# CS794/CO673: Optimization for Data Science Lec 00: Introduction

Yaoliang Yu



September 9, 2022

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Instructor: Yao-Liang Yu (yaoliang.yu@uwaterloo.ca)
- Office hours: Friday 4-5pm (DC3617) or by email appointment
- TA: Zeou Hu (zeou.hu@uwaterloo.ca)
- Website: cs.uwaterloo.ca/~y328yu/mycourses/794 slides, notes, videos, assignments, policy, etc.
- Piazza: piazza.com/uwaterloo.ca/fall2022/co673cs794 announcements, questions, discussions, etc.
- Learn: learn.uwaterloo.ca/d21/home/825963 assignments, solutions, grades, etc.

- Basic linear algebra, calculus, probability, algorithm
- Some relevant books on course website
- Coding

"Coding to programming is like typing to writing."

- Basic linear algebra, calculus, probability, algorithm
- Some relevant books on course website
- Coding

"Coding to programming is like typing to writing. "  $\sim$ 

- Basic linear algebra, calculus, probability, algorithm
- Some relevant books on course website
- Coding



https://www.python.org/



"Coding to programming is like typing to writing."

- Basic linear algebra, calculus, probability, algorithm
- Some relevant books on course website
- Coding



https://www.python.org/



"Coding to programming is like typing to writing."

- Basic linear algebra, calculus, probability, algorithm
- Some relevant books on course website
- Coding



https://www.python.org/

https://julialang.org/

**u**la

"Coding to programming is like typing to writing." — Leslie Lamport

### Textbooks

#### • No required textbook

- Notes, slides, and code will be posted on the course website
- Some fine textbooks for the ambitious ones:

links available on the course website

### Textbooks

- No required textbook
- Notes, slides, and code will be posted on the course website
- Some fine textbooks for the ambitious ones:

links available on the course website

### Textbooks

- No required textbook
- Notes, slides, and code will be posted on the course website
- Some fine textbooks for the ambitious ones:



links available on the course website

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often
  - typeset using LATEX is recommended

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often

- typeset using <code>LTEX</code> is recommended

- Roughly 24 lectures, each lasting 80 mins (I hope)
- Expect 5 assignments, approx. 1 bi-weekly
  - 20 points each; total: 100
  - per approval, may substitute 1 assignment with a course project
- Small, constant progress every week
- Submit on LEARN. Submit early and often
  - typeset using LATEX is recommended

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website.
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse

good online discussion, more on course website.

- Serious offense will result in expulsion...
- NO late submissions!

– except hospitalization, family urgency, .... notify beforehand

• Appeal within two weeks

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks

- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!



Appeal within two weeks



- Do your work independently and individually
  - discussion is fine, but no sharing of text or code
  - explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks



#### • Do your work independently and individually

- discussion is fine, but no sharing of text or code
- explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks



#### • Do your work independently and individually

- discussion is fine, but no sharing of text or code
- explicitly acknowledge any source that helped you
- Ignorance is no excuse
  - good online discussion, more on course website
- Serious offense will result in expulsion...
- NO late submissions!
  - except hospitalization, family urgency, ... notify beforehand
- Appeal within two weeks





## Machine Learning is Everywhere

• Everyone uses ML everyday



Lots of cool applications

Excellent for job-hunting

## Machine Learning is Everywhere

• Everyone uses ML everyday



#### • Lots of cool applications



Excellent for job-hunting

## Machine Learning is Everywhere

• Everyone uses ML everyday



#### • Lots of cool applications



• Excellent for job-hunting

## At the Core is Optimization



### What You Will Learn

- Learn the basic theory and algorithms
- Gain some implementation experience
- Know when to use which algorithm with what guarantees
- Start to formulate problems with algorithms in mind


#### What You Will Learn

- Learn the basic theory and algorithms
- Gain some implementation experience
- Know when to use which algorithm with what guarantees
- Start to formulate problems with algorithms in mind



#### What You Will Learn

- Learn the basic theory and algorithms
- Gain some implementation experience
- Know when to use which algorithm with what guarantees
- Start to formulate problems with algorithms in mind



#### What You Will Learn

- Learn the basic theory and algorithms
- Gain some implementation experience
- Know when to use which algorithm with what guarantees
- Start to formulate problems with algorithms in mind



	Date	Topic	Slides	Notes	Comments	Applications
00	Sep 09, 2022	Introduction	pdf		pdf	perceptron
01	Sep 09, 2022	Linear System	pdf	pdf		linear regression
02	Sep 16, 2022	Gradient Descent				logistic regression
03	Sep 16, 2022	Projection			hw1	white-box attack
04	Sep 23, 2022	Proximal Gradient				lasso
05	Sep 23, 2022	Subgradient				svm
06	Sep 30, 2022	Conditional Gradient				recommendation
07	Sep 30, 2022	Fictitious Play			hw2	poker
08	Oct 07, 2022	Mirror Descent				sparsity
09	Oct 07, 2022	Metric Gradient				compression
	Oct 14, 2022					reading week
	Oct 14, 2022					reading week
10	Oct 21, 2022	Acceleration				total variation
11	Oct 21, 2022	Smoothing			hw3	robustness
12	Oct 28, 2022	Alternating				expectation-maximization
13	Oct 28, 2022	Coordinate Gradient				covariance estimation
14	Nov 04, 2022	Minimax				adversarial training
15	Nov 04, 2022	Averaging			hw4	GAN
16	Nov 11, 2022	Extragradient				max entropy
17	Nov 11, 2022	Splitting				federated learning
18	Nov 18, 2022	Stochastic Gradient				neural nets
19	Nov 18, 2022	Variance Reduction			hw5	boosting
20	Nov 25, 2022	Randomized Smoothing				certification
21	Nov 25, 2022	Search				black-box attack
22	Dec 02, 2022	Newton				data poisoning
23	Dec 02, 2022	Quasi-Newton				page rank

# Let the Journey Begin

#### What a Dataset Looks Like

	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	•••	$\mathbf{x}_n$	x	$\mathbf{x}'$
(	0	1	0	1	•••	1	1	0.9
$\mathbb{R}^d \ni $	0	0	1	1		0	1	
							:	
L L	1	0	1	0	•••	1	1	-0.1
У	+	+	—	+	•••	—	?	?!

each column is a data point: n in total; each has d features

bottom y is the label vector; binary in this case

ullet  $\mathbf{x}$  and  $\mathbf{x}'$  are test samples whose labels need to be predicted

	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	•••	$\mathbf{x}_n$	x	$\mathbf{x}'$
(	0	1	0	1	•••	1	1	0.9
$\mathbb{R}^d \ni \left\{ \right\}$	0	0	1	1		0	1	
							÷	
U	1	0	1	0	•••	1	1	-0.1
У	+	+	—	+	•••	—	?	?!

- each column is a data point: n in total; each has d features
- bottom y is the label vector; binary in this case
- ullet  $\mathbf{x}$  and  $\mathbf{x}'$  are test samples whose labels need to be predicted

	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	•••	$\mathbf{x}_n$	x	$\mathbf{x}'$
(	0	1	0	1	•••	1	1	0.9
$\mathbb{R}^d \ni \left\{ \right\}$	0	0	1	1		0	1	
							:	
U	1	0	1	0	•••	1	1	-0.1
У	+	+	—	+	•••	—	?	?!

- each column is a data point: n in total; each has d features
- bottom y is the label vector; binary in this case

ullet  $\mathbf{x}$  and  $\mathbf{x}'$  are test samples whose labels need to be predicted

	$\mathbf{x}_1$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\mathbf{x}_4$	•••	$\mathbf{x}_n$	x	$\mathbf{x}'$
(	0	1	0	1	•••	1	1	0.9
$\mathbb{R}^{d} \rightarrow $	0	0	1	1		0	1	
							:	
U	1	0	1	0		1	1	-0.1
У	+	+	—	+	•••	—	?	?!

- each column is a data point: n in total; each has d features
- bottom y is the label vector; binary in this case
- $\mathbf{x}$  and  $\mathbf{x}'$  are test samples whose labels need to be predicted











# The Early Hype in Al...



reproduce itself and be conscious of its existence. The embryo-the Weather Bureau's \$2,000,000 "704" computer-learned to differentiate between right and left after fifty altempts in the <u>Navy's</u>

demonstration for newsmen.. The service said it would use this principle to build the first of its Perceptron thinking machines that will be able to read and write. It is expected to be finished in about a year at a cost of \$100.000.

Dr. Frank Rosenblatt, designer of the Perceptron, conducted the demonstration. He said the machine would be the first device to think as the human brain. As do human beings, Perceptron will make mistakes at first, but will grow wiser as it gains experience, he said.

Dr. Rosenblatt, a research psychologist at the Cornell Aeronautical Laboratory, Buffalo, said Perceptrons might be fired to the planets as mechanical space explorers.

#### Without Human Controls

The Navy said the perceptron would be the first non-living mechanism "capable of receiving, recognizing and identifying its surroundings without any human training or control."

The "brain" is designed to remember images and information it has perceived itself. Ordinary computers remember only what is fed into them on punch cards or magnetic tape.

Later Perceptrons will be able to recognize people and call out their names and instantly translate speech in one language to speech or writing in another language, it was predicted.

Mr. Eosenblatt said in principle it would be possible to build brains that could reproduce themselves on an assembly line and which would be conscious of their existence.

In today's demonstration, the "704" was fed two cards, one with squares marked on the left side and the other with squares on the right side.

#### Learns by Doing

In the first fifty trials, the machine made no distinction between them. It then started registering a "Q" for the left squares and "O" for the right squares.

Dr. Rosenblatt said he could machine why the explain learned only in highly technical terms. But he said the computer had undergone a "self-induced change in the wiring diagram." first Perceptron will The 1.000 electronic about have cells" receiving "association electrical impulses from an eyelike scanning device with 400 photo-cells. The human brain 10,000,000,000 responsive has cells, including 100,000,000 connections with the eyes.

#### ...due to Perceptron





Frank Rosenblatt (1928 – 1971)

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathsf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

- we often can only describe S partially.

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathbf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

- we often can only describe S partially.

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathbf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

we often can only describe S partially.

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathsf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

we often can only describe S partially.

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathsf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

#### find $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

we often can only describe S partially.

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_{j} x_{j} w_{j}$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathsf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

– we often can only describe  ${\mathcal S}$  partially

• Affine function:  $f(\mathbf{x}) = \langle \mathbf{x}, \mathbf{w} \rangle + b$ , where  $\langle \mathbf{x}, \mathbf{w} \rangle := \sum_j x_j w_j$ 

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathsf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ .

- Perceptron solves the above optimization problem!
  - it is iterative: going through the data one by one
  - it converges faster if the problem is easier
  - it behaves benignly even if no solution exists
- Abstract a bit more:

find  $\mathbf{w} \in \mathcal{S} \subseteq \mathbb{R}^d$ .

- we often can only describe  ${\cal S}$  partially

# Geometrically



# Geometrically



#### Algorithm 1: Perceptron

Input: Dataset  $\mathcal{D} = \mathcal{J}(\mathbf{x}_i, \mathbf{y}_i) \in \mathbb{R}^d \times \{\pm 1\} : i = 1, \dots, n \mathcal{J}$ initialization  $\mathbf{w} \in \mathbb{R}^d$  and  $b \in \mathbb{R}$ , threshold  $\delta \geq 0$ **Output:** approximate solution  $\mathbf{w}$  and b1 for t = 1, 2, ... do receive index  $I_t \in \{1, \ldots, n\}$  $// I_t$  can be random 2 if  $y_{I_t}(\langle \mathbf{x}_{I_t}, \mathbf{w} \rangle + b) \leq \delta$  then // update after a ''mistake'' 4

• Typically  $\delta = 0$  and  $\mathbf{w}_0 = \mathbf{0}, b = 0$ 

3

5

F. Rosenblatt (1958). "The perceptron: A probabilistic model for information storage and organization in the brain", Psychological Review, vol. 65, no. 6, pp. 386-408.

#### Algorithm 2: Perceptron

Input: Dataset  $\mathcal{D} = \mathcal{J}(\mathbf{x}_i, \mathbf{y}_i) \in \mathbb{R}^d \times \{\pm 1\} : i = 1, \dots, n \mathcal{J}$ initialization  $\mathbf{w} \in \mathbb{R}^d$  and  $b \in \mathbb{R}$ , threshold  $\delta \geq 0$ **Output:** approximate solution  $\mathbf{w}$  and b1 for t = 1, 2, ... do receive index  $I_t \in \{1, \ldots, n\}$  $// I_t$  can be random 2 if  $y_{I_t}(\langle \mathbf{x}_{I_t}, \mathbf{w} \rangle + b) \leq \delta$  then // update after a ''mistake'' 4

• Typically  $\delta = 0$  and  $\mathbf{w}_0 = \mathbf{0}, b = 0$ 

-  $y\hat{y} > 0$  vs.  $y\hat{y} < 0$  vs.  $y\hat{y} = 0$ , where  $\hat{y} = \langle \mathbf{x}, \mathbf{w} \rangle + b$ 

3

5

F. Rosenblatt (1958). "The perceptron: A probabilistic model for information storage and organization in the brain", Psychological Review, vol. 65, no. 6, pp. 386-408.

#### Algorithm 3: Perceptron

Input: Dataset  $\mathcal{D} = \mathcal{J}(\mathbf{x}_i, \mathbf{y}_i) \in \mathbb{R}^d \times \{\pm 1\} : i = 1, \dots, n \mathcal{J}$ initialization  $\mathbf{w} \in \mathbb{R}^d$  and  $b \in \mathbb{R}$ , threshold  $\delta \geq 0$ **Output:** approximate solution  $\mathbf{w}$  and b1 for t = 1, 2, ... do receive index  $I_t \in \{1, \ldots, n\}$  $// I_t$  can be random 2 if  $y_{I_t}(\langle \mathbf{x}_{I_t}, \mathbf{w} \rangle + b) \leq \delta$  then // update after a ''mistake'' 4

• Typically  $\delta = 0$  and  $\mathbf{w}_0 = \mathbf{0}, b = 0$ 

-  $y\hat{y} > 0$  vs.  $y\hat{y} < 0$  vs.  $y\hat{y} = 0$ , where  $\hat{y} = \langle \mathbf{x}, \mathbf{w} \rangle + b$ 

• Lazy update: "if it ain't broke, don't fix it"

3

5

F. Rosenblatt (1958). "The perceptron: A probabilistic model for information storage and organization in the brain", Psychological Review, vol. 65, no. 6, pp. 386-408.





 $\hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [0, 0], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [0,0], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [0,0], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [0, 0], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 

#### Does it work?





 $\mathbf{w} = [1,0], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1, 0], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1,0], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$




 $\mathbf{w} = [1,0], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1, 1], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1, 1], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1, 1], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [1, 1], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 1], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 1], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 1], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2,1], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 2], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 2], \ b = 0, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 





 $\mathbf{w} = [2, 2], \ b = -1, \ \hat{\mathbf{y}} = \operatorname{sign}(\langle \mathbf{x}, \mathbf{w} \rangle + b),$ 

## XOR Dataset



Prove that no line can separate + from -

• What happens if we run Perceptron regardless?

## XOR Dataset



• Prove that no line can separate + from -

• What happens if we run Perceptron regardless?

## XOR Dataset



- Prove that no line can separate + from -
- What happens if we run Perceptron regardless?

## Perceptron and the 1<sup>st</sup> Al Winter



M. L. Minsky and S. A. Papert (1969). "Perceptron". MIT press.

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathbf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ find  $\mathbf{w} = [\mathbf{w}; b] \in \mathbb{R}^{d+1}$  such that  $\forall i, \ \langle \mathbf{a}_i, \mathbf{w} \rangle \le c_i, \ \mathbf{a}_i = -\mathbf{y}_i[\mathbf{x}_i; 1]$ find  $\mathbf{w} \in \mathbb{R}^p$  such that  $\mathbf{A}^\top \mathbf{w} \le \mathbf{c}$ 

Algorithm 4: Projection Algorithm for Linear Inequalities

Input:  $\mathbf{A} \in \mathbb{R}^{p \times n}, \mathbf{c} \in \mathbb{R}^n$ , initialization  $\mathbf{w} \in \mathbb{R}^p$ , relaxation parameter  $\eta \in (0, 2]$ 

1 for t = 1, 2, ... do

 $\mathbf{r}_{t}$  select index  $I_{t} \in \{1,\ldots,n\}$  // index  $I_{t}$  can be random

$$\mathbf{3} \quad \mathbf{w} \leftarrow (1-\eta)\mathbf{w} + \eta \quad \mathbf{w} - \frac{(\langle \mathbf{a}_{I_t}, \mathbf{w} \rangle - c_{I_t})^+}{\|\mathbf{a}_{I_t}\|_2} \cdot \frac{\mathbf{a}_{I_t}}{\|\mathbf{a}_{I_t}\|_2}$$

T. S. Motzkin and I. J. Schoenberg (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 393–404; S. Agmon (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 382–392.

# Projection Algorithms

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ y_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ find  $\mathbf{w} = [\mathbf{w}; b] \in \mathbb{R}^{d+1}$  such that  $\forall i, \ \langle \mathbf{a}_i, \mathbf{w} \rangle \le c_i, \ \mathbf{a}_i = -y_i[\mathbf{x}_i; 1]$ find  $\mathbf{w} \in \mathbb{R}^p$  such that  $\mathbf{A}^\top \mathbf{w} \le \mathbf{c}$ 

Algorithm 5: Projection Algorithm for Linear Inequalities

Input:  $\mathbf{A} \in \mathbb{R}^{p \times n}, \mathbf{c} \in \mathbb{R}^n$ , initialization  $\mathbf{w} \in \mathbb{R}^p$ , relaxation parameter  $\eta \in (0, 2]$ 

1 for t = 1, 2, ... do

e i select index  $I_t \in \{1,\ldots,n\}$  // index  $I_t$  can be random

 $\mathbf{B} \quad \mathbf{w} \leftarrow (1-\eta)\mathbf{w} + \eta \quad \mathbf{w} - \frac{(\langle \mathbf{a}_{I_t}, \mathbf{w} \rangle - c_{I_t})^+}{\|\mathbf{a}_{I_t}\|_2} \cdot \frac{\mathbf{a}_{I_t}}{\|\mathbf{a}_{I_t}\|_2}$ 

T. S. Motzkin and I. J. Schoenberg (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 393–404; S. Agmon (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 382–392.

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ y_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ find  $\mathbf{w} = [\mathbf{w}; b] \in \mathbb{R}^{d+1}$  such that  $\forall i, \ \langle \mathbf{a}_i, \mathbf{w} \rangle \le c_i, \ \mathbf{a}_i = -y_i[\mathbf{x}_i; 1]$ find  $\mathbf{w} \in \mathbb{R}^p$  such that  $\mathbf{A}^\top \mathbf{w} \le \mathbf{c}$ 

Algorithm 6: Projection Algorithm for Linear Inequalities Input:  $\mathbf{A} \in \mathbb{R}^{p imes n}, \mathbf{c} \in \mathbb{R}^{n}$ , initialization  $\mathbf{w} \in \mathbb{R}^{p}$ , relaxation parame

1 for t = 1, 2 do

 $\mathbf{2} \hspace{0.1 cm} \mid \hspace{0.1 cm}$  select index  $I_t \in \{1, \ldots, n\}$  // index  $I_t$  can be random

$$\mathbf{3} \qquad \mathbf{w} \leftarrow (1-\eta)\mathbf{w} + \eta \quad \mathbf{w} - \frac{(\langle \mathbf{a}_{I_t}, \mathbf{w} \rangle - c_{I_t})^+}{\|\mathbf{a}_{I_t}\|_2} \cdot \frac{\mathbf{a}_{I_t}}{\|\mathbf{a}_{I_t}\|_2}$$

T. S. Motzkin and I. J. Schoenberg (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 393–404; S. Agmon (1954). "The Relaxation Method for Linear Inequalities". *Canadian Journal of Mathematics*, vol. 6, pp. 382–392.

find  $\mathbf{w} \in \mathbb{R}^d, b \in \mathbb{R}$  such that  $\forall i, \ \mathbf{y}_i(\langle \mathbf{x}_i, \mathbf{w} \rangle + b) > 0$ find  $\mathbf{w} = [\mathbf{w}; b] \in \mathbb{R}^{d+1}$  such that  $\forall i, \ \langle \mathbf{a}_i, \mathbf{w} \rangle \le c_i, \ \mathbf{a}_i = -\mathbf{y}_i[\mathbf{x}_i; 1]$ find  $\mathbf{w} \in \mathbb{R}^p$  such that  $\mathbf{A}^\top \mathbf{w} \le \mathbf{c}$ 

Algorithm 7: Projection Algorithm for Linear Inequalities

Input:  $\mathbf{A} \in \mathbb{R}^{p \times n}$ ,  $\mathbf{c} \in \mathbb{R}^{n}$ , initialization  $\mathbf{w} \in \mathbb{R}^{p}$ , relaxation parameter  $\eta \in (0, 2]$ 

1 for t = 1, 2, ... do

2 | select index  $I_t \in \{1, \dots, n\}$  // index  $I_t$  can be random

 $\mathbf{3} \quad \mathbf{w} \leftarrow (1-\eta)\mathbf{w} + \eta \left[\mathbf{w} - \frac{(\langle \mathbf{a}_{I_t}, \mathbf{w} \rangle - c_{I_t})^+}{\|\mathbf{a}_{I_t}\|_2} \cdot \frac{\mathbf{a}_{I_t}}{\|\mathbf{a}_{I_t}\|_2}\right]$ 

T. S. Motzkin and I. J. Schoenberg (1954). "The Relaxation Method for Linear Inequalities". Canadian Journal of Mathematics, vol. 6, pp. 393–404; S. Agmon (1954). "The Relaxation Method for Linear Inequalities". On Canadian Journal of Mathematics, vol. 6, pp. 382–392.

### Theorem:

int cone<sup>\*</sup>  $A \neq \emptyset \iff$  int cone<sup>\*</sup>  $A \cap$  cone  $A \neq \emptyset$ .



### Theorem:

int cone<sup>\*</sup>  $A \neq \emptyset \iff$  int cone<sup>\*</sup>  $A \cap$  cone  $A \neq \emptyset$ .



### Theorem:

### int cone<sup>\*</sup> $A \neq \emptyset \iff$ int cone<sup>\*</sup> $A \cap$ cone $A \neq \emptyset$ .



### Theorem:

int cone<sup>\*</sup>  $A \neq \emptyset \iff$  int cone<sup>\*</sup>  $A \cap$  cone  $A \neq \emptyset$ .



### Theorem:

## int cone<sup>\*</sup> $A \neq \emptyset \iff$ int cone<sup>\*</sup> $A \cap$ cone $A \neq \emptyset$ .



### Theorem:

## int cone<sup>\*</sup> $A \neq \emptyset \iff$ int cone<sup>\*</sup> $A \cap$ cone $A \neq \emptyset$ .



# Is Perceptron Unique?



# Is Perceptron Unique?


















#### Support Vector Machines: Primal





where  $\hat{y}_i := \langle \mathbf{x}_i, \mathbf{w} 
angle + b$ 



















 $\min_{\mathbf{w}} \hat{\mathsf{E}}\ell(\mathbf{y}\hat{y}) + \operatorname{reg}(\mathbf{w}), \quad \text{s.t.} \quad \hat{y} := \langle \mathbf{x}, \mathbf{w} \rangle + l$ 

#### Empirical Risk Minimization



#### Regularization



Regression



- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth  $\operatorname{reg}$
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical

- Lec04: Proximal Gradient: smooth  $\ell$  + nonsmooth reg
- Lec05: Subgradient: nonsmooth  $\ell$  + nonsmooth reg
- Lec10: Acceleration: optimal algorithm under smoothness
- Lec11: Smoothing: nonsmooth —> smooth
- Lec12: Alternating: divide and conquer
- Lec13: Coordinate Gradient: large model
- Lec18: Stochastic Gradient: large dataset
- Lec22: Newton: even faster under smoothness
- Lec23: Quasi-Newton: Newton made economical



# $\min_{\mathbf{z}} \underbrace{\frac{1}{2} \|\mathbf{x} - \mathbf{z}\|_{2}^{2}}_{\text{fidelity}} + \underbrace{\lambda \cdot \|\mathbf{z}\|_{\text{tv}}}_{\text{regularization}}$

•  $\lambda$  controls the trade-off

- regularization encodes prior knowledge
- crucial to not over-smooth



# $\min_{\mathbf{z}} \underbrace{\frac{1}{2} \|\mathbf{x} - \mathbf{z}\|_{2}^{2}}_{\text{fidelity}} + \underbrace{\lambda \cdot \|\mathbf{z}\|_{\text{tv}}}_{\text{regularization}}$

#### • $\lambda$ controls the trade-off

- regularization encodes prior knowledge
- crucial to not over-smooth



# $\min_{\mathbf{z}} \underbrace{\frac{1}{2} \|\mathbf{x} - \mathbf{z}\|_{2}^{2}}_{\text{fidelity}} + \underbrace{\lambda \cdot \|\mathbf{z}\|_{\text{tv}}}_{\text{regularization}}$

- $\lambda$  controls the trade-off
- regularization encodes prior knowledge
- crucial to not over-smooth



$$\min_{\mathbf{z}} \; \underbrace{\frac{1}{2} \|\mathbf{x} - \mathbf{z}\|_2^2}_{\text{fidelity}} \; + \; \underbrace{\lambda \cdot \|\mathbf{z}\|_{\text{tv}}}_{\text{regularization}}$$

- $\lambda$  controls the trade-off
- regularization encodes prior knowledge
- crucial to not over-smooth

#### Adversarial Examples



#### Adversarial Examples



#### Adversarial Examples







- Mathematically, a neural network is a function f(w);
- ullet Typically, input imes is given and network weights imes optimized
- Could also freeze weights w and optimize x, adversarially!

 $\min_{\boldsymbol{\delta}} |\operatorname{size}(\boldsymbol{\delta}) - \operatorname{s.t.} - \operatorname{pred}[/(\operatorname{wax} + \boldsymbol{\delta})] \neq y.$ 

• More generally:  $\max_{\delta \in \mathcal{S}} |\langle (\max + \delta, \gamma) - \operatorname{stat} | \operatorname{size}(\delta) | \leq |\langle \delta - \gamma \rangle|$ 



- Mathematically, a neural network is a function  $f(\mathbf{w}; \mathbf{x})$
- ullet Typically, input  ${f x}$  is given and network weights  ${f w}$  optimized
- Could also freeze weights w and optimize x, adversarially!

 $\min_{\boldsymbol{\delta}} \operatorname{size}(\boldsymbol{\delta}) \quad \text{s.t.} \quad \operatorname{pred}[f(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta})] \neq \mathsf{y}$ 

• More generally:  $\max_{oldsymbol{\delta}} \; \ell(\mathbf{w}; \mathbf{x} + oldsymbol{\delta}, \mathsf{y}) \quad ext{s.t.} \quad ext{size}(oldsymbol{\delta}) \leq \epsilon$ 



- Mathematically, a neural network is a function  $f(\mathbf{w}; \mathbf{x})$
- Typically, input  $\mathbf{x}$  is given and network weights  $\mathbf{w}$  optimized
- Could also freeze weights w and optimize x, adversarially!

 $\min_{\boldsymbol{\delta}} \ \mathrm{size}(\boldsymbol{\delta}) \quad \mathrm{s.t.} \quad \mathrm{pred}[f(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta})] \neq \mathsf{y}$ 

• More generally:  $\max_{oldsymbol{\delta}} \; \ell(\mathbf{w}; \mathbf{x} + oldsymbol{\delta}, \mathsf{y}) \quad ext{s.t.} \quad ext{size}(oldsymbol{\delta}) \leq \epsilon$ 



- Mathematically, a neural network is a function  $f(\mathbf{w}; \mathbf{x})$
- Typically, input  $\mathbf{x}$  is given and network weights  $\mathbf{w}$  optimized
- Could also freeze weights  $\mathbf{w}$  and optimize  $\mathbf{x}$ , adversarially!

 $\min_{\boldsymbol{\delta}} \operatorname{size}(\boldsymbol{\delta}) \quad \text{s.t.} \quad \operatorname{pred}[f(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta})] \neq \mathsf{y}$ 

• More generally:  $\max_{oldsymbol{\delta}} \; \ell(\mathbf{w}; \mathbf{x} + oldsymbol{\delta}, \mathsf{y}) \quad ext{s.t.} \quad ext{size}(oldsymbol{\delta}) \leq \epsilon$ 



- Mathematically, a neural network is a function  $f(\mathbf{w}; \mathbf{x})$
- Typically, input  $\mathbf{x}$  is given and network weights  $\mathbf{w}$  optimized
- Could also freeze weights  $\mathbf{w}$  and optimize  $\mathbf{x}$ , adversarially!

 $\min_{\boldsymbol{\delta}} \operatorname{size}(\boldsymbol{\delta}) \quad \text{s.t.} \quad \operatorname{pred}[f(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta})] \neq \mathsf{y}$ 

• More generally:  $\max_{\delta} \ell(\mathbf{w}; \mathbf{x} + \delta, \mathbf{y})$  s.t.  $\operatorname{size}(\delta) \leq \epsilon$ 


- Empirical risk minimization recalled:  $\min_{\mathbf{w}} \hat{E}\ell(\mathbf{w}; \mathbf{x}, y)$
- Adversarial attack perturbs  $(\mathbf{x}, y)$  while fixing w:

 $\max_{ ext{size}(oldsymbol{\delta})\leq\epsilon} \ell(\mathbf{w};\mathbf{x}+oldsymbol{\delta},y)$ 

• Robustness by anticipating the worst-case:

 $\min_{\mathbf{w}} \hat{\mathsf{E}} \max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

• The game continues by anticipating the anticipation:

 $\max_{\substack{\text{size}(\delta) \le \epsilon}} \ell(\mathbf{w}; \mathbf{x} + \delta, y)$  leader  $\min \hat{\mathsf{E}}\ell(\mathbf{w}; \mathbf{x} + \delta, y)$  follower

- Empirical risk minimization recalled:  $\min_{\mathbf{w}} \hat{E}\ell(\mathbf{w}; \mathbf{x}, y)$
- Adversarial attack perturbs  $(\mathbf{x}, y)$  while fixing  $\mathbf{w}$ :

 $\max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

Robustness by anticipating the worst-case:

 $\min_{\mathbf{w}} \hat{\mathsf{E}} \max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

The game continues by anticipating the anticipation:

 $\max_{\substack{\text{size}(\delta) \le \epsilon}} \ell(\mathbf{w}; \mathbf{x} + \delta, y) \qquad \text{leader} \\ \min \hat{E}\ell(\mathbf{w}; \mathbf{x} + \delta, y) \qquad \text{follower}$ 

- Empirical risk minimization recalled:  $\min_{\mathbf{w}} \hat{E}\ell(\mathbf{w}; \mathbf{x}, y)$
- Adversarial attack perturbs  $(\mathbf{x}, y)$  while fixing w:

 $\max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

• Robustness by anticipating the worst-case:

 $\min_{\mathbf{w}} \hat{\mathsf{E}} \max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

The game continues by anticipating the anticipation:

 $\max_{\text{size}(\delta) \le \epsilon} \ell(\mathbf{w}; \mathbf{x} + \delta, y) \qquad \text{leader}$ 

 $\min_{\mathbf{w}} \; \mathsf{E}\ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y) \qquad \qquad \mathsf{follower}$ 

- Empirical risk minimization recalled:  $\min_{\mathbf{w}} \hat{E}\ell(\mathbf{w}; \mathbf{x}, y)$
- Adversarial attack perturbs  $(\mathbf{x}, y)$  while fixing  $\mathbf{w}$ :

 $\max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

• Robustness by anticipating the worst-case:

 $\min_{\mathbf{w}} \hat{\mathsf{E}} \max_{\text{size}(\boldsymbol{\delta}) \leq \epsilon} \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$ 

• The game continues by anticipating the anticipation:

 $\max_{\substack{\text{size}(\boldsymbol{\delta}) \leq \epsilon \\ \mathbf{w}}} \ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$  leader  $\min_{\mathbf{w}} \hat{\mathsf{E}}\ell(\mathbf{w}; \mathbf{x} + \boldsymbol{\delta}, y)$  follower

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

- Lec07: Fictitious Play: playing against oneself
- Lec14: Minimax: understanding duality
- Lec15: Averaging: projected gradient descent ascent
- Lec16: Extragradient: faster under smoothness
- Lec17: Splitting: exploiting structure
- Lec20: Randomized Smoothing: simulating gradient

#### Generative Adversarial Networks

$$\min_{\theta} \max_{\varphi} \hat{\mathsf{E}} \log S_{\varphi}(\mathbf{x}) + \hat{\mathsf{E}} \log(1 - S_{\varphi} \circ T_{\theta}(\mathbf{z}))$$



I. Goodfellow et al. (2014). "Generative Adversarial Nets". In: NIPS.

#### Generative Adversarial Networks



I. Goodfellow et al. (2014). "Generative Adversarial Nets". In: NIPS.



# Plan III: Exotic



#### • Lec06: Conditional Gradient: model weights quantization

Lec09: Metric Gradient: model gradient quantization

• Lec08: Mirror Descent: gradient under non-Euclidean geometry

# Plan III: Exotic



- Lec06: Conditional Gradient: model weights quantization
- Lec09: Metric Gradient: model gradient quantization
- Lec08: Mirror Descent: gradient under non-Euclidean geometry

# Plan III: Exotic



- Lec06: Conditional Gradient: model weights quantization
- Lec09: Metric Gradient: model gradient quantization
- Lec08: Mirror Descent: gradient under non-Euclidean geometry

## History Goes A Long Way Back

"Nothing in the world takes place without optimization, and there is no doubt that all aspects of the world that have a rational basis can be explained by optimization methods." — Leonhard Euler, 1744

### History Goes A Long Way Back

"Nothing in the world takes place without optimization, and there is no doubt that all aspects of the world that have a rational basis can be explained by optimization methods." — Leonhard Euler, 1744

"Every year I meet Ph.D. students of different specializations who ask me for advice on reasonable numerical schemes for their optimization models. And very often they seem to have come too late. In my experience, if an optimization model is created without taking into account the abilities of numerical schemes, the chances that it will be possible to find an acceptable numerical solution are close to zero. In any field of human activity, if we create something, we know in advance why we are doing so and what we are going to do with the result." — Yurii Nesterov

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits.
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits.
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

'There are no stupid questions, only stupid answers."

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

'There are no stupid questions, only stupid answers.'

<sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

#### "There are no stupid questions, only stupid answers."

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

#### "There are no stupid questions, only stupid students."

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

- On average, no algorithm is better than any other<sup>1</sup>
- In general, optimization problems are unsolvable<sup>2</sup>
- Implications:
  - don't try to solve all problems; one (class) at a time!
  - "efficient optimization methods can be developed only by intelligently employing the structure of particular instances of problems"
  - know your algorithms and their limits
  - be open to the impossible

#### "There are no inferior algorithms, only inferior engineers."

<sup>&</sup>lt;sup>1</sup>D. H. Wolpert and W. G. Macready (1997). "No free lunch theorems for optimization". *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82.

<sup>&</sup>lt;sup>2</sup>K. G. Murty and S. N. Kabadi (1987). "Some NP-complete problems in quadratic and nonlinear programming". *Mathematical Programming*, vol. 39, no. 2, pp. 117–129.

