Advanced Machine Learning

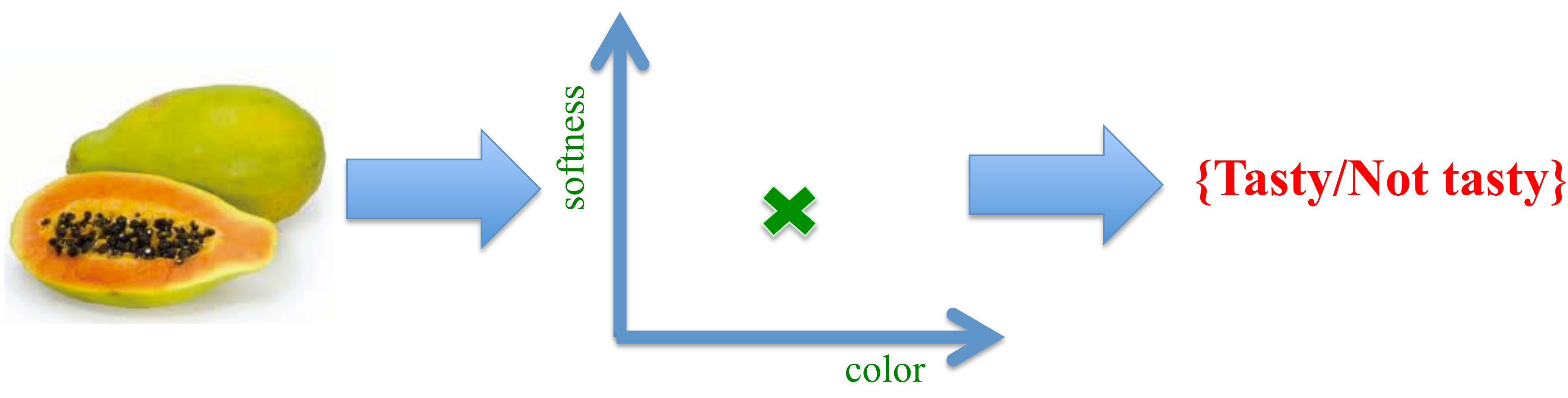
Bogdan Alexe,

bogdan.alexe@fmi.unibuc.ro

University of Bucharest, 2^{nd} semester, 2021-2022

Recap

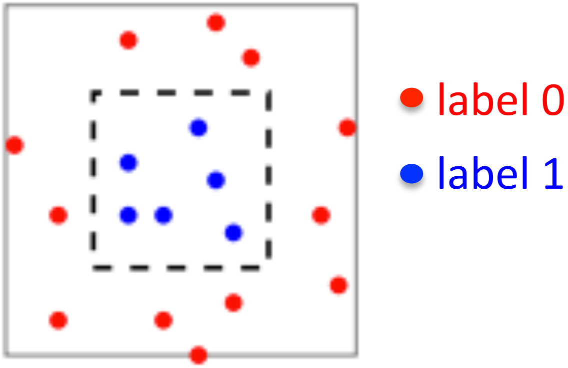
- A Formal Model – The Statistical learning framework
  - papaya tasting learning scenario, classification task: tasty – label 1, not tasty – label 0
  - domain set $\mathcal{X}$, label set $\mathcal{Y}$, training data S, prediction rule $h : \mathcal{X} \to \mathcal{Y}$
  - empirical error, generalization error
  - data generation model: i.i.d + realizability (there exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$)



Recap

- Empirical Risk Minimization
  - learning paradigm that returns a predictor *h* that minimizes the empirical error on sample S
  - might overfit: small error on the training data, large error on the other samples

$$h_S(x) = \begin{cases} y_i & \text{if } \exists i \in [m] \text{ s.t. } x_i = x \\ 0 & \text{otherwise.} \end{cases}$$



  - $L_S(h_S) = 0$, but $L_{\mathcal{D},f}(h_S) = ½$ (h predicts the label 1 on a finite number of instances)
  - inductive bias: use prior knowledge and choose a hypothesis class $\mathcal{H} \subset \mathcal{Y}^{\mathcal{X}}$
  - apply the ERM learning paradigm over $\mathcal{H}$

Recap

- Probably Approximately Correct learning
  - can only be approximately correct: happy to find h_S with $L_{(\mathcal{D},f)}(h_S) \leq \varepsilon$, where $\varepsilon \in (0, 1)$ is the accuracy parameter, user-specified
  - can only be probably correct: allow the algorithm to fail with probability δ, where $\delta \in (0, 1)$ is the confidence parameter, user-specified
  - definition of PAC learnability of hypothesis class $\mathcal{H}$ in the realizability case

PAC learnability of a class $\mathcal{H}$

A hypothesis class $\mathcal{H}$ is called ***PAC learnable*** if:

There exists a learning algorithm A with the property that given enough samples m $\geq m_{\mathcal{H}}(\varepsilon, \delta)$ drawn i.i.d. from $\mathcal{D}$ and labeled by f, if the realizability assumption holds wrt. $\mathcal{H}$, $\mathcal{D}$, f (there exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$) then with probability 1 - δ it will return a hypothesis h_S from $\mathcal{H}$ that has an error smaller than ε:

$$\underset{S\sim D^m}{P}(L_{D,f}(h_S) \leq \varepsilon) \geq 1-\delta$$

$$\underset{S\sim D^m}{P}(L_{D,f}(h_S) \leq \varepsilon) \geq 1-\delta \Leftrightarrow \underset{S\sim D^m}{P}(L_{D,f}(h_S) > \varepsilon) < \delta$$

PAC learnability of a class $\mathcal{H}$

A hypothesis class $\mathcal{H}$ is called ***PAC learnable*** if there exists a function $m_{\mathcal{H}}: (0,1)^2 \rightarrow N$ and a learning algorithm A with the following property:

- for every $\varepsilon > 0$ (*accuracy* → *"approximately correct"*)
- for every $\delta > 0$ (*confidence* → *"probably"*)
- for every labeling $f \in \mathcal{H}$
- for every distribution $\mathcal{D}$ over $\mathcal{X}$

if the realizability assumption holds wrt. $\mathcal{H}$, $\mathcal{D}$, f (there exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$),when we run the learning algorithm A on a training set S, consisting of $m \geq m_{\mathcal{H}}(\varepsilon, \delta)$ examples sampled i.i.d. from $\mathcal{D}$ and labeled by f the algorithm A returns a hypothesis $h_S \in \mathcal{H}$ such that, with probability at least $1-\delta$ (over the choice of examples), $L_{D,f}(h_S) \leq \varepsilon$.

$$\underset{S \sim D^m}{P}\left(L_{D,f}(h_S) \leq \varepsilon\right) \geq 1 - \delta$$

- $h_S = A(S)$
- the function $m_{\mathcal{H}}: (0,1)^2 \rightarrow N$ is called sample complexity of learning $\mathcal{H}$
- $m_{\mathcal{H}}(\varepsilon, \delta)$ – the minimum number of examples required to guarantee a PAC solution

L. G. Valiant, *A theory of the Learnable*, Communications ACM, 27(11):1134-1142, 1984

PAC learnability of a class $\mathcal{H}$

A hypothesis class $\mathcal{H}$ is called ***PAC learnable*** if there exists a function $m_{\mathcal{H}}: (0,1)^2 \rightarrow N$ and a learning algorithm A with the following property:

- for every $\varepsilon > 0$ (*accuracy* → "*approximately correct*")
- for every $\delta > 0$ (*confidence* → "*probably*")
- for every labeling $f \in \mathcal{H}$
- for every distribution $\mathcal{D}$ over $\mathcal{X}$

if the realizability assumption holds wrt. $\mathcal{H}$, $\mathcal{D}$, f (there exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$),when we run the learning algorithm A on a training set S, consisting of $m \geq m_{\mathcal{H}}(\varepsilon, \delta)$ examples sampled i.i.d. from $\mathcal{D}$ and labeled by f the algorithm A returns a hypothesis $h_S \in \mathcal{H}$ such that, with probability at least $1-\delta$ (over the choice of examples), $L_{D,f}(h_S) \leq \varepsilon$.

$$\underset{S \sim D^m}{P}\left(L_{D,f}(h_S) \leq \varepsilon\right) \geq 1-\delta \Leftrightarrow \underset{S \sim D^m}{P}\left(L_{D,f}(h_S) > \varepsilon\right) < \delta$$

L. G. Valiant, *A theory of the Learnable*, Communications ACM, 27(11):1134-1142, 1984

PAC learnability of a class $\mathcal{H}$

A hypothesis class $\mathcal{H}$ is called ***PAC learnable*** if:

If the realizability assumption holds, I can find a hypothesis h from $\mathcal{H}$ based on the learning algorithm A with:

- whatever accuracy $\varepsilon > 0$ I want
- whatever confidence $\delta > 0$ I want
- whatever the distribution $\mathcal{D}$ is
- whatever the labeling function f is

given that I provide to A enough samples $m \geq m_{\mathcal{H}}(\varepsilon, \delta)$ drawn from $\mathcal{D}$ then we have:

$$\underset{S \sim D^m}{P}\left(L_{D,f}(h_S) \leq \varepsilon\right) \geq 1 - \delta$$

Learning finite classes

Theorem:
Finite hypothesis classes $\mathcal{H}$ are PAC-learnable.

Idea of the proof

- a bad predictor h_b has $L_{\mathrm{D},f}\,(h_b) > \varepsilon$
- h_b can be output by the $ERM_{\mathcal{H}}$ learning paradigm if has zero empirical error: $L_{\mathrm{S}}\,(h_b) = 0$
- this can happen if h_b labels correctly all the m training examples from S i.i.d from $\mathcal{D}$
- given a random example from $\mathcal{D}$, h_b has < 1-ε probability to label it correctly
- h_b labels correctly all the m training examples from S with probability $< (1-\varepsilon)^m \leq e^{-\varepsilon m}$
- there are at most $|\mathcal{H}|$ bad hypthotesis, so consider $|H| \times e^{-\varepsilon m} \leq \delta$, so take $m \geq \dfrac{\log(|\mathcal{H}|/\delta)}{\epsilon}$

Sample complexity

- the function $m_{\mathcal{H}}: (0,1)^2 \rightarrow N$ is called sampled complexity of learning $\mathcal{H}$

- $m_{\mathcal{H}}$ (ε, δ) – the minimum number of examples required to guarantee a PAC solution

- depends on:
  - accuracy ε
  - confidence δ
  - properties of $\mathcal{H}$

- different than *time complexity* (discuss it in the following lectures)

Every finite hypothesis class H is PAC learnable with sample complexity

$$m_{\mathcal{H}}(\epsilon, \delta) \leq \left\lceil \frac{\log(|\mathcal{H}|/\delta)}{\epsilon} \right\rceil$$

Concept class

- h: $\mathcal{X} \rightarrow \{0,1\}$ the *target concept* to learn
  - can be identified with its support $\{x \in \mathcal{X} \mid h(x) = 1\}$
  - set of points inside a rectangle
    - h = indicator function of these points
    - the concept to learn is a rectangle

- $\mathcal{H}$ can be interpreted as the concept class, a set of target concepts h
  - set of all rectangles in the plane
  - conjunction of Boolean literals

Conjunctions of Boolean literals

- C_n = concept class of conjunctions of at most n Boolean literals $x_1, \ldots, x_n$
  - a Boolean literal is either x_i or its negation $\overline{x_i}$
  - can interpret x_i as feature i
  - example: $h = x_1 \wedge \overline{x_2} \wedge x_4$ where $\overline{x_2}$ denotes the negation of the Boolean literal x_2

- observe that for n = 4:
  - a positive example such as (1, 0, 0, 1) implies that the target concept cannot contain the literals $\overline{x_1}$, x_2, x_3 and $\overline{x_4}$
    - for example if x_2 was present in the conjunction then for the current positive example (where x_2 has value 0) the label should have been 0
  - cannot say anything about literals x_1, $\overline{x_2}$, $\overline{x_3}$ and x_4. They might be present or absent in the conjunction (target concept) that we are searching for
  - the first positive example eliminates half of the literals

  - in contrast, a negative example such as (1, 0, 0, 0) is not as informative since it is not known which of its n bits are incorrect.

Conjunctions of Boolean literals

- C_n = concept class of conjunctions of at most n Boolean literals $x_1, \ldots, x_n$
- a simple algorithm for finding a consistent hypothesis is thus based on positive examples and consists of the following:
  - for each positive example $(b_1, \ldots b_n)$,
    - if $b_i = 1$ then $\overline{x_i}$ is ruled out as a possible literal in the concept class
    - if $b_i = 0$ then x_i is ruled out.
  - the conjunction of all the literals not ruled out is thus a hypothesis consistent with the target

0	1	1	0	1	1	+
0	1	1	1	1	1	+
0	0	1	1	0	1	-
0	1	1	1	1	1	+
1	0	0	1	1	0	-
0	1	0	0	1	1	+

$x_1 \;\; \overline{x_1} \;\; x_2 \;\; \overline{x_2} \;\; x_3 \;\; \overline{x_3} \;\; x_4 \;\; \overline{x_4} \;\; x_5 \;\; \overline{x_5} \;\; x_6 \;\; \overline{x_6}$

$\rightarrow \overline{x}_1 \wedge x_2 \wedge x_5 \wedge x_6$

Conjunctions of Boolean literals

- C_n = concept class of conjunctions of at most n Boolean literals $x_1, \ldots, x_n$
- $|C_n| = 3^n$, finite, so is PAC learnable with sample complexity $m_{\mathcal{H}}(\varepsilon, \delta) \leq m$:

$$m \geq \frac{\log(|\mathcal{H}|/\delta)}{\epsilon}$$

$$m \geq \left\lceil \frac{1}{\varepsilon}\left(n\log(3) + \log(\frac{1}{\delta})\right)\right\rceil$$

$$m \geq \left\lceil \frac{1}{\varepsilon}\left(n\log(3) - \log(\delta)\right)\right\rceil$$

- for $\varepsilon = 0.01$, $\delta = 0.02$, $n = 10$, $m \geq 149$, no matter how $\mathcal{D}$ looks like, all possible examples are $2^{10} = 1024$
- we need at least 149 examples; the bound guarantees (at least) 99% accuracy with (at least) 98% confidence

Universal concept class $\mathcal{U}_n$

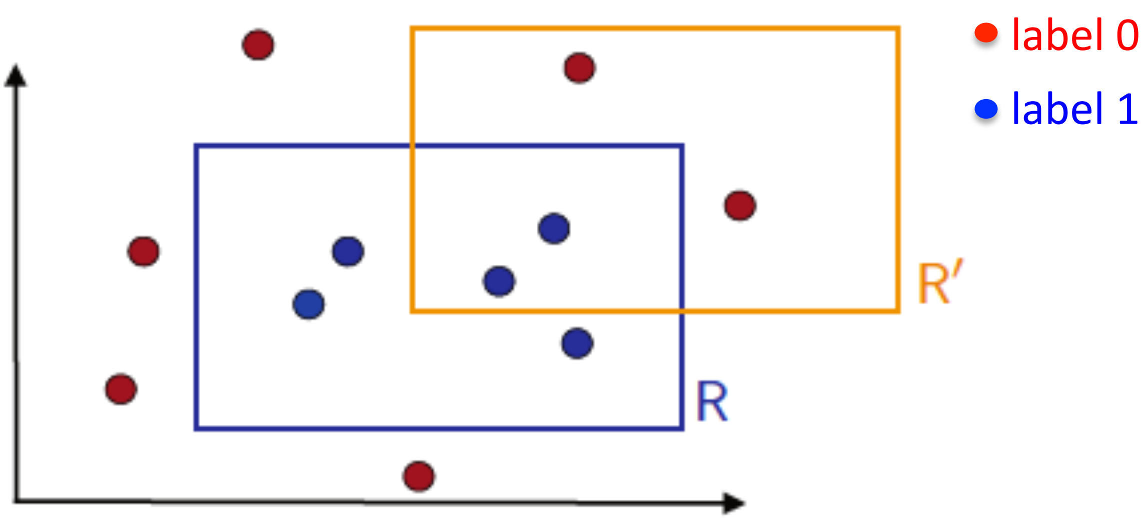
- B^n = set of boolean n-tuples, $|B| = 2^n$
- want to learn arbitrary subsets of B^n
- $\mathcal{U}_n = \{h: B^n \to \{0,1\}\}$ - the concept class formed by all subsets of B^n
- $\mathcal{U}_n$ – universal class
- is this concept class PAC-learnable?
- $|\mathcal{U}_n| = 2^{2^n}$ – finite, so is PAC learnable with $m_{\mathcal{H}}(\varepsilon, \delta)$ in the order of m:

$$m \geq \left\lceil \frac{1}{\varepsilon}\left(2^n \log(2) + \log(\frac{1}{\delta})\right)\right\rceil$$

- sample complexity exponential in n, number of variables
- $\mathcal{U}_n$ is finite and hence PAC-learnable, but we will need exponential time (to inspect exponentially many examples)
- for $\varepsilon = 0.01$, $\delta = 0.02$, $n = 10$, $m \geq 71370$, no matter how $\mathcal{D}$ looks like, all possible examples are $2^{10} = 1024$
- it is not PAC-learnable in any practical sense (need polynomial time complexity = later require $m_{\mathcal{H}}$ be polynomial in $1/\varepsilon, 1/\delta, n$)

Axis-aligned rectangles

- $\mathcal{X} = \mathrm{R}^2$ points in the plane
- $\mathcal{H}$ = set of all axis-aligned rectangle lying in R^2
- each concept $h \in \mathcal{H}$ is an indicator function of a rectangle
- the learning problem consists of determining with small error a target axis-aligned rectangle using the labeled training sample



Target concept R and possible hypothesis R′. Circles represent training instances. A blue circle is a point labeled with 1, since it falls within the rectangle R. Others are red and labeled with 0.

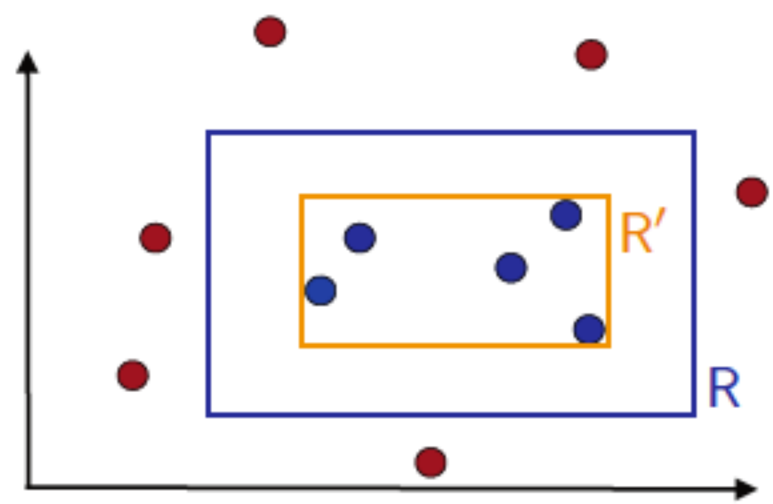
Axis-aligned rectangles

- $\mathcal{X} = \mathrm{R}^2$ points in the plane
- $\mathcal{H}$ = set of all axis-aligned rectangle lying in R^2
- $|\mathcal{H}| = \infty$
- still $\mathcal{H}$ is PAC-learnable with sample complexity in the order of:

$$m \geq \left\lceil \frac{4}{\varepsilon} \log(\frac{1}{\delta}) \right\rceil$$

- simple algorithm: take the tightest rectangle enclosing all the positive examples (or take the largest rectangle not including negative samples)

- discuss this example in seminar



The general PAC model

Relaxing the realizability assumption – Agnostic PAC learning

- so far we assumed that labels are generating by some labeling function f
  - f is a function: the features fully determines the label (two papayas with the same color and softness will have the same label)
- the realizability assumption holds wrt. $\mathcal{H}$, $\mathcal{D}$, f (there exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$)
  - h^* is in $\mathcal{H}$, e.g. there is a rectangle in the color-softness space that with probability 1 determines the labels of papayas

- this assumption may be too strong

- relax the realizability assumption by replacing the "target labeling function" with a more flexible notion, a data-labels generating distribution.
  - f might not be a function
  - there might not exists $h^* \in \mathcal{H}$ such that $L_{\mathcal{D},f}(h^*) = 0$

Relaxing the realizability assumption – Agnostic PAC learning

- recall: in the PAC model, $\mathcal{D}$ is a distribution over $\mathcal{X}$
  - if example *x* appears in the training data it has a fixed label

- consider from now on that $\mathcal{D}$ is a distribution over $\mathcal{X} \times \mathcal{Y}$
  - if example *x* appears in the training data it might have a different label

- redefine the risk = generalization error as:

$$L_{\mathcal{D}}(h) \stackrel{\text{def}}{=} \mathop{\mathbb{P}}_{(x,y)\sim\mathcal{D}}[h(x) \neq y] \stackrel{\text{def}}{=} \mathcal{D}(\{(x,y) : h(x) \neq y\})$$

- redefine the "approximately correct" notion to:

$$L_{\mathcal{D}}(A(S)) \leq \min_{h\in\mathcal{H}} L_{\mathcal{D}}(h) + \epsilon$$

$A(S) = h_S$ is ε-accurate wrt $\mathcal{D}$, $\mathcal{H}$

PAC vs. Agnostic PAC learning

	PAC	Agnostic PAC

PAC vs. Agnostic PAC learning

	PAC	Agnostic PAC
Distribution	$\mathcal{D}$ over $\mathcal{X}$	$\mathcal{D}$ over $\mathcal{X} \times \mathcal{Y}$
Truth	$f \in \mathcal{H}$	not in class or doesn't exist
Risk	$L_{\mathcal{D},f}(h) =$ $\mathcal{D}(\{x : h(x) \neq f(x)\})$	$L_{\mathcal{D}}(h) =$ $\mathcal{D}(\{(x, y) : h(x) \neq y\})$
Training set	$(x_1, \ldots, x_m) \sim \mathcal{D}^m$ $\forall i,\ y_i = f(x_i)$	$((x_1, y_1), \ldots, (x_m, y_m)) \sim \mathcal{D}^m$
Goal	$L_{\mathcal{D},f}(A(S)) \leq \epsilon$	$L_{\mathcal{D}}(A(S)) \leq \min_{h \in \mathcal{H}} L_{\mathcal{D}}(h) + \epsilon$

The Bayes optimal predictor

- given any probability distribution $\mathcal{D}$ over $\mathcal{X} \times \{0,1\}$, the best label prediction function we can achieve is the Bayes rule:

$$f_{\mathcal{D}}(x) = \begin{cases} 1 & \text{if } \mathbb{P}[y=1|x] \geq 1/2 \\ 0 & \text{otherwise} \end{cases} \Leftrightarrow \mathcal{D}((x,1)|x) \geq ½$$

- for any probability distribution $\mathcal{D}$, the Bayes predictor $f_{\mathcal{D}}$ is optimal, in the sense that no other classifier $g\colon \mathcal{X} \rightarrow \{0,1\}$ has a lower error, $L_{\mathcal{D}}(f_{\mathcal{D}}) \leq L_{\mathcal{D}}(g)$ (seminar exercise)

- we don't know the probability distribution $\mathcal{D}$ that produces the data (x, y), we only see a sample S generated by $\mathcal{D}$

- so, we cannot utilize the Bayes optimal predictor $f_{\mathcal{D}}$

Beyond binary classification

Scope of learning problems

- multiclass classification: $\mathcal{Y}$ is finite representing $|\mathcal{Y}|$ different classes. E.g. $\mathcal{X}$ is documents and $\mathcal{Y} = \{\text{News, Sports, Biology, Medicine}\}$

- regression: Y = R. E.g. one wishes to predict the stock price tomorrow, the max temperature, a baby's birth weight based on ultrasound measure of his head circumference, abdominal circumference and femur length
  - what is fundamental difference to multiclass classification?
  - the loss suffered when making a bad prediction

Loss functions

- let $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$

- given hypothesis $h \in \mathcal{H}$ and an example z = $(x,y) \in \mathcal{Z}$, how good is h on (x,y)?
- loss function $\ell : \mathcal{H} \times \mathcal{Z} \rightarrow \mathrm{R}_+$
  - measures the error that model h does it on the instance $z = (x,y)$
  - the true risk (generalization error) of model h is: $L_{\mathcal{D}}(h) \stackrel{\text{def}}{=} \underset{z \sim \mathcal{D}}{\mathbb{E}}[\ell(h,z)]$

- example: 0-1 loss: $\ell(h,(x,y)) = \begin{cases} 1 & \text{if } h(x) \neq y \\ 0 & \text{if } h(x) = y \end{cases}$ binary class prediction, multiclass prediction

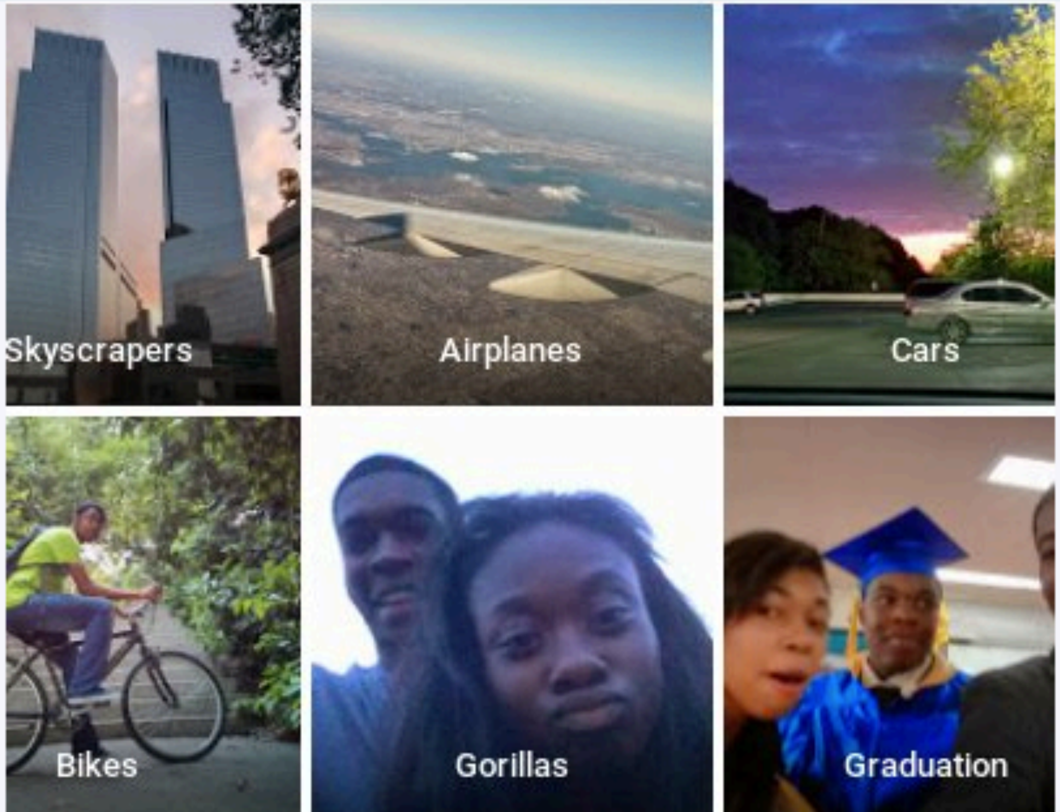
$$\mathrm{E}_{z\sim\mathcal{D}}[\ell(h, z)] = \mathrm{E}_{(x,y)\sim\mathcal{D}}[\ell(h, (x,y)] = \mathrm{E}_{(x,y)\sim\mathcal{D}}[0 \times 1_{[h(x) = y]} + 1 \times 1_{[h(x) \neq y]}] =$$
$$= \mathrm{E}_{(x,y)\sim\mathcal{D}}[1_{[h(x) \neq y]}] = \mathcal{D}(\{(x,y) |\ h(x) \neq y\}) = \mathrm{P}_{(x,y)\sim\mathcal{D}}(h(x) \neq y)$$

Loss functions

- let $\mathcal{Z} = \mathcal{X} \times \mathcal{Y}$
- given hypothesis $h \in \mathcal{H}$ and an example z = $(x,y) \in \mathcal{Z}$, how good is h on (x,y)?
- loss function $\ell : \mathcal{H} \times \mathcal{Z} \rightarrow \mathrm{R}_+$
  - measures the error that model h does it on the instance $z = (x,y)$
  - the true risk (generalization error) of model h is: $L_{\mathcal{D}}(h) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{z \sim \mathcal{D}}[\ell(h, z)]$
- example of other loss functions:

Squared loss: $\ell(h, (x, y)) = (h(x) - y)^2$
Absolute-value loss: $\ell(h, (x, y)) = |h(x) - y|$
Cost-sensitive loss: $\ell(h, (x, y)) = C_{h(x),y}$ where C is some $|\mathcal{Y}| \times |\mathcal{Y}|$ matrix

Cost-sensitive loss



I post from https://v2.jacky.wtf. FREE != safe.
@jackyalcine

Google Photos, y'all fucked up. My friend's not a gorilla.

♡ 2,362 3:22 AM - Jun 29, 2015

Cost-sensitive loss

GOOGLE TECH ARTIFICIAL INTELLIGENCE

Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech

Nearly three years after the company was called out, it hasn't gone beyond a quick workaround

By James Vincent | Jan 12, 2018, 10:35am EST

A spokesperson for Google confirmed to *Wired* that the image categories "gorilla," "chimp," "chimpanzee," and "monkey" remained blocked on Google Photos after Alciné's tweet in 2015. "Image labeling technology is still early and unfortunately it's nowhere near perfect," said the rep. The categories are still available on other Google services, though, including the Cloud Vision API it sells to other companies and Google Assistant.

Next time