### **Lecture #3: Machine Learning**

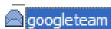
Janardhan Rao (Jana) Doppa

School of EECS, Washington State University

 "If you invent a breakthrough in artificial intelligence, so machines can learn," Mr. Gates responded, "that is worth 10 Microsofts."

(Quoted in NY Times, Monday March 3, 2004)

### Spam filtering



GOOGLE LOTTERY WINNER! CONTAC

From: googleteam To:

Subject: GOOGLE LOTTERY WINNER! CONTACT YOUR AGENT TO CLAIM YOUR PRIZE.

GOOGLE LOTTERY INTERNATIONAL

INTERNATIONAL PROMOTION / PRIZE AWARD .

(WE ENCOURAGE GLOBALIZATION)

FROM: THE LOTTERY COORDINATOR,

GOOGLE B.V. 44 9459 PE.

RESULTS FOR CATEGORY "A" DRAWS

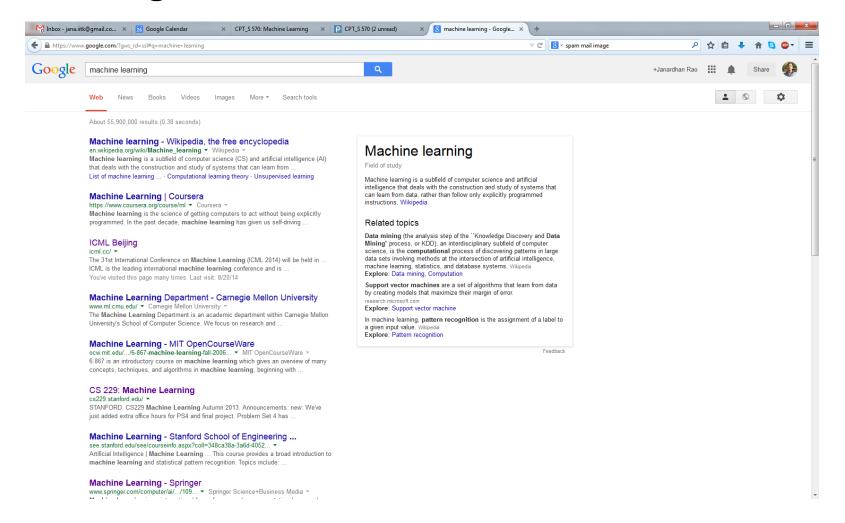
Congratulations to you as we bring to your notice, the results of the First Ca inform you that your email address have emerged a winner of One Million (1,0 money of Two Million (2,000,000.00) Euro shared among the 2 winners in this email addresses of individuals and companies from Africa, America, Asia, Au CONGRATULATIONS!

Your fund is now deposited with the paying Bank. In your best interest to avo award strictly from public notice until the process of transferring your claims | NOTE: to file for your claim, please contact the claim department below on e

Optical Character Recognition (OCR)



### Search engines



Automatic Translation



Recommendation Engines



<sup>&</sup>gt; View or edit your browsing history

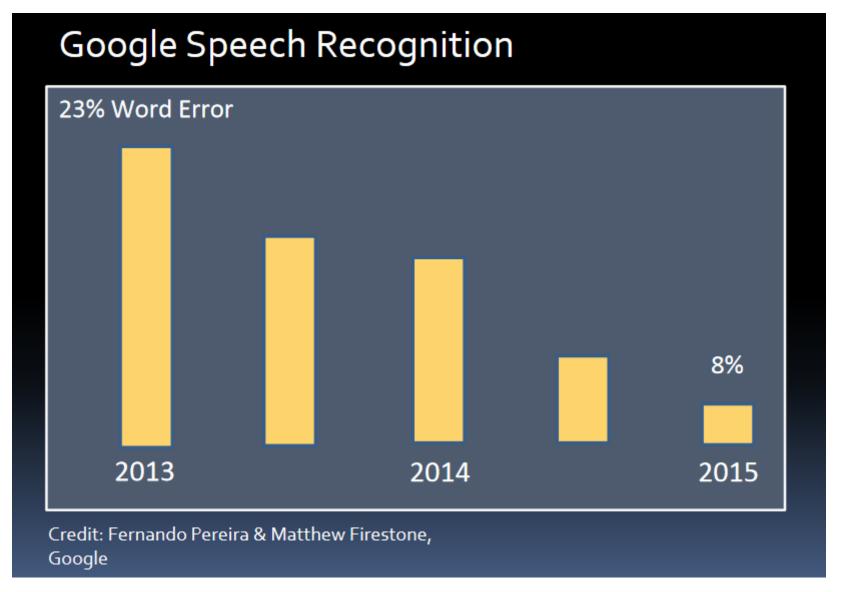
Self-driving cars

### Google's Self Driving Car for Blind People

by EDITORS on Apr 6, 2012 - 4:07 pm



### **ML Successes: Perception**



Credit: Tom Dietterich

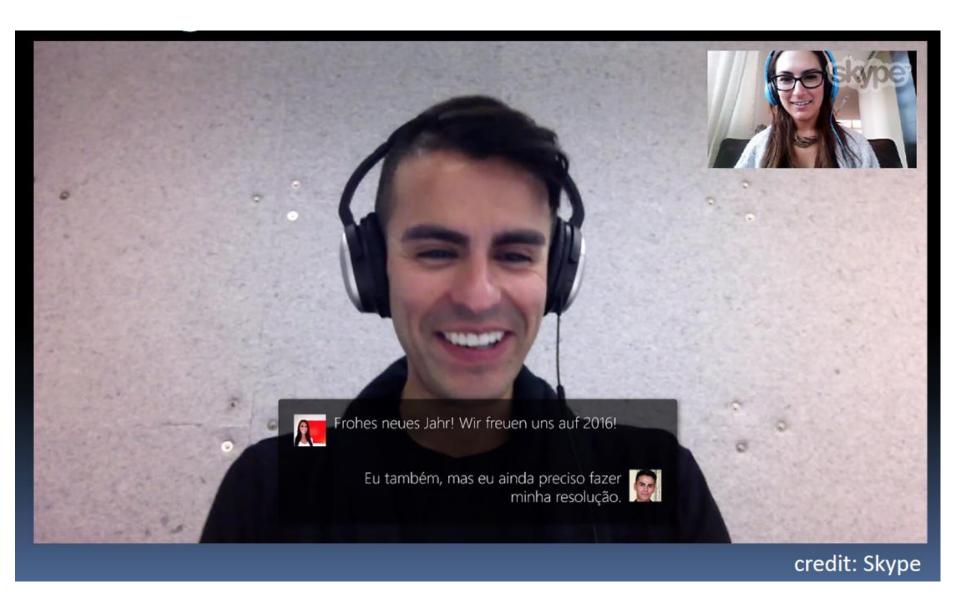
### **ML Successes: Image Captioning**



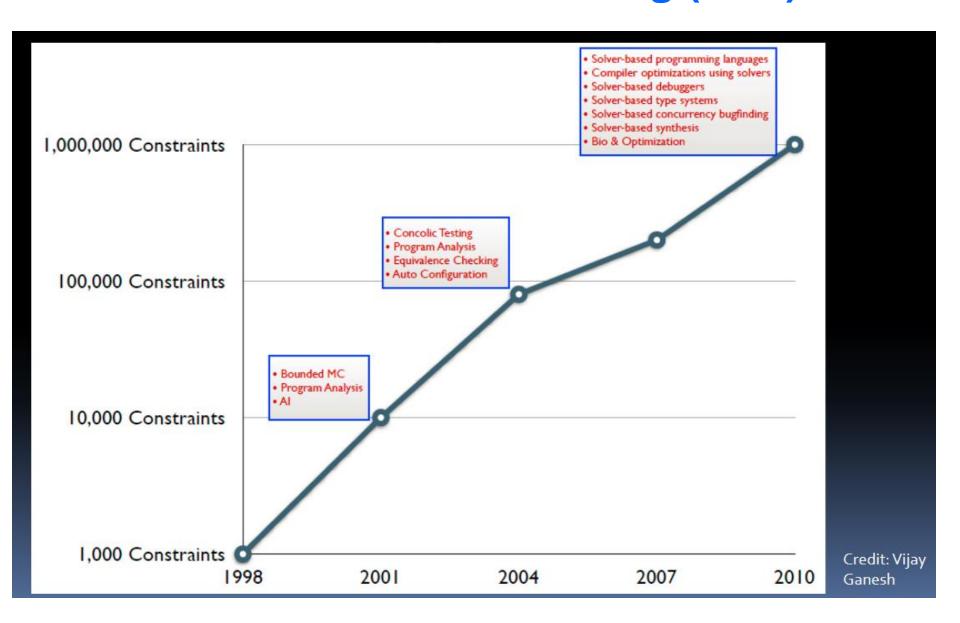
### **ML Successes: Perception + Translation**



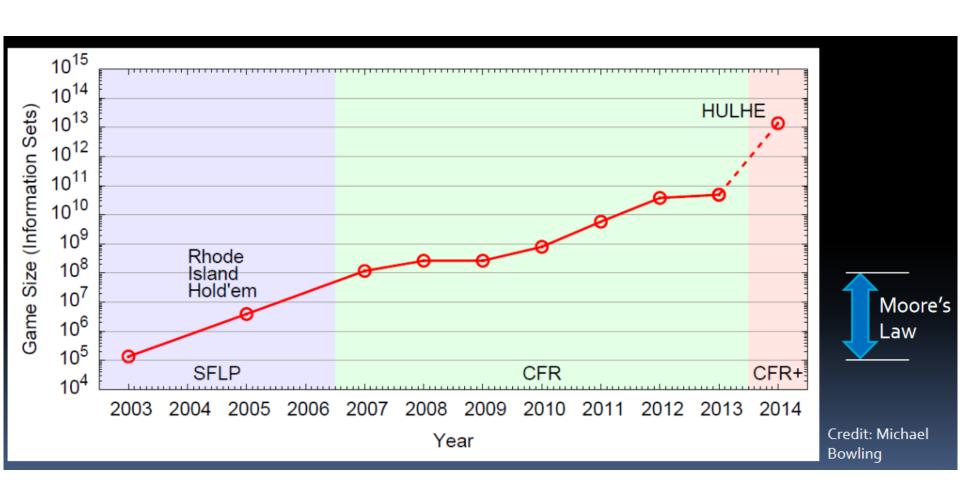
### **ML Successes: Skype Translator**



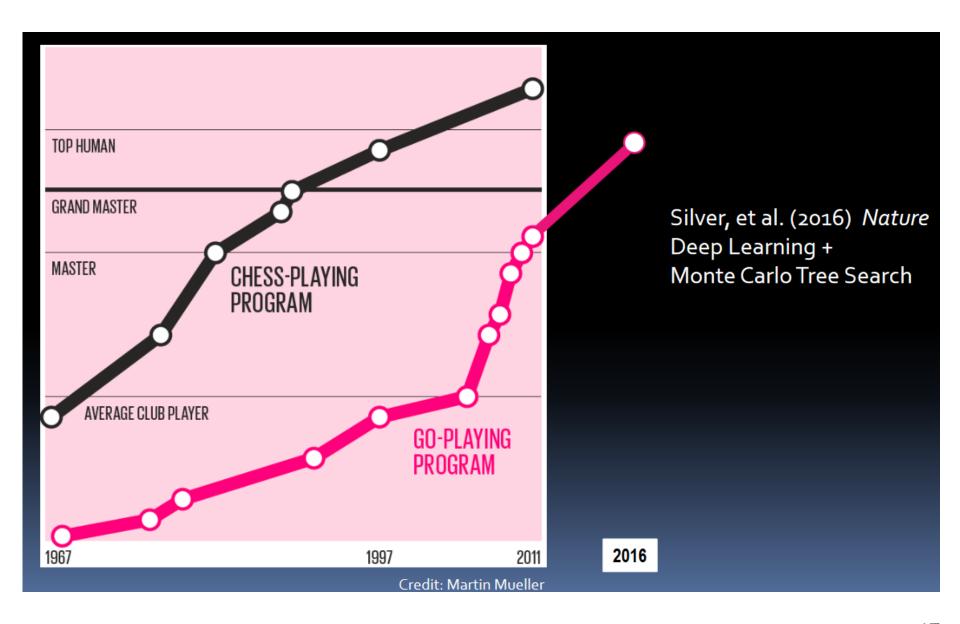
### **ML Successes: Reasoning (SAT)**



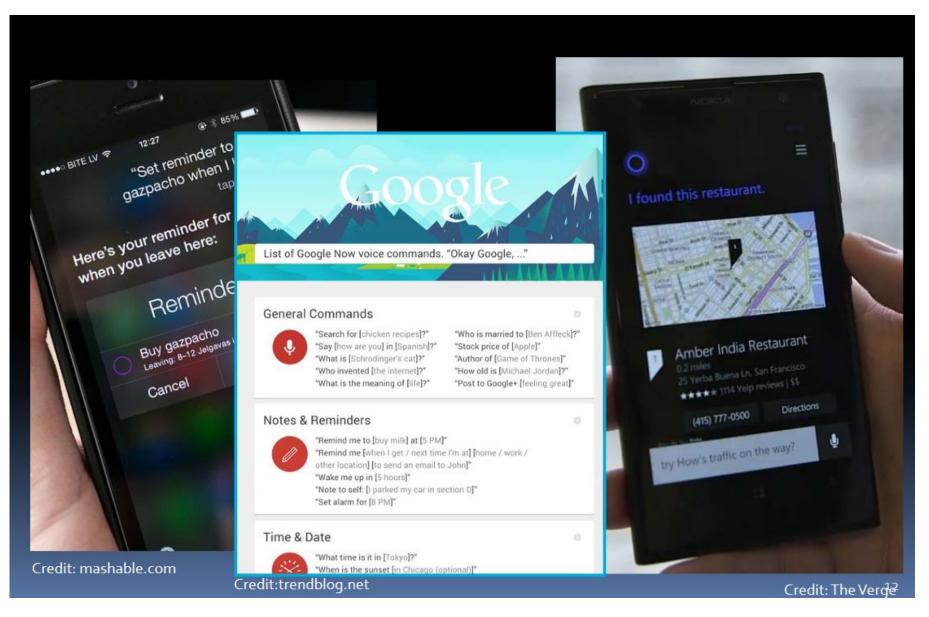
### **ML Successes: Poker**



### **ML Successes: Chess and Go**



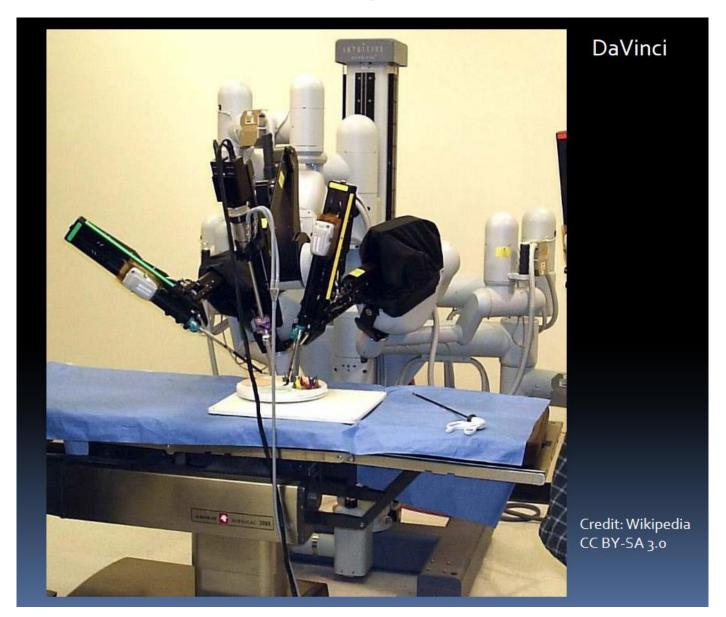
### **ML Successes: Personal Assistants**



### **High-Stakes Applications: Self-Driving Cars**



### High-Stakes Applications: Automated Surgical Assistants



# High-Stakes Applications: Al Hedge Funds



## High-Stakes Applications: Power Grid Control

## CONTROLLING THE POWER GRID WITH ARTIFICIAL INTELLIGENCE

02.07.2015

Credit: EBM Netz AG

### DARPA Exploring Ways to Protect Nation's Electrical Grid from Cyber Attack

Effort calls for creation of automated systems to restore power within seven days or less after attack

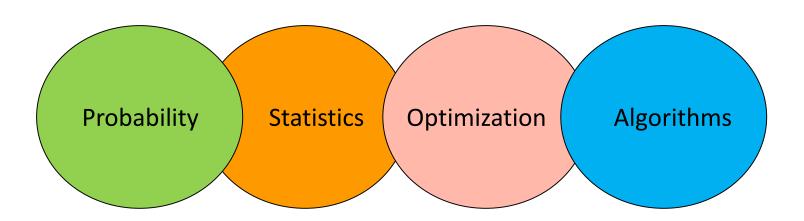
Credit: DARPA

# High-Stakes Applications: Autonomous Weapons



## What is Machine Learning?

- Machine learning is the branch of engineering that develops technology for automated inference
  - It combines



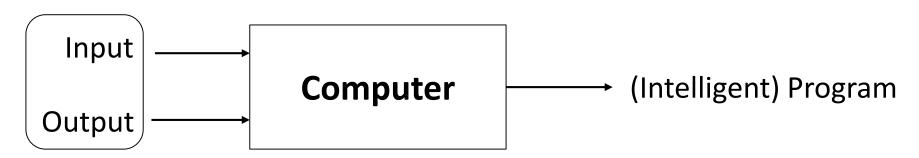
### What is Machine Learning?

Machine learning = Automating Automation

### **Traditional Programming**



### **Machine Learning**



**Training data** 

## **Learning Paradigms**

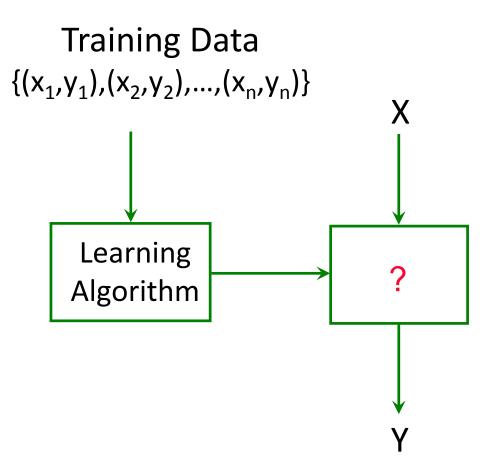
Supervised Learning – main focus of this course

- Semi-Supervised Learning
- Active Learning
- Reinforcement Learning

## **Supervised Learning**

### Learning a Classifier



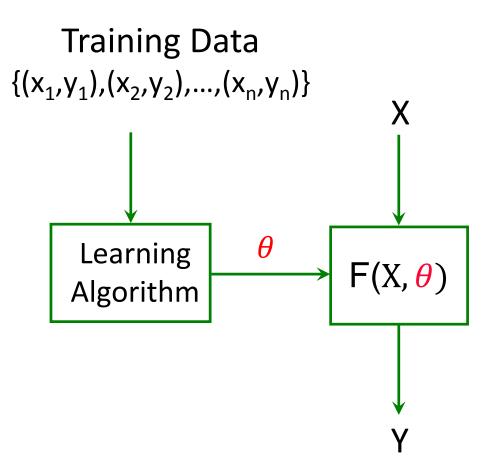


#### **Example problem:**

X - image of a face

Y ∈ {male, female}

### Learning a Classifier

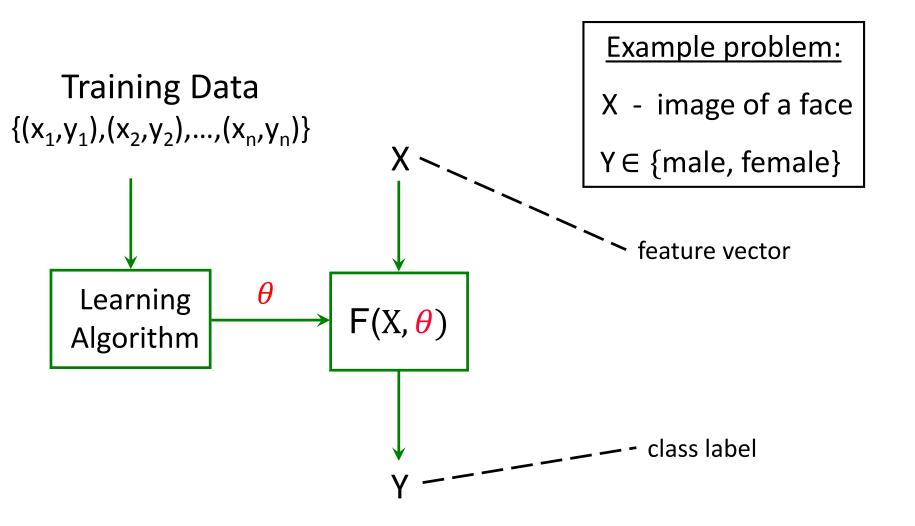


#### **Example problem:**

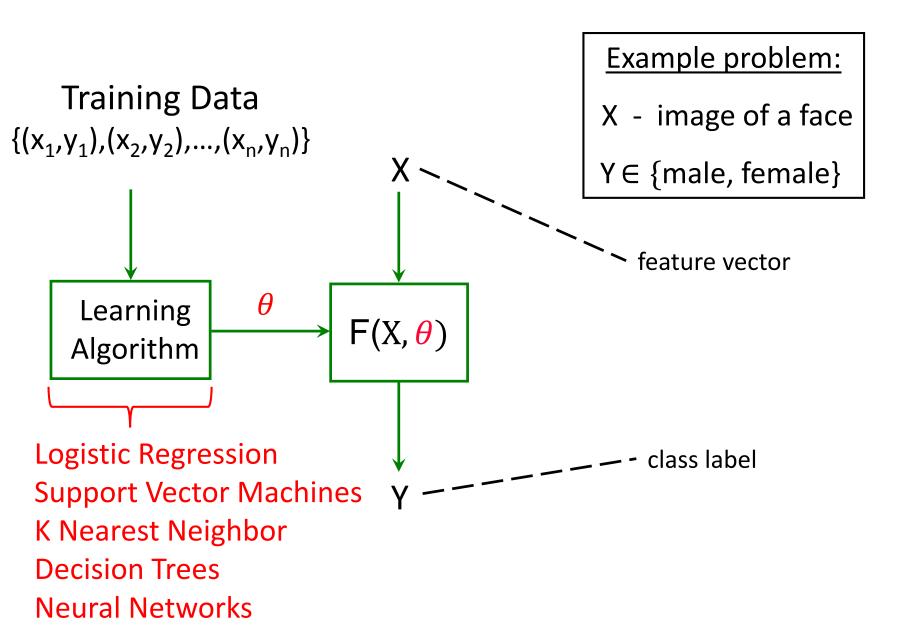
X - image of a face

Y ∈ {male, female}

### **Learning for Simple Outputs**

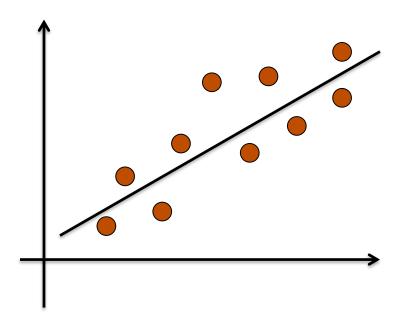


### **Learning for Simple Outputs**

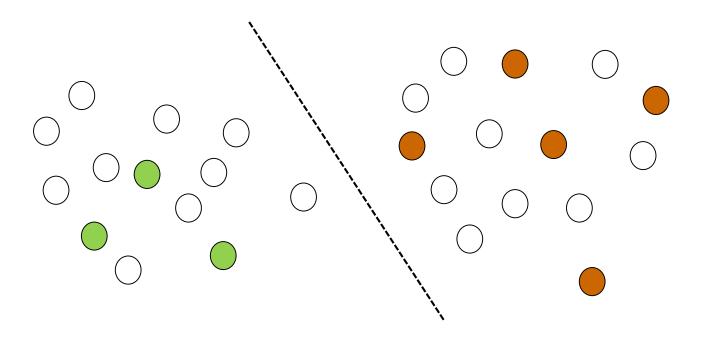


## Regression

- **Setting:** output *y* is a continuous value instead of a discrete value
  - Stock market price as a function of financial specs



 Setting: small amount of labeled data and large amount of unlabeled data



find a classifier that separates the labeled points and separates the unlabeled points "well"

### Co-Training Style Algorithms

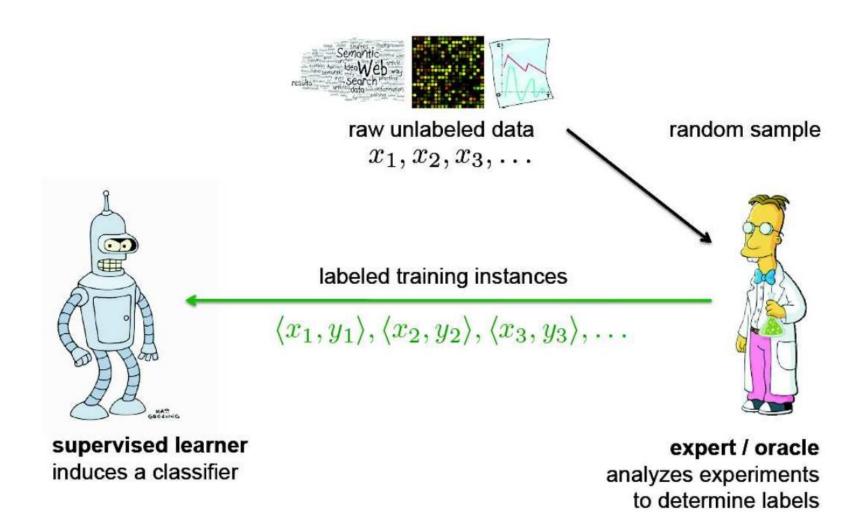
 Leverage diversity in the learners to learn from each other

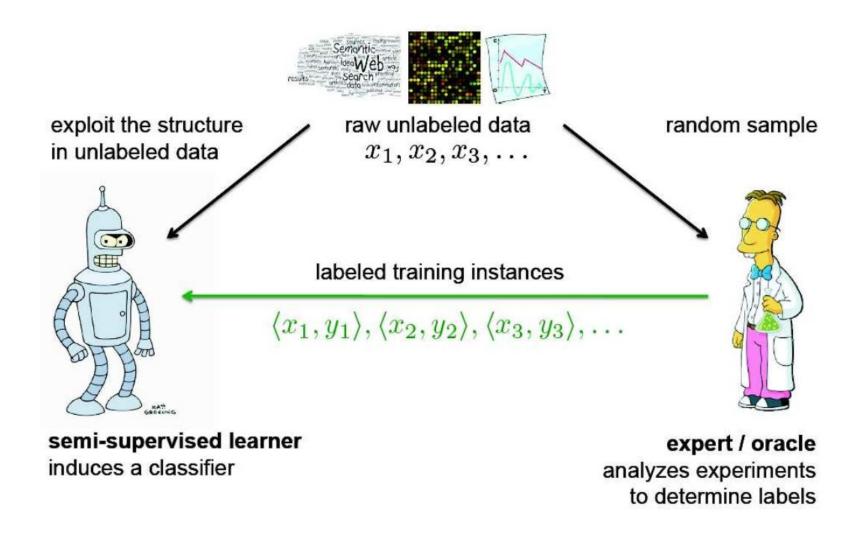
◆ Diversity comes from multiple (redundant) views of the input – In webpage classification, one view is the "words" on the page and another view is the "links" that point to that page

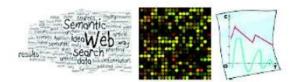
▲ If only one view, employ learners with different hypothesis spaces to achieve diversity

## **Active Learning**

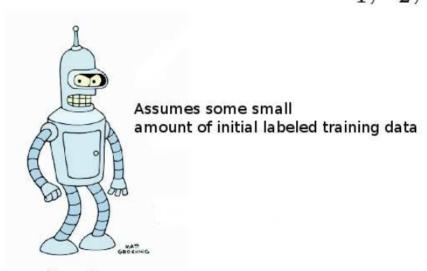
### (Passive) Supervised Learning







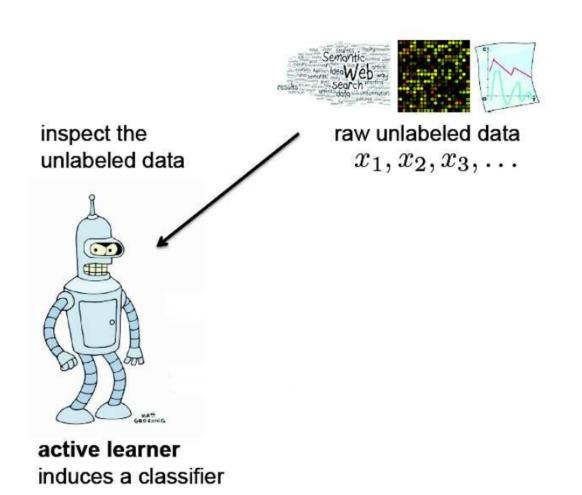
raw unlabeled data  $x_1, x_2, x_3, \dots$ 



active learner induces a classifier

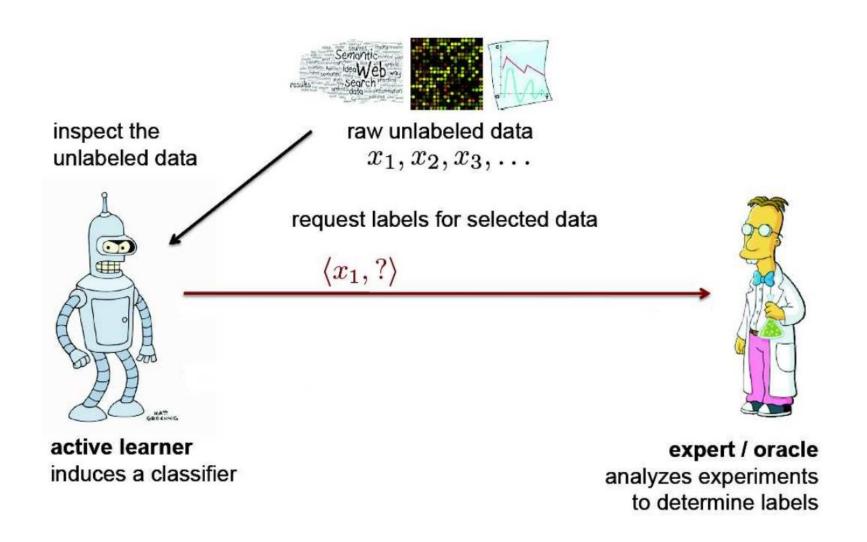


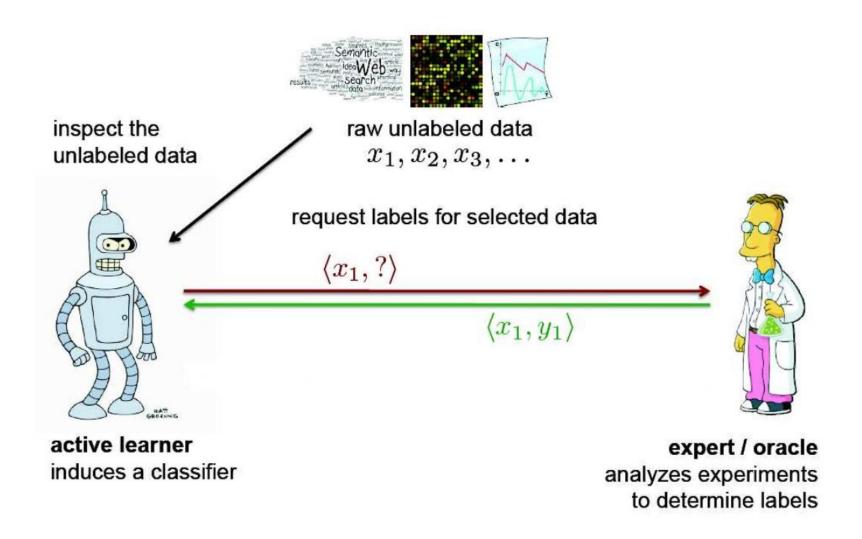
expert / oracle analyzes experiments to determine labels

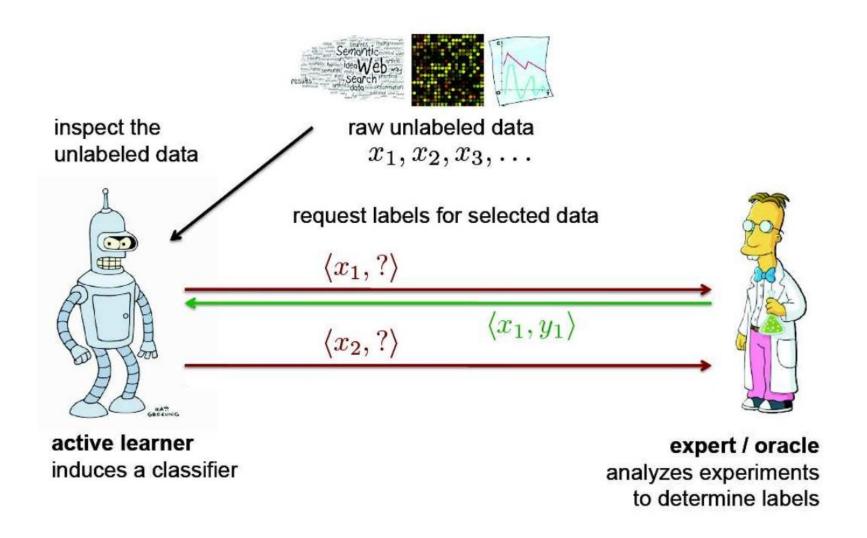


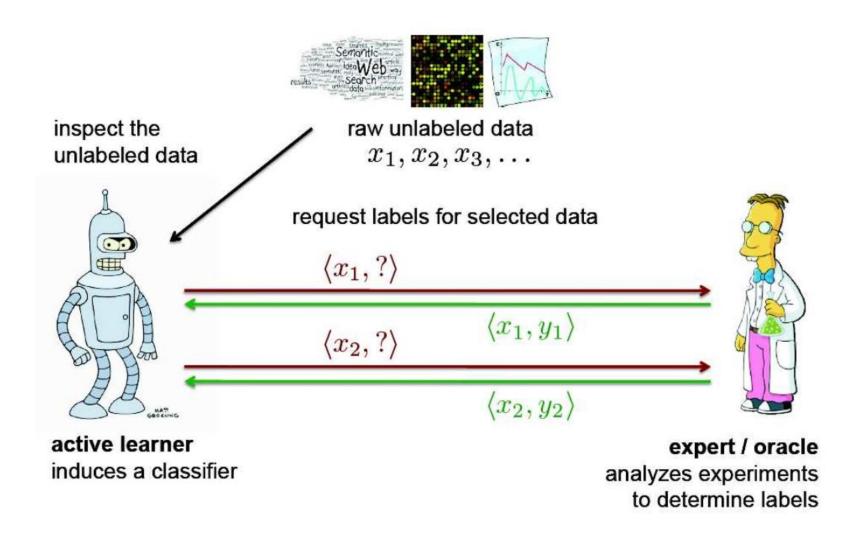


expert / oracle analyzes experiments to determine labels









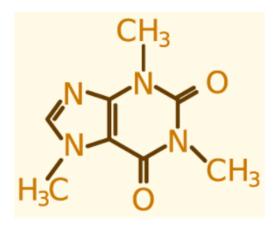
#### **Motivation**

#### • Why do we need active learning?

- Supervised learning can solve all our problems, right?
- Yes, if we have enough labeled data (input-output pairs)
- But Labeling is expensive
- We want to learn a highly-accurate function with few labeled examples
- Intelligently select the examples for which we want to get labels for (unlabeled data is plentiful and cheap)

#### **Active Learning Example: Drug Design**

#### Goal: find compounds which bind to a particular target



Large collection of compounds, from:

- vendor catalogs
- corporate collections
- combinatorial chemistry

```
unlabeled point \equiv description of chemical compound label \equiv active (binds to target) vs. inactive
```

getting a label ≡ chemistry experiment

#### Who uses Active Learning?



Sentiment analysis for blogs; Noisy relabeling

Prem Melville



Biomedical NLP & IR; Computer-aided diagnosis

- Balaji Krishnapuram



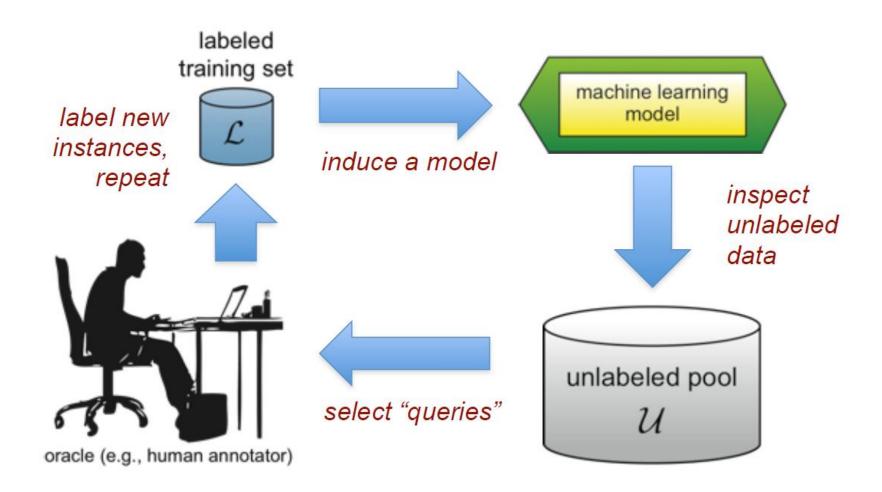
MS Outlook voicemail plug-in [Kapoor et al., IJCAl'07]; "A variety of prototypes that are in use throughout the company." – *Eric Horvitz* 



"While I can confirm that we're using active learning in earnest on many problem areas... I really can't provide any more details than that. Sorry to be so opaque!"

David Cohn

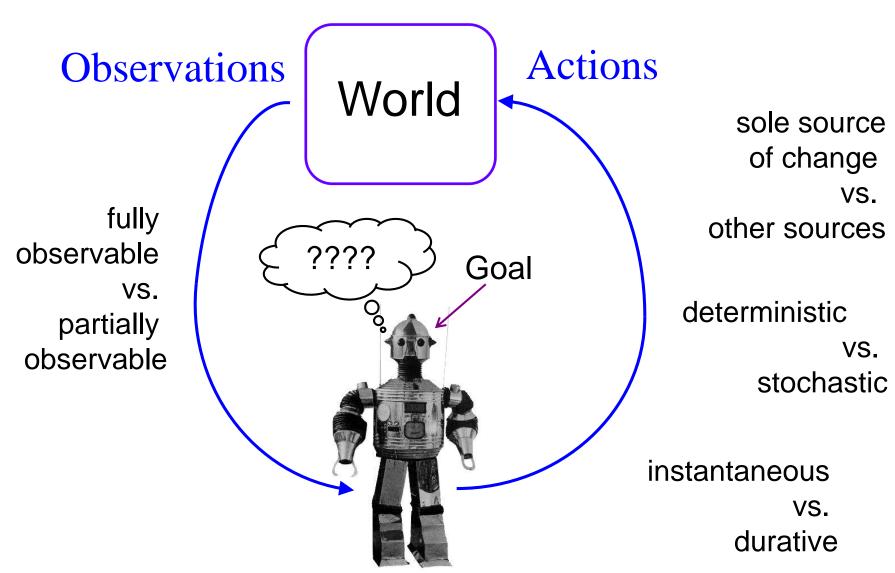
#### **Pool based Active Learning**



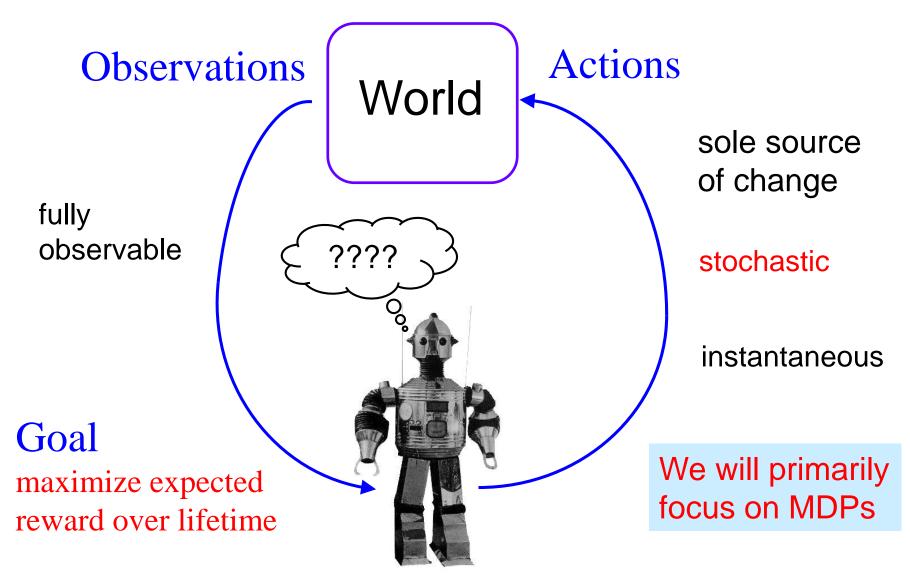
Credit: Burr Settles

# **Reinforcement Learning**

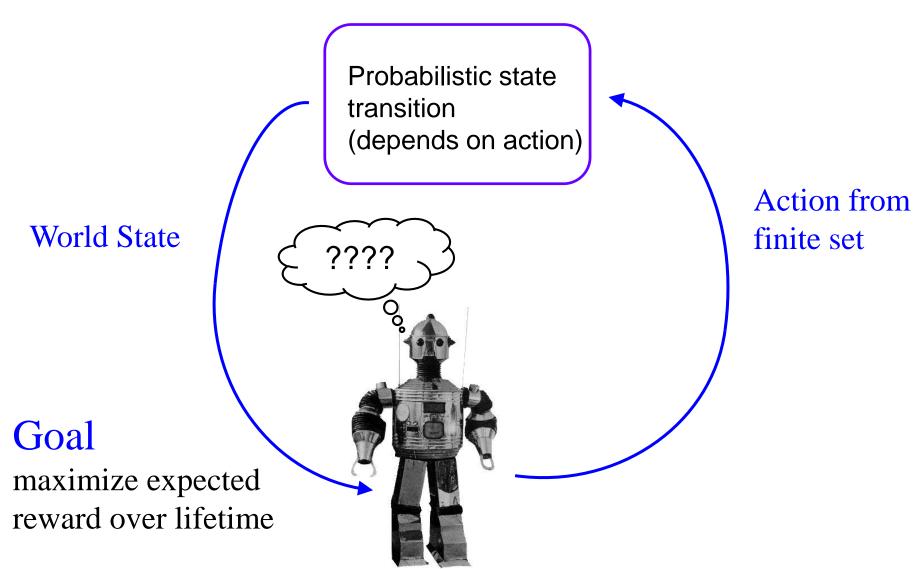
# Reinforcement Learning



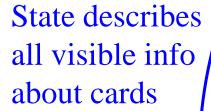
### Stochastic/Probabilistic Planning: Markov Decision Process (MDP) Model



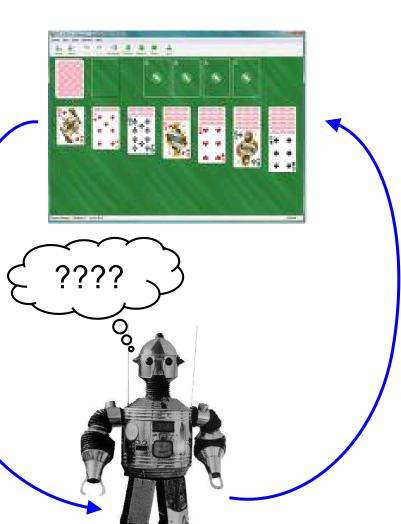
### Stochastic/Probabilistic Planning: Markov Decision Process (MDP) Model



#### **Example MDP**



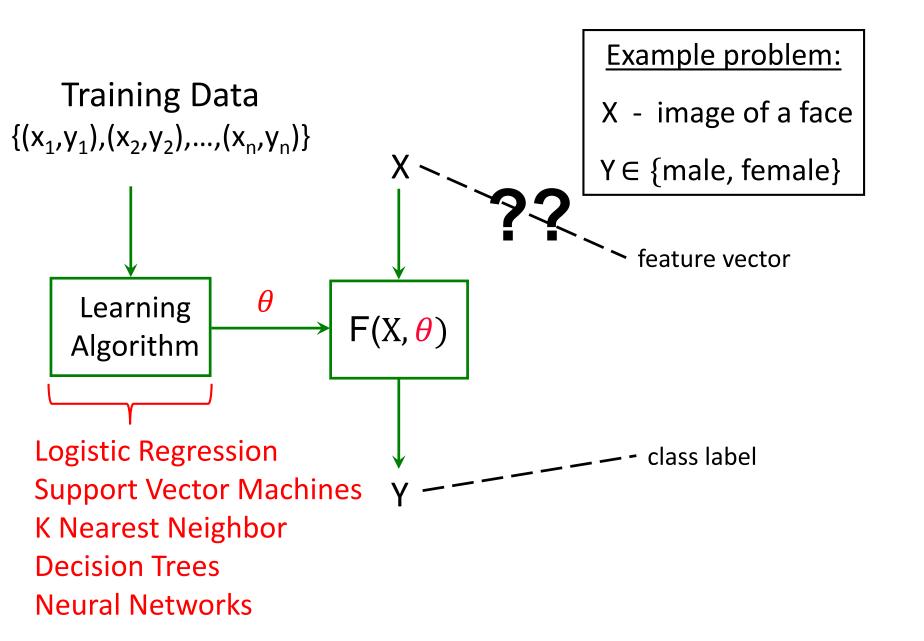
Goal
win the game or
play max # of cards



Action are the different legal card movements

# Input Representation and Abstract Machine Learning Algorithm

# **Learning for Simple Outputs**



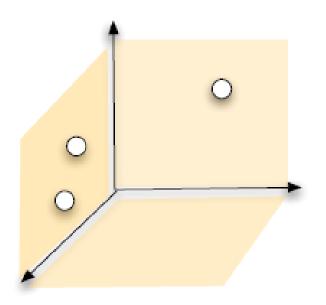
In ML, our input examples (emails, text documents, images) are often represented as real-valued vectors:
 x ∈ R<sup>d</sup>

each co-ordinate of x is called a feature

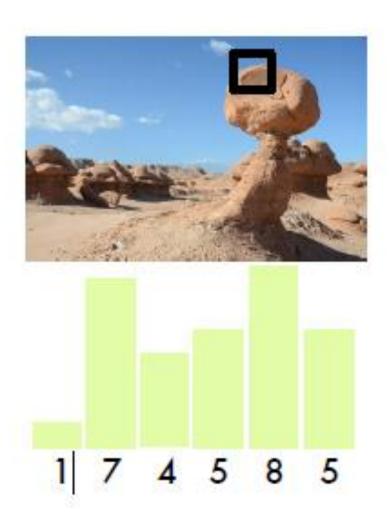
- Some examples
  - Bag-of-words representation of text
  - Histograms of colors in image
  - Sound frequency histogram

- Bag-of-words model
  - sentences to points
  - 1. To be, or not to be,
  - 2. To be a woman,
  - 3. To not be a man

To	be	or	not	woman	a	man
2	2	1	1	0	0	0
1	1	0	0	1	1	0
1	1	0	1	0	1	1



Histogram of colors in image



Sound frequency histogram



## **Overview of ML Algorithms**

There are lot of machine learning algorithms

- Every machine learning algorithm has three components
  - Representation
  - Evaluation
  - Optimization

# Representation: Examples

- Linear hyper-planes
- Decision trees
- Sets of conjunctive / logical rules
- Graphical models (Bayes/Markov nets)
- Neural Networks

•

# **Evaluation: Examples**

- Accuracy
- Precision and recall
- Squared error
- Likelihood
- Cost / Utility
- Margin
- Entropy
- •

# **Optimization: Examples**

- Combinatorial Optimization
  - greedy search, dynamic programming

- Convex Optimization
  - gradient descent, co-ordinate descent

- Constrained Optimization
  - linear programming, quadratic programming
- •

# Learning Classifiers via Perceptron Algorithm

# Formal setting – Classification

- Instances
  - emails
- Labels
  - Spam vs. non-spam
- Prediction rule
  - Linear prediction rule
- Loss
  - No. of mistakes

$$\mathbf{x} \in \mathcal{X}$$

$$y \in \mathcal{Y} = \{-1 ; 1\}$$

$$f(\mathbf{x}) = \hat{y}$$

$$\ell(\hat{y}, y) \in \mathbb{R}_+$$

#### **Predictions**

- ullet Continuous predictions:  $f:\mathcal{X} 
  ightarrow \mathbb{R}$ 
  - Label sign(f(x))
  - Confidence  $|f(\mathbf{x})|$
- Linear Classifiers
  - Prediction:  $\widehat{y} = \operatorname{sign}(f(\mathbf{x}))$   $= \operatorname{arg} \max_{y \in \mathcal{Y}} \mathbf{w} \cdot \Phi(\mathbf{x}, y)$   $= \operatorname{sign}(\mathbf{w} \cdot \mathbf{x})$   $|f(\mathbf{x})| = |\mathbf{w} \cdot \mathbf{x}|$

#### **Loss Functions**

- Natural Loss:
  - Zero-One loss

$$\ell(\hat{y}, y) = \begin{cases} 0 & y = \hat{y} \\ 1 & y \neq \hat{y} \end{cases}$$

#### **Online Framework**

- Initialize Classifier  $f_1(\mathbf{x})$
- Algorithm works in rounds  $t = 1 \dots T \dots$
- On round t the online algorithm :
  - Receives an input instance
  - Outputs a prediction
  - Receives a feedback label
  - Computes loss
  - Updates the prediction rule
- Goal:
  - Suffer small cumulative loss

$$\mathbf{x}_t$$

$$f_t(\mathbf{x}_t) = \hat{y}_t$$

 $y_t$ 

$$\ell(\hat{y}_t, y_t)$$

$$f_t \rightarrow f_{t+1}$$

 $\sum_t \ell(\widehat{y}_t, y_t)$ 

# Why Online Learning?

- Fast
- Memory efficient process one example at a time
- Simple to implement
- Formal guarantees Mistake bounds
- Online to Batch conversions
- No statistical assumptions
- Adaptive

# **Update Rules**

- Online algorithms are based on an update rule which defines  $f_{t+1}$  from  $f_t$  (and possibly other information)
- Linear Classifiers : find  $\mathbf{w}_{t+1}$  from  $\mathbf{w}_t$  based on the input  $(\mathbf{x}_t, y_t)$
- Perceptron algorithm employs a specific update rule

# Design Principle of Online Learning Algorithms

- If the learner suffers non-zero loss at any round, then we want to balance two goals:
  - Corrective: Change weights so that we don't make this error again
  - Conservative: Don't change the weights too much

# The Perceptron Algorithm ( $\eta = 1$ )

If No-Mistake

$$y_t(\mathbf{w}_t \cdot \mathbf{x}_t) > 0$$

Do nothing

$$\mathbf{w}_{t+1} \leftarrow \mathbf{w}_t$$

If Mistake

$$y_t(\mathbf{w}_t \cdot \mathbf{x}_t) \leq 0$$

Update

$$\mathbf{w}_{t+1} \leftarrow \mathbf{w}_t + y_t \mathbf{x}_t$$

# The Perceptron Algorithm ( $\eta = 1$ )

When mistake happens, what does the update do?

- $w_{t+1}$  moves "closer to"  $x_t$  OR
- $\sim x_t$  moves towards the positive side of the decision boundary

- $w_{t+1}$  moves "away from"  $x_t$  OR
- $x_t$  moves towards the negative side of the decision boundary
- In both cases, we are moving towards the "correct solution"