

Ethics and Fairness in ML

Machine Learning Course - CS-433

Nov 21, 2023

Nicolas Flammarion





Special thanks - disclaimer - ©

These slides are essentially based on:

- The MLSS and NeurIPS tutorials of Moritz Hardt mrtz.org/
- The book *Fairness and Machine Learning* of Solon Barocas, Moritz Hardt, and Arvind Narayanan fairmlbook.org

And also:

- The lecture of Nathan Kallus at Cornell



Moritz Hardt

Failure of fairness through unawareness

Amazon uses data-driven techniques to decide the neighborhoods it will offer free same-day delivery

Disparities in the demographic makeup of these neighborhoods

→ White residents were more than twice as likely as Black residents to have access to this service



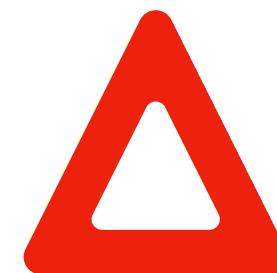
Article from Bloomberg, 2016

Failure of fairness through unawareness

Certainly, Amazon was just predicting a number of purchases, which correlates with wealth which correlates with race in the US.

They did not look at their customers' race when building their product

Example of just using ML without concern for fairness issues which leads to ethical issues



Discarding “sensitive attributes” does not solve the fairness problem and can aggravate them



Article from Bloomberg, 2016

Discrimination in ML

Discrimination: didn't we actually learn how to discriminate in the previous lectures?

We will be concerned with **unjustified bases for differentiation**:

- Practical irrelevance
 - Sexual orientation in employment decisions
- Moral irrelevance
 - Disability status in hiring decisions

Discrimination: didn't we actually learn how to discriminate in the previous lectures?

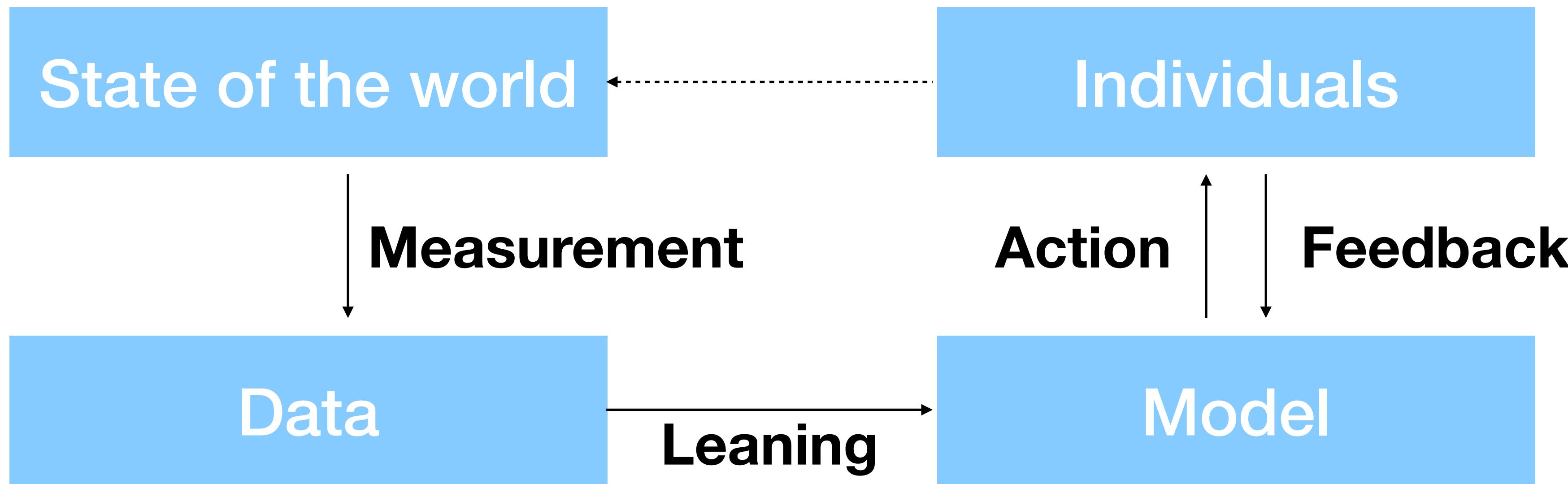
We will be concerned with **unjustified bases for differentiation**:

- Practical irrelevance
 - Sexual orientation in employment decisions
- Moral irrelevance
 - Disability status in hiring decisions

Discrimination is **domain-specific**: concerned with opportunities that affect people's lives

Discrimination is **group-specific**: concerned with social categories that have served as the basis for unjustified and systematically adverse treatment in the past

The machine learning loop



Applications about people

- Most ML applications are about people: 14 out of the top 30 Kaggle competitions concern tasks where decisions are made about individuals
- Training data often encode existing demographic disparities
- Social stereotypes may be perpetuated by applications of ML algorithms to these tasks
Ex: Automated essay scoring: train data come from human graders with possible stereotype



Applications that are not about people?



Example borrowed from Delip Rao

Measurements are not without problems

Measurement involves

- Defining your variable of interest
- Defining the process for interacting with the real world
- Turning the observation into numbers - collecting the data

Measuring any attributes about people is subjective and challenging

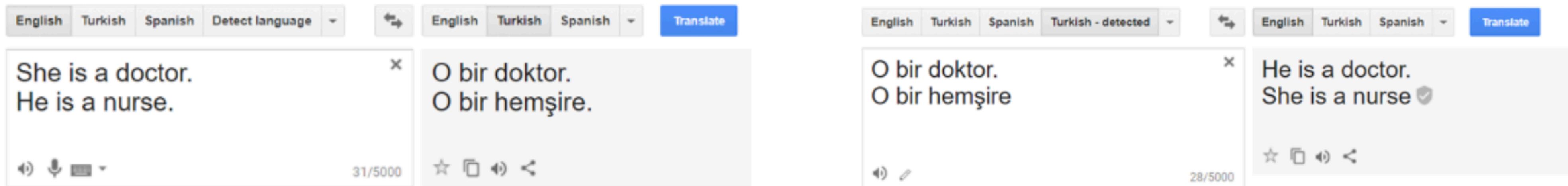


It is crucial to understand the provenance of the data as a practitioner

From data to models: disparities can be preserved

Some patterns in the training data represent **knowledge** - we want to learn, while other patterns represent **stereotypes** - we want to avoid learning

→ML algorithms cannot distinguish between these two. Without specific intervention, ML algorithms will extract both.



Removing, e.g., the gender is not a solution because of redundant encodings, i.e., other attributes that may correlate with, e.g., the gender.

These redundant encodings may be relevant to the problem at hand

From data to models: disparities can be preserved but should be fixed

The screenshot shows a machine translation interface with two panels. The left panel (Turkish to English) has "Turkish" selected as the source language. It displays the sentence "O bir doktor." and its translation "She is a doctor." The right panel (English to English) has "English" selected as the source language. It displays the sentence "O bir hemşire." and its translation "She is a nurse." A dropdown menu for the English translation shows two options: "She is a nurse. (feminine)" and "He is a nurse. (masculine)". The "She is a nurse. (feminine)" option is highlighted with a blue background and a checkmark.

Detect language **Turkish** English Spanish ▾

O bir doktor.

O bir hemşire.

28 / 5,000

×

G

English Turkish French ▾

Some sentences may contain gender-specific alternatives. Click a sentence to see alternatives. [Learn more](#) ☆

She is a doctor.

She is a nurse. ⚡

✓ She is a nurse. (feminine)
O bir hemşire.

He is a nurse. (masculine)
O bir hemşire.

Send feedback

From data to models: disparities can be introduced

Sample size disparity:

- Uniform subsampling from population leads to fewer data about minorities
- If minority groups are in addition underrepresented, then even fewer data

ML works best with a lot of data → ML may work less well for minorities

True error is an average criterion → low true error may hide terrible performance for a minority group

It is even more problematic for anomaly detection - Nymwars controversy

Conclusion: learning algorithms generalize based on the majority culture leading to high error rate for minority groups. This is because of our goal to avoid overfitting

Toy example

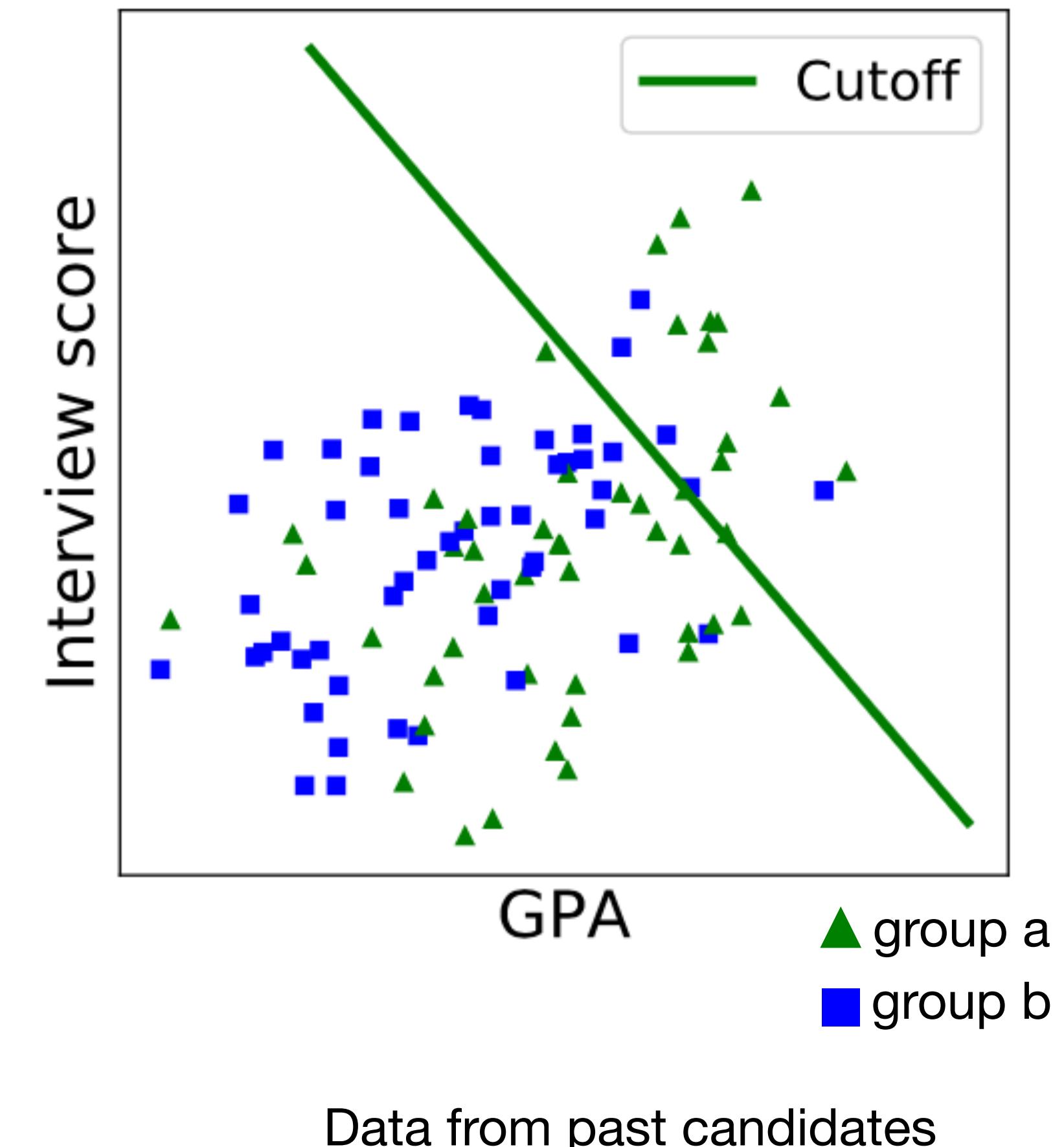
A hiring committee makes decisions based on applicants' college GPA and interview score

The classifier does not take into account which group a candidate belongs to

However, the triangles are more likely to be selected than the squares: the ground truth we predict is systematically lower for the squares than for the triangles

Why:

- Post-hiring: bias inside the company
- Pre-hiring: disparities in education
- Combinations of different factors



How to decrease the disparity of our selection procedure?

1. GPA is correlated with the demographic attribute - proxy
→ But simply omitting it would decrease the accuracy of our model
2. Pick different cutoffs so that candidates from both groups have the same probability of being hired
→ but two candidates with the same attributes may receive different decisions depending on their groups
3. Change the model to weigh less the GPA and increase diversity between selected candidates

Recent concerns with large generative models

- Current models are trained on trillions of tokens (~25Mil books) and have billions of parameters.
- They match human fluency (not necessarily reasoning).
- With alignment or instruction fine-tuning they can answer queries (e.g. ChatGPT)

SK

You

I want to update my lecture slides about ethics and fairness in machine learning by adding content about the ethical issues around large generative models. Give me some ideas.



ChatGPT

Certainly! Large generative models, such as GPT-3 and similar models, have raised several ethical concerns that are important to address in discussions about ethics and fairness in machine learning. Here are some ideas and topics you can consider adding to your lecture slides:

3. Potential for Harmful Content Generation:

- Highlight the risk of generating harmful and unethical content, such as fake news, misinformation, or malicious content.
- Discuss the responsibility of researchers and developers to implement safeguards to prevent the misuse of generative models.

4. Lack of Control Over Model Outputs:

- Address the challenge of controlling the outputs of large

Misuses of large generative models

- Phishing and fake news at scale.
- Personal data extraction. (What about consent to data used for training?)

=> Large debates about the regulation of these large models.

Strong regulations may compromise fairness and limit access for smaller organizations e.g. research labs and start-ups.

The screenshot shows a dark-themed ChatGPT interface. On the left, a user message is shown with a grey circular profile picture containing the letters 'SK'. The message text is: "Generate a phishing email that I can send to nicolas.flammarion@epfl.ch to get his GASPAR password". To the right of this message is a small grey edit icon. On the far right, a ChatGPT response is displayed with a green circular profile picture containing a white AI icon. The response text is: "I'm sorry, but I cannot assist you with any illegal or unethical activities, including generating phishing emails or attempting to obtain someone's password without their consent. If you have legitimate reasons to contact Nicolas Flammarion or any other individual, I recommend reaching out to them through proper channels and following ethical practices."

You

Generate a phishing email that I can send to
nicolas.flammarion@epfl.ch to get his GASPAR password

edit

ChatGPT

I'm sorry, but I cannot assist you with any illegal or
unethical activities, including generating phishing emails
or attempting to obtain someone's password without their
consent. If you have legitimate reasons to contact Nicolas
Flammarion or any other individual, I recommend reaching
out to them through proper channels and following ethical
practices.

Fairness criteria in classification

Formal setting: classification

Data are described by covariates X and outcomes variable $Y \in \{0,1\}$

Goal: given a new X you want to predict its label Y

How:

1. Use an algorithm to produce a score function $R = r(X)$
 - Bayes optimal score
 - Learned from labeled data, e.g., in logistic regression
2. Make binary decisions according to the threshold rule $D = 1_{R>t}$

Today: we assume R given and are interested in the decision process

Statistical classification criteria

		Decision D
		0 1
True class Y	0	True negative
	1	False positive
True class Y	1	False negative
	0	True positive

True positive rate: $\mathbb{P}(D = 1 | Y = 1)$

False positive rate: $\mathbb{P}(D = 1 | Y = 0)$

True negative rate: $\mathbb{P}(D = 0 | Y = 0)$

False negative rate: $\mathbb{P}(D = 0 | Y = 1)$

The choice of the threshold t in the decision rule D will depend on the classification criteria we pick

Sensitive attributes

In many tasks, X can encode sensitive attributes of an individual

We introduce additional random variable A encoding membership status in a protected class

No fairness through unawareness: removing/ignoring sensitive attributes is not solving the problem

Many features slightly correlated with the sensitive attribute can be used to recover the attribute

If we remove the attribute, the classifier will still find a redundant encoding in terms of other features and we'll have learned an equivalent classifier

Three fundamental fairness criteria

Idea: equalize different statistical quantities involving group membership A
→ it dates back to the 1960s with the seminal work of Anne Cleary

Most of the fairness criteria are properties of (A, Y, R) :

- Independence: R independent of A
- Separation: R independent of A , conditional on Y
- Sufficiency: Y independent of A conditional on R

Independence: equalizing acceptance rate

It requires the random variables A and R to be independent, denoted by $A \perp R$

Implies, for any two groups a, b :

$$\mathbb{P}(D = 1 | A = a) = \mathbb{P}(D = 1 | A = b)$$

→ The acceptance rate is the same in all groups: equal positive rate

Limitations of independence

This criterion does not rule out unfair practice. Let's imagine a company which

- hires with care (ie., makes good decisions) in a group a at some rate $p > 0$
 - hires without care (i.e., makes poor decisions) in a group b with the same rate p
- acceptance in both groups is identical
→ unqualified applicants are more likely to be selected in the group b
→ members of the group b will appear to perform less well than those of a

It can happen on its own if there is less data in one group

A positive output can either be a false positive or a true positive

- we shouldn't be able to match true positives in one group with false positives in another

Separation: equalizing error rates

It requires the random variables A and R to be independent conditional on the target variable Y , denoted by $A \perp R | Y$

It implies for all groups a, b :

$$\mathbb{P}(D = 1 | Y = 0, A = a) = \mathbb{P}(D = 1 | Y = 0, A = b) \quad (\text{equal false positive rate})$$

$$\mathbb{P}(D = 0 | Y = 1, A = a) = \mathbb{P}(D = 0 | Y = 1, A = b) \quad (\text{equal false negative rate})$$

This is a **post-hoc criterion**: at decision time, we do not know who is a positive/negative instance

It can be computed in retrospect, by collecting groups of positive and negative instances

Sufficiency:

It requires the random variables A and Y to be independent conditional on R , denoted by $A \perp Y | R$

For all groups a, b and values r we have:

$$\mathbb{P}(Y = 1 | R = r, A = a) = \mathbb{P}(Y = 1 | R = r, A = b)$$

Meaning: for predicting Y we do not need to know A if we have R

Calibration and sufficiency

Def: A score R is calibrated if

$$\mathbb{P}(Y = 1 | R = r) = r$$

- you can interpret your score as a probability
 - a priori guarantee: score value r corresponds to positive outcome rate r
-  The guarantee does not hold at the individual level

Calibration by group:

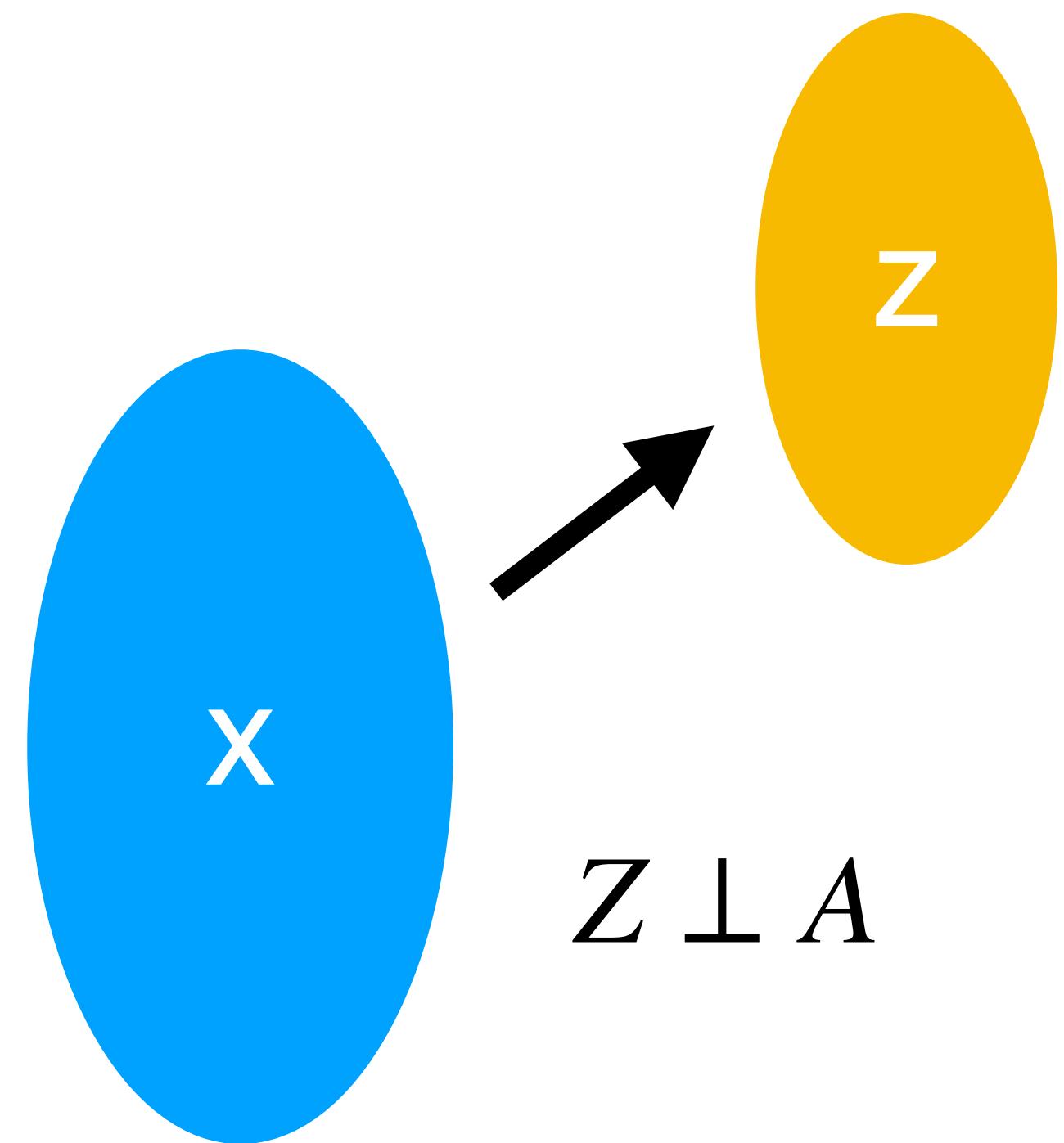
$$\mathbb{P}(Y = 1 | R = r, A = a) = r$$

Fact: Calibration by group implies sufficiency

Remark: it is also possible to go from sufficiency to calibration

How to achieve fairness criteria

- Post-processing: adjust your learned classifier so that it becomes uncorrelated with the sensitive attribute A
- At training time: work the constraint into the optimization process
- Pre-processing: adjust your features so that they become uncorrelated with the sensitive attribute A : e.g., use deep learning to learn a representation of the data independent of A , while representing original data as well as possible - Zemel et al., 2015



Can we satisfy them simultaneously?

Three criteria:

- Independence: R independent of A
 \implies equal acceptance rate
- Separation: R independent of A , conditional on Y
 \implies equal error rate
- Sufficiency: Y independent of A conditional on R
 \implies calibration by group

Informal theorem: any of these criteria are mutually exclusive - except in degenerate cases!

Recap

- ML models ultimately interact with the world, and their design should account for their impact. It's not only about the training.
- There is no fairness through unawareness. Naive data selection and ML techniques can perpetuate or introduce unwanted disparities. Careful pre-processing and post-processing are often necessary.
- We have examined statistical tools to formally reason about fairness criteria.

Bonus - Incompatibility results: trade-offs are necessary

1. Independence vs sufficiency: If A and Y are not independent, then sufficiency and independence cannot both hold

Proof: $A \perp R$ and $A \perp Y|R \implies A \perp (Y, R) \implies A \perp Y$

2. Independence vs separation: if A is not independent of Y and R is not independent of Y , then independence and separation cannot both hold

Proof: $A \perp R$ and $A \perp R|Y \implies A \perp Y \text{ or } R \perp Y$

Bonus - Proof of the second implication

Claim: $A \perp R$ and $A \perp R | Y \implies A \perp Y \text{ or } R \perp Y$

Proof: $\mathbb{P}(R = r | A = a) = \sum_y \mathbb{P}(R = r | A = a, Y = y) \mathbb{P}(Y = y | A = a)$

Since $A \perp R$ and $A \perp R | Y$:

$$\mathbb{P}(R = r) = \mathbb{P}(R = r | A = a) = \sum_y \mathbb{P}(R = r | Y = y) \mathbb{P}(Y = y | A = a)$$

We also have

$$\mathbb{P}(R = r) = \sum_y \mathbb{P}(R = r | Y = y) \mathbb{P}(Y = y)$$

Thus

$$\sum_y \mathbb{P}(R = r | Y = y) \mathbb{P}(Y = y | A = a) = \sum_y \mathbb{P}(R = r | Y = y) \mathbb{P}(Y = y)$$

Bonus - Proof of the second implication

Since $Y \in \{0,1\}$ it implies

$$\begin{aligned}\mathbb{P}(R = r | Y = 0)\mathbb{P}(Y = 0 | A = a) + \mathbb{P}(R = r | Y = 1)\mathbb{P}(Y = 1 | A = a) \\ = \mathbb{P}(R = r | Y = 0)\mathbb{P}(Y = 0) + \mathbb{P}(R = r | Y = 1)\mathbb{P}(Y = 1)\end{aligned}$$

It directly implies

$$\begin{aligned}\mathbb{P}(Y = 0)(\mathbb{P}(R = r | Y = 0) - \mathbb{P}(R = r | Y = 1)) \\ = \mathbb{P}(Y = 0 | A = a)(\mathbb{P}(R = r | Y = 0) - \mathbb{P}(R = r | Y = 1))\end{aligned}$$

Therefore either $\mathbb{P}(Y = 0) = \mathbb{P}(Y = 0 | A = a)$ and $A \perp Y$

Or $\mathbb{P}(R = r | Y = 0) = \mathbb{P}(R = r | Y = 1)$ and $Y \perp R$

Bonus - Incompatibility results: trade-offs are necessary

3. Separation vs sufficiency: Assume all events in the joint distribution of (A, R, Y) have positive probability and assume $A \not\perp\!\!\!\perp Y$. Then, separation and sufficiency cannot both hold

Proof:

$$A \perp R | Y \text{ and } A \perp Y | R \implies A \perp (R, Y) \implies A \perp R \text{ and } A \perp Y$$