# Optimization and (Under/over)fitting

EECS 442 – David Fouhey Winter 2023, University of Michigan

http://web.eecs.umich.edu/~fouhey/teaching/EECS442\_W23/

### Regularized Least Squares

Add **regularization** to objective that prefers some solutions:

Before: 
$$\arg \min_{\mathbf{w}} ||\mathbf{y} - \mathbf{X}\mathbf{w}||_2^2 \longrightarrow \text{Loss}$$

After: 
$$\underset{w}{\operatorname{arg min}} \| \mathbf{y} - \mathbf{X} \mathbf{w} \|_{2}^{2} + \lambda \| \mathbf{w} \|_{2}^{2}$$

Loss Trade-off Regularization

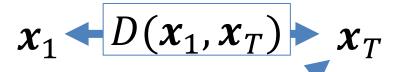
Want model "smaller": pay a penalty for w with big norm

Intuitive Objective: accurate model (low loss) but not too complex (low regularization). λ controls how much of each.

### **Nearest Neighbors**

Known Images Labels





 $D(\boldsymbol{x}_N, \boldsymbol{x}_T)$ 

Test Image



. . .



 $\boldsymbol{x}_N$ 

(1) Compute distance between feature vectors (2) find nearest(3) use label.

### Picking Parameters

What distance? What value for  $k / \lambda$ ?

Training Validation Test

Use these data points for lookup

Evaluate on these points for different k, λ, distances

#### **Linear Models**

Example Setup: 3 classes



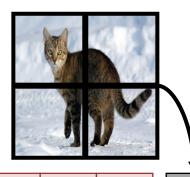




Model – one weight per class:  $w_0, w_1, w_2$   $w_0^T x$  big if cat Want:  $w_1^T x$  big if dog  $w_2^T x$  big if hippo

Stack together:  $W_{3xF}$  where **x** is in R<sup>F</sup>

#### Linear Models



Cat weight vector Dog weight vector Hippo weight vector

0.2	-0.5	0.1	2.0	1.1
1.5	1.3	2.1	0.0	3.2
0.0	0.3	0.2	-0.3	-1.2

231

Cat score

437.9

-96.8

Dog score

61.95

Hippo score

W

Weight matrix a collection of scoring functions, one per class

56

24

X

Wx

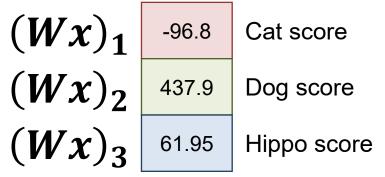
Prediction is vector where jth component is "score" for jth class.

### How Badly Are We Doing?



Loss: dog score – cat score How much higher-scored is "dog" vs "cat"?  $(Wx)_2 - (Wx)_1$ 

Don't give negative penalties  $\max(0, (Wx)_2 - (Wx)_1)$ 



#### Wx

Prediction is vector where jth component is "score" for jth class.

### Objective 1: Multiclass SVM\*

Inference (x):  $\underset{k}{\text{arg max}} (Wx)_k$ 

(Take the class whose weight vector gives the highest score)

Training  $(\mathbf{x}_i, \mathbf{y}_i)$ :

$$\arg\min_{\mathbf{W}} \lambda \|\mathbf{W}\|_{2}^{2} + \sum_{i=1}^{\infty} \sum_{j \neq y_{i}} \max(0, (\mathbf{W}x_{i})_{j} - (\mathbf{W}x_{i})_{y_{i}})$$

Regularization

Over all data points

For every class j that's NOT the correct one (y<sub>i</sub>)

Pay no penalty if prediction for class y<sub>i</sub> is bigger than j. Otherwise, pay proportional to the score of the wrong class.

### Objective 1: Multiclass SVM

Inference (x):  $\underset{k}{\text{arg max}} (Wx)_k$ 

(Take the class whose weight vector gives the highest score)

Training  $(\mathbf{x}_i, \mathbf{y}_i)$ :

$$\arg\min_{\mathbf{W}} \lambda \|\mathbf{W}\|_{2}^{2} + \sum_{i=1}^{\infty} \sum_{j \neq y_{i}} \sum_{i=1}^{\infty} \sum_{j \neq y_{i}} \sum_{$$

 $\max(0, (\boldsymbol{W}\boldsymbol{x}_i)_j - (\boldsymbol{W}\boldsymbol{x}_i)_{y_i} + m)$ 

Regularization

Over all data points

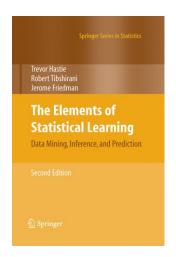
For every class j that's NOT the correct one (y<sub>i</sub>)

Pay no penalty if prediction for class y<sub>i</sub> is bigger than j by m ("margin"). Otherwise, pay proportional to the score of the wrong class.

### Objective 1:

Called: Support Vector Machine

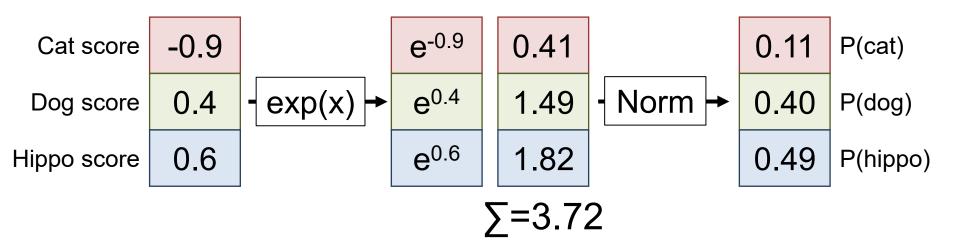
Lots of great theory as to why this is a sensible thing to do (but kernel SVMs are just secret nearest neighbor machines). See:



Useful book (Free too!):
The Elements of Statistical Learning
Hastie, Tibshirani, Friedman
<a href="https://web.stanford.edu/~hastie/ElemStatLearn/">https://web.stanford.edu/~hastie/ElemStatLearn/</a>

### Objective 2: Making Probabilities

Converting Scores to "Probability Distribution"



Generally P(class j): 
$$\frac{\exp((Wx)_j)}{\sum_k \exp((Wx)_k)}$$

Called softmax function

### Objective 2: Softmax

Inference (x): 
$$\underset{k}{\text{arg max}} (Wx)_k$$

(Take the class whose weight vector gives the highest score)

P(class j): 
$$\frac{\exp((Wx)_j)}{\sum_k \exp((Wx)_k)}$$

Why can we skip the exp/sum exp thing to make a decision?

### Objective 2: Softmax

Inference (x):  $\underset{k}{\text{arg max}} (Wx)_k$ 

(Take the class whose weight vector gives the highest score)

Training  $(\mathbf{x}_i, \mathbf{y}_i)$ :  $\text{arg min } \lambda ||\mathbf{W}||_2^2 + \sum_{i=1}^n -\log\left(\frac{\exp((Wx)_{y_i})}{\sum_k \exp((Wx)_k))}\right)$ Regularization

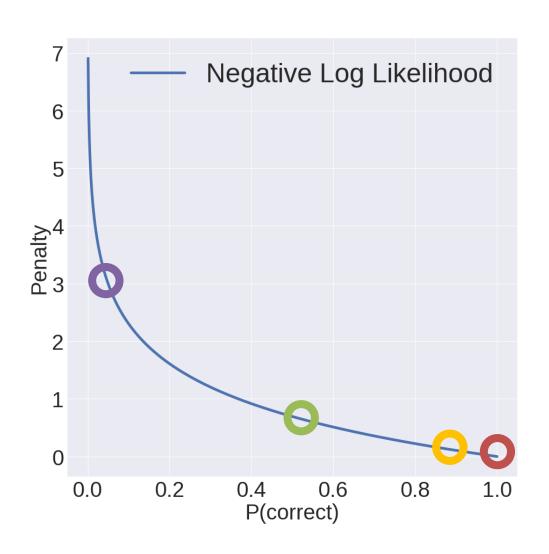
Over all data

Pay penalty for not making points correct class likely

correct class likely.

"Negative log-likelihood"

### Objective 2: Softmax



```
P(correct) = 0.05: 3.0 penalty
```

P(correct) = 0.5: 0.11 penalty

**P(correct) = 0.9: 0.11 penalty** 

P(correct) = 1: No penalty!

### How Do We Optimize Things?

Goal: find the **w** minimizing some loss function L.

$$\underset{\boldsymbol{w}\in R^N}{\operatorname{arg}} \min_{\boldsymbol{w}\in R^N} L(\boldsymbol{w})$$

Works for lots of different Ls:

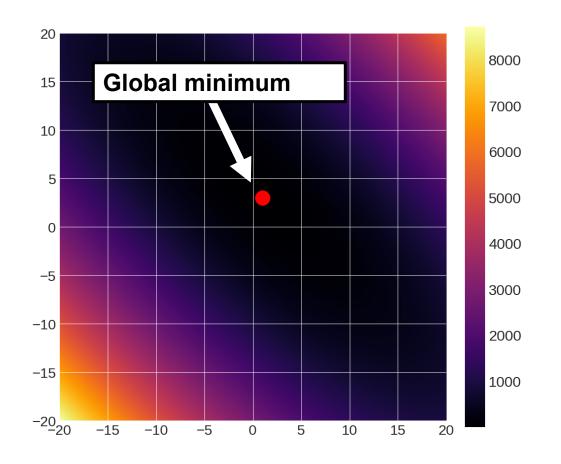
$$L(\mathbf{W}) = \lambda \|\mathbf{W}\|_{2}^{2} + \sum_{i=1}^{n} -\log \left(\frac{\exp((Wx)_{y_{i}})}{\sum_{k} \exp((Wx)_{k})}\right)$$

$$L(\mathbf{w}) = \lambda \|\mathbf{w}\|_{2}^{2} + \sum_{i=1}^{n} (y_{i} - \mathbf{w}^{T} \mathbf{x}_{i})^{2}$$

$$L(\mathbf{w}) = C \|\mathbf{w}\|_{2}^{2} + \sum_{i=1}^{n} \max(0.1 - y_{i} \mathbf{w}^{T} \mathbf{x}_{i})$$

### Sample Function to Optimize

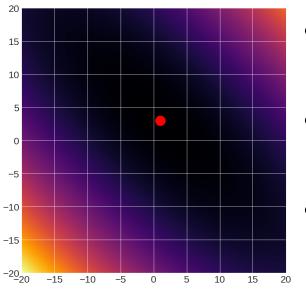
$$f(x,y) = (x+2y-7)^2 + (2x+y-5)^2$$



### Sample Function to Optimize

- I'll switch back and forth between this 2D function (called the *Booth Function*) and other more-learning-focused functions
- Beauty of optimization is that it's all the same in principle
- But don't draw too many conclusions: 2D space has qualitative differences from 1000D space

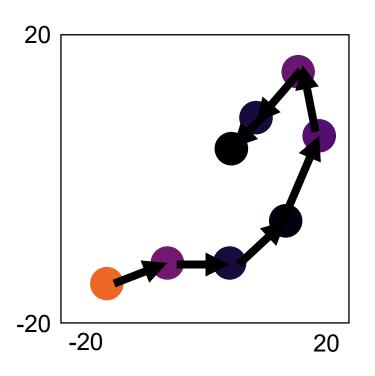
#### A Caveat

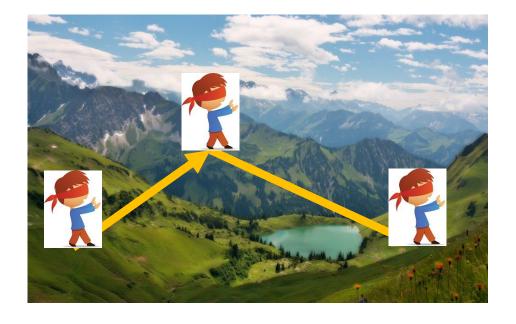


- Each point in the picture is a function evaluation
- Here it takes microseconds so we can easily see the answer
- Functions we want to optimize may take hours to evaluate

#### A Caveat

## Model in your head: moving around a landscape with a teleportation device



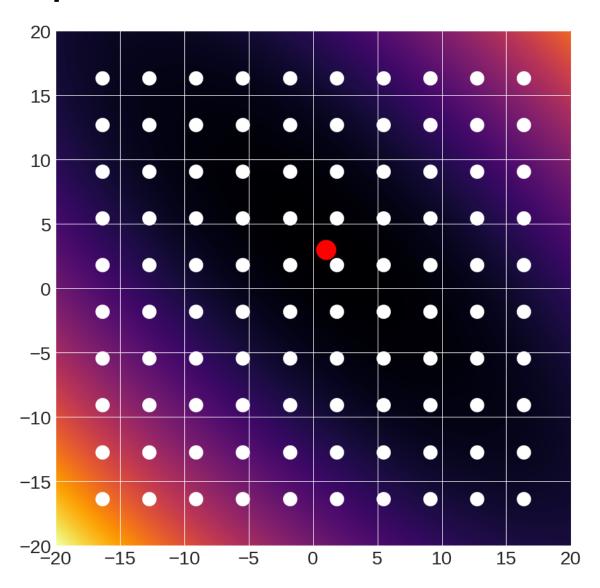


Landscape diagram: Karpathy and Fei-Fei

### Option #1A – Grid Search

```
#systematically try things
best, bestScore = None, Inf
for dim1Value in dim1Values:
      for dimNValue in dimNValues:
            w = [dim1Value, ..., dimNValue]
            if L(w) < bestScore:
                   best, bestScore = \mathbf{w}, L(\mathbf{w})
return best
```

### Option #1A – Grid Search



### Option #1A – Grid Search

#### Pros:

- 1. Super simple
- 2. Only requires being able to evaluate model

#### Cons:

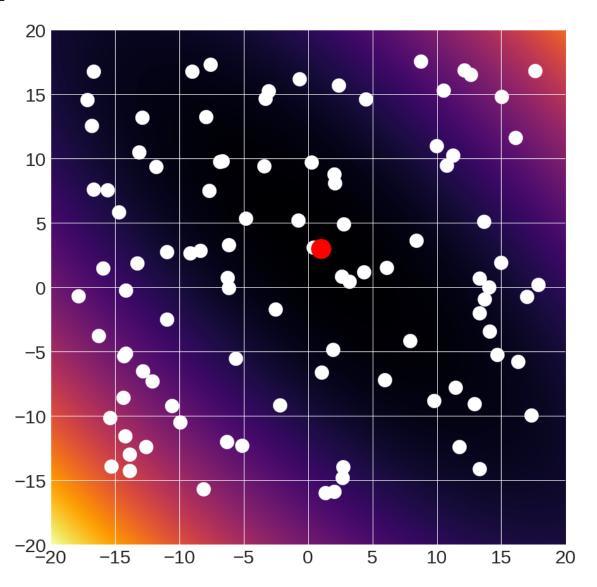
Scales horribly to high dimensional spaces

Complexity: samplesPerDim<sup>numberOfDims</sup>

### Option #1B – Random Search

```
#Do random stuff RANSAC Style
best, bestScore = None, Inf
for iter in range(numIters):
      \mathbf{w} = \text{random}(N,1) \#\text{sample}
      score = L(w) #evaluate
      if score < bestScore:
             best, bestScore = w, score
return best
```

### Option #1B – Random Search



### Option #1B – Random Search

#### Pros:

- 1. Super simple
- 2. Only requires being able to sample model and evaluate it

#### Cons:

- Slow –throwing darts at high dimensional dart board
- Might miss something

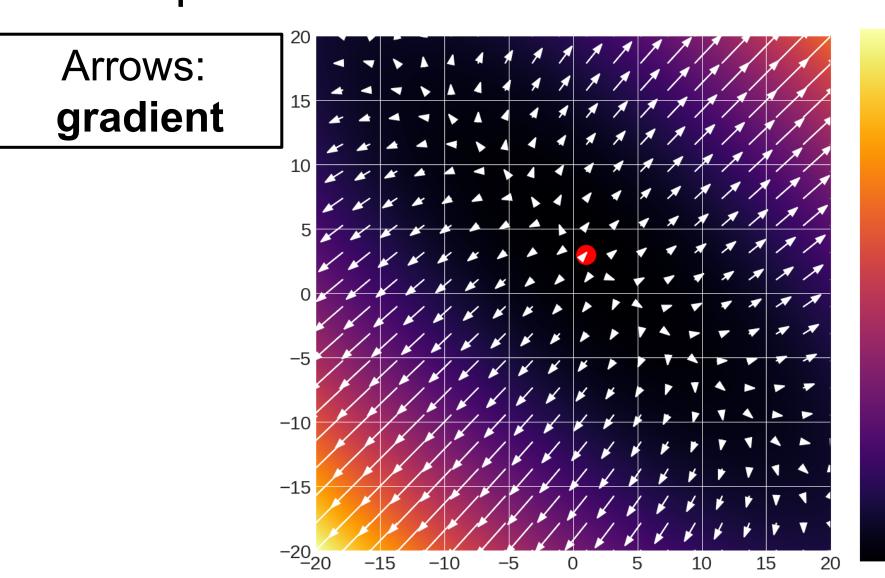
$$\begin{array}{c} P(\text{all correct}) = \\ \epsilon^{N} \\ \text{All parameters} & \bullet \\ 0 & 1 \\ \end{array}$$

### When Do You Use Options 1A/1B?

#### Use these when

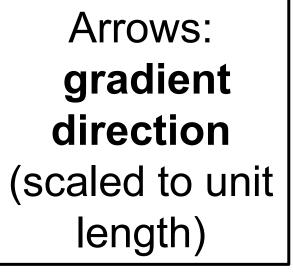
- Number of dimensions small, space bounded
- Objective is impossible to analyze (e.g., validation accuracy if one uses a distance function)

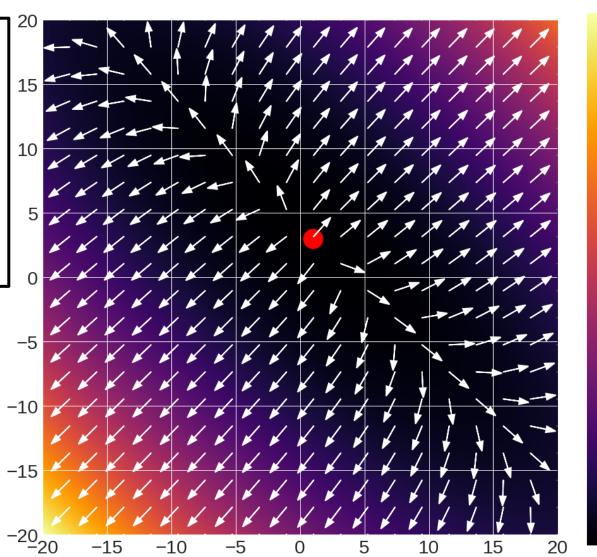
Random search is more effective; grid search makes it easy to systematically test something (people love certainty)



-10

-15





Want: 
$$\underset{\boldsymbol{w}}{\operatorname{arg min}} L(\boldsymbol{w})$$

What's the geometric

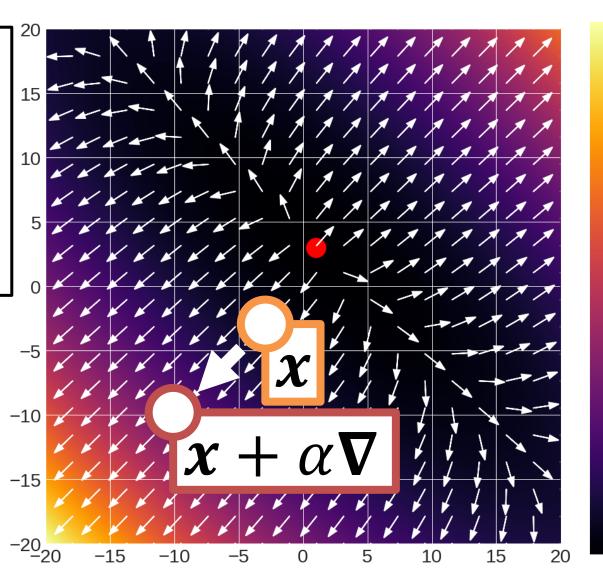
Want: 
$$\underset{w}{\arg\min} L(w)$$
 at's the geometric interpretation of: 
$$\nabla_w L(w) = \begin{bmatrix} \partial L/\partial x_1 \\ \vdots \\ \partial L/\partial x_N \end{bmatrix}$$

Which is bigger (for small  $\alpha$ )?

$$L(\mathbf{w}) \leq ?$$

$$>? L(\mathbf{w} + \alpha \nabla_{\mathbf{w}} L(\mathbf{w}))$$

Arrows:
gradient
direction
(scaled to unit
length)

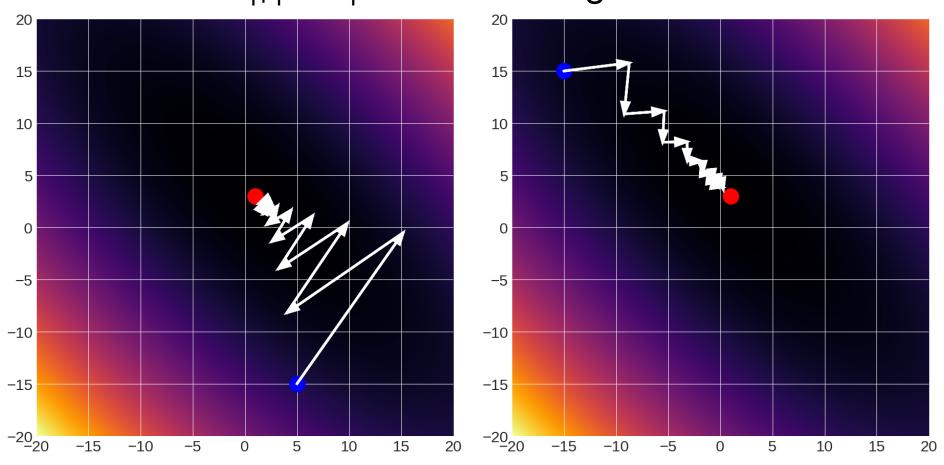


Method: at each step, move in direction of negative gradient

```
w0 = initialize() #initialize
for iter in range(numIters):
    g = ∇<sub>w</sub>L(w) #eval gradient
    w = w + -stepsize(iter)*g #update w
return w
```

#### **Gradient Descent**

Given starting point (blue)  $w_{i+1} = w_i + -9.8 \times 10^{-2} \text{ x gradient}$ 



### How Do You Compute The Gradient? **Numerical Method:**

$$\nabla_{\boldsymbol{w}}L(\boldsymbol{w}) = \begin{bmatrix} \frac{\partial L(\boldsymbol{w})}{\partial x_1} \\ \vdots \\ \frac{\partial L(\boldsymbol{w})}{\partial x_n} \end{bmatrix}$$
How do you compute this?
$$\frac{\partial f(x)}{\partial x} = \lim_{\epsilon \to 0} \frac{f(x+\epsilon) - f(x)}{\epsilon}$$
In practice, use:
$$\frac{f(x+\epsilon) - f(x-\epsilon)}{2\epsilon}$$

#### How do you compute this?

$$\frac{\partial f(x)}{\partial x} = \lim_{\epsilon \to 0} \frac{f(x+\epsilon) - f(x)}{\epsilon}$$

$$\frac{f(x+\epsilon)-f(x-\epsilon)}{2\epsilon}$$

### How Do You Compute The Gradient? **Numerical Method:**

$$\nabla_{w}L(w) = \begin{bmatrix} \frac{\partial L(w)}{\partial x_{1}} \\ \frac{\partial L(w)}{\partial x_{n}} \end{bmatrix}$$
 Use: 
$$\frac{f(x+\epsilon) - f(x-\epsilon)}{2\epsilon}$$
 How many function evaluations per dimension?

Use: 
$$\frac{f(x+\epsilon) - f(x-\epsilon)}{2\epsilon}$$

How Do You Compute The Gradient?

Analytical Method:

$$\nabla_{\mathbf{w}} L(\mathbf{w}) = \begin{bmatrix} \frac{\partial L(\mathbf{w})}{\partial x_1} \\ \vdots \\ \frac{\partial L(\mathbf{w})}{\partial x_n} \end{bmatrix}$$

Use calculus!

$$L(w) = \lambda ||w||_{2}^{2} + \sum_{i=1}^{n} (y_{i} - w^{T}x_{i})^{2}$$

$$\downarrow \frac{\partial}{\partial w} \downarrow$$

$$\nabla_{w}L(w) = 2\lambda w + \sum_{i=1}^{n} -(2(y_{i} - w^{T}x_{i})x_{i})$$

Note: if you look at other derivations, things are written either  $(y-w^Tx)$  or  $(w^Tx - y)$ ; the gradients will differ by a minus.

# Interpreting Gradients (1 Sample)

Recall:

$$\mathbf{w} = \mathbf{w} + -\nabla_{\mathbf{w}} L(\mathbf{w})$$
 #update w

$$\nabla_{\mathbf{w}} L(\mathbf{w}) = 2\lambda \mathbf{w} + -(2(y - \mathbf{w}^T \mathbf{x})\mathbf{x})$$

Push w towards 0

$$T_{\infty}$$

$$-\nabla_{\mathbf{w}}L(\mathbf{w}) = -2\lambda\mathbf{w} + (2(\mathbf{y} - \mathbf{w}^{T}\mathbf{x})\mathbf{x})$$

If  $y > w^Tx$  (too *low*): then  $w = w + \alpha x$  for some  $\alpha$ 

**Before**: w<sup>T</sup>x

After:  $(w + \alpha x)^T x = w^T x + \alpha x^T x$ 

## Quick annoying detail: subgradients

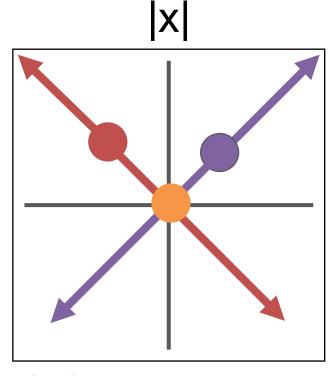
What is the derivative of |x|?

<u>Derivatives/Gradients</u> Defined everywhere but 0

$$\frac{\partial}{\partial x}f(x) = \text{sign}(x) \quad x \neq 0$$

undefined

$$x = 0$$



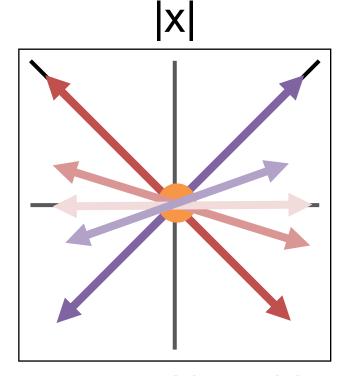
Oh no! A discontinuity!

# Quick annoying detail: subgradients

Subgradient: any underestimate of function

Subderivatives/subgradients
Defined everywhere

$$\frac{\partial}{\partial x} f(x) = \text{sign}(x) \quad x \neq 0$$
$$\frac{\partial}{\partial x} f(x) \in [-1,1] \quad x = 0$$



In practice: at discontinuity, pick value on either side.

# Computing The Gradient

- Numerical: foolproof but slow
- Analytical: can mess things up ©
- In practice: do analytical, but check with numerical (called a gradient check)

Slide: Karpathy and Fei-Fei

# Loss is a function that we can evaluate over data

All Data 
$$-\nabla_{w}L(w) = -2\lambda w + \sum_{i=1}^{N} (2(y_{i} - w^{T}x_{i})x_{i})$$

Subset B 
$$-\nabla_{\boldsymbol{w}}L_B(\boldsymbol{w}) = -2\lambda \boldsymbol{w} + \sum_{i \in B} (2(y_i - \boldsymbol{w}^T \boldsymbol{x_i})\boldsymbol{x_i})$$

Option 1: Vanilla Gradient Descent Compute gradient of L over all data points

```
for iter in range(numIters):

g = gradient(data,L)
```

w = w + -stepsize(iter)\*g #update w

Option 2: *Stochastic* Gradient Descent Compute gradient of L over 1 random sample

```
for iter in range(numIters):
  index = randint(0,#data)
  g = gradient(data[index],L)
  w = w + -stepsize(iter)*g #update w
```

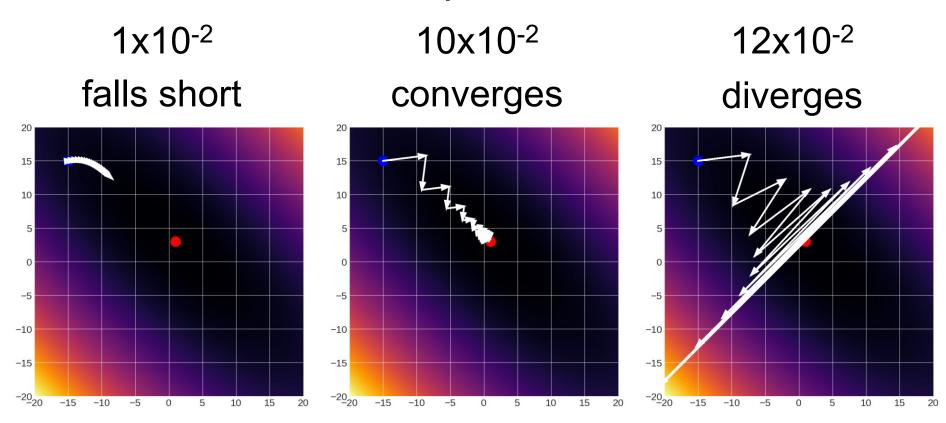
Option 3: *Minibatch* Gradient Descent Compute gradient of L over subset of B samples

```
for iter in range(numIters):
    subset = choose_samples(#data,B)
    g = gradient(data[subset],L)
    w = w + -stepsize(iter)*g #update w
```

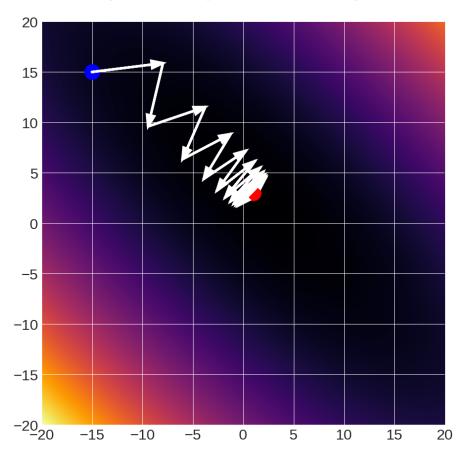
Typical batch sizes: ~100 (although there's lots of great research on huge batch sizes)

Step size (also called **learning rate** / **lr**)

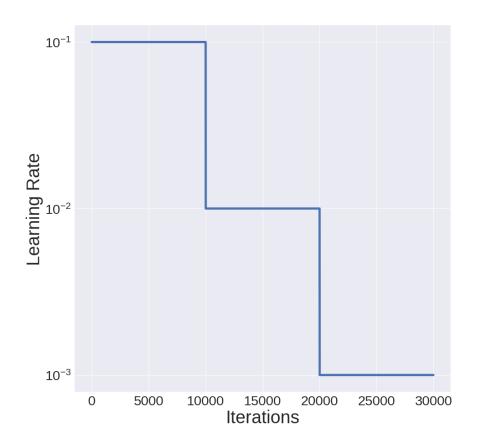
critical parameter



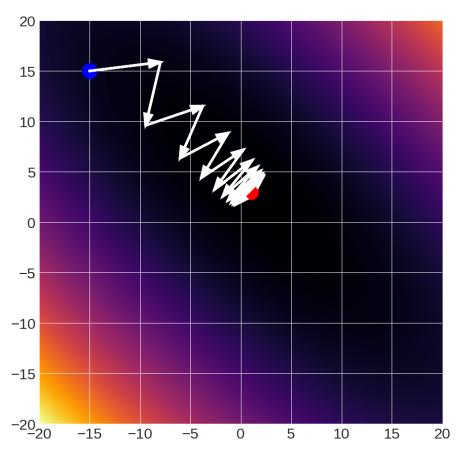
11x10<sup>-2</sup>:oscillates (Raw gradients)



# One solution: start with initial rate Ir, multiply by f every N interations

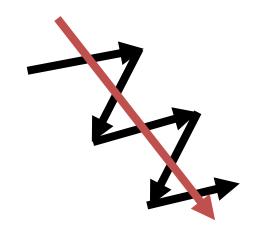


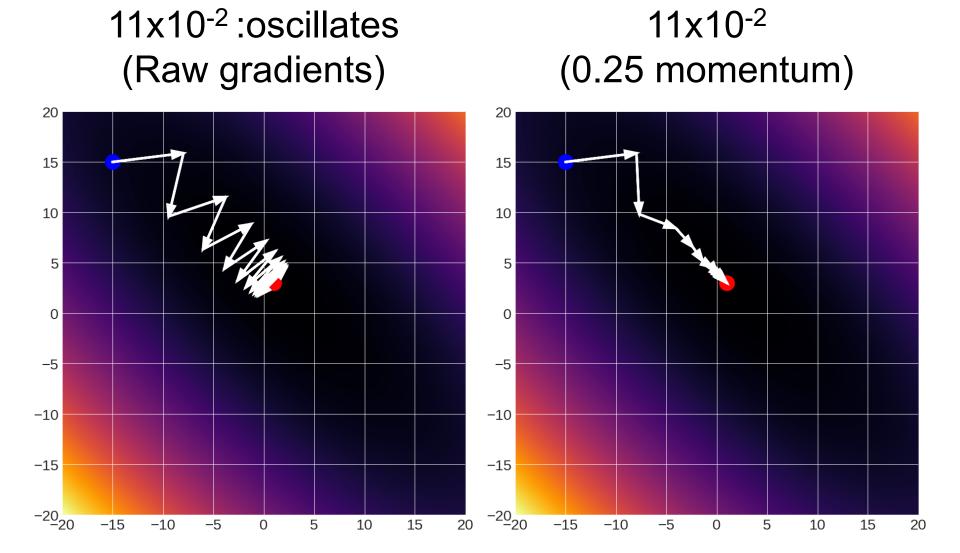
11x10<sup>-2</sup>:oscillates (Raw gradients)



# Solution: Average gradients

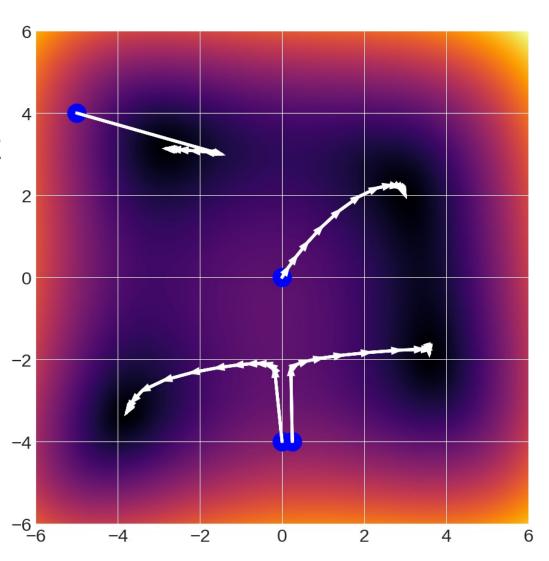
With exponentially decaying weights, called "momentum"



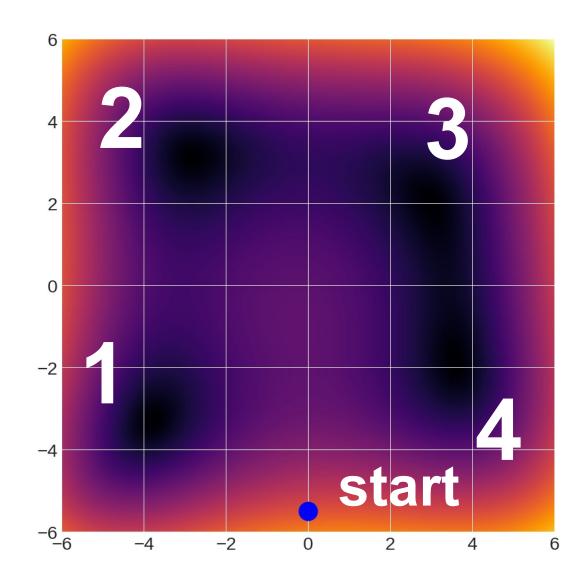


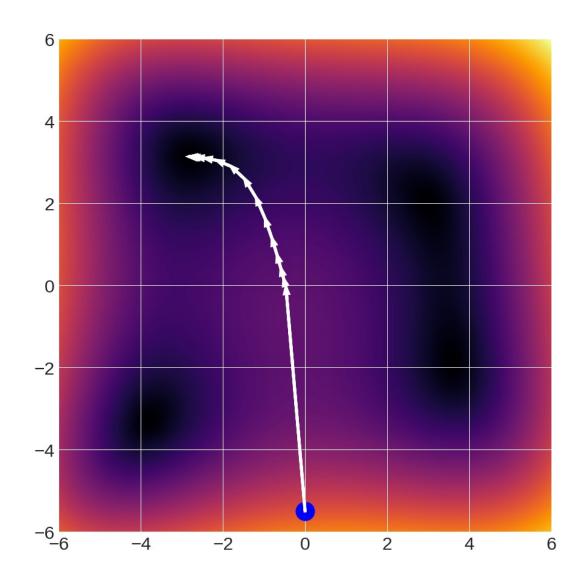
Multiple Minima

Gradient Descent Finds **local minimum** 

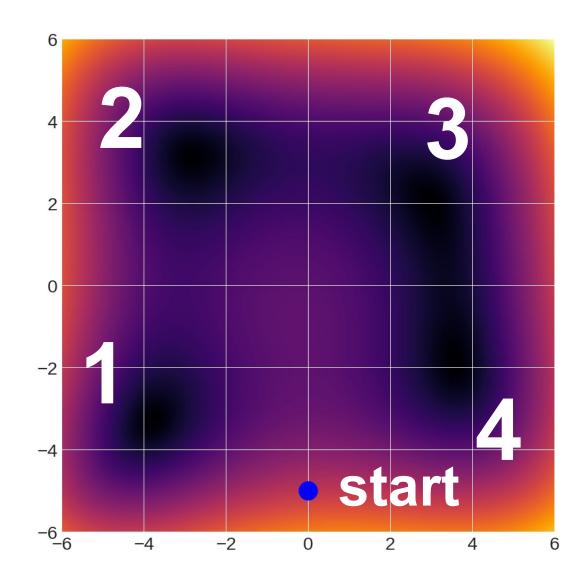


Guess the minimum!





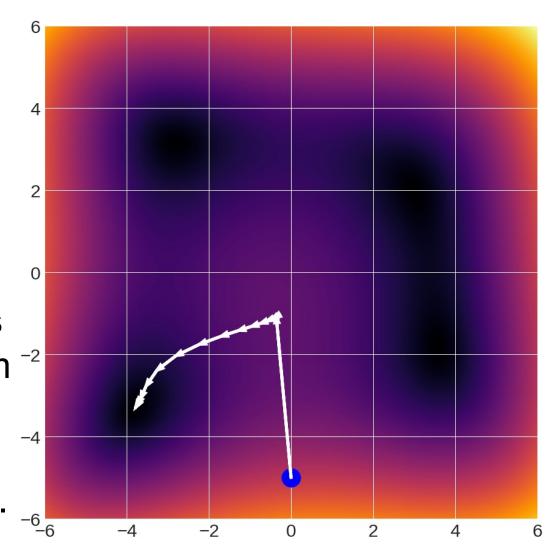
Guess the minimum!



Dynamics are fairly complex

Many important functions are convex: any local minimum is a global minimum

Many important functions are not.



#### In practice

- Conventional wisdom: minibatch stochastic gradient descent (SGD) + momentum (package implements it for you) + some sensibly changing learning rate
- The above is typically what is meant by "SGD"
- Other update rules exist (e.g., AdamW). Can often work better on some problems.

# Optimizing Everything

$$L(W) = \lambda ||W||_2^2 + \sum_{i=1}^n -\log \left( \frac{\exp((Wx)_{y_i})}{\sum_k \exp((Wx)_k))} \right)$$
$$L(W) = \lambda ||W||_2^2 + \sum_{i=1}^n (y_i - w^T x_i)^2$$

- Optimize w on training set with SGD to maximize training accuracy
- Optimize λ with random/grid search to maximize validation accuracy
- Note: Optimizing λ on training sets it to 0

## (Over/Under)fitting and Complexity

Let's fit a polynomial: given x, predict y

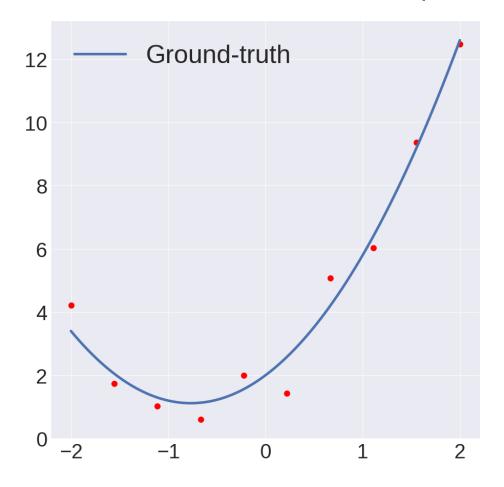
Note: can do non-linear regression with copies of x

$$\begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix} = \begin{bmatrix} x_1^F & \cdots & x_1^2 & x_1 & 1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ x_N^F & \cdots & x_N^2 & x_N & 1 \end{bmatrix} \begin{bmatrix} w_F \\ \vdots \\ w_2 \\ w_1 \\ w_0 \end{bmatrix}$$
Matrix of all polynomial degrees

Weights: one per polynomial degree

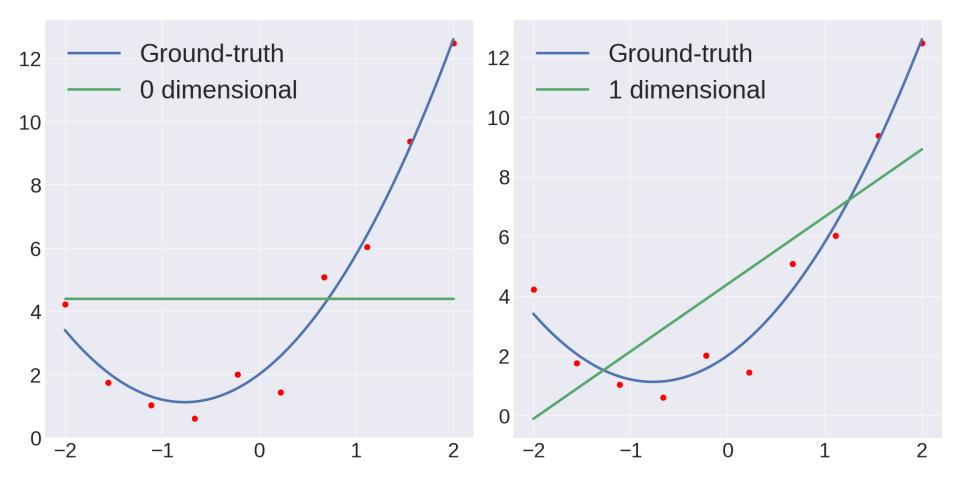
# (Over/Under)fitting and Complexity

Model:  $1.5x^2 + 2.3x + 2 + N(0,0.5)$ 

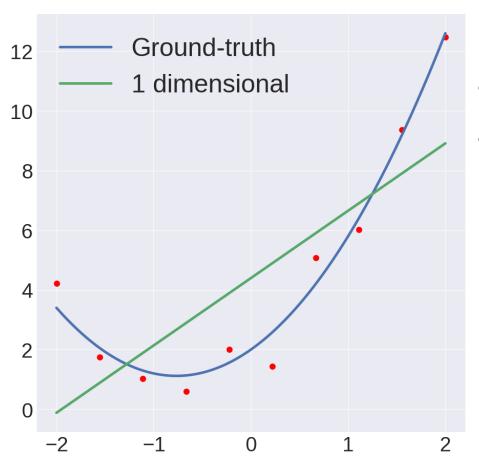


### Underfitting

Model:  $1.5x^2 + 2.3x + 2 + N(0,0.5)$ 



#### Underfitting

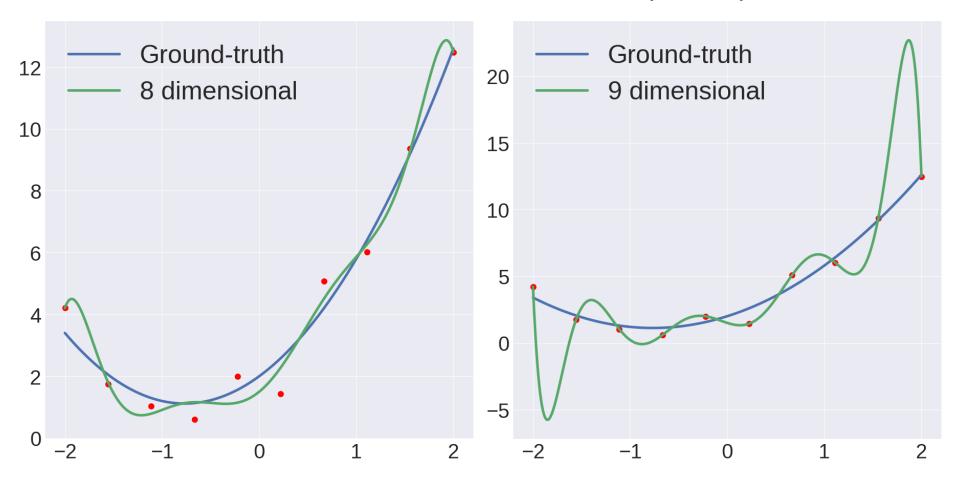


Model doesn't have the parameters to fit the data.

Bias (statistics): Error intrinsic to the model.

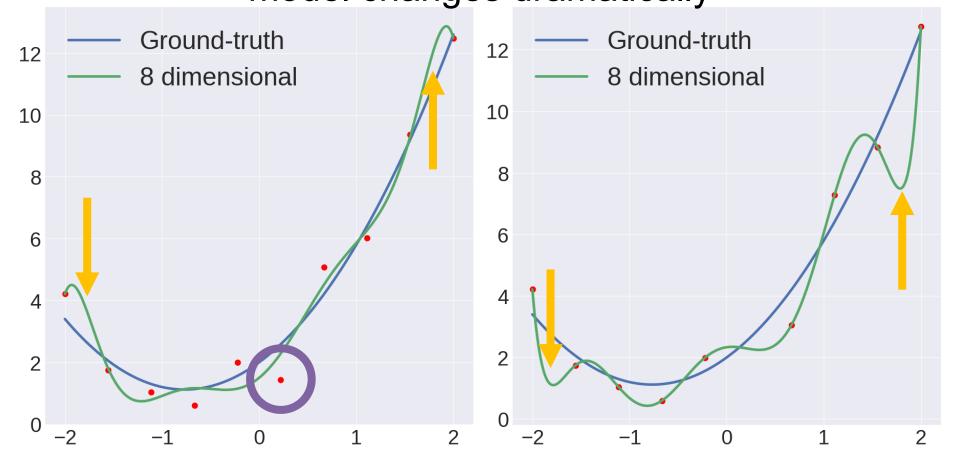
#### Overfitting

Model:  $1.5x^2 + 2.3x + 2 + N(0,0.5)$ 



#### Overfitting

Model has high *variance*: remove **one point**, and model changes dramatically



# (Continuous) Model Complexity

$$\arg\min_{\boldsymbol{W}} \lambda \|\boldsymbol{W}\|_{2}^{2} + \sum_{i=1}^{n} -\log\left(\frac{\exp((\boldsymbol{W}\boldsymbol{x})_{y_{i}})}{\sum_{k} \exp((\boldsymbol{W}\boldsymbol{x})_{k}))}\right)$$

Regularization: penalty for complex model

Pay penalty for negative loglikelihood of correct class

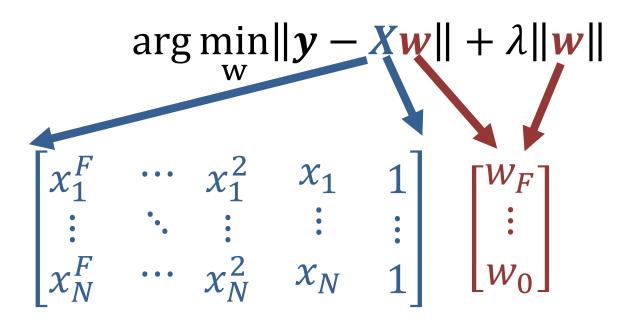
Intuitively: big weights = more complex model

Model 1:  $0.01*x_1 + 1.3*x_2 + -0.02*x_3 + -2.1x_4 + 10$ 

Model 2:  $37.2*x_1 + 13.4*x_2 + 5.6*x_3 + -6.1x_4 + 30$ 

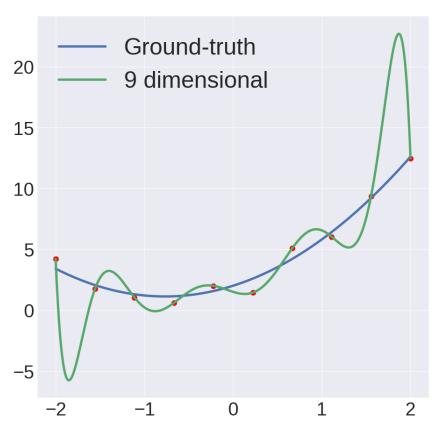
### Fitting Model

Again, fitting polynomial, but with regularization

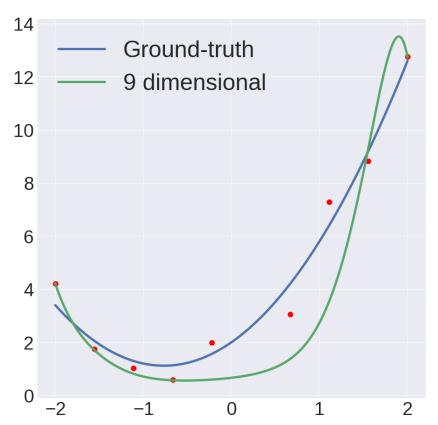


### Adding Regularization

# No regularization: fits all data points



# Regularization: can't fit all data points

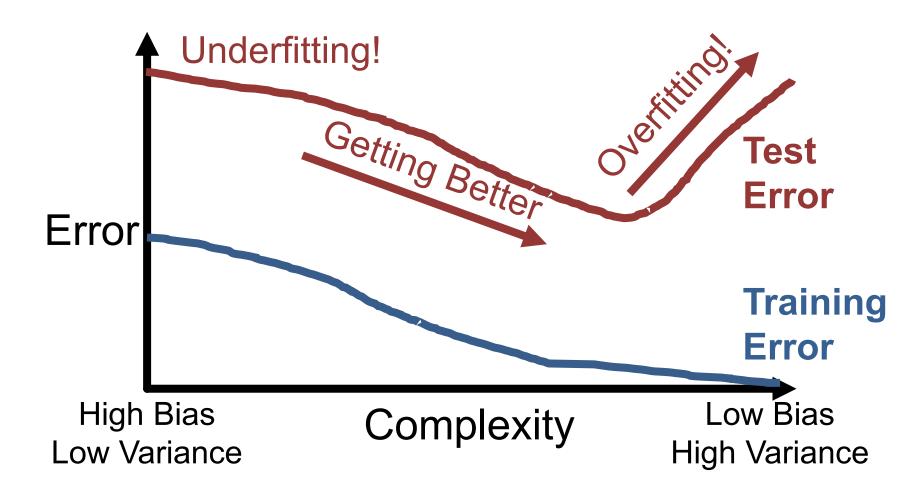


#### In General

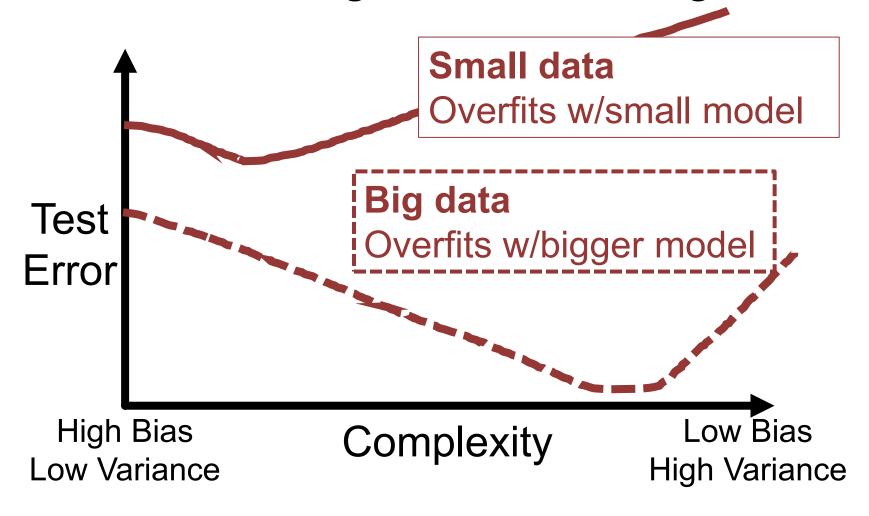
Error on new data comes from combination of:

- 1. Bias: model is oversimplified and can't fit the underlying data
- 2. Variance: you don't have the ability to estimate your model from limited data
- 3. Inherent: the data is intrinsically difficult Bias and variance trade-off. Fixing one hurts the other.

### **Underfitting and Overfitting**



## **Underfitting and Overfitting**



#### **Underfitting and Overfitting**





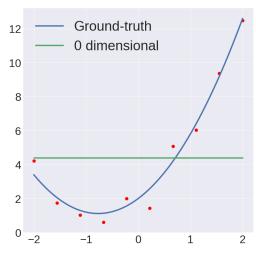
Lots of this behavior doesn't seem to replicate in models with high learning capacity.

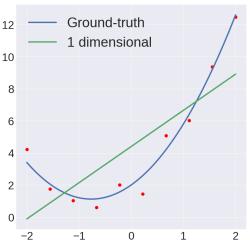
See below for details.

LOW VARIATION

ngn vanance

### Underfitting



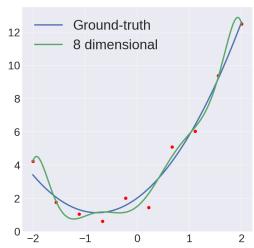


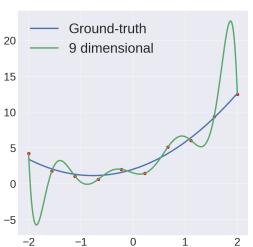
Do poorly on both training and validation data due to bias.

#### Solution:

- 1. More features
- 2. More powerful model
  - 3. Reduce regularization

#### Overfitting





Do well on training data, but poorly on validation data due to variance Solution:

- 1. More data
- 2. Less powerful model
  - 3. Regularize your model more

Cris Dima rule: first make sure you can overfit, then stop overfitting.

#### **Next Class**

Non-linear models (neural nets)

## Let's Compute Another Gradient

 Below is another derivation that's worth looking at on your own time if you're curious

# Computing The Gradient Multiclass Support Vector Machine

$$\arg\min_{\mathbf{W}} \lambda \|\mathbf{W}\|_{2}^{2} + \sum_{i=1}^{n} \sum_{j \neq y_{i}} \max(0, (\mathbf{W}x_{i})_{j} - (\mathbf{W}x_{i})_{y_{i}} + m)$$

#### **Notation:**

$$W \rightarrow rows \ w_i \ (i.e., per-class scorer) \ (Wx_i)_j \rightarrow w_j^T x_i$$

$$\arg\min_{\mathbf{W}} \lambda \sum_{j=1}^{K} ||\mathbf{w}_{j}||_{2}^{2} + \sum_{i=1}^{n} \sum_{j \neq y_{i}} \max(0, \mathbf{w}_{j}^{T} \mathbf{x}_{i} - \mathbf{w}_{y_{i}}^{T} \mathbf{x}_{i} + m)$$

# Computing The Gradient

$$\arg\min_{W} \lambda \sum_{j=1}^{K} \|w_{j}\|_{2}^{2} + \sum_{i=1}^{n} \sum_{\substack{i \neq y_{i} \\ j \neq y_{i}}} \max(0, w_{j}^{T} x_{i} - w_{y_{i}}^{T} x_{i} + m)$$

$$\rightarrow 1(w_i^T x_i - w_{y_i}^T x_i + m > 0)x_i$$

# Computing The Gradient

$$\arg\min_{W} \lambda \sum_{j=1}^{K} ||w_{j}||_{2}^{2} + \sum_{i=1}^{n} \sum_{\substack{j \neq y_{i}}} \max(0, w_{j}^{T} x_{i} - w_{y_{i}}^{T} x_{i} + m)$$

$$\frac{\partial}{\partial w_{y_i}}: \sum_{j \neq y_i} 1(w_j^T x_i - w_{y_i}^T x_i + m > 0)(-x_i)$$

### Interpreting The Gradient

$$-\frac{\partial}{\partial w_j}: 1(w_j^T x_i - w_{y_i}^T x_i + m > 0) - x_i$$

If we do not predict the correct class by at least a score difference of m ...

Want incorrect class's scoring vector to score that point lower.

Recall:

**Before**: w<sup>T</sup>x;

**After**:  $(w-\alpha x)^T x = w^T x - ax^T x$