281 Live Session

Week 12 — 2023/4/5

Agenda

- Final project updates
- Linear Classifiers overview
- Practical applications of SVMs
- Exercise: Face Classification (Part 1)

Project Updates

Order: Vehicles, Satellite, Recycling, Fruit

This week: PCA results

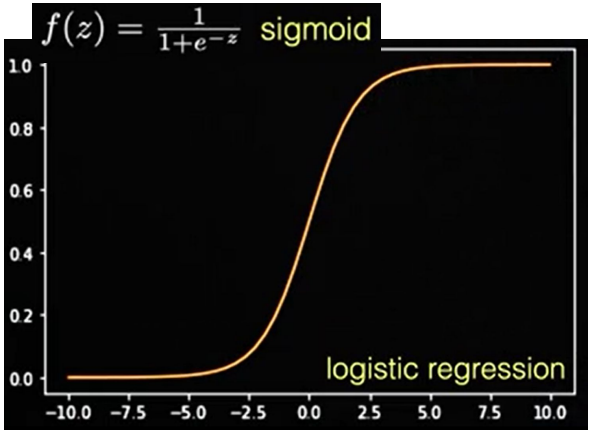
Next week: Confusion matrix

Big picture

Intuition goals:

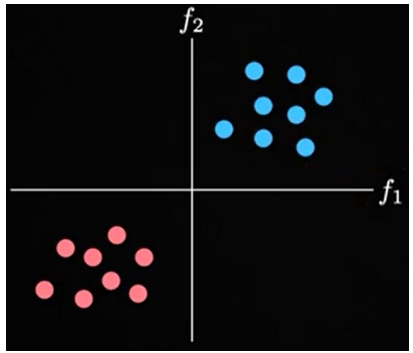
- What is a classifier model?
- How do we evaluate quality of fit?
- Is it better to have more false positives or false negatives? Why?
- What is the goal of an LDA classifier?
- What is the goal of an SVM classifier?
- Why do we maximize the margin?

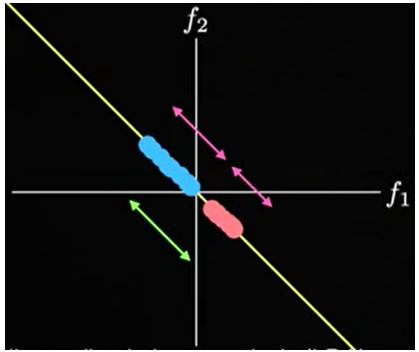
Overview — Linear classifiers



y -> class label
wx -> model output
f(z) -> sigmoid

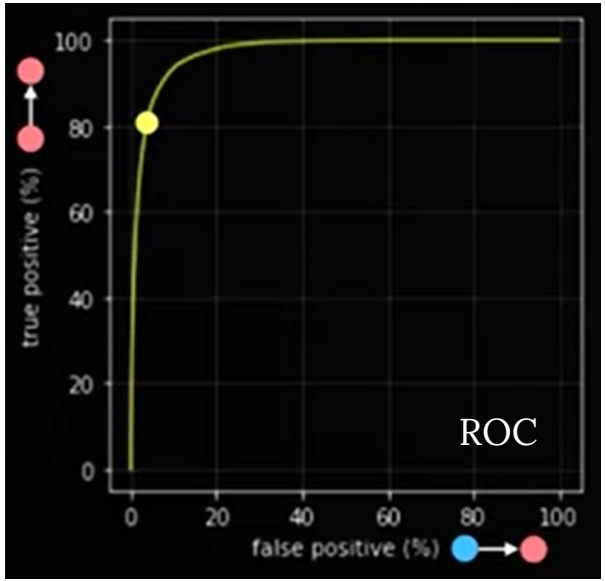
$$P(Y = y \mid X = \vec{x}) = [f(\vec{w}^t\vec{x})]^y \cdot [1 - f(\vec{w}^t\vec{x})]^{1-y}$$

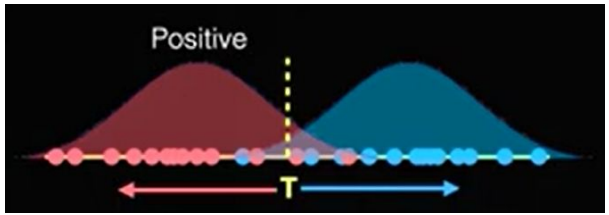




Two covariance matrices - within & across

Overview — Classifier evaluation





Confusion Matrix

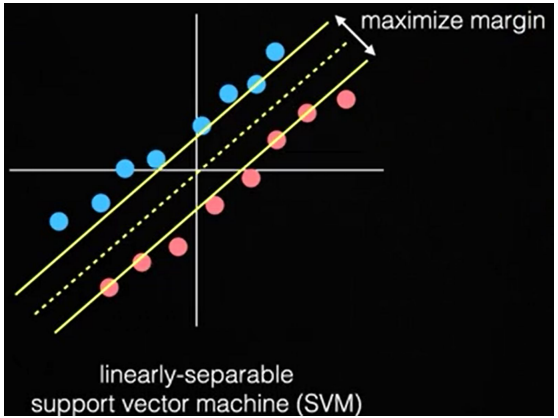
Predicted \ Expected	1	2	3	4
1	52	3	7	2
2	2	28	2	0
3	5	2	25	12
4	1	1	9	40

False Positive (I)
False Negative (II)

Distributions must be separable to perform classification

Error tolerance depends on specific application domain

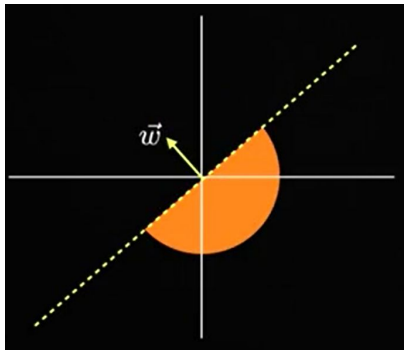
Overview — Support vector machines (SVMs)

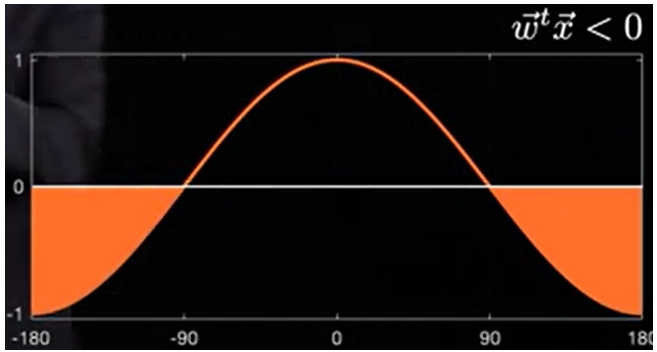


goal is to maximize distance between boundary points

classification -> sign of dot product between w and our boundary plane

minimize inverse of $\lambda||w||$ subject to classification constraint





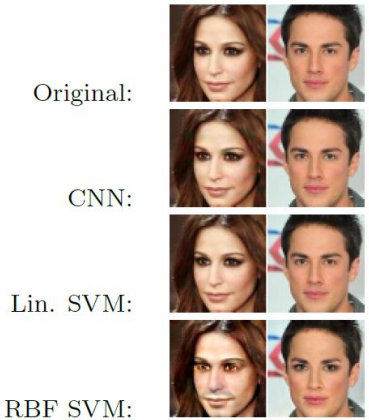
Big picture

Intuition goals:

- What is a classifier model?
- How do we evaluate quality of fit?
- Is it better to have more false positives or false negatives? Why?
- What is the goal of an LDA classifier?
- What is the goal of an SVM classifier?
- Why do we maximize the margin?

Practical Applications of SVMs

Maximizing the margin produces a more robust classifier



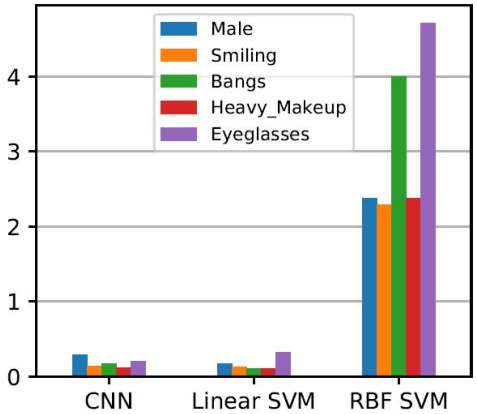
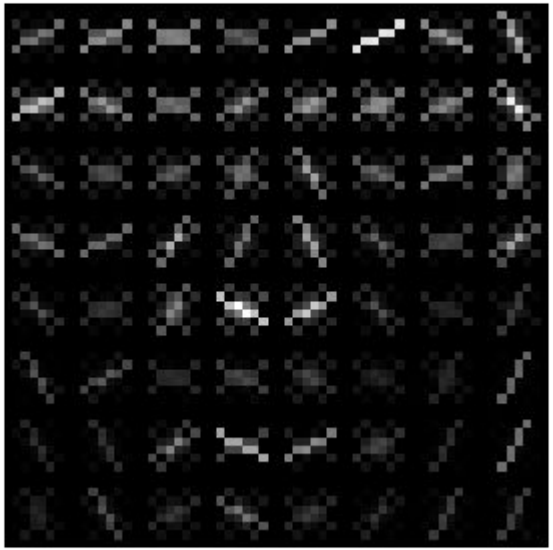


Figure 11: Adversarial examples for class Male/Female (left) and mean perturbation sizes (right) for different models trained on real CelebA images – results are consistent with our other experiments.

Richardson, Eitan, and Yair Weiss. "A bayes-optimal view on adversarial examples." *The Journal of Machine Learning Research* 22.1 (2021): 10076-10103.

Group Exercise – Face Classification Part 1



Upcoming ToDo’s

Watch Async lectures for Unit 12

Final Projects - Confusion Matrix

Final Presentations will be in class April 19th

Final Reports will be due Sunday April 23rd