# Introduction

ECE 449, Machine Learning

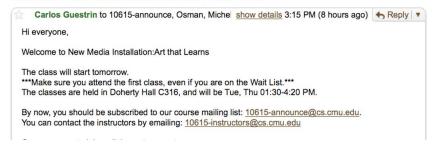
#### Classification

• From data to discrete classes

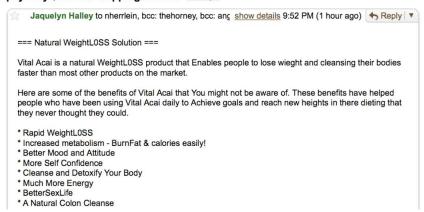
## Examples: Spam Filtering

#### Data

#### Welcome to New Media Installation: Art that Learns



#### Natural \_LoseWeight SuperFood Endorsed by Oprah Winfrey, Free Trial 1 bottle, pay only \$5.95 for shipping mfw rlk $_{\mbox{\tiny Spam}}$ $|\times$



#### Prediction

Spam/Not Spam

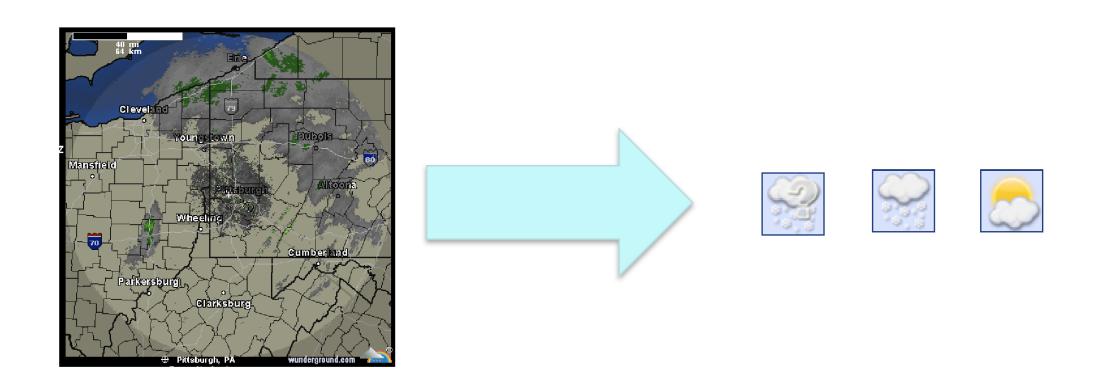
## Examples: Image Classification







## Examples: Weather Prediction



## Regression

• Predicting a numeric value

## Examples: Stock Market

Predict stock prices given stock history and today's news



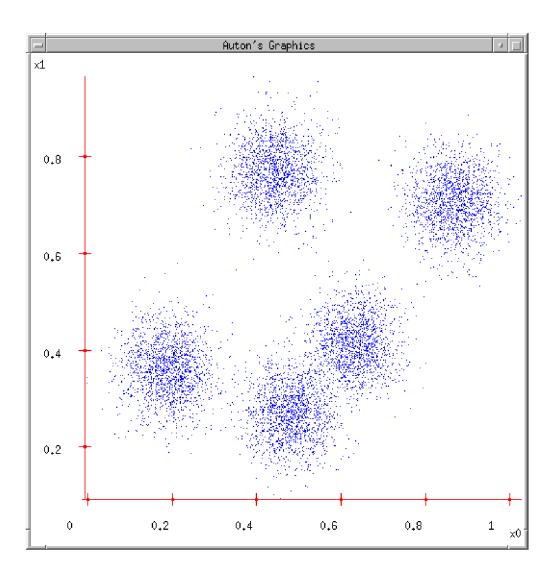
## Examples: Weather Prediction Revisited



## Clustering

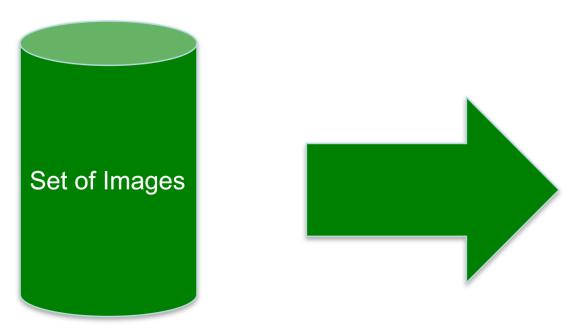
• Discovering structure in data

## Examples: Clustering Data



## Examples: Clustering Images

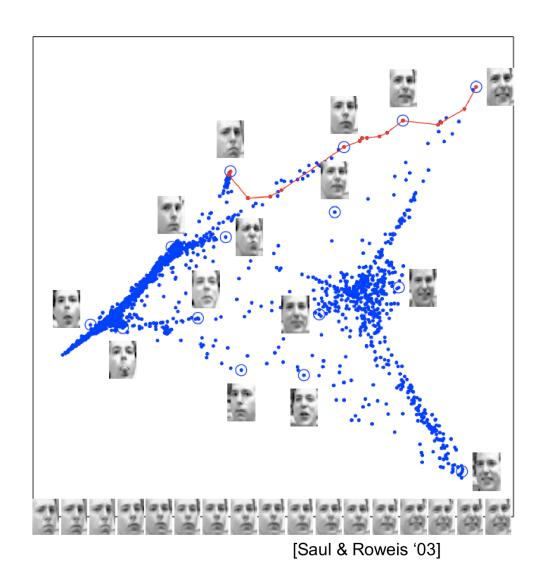




## Embedding

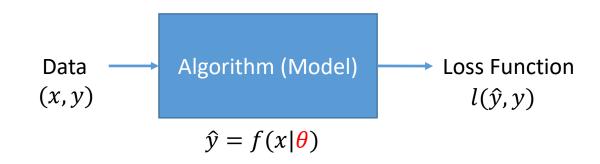
• Visualization and discriminative feature learning

## Examples: Face Embedding



#### Big Picture

- Algorithms that give computers the ability to learn from experience (data) to do specific tasks
  - Different tasks use different types of data, different learning algorithms
  - Performance driven learning: minimize loss function



x: Input data

y: Ground truth label or supervision signal

 $\theta$ : Model parameters

 $f(x|\theta)$ : Mapping from input to the target output

*l*: Loss function

#### Types of Data

- Data can be
  - Binary, numerical or categorical (ordered or not) or a combination
  - A vector/matrix/graph
- Raw input data gets mapped to numerical or indicator form (feature extraction)
- Form of output data impacts loss function

## Types of Learning Algorithms/Models

- Supervised learning
  - Learning data includes examples with target output, goal is to find a decision function
- Unsupervised learning
  - Learning data has no target output, goal is to learn interesting structure
- Reinforcement learning
  - Sequential decision making in a scenario with changing state and occasional reward/penalty
- Semi-supervised learning, active learning, incremental learning, curriculum learning, federated learning ...

#### Types of Loss Function

 Mean squared error (usually for regression, i.e., the goal is to predict continuous numerical values)

• 
$$\frac{1}{N}\sum (y_i - \hat{y}_i)^2$$

- Cross entropy (usually for classification, i.e., the goal is to predict discrete classes)
  - $-\sum_{i=1}^{C} y_i \log \hat{y}_i$

## Supervised Learning

- Learning Data = input-output pairs  $\{(x_i, y_i) | i = 1, 2, ..., N\}$
- Given input x, predict output y
- Learn decision function  $\hat{y} = f(x)$  using loss function  $l(\hat{y}, y)$
- Tasks
  - Classification: y is categorical (class label)
  - Regression: *y* is numerical

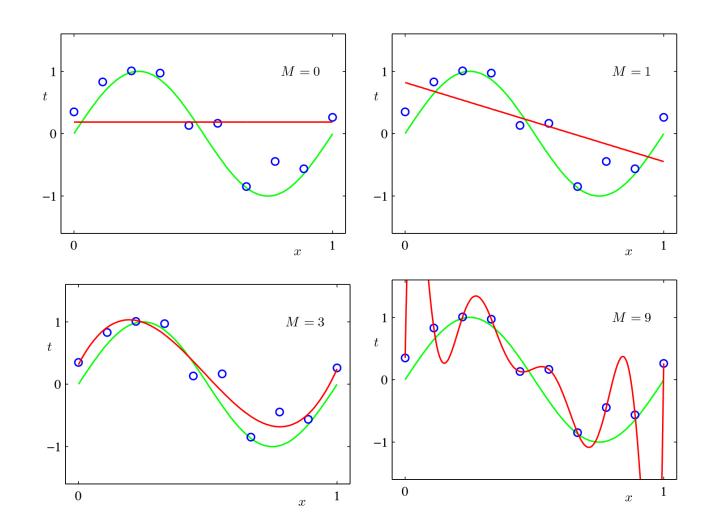
## Training and Inference/Testing

- Training
  - Given data (x, y), algorithm, minimize the loss function to estimate the model parameters  $\theta$
- Inference/Testing
  - Given data x (without y), algorithm and model parameters  $\theta$ , get the prediction  $\hat{y} = f(x|\theta)$

## Machine Learning Options

- Non-parametric
  - use the data directly
  - Ex: nearest-neighbor
- Parametric
  - Assume a particular distribution
    - Ex: Gaussian → find mean & var from data
  - Assume a functional form
    - Ex: linear  $(a^tx) \rightarrow find coeffs a^t from data$

- Example
  - N-th order regression



- Consider the regression problem
- Assume the perfect decision function exists: y = f(x)

$$MSE = E_{\mathcal{T}} \left[ (\hat{y}_0 - f(x_0))^2 \right]$$

$$= E_{\mathcal{T}} [(\hat{y}_0 - E_{\mathcal{T}}[\hat{y}_0])^2] + (E_{\mathcal{T}}[\hat{y}_0] - f(x_0))^2$$

$$= Var(\hat{y}_0) + Bias^2(\hat{y}_0)$$

• where  $\mathcal{T}$  is the training set (random samples)

$$MSE(x_0) = E_{\mathcal{T}} \left[ \left( \hat{y}_0 - f(x_0) \right)^2 \right]$$

$$= E_{\mathcal{T}} \left[ \left( \hat{y}_0 - E_{\mathcal{T}} [\hat{y}_0] + E_{\mathcal{T}} [\hat{y}_0] - f(x_0) \right)^2 \right]$$

$$= E_{\mathcal{T}} \left[ \left( \hat{y}_0 - E_{\mathcal{T}} [\hat{y}_0] \right)^2 \right] + E_{\mathcal{T}} \left[ \left( E_{\mathcal{T}} [\hat{y}_0] - f(x_0) \right)^2 \right]$$

$$+ 2E_{\mathcal{T}} \left[ \left( \hat{y}_0 - E_{\mathcal{T}} [\hat{y}_0] \right) \left( E_{\mathcal{T}} [\hat{y}_0] - f(x_0) \right) \right]$$

$$= E_{\mathcal{T}} \left[ \left( \hat{y}_0 - E_{\mathcal{T}} [\hat{y}_0] \right)^2 \right] + \left( E_{\mathcal{T}} [\hat{y}_0] - f(x_0) \right)^2$$

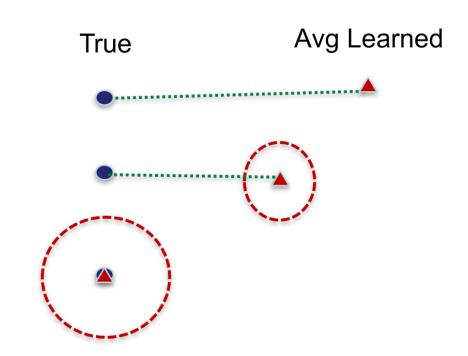
$$= Var(\hat{y}_0) + Bias^2(\hat{y}_0)$$

- Bias = distance between average model & theoretical best
- Variance = variability with different training samples

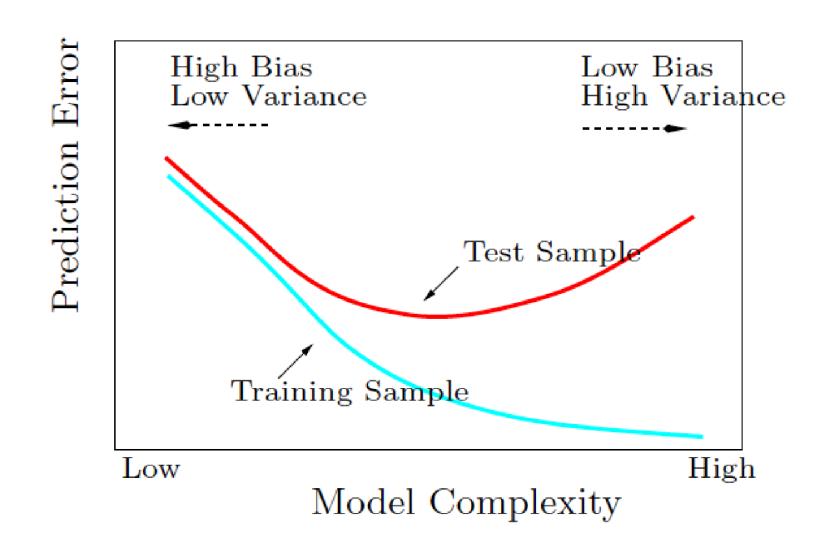
Deterministic classifier  $\alpha(x) = \omega_j \ \forall x$ 

Linear classifier

True n-th order classifier

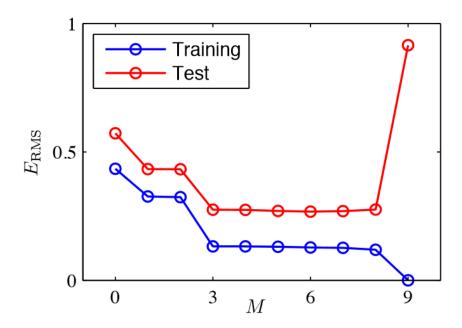


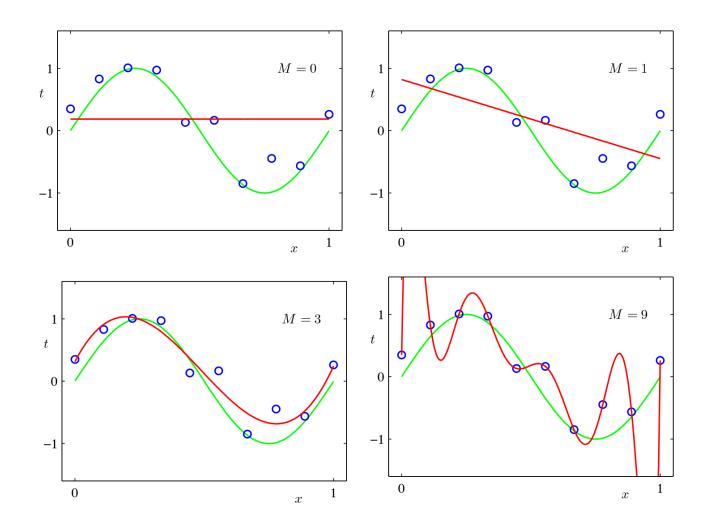
## Given a Fixed Training Set



## Examples

• N-th order regression





#### Set the Hyper-Parameters

- The model complexity ≫ #training samples → overfitting
- Whether overfitting → check the testing error
- What happens when # samples N grows?
  - For a specific model: variance ↓as N ↑
- Model complexity also depends on feature dimensionality d (higher d more params)
  - For y=Ax: scalar x,y  $\rightarrow$  scalar A, vector x,y  $\rightarrow$  d<sub>y</sub>d<sub>x</sub> params in A
  - Dimensionality reduction (feature selection or projection, supervised or unsupervised)
  - Feature extraction driven by domain knowledge

#### Practical Implications

- ALWAYS assess performance on data that you haven't looked at in training or model selection (independent test set)
- What does it mean to be "independent"?
  - Two sentences in the same document are not independent
  - Two segments in the same image are not independent
- Use regularization to encourage some parameters to be small

Training Data

**Test Data** 

#### Practical Implications

- Use a held-out validation set or cross-validation for model selection and parameter tuning
- Cross-validation (CV)
  - Partition data into N subsets
  - Train on N-1, validate on Nth
  - Rotate through all N options
  - Choose best configuration
  - Retrain on all the data with best config
- Trade-offs of CV vs. held-out
  - CV makes better use of small data sets
  - CV is more expensive

Training Data

Validation Set

Test Data

## Other Wrong "Model" Problems

- Training data is not representative → impacts all ML approaches
- Could be due to
  - Sampling bias
  - Noisy observations
  - Samples are not independent