

#### 10-601 Introduction to Machine Learning

Machine Learning Department School of Computer Science Carnegie Mellon University

# Support Vector Machines + Kernels

Matt Gormley Lecture 27 Nov. 22, 2019

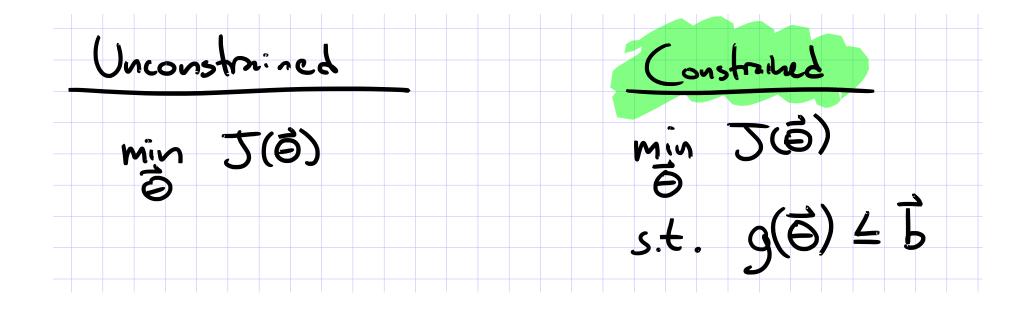
# Reminders

- Homework 7: HMMs
  - Out: Fri, Nov. 8
  - Due: Mon, Nov. 25 at 11:59pm
- Homework 8: Learning Paradigms
  - Out: Mon, Nov. 25
  - Due: Wed, Dec. 4 at 11:59pm
  - Can only be submitted up to 3 days late, so we can return grades before final exam

- Today's In-Class Poll
  - http://p27.mlcourse.org

### **CONSTRAINED OPTIMIZATION**

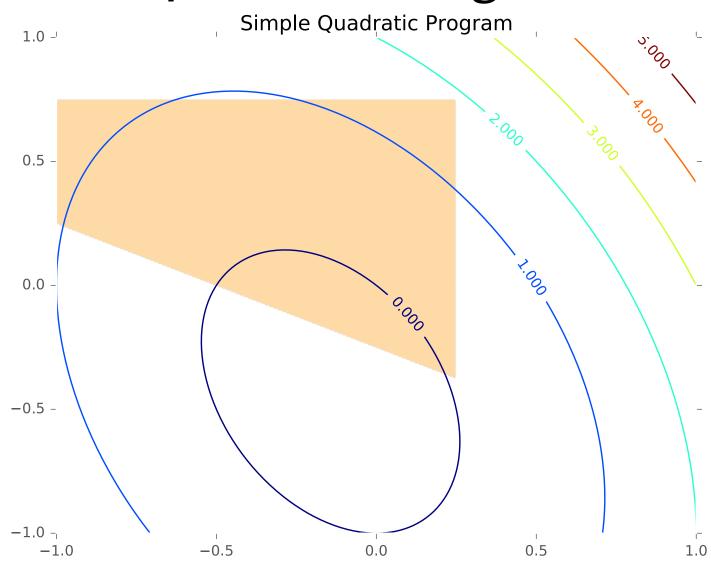
#### **Constrained Optimization**

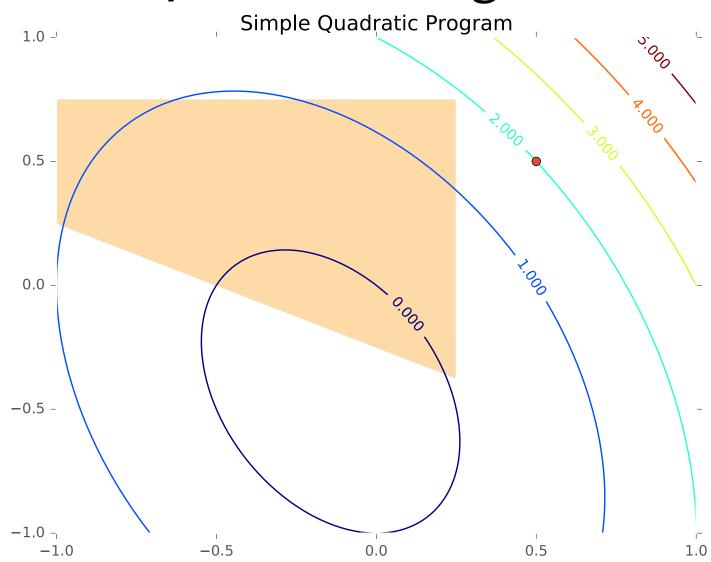


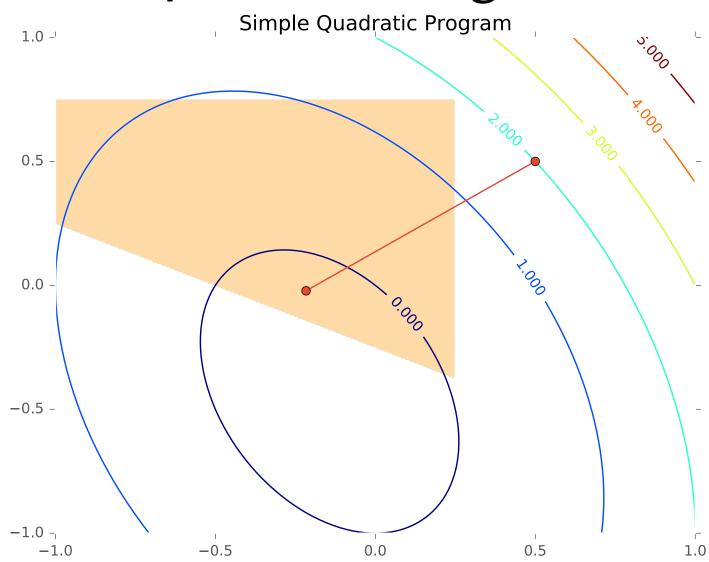
# **SVM: Optimization Background**

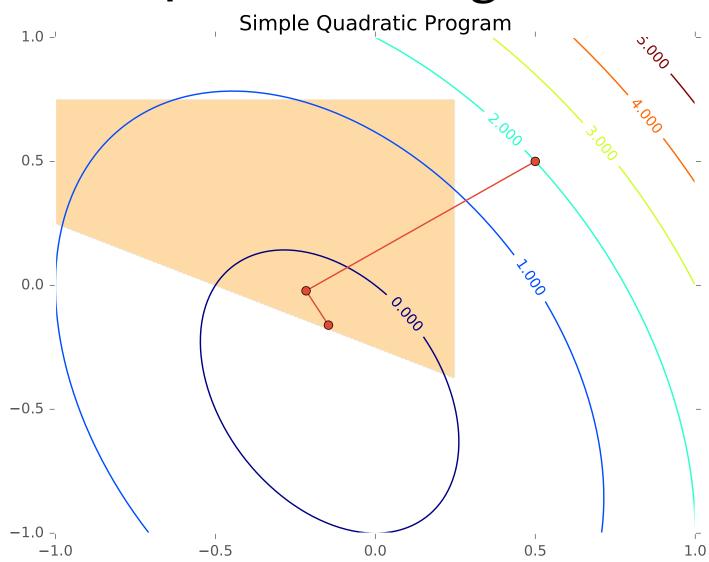
#### Whiteboard

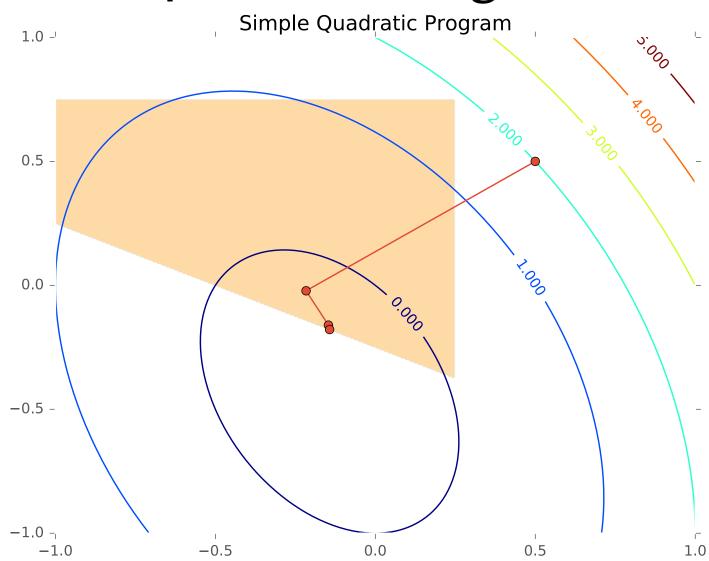
- Constrained Optimization
- Linear programming
- Quadratic programming
- Example: 2D quadratic function with linear constraints











# SUPPORT VECTOR MACHINE (SVM)

#### Example: Building a Canal



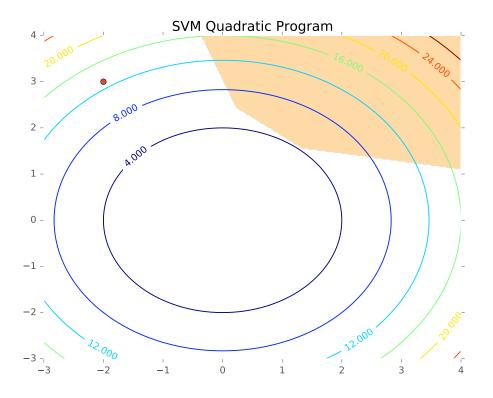
https://www.flickr.com/photos/hereistom/10438848375

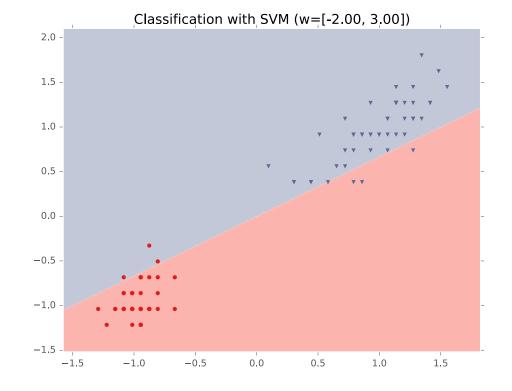
# SVM

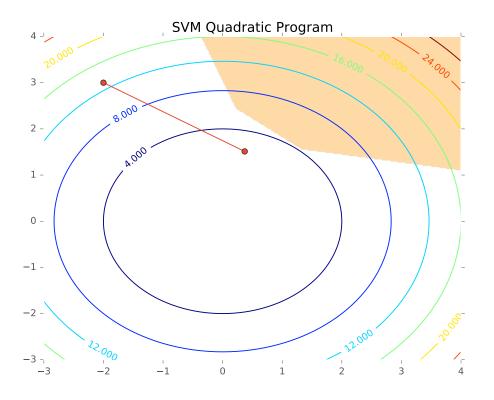
#### Whiteboard

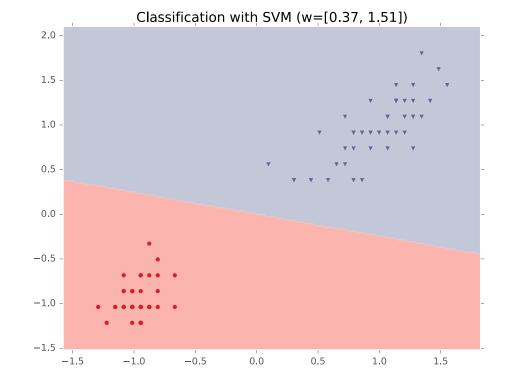
- SVM Primal (Linearly Separable Case)

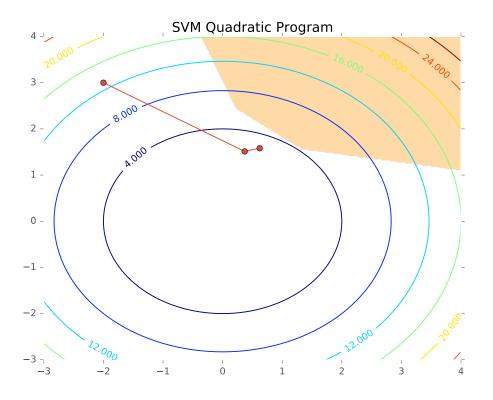
This section borrows ideas from Nina Balcan's SVM lectures at CMU and Patrick Winston's "widest street" SVM lecture at MIT (<u>https://www.youtube.com/watch?v=\_PwhiWxHK8o</u>).

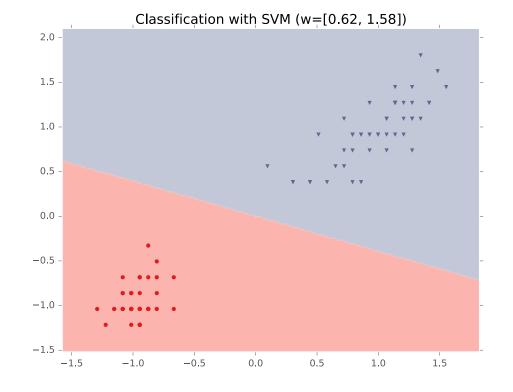


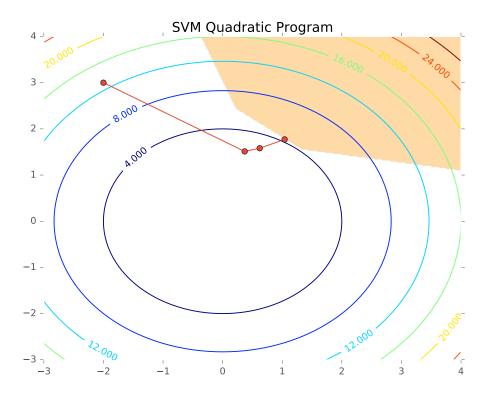


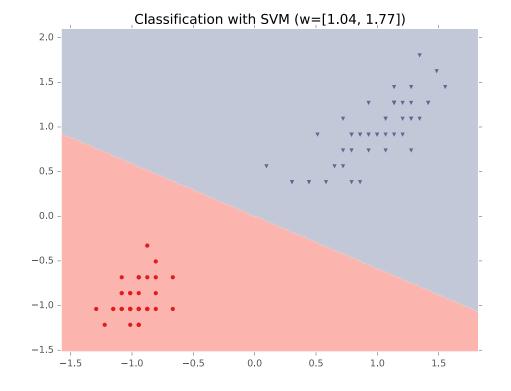


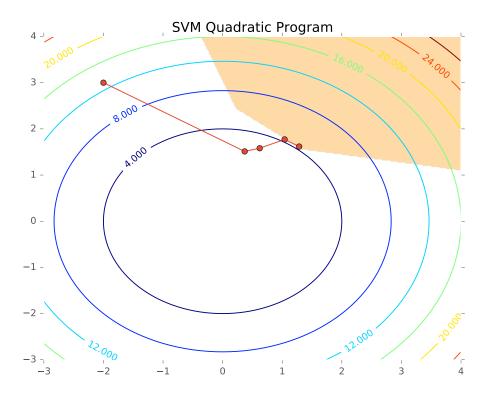


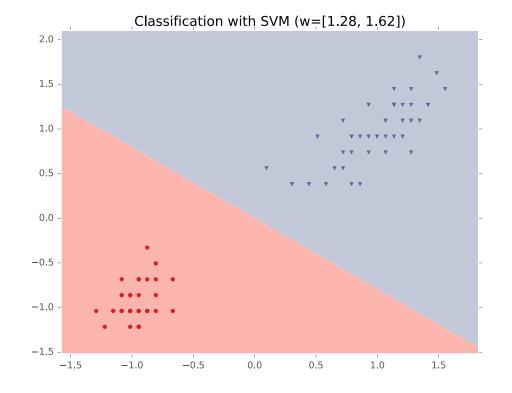


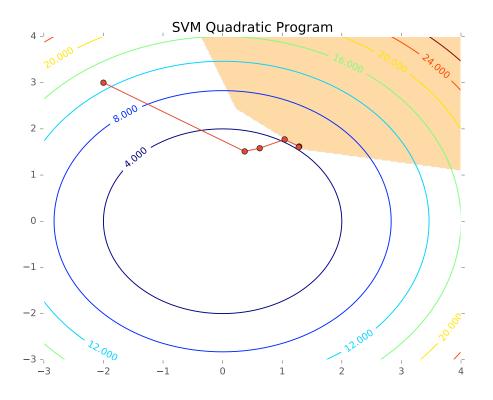


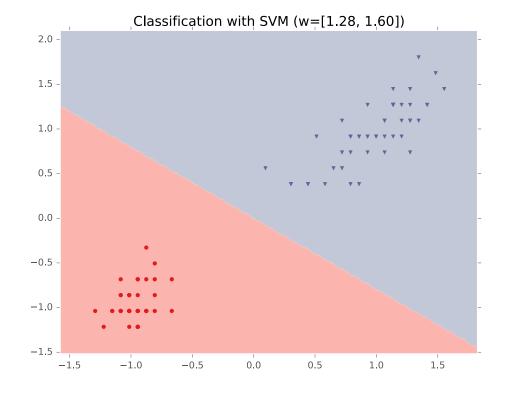












# Support Vector Machines (SVMs)

Hard-margin SVM (Primal)

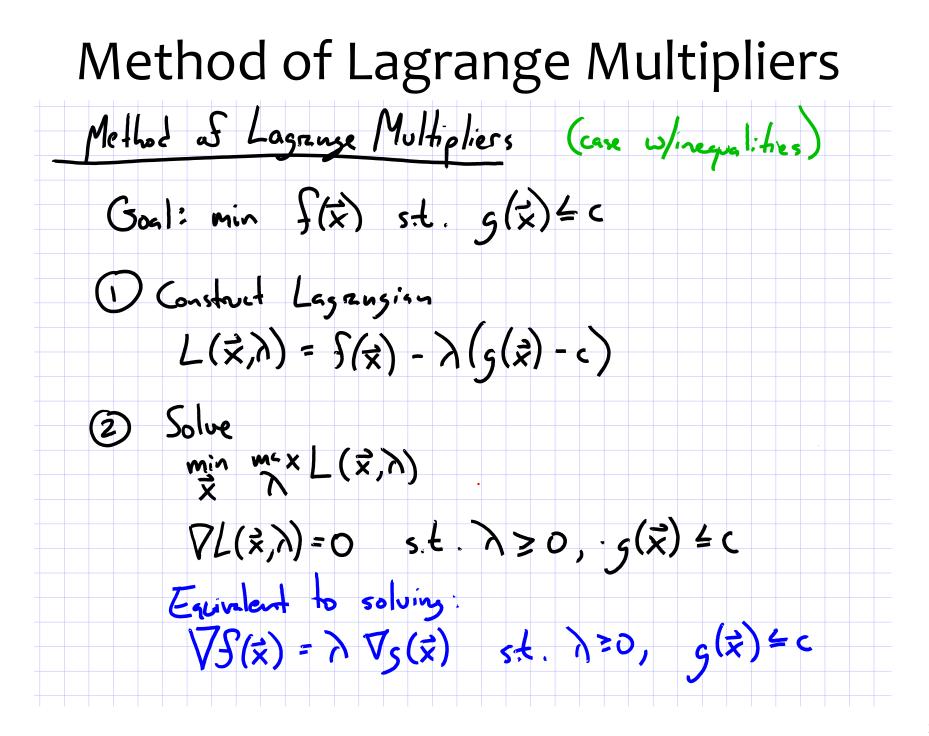
$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_2^2$$
  
s.t.  $y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \ge 1, \quad \forall i = 1, \dots, N$ 

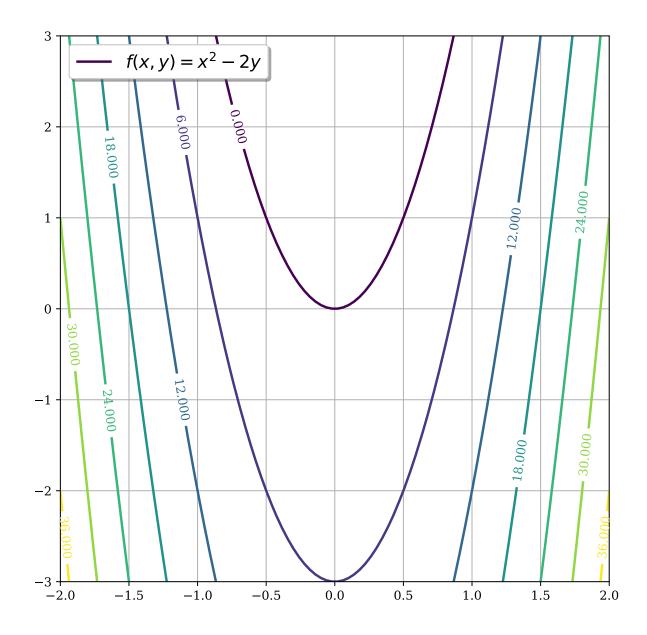
Hard-margin SVM (Lagrangian Dual)

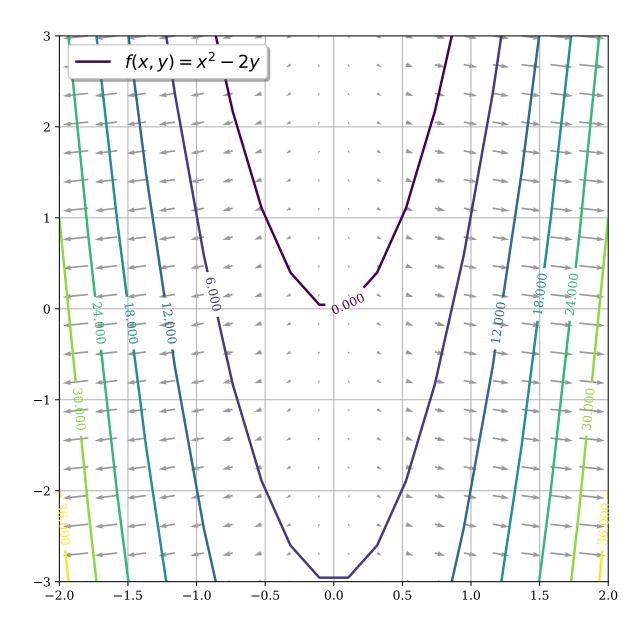
$$\max_{\boldsymbol{\alpha}} \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y^{(i)} y^{(j)} \mathbf{x}^{(i)} \cdot \mathbf{x}^{(j)}$$
  
s.t.  $\alpha_i \ge 0$ ,  $\forall i = 1, \dots, N$ 
$$\sum_{i=1}^{N} \alpha_i y^{(i)} = 0$$

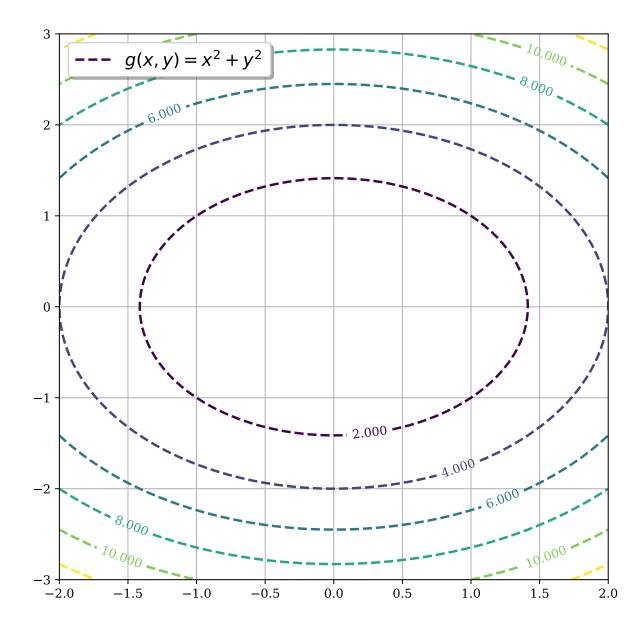
- Instead of minimizing the primal, we can maximize the dual problem
- For the SVM, these two problems give the same answer (i.e. the minimum of one is the maximum of the other)
- Definition: support vectors are those points  $x^{(i)}$  for which  $\alpha^{(i)} \neq 0$

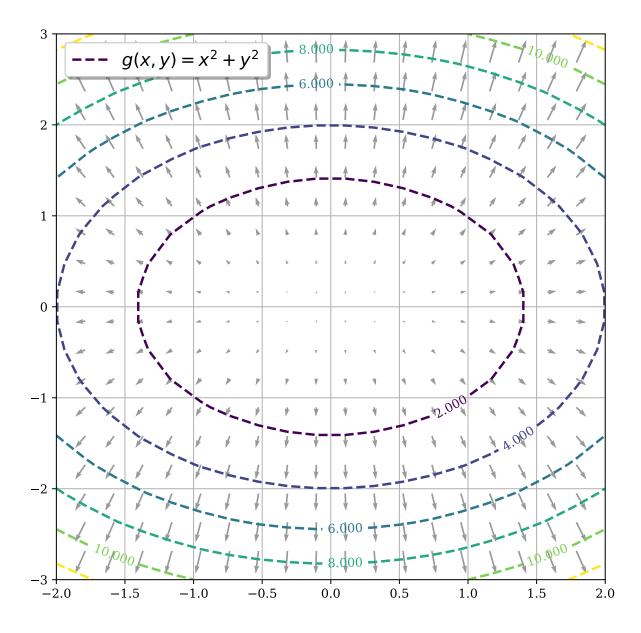
# METHOD OF LAGRANGE MULTIPLIERS

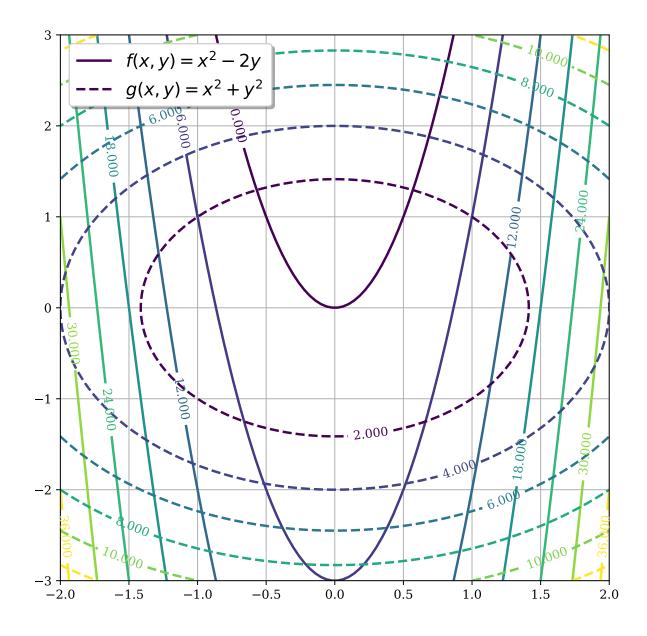












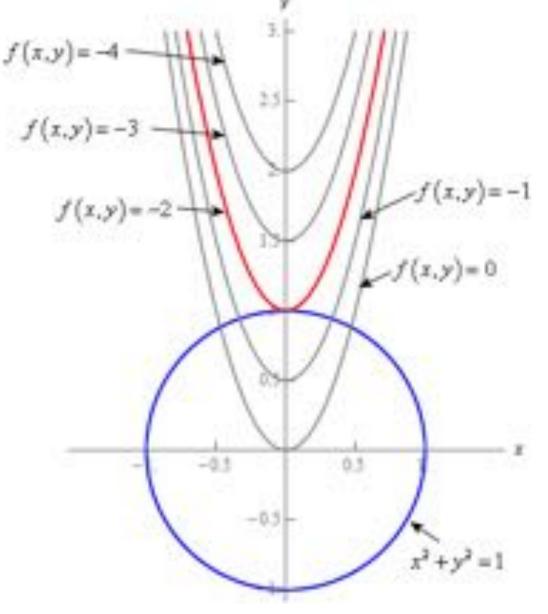
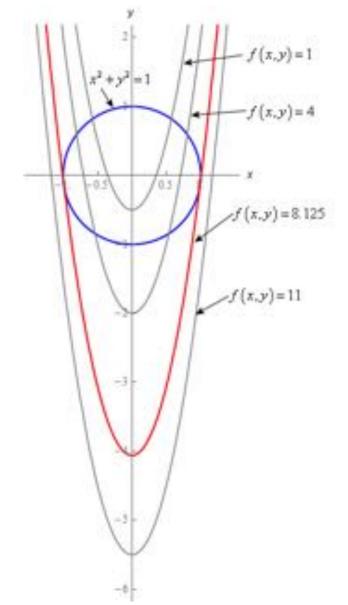


Figure from http://tutorial.math.lamar.edu/Classes/CalcIII/LagrangeMultipliers.aspx



#### **SVM DUAL**

#### Whiteboard

- Lagrangian Duality
- Example: SVM Dual

# Support Vector Machines (SVMs)

Hard-margin SVM (Primal)

$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_2^2$$
  
s.t.  $y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \ge 1, \quad \forall i = 1, \dots, N$ 

Hard-margin SVM (Lagrangian Dual)

$$\max_{\boldsymbol{\alpha}} \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y^{(i)} y^{(j)} \mathbf{x}^{(i)} \cdot \mathbf{x}^{(j)}$$
  
s.t.  $\alpha_i \ge 0$ ,  $\forall i = 1, \dots, N$ 
$$\sum_{i=1}^{N} \alpha_i y^{(i)} = 0$$

- Instead of minimizing the primal, we can maximize the dual problem
- For the SVM, these two problems give the same answer (i.e. the minimum of one is the maximum of the other)
- Definition: support vectors are those points  $x^{(i)}$  for which  $\alpha^{(i)} \neq 0$

#### **SVM EXTENSIONS**

# Soft-Margin SVM

Hard-margin SVM (Primal)

$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_2^2$$
s.t.  $y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) > 1, \quad \forall i = 1, \dots, N$ 

Soft-margin SVM (Primal)

$$\begin{split} \min_{\mathbf{w},b} \ &\frac{1}{2} \|\mathbf{w}\|_2^2 + C\left(\sum_{i=1}^N e_i\right) \\ \text{s.t. } y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \geq 1 - e_i, \quad \forall i = 1, \dots, N \\ e_i \geq 0, \quad \forall i = 1, \dots, N \end{split}$$

- **Question:** If the dataset is not linearly separable, can we still use an SVM?
- **Answer**: Not the hardmargin version. It will never find a feasible solution.

In the soft-margin version, we add "slack variables" that allow some points to violate the large-margin constraints.

The constant C dictates **how large** we should allow the slack variables to be

# Soft-Margin SVM

Hard-margin SVM (Primal)

$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_2^2$$
s.t.  $y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \ge 1, \quad \forall i = 1, \dots, N$ 

Soft-margin SVM (Primal)

$$\begin{split} \min_{\mathbf{w},b} & \frac{1}{2} \|\mathbf{w}\|_2^2 + C\left(\sum_{i=1}^N e_i\right) \\ \text{s.t. } y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \geq 1 - e_i, \quad \forall i = 1, \dots, N \\ & e_i \geq 0, \quad \forall i = 1, \dots, N \end{split}$$

# Soft-Margin SVM

Hard-margin SVM (Primal)

$$\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_2^2$$
s.t.  $y^{(i)}(\mathbf{w}^T \mathbf{x}^{(i)} + b) \ge 1, \quad \forall i = 1, \dots, N$ 

Hard-margin SVM (Lagrangian Dual)

$$\begin{aligned} \max_{\boldsymbol{\alpha}} \; \sum_{i=1}^{N} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_{i} \alpha_{j} y^{(i)} y^{(j)} \mathbf{x}^{(i)} \cdot \mathbf{x}^{(j)} \\ \text{s.t.} \; \alpha_{i} \geq 0, \quad \forall i = 1, \dots, N \\ \sum_{i=1}^{N} \alpha_{i} y^{(i)} = 0 \end{aligned}$$

Soft-margin SVM (Primal)  $\min_{\mathbf{w},b} \frac{1}{2} \|\mathbf{w}\|_{2}^{2} + C\left(\sum_{i=1}^{N} e_{i}\right)$ s.t.  $y^{(i)}(\mathbf{w}^{T}\mathbf{x}^{(i)} + b) \ge 1 - e_{i}, \quad \forall i = 1, \dots, N$  $e_{i} \ge 0, \quad \forall i = 1, \dots, N$   $\sum_{i=1}^{N} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_{i} \alpha_{j} y^{(i)} y^{(j)} \mathbf{x}^{(i)} \cdot \mathbf{x}^{(j)}$ s.t.  $0 \le \alpha_{i} \le C, \quad \forall i = 1, \dots, N$   $\sum_{i=1}^{N} \alpha_{i} y^{(i)} = 0$ 

We can also work with the dual of the soft-margin SVM

# Multiclass SVMs

The SVM is **inherently** a **binary** classification method, but can be extended to handle K-class classification in many ways.

- 1. one-vs-rest:
  - build K binary classifiers
  - train the k<sup>th</sup> classifier to predict whether an instance has label k or something else
  - predict the class with largest score
- 2. one-vs-one:
  - build (K choose 2) binary classifiers
  - train one classifier for distinguishing between each pair of labels
  - predict the class with the most "votes" from any given classifier

# Learning Objectives

#### **Support Vector Machines**

You should be able to...

- 1. Motivate the learning of a decision boundary with large margin
- 2. Compare the decision boundary learned by SVM with that of Perceptron
- 3. Distinguish unconstrained and constrained optimization
- 4. Compare linear and quadratic mathematical programs
- 5. Derive the hard-margin SVM primal formulation
- 6. Derive the Lagrangian dual for a hard-margin SVM
- 7. Describe the mathematical properties of support vectors and provide an intuitive explanation of their role
- 8. Draw a picture of the weight vector, bias, decision boundary, training examples, support vectors, and margin of an SVM
- 9. Employ slack variables to obtain the soft-margin SVM
- 10. Implement an SVM learner using a black-box quadratic programming (QP) solver

#### KERNELS

# Kernels: Motivation

# Most real-world problems exhibit data that is not linearly separable.

Example: pixel representation for Facial Recognition:



- **Q:** When your data is **not linearly separable**, how can you still use a linear classifier?
- A: Preprocess the data to produce nonlinear features

# Kernels: Motivation

- Motivation #1: Inefficient Features
  - Non-linearly separable data requires high dimensional representation
  - Might be prohibitively expensive to compute or store
- Motivation #2: Memory-based Methods
  - k-Nearest Neighbors (KNN) for facial recognition allows a distance metric between images -- no need to worry about linearity restriction at all

# Kernel Methods

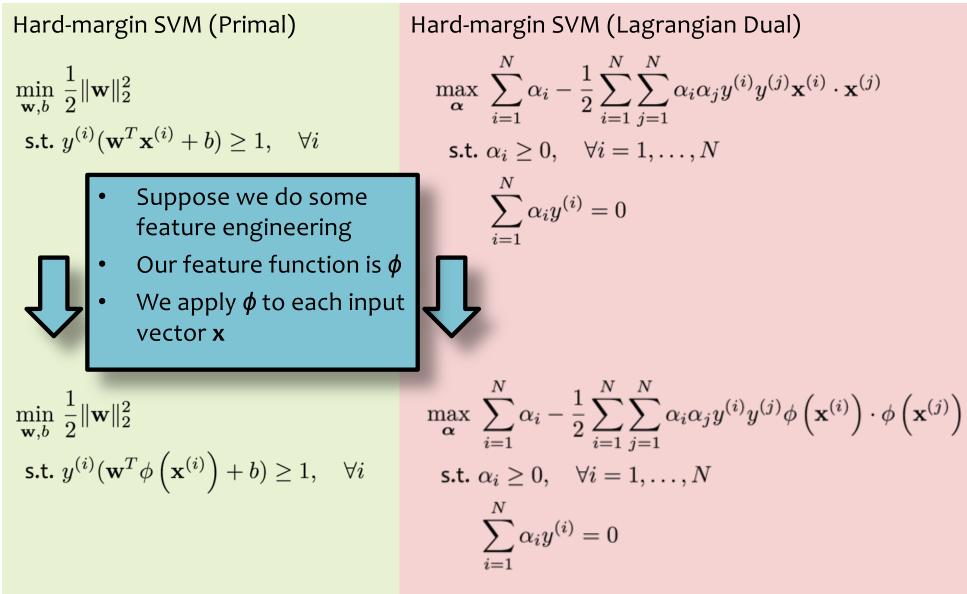
- Key idea:
  - 1. Rewrite the algorithm so that we only work with **dot products** x<sup>T</sup>z of feature vectors
  - 2. Replace the dot products  $x^T z$  with a kernel function k(x, z)
- The kernel k(x,z) can be **any** legal definition of a dot product:

 $k(x, z) = \varphi(x)^{T} \varphi(z)$  for any function  $\varphi: X \rightarrow \mathbf{R}^{D}$ 

So we only compute the  $\phi$  dot product **implicitly** 

- This "kernel trick" can be applied to many algorithms:
  - classification: perceptron, SVM, ...
  - regression: ridge regression, ...
  - clustering: k-means, ...

# SVM: Kernel Trick



# SVM: Kernel Trick

Hard-margin SVM (Lagrangian Dual)

$$\begin{aligned} \max_{\boldsymbol{\alpha}} & \sum_{i=1}^{N} \alpha_{i} - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_{i} \alpha_{j} y^{(i)} y^{(j)} \phi\left(\mathbf{x}^{(i)}\right) \cdot \phi\left(\mathbf{x}^{(j)}\right) \\ \text{s.t.} & \alpha_{i} \geq 0, \quad \forall i = 1, \dots, N \\ & \sum_{i=1}^{N} \alpha_{i} y^{(i)} = 0 \end{aligned}$$

We could replace the dot product of the two feature vectors in the transformed space with a function k(x,z) where  $k(\mathbf{x}^{(i)}, \mathbf{x}^{(j)}) = \phi(\mathbf{x}^{(i)}) \cdot \phi(\mathbf{x}^{(j)})$ 

# SVM: Kernel Trick

Hard-margin SVM (Lagrangian Dual)

$$\max_{\boldsymbol{\alpha}} \sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y^{(i)} y^{(j)} k(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$$
  
s.t.  $\alpha_i \ge 0, \quad \forall i = 1, \dots, N$ 
$$\sum_{i=1}^{N} \alpha_i y^{(i)} = 0$$

We could replace the dot product of the two feature vectors in the transformed space with a function k(x,z) where  $k(\mathbf{x}^{(i)}, \mathbf{x}^{(j)}) = \phi(\mathbf{x}^{(i)}) \cdot \phi(\mathbf{x}^{(j)})$ 

# Kernel Methods

- Key idea:
  - 1. Rewrite the algorithm so that we only work with **dot products** x<sup>T</sup>z of feature vectors
  - 2. Replace the dot products  $x^T z$  with a kernel function k(x, z)
- The kernel k(x,z) can be **any** legal definition of a dot product:

 $k(x, z) = \varphi(x)^{T} \varphi(z)$  for any function  $\varphi: X \rightarrow \mathbb{R}^{D}$ 

So we only compute the  $\phi$  dot product **implicitly** 

- This "kernel trick" can be applied to many algorithms:
  - classification: perceptron, SVM, ...
  - regression: ridge regression, ...
  - clustering: k-means, ...

# Kernel Methods

- Q: These are just non-linear features, right?A: Yes, but...
- **Q:** Can't we just compute the feature transformation φ explicitly?
- A: That depends...
- Q: So, why all the hype about the kernel trick?
  A: Because the explicit features might either be prohibitively expensive to compute or infinite length vectors

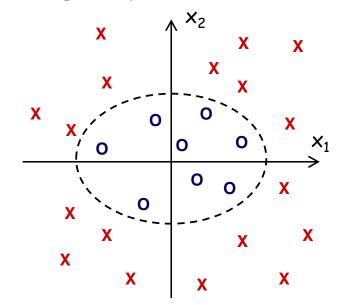
#### **Example: Polynomial Kernel**

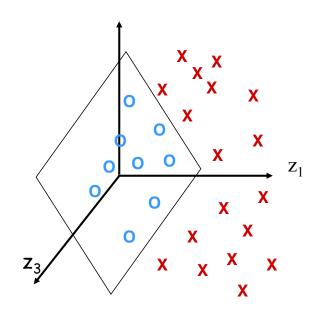
For n=2, d=2, the kernel  $K(x, z) = (x \cdot z)^d$  corresponds to

$$\begin{aligned} \varphi \colon \mathbb{R}^2 \to \mathbb{R}^3, \, (x_1, x_2) \to \Phi(x) &= (x_1^2, x_2^2, \sqrt{2}x_1 x_2) \\ \varphi(x) \cdot \varphi(z) &= (x_1^2, x_2^2, \sqrt{2}x_1 x_2) \cdot (z_1^2, z_2^2, \sqrt{2}z_1 z_2) \\ &= (x_1 z_1 + x_2 z_2)^2 = (x \cdot z)^2 = \mathbb{K}(x, z) \end{aligned}$$

Original space

 $\Phi$ -space

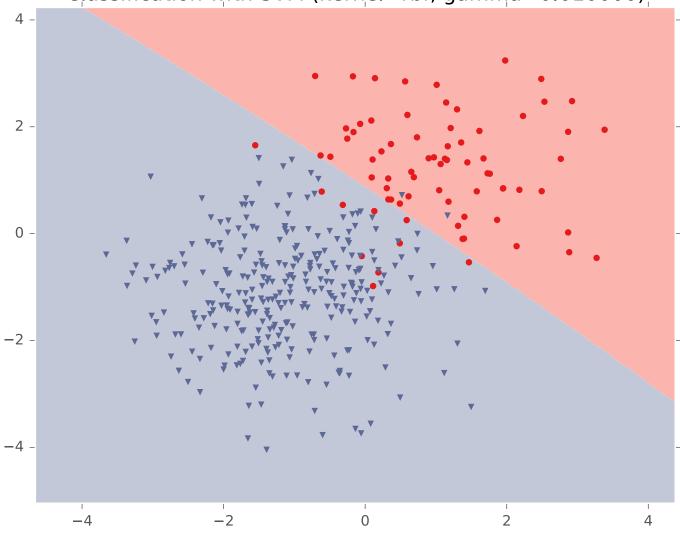




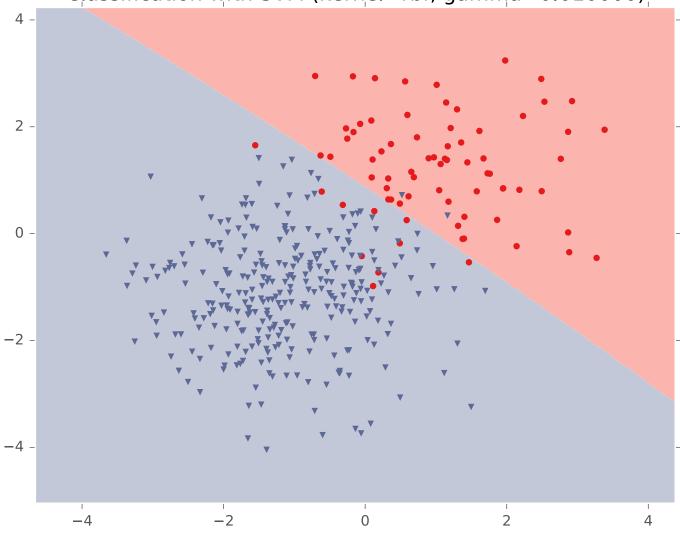
# Kernel Examples

Name	Kernel Function (implicit dot product)	Feature Space (explicit dot product)
Linear	$K(\mathbf{x}, \mathbf{z}) = \mathbf{x}^T \mathbf{z}$	Same as original input space
Polynomial (v1)	$K(\mathbf{x}, \mathbf{z}) = (\mathbf{x}^T \mathbf{z})^d$	All polynomials <b>of</b> degree d
Polynomial (v2)	$K(\mathbf{x}, \mathbf{z}) = (\mathbf{x}^T \mathbf{z} + 1)^d$	All polynomials <b>up to</b> degree d
Gaussian	$K(\mathbf{x}, \mathbf{z}) = \exp(-\frac{  \mathbf{x} - \mathbf{z}  _2^2}{2\sigma^2})$	Infinite dimensional space
Hyperbolic Tangent (Sigmoid) Kernel	$K(\mathbf{x}, \mathbf{z}) = \tanh(\alpha \mathbf{x}^T \mathbf{z} + c)$	(With SVM, this is equivalent to a 2-layer neural network)

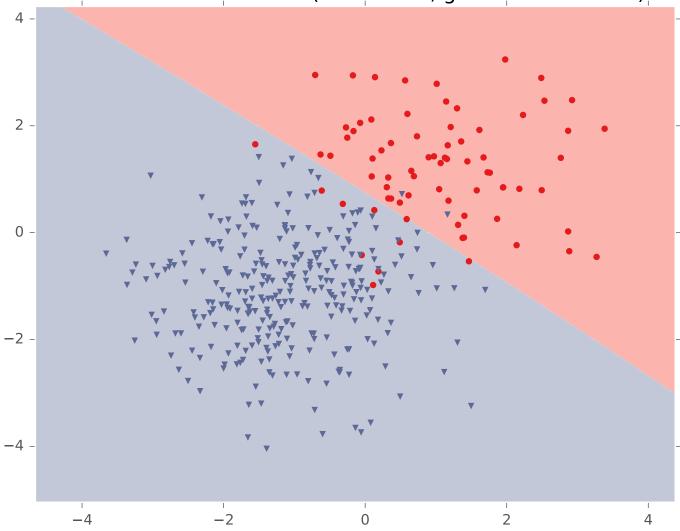
Classification with SVM (kernel=rbf, gamma=0.010000)



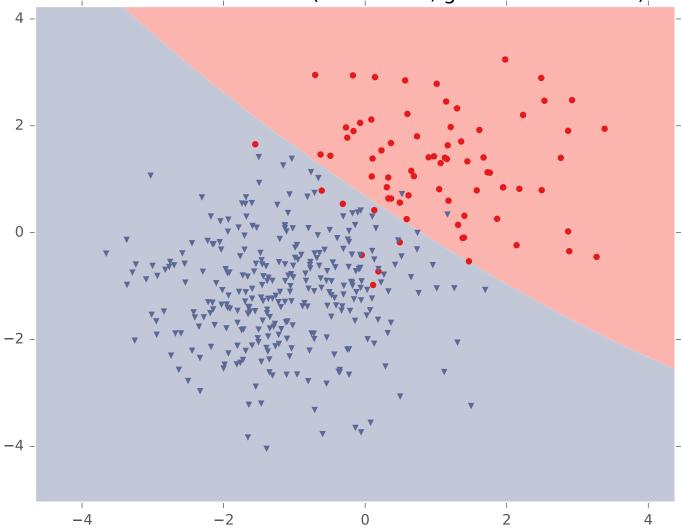
Classification with SVM (kernel=rbf, gamma=0.010000)



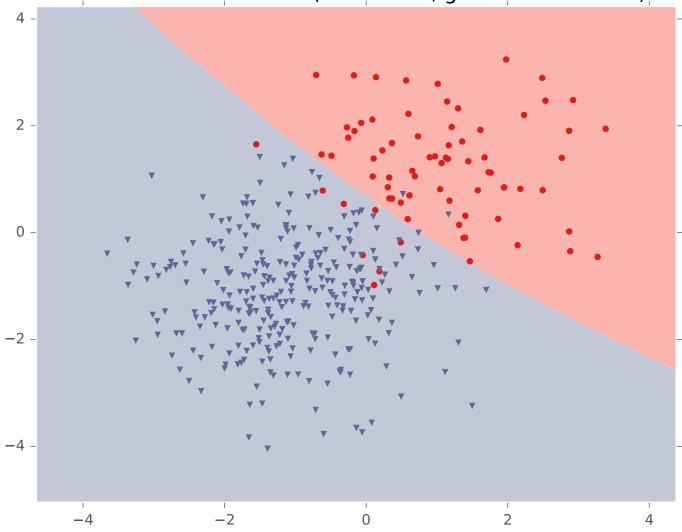
Classification with SVM (kernel=rbf, gamma=0.02000)



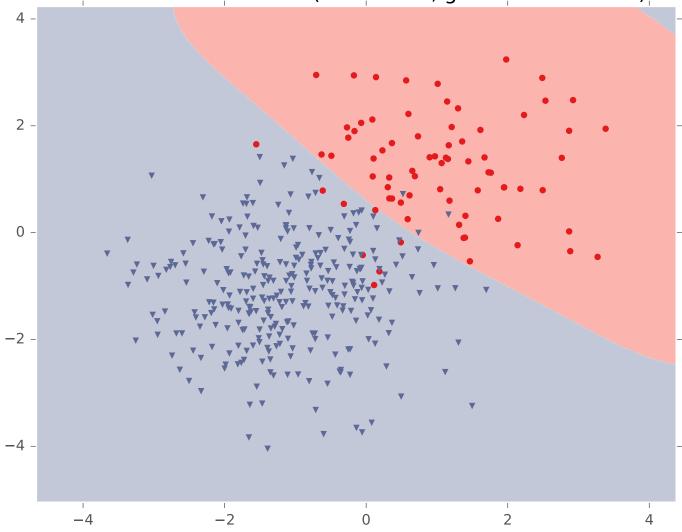
Classification with SVM (kernel=rbf, gamma=0.040000)



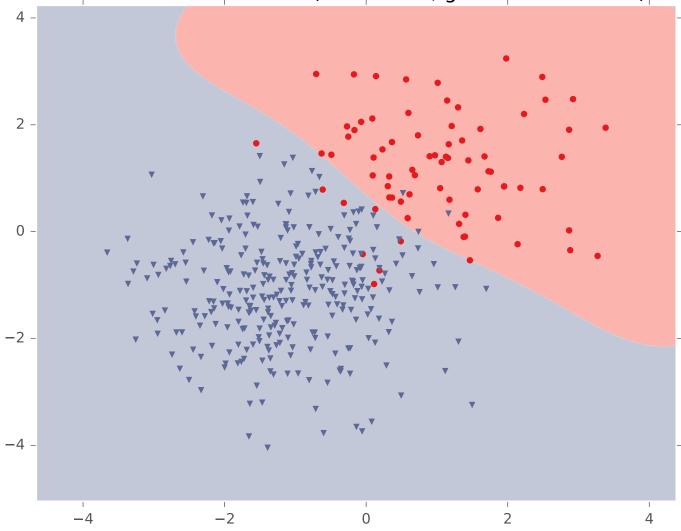
Classification with SVM (kernel=rbf, gamma=0.080000)



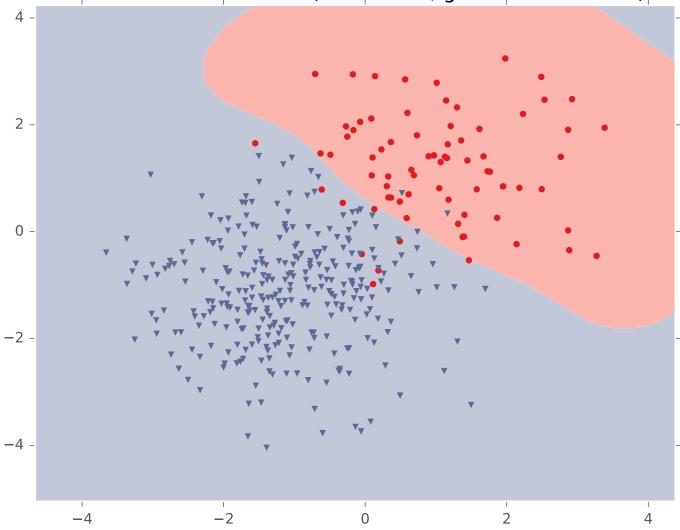
Classification with SVM (kernel=rbf, gamma=0.160000)



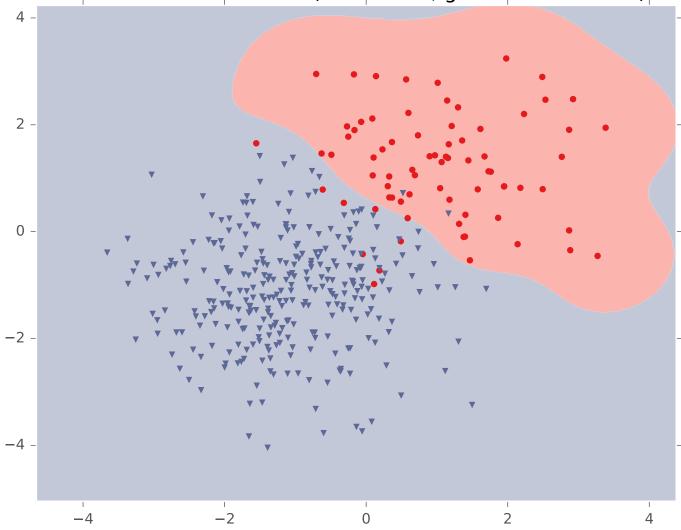
Classification with SVM (kernel=rbf, gamma=0.32000)



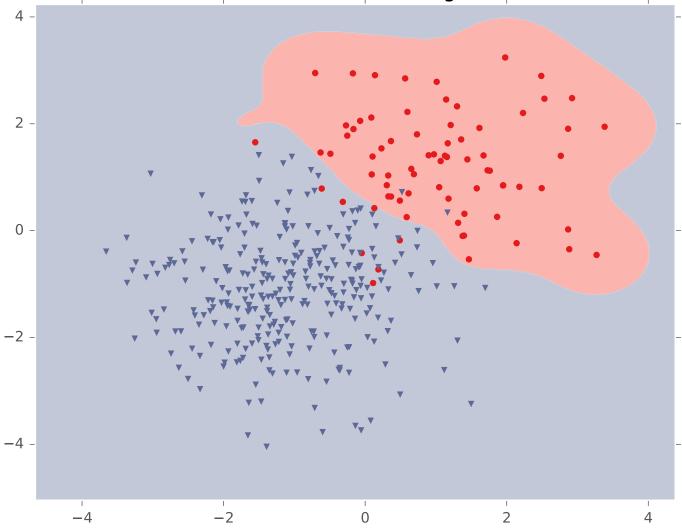
Classification with SVM (kernel=rbf, gamma=0.640000)



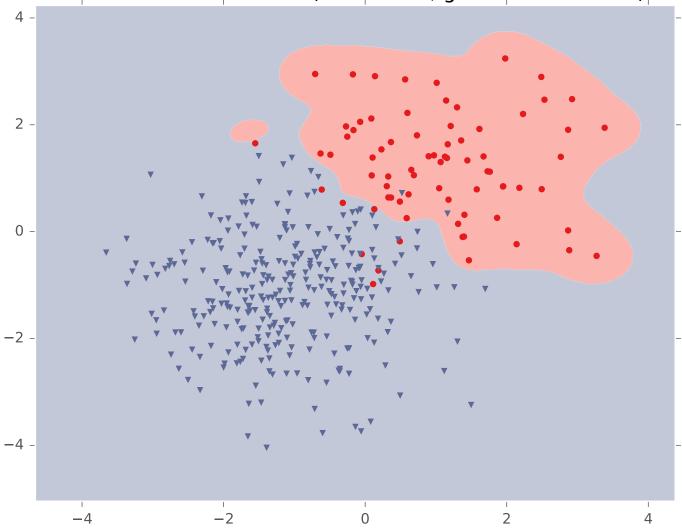
Classification with SVM (kernel=rbf, gamma=1.280000)



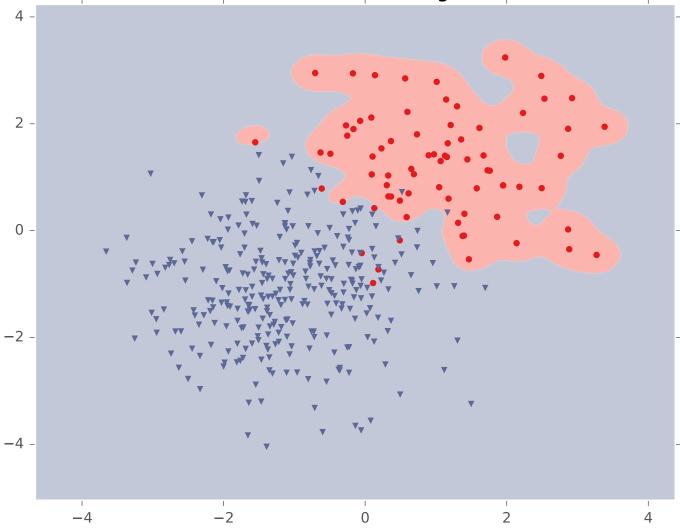
Classification with SVM (kernel=rbf, gamma=2.560000)



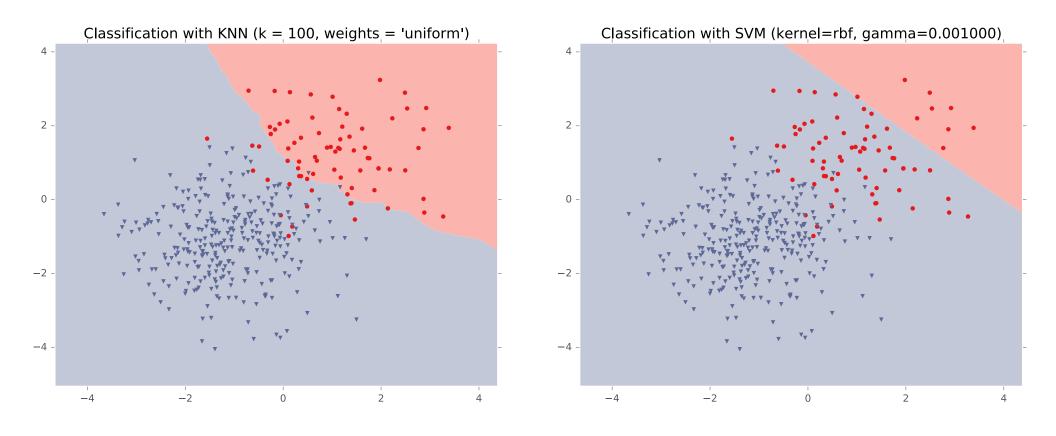
Classification with SVM (kernel=rbf, gamma=5.120000)



Classification with SVM (kernel=rbf, gamma=10.00000)

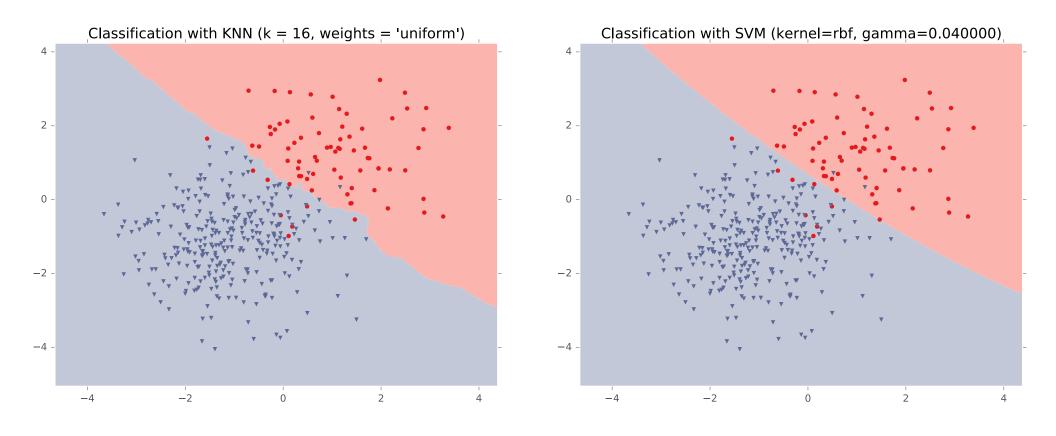


#### KNN vs. SVM

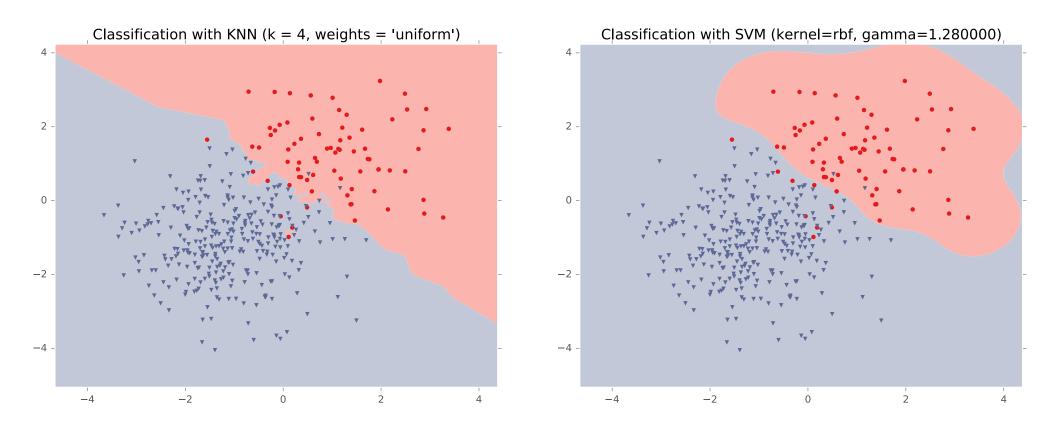


RBF Kernel: 
$$K(\mathbf{x}^{(i)}, \mathbf{x}^{(j)}) = \exp(-\gamma ||\mathbf{x}^{(i)} - \mathbf{x}^{(j)}||_2^2)$$

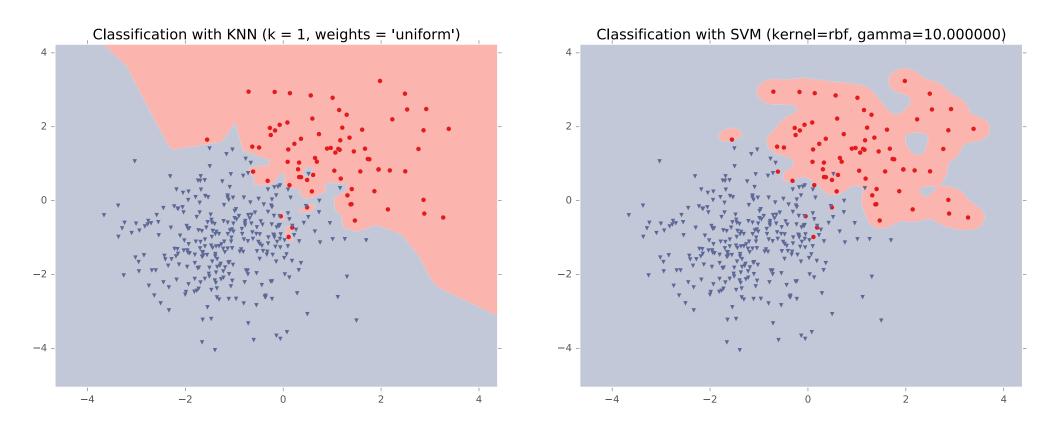
#### KNN vs. SVM



#### KNN vs. SVM



#### KNN vs. SVM



# Kernel Methods

- Key idea:
  - 1. Rewrite the algorithm so that we only work with **dot products** x<sup>T</sup>z of feature vectors
  - 2. Replace the dot products  $x^T z$  with a kernel function k(x, z)
- The kernel k(x,z) can be **any** legal definition of a dot product:

 $k(x, z) = \varphi(x)^{T} \varphi(z)$  for any function  $\varphi: X \rightarrow \mathbf{R}^{D}$ 

So we only compute the  $\phi$  dot product **implicitly** 

- This "kernel trick" can be applied to many algorithms:
  - classification: perceptron, SVM, ...
  - regression: ridge regression, ...
  - clustering: k-means, ...

# SVM + Kernels: Takeaways

- Maximizing the margin of a linear separator is a good training criteria
- Support Vector Machines (SVMs) learn a max-margin linear classifier
- The SVM optimization problem can be solved with black-box Quadratic Programming (QP) solvers
- Learned decision boundary is defined by its support vectors
- Kernel methods allow us to work in a transformed feature space without explicitly representing that space
- The kernel-trick can be applied to SVMs, as well as many other algorithms

# Learning Objectives

#### Kernels

You should be able to...

- 1. Employ the kernel trick in common learning algorithms
- 2. Explain why the use of a kernel produces only an implicit representation of the transformed feature space
- Use the "kernel trick" to obtain a computational complexity advantage over explicit feature transformation
- 4. Sketch the decision boundaries of a linear classifier with an RBF kernel