## CS-GY 6923: Lecture 2 Multiple Linear Regression + Feature Transformations + Model Selection

NYU Tandon School of Engineering, Prof. Christopher Musco

- Lab 1 due Monday, by midnight.
- Lab 2 will be released today, due in 10 days.
- First written assignment will be released early next, due in 10 days.

10% bonus on the first written assignment if you typeset your solutions in Latex or Markdown. More information on course website.

## Training Dataset:

- Given input pairs  $(\mathbf{x}_1, y_1), \ldots, (\mathbf{x}_n, y_n)$ .
- Each  $\mathbf{x}_i$  is an input data vector (the predictor).
- Each y<sub>i</sub> is an output variable (the target).

## Objective:

• Have the computer automatically find some function  $f(\mathbf{x})$  such that  $f(\mathbf{x}_i)$  is close to  $y_i$  for the input data.

**Standard approach:** Convert the supervised learning problem to a multi-variable <u>optimization problem</u>.

# What are the three components needed to setup a supervised learning problem?

- Model  $f_{\theta}(x)$ : Class of equations or programs which map input x to predicted output. We want  $f_{\theta}(x_i) \approx y_i$  for training inputs.
- Model Parameters θ: Vector of numbers. These are numerical nobs which parameterize our class of models.
- Loss Function  $L(\theta)$ : Measure of how well a model fits our data. Typically some function of  $f_{\theta}(x_1) - y_1, \dots, f_{\theta}(x_n) - y_n$

Empirical Risk Minimization: Choose parameters  $\theta^*$  which minimize the Loss Function:

$$heta^* = rgmin_{ heta} L( heta)$$

#### SIMPLE LINEAR REGRESSION

#### Simple Linear Regression

- Model:  $f_{\beta_0,\beta_1}(x) = \beta_0 + \beta_1 \cdot x$
- Model Parameters:  $\beta_0, \beta_1$
- Loss Function:  $L(\beta_0, \beta_1) = \sum_{i=1}^{n} (y_i f_{\beta_0, \beta_1}(x_i))^2$

**Goal:** Choose  $\beta_0, \beta_1$  to minimize  $L(\beta_0, \beta_1) = \sum_{i=1}^{n} |y_i - \beta_0 - \beta_1 x_i|^2$ .

Simple closed form solution:  $\beta_1 = \sigma_{xy}/\sigma_x^2$ ,  $\beta_0 = \bar{y} - \beta_1 \bar{x}$ . How did we solve for this solution?

## Multiple Linear Regression Model:

Predict  $y_i \approx \beta_1 x_{i1} + \beta_2 x_{i2} + \ldots + \beta_d x_{id}$ 

#### Data matrix:

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1d} \\ x_{21} & x_{22} & \dots & x_{2d} \\ x_{31} & x_{32} & \dots & x_{3d} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nd} \end{bmatrix} = \begin{bmatrix} 1 & x_{12} & \dots & x_{1d} \\ 1 & x_{22} & \dots & x_{2d} \\ 1 & x_{32} & \dots & x_{3d} \\ \vdots & \vdots & & \vdots \\ 1 & x_{n2} & \dots & x_{nd} \end{bmatrix}$$

Linear algebraic form:

$$y_i \sim \langle \mathbf{x}, \boldsymbol{\beta} \rangle$$
  
 $\mathbf{y} \sim \mathbf{X} \boldsymbol{\beta}$ 

#### MULTIPLE LINEAR REGRESSION

## Linear Least-Squares Regression.

• Model Parameters:

$$\boldsymbol{\beta} = [\beta_1, \beta_2, \dots, \beta_d]$$

• Model:

$$f_{\boldsymbol{\beta}}(\mathbf{x}) = \langle \mathbf{x}, \boldsymbol{\beta} \rangle$$

• Loss Function:

$$L(\boldsymbol{\beta}) = \sum_{i=1}^{n} |\mathbf{y}_i - \langle \mathbf{x}_i, \boldsymbol{\beta} \rangle|^2$$
$$= \|\mathbf{y} - \mathbf{X}\boldsymbol{\beta}\|_2^2$$

**Goal:** minimize the loss function  $L(\beta) : \mathbb{R}^d \to \mathbb{R}$ .

Find possible optima by determining for which  $\beta = [\beta_1, \dots, \beta_d]$ all partial derivatives equal **0**. I.e., when do we have:

$$\nabla L(\boldsymbol{\beta}) = \begin{bmatrix} \frac{\partial L}{\partial \beta_1} \\ \frac{\partial L}{\partial \beta_2} \\ \vdots \\ \frac{\partial L}{\partial \beta_d} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{bmatrix}$$

The list of partial derivatives is called the **gradient** of *L* at  $\beta$ , denoted by  $\nabla L(\beta)$ .<sup>1</sup>

<sup>&</sup>lt;sup>1</sup>Sanity check: For a model with *d* parameters, gradient always has length *d*.

**Claim:** The gradient of the multivariate linear regression least squares loss function,  $L(\beta) = ||\mathbf{y} - \mathbf{X}\beta||_2^2$ , is:

$$\nabla L(\boldsymbol{\beta}) = -2 \cdot \mathbf{X}^{\mathsf{T}}(\mathbf{y} - \mathbf{X}\boldsymbol{\beta})$$

Can check that this is equal to 0 only when  $\beta = (X^T X)^{-1} X^T y$ . There are no other options, so this must be the minimum. What is the derivative of:  $f(x) = x^2$ ?

GRADIENT

## Loss function: $L(\beta) = \|\mathbf{y} - \mathbf{X}\beta\|_2^2$ .

GRADIENT

## Loss function: $L(\beta) = \|\mathbf{y} - \mathbf{X}\beta\|_2^2$ .

**Take away:** simple form for the gradient means that multiple linear regression models are easy and efficient to train.

$$\boldsymbol{\beta}^* = \arg\min_{\boldsymbol{\beta}} \|\mathbf{y} - \mathbf{X}\boldsymbol{\beta}\|_2^2 = \left(\mathbf{X}^{\mathsf{T}}\mathbf{X}\right)^{-1} \mathbf{X}^{\mathsf{T}}\mathbf{y}$$

Exactly how efficient?

$$eta^* = \operatorname*{arg\,min}_{oldsymbol{eta}} \|\mathbf{y} - \mathbf{X}oldsymbol{eta}\|_2^2 = \left(\mathbf{X}^{\mathsf{T}}\mathbf{X}
ight)^{-1}\mathbf{X}^{\mathsf{T}}\mathbf{y}$$

- β\* can be computed directly in O(nd<sup>2</sup>) time for an n × d data matrix X.
- There are iterative approximation methods (fancy versions of gradient descent) that run in roughly *O*(*nd*) time. We will use one called LSQR for Lab 2, since *d* is large.

**Take away:** simple form for the gradient means that multiple linear regression models are easy and efficient to train.

$$\boldsymbol{\beta}^* = \arg\min_{\boldsymbol{\beta}} \|\mathbf{y} - \mathbf{X}\boldsymbol{\beta}\|_2^2 = (\mathbf{X}^{\mathsf{T}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{T}}\mathbf{y}$$

- Often the "go to" first regression method. Throw your data in a matrix and see what happens.
- Serve as the basis for much richer classes of models.

:

It is not always immediately clear how to do this! One of the first issue we run into is categorical data:

 $\begin{aligned} & \textbf{x}_1 = [42, 4, 104, \textbf{hybrid}, \textbf{ford}] \\ & \textbf{x}_2 = [18, 8, 307, \textbf{gas}, \textbf{bmw}] \\ & \textbf{x}_2 = [31, 4, 150, \textbf{gas}, \textbf{honda}] \end{aligned}$ 

Binary data is easy to deal with – pick one category to be 0, one to be 1. The choice doesn't matter – it will not impact the overall loss of the model

> $x_1 = [42, 4, 104, hybrid, ford]$  $x_2 = [18, 8, 307, gas, bmw]$  $x_2 = [31, 4, 150, gas, honda]$  $x_1 = [42, 4, 104, 1, ford]$  $\mathbf{x}_2 = [18, 8, 307, 0, bmw]$  $x_2 = [31, 4, 150, 0, honda]$

What about a categorical predictor variable for car make with more than 2 options: e.g. Ford, BMW, Honda. **How would you encode as a numerical column?** 



#### ONE HOT ENCODING

#### Better approach: One Hot Encoding.

[ford]	$\rightarrow$	[1	0	0]
ford		1	0	0
honda		0	1	0
bmw		0	0	1
honda		0	1	0
ford		1	0	0

- Create a separate feature for every category, which is 1 when the variable is in that category, zero otherwise.
- Not too hard to do by hand, but you can also use library functions like sklearn.preprocessing.OneHotEncoder.

## Avoids adding inadvertent linear relationships.

## TRANSFORMED LINEAR MODELS

Instead of fitting the model mpg  $\approx \beta_0 + \beta_1 \cdot$  horsepower, fit the model mpg  $\approx \beta_0 + \beta_1 \cdot 1/$ horsepower.



#### How would you know to make such a transformation?

Better approach: Choose a more flexible <u>non-linear</u> model class. What is would be an example of a non-linear curve you could fit?

Suppose we have singular variate data examples (x, y). We could fit the <u>non-linear</u> polynomial model:

$$y \approx \beta_0 + \beta_1 x + \beta_2 x^2 + \beta_3 x^3.$$



**Claim:** This can be done using an algorithm for multivariate regression! No need to compute another gradient or write good to optimize  $\beta_0, \ldots, \beta_3$ .

Transform into a multiple linear regression problem:

$$\mathbf{X} = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & x_n^3 \end{bmatrix}$$

What is the output of the model  $X\beta$  with parameters  $\beta = [\beta_0, \dots, \beta_3]$ ?

More generally, each column *j* can be generated by a different basis function  $\phi_i(x)$ . Could have:

- $\phi_j(x) = x^q$
- $\phi_j(x) = \sin(x)$
- $\phi_j(x) = cos(10x)$
- $\phi_j(x) = 1/x$

When might you want to include sins and cosines?

When might you want to include sines and cosines?

Time series data:



#### Transformations can also be for multivariate data.

**Example:** Multivariate polynomial model.

- Given a dataset with <u>target y</u> and <u>predictors x, z</u>.
- For inputs  $(x_1, z_1), \ldots, (x_n, z_n)$  construct the data matrix:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & z_1 & z_1^2 & x_1z_1 \\ 1 & x_2 & x_2^2 & z_2 & z_2^2 & x_2z_2 \\ \vdots & \vdots & \vdots & & \\ 1 & x_n & x_n^2 & z_n & z_n^2 & x_nz_n \end{bmatrix}$$

• Captures non-linear interaction between x and z.

We use multivariate polynomials a lot in my work to fit models for physical phenomenon over low-dimensional surfaces:



Feature transformation is an extremely powerful tool that can improve models substantially. However, as will see in the remainder of the lecture, it must be used <u>with care</u>.

**Remainder of lecture:** Through a simple example, learn about the **overfitting problem** and how it can be addressed with model selection tools like the **test/train paradigm** and **cross-validation** 

We will post a Python demo working through this example.

## Simple experiment:

- Randomly select data points  $x_1, \ldots, x_n \in [-1, 1]$ .
- Choose a degree 3 polynomial p(x).
- Create some fake data: y<sub>i</sub> = p(x<sub>i</sub>) + η where η is a random number (e.g., random Gaussian).



#### FITTING A POLYNOMIAL

## Simple experiment:

• Use multiple linear regression to fit a line (degree 1 polynomial). This mode seems **underfit**.



#### FITTING A POLYNOMIAL

## Simple experiment:

• Use multiple linear regression to fit a degree 3 polynomial. Almost perfectly captures the true function!



#### What if we fit a higher degree polynomial?

- Fit degree 5 polynomial under squared loss.
- Fit degree 10 polynomial under squared loss.



#### FITTING A POLYNOMIAL

## Even higher?

• Fit degree 40 polynomial under squared loss. This model seems **overfit**.



The model "overreacts" to minor variations in the data, which can lead to some bad behavior.

In the demo we have you use numpy.polynomial.polynomial. However, as we discussed early, we can use multiple linear regression instead by constructing the data matrix:

$$\mathbf{X} = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^1 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & x_n^3 \end{bmatrix}$$

Then find polynomial coefficents as  $\beta = (X^T X)^{-1} X^T y$ .

#### QUICK ASIDE ON NUMERICAL ISSUES

```
# built in function
beta_hat = poly.polyfit(xdat,ydat,d)
# manual fit using naive multivariate regression
X = np.zeros([len(xdat),d+1])
for i in range(d+1):
X[:,i] = xdat**i
my_beta = np.linalg.inv(np.transpose(X)@X)@np.transpose(X)@ydat
```

3.0 Manual Fit Manual Fit 2.5 Built-in Fit Built-in Fit Data Data . 2.0 2.0 15 1.5 > 1.0  $\geq$ 10 0.5 0.5 0.0 0.0 -0.5 -0.5 -1.0 -1.0 -1.00 -0.75 -0.50 -0.25 -1.00 -0.75 -0.50 -0.25 0.00 0.25 0.50 0.75 1.00 0.00 0.25 0.50 0.75 1.00 x Degree 3 Degree 22

#### QUICK ASIDE ON NUMERICAL ISSUES

```
# built in function
beta_hat = poly.polyfit(xdat,ydat,d)
# manual fit using naive multivariate regression
X = np.zeros([len(xdat),d+1])
for i in range(d+1):
X[:,i] = xdat**i
my_beta = np.linalg.inv(np.transpose(X)@X)@np.transpose(X)@ydat
```



Has to due with <u>numerical roundoff error</u>. Scipy still uses linear regression, but with extra "tricks" to avoid numerical issues.
#### QUICK ASIDE ON NUMERICAL ISSUES

- Your computer can easily deal with both very large and very small numbers. Underflow and overflow are extremely unlikely to be issues in floating point arithmetic.
- The issue is when you compute using numbers of very differing magnitude.

```
print(.3*10**-34 + 10**-36 - 10**-36)
3e-35
print(.3*10**-34 + 10 - 10)
0.0
```

#### Recall that we chose each $x_i \in [-1, 1]$ uniformly at random.

$$\mathbf{X} = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^1 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & x_n^3 \end{bmatrix}$$

#### BACK TO THE PROBLEM AT HAND



Underfit, overfit, just right.

For high-dimensional data, we cannot produce such easy to read plots. How can we automatically detect when we have "underfit" or "overfit" to choose the right model?

#### MODEL COMPLEXITY VS. LOSS

Typically, the more **complex** our model, the better our loss:



For transformed linear models, this is <u>formally true</u>: more feature transformations leads to lower loss.

Consider  $X \in \mathbb{R}^{n \times d}$  and  $\overline{X} = [X, z] \in \mathbb{R}^{n \times d+1}$  with one additional column appended on.

Claim:

$$\min_{\bar{\boldsymbol{\beta}}\in\mathbb{R}^{d+1}}\|\bar{\boldsymbol{X}}\bar{\boldsymbol{\beta}}-\boldsymbol{y}\|_2^2\leq\min_{\boldsymbol{\beta}\in\mathbb{R}^d}\|\boldsymbol{X}\boldsymbol{\beta}-\boldsymbol{y}\|_2^2.$$

The more **complex** our model class the better our loss:



So <u>training loss</u> alone is not usually a good metric for model selection.

**Problem:** Small loss does not imply <u>generalization</u>. **Generalization:** How well do we do on <u>new</u> data.



#### Solution: Directly test model on "new data".



- Train loss decreases as model complexity grows.
- **Test loss** "turns around" once our model gets too complex. Minimized around degree 3 – 4.

**More reasonable approach:** Evaluate model on fresh <u>test data</u> which was not used during training.

#### Test/train split:

- Given data set (X, y), split into two sets (X<sub>train</sub>, y<sub>train</sub>) and (X<sub>test</sub>, y<sub>test</sub>).
- Train q models  $f^{(1)}, \ldots, f^{(q)}$  of varying complexity by finding parameters which minimize the loss on  $(X_{train}, y_{train})$ .
- $\cdot$  Evaluate loss of each trained model on  $(X_{\text{test}}, y_{\text{test}}).$
- Pick model with lowest test loss.

Sometimes you will see the term validation set instead of test set. Sometimes there will be both: use validation set for choosing the model, and test set for getting a final performance measure.

#### THE FUNDAMENTAL CURVE OF ML

The above trend is fairly representative of what we tend to see across the board:



### If the test loss remains low, we say that the model **generalizes**. Test lost is often called **generalization error**.

# **Typical train-test split:** 90-70% / 10-30%. Trade-off between between optimization of model parameters and better estimate of model performance.

#### **K-FOLD CROSS VALIDATION**



- Randomly divide data in K parts.
  - Typical choice: K = 5 or K = 10.
- Use K − 1 parts for training, 1 for test.
- For each model, compute test loss *L*<sub>ts</sub> for each "fold".
- Choose model with best average loss.
- · Retrain best model on entire dataset.

#### Is there any disadvantage to choosing *K* larger?

### Is "test error" the end goal though? Don't we care about "future" error?

**Intuition:** Models which perform better on the test set will **generalize** better to future data.

**Goal:** Introduce a little bit of formalism to better understand what this means. What is "future" data?

#### Statistical Learning Model:

- Assume each data example is randomly drawn from some distribution (x, y) ~ D.
- E.g.  $x_1, \ldots, x_d$  are Gaussian random variables with parameters  $\mu_1, \sigma_1, \ldots, \mu_d, \sigma_d$ .



This is not really a simplifying assumption! The distribution could be arbitrarily complicated.

#### Statistical Learning Model:

- Assume each data example is randomly drawn from some distribution (x, y) ~ D.
- Define the **Risk** of a model/parameters:

$$R(f, \boldsymbol{\theta}) = \mathbb{E}_{(\mathbf{x}, y) \sim \mathcal{D}} \left[ L \left( f(\mathbf{x}, \boldsymbol{\theta}), y \right) \right]$$

here L is our loss function (e.g. L(z, y) = |z - y| or  $L(z, y) = (z - y)^2$ ).

**Ultimate Goal:** Find model  $f \in \{f^{(1)}, \ldots, f^{(q)}\}$  and parameter vector  $\boldsymbol{\theta}$  to minimize the  $R(f, \boldsymbol{\theta})$ .

 $\cdot$  (Population) Risk:

$$R(f, \theta) = \mathbb{E}_{(\mathbf{x}, y) \sim \mathcal{D}} [L(f(\mathbf{x}, \theta), y)]$$

• Empirical Risk: Draw  $(x_1, y_1), \dots, (x_n, y_n) \sim \mathcal{D}$ 

$$R_E(f,\boldsymbol{\theta}) = \frac{1}{n} \sum_{i=1}^n L(f(\mathbf{x},\boldsymbol{\theta}), y)$$

#### For any fixed model f and parameters $\theta$ ,

 $\mathbb{E}\left[R_{E}(f,\boldsymbol{\theta})\right]=R(f,\boldsymbol{\theta}).$ 

Only true if f and  $\theta$  are chosen without looking at the data used to compute the empirical risk.

- Train q models  $(f^{(1)}, \boldsymbol{\theta}_1^*), \ldots, (f^{(q)}, \boldsymbol{\theta}_q^*).$
- For each model, compute empirical risk  $R_E(f^{(i)}, \theta_i^*)$  using test data.
- Since we assume our original dataset was drawn independently from  $\mathcal{D}$ , so is the random test subset.

No matter how our models were trained or how complex they are,  $R_E(f^{(i)}, \theta_i^*)$  is an <u>unbiased estimate</u> of the true risk  $R(f^{(i)}, \theta_i^*)$  for every *i*. Can use it to distinguish between models.

#### bag-of-words models and n-grams

Common way to represent documents (emails, webpages, books) as numerical data. The ultimate example of 1-hot encoding.



bag-of-words

#### bag-of-words models and n-grams

Common way to represent documents (emails, webpages, books) as numerical data. The ultimate example of 1-hot encoding.



bi-grams

#### bag-of-words models and n-grams

Common way to represent documents (emails, webpages, books) as numerical data. The ultimate example of 1-hot encoding.



tri-grams

Models of increasing order:

- Model  $f_{\theta_1}^{(1)}$ : spam filter that looks at single words.
- Model  $f_{\theta_2}^{(2)}$ : spam filter that looks at **bi-grams**.
- Model  $f_{\theta_3}^{(3)}$ : spam filter that looks at **tri-grams**.

• . . .

"interest" "low interest" "low interest loan"

Increased length of **n-gram** means more expressive power.

### Will be very relevant in our lab on generative language models!

#### Electrocorticography ECoG (next lab):

• Implant grid of electrodes on surface of the brain to measure electrical activity in different regions.



- Predict hand motion based on ECoG measurements.
- Model order: predict movement at time t using brain signals at time t, t 1, ..., t q for varying values of q.

Our lab uses data collected from monkeys. Precursor to technologies like Braingate, Neuralink, etc.



Paralellized or impaired person could control computer curser, robotic arm, etc. simply by thinking about it.

Small implant reads brainwaves and recognizes their intent.

Predicting time t based on a linear function of the signals at time t, t - 1, ..., t - q is <u>not the same</u> as fitting a line to the time series. It's much more expressive.



#### Electrocorticography ECoG lab:



### First lab where computation actually matters (solving regression problems with $\sim 40k$ examples, $\sim 1500$ features)

Makes sense to test and debug code using a subset of the data.

Slight caveat: The train-test paradigm is typically not how machine learning or scientific discovery works in practice!

#### Typical workflow:

- Train a class of models.
- Test.
- Adjust class of models.
- Test.
- Adjust class of models.
- Cont...

Final model implicitly depends on test set because performance on the test set guided how we changed our model.

#### ADAPTIVE DATA ANALYSIS

### Popularity of ML benchmarks and competitions leads to adaptivity at a massive scale.

11 Active Competitions		
#DFDC	Deepfake Detection Challenge Identify videos with facial or videa manpulations Featured - Code Competition - 2 months to go - ♦ video data, online video	\$1,000,000 1,595 teams
6	Google QUEST Q&A Labeling           Improving automated understanding of complex question answer content           Featured         - Code Competition - 19 hours to go - % text data, nb	\$25,000 1,559 teams
	Real or Not? NLP with Disaster Tweets Predict which Tweets are about real disasters and which ones are not Cetting Started - Ongoing - % text data, binary classification	\$10,000 2,657 teams
B	Bengali.AI Handwritten Grapheme Classification Classify the components of handwritten Bengali Research - Code Competition - a month to go - 🏘 multiclass classification, image data	\$10,000 1,194 teams

#### Kaggle (various competitions)



14,197,122 images, 21841 synsets indexed

Explore Download Challenges Publications Updates About

Not logged in. Login I Signup

Imagenet (image classification and categorization)

#### Is adaptivity a problem? Does it lead to over-fitting? How much? How can we prevent it? All current research. Related to the problem of "p-value hacking" in science.

REPORT

### The reusable holdout: Preserving validity in adaptive data analysis

Cynthia Dwork<sup>1,\*</sup>, Vitaly Feldman<sup>2,\*</sup>, Moritz Hardt<sup>3,\*</sup>, Toniann Pitassi<sup>4,\*</sup>, Omer Reingold<sup>5,\*</sup>, Aaron Roth<sup>6,\*</sup>

+ See all authors and affiliations

Science 07 Aug 2015: Vol. 349, Issue 6248, pp. 636-638 DOI: 10.1126/science.aaa9375

Do ImageNet Classifiers Generalize to ImageNet?

Benjamin Recht\* Rebecca Roelofs Ludwig Schmidt Vaishaal Shankar UC Berkeley UC Berkeley UC Berkeley UC Berkeley

#### Abstract

12 Jun 2019

We build new test sets for the CIPAR-10 and ImageNet datasets. Both benchmarks have been the focus of inteme research for almost a decade, raising the danger of overfitting to excessively re-used test sets. By closely following the original dataset creation processes, we test to what extent current classification models generalize to new data. We evaluate a broad range of models and find accuracy drops of 3% - 15% on CIFAR-10 and 11% - 14% on ImageNet. However, accuracy gains on the original test sets translate to larger gains on the new test sets. Our results suggest that the accuracy drops are not caused by adaptivity, but by the models' inability to generalize to slightly "harder" images than those found in the original test sets.



## Collected by Fei-Fei Li's group at Stanford in 2006ish and labeled using Amazon Mechanical Turk.



We now have neural network models that can solve these classification problems with > 95% accuracy.

#### ADAPTIVE DATA ANALYSIS

#### Do ImageNet Classifiers Generalized to ImageNet?



Interestingly, when comparing popular vision models on "fresh" data, while performance dropped across the board, the relative rank of model performance did not change significantly.