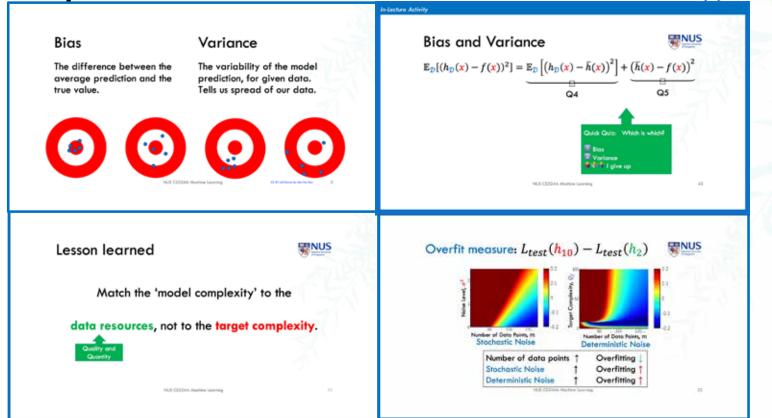


Recap from Week 05





Upcoming Milestones



Midterm

- 60-minute, 60 marks midterm, on first day of Week 07.
- Open lecture notes, mostly MCQ/MRQ
- Multiple Response Questions that correct for random chance scoring.

Projects

- Project Proposals due on Tue.
- Project Mentors to be assigned after proposal deadline.
- Peer review due next Tue. Done via Google Forms.

Multiple Response Question (MRQ)



Example:

- 5 option, 4 mark question. Note that leaving all options blank may be a valid entry.
- You marked A, B, C but correct answer was B, C, D.

Treated as a set of binary questions, where random chance agreement, rounded down, is subtracted away.

- 5 options: expected # of binary questions correct: 2.5, rounded to 2.
- You got B, C and E correct, but A, D incorrect: 3 of 5 binary questions correct.
- After chance agreement: 1 of 3 correct = awarded 1.33 marks out of 4 marks.





									I3 Seminar Room									
									Screen									
			ARE	A 4							AREA 5					A	REA 6	
í.	1	2					A	1	2	3	4	5	6	A	1	2		
	1	2		3			8	1	2	3	4	5	6	8	1	2	3	
	1	2		3			C	1	2	3	4	5	6	C	1	2	3	The same of
	1	2		3	4	- >	D	1	2	3	4	5	6	0	1	2	3	4
		2					E	1	2	3	4	10000		E	1	2		1000

Forecast for Week 06



Learning Outcomes for this week:

- Understand Regularization as a means of restraining the model.
- Choose appropriate doses of regularization for a model.
- Understand and execute Validation, as a reality check by peeking (at the bottom line).
- Understand the different forms extending validation to encompass additional estimation.
- Understand how validation and regularization complement each other and their roles in affecting learning.

NUS CS3244: Machine Learning



Two Cures



In one form or another, $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

1. Regularization: Restrain the model $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

Regularization estimates this quantity

2. Validation: Reality check by peeking (at the bottom line) $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

Restraining the model



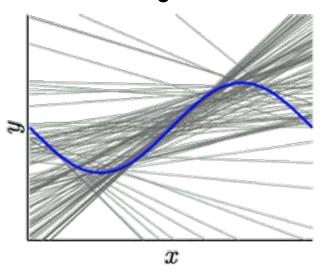
Regularization

- What is it: A cure for our tendency to fit (get distracted by) the noise, hence improving L_{test} .
- How does it work?
 By constraining the model so that we cannot fit the noise.
- Side effect: if we cannot fit the noise, maybe we cannot fit the signal f.

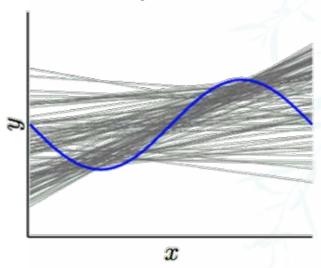
A familiar example



Without regularization



With regularization

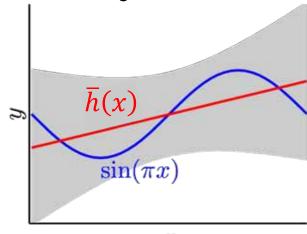


Constrain weights to be a bit smaller

Bias goes up a little



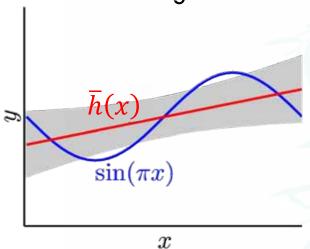




Bias = 0.21

Variance = 1.69

With regularization



Bias = 0.23

Variance = 0.33



Constraining the model:

$$\mathcal{H}_2$$
 versus \mathcal{H}_{10}

$$\mathcal{H}_{10} = \{h(x) = \theta_0 + \theta_1 x + \dots + \theta_{10} x^{10}\}$$

$$\mathcal{H}_2 = \{h(x) = \theta_0 + \theta_1 x + \dots + \theta_{10} x^{10} \}$$
 such that $\theta_3 = \theta_4 = \dots = \theta_{10} = 0$



A "hard" order constraint that sets some weights to zero.

$$\mathcal{H}_2 \subset \mathcal{H}_{10}$$



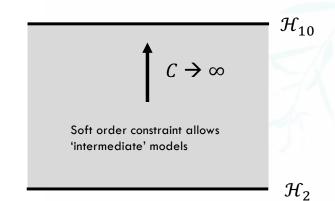
Soft Order Constraint



Don't set weights explicitly to zero.

Re-use loss optimization by giving a budget and let the learning process choose. Introduce a regularization function $\Omega(h)$.

$$\Omega(h) \equiv \sum_{q=0}^{Q} \theta_q^2 \le C$$



NUS CS3244: Machine Learning

13

Soft Order Constrained Model

are unrelated!



$$\mathcal{H}_{10} = \{ h(x) = \theta_0 + \theta_1 x + \dots + \theta_{10} x^{10} \}$$

$$\mathcal{H}_{\mathcal{C}}=\{h(x)=\theta_0+\theta_1x+\cdots+\theta_{10}x^{10}\ \}$$
 such that $\sum_{q=0}^{10}\theta_q^2\leq\mathcal{C}$

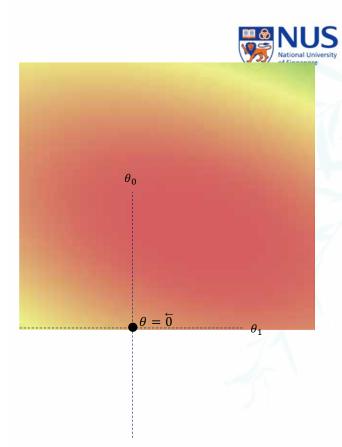
$$\mathcal{H}_2 = \{h(x) = \theta_0 + \theta_1 x + \dots + \theta_{10} x^{10}\}$$
such that $\theta_3 = \theta_4 = \dots = \theta_{10} = 0$



Solving for θ_{reg}

Minimize $L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\top} (\mathbf{X} \mathbf{\theta} - \mathbf{y})$

Subject to a regularization function $\Omega(h) \equiv \mathbf{\theta}^{\mathsf{T}} \mathbf{\theta} \leq C$



Solving for θ_{reg}

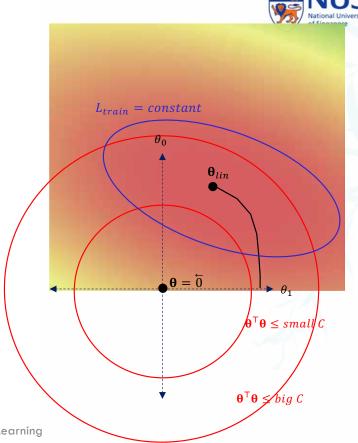
Minimize $L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \mathbf{\theta} - \mathbf{y})$ Subject to $\mathbf{\theta}^{\mathsf{T}} \mathbf{\theta} \leq \mathbf{C}$

Pictorially with 2 weights θ_0 , θ_1 :

 L_{train} gradient as heatmap.

Blue oval is a contour where L_{train} is a constant value (same color)

Red disc defines uniform weight decay region where $\theta^{\top}\theta \leq C$.



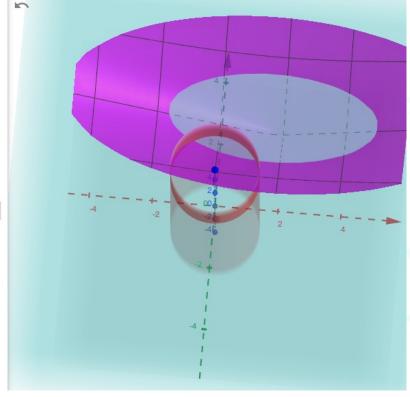
Ge@Gebra Calculator Suite

Input...

•	3D Calculator	_	
4	3D Calculator		

<		NU	JS
		National L	Inivers

0	Cone: $z = 0.2 \sqrt{(3 \times -5)^2 + (7 \text{ y} - 15)^2} + 2$:
0	11: $abs(abs(x) + abs(y)) = 2$:
0	12: $x^2 + y^2 = 2$:
	f: z = 4	:

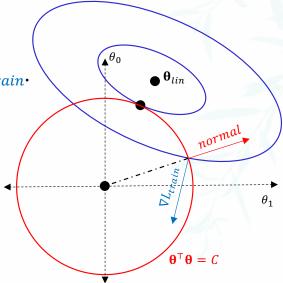


Solving for θ_{reg}



Observations:

- 1. Optimal θ tries to get as 'close' to θ_{lin} as possible Optimal θ will use full budget and be on the surface $\theta^{\top}\theta = C$.
- 2. Surface $\mathbf{\theta}^{\mathsf{T}}\mathbf{\theta} = \mathcal{C}$, at optimal $\mathbf{\theta}$, must be perpendicular to ∇L_{train} . Otherwise can move along the surface and decrease L_{train} .
- 3. Normal to surface $\theta^T \theta = C$ is the vector θ .
- 4. Surface is $\perp \nabla L_{train}$; surface is \perp normal. ∇L_{train} is parallel to normal (but in the opposite direction).



 $L_{train} = constant$

Solving for θ_{reg}

Minimize
$$L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\top} (\mathbf{X} \mathbf{\theta} - \mathbf{y})$$

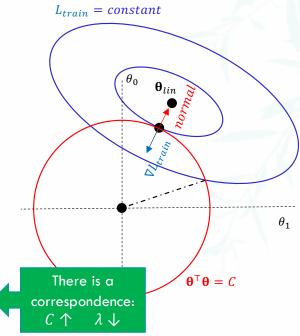
Subject to $\mathbf{\theta}^{\top} \mathbf{\theta} \leq C$

Observations:

- 1. Optimal $\boldsymbol{\theta}$ tries to get as 'close' to $\boldsymbol{\theta}_{lin}$ as possible Optimal $\boldsymbol{\theta}$ will use full budget and be on the surface $\boldsymbol{\theta}^{\top}\boldsymbol{\theta} = C$.
- 2. Surface $\mathbf{\theta}^{\top}\mathbf{\theta} = \mathcal{C}$, at optimal $\mathbf{\theta}$, should be perpendicular to VL_{train} .

 Otherwise can move along the surface and decrease L_{train} .
- 3. Normal to surface $\theta^T \theta = C$ is the vector θ .
- 4. Surface is $\perp \nabla L_{train}$; surface is \perp normal. ∇L_{train} is parallel to normal (but in the opposite direction).





NUS CS3244: Machine Learning

Comparison with Linear Regression



$\underline{\mathsf{Unconstrained}}$

$$\overline{\min L_{train}} = \frac{1}{m} \sum_{j=1}^{m} (\mathbf{\theta}^{\mathsf{T}} \mathbf{x}^{(j)} - y^{(j)})^{2}$$

$$\min L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \mathbf{\theta} - \mathbf{y})$$

Constrained:

min
$$L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \mathbf{\theta} - \mathbf{y})$$
, subject to: $\mathbf{\theta}^{\mathsf{T}} \mathbf{\theta} \leq C$

$$\boldsymbol{\theta}_{lin} = (\mathbf{X}^{\mathsf{T}}\mathbf{X})^{-1}\mathbf{X}\mathbf{y}$$

$$\mathbf{\theta}_{reg} = (\mathbf{X}^{\mathsf{T}}\mathbf{X} + \lambda \mathbf{I})^{-1}\mathbf{X}^{\mathsf{T}}\mathbf{y}$$

Augmented Error Laug



Unconstrained

$$\begin{aligned} &\min L_{train} = \frac{1}{m} \sum_{j=1}^{m} \left(\mathbf{\theta}^{\mathsf{T}} \mathbf{x}^{(j)} - y^{(j)} \right)^{2} \\ &\min L_{train} = \frac{1}{m} (\mathbf{X} \mathbf{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \mathbf{\theta} - \mathbf{y}) \end{aligned}$$

Constrained:

$$\begin{aligned} \overline{\min L_{train}} &= \frac{1}{m} (\mathbf{X} \boldsymbol{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \boldsymbol{\theta} - \mathbf{y}) \text{, subject to: } \boldsymbol{\theta}^{\mathsf{T}} \boldsymbol{\theta} \leq \mathbf{C} \\ & \qquad \qquad ||| \\ \min L_{aug}(\boldsymbol{\theta}) &= L_{train}(\boldsymbol{\theta}) + \frac{\lambda}{m} \boldsymbol{\theta}^{\mathsf{T}} \boldsymbol{\theta} \\ &= \frac{1}{m} \big((\mathbf{X} \boldsymbol{\theta} - \mathbf{y})^{\mathsf{T}} (\mathbf{X} \boldsymbol{\theta} - \mathbf{y}) + \lambda \boldsymbol{\theta}^{\mathsf{T}} \boldsymbol{\theta} \big) \end{aligned}$$

Take derivatives:

Set
$$\nabla L_{aug}(\theta) = \overleftarrow{\mathbf{0}} \Longrightarrow$$

= $\mathbf{X}^{\mathsf{T}}(\mathbf{X}\theta - \mathbf{y}) + \lambda \theta$
= $(\mathbf{X}^{\mathsf{T}}\mathbf{X} + \lambda \mathbf{I})\theta - \mathbf{X}^{\mathsf{T}}\mathbf{y}$

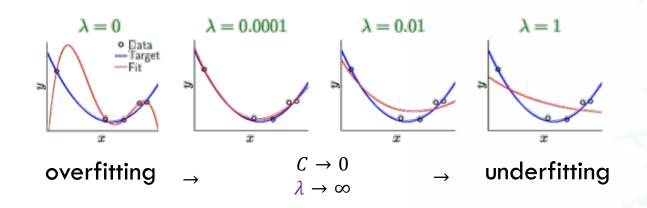
$$\mathbf{\theta}_{reg} = (\mathbf{X}^{\mathsf{T}}\mathbf{X} + \lambda \mathbf{I})^{-1}\mathbf{X}^{\mathsf{T}}\mathbf{y}$$

Still 1 step learning! λ determines the amount of regularization.

Take the right λ amount of medicine



Minimizing $[L_{train}(\mathbf{\theta}) + \frac{\lambda}{m} \mathbf{\theta}^{\mathsf{T}} \mathbf{\theta}]$ for different λ 's:



Q1: What happens to θ in the limit as $\lambda \to \infty$?

NUS CS3244: Machine Learning



Regularizer variations $\Omega(h)$

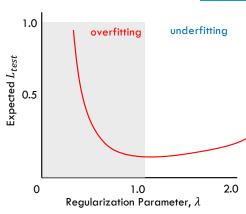


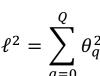
Uniform weight decay

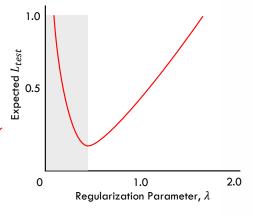
Why is it called "weight decay"? We'll see in neural networks.

Low Order Fit

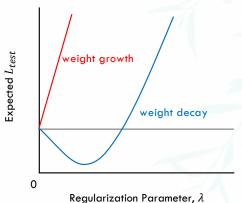








$$\sum_{q=0}^{Q} q\theta_q^2$$



 $\sum_{q=0}^{Q} \frac{1}{\theta_q^2}$

NUS CS3244: Machine Learning

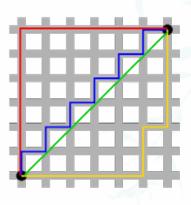
Geometry of ℓ^p norms



$$\left||\theta|\right|_p \equiv \left(\sum_{i=1}^n |\theta_i|^p\right)^{\frac{1}{p}}$$

$$\ell^1$$
 = Manhattan (Taxicab) distance $\sum_{i=1}^n |\theta_i|$

$$\ell^2$$
 = Euclidean distance (weight decay) $\sqrt[2]{\sum_{i=1}^{n} |\theta_i|^2}$



ℓ^p ball visualized



As the value of p decreases, the size of the corresponding space also decreases.

In 3 equally weighted dimensions (e.g., θ_1 , θ_2 , θ_3):



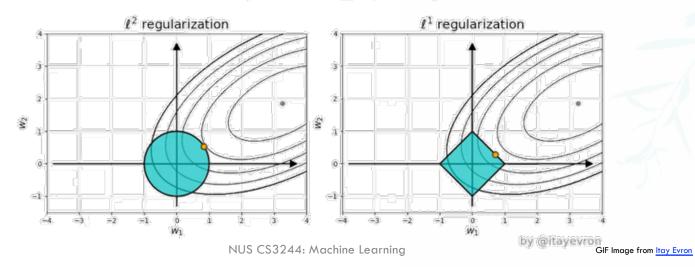
Properties from geometry



 ℓ^1 encourages sparse solutions; akin to feature selection.

 ℓ^2 can be used for homogenous data.

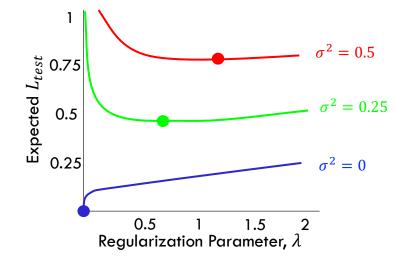
• induces sparse solutions for least squares

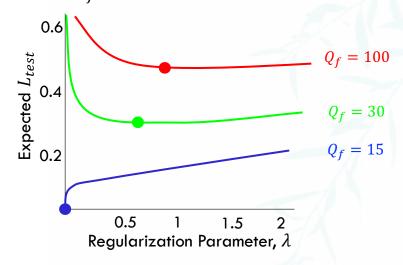


Getting the right dose



Recall the bias-variance experiment varying σ^2 (noise) and Q_f (target complexity) from last week:





Stochastic Noise

(also non-smooth w.r.t. to \mathcal{H})

Deterministic Noise (Bias)

(high frequency)

Regularization — Summary



Give up modeling a subset of of ${\mathcal H}$ to lower variance error.

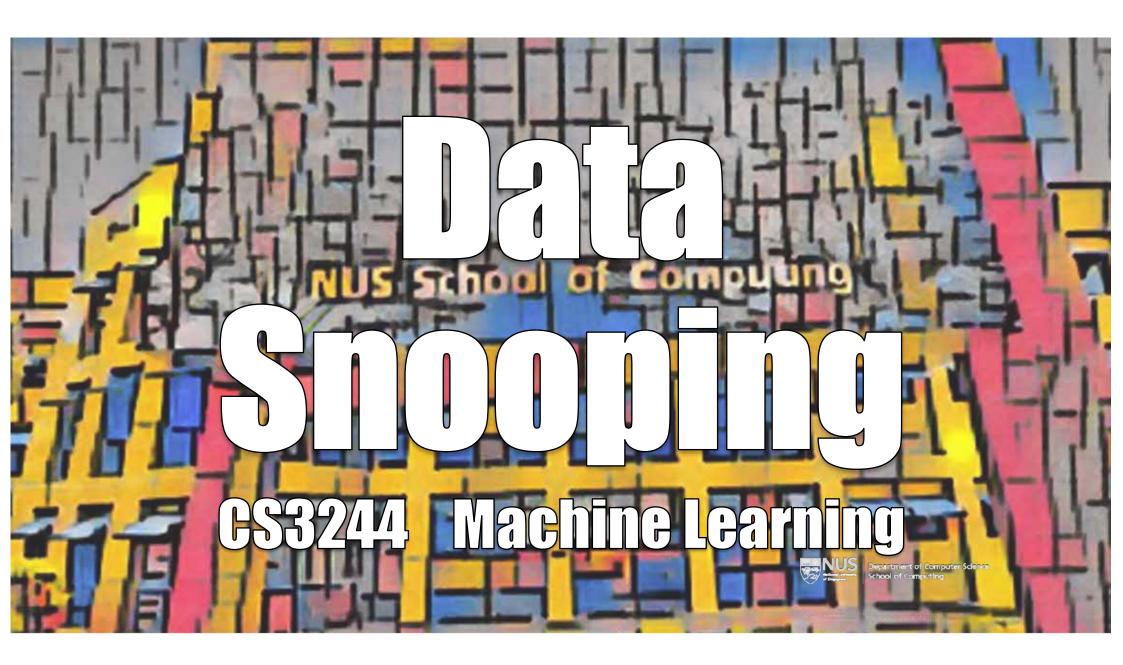
$$L_{aug}(\mathbf{\theta}) \equiv L_{train}(\mathbf{\theta}) + \frac{\lambda}{m} \Omega(h)$$

 λ is the dose of regularization: the higher the dose, the smaller the budget C.

Choosing a regularizer $\Omega(h)$:

Weight decay is common
$$\sum_{q=0}^Q \theta_q^2 \equiv \mathbf{\theta}^{\mathsf{T}} \mathbf{\theta}$$
 (ℓ^2 regularization)

Choose λ by validation ...



Data Snooping



Predict USD versus GBP

Normalize data, split randomly: X_{train}, X_{test}

Train only on \mathbf{X}_{train} , Test h_{θ} on \mathbf{X}_{test}

Got great performance! Let's invest!

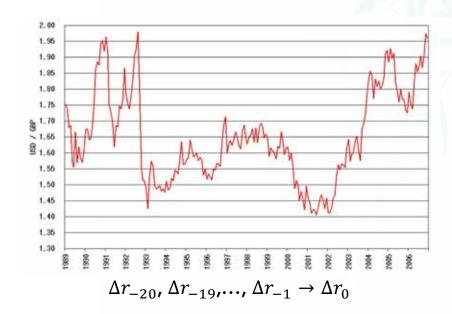


Chart credits: Monaneko @ Wikimedia Commons

Data Snooping



In Zoom breakout or physical subgroups,

(5 mins): Answer why we lost our money

Ask one member to write it to the #lectures thread. Upvote others that you like.

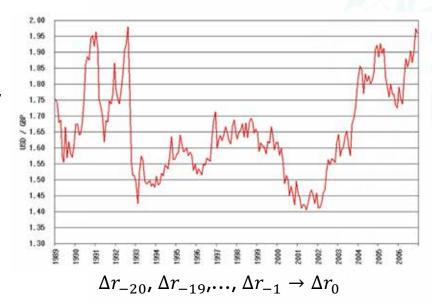


Chart credits: Monaneko @ Wikimedia Commons

NUS CS3244: Machine Learning

Data Snooping



Lost our \$\$\$. Why?



If a data set has affected any step in the learning process, its ability to assess the outcome has been compromised.



Most common trap for practitioners – many ways to slip.

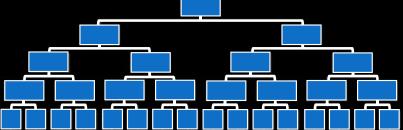
Chart credits: Monaneko @ Wikimedia Commons

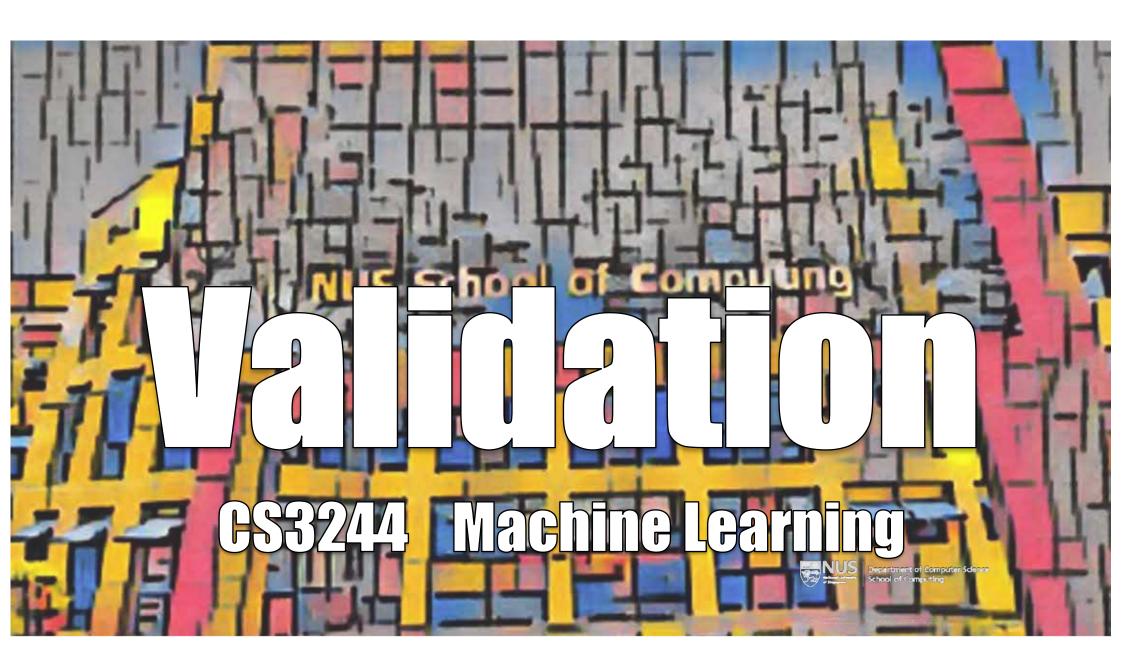
Perfect Forecasting — or luck of the draw?

There always is that political pundit, stock picker and other high-value forecaster that nails all of their predictions.

Is this person to be trusted?







Two Cures



In one form or another, $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

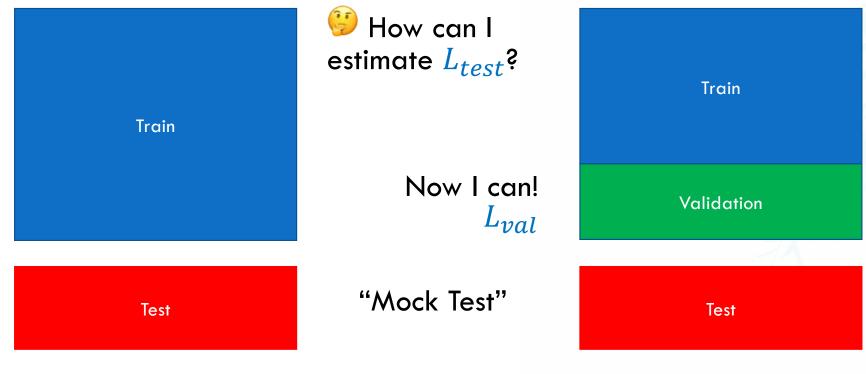
1. Regularization: Restrain the model $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

2. Validation: Reality check by peeking (at the bottom line) $L_{test}(h) = L_{train}(h) + \text{overfit penalty}$

Validation estimates this quantity

What is validation?





NUS CS3244: Machine Learning

37

Analyzing the estimated loss



On a test point (x, y), the cost $I(h_{\theta}(x), y)$ is:

Squared error:
$$(h_{\theta}(x) - y)^2$$

Binary error:

$$\left[\left[h_{\theta}(x)\neq y\right]\right]$$

$$\mathbb{E}[I(h_{\theta}(x), y)] = L_{test}(h_{\theta})$$

$$Var[I(h_{\theta}(x), y)] = \sigma^2$$

From a point to a set



On a validation set $(\mathbf{x}^{(1)}, y^{(1)}), \dots, (\mathbf{x}^{(K)}, y^{(K)}),$ the cost is $L_{val}(h) = \frac{1}{K} \sum_{k=1}^{K} l\left(h(\mathbf{x}^{(k)}), y^{(k)}\right)$

$$\mathbb{E}[L_{val}(h)] = \frac{1}{K} \sum_{k=1}^{K} \mathbb{E}[l(h(\mathbf{x}^{(k)}), y^{(k)})] = L_{test}(h)$$

$$Var[L_{val}(h)] = \frac{1}{K^2} \sum_{k=1}^{K} Var[l(h(\mathbf{x}^{(k)}), y^{(k)})] = \frac{\sigma^2}{K}$$



$$L_{val}(h) = L_{test}(h) \pm O\left(\frac{1}{\sqrt{K}}\right)$$



K is taken out of m



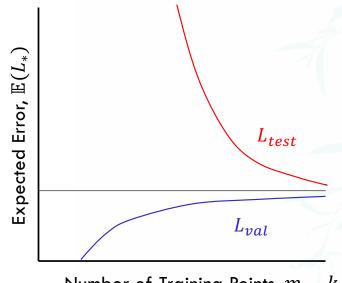
Given the data set \mathcal{D} , separate:

- 1. K points for validation
- 2. m-K points for training

$$O\left(\frac{1}{\sqrt{K}}\right)$$
:

Small K = bad estimate

Large
$$K = ?$$



Number of Training Points, m-k

K is put back into m



- 2. Test h^- on \mathcal{D}_{val} to yield L_{val}
- 3. Use cost L_{val} to estimate $L_{test}(h^-)$
- 4. Use h (not h^{-1}) in the end

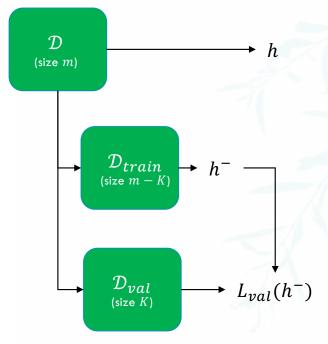
Large K?

 h^- trained on too few examples.

Leads to bad h^- , poor estimate.

Rule of Thumb:
$$K = \frac{m}{5}$$

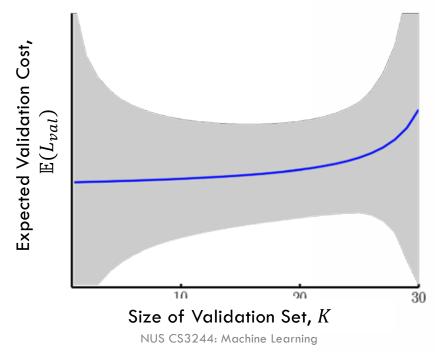


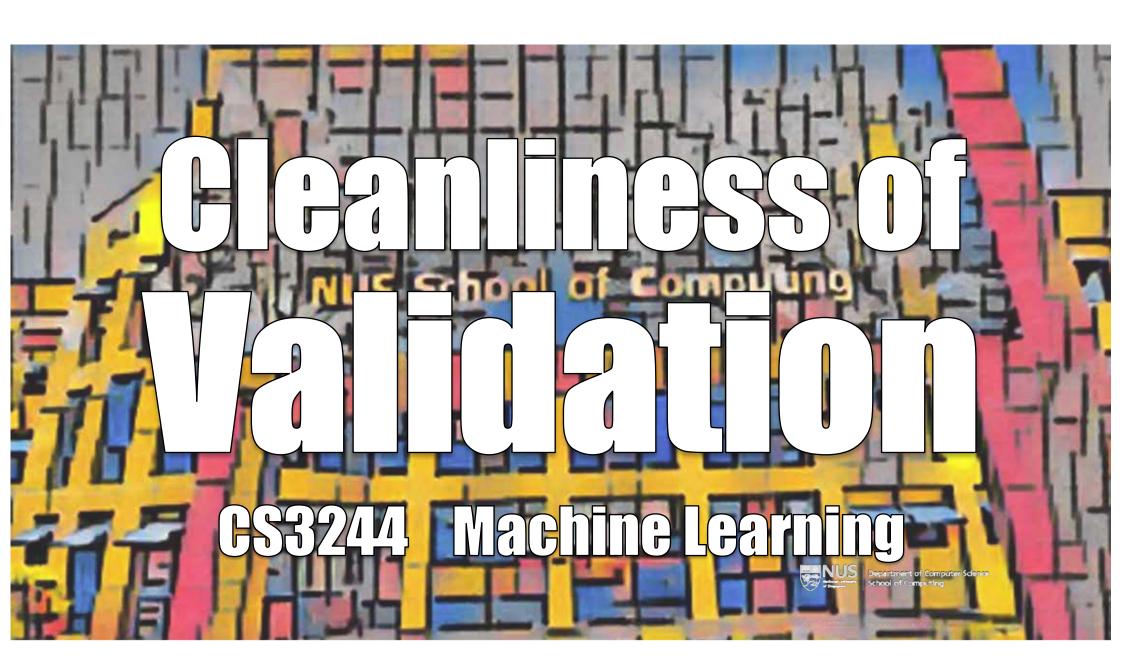


Expected Validation Error for \mathcal{H}_2



With m = 40, and noise level = 0.4

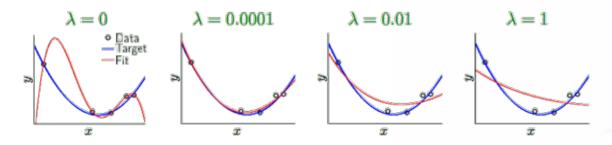




Why 'validation'?



Because \mathcal{D}_{val} is used to make learning choices, e.g. choosing the level of regularization to minimize L_{val}



If an estimate L_{test} affects learning:

The set is no longer a test set, it becomes a validation set!

What's the difference?



We know that the test set is unbiased. But what about the validation set?

Your Turn: Does the validation set have an optimistic or pessimistic bias?

Two hypotheses h_a and h_b with $L_{test}(h_a) = L_{test}(h_b) = 0.5$ Error estimates l_a and l_b uniform on [0,1] We pick $h \in \{h_a, h_b\}$ by virtue of its $l = \min(l_a, l_b)$.

What then, is the value of $\mathbb{E}(l)$?

Q4 leading to Q5 bias.

What's the difference?



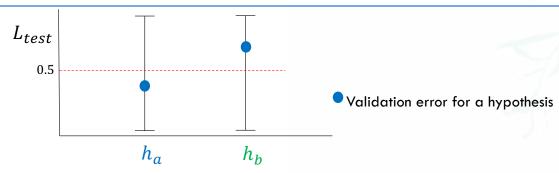
Two hypotheses h_a and h_b with $L_{test}(h_a) = L_{test}(h_b) = 0.5$

Error estimates l_a and l_b uniform on [0,1]

We pick $h \in \{h_a, h_b\}$ by virtue of its $l = \min(l_a, l_b)$.

What then, is the value of $\mathbb{E}(l)$?

 $\mathbb{E}(l) < 0.5$, leading to an optimistic bias.



NUS CS3244: Machine Learning

Hypothesis Selection: Using \mathcal{D}_{val} more than once



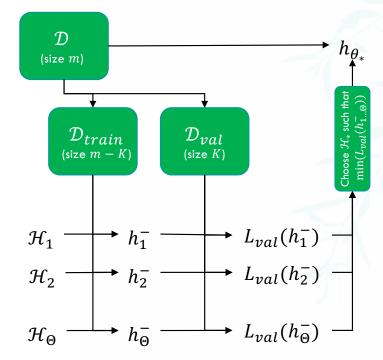
 Θ models \mathcal{H}_1 , ..., \mathcal{H}_{Θ}

Use \mathcal{D}_{train} to learn $h_{ heta}^-$ for each model

Evaluate
$$h_{\theta}^{-}$$
 using \mathcal{D}_{val} : $L_{\theta} = L_{val}(h_{\theta}^{-}); \ \theta = 1, \dots, \Theta$

Pick model $\theta = \theta_*$ with smallest L_{θ}





NUS CS3244: Machine Learning

Data contamination



Error estimates: L_{train} , L_{test} , L_{val}

Contamination: optimistic (deceptive) bias in estimating L_{test}

- Training set: totally contaminated
- Validation set: slightly contaminated
- Test set: totally 'clean'

Time Out: Check your understanding



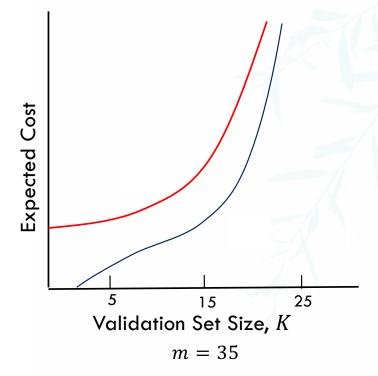
We selected the model \mathcal{H}_{θ^*} using \mathcal{D}_{val} . We can think of validation as training among the set of Θ models.

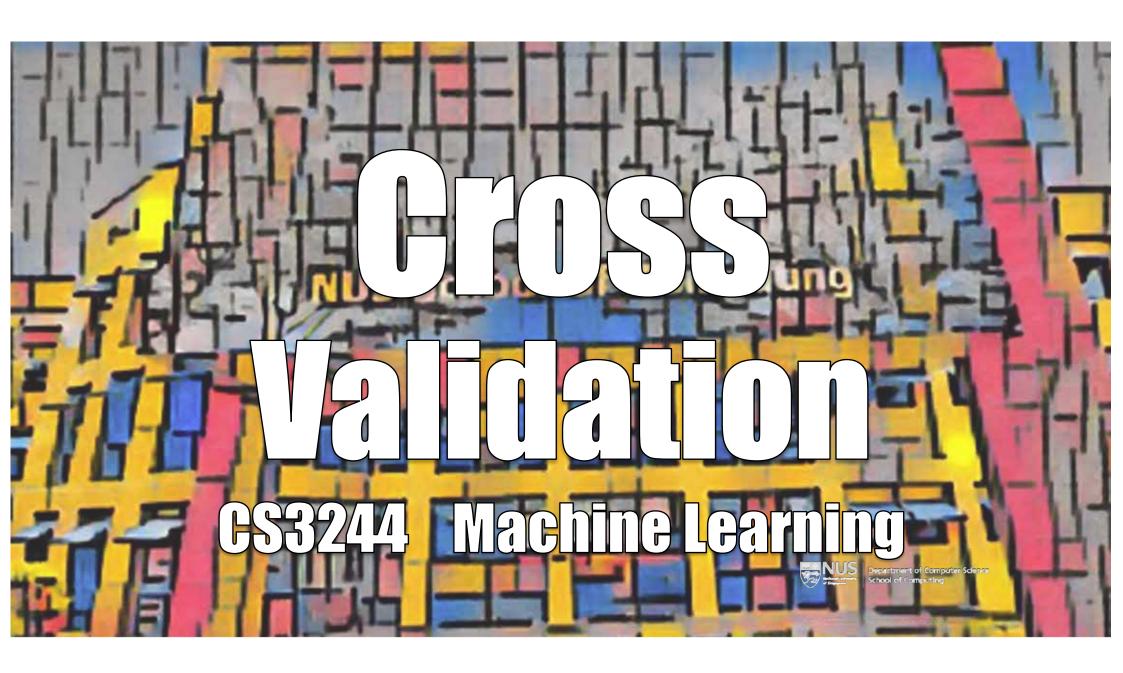
 $L_{val}(h_{ heta^*}^-)$ is a biased estimate of $L_{test}(h_{ heta^*}^-)$

Your Turn:

One curve is L_{val} , and the other L_{test}

- I. Which curve is L_{val} ? lacksquare or lacksquare
- 2. Why are the curves going up?
- 3. Why do the curves get closer together?

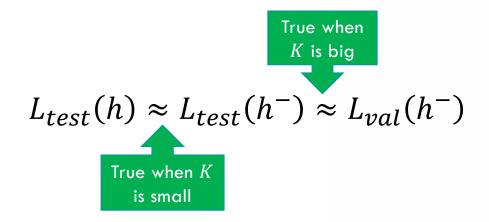




The dilemma about K



Validation relies on the following chain of reasoning:



Can we have both K being both big and small? Yes, we can!

Leave out out cross validation



m-1 points for training and 1 point for validation (Sounds familiar? It was at the beginning of the pre validation lecture)

$$\mathcal{D}_{cv} = \left(\mathbf{x}^{(1)}, y^{(1)}\right), \dots, \left(\mathbf{x}^{(cv)}, y^{(cv)}\right), \dots, \left(\mathbf{x}^{(m)}, y^{(m)}\right) \text{ validation}$$

Final hypothesis learned from \mathcal{D}_{cv} is h_{cv}^- .

$$l_{cv} = l_{val}(h_{cv}^{-}) = l(h_{cv}^{-}(\mathbf{x}^{(cv)}), y^{(cv)})$$

Caveat: Hypothesis learned will be highly correlated.

As most points are identical: The 1st hypothesis will use points 2, 3, ..., m and the 2nd will use 1, 3, ..., m.

Leave out out cross validation



Final hypothesis learned from \mathcal{D}_{cv} is h_{cv}^- .

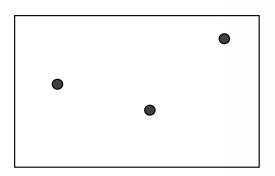
$$l_{cv} = l_{val}(h_{cv}^{-}) = l(h_{cv}^{-}(\mathbf{x}^{(cv)}), y^{(cv)})$$

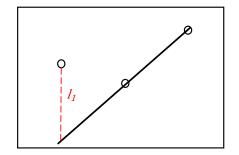
Cross validation cost: $L_{loocv} = \frac{1}{m} \sum_{cv=1}^{m} l_{cv}$.

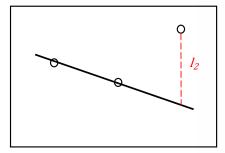
(Almost) using m examples for K.

Illustration of cross validation

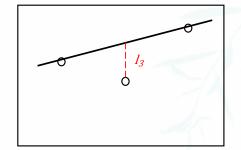








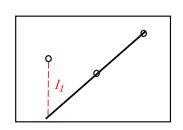
$$L_{loocv} = \frac{1}{3}(l_1 + l_2 + l_3)$$

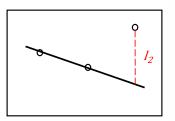


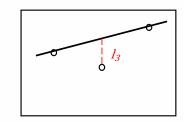
Model selection using CV



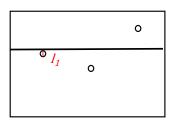
Linear

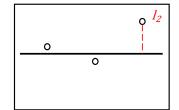


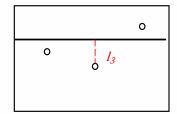




Constant



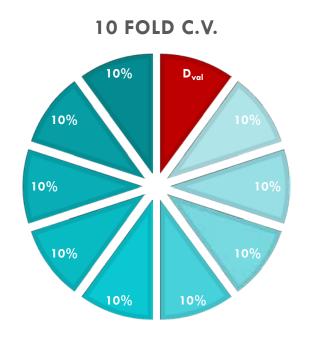




 L_{cv} empirically shows that the constant model is a better fit for this dataset

Have your cake and eat it too: K fold cross validation





LOOCV can be very expensive for large datasets. Why?

Instead, use K fold cross validation: i.e., K training sessions on $\frac{m}{K}$ points each.

Recommend: 10-fold CV

Assigned Task (due before next Mon)



Read the post https://www.kaggle.com/alexisbcook/cross-validation (10 mins)

Post a 1-2 sentence answer to the topic in your tutorial group: $\#tg-\underline{xx}$

How does cross validation relate to variance?

[There's an optional exercise with this course page, using random forest and MAE, you're welcomed to do it if you'd like]

Pre-Lecture Activity for next week



Cross-validation can help to reduce variance



Cross-validation helps improve the model to reduce variance with unseen data samples



Cross-validation is able to reduce variance as all the data points will get to be used as both the training and validation sets. As long as the sets are not too small, there will be less impact from noise.



Cross validation is a method to gauge the performance of a machine learning model. In the case of how cross variance affects the variance, the number of folds impacts how the variance and the bias of the model would vary. The lower the number of folds, the greater bias and lower the variance and the greater the number of folds, the greater the variance. This is because the more folds there are the smaller the sample size of the training data set, leading to a greater influence of random chances/data points on the model.



How does cross validation relate to variance?



If cross-validation were averaging independent estimates: LOOCV should see lower variance, since training sets overlap substantially.

This is not true when training sets are highly correlated: Then, LOOCV may be blind to instabilities that may not be triggered by changing a single point in the training data. This makes it highly variable to the realization of the training set, hence high variance.

A more definitive answer to the paraphrase is here:

https://stats.stackexchange.com/questions/61783/bias-and-variance-in-leave-one-out-vs-k-fold-cross-validation

Cross Validation – Summary

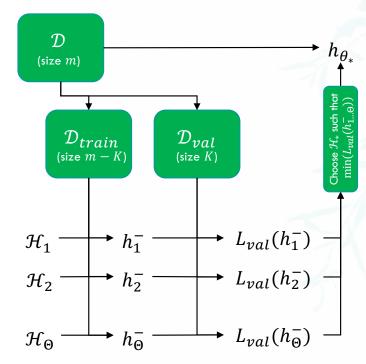


Estimate L_{val} multiple times

Breaks independence assumption: performance is correlated.

Introduces the factor of efficiency as a tradeoff.

To think about: How else can we produce estimates of L_{test} ?





What did we learn this week?



Understand Regularization as a means of restraining the model.

Choose appropriate doses of regularization for a model.

Understand and execute Validation, as a reality check by peeking (at the bottom line).

Understand the different forms extending validation to encompass additional estimation.

Understand how validation and regularization complement each other and their roles in affecting learning.

NUS CS3244: Machine Learning

—Sugar Ray Leonard

Photo by $\underline{\text{the blowup}}$ on $\underline{\text{Unsplash}}$

63

Assigned Task (due before next Mon)



Take a break, you deserve it!