CSCI 567: Machine Learning

Vatsal Sharan Spring 2024

Lecture 1, Jan 12



Logistics

Course website: https://vatsalsharan.github.io/spring24.html

Logistics, slides, homework etc.

Ed Discussion: https://edstem.org/

Main forum for communication

DEN: https://courses.uscden.net/d2l/home/27576

Recordings

Gradescope: https://www.gradescope.com/

Homework submission

Prerequisites

This is a mathematically advanced and intensive class (that makes it more interesting!)

- (1) Undergraduate level training or coursework on linear algebra, (multivariate) calculus, and probability and statistics;
- (2) Programming with Python;
- (3) Undergraduate level training in the analysis of algorithms (e.g. runtime analysis).

Overview of logistics, go through course website for details:

Homeworks: 4 homeworks (groups of 2), 2 late days per student (max 1 per HW)

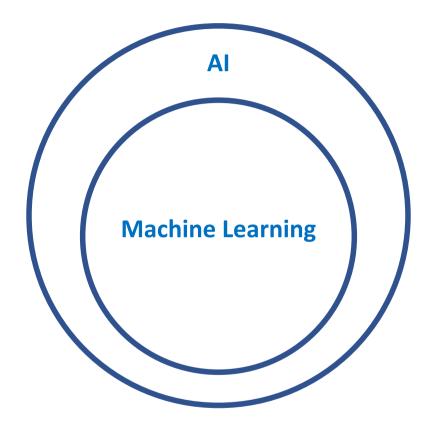
Exams: 3/1 and 4/26 during lecture hours (1pm-3:20pm)

Project: You can choose your topic, groups of 4, more details later

Note: Plagiarism and other unacceptable violations

- Neither ethical nor in your self-interest
- Zero-tolerance
- Read collaboration policy on course website





ML has been driving the recent advances in Al

What is ML?

"Humans appear to be able to learn new concepts without needing to be programmed explicitly in any conventional sense. In this paper we regard **learning as the phenomenon of knowledge acquisition in the absence of explicit programming**."

--- A Theory of the Learnable, 1984, Leslie Valiant



What is ML?

"Humans appear to be able to learn new concepts without needing to be programmed explicitly in any conventional sense. In this paper we regard **learning as the phenomenon of knowledge acquisition in the absence of explicit programming**."

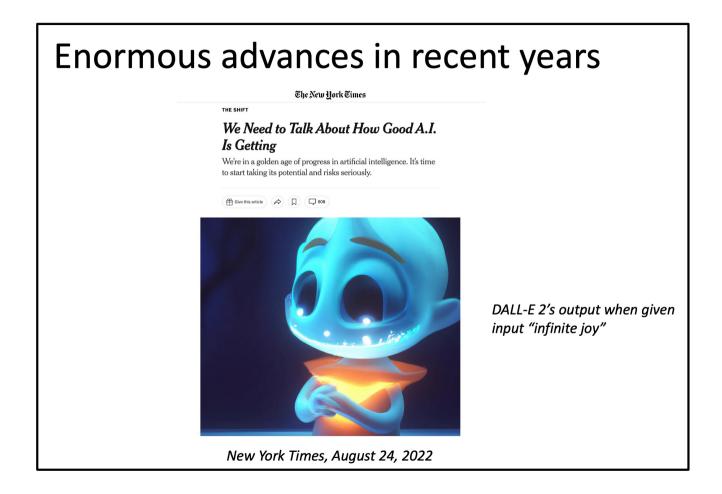
--- A Theory of the Learnable, 1984, Leslie Valiant

"A computer program is said to **learn** from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E."

--- Machine Learning, 1998, Tom Mitchell







Text generation: GPT-3

The New York Times

Meet GPT-3. It Has Learned to Code (and Blog and Argue).

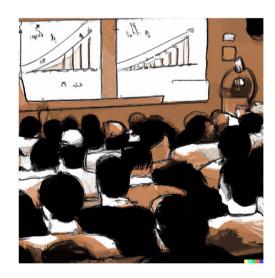
The latest natural-language system generates tweets, pens poetry, summarizes emails, answers trivia questions, translates languages and even writes its own computer programs.



Image generation: Dall-E 2

I gave the prompt:

A digital art image of a lecture on statistical machine learning. 200 students are sitting in a classroom, hearing about linear regression.



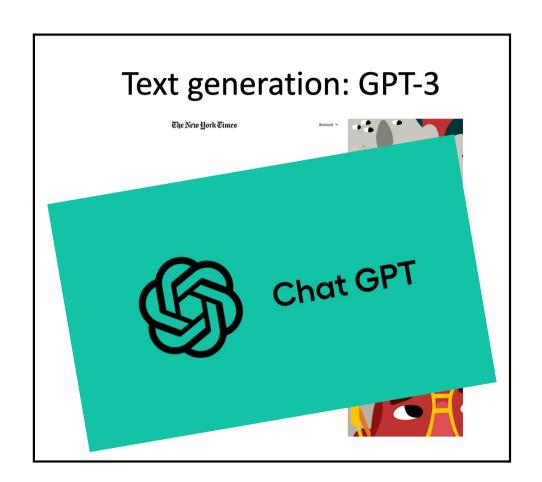
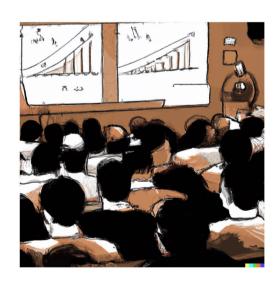
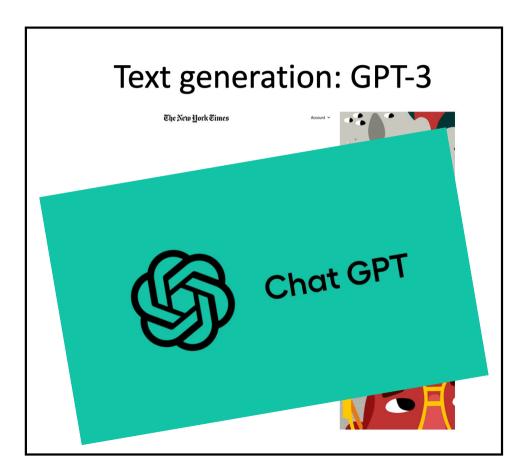


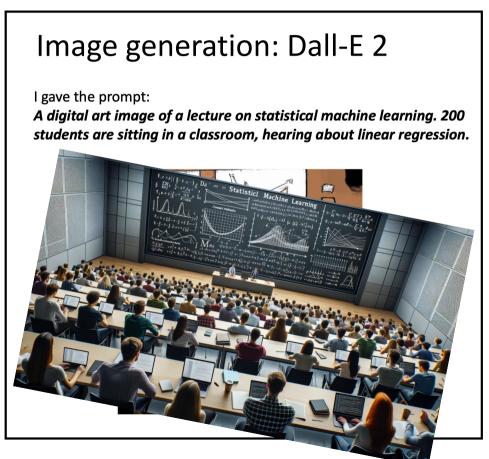
Image generation: Dall-E 2

I gave the prompt:

A digital art image of a lecture on statistical machine learning. 200 students are sitting in a classroom, hearing about linear regression.







What do you think are the most

important advances?

Some other flashy highlights...

Game playing: AlphaGo



Protein folding: AlphaFold

DeepMind's protein-folding Al cracks biology's biggest problem

Artificial intelligence firm DeepMind has transformed biology by predicting the structure of nearly all proteins known to science in just 18 months, a breakthrough that will speed drug development and revolutionise basic science











TECHNOLOGY 28 July 2022

By Matthew Sparkes



Exciting time, but a lot needs to be done..

- Require significant computational resources
- Lack of understanding
- Fairness
- Robustness
- Interpretability
- Privacy
- Alignment
- **...**

This class:

- Understand the fundamentals
- Understand when ML works, its limitations, think critically

This class:

- Understand the fundamentals
- Understand when ML works, its limitations, think critically

In particular,

- Study fundamental statistical ML methods (supervised learning, unsupervised learning, etc.)
- Solidify your knowledge with hands-on programming tasks
- Prepare you for studying advanced machine learning techniques

A simplistic taxonomy of ML

Supervised learning:

Aim to predict outputs of future datapoints

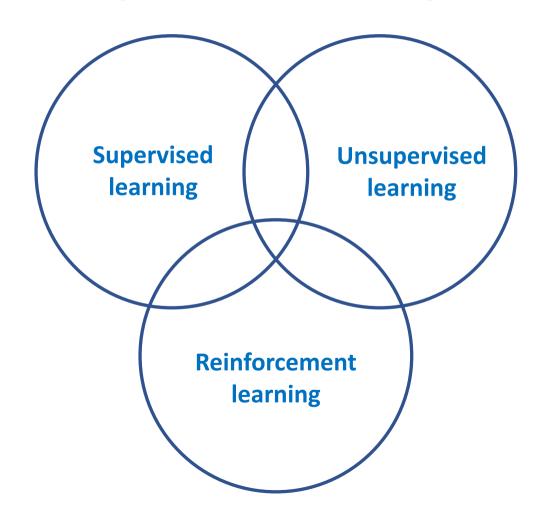
Unsupervised learning:

Aim to discover hidden patterns and explore data

Reinforcement learning:

Aim to make sequential decisions

A simplistic taxonomy of ML



Supervised Machine Learning

Supervised ML: Predict future outcomes using past outcomes

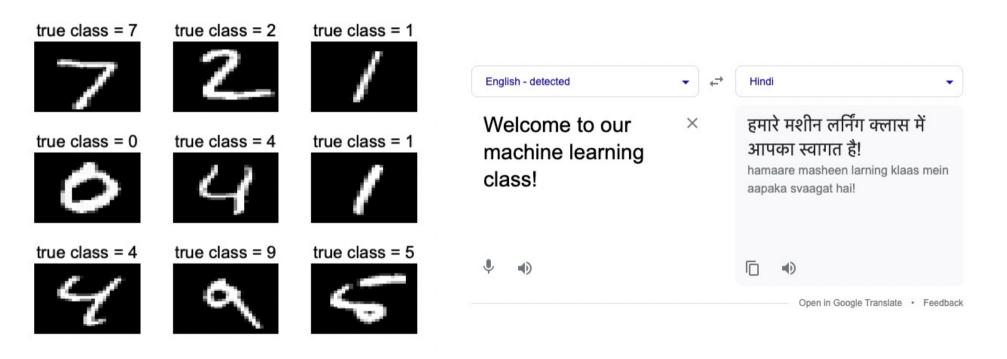
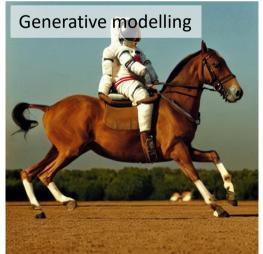


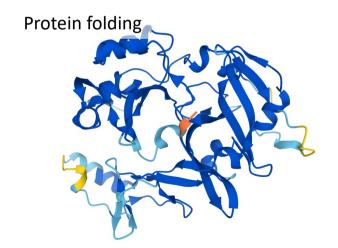
Image classification

Machine translation





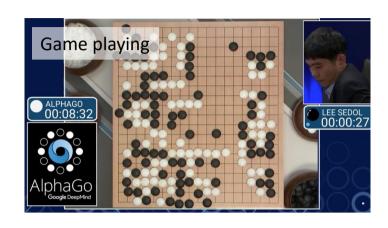


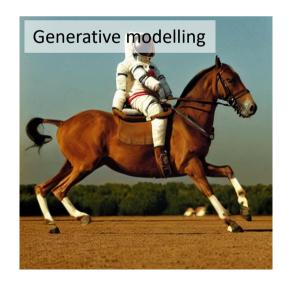


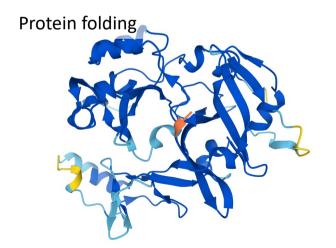


Language modelling

Given previous words -> Predict next word







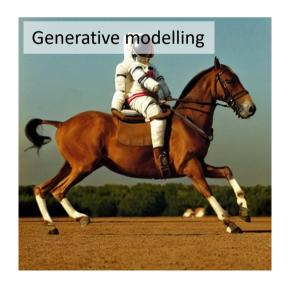


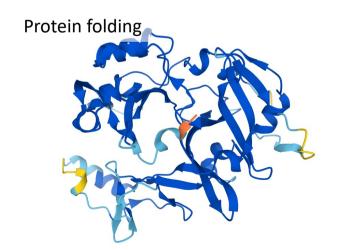
Language modelling

Given previous words -> Predict next word

Game playing

Given current board state -> Predict probability of winning







Language modelling

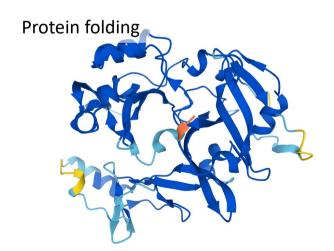
Given previous words -> Predict next word

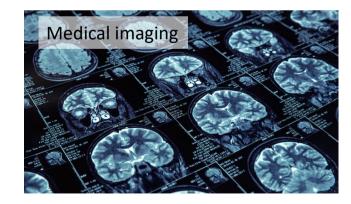
Game playing

Given current board state -> Predict probability of winning

Generative modelling

Given noisy image -> Predict denoised image





Language modelling

Given previous words -> Predict next word

Game playing

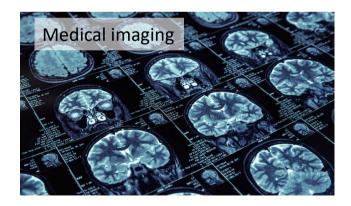
Given current board state -> Predict probability of winning

Generative modelling

Given noisy image -> Predict denoised image

Protein folding

Given protein chain -> Predict 3D structure



Language modelling

Given previous words -> Predict next word

Game playing

Given current board state -> Predict probability of winning

Generative modelling

Given noisy image -> Predict denoised image

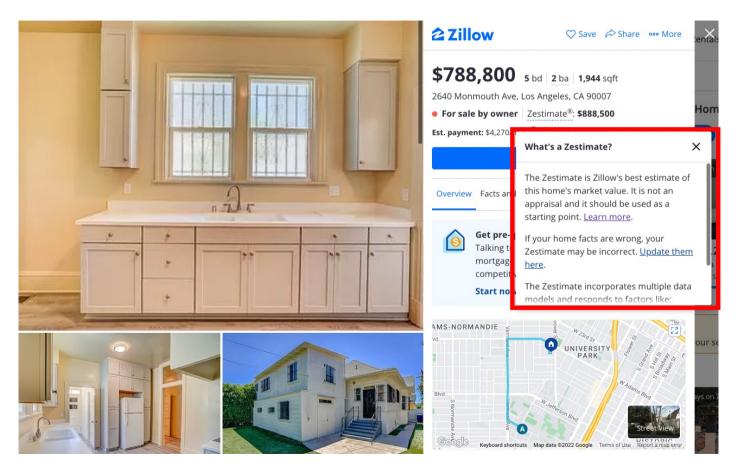
Protein folding

Given protein chain -> Predict 3D structure

Medical imaging

Given image -> Predict if there is tumor etc.

Supervised ML: Predict future outcomes using past outcomes

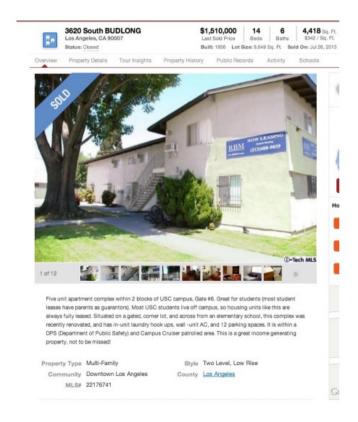


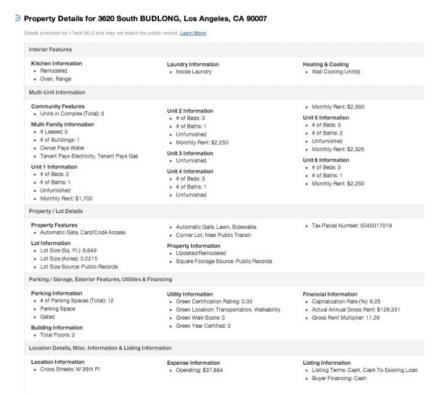
Predicting sale price of a house

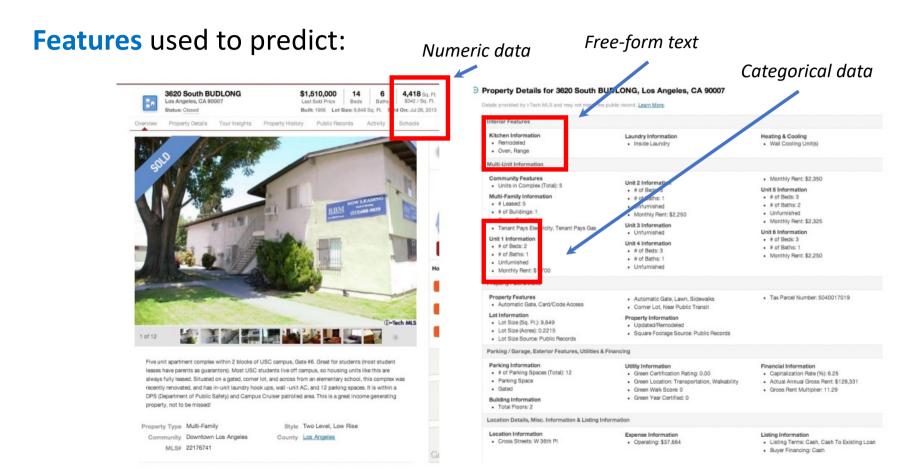
Retrieve historical sales records (training data):



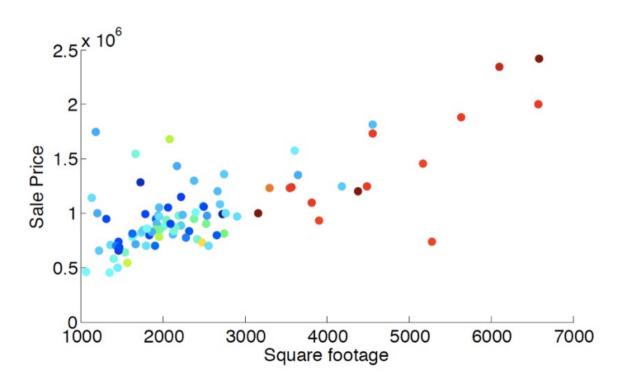
Features used to predict:







Correlation between square footage and sale price:



Possibly linear relationship:

Sale price ≈ price per sqft × square footage + fixed expense

(intercept) (slope) 2.5 × 10⁶ Sale Price 1.5 1000 2000 3000 5000 6000 4000 7000 Square footage

General framework for supervised learning

→ An input space : X ⊆ IR d Feature * Datapoints in 2 dimensions | engineering! * In prievious example, d=1 -> An output space ; >> * JEIR for sale price prediction God: Learn a predictor (2): X > Y which predicts output of x

Loss function:
$$l(f(x), y)$$

e.g. squared loss for $Y = IR$: $l(f(x), y) = (f(x), y)^2$

what to minimize over?

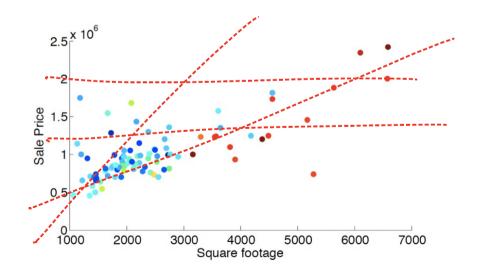
Det: Given a set of labelled data points

 $S = \{(+1, y), (+2, y), \dots, (+n, y)\}, \text{ the empirical rusk for predictor } f: X \Rightarrow Y \text{ wat set } S \text{ is } R_S(f) = \frac{L}{n} \stackrel{R}{\geq} l(f(x), y)$

Function class

Def: A function class (or hypothesis class) is a collection of functions $f: X \to Y$.

- Each of these is a linear function.
- The class of all linear functions is a function class.



Empirical risk minimizer (ERM)

Def: Given a function class $f = \{ f: \chi \rightarrow \gamma \}$, empirical risk minimization over a set of labelled datapoints 5 corresponds to: min $R_s(f) = \frac{1}{n} \sum_{i=1}^{n} l(f(x_i), y_i)$ Opt imization

Generalization

* We want predictor to generalize on unseen points.

Def. (Test error): The test error of a predictor f is the average loss on a "new "set s' of m points $s' = \{(x_i', y_i'), i \in m\}$ $\frac{1}{m} \sum_{i=1}^{\infty} \ell(f(x_i), y_i')$

Training Test paradigm: Assume training set S le test set s' are drawn From same distribution.

Measuring generalization: Training/Test paradigm

Randomly divide data into Training set: Subset of data to train model Test set: subset used to test model heneralization gap: Difference the test & training set errors

Generalization: More formally

Minimize loss over distribution of instances Definition: Risk of predictory f $R(f) = \mathbb{E}_{(x,y) \sim D} \left[l(f(x), y) \right]$ $= \frac{1}{x',y'} | nob_D (x = x',y = y') l(f(x'),y')$

tautology:

$$R(f) = \hat{R}_{s}(f) + (R(f) - \hat{R}_{s}(f))$$

To minimize R(F)

To minimize R(F)

To minimize Rs(f)

→ What's left is R(F)- Rs(F). This is the generalization gap.

Loss function: What is the right loss function for the task?

Depends on the problem that one is trying to solve, and on the rest...

Loss function: What is the right loss function for the task?

Representation: What class of functions should we use?

Also known as the "inductive bias".

No-free lunch theorem from learning theory tells us that

no model can do well on every task

"All models are wrong, but some are useful", George Box

Loss function: What is the right loss function for the task?

Representation: What class of functions should we use?

Optimization: How can we efficiently solve the empirical risk minimization problem?

Depends on all the above and also...

Loss function: What is the right loss function for the task?

Representation: What class of functions should we use?

Optimization: How can we efficiently solve the empirical risk minimization problem?

Generalization: Will the predictions of our model transfer gracefully to unseen examples?

Loss function: What is the right loss function for the task?

Representation: What class of functions should we use?

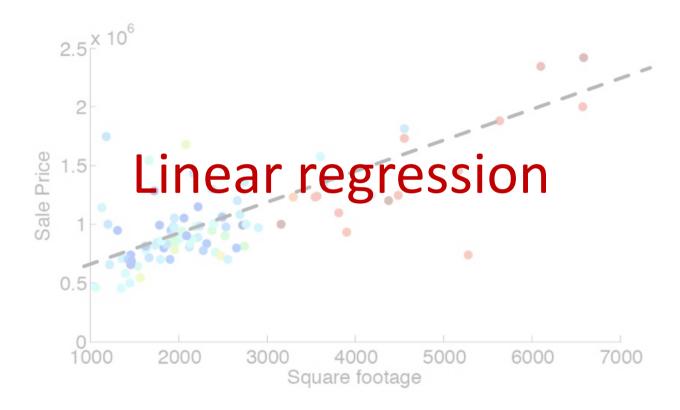
Optimization: How can we efficiently solve the empirical risk

minimization problem?

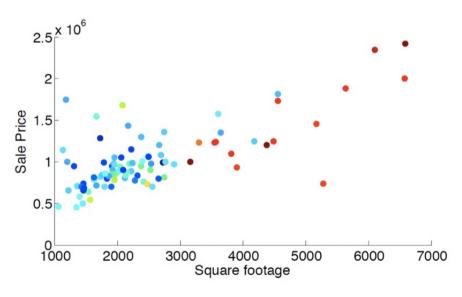
Generalization: Will the predictions of our model transfer

gracefully to unseen examples?

All related! And the fuel which powers everything is data.



House price prediction: the loss function



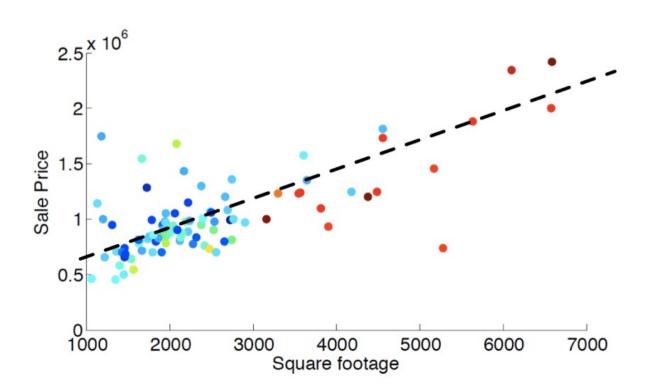
We're looking at real-valued outputs. Some popular loss functions:

- Squared loss (most common): $(prediction sale price)^2$.
- Absolute value loss: |prediction sale price|.

House price prediction: the function class

Possibly linear relationship:

Sale price ≈ price per sqft × square footage + fixed expense



Linear regression

Predicted sale price = price_per_sqft × square footage + fixed_expense

one model: price_per_sqft = 0.3K, fixed_expense = 210K

sqft	sale price (K)	prediction (K)	squared error
2000	810	810	0
2100	907	840	67^{2}
1100	312	540	228^{2}
5500	2,600	1,860	740^{2}
		•••	• • • •
Total			$0 + 67^2 + 228^2 + 740^2 + \cdots$

Adjust price_per_sqft and fixed_expense such that the total squared error is minimized.

Putting things together: Linear regression

- Input: $\boldsymbol{x} \in \mathbb{R}^d$, Output: $y \in \mathbb{R}$.
- Loss for predictor $f: \mathbb{R}^d \to \mathbb{R}$ on (\boldsymbol{x}, y) : $(f(\boldsymbol{x}) y)^2$.
- Training data $S = \{(x_i, y_i), i = 1, ..., n\}.$
- Linear model $\{f: f(x) = w_0 + \sum_{j=1}^d w_j x_j = w_0 + \boldsymbol{w}^T \boldsymbol{x}, \boldsymbol{w} \in \mathbb{R}^d\}.$
 - $\boldsymbol{w} = [w_1, \dots, w_d]^{\top}$ are the weights.
 - w_0 is bias.

Note: For notational convenience

Append 1 to each x as first feature: $\tilde{x} = [1 x_1 x_2 ... x_d]^T$

Let $\widetilde{\boldsymbol{w}}$ = $[w_0, w_1, w_2, ..., w_d]^T$ represent all d+1 parameters

Model becomes $f(\mathbf{x}) = \widetilde{\mathbf{w}}^T \widetilde{\mathbf{x}}$

Sometimes, we'll use w, x, d for \widetilde{w} , \widetilde{x} , d+1

Goal

• Goal is to minimize total error (empirical risk minimization):

$$\hat{R}_S(\tilde{\boldsymbol{w}}) = \frac{1}{n} \sum_{i=1}^n (f(\boldsymbol{x}_i) - y_i)^2 = \frac{1}{n} \sum_{i=1}^n (\tilde{\boldsymbol{x}_i}^{\top} \tilde{\boldsymbol{w}} - y_i)^2.$$

• Define Residual Sum of Squares:

$$RSS(\tilde{\boldsymbol{w}}) = n\hat{R}_S(\tilde{\boldsymbol{w}}) = \sum_{i=1}^n (\tilde{\boldsymbol{x}_i}^\top \tilde{\boldsymbol{w}} - y_i)^2.$$

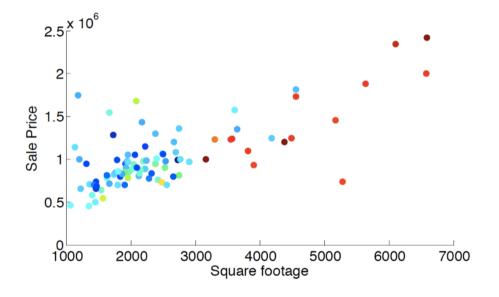
• Goal of empirical risk minimization:

$$ilde{m{w}}^* = \operatorname*{argmin}_{ ilde{m{w}} \in \mathbb{R}^{d+1}} \mathsf{RSS}(ilde{m{w}})$$

This is known as the least squares solution.

Warmup: d = 0

Only one parameter w_0 : constant prediction $f(x) = w_0$



f is a horizontal line, where should it be?

Warmup:
$$d = 0$$

Warmup:
$$d = 1$$

RSS(W)= { (wo+ w, z;-y;) 2

heneral apprach: find stationary points i.e. point with

zero gradient

 $\frac{\partial RSS(\tilde{w})}{\partial w_0} = 0$ = > = > nwo + w, zi - yi = 0 $= > \text{nwo + w, } \neq zi = \neq yi$ $= \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{j=$

るい、 できていけい、ではこうでは、 いのきていけい、それここをなける。

Warmup:
$$d = 1$$

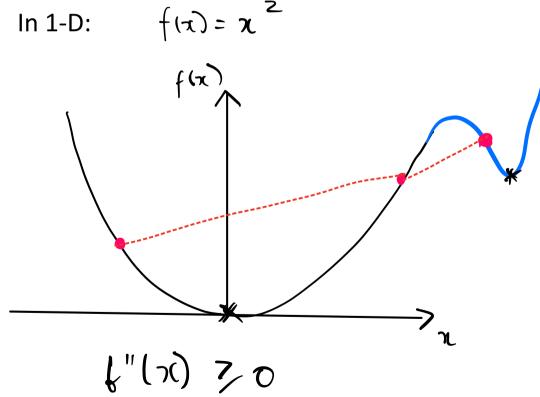
Walliup.
$$u = 1$$

$$\begin{pmatrix}
n & \xi & \tau_i \\
\xi & \tau_i & \xi & \tau_i^2
\end{pmatrix}
\begin{pmatrix}
w_o \\
w_i
\end{pmatrix} = \begin{pmatrix}
x & \xi & \tau_i \\
\xi & \tau_i & \xi & \tau_i
\end{pmatrix}
\begin{pmatrix}
x & \xi & \tau_i \\
\xi & \tau_i & \xi & \tau_i
\end{pmatrix}
\begin{pmatrix}
\xi & \xi & \xi & \xi \\
\xi & \tau_i & \xi & \tau_i
\end{pmatrix}
\begin{pmatrix}
\xi & \xi & \xi & \xi \\
\xi & \tau_i & \xi & \tau_i
\end{pmatrix}$$

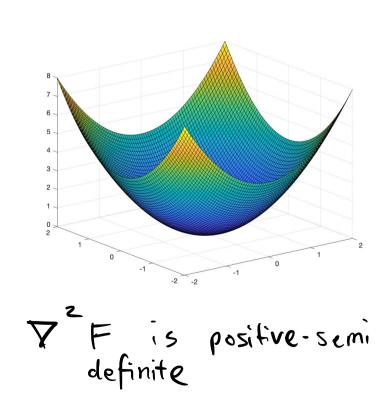
Are stationary points minimizers?

Yes, for *convex* objectives!

In 1-D:



In high dimensions, this looks like:



General least square solution

R >>(
$$\omega$$
) = $\frac{2}{2}$ ($\frac{7}{2}$; $\frac{7}{2}$ ω - $\frac{7}{2}$) $\frac{2}{2}$

$$K > (w) = \{ (\chi_i \mid w - y_i) \}$$

Set
$$\nabla RSS(\tilde{w}) = 0$$

What is $\nabla_w F(w)$ where $F(w) = (\omega^T w - y)^2$?

$$f(w): (\xi \circ i w - y) z$$

$$\nabla_{w}F_{z}[2(\xi(v_{i}w_{i}-y))v_{1}, 2(\xi(v_{i}w_{i}-y))v_{2}, ...$$
= 2 ($v_{i}w_{i}-y$) v_{i}

$$\nabla RSS(\vec{\omega}) = 2 \left(\vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\omega} - \vec{y}_{i} \right) \vec{\lambda}_{i} = 2 \left(\vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\omega} - \vec{y}_{i} \right)$$

$$= 2 \left(\vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \right) \vec{\omega} - 2 \left(\vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \vec{\lambda}_{i} \right)$$

$$\nabla RSS(\vec{\omega}) = 2 \left(\left(\left(\frac{1}{2} \right) \left(\frac{1}{2} \right) \right) \left(\frac{1}{2} \right) \left($$

 $\mathcal{C}^{*} = (\mathcal{C}^{*} \mathcal{C}^{*})^{-1} \times \mathcal{C}^{*}$ (assume 27 is invertible)

Covariance matrix and understanding LS

Here, we assume all features of, in the service of the order of the order of the service of the Xi, is the (i,i) entry of motrix X)

Suppose $Z T \vec{X} = I$, then $\tilde{w}^* = X T y$ each weight w_i is just the covariance of the jth feature with the label

Another approach

RSS is a quadratic, so let's complete the square:

$$\begin{split} & \operatorname{RSS}(\tilde{\boldsymbol{w}}) = \sum_{i} (\tilde{\boldsymbol{w}}^{\mathrm{T}} \tilde{\boldsymbol{x}}_{i} - y_{i})^{2} = \|\tilde{\boldsymbol{X}} \tilde{\boldsymbol{w}} - \boldsymbol{y}\|_{2}^{2} \\ &= \left(\tilde{\boldsymbol{X}} \tilde{\boldsymbol{w}} - \boldsymbol{y}\right)^{\mathrm{T}} \left(\tilde{\boldsymbol{X}} \tilde{\boldsymbol{w}} - \boldsymbol{y}\right) \\ &= \tilde{\boldsymbol{w}}^{\mathrm{T}} \tilde{\boldsymbol{X}}^{\mathrm{T}} \tilde{\boldsymbol{X}} \tilde{\boldsymbol{w}} - \boldsymbol{y}^{\mathrm{T}} \tilde{\boldsymbol{X}} \tilde{\boldsymbol{w}} - \tilde{\boldsymbol{w}}^{\mathrm{T}} \tilde{\boldsymbol{X}}^{\mathrm{T}} \boldsymbol{y} + \mathrm{cnt.} \\ &= \left(\tilde{\boldsymbol{w}} - (\tilde{\boldsymbol{X}}^{\mathrm{T}} \tilde{\boldsymbol{X}})^{-1} \tilde{\boldsymbol{X}}^{\mathrm{T}} \boldsymbol{y}\right)^{\mathrm{T}} \left(\tilde{\boldsymbol{X}}^{\mathrm{T}} \tilde{\boldsymbol{X}}\right) \left(\tilde{\boldsymbol{w}} - (\tilde{\boldsymbol{X}}^{\mathrm{T}} \tilde{\boldsymbol{X}})^{-1} \tilde{\boldsymbol{X}}^{\mathrm{T}} \boldsymbol{y}\right) + \mathrm{cnt.} \end{split}$$

Note:
$$\boldsymbol{u}^{\mathrm{T}}\left(\tilde{\boldsymbol{X}}^{\mathrm{T}}\tilde{\boldsymbol{X}}\right)\boldsymbol{u}=\left(\tilde{\boldsymbol{X}}\boldsymbol{u}\right)^{\mathrm{T}}\tilde{\boldsymbol{X}}\boldsymbol{u}=\|\tilde{\boldsymbol{X}}\boldsymbol{u}\|_{2}^{2}\geq0$$
 and is 0 if $\boldsymbol{u}=0$. So $\tilde{\boldsymbol{w}}^{*}=(\tilde{\boldsymbol{X}}^{\mathrm{T}}\tilde{\boldsymbol{X}})^{-1}\tilde{\boldsymbol{X}}^{\mathrm{T}}\boldsymbol{y}$ is the minimizer.

Computational complexity

Bottleneck of computing

$$\widetilde{\boldsymbol{w}}^* = (\widetilde{\boldsymbol{X}}^T \widetilde{\boldsymbol{X}})^{-1} \widetilde{\boldsymbol{X}}^T \boldsymbol{y}$$

is to invert the matrix $\widetilde{\pmb{X}}^T\widetilde{\pmb{X}} \in \mathbb{R}^{(d+1)} \times \mathbb{R}^{(d+1)}$.

Optimization methods

Problem setup

Given: a function F(w)

Goal: minimize F(w) (approximately)

Two simple yet extremely popular methods

Gradient Descent (GD): simple and fundamental

Stochastic Gradient Descent (SGD): faster, effective for large-scale problems

Gradient is the *first-order information* of a function.

Therefore, these methods are called *first-order methods*.

Gradient descent

GD: keep moving in the *negative gradient direction*

Start from some
$$w^{(0)}$$
. For $t=0,1,...$

$$w^{(t+1)} = w^{(+)} - \eta \nabla F(w)$$
where $\eta > 0$ is called step size on learning rate.

- in theory η should be set in terms of some parameters of f
- in practice we just try several small values
- might need to be changing over iterations (think f(w) = |w|)
- adaptive and automatic step size tuning is an active research area

An example

Consider squared loss on one datapoint (x, y) where $x = (x^{(1)}, x^{(2)})$ for $\mathbf{w} = (w_1, w_2)$.

$$F(\mathbf{w}) = (w_1 x^{(1)} + w_2 x^{(2)} - y)^2.$$

Gradient is

$$\frac{\partial F}{\partial w_1} = 2(w_1 x^{(1)} + w_2 x^{(2)} - y) \cdot x^{(1)} \qquad \frac{\partial F}{\partial w_2} = 2(w_1 x^{(1)} + w_2 x^{(2)} - y) \cdot x^{(2)}$$

GD:

- Initialize $w_1^{(0)}$ and $w_2^{(0)}$ (to be 0 or *randomly*), t=0
- do

$$w_1^{(t+1)} \leftarrow w_1^{(t)} - \eta \left[2(w_1 x^{(1)} + w_2 x^{(2)} - y) \cdot x^{(1)} \right]$$

$$w_2^{(t+1)} \leftarrow w_2^{(t)} - \eta \left[2(w_1 x^{(1)} + w_2 x^{(2)} - y) \cdot x^{(2)} \right]$$

$$t \leftarrow t + 1$$

ullet until $F(oldsymbol{w}^{(t)})$ does not change much or t reaches a fixed number

Switch to Colab

```
🛆 optimization.jpvnb 🕱
 File Edit View Insert Runtime Tools Help
+ Code + Text
         this theta[1] = last theta[1] - eta * grad1
         theta.append(this_theta)
        J.append(cost func(*this theta))
     # Annotate the objective function plot with coloured points indicating the
     # parameters chosen and red arrows indicating the steps down the gradient.
     for j in range(1,N):
        ax.annotate('', xy=theta[j], xytext=theta[j-1],
                        arrowprops={'arrowstyle': '->', 'color': 'orange', 'lw': 1},
                        va='center', ha='center')
     ax.scatter(*zip(*theta), facecolors='none', edgecolors='r', lw=1.5)
     # Labels, titles and a legend.
     ax.set xlabel(r'$w 1$')
     ax.set_ylabel(r'$w_2$')
     ax.set_title('objective function')
     plt.show()
 ₽
                                     objective function
```