}(\boldsymbol{x}_{n})$$

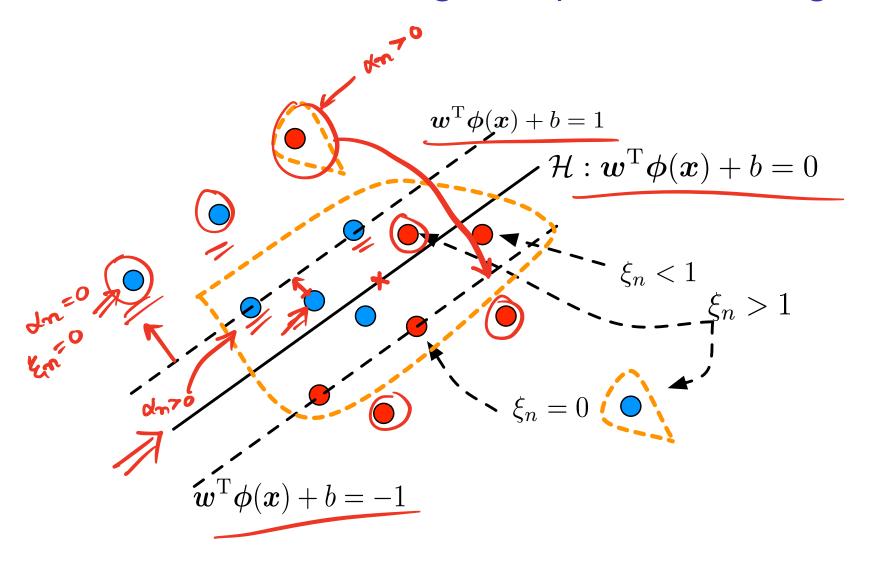




- If $\alpha_n=0$, then the example n does not affect the hyperplane/decision boundary computed by SVM. $y_n[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_n)+b]\geq 1.$
- Only those examples with $\alpha_n > 0$ affect the hyerplane/decision boundary. These examples are termed support vectors.
- When will $\alpha_n > 0$?



Visualization of how training data points are categorized



Support vectors are highlighted by the dotted orange lines

Outline

- 1 Review of last lecture
- 2 SVM Hinge loss
- 3 Kernelized SVMs
- 4 Evaluating ML algorithms

Binary classification

Goal is to achieve high accuracy

Accuracy: defined to be the mean of the 0/1 loss $l(y, \hat{y})$.

$$\ell(y, h(\boldsymbol{x})) = \frac{1\{y \neq h(\boldsymbol{x})\}}{1}$$
 $R^{\text{EMP}}[h(\boldsymbol{x})] = \frac{1}{N} \sum_{n} \ell(h(\boldsymbol{x}_n), y_n)$

Assumes $y \in \{0,1\}$ and h outputs values in $\{0,1\}$.

Binary classification

Goal is to achieve high accuracy

Accuracy: defined to be the mean of the 0/1 loss $l(y, \hat{y})$.

$$\ell(y, h(\boldsymbol{x})) = \mathbf{1}\{y \neq h(\boldsymbol{x})\}$$
 $R^{\text{EMP}}[h(\boldsymbol{x})] = \frac{1}{N} \sum_{n} \ell(h(\boldsymbol{x}_n), y_n)$

Assumes $y \in \{0,1\}$ and h outputs values in $\{0,1\}$.

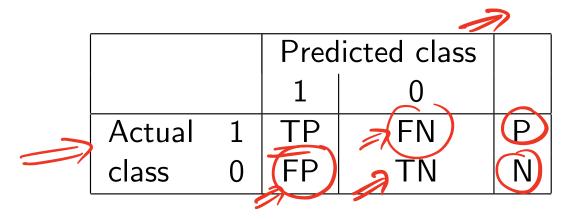
May not be what we want

Is this email spam?

Does the patient have cancer?

Confusion matrix

Given a dataset of P positive instances and N negative instances,



P = Positive, N = Negative

TN = True negative, FP = False positive

TP = True positive, FN = False negative

Spam classification

Positive : spam, Negative: non-spam

TP: Spam email classified as spam

• FP: Non-spam email classified as spam

Confusion matrix

Given a dataset of P positive instances and N negative instances,

		Pred		
		1	0	
Actual	1	TP	FN	Р
class	0	FP	TN	N

P = Positive, N = Negative

TN = True negative, FP = False positive

TP = True positive, FN = False negative

• Accuracy =
$$\frac{TP+TN}{P+N}$$

• Error = 1 - Accuracy

Confusion matrix

Given a dataset of P positive instances and N negative instances,

		Pred		
		1	0	
Actual	1	TP	FN	Р
class	0	FP	TN	N

P = Positive, N = Negative

TN = True negative, FP = False positive

TP = True positive, FN = False negative

- True Positive Rate (TPR) = Recall = Sensitivity = $\frac{\mathrm{TP}}{\mathrm{P}}$
- Probability of classifying a spam email as spam.

Confusion matrix

Given a dataset of P positive instances and N negative instances,

		Pred		
		1	0	
Actual	1	TP	FN	Р
class	0	FP	TN	N

P = Positive, N = Negative

TN = True negative, FP = False positive

TP = True positive, FN = False negative

- Specificity $=\frac{TN}{N}$
- Probability of classifying a non-spam email as non-spam.
- ullet False Positive Rate (FPR) = 1 Specificity

Confusion matrix

Given a dataset of P positive instances and N negative instances,

		Pred		
		1	0	
Actual	1	(TP)	FN	Р
class	0	FP	TN	N

P = Positive, N = Negative

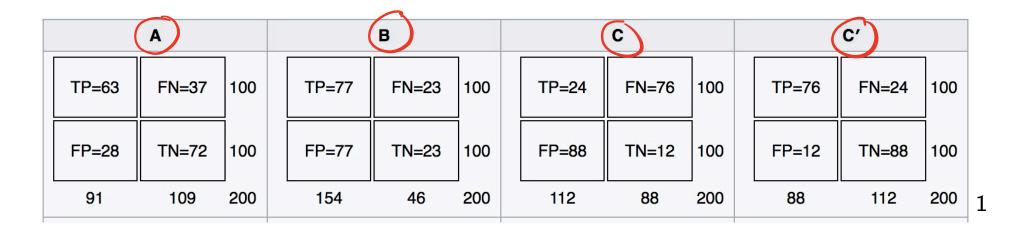
TN = True negative, FP = False positive

TP = True positive, FN = False negative

- Precision = Positive Predictive Value (PPV) = $\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}}$
- Probability that an email classified as spam is spam.
- Different from specificity!

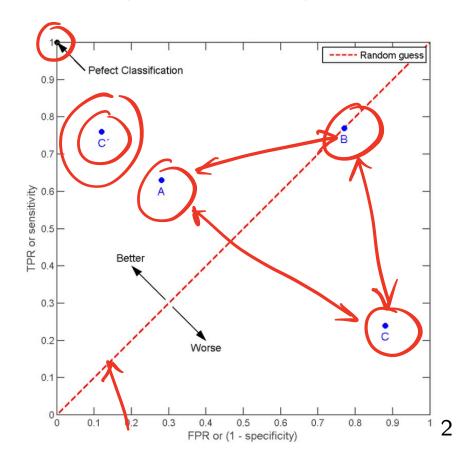
Visualizing performance

Many different performance measures



ROC curve

TPR (sensitivity) vs FPR (1-specificity)



- Best possible method is in the upper left corner.
- Random guess would fall on the diagonal.

Sometimes we care about the confidence of predictions

- For linear models (e.g., perceptron, logistic regression), the activation $a(\mathbf{x}) = \mathbf{w}^{\mathrm{T}}\mathbf{x} + b$ gives us a ranking of the predictions.
- In the case of the perceptron, given \underline{x}_1 and \underline{x}_2 such that $a(\underline{x}_1) > a(\underline{x}_2) > 0$.
 - lacksquare Both $\widehat{x_1}$ and x_2 are classified as positive.
 - ightharpoonup Perceptron is more confident in the prediction for x_1 than for x_2 .

ROC curve allows us to visualize the ranking of predictions

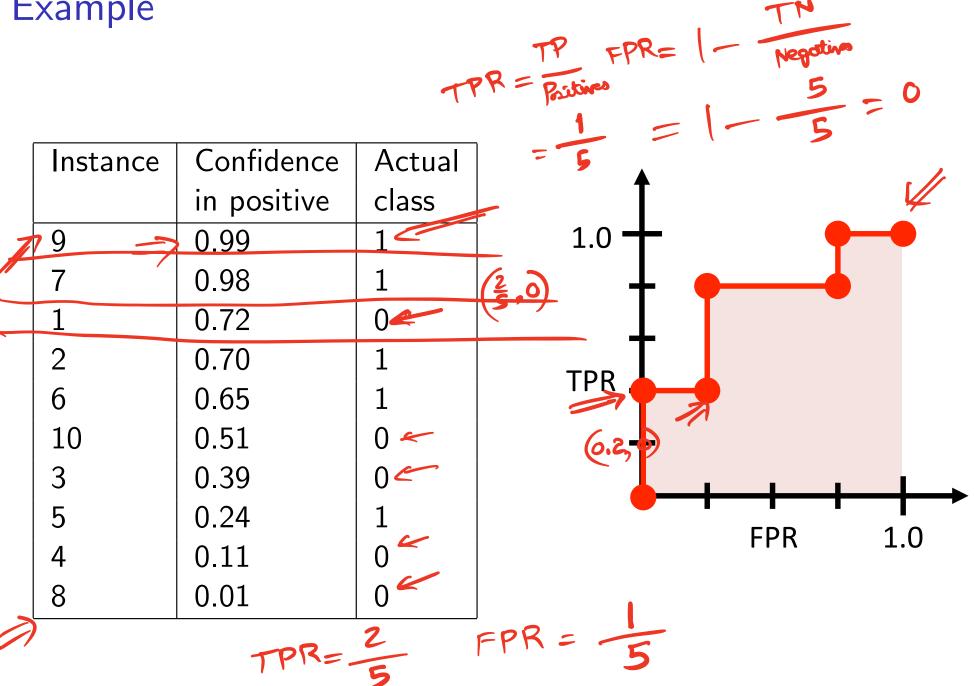
- Sort the instances according to the confidence of instance being in class 1 (positive class).
 - How confident is the classifier that an email is spam?

- Sort the instances according to the confidence of instance being in class 1 (positive class).
 - How confident is the classifier that an email is spam?
- Step through the sorted list from high to low confidence.
- As you step through, build a binary classifier that predicts the top k instances as belonging to class 1 and the remaining to class 0.
 - How aggressively do you want to mark a message as spam ?

- Sort the instances according to the confidence of instance being in class 1 (positive class).
 - How confident is the classifier that an email is spam?
- Step through the sorted list from high to low confidence.
- As you step through, build a binary classifier that predicts the top k instances as belonging to class 1 and the remaining to class 0.
 - How aggressively do you want to mark a message as spam ?
- Compute the TPR (True Positive Rate) and FPR (False Positive Rate).
 - High up in the list: Low TPR and low FPR.
 - As we move down, TPR increases but so does FPR.

- Sort the instances according to the confidence of instance being in class 1 (positive class).
 - How confident is the classifier that an email is spam?
- Step through the sorted list from high to low confidence.
- As you step through, build a binary classifier that predicts the top k instances as belonging to class 1 and the remaining to class 0.
 - How aggressively do you want to mark a message as spam ?
- Compute the TPR (True Positive Rate) and FPR (False Positive Rate).
 - High up in the list: Low TPR and low FPR.
 - As we move down, TPR increases but so does FPR.
- Plot TPR vs FPR.

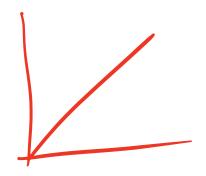
Example



Interpreting ROC curves

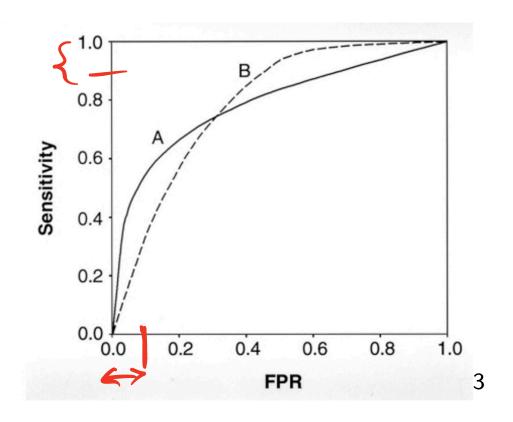
Area under the ROC Curve (AUC or AUROC)

- The probability that a classifier will rank a randomly chosen positive instance (instance with class label 1) higher than a randomly chosen negative one (instance with class label 0).
- A measure of the overall performance of a classifier.
- A random classifier has AUROC = $\frac{1}{2}$.
- A perfect classifier has AUROC = 1.



Interpreting ROC curves

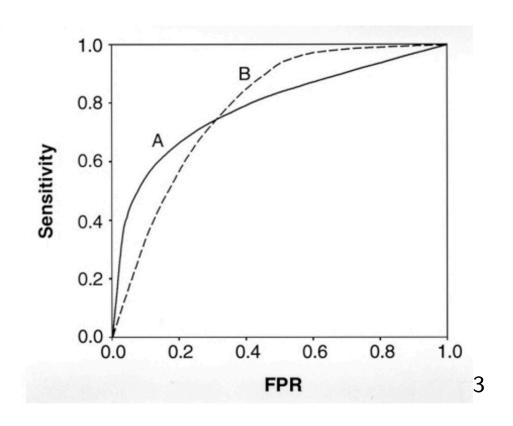
Classifiers A and B with equal AUROC



Which one do we choose?

Interpreting ROC curves

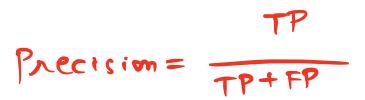
Classifiers A and B with equal AUROC



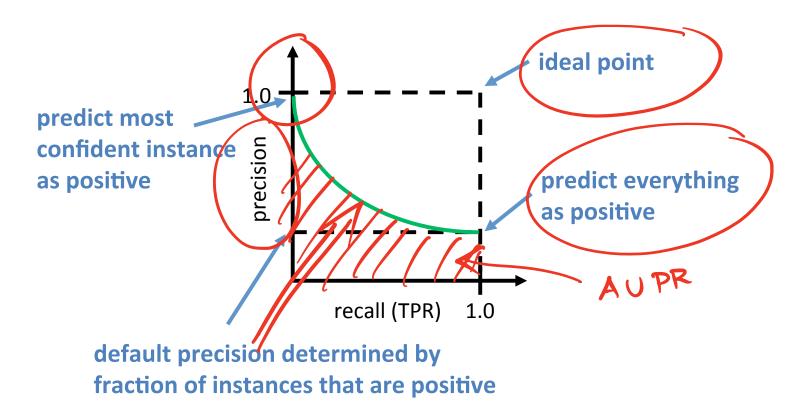
Which one do we choose?

Depends on whether we care about sensitivity or FPR

Other trade-offs



Precision-recall curve



Interpreting precision-recall curves

Area under the precision-recall curve (AUPR)

• Can compute the area under the precision-recall curve.

Interpreting precision-recall curves

F₁-score

$$F_1 = \frac{1}{\frac{1}{2} \frac{1}{\text{PRECISION}} + \frac{1}{2} \frac{1}{\text{RECALL}}}$$

- Want F₁ to be high.
- The Harmonic mean of precision and recall.
- A single number that trades off precision and recall.
- If a classifier has high precision and low recall (or other way round), its F_1 -score will be low.
- Encourages precision and recall values that are similar.

Summary

- Many ways to measure accuracy.
- Think carefully about which ones are most relevant.
- Often there are trade-offs
 - TPR vs FPR, Precision vs recall
- Graphical displays useful.
 - ▶ ROC and Precision-recall curves display performance at various levels of confidence.
 - ▶ Can be summarized by area under the curve (AUROC, AUPR) as well as numbers such as the F_1 -score.