

# Robustness Quantification

using imprecise probabilities to assess the reliability  
of probabilistic classifiers





Want more than  
just these slides?

You can watch  
the entire talk on  
YouTube!





# FLip

Foundations Lab for  
imprecise probabilities



GHENT  
UNIVERSITY







Adrián  
Detavernier



Rodrigo  
Lassance



MACHINE  
LEARNING

IMPRECISE  
PROBABILITIES





Adrián  
Detavernier



Rodrigo  
Lassance



MACHINE  
LEARNING

IMPRECISE  
PROBABILITIES

ROBUSTNESS  
QUANTIFICATION





Adrián  
Detavernier



Rodrigo  
Lassance



MACHINE  
LEARNING

IMPRECISE  
PROBABILITIES

**PROBLEM 1:**

**MACHINE  
LEARNING**

**... is unreliable**





media saying AI will  
take over the world



my neural network:

Dog

# CLASSIFICATION

features  $x$

FEATURES

photo

medical data

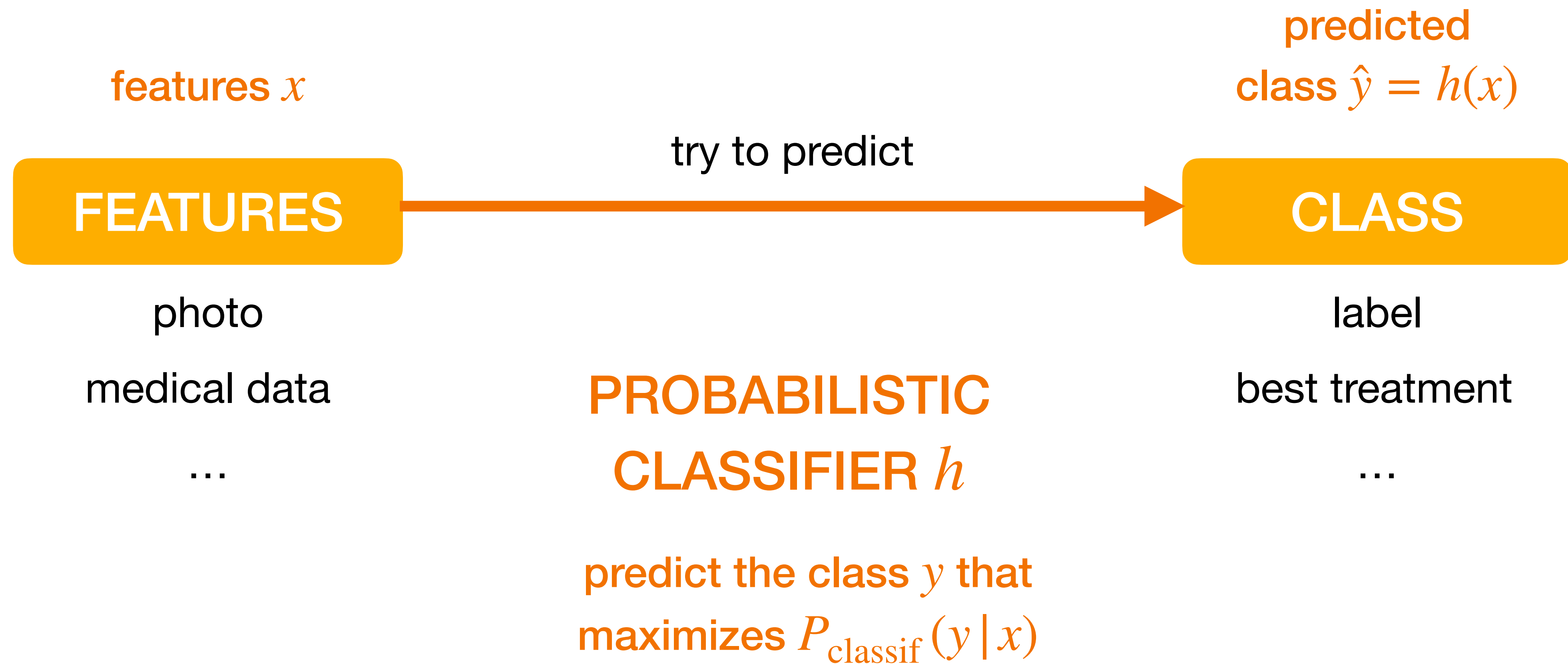
...

# CLASSIFICATION

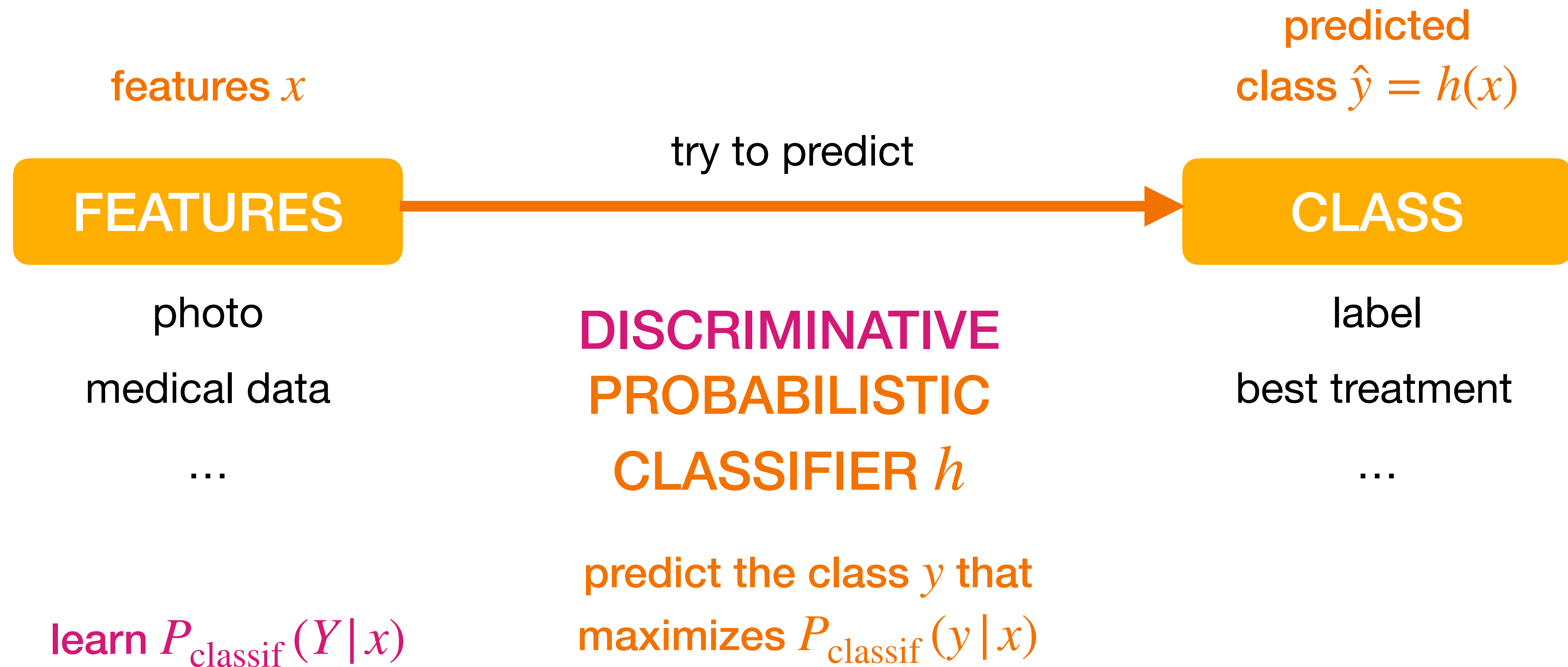




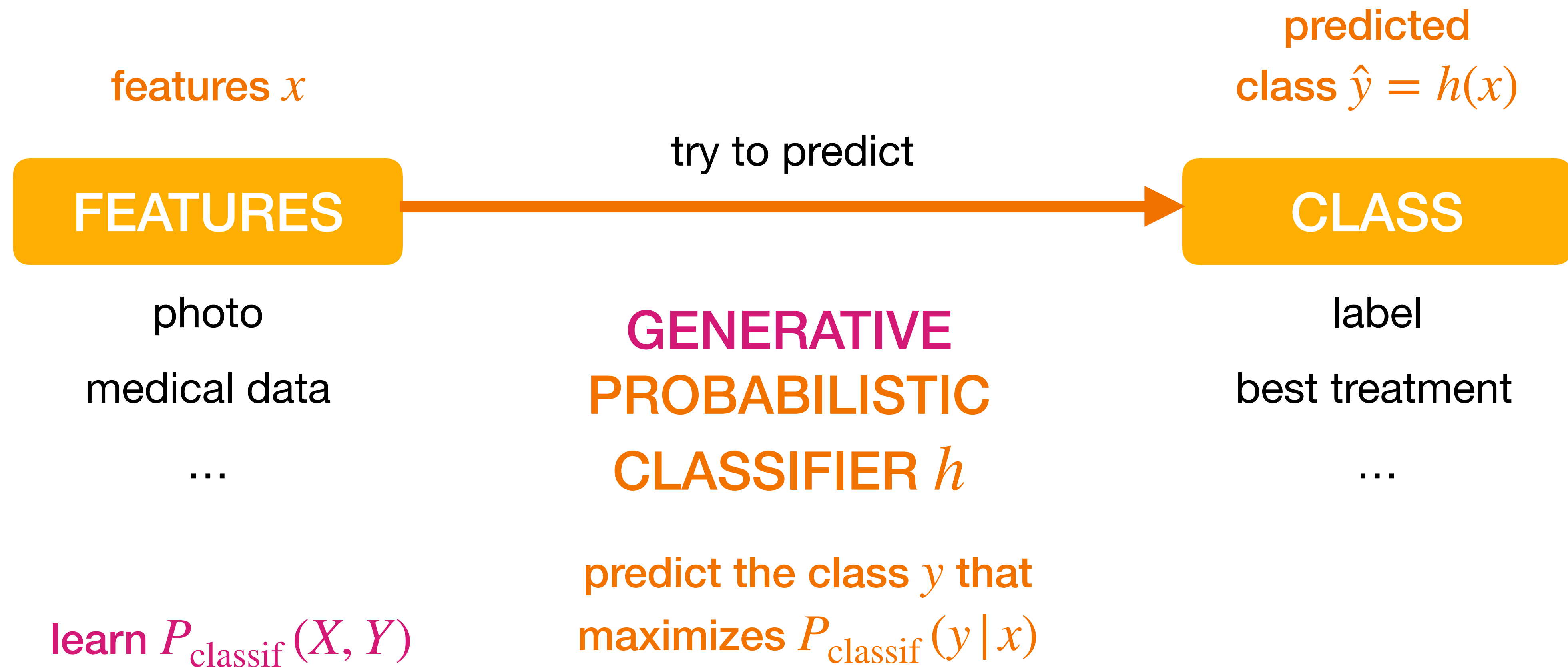
# CLASSIFICATION



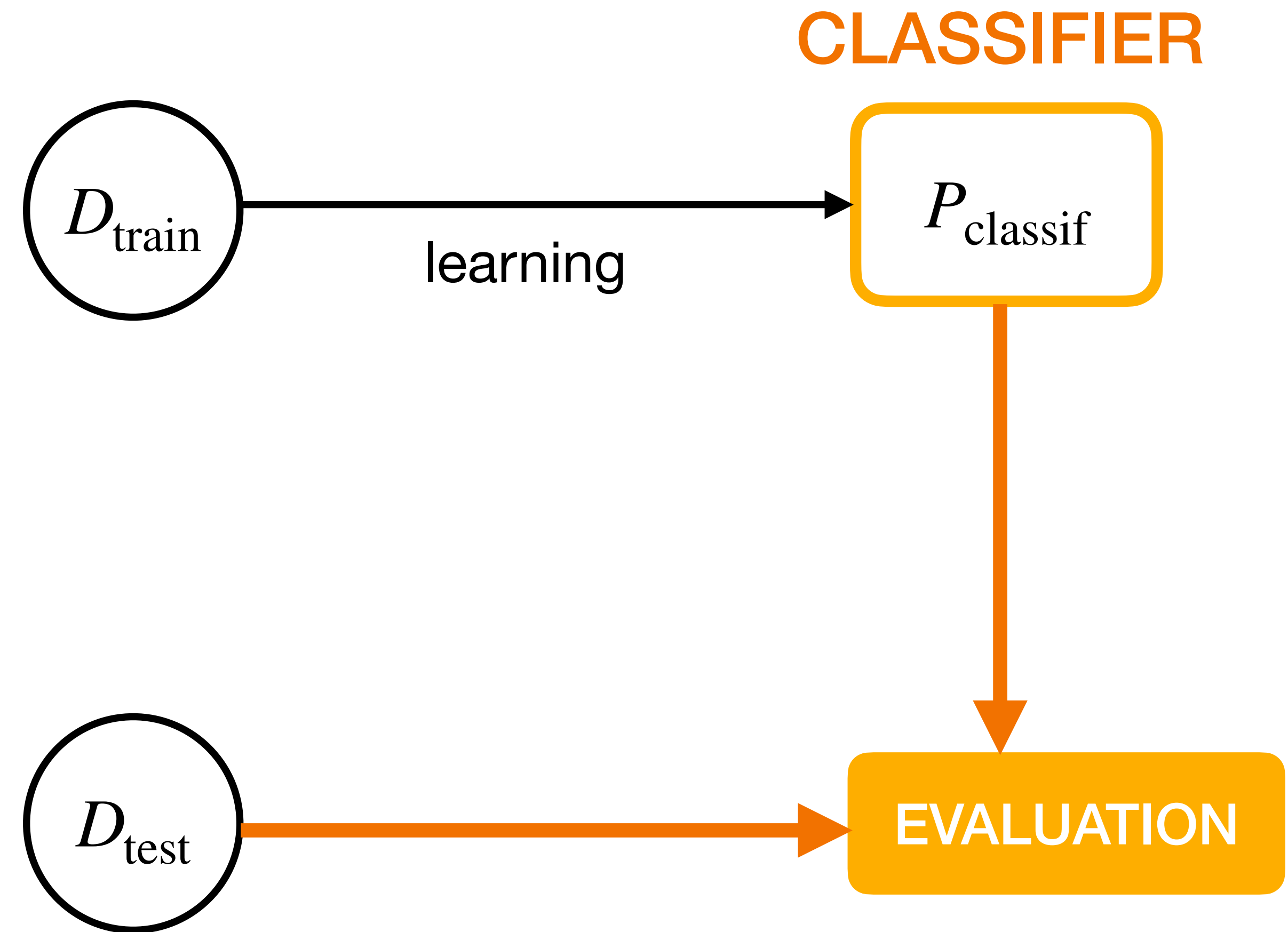
# CLASSIFICATION



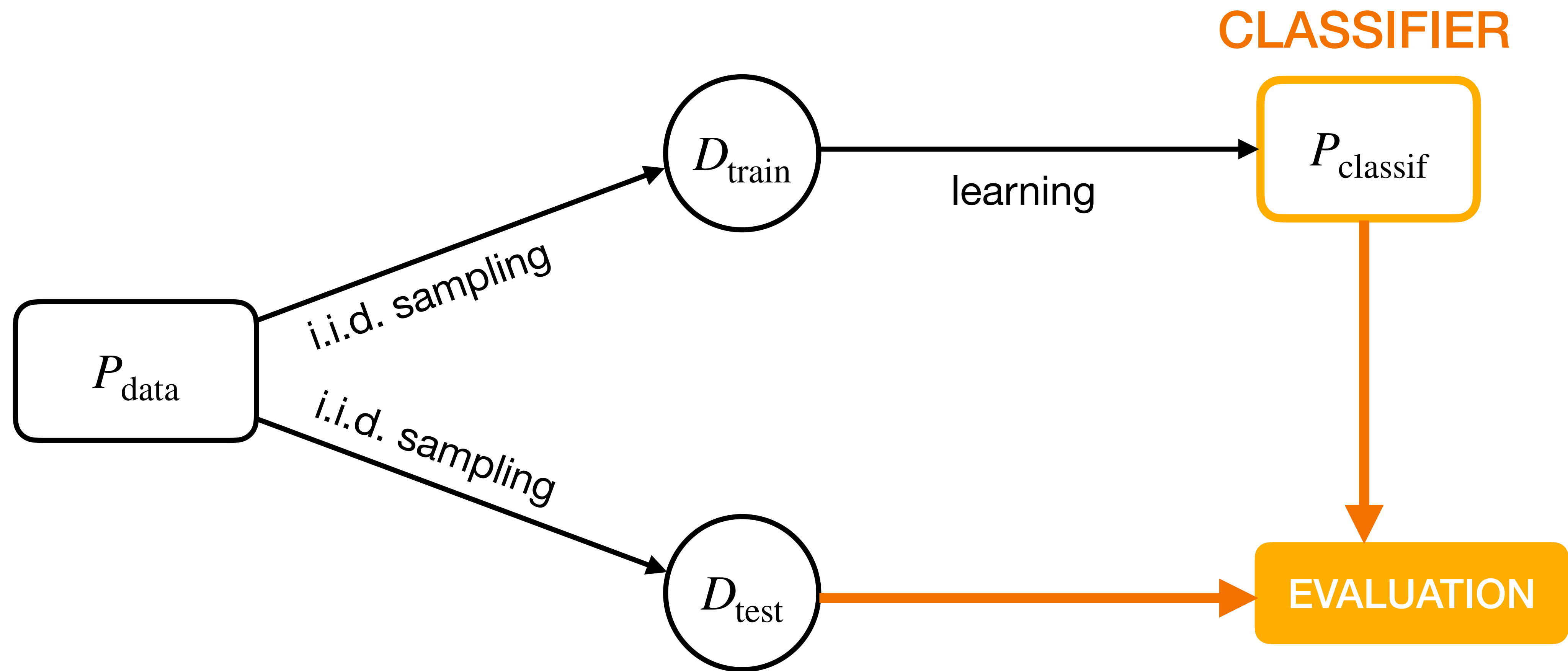
# CLASSIFICATION



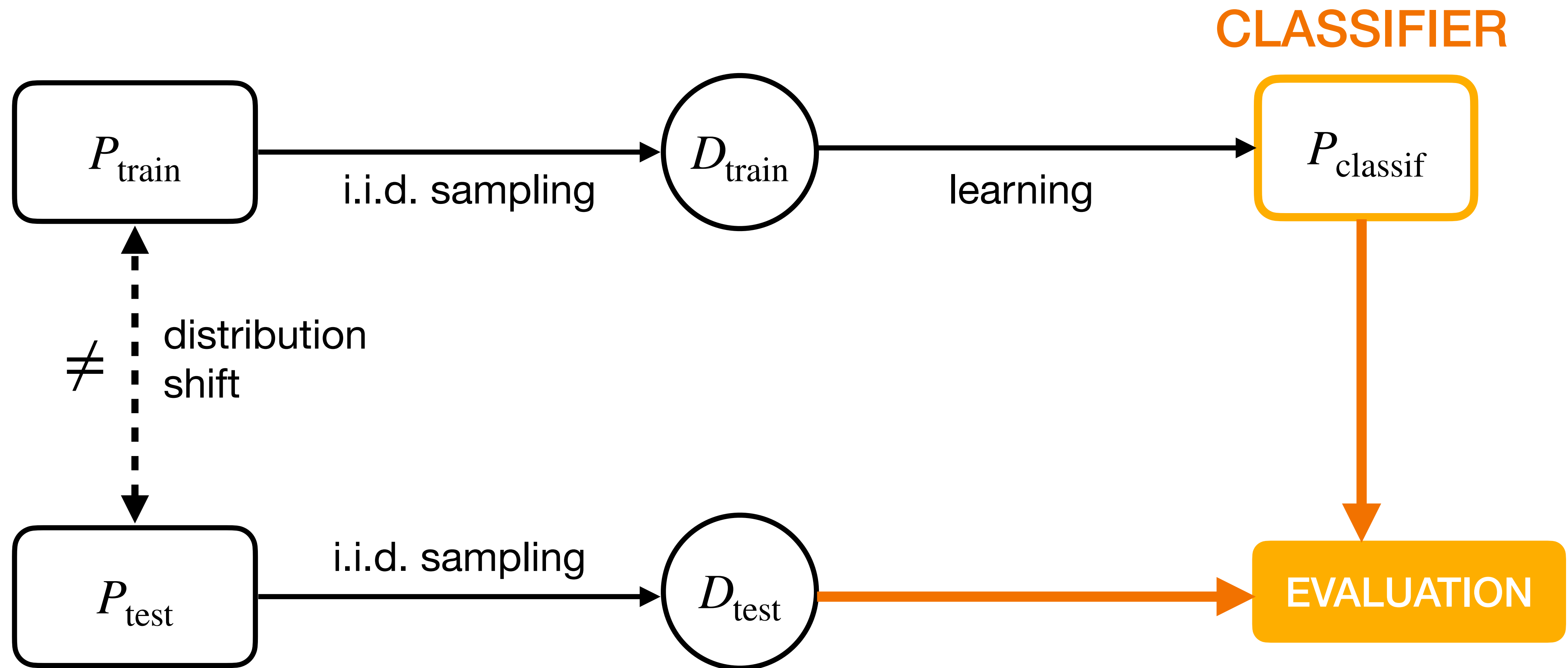
# CLASSIFICATION



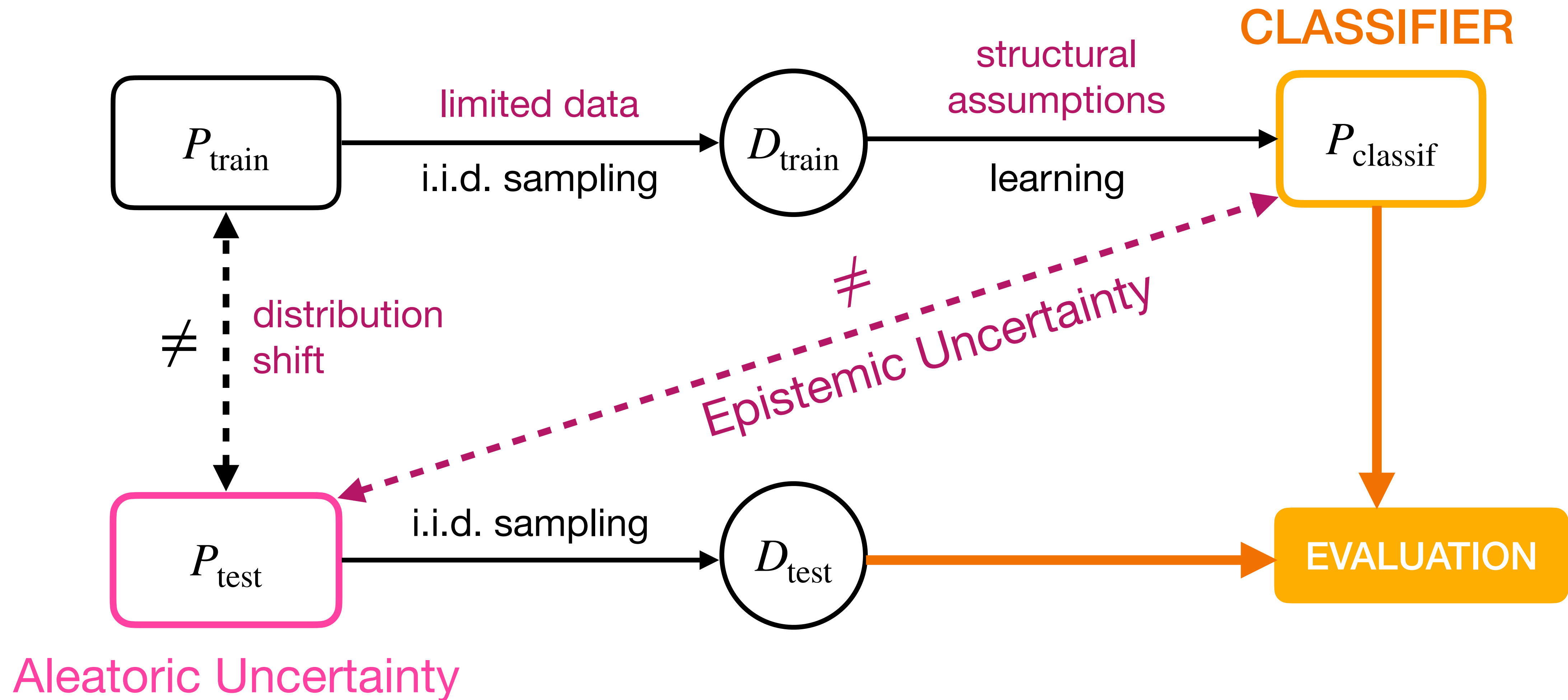
# CLASSIFICATION



# CLASSIFICATION



# CLASSIFICATION ... is unreliable



# PROBLEM 2:

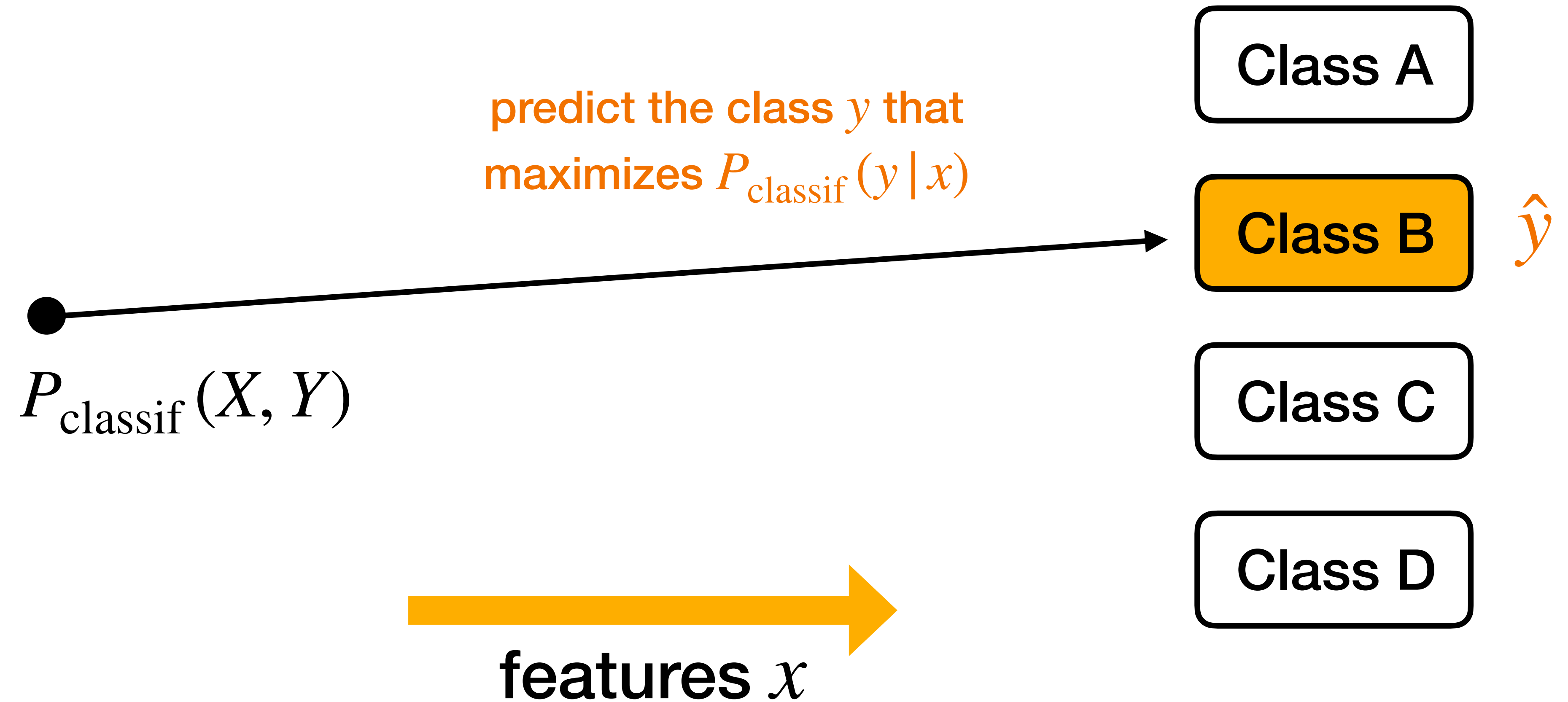
IMPRECISE  
PROBABILITIES

... are arbitrary



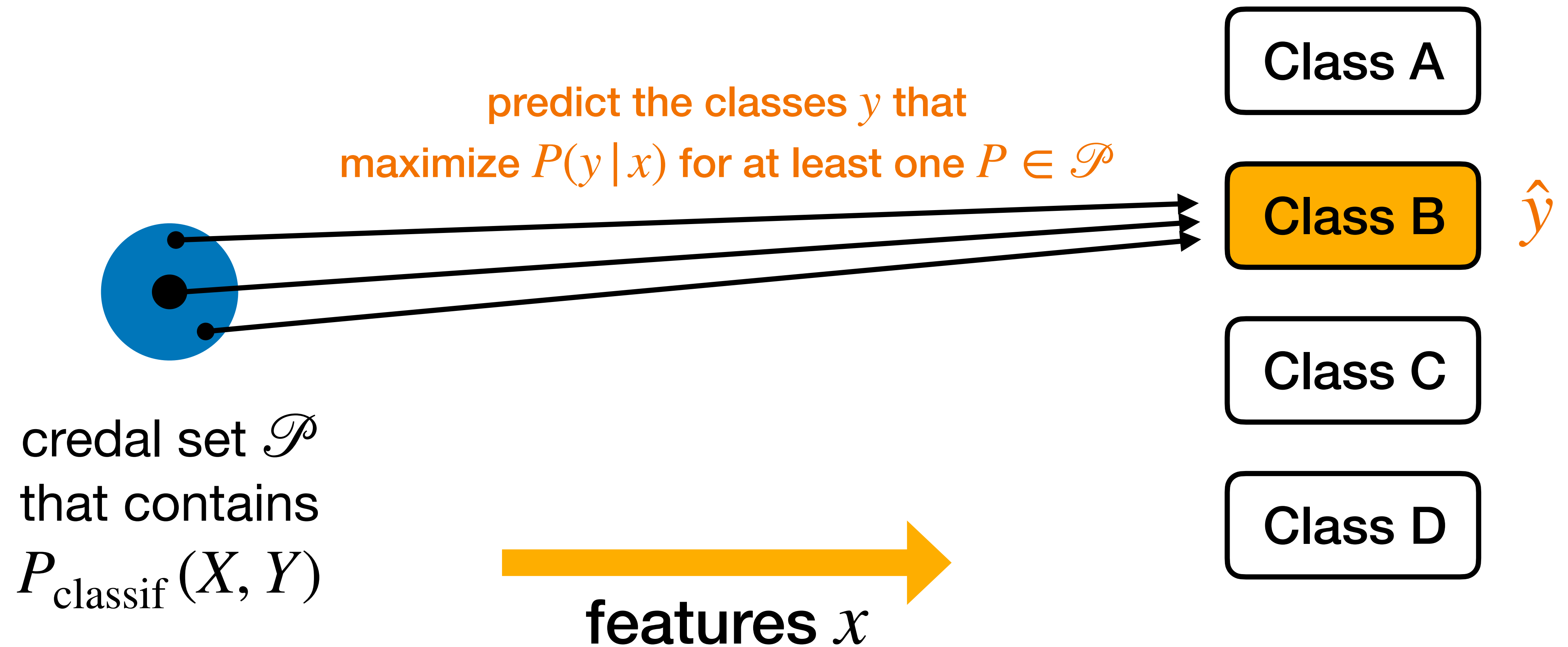
# IMPRECISE PROBABILITIES

## PROBABILISTIC CLASSIFIER



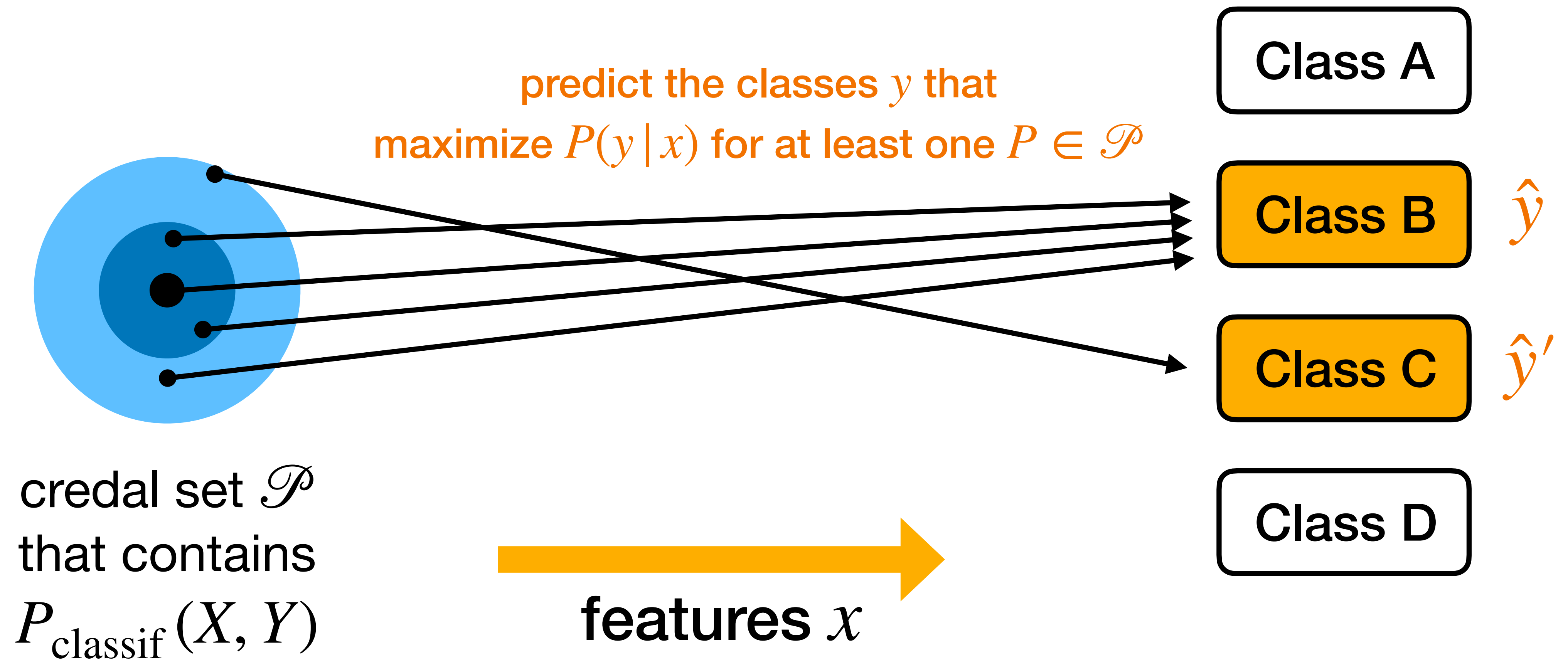
# IMPRECISE PROBABILITIES

## CREDAL CLASSIFIER



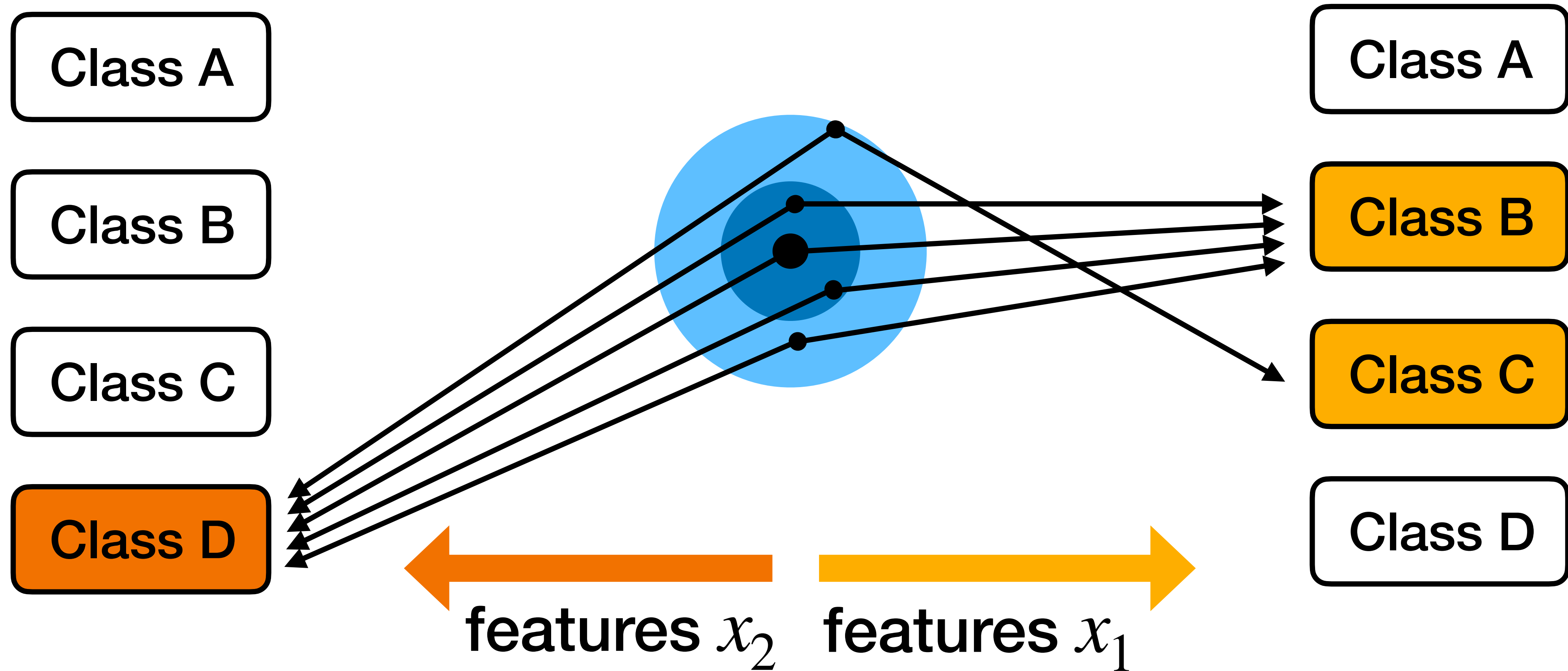
# IMPRECISE PROBABILITIES

## CREDAL CLASSIFIER



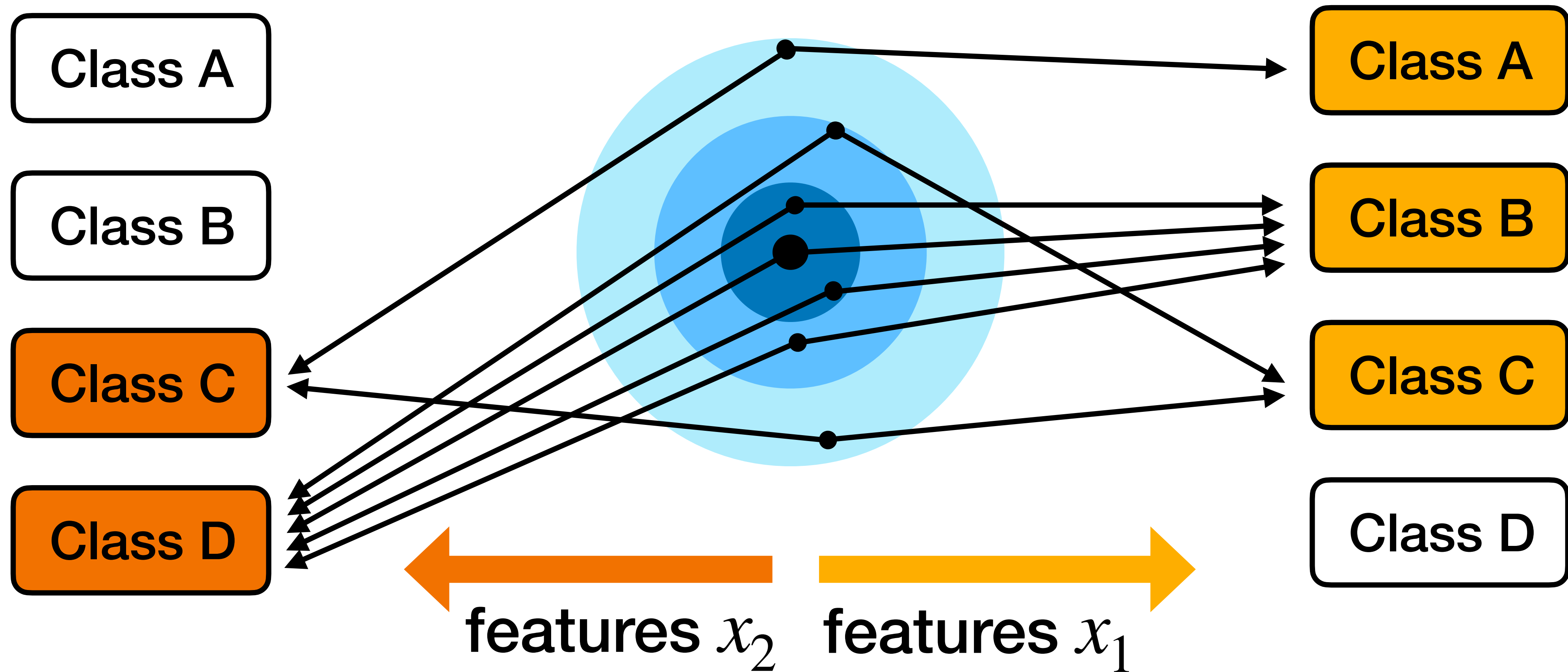
# IMPRECISE PROBABILITIES

## CREDAL CLASSIFIER



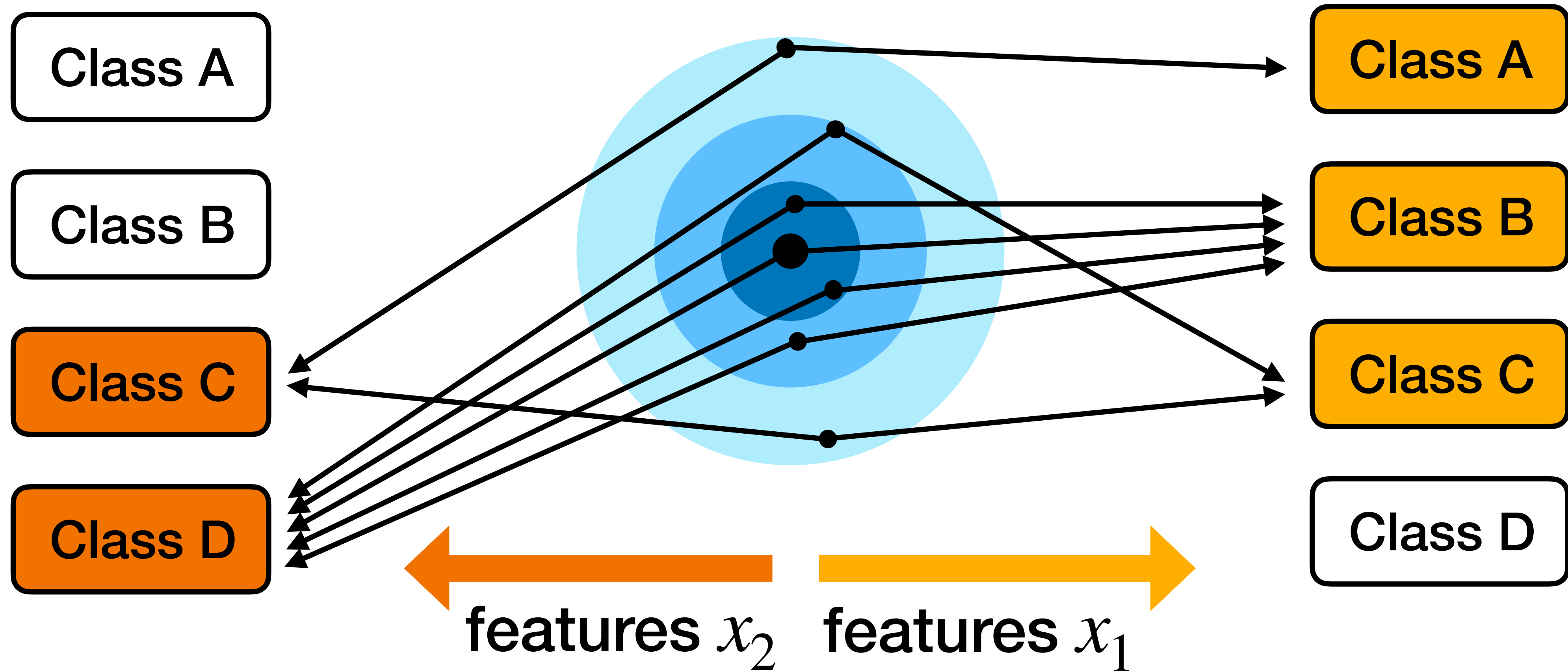
# IMPRECISE PROBABILITIES

## CREDAL CLASSIFIER



# IMPRECISE PROBABILITIES ... are arbitrary

## CREDAL CLASSIFIER







Adrián  
Detavernier



Rodrigo  
Lassance



MACHINE  
LEARNING

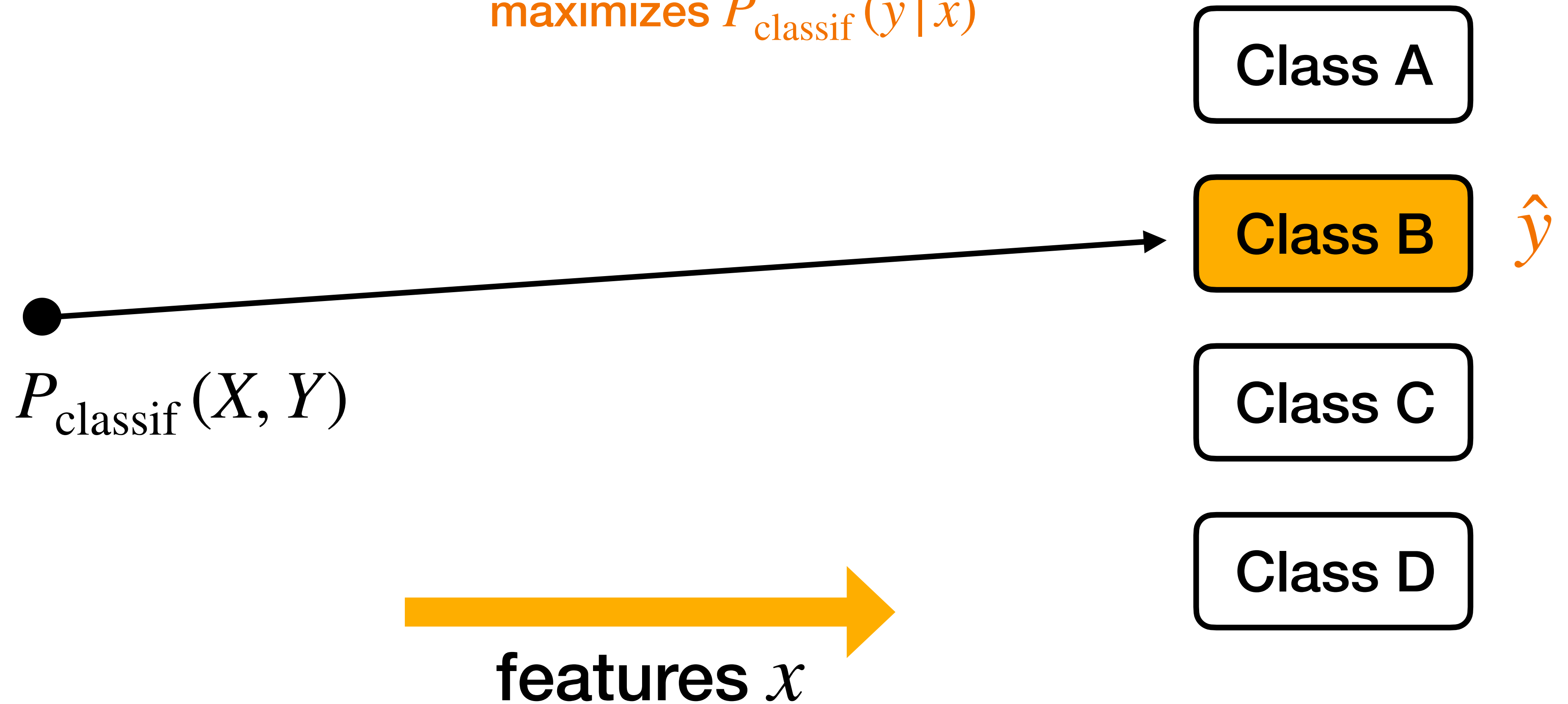
IMPRECISE  
PROBABILITIES

ROBUSTNESS  
QUANTIFICATION

# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER

predict the class  $y$  that  
maximizes  $P_{\text{classif}}(y | x)$



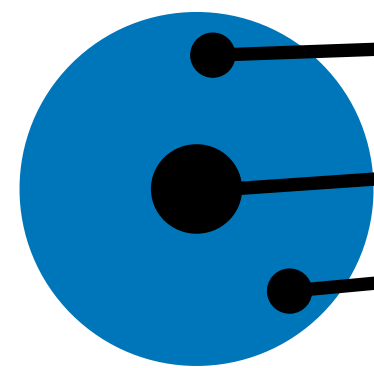


# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER

predict the class  $y$  that  
maximizes  $P_{\text{classif}}(y | x)$

credal set  $\mathcal{P}$   
that contains  
 $P_{\text{classif}}(X, Y)$



features  $x$

**ROBUST  
prediction**

Class A

**Class B**

$\hat{y}$

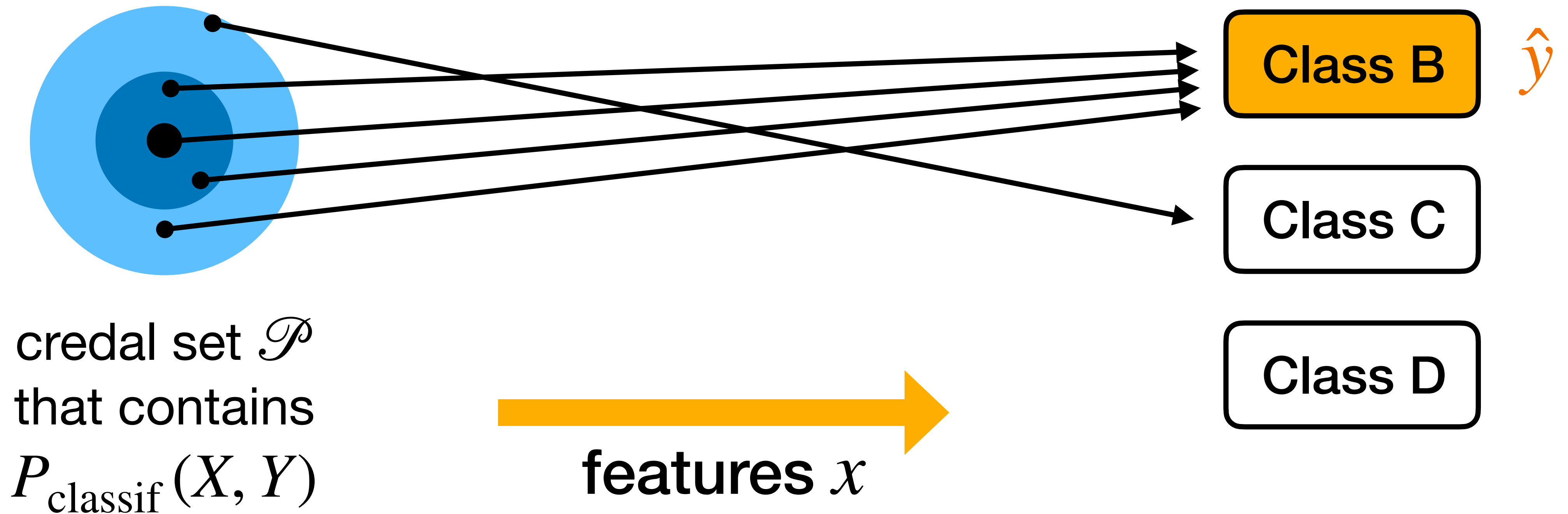
Class C

Class D

# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER

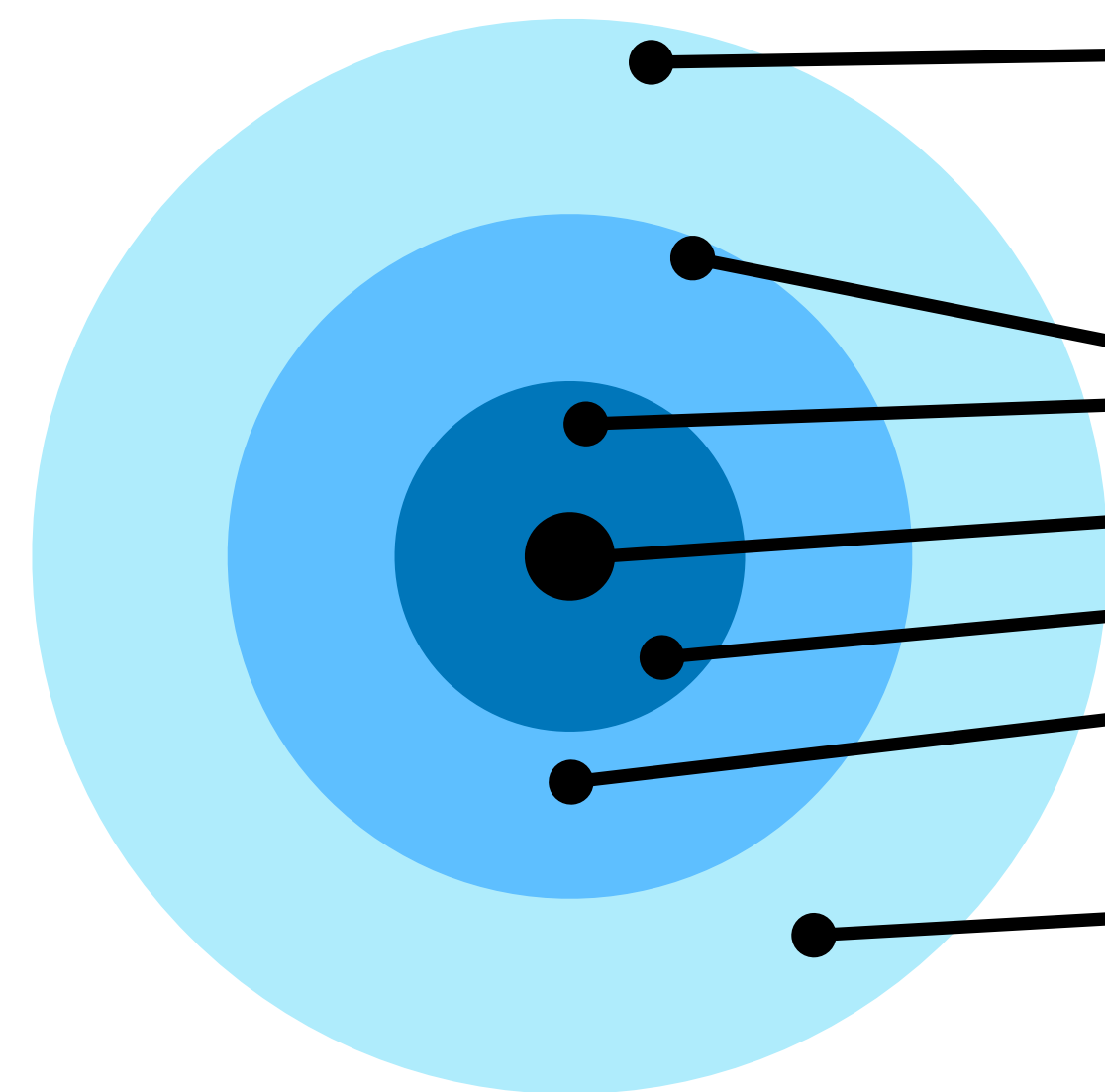
predict the class  $y$  that  
maximizes  $P_{\text{classif}}(y | x)$



# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER

predict the class  $y$  that  
maximizes  $P_{\text{classif}}(y | x)$



credal set  $\mathcal{P}$   
that contains  
 $P_{\text{classif}}(X, Y)$

features  $x$

~~ROBUST~~  
prediction

Class A

Class B

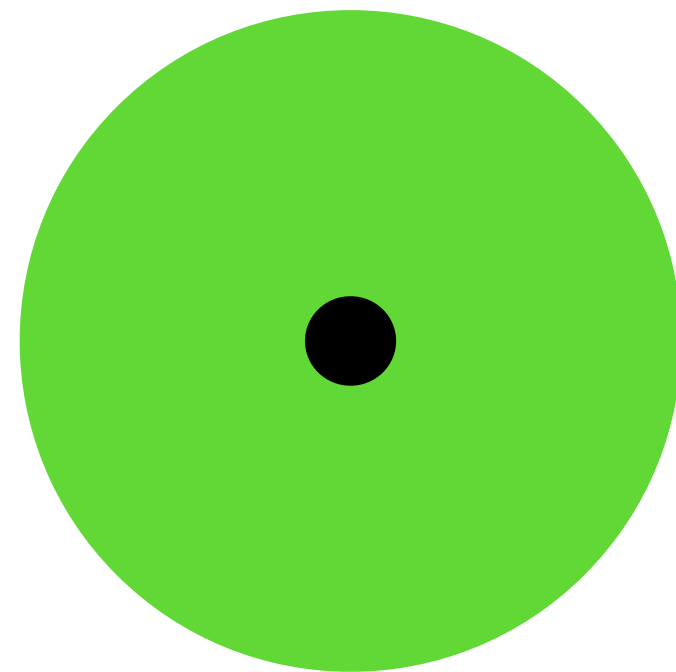
Class C

Class D

$\hat{y}$

# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER



credal set  $\mathcal{P}$   
that contains  
 $P_{\text{classif}}(X, Y)$

**ROBUSTNESS:**  
“size” of largest  $\mathcal{P}$  for  
which the precise  
prediction is robust



Adrián  
Detavernier



Rodrigo  
Lassance



MACHINE  
LEARNING

IMPRECISE  
PROBABILITIES

ROBUSTNESS  
QUANTIFICATION

# PROBLEM 2:

IMPRECISE  
PROBABILITIES

... ~~are arbitrary~~

PROBLEM 1:

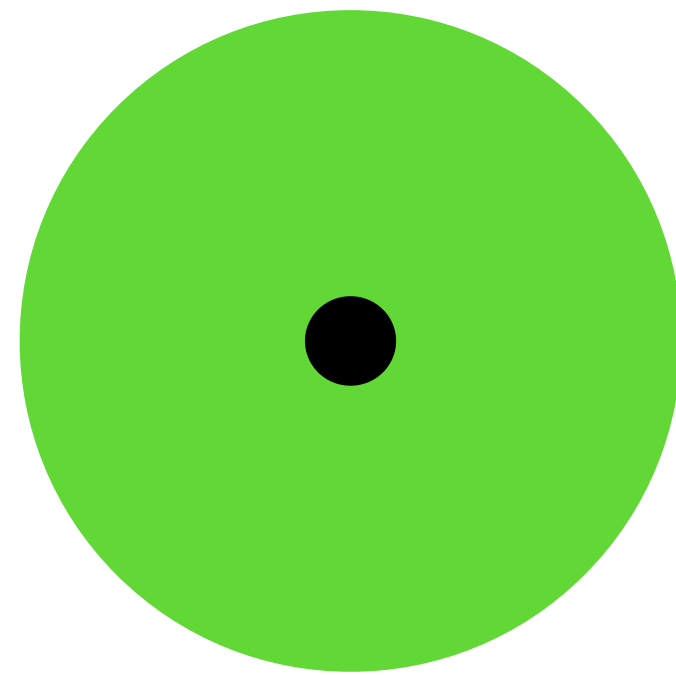
MACHINE  
LEARNING

... is unreliable



# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER

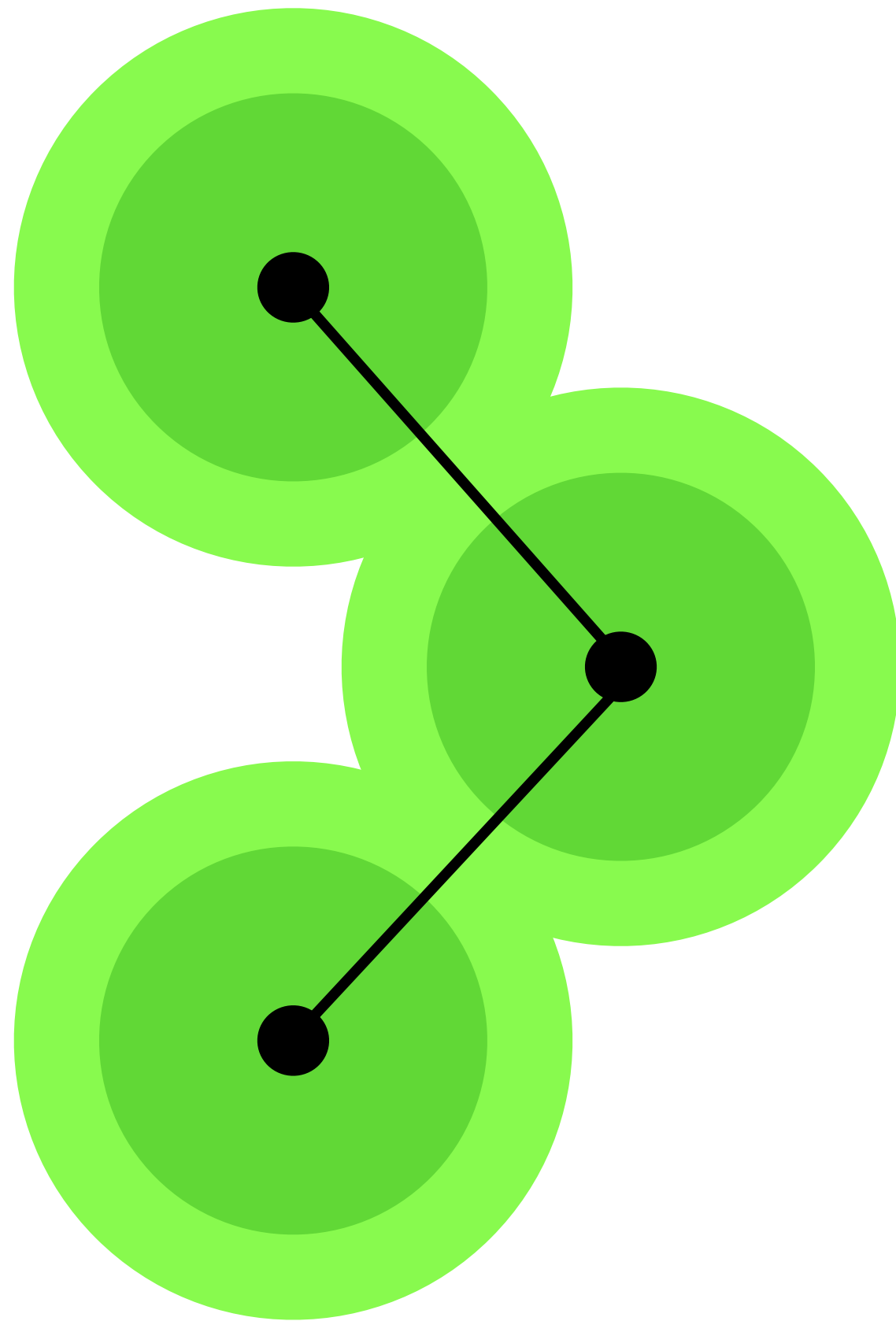


credal set  $\mathcal{P}$   
that contains  
 $P_{\text{classif}}(X, Y)$

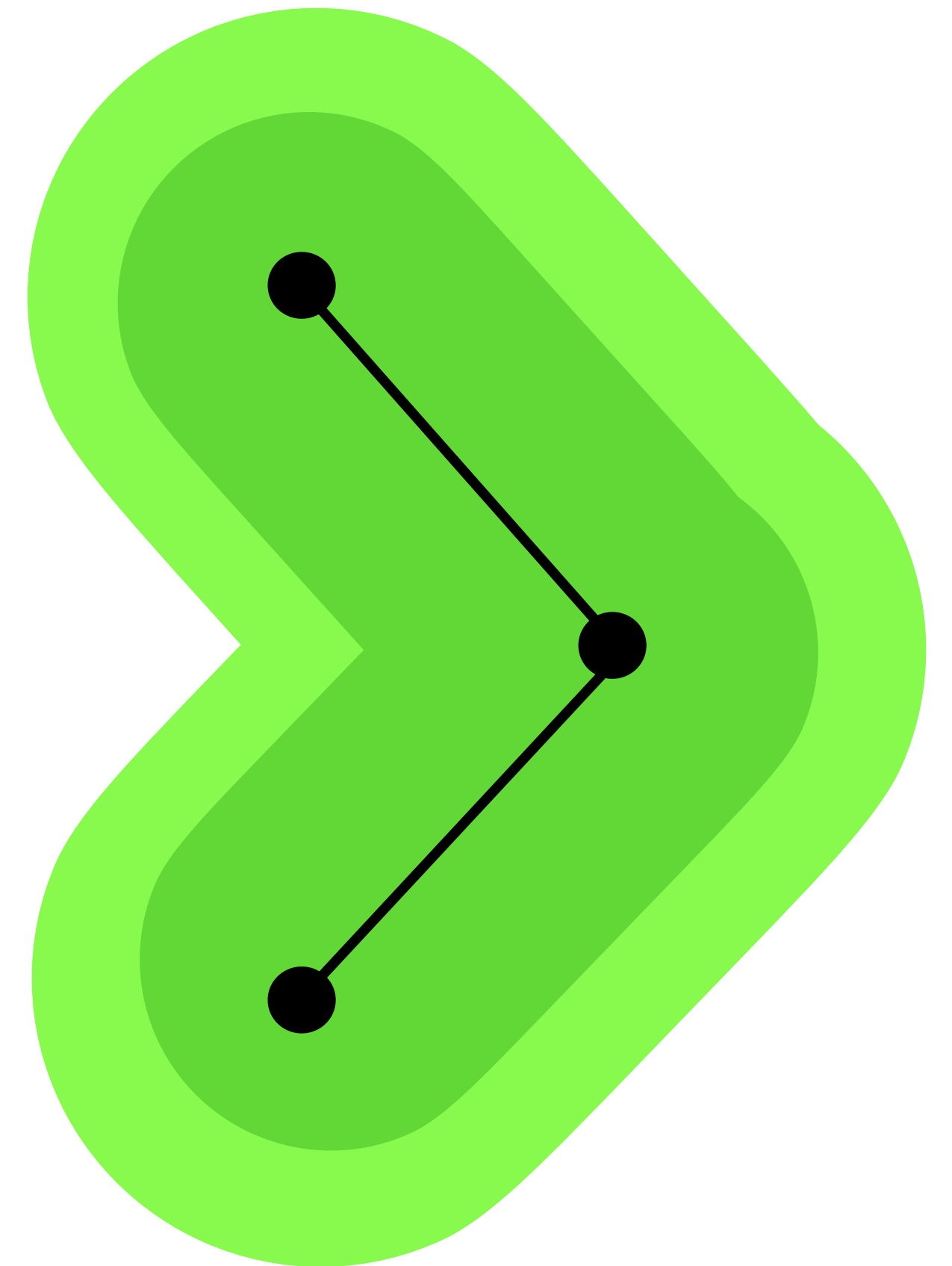
**ROBUSTNESS:**  
“size” of largest  $\mathcal{P}$  for  
which the precise  
prediction is robust



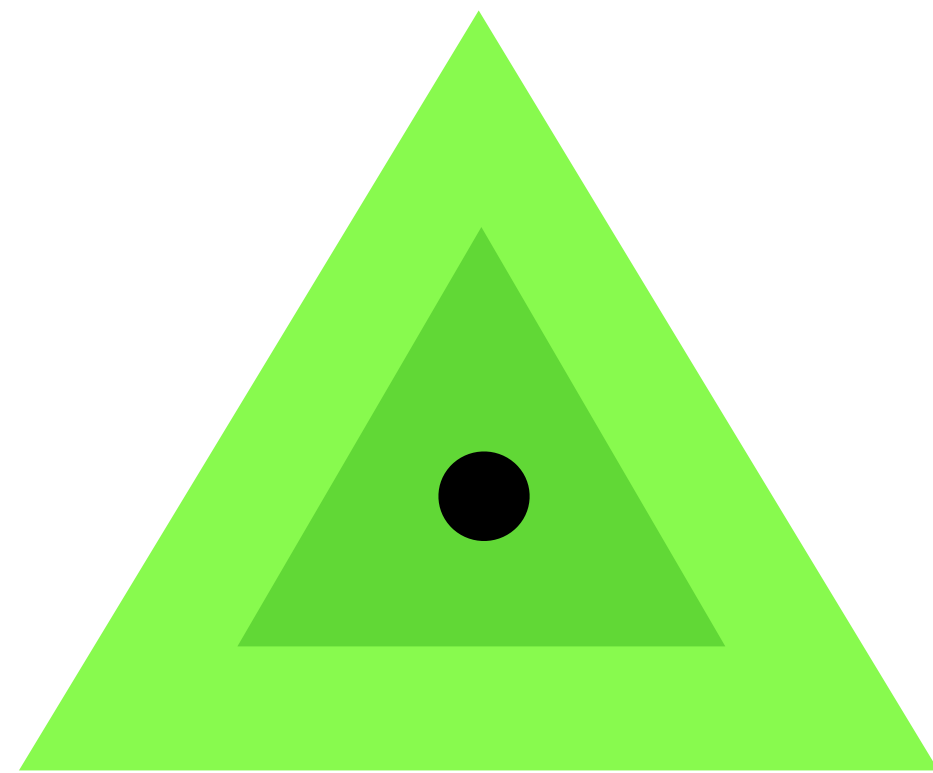
LOCAL



GLOBAL



## $\epsilon$ -CONTAMINATION



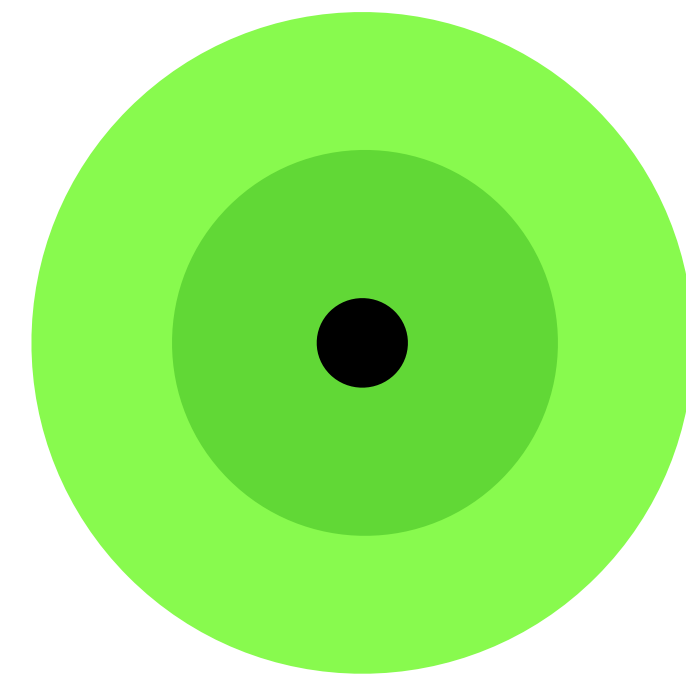
$\mathcal{P}_\epsilon$

$\parallel$

$$\{(1 - \epsilon)P_{\text{classif}} + \epsilon P : P \in \Delta\}$$

## OTHER STUFF

distance-based, ...



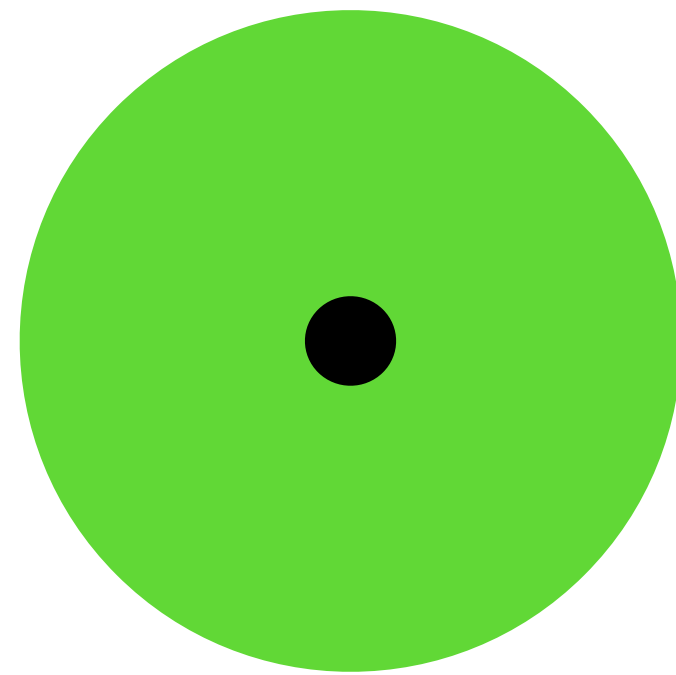
$\mathcal{P}_\epsilon$

$\parallel$

$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$

# ROBUSTNESS QUANTIFICATION

## PROBABILISTIC CLASSIFIER



credal set  $\mathcal{P}$   
that contains  
 $P_{\text{classif}}(X, Y)$

**ROBUSTNESS:**  
“size” of largest  $\mathcal{P}$  for  
which the precise  
prediction is robust





2014

MRF  
BN



Cassio  
de Campos



Alessandro  
Antonucci

# Global Sensitivity Analysis for MAP Inference in Graphical Models

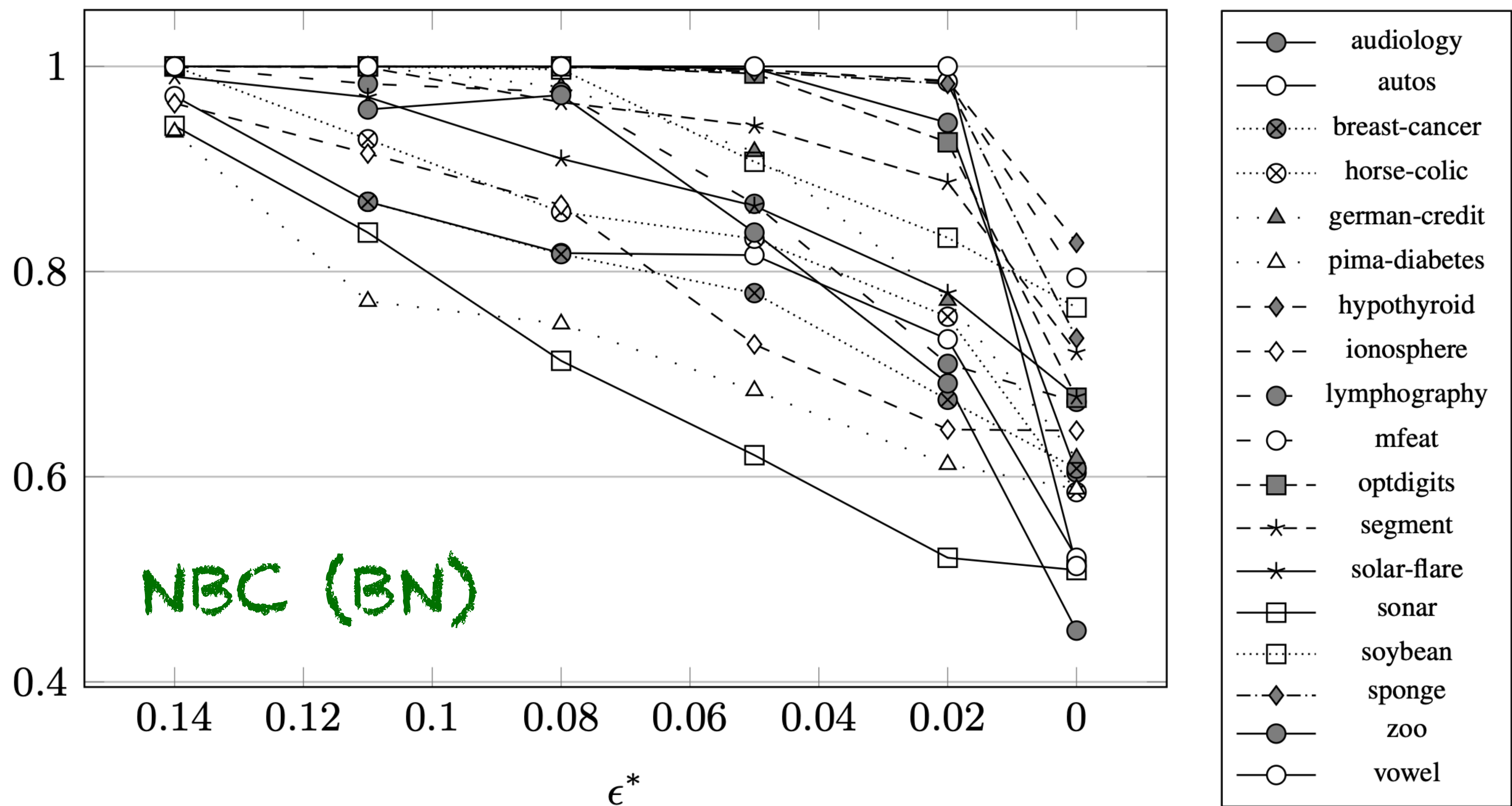
**Jasper De Bock**  
Ghent University, SYSTeMS  
Ghent (Belgium)  
jasper.debock@ugent.be

**Cassio P. de Campos**  
Queen's University  
Belfast (UK)  
c.decampos@qub.ac.uk

**Alessandro Antonucci**  
IDSIA  
Lugano (Switzerland)  
alessandro@idsia.ch

## Abstract

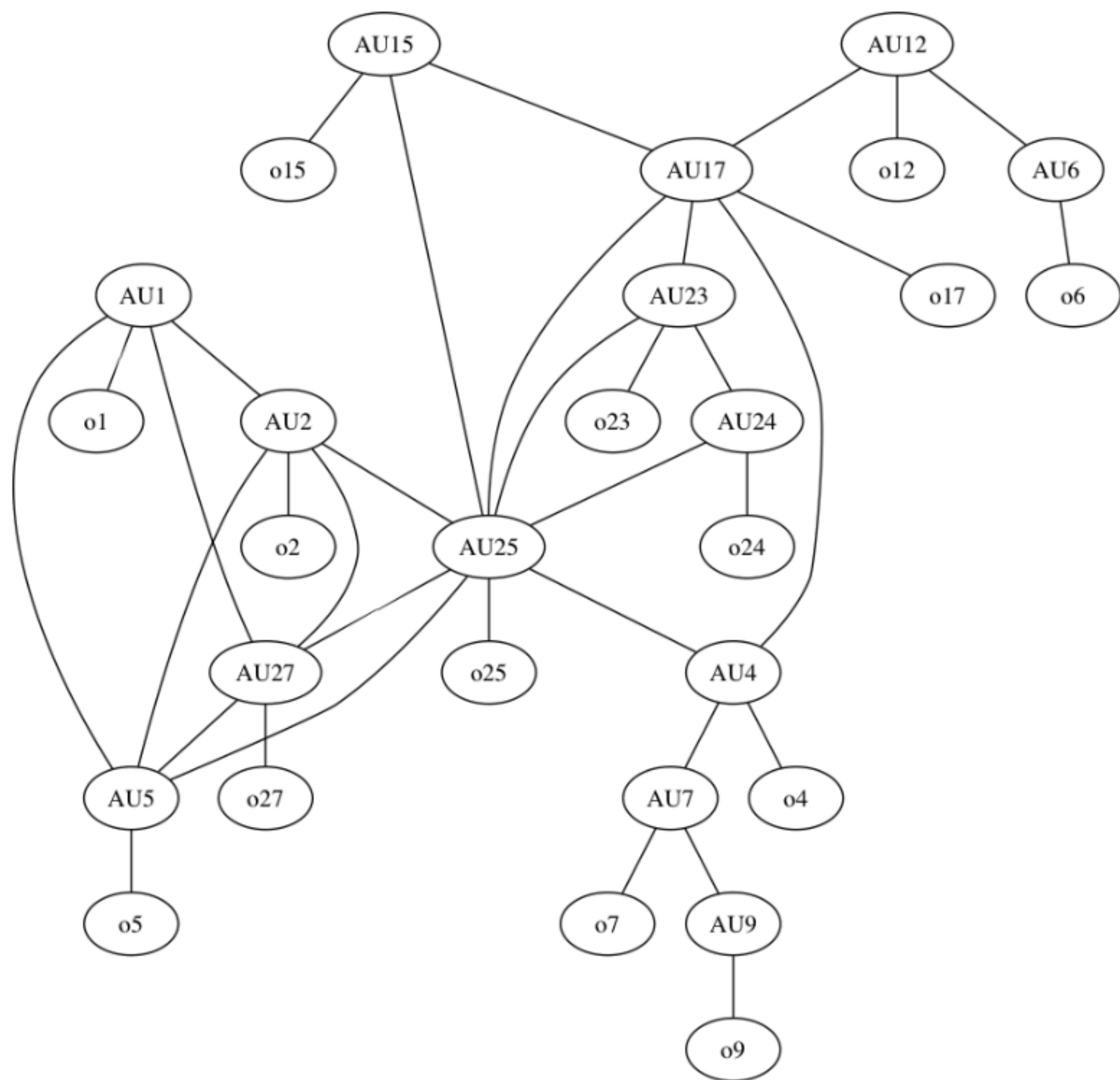
We study the sensitivity of a MAP configuration of a discrete probabilistic graphical model with respect to perturbations of its parameters. These perturbations are global, in the sense that simultaneous perturbations of all the parameters (or any chosen subset of them) are allowed. Our main contribution is an exact algorithm to check whether the MAP configuration is robust with respect to given perturbations. Sensitivity is essentially the same as that of obtaining the MAP configuration, which can be used with minimal effort. We use our algorithm to measure the sensitivity of a MAP configuration to perturbations of its parameters.



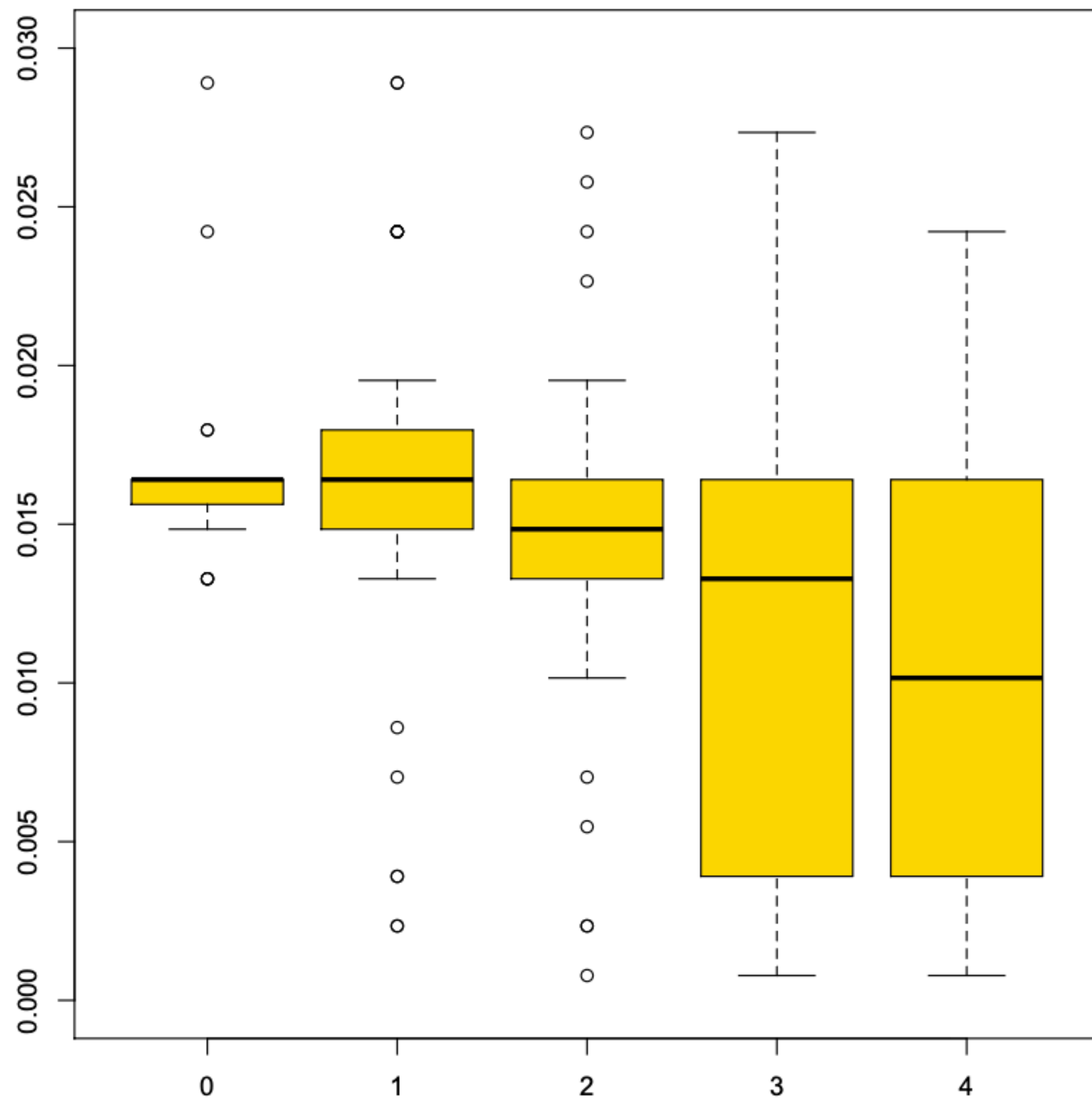




MRF



(a) MRF used in the computations.



(b) Robustness split by Hamming distances.



2017-2020

SPN

[2-4, ...]



Cassio de Campos & various co-authors

[5]

GeF+

ILR: Proceedings of Machine Learning Research, vol. 62, 205-216, 2017

### Credal Sum-Product Networks

**Denis Deratani Mauá**  
Institute of Mathematics and Statistics, Universidade de São Paulo (Brazil)  
**Fabio Gagliardi Cozman**  
Escola Politécnica, Universidade de São Paulo (Brazil)  
**Diarmaid Conaty**  
**Cassio Polpo de Campos**  
Queen's University Belfast (United Kingdom)

#### Abstract

Sum-product networks are a relatively new and increasingly graphical models that allow for marginal inference with probabilistic models, sum-product networks are often learned. Hence, their results are prone to be unreliable and imprecise. credal sum-product networks, an imprecise extension of algorithms and complexity results for common inference classification task using images of digits and show the a perturbation of the parameters of learned sum-product networks to distinguish between reliable and unreliable classifications with high accuracy.

**Keywords:** Sum-product networks; tractable probabilistic models; credal classification; sensitivity analysis; robust statistics

#### 1. Introduction

Probabilistic models are usually built so that quantitative (probabilistic) conclusions about uncertain knowledge to be learned from data, such as Bayesian networks and Markov networks, depend heavily on the graph topology [32,64,62]. In this graphical representation, the nodes represent random variables and the edges represent conditional dependencies [16].



### Robustifying sum-product networks

**Denis Deratani Mauá<sup>a,\*</sup>**, **Diarmaid Conaty<sup>b</sup>**, **Fabio Gagliardi<sup>c</sup>**, **Katja Poppenhaeger<sup>d</sup>**, **Cassio Polpo de Campos<sup>b,e</sup>**

<sup>a</sup> Institute of Mathematics and Statistics, Universidade de São Paulo, Brazil  
<sup>b</sup> Centre for Data Science and Scalable Computing, Queen's University Belfast, UK  
<sup>c</sup> Escola Politécnica, Universidade de São Paulo, Brazil  
<sup>d</sup> Astrophysics Research Centre, Queen's University Belfast, UK  
<sup>e</sup> Dept. of Information and Computing Sciences, Utrecht University, the Netherlands

#### ARTICLE INFO

Article history:  
Received 6 December 2017  
Received in revised form 5 July 2018  
Accepted 10 July 2018  
Available online 18 July 2018

**Keywords:**  
Sum-product networks  
Tractable probabilistic models  
Credal classification  
Sensitivity analysis  
Robust statistics

#### ABSTRACT

Sum-product networks are a relatively new and increasingly graphical models that allow for marginal inference with probabilistic models, sum-product networks are often learned. Hence, their results are prone to be unreliable and imprecise. credal sum-product networks, an imprecise extension of algorithms and complexity results for common inference classification task using images of digits and show the a perturbation of the parameters of learned sum-product networks to distinguish between reliable and unreliable classifications with high accuracy.

#### 1. Introduction

Probabilistic graphical models such as Bayesian networks and Markov networks allow for the compact specification of uncertain knowledge through a graphical language that represents variables as nodes and dependences as graph connectivity [30,17]. Not only this graphical approach facilitates knowledge elicitation and communication, but is key to efficient inference. For example, while marginal inference in Bayesian and Markov networks is #P-complete, popular approximate inference algorithms are based on passing messages along the edges of the graph topology [32,64,62]. In this graphical representation, the nodes represent random variables and the edges represent conditional dependencies [16].

### Towards Scalable and Robust Sum-Product Networks

Alvaro H. C. Correia and Cassio P. de Campos<sup>(✉)</sup>  
Eindhoven University of Technology, Eindhoven, The Netherlands  
c.decampos@tue.nl

**Abstract.** Sum-Product Networks (SPNs) and their credal counterparts are machine learning models that combine good representational power with tractable inference. Yet they often have thousands of nodes which result in high processing times. We propose the addition of caches to the SPN nodes and show how this memoisation technique reduces inference times in a range of experiments. Moreover, we introduce class-selective SPNs, an architecture that is suited for classification tasks and enables efficient robustness computation in Credal SPNs. We also illustrate how robustness estimates relate to reliability through the accuracy of the model, and how one can explore robustness in ensemble modelling.

**Keywords:** Sum-Product Networks · Robustness

#### 1 Introduction

Sum-Product Networks (SPNs) [15] (conceptually similar to Circuits [4]) are a class of deep probabilistic graphical models where marginal inference is always tractable. More precisely, any marginal query can be computed in time polynomial in the network size. Still, SPNs can be high tree-width models [15] and are capable of representing complex and multidimensional distributions [5]. This promising combination of efficiency and machine learning power has motivated several applications of SPNs to a variety of machine learning tasks [1,3,11,16-18].

As any other standard probabilistic graphical model, SPNs learned from data are prone to overfitting when evaluated at poorly represented regions of the feature space, leading to overconfident and often unreliable conclusions. However, due to the probabilistic semantics of each output. A notable example is Credal SPNs (CSPNs) [9], an extension of SPNs to imprecise probabilities where we can compute a measure of the reliability of each prediction. Such robustness values are useful tools for decision-making, as they are highly correlated with accuracy, and thus tell us when to trust the CSPN's prediction: if the robustness of a prediction is low, we can suspend judgement or even resort to another machine

### Towards Robust Classification with Deep Generative Forests

Alvaro H. C. Correia<sup>1</sup> Robert Peharz<sup>1</sup> Cassio de Campos<sup>1</sup>

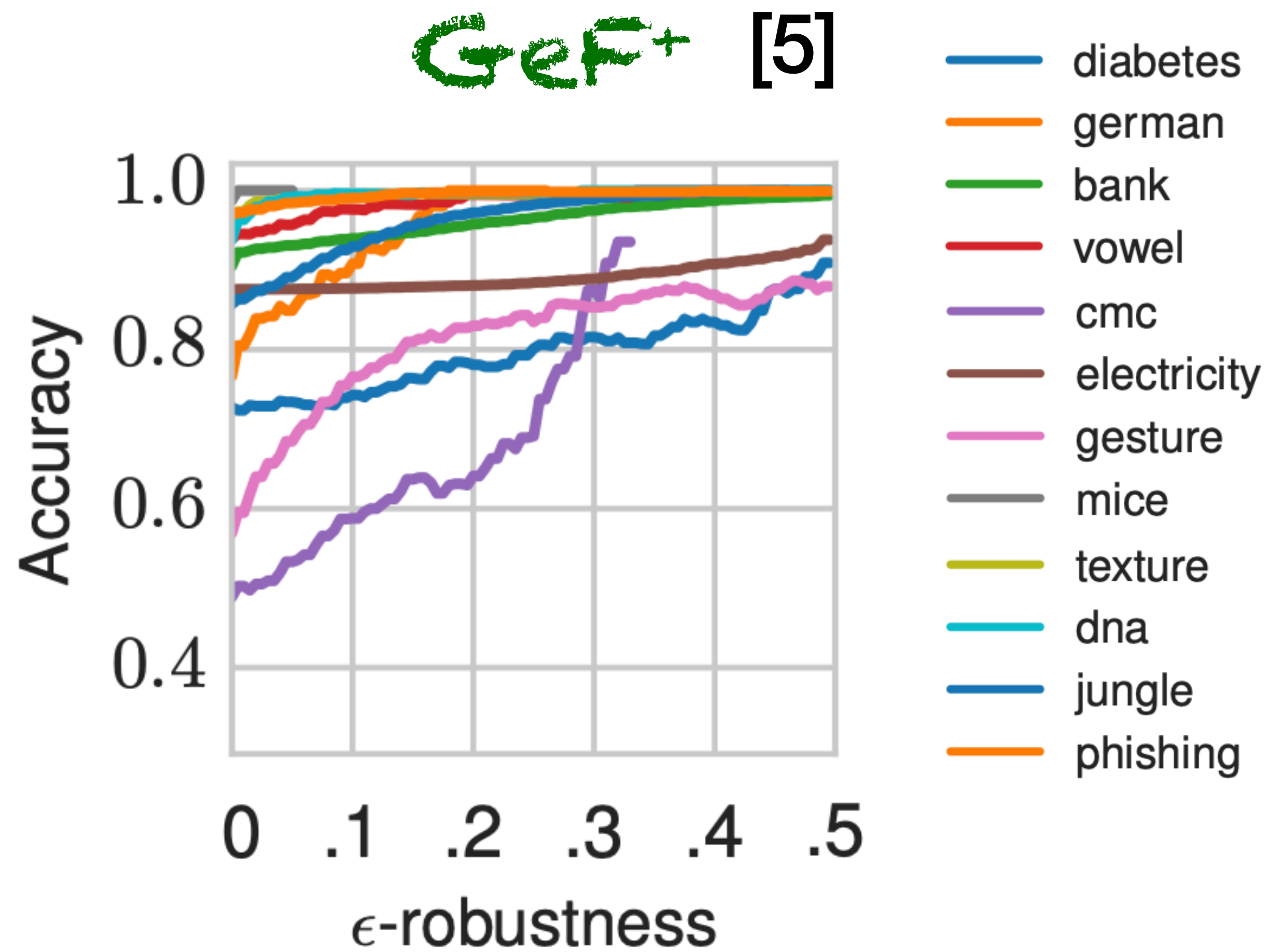
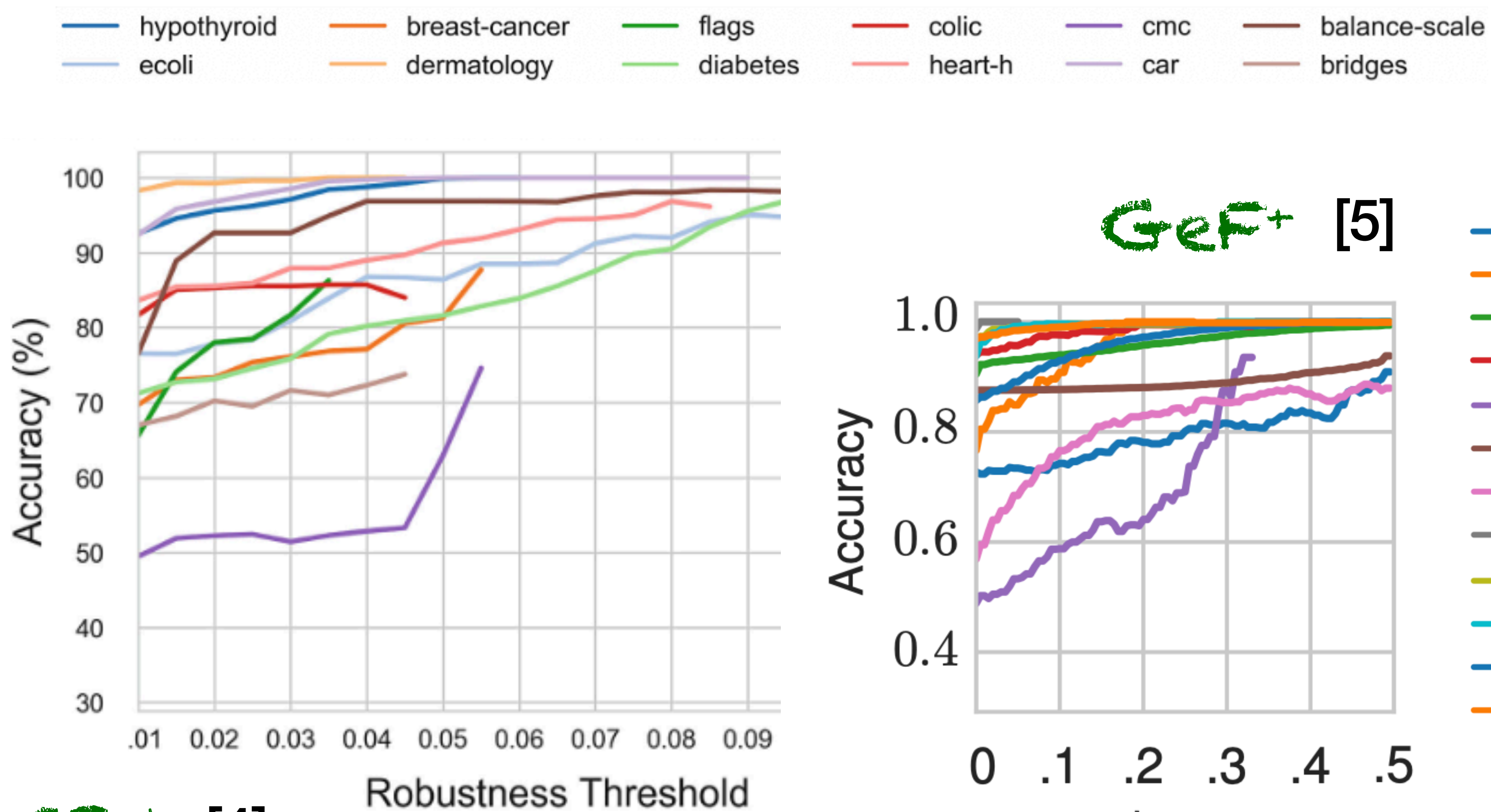
#### Abstract

Decision Trees and Random Forests are among the most widely used machine learning models, and often achieve state-of-the-art performance in tabular, domain-agnostic datasets. Nonetheless, they are prone to overfitting when evaluated at poorly represented regions of the feature space, leading to overconfident and often unreliable conclusions. However, due to the probabilistic semantics of each output. A notable example is Credal SPNs (CSPNs) [9], an extension of SPNs to imprecise probabilities where we can compute a measure of the reliability of each prediction. Such robustness values are useful tools for decision-making, as they are highly correlated with accuracy, and thus tell us when to trust the CSPN's prediction: if the robustness of a prediction is low, we can suspend judgement or even resort to another machine

#### 2. Generative Forests

Before discussing the main ideas of the paper, we introduce Generative Forests and the required notation. As we focus on classification tasks, we denote the set of explanatory variables as  $\mathbf{X} = \{X_1, X_2, \dots, X_m\}$  and the target variable as  $Y$ . As usual, we write realizations of random variables as  $x$ .





# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures ✓





Adrián  
Detavernier

Rodrigo  
Lassance

2025...

[6, 7, ...]

## Robustness quantification: a new method for assessing the reliability of the predictions of a classifier

Jasper De Bock<sup>1</sup>

Adrián Detavernier<sup>1</sup>

<sup>1</sup>Foundations Lab for imprecise probabilities, Ghent University, Belgium

ness quantification compare in cases wh  
data is limited or when there is a distri  
train and test data. Our motiv  
by the fact that the  
have a big

## Robustness and uncertainty: two complementary aspects of the reliability of the predictions of a classifier

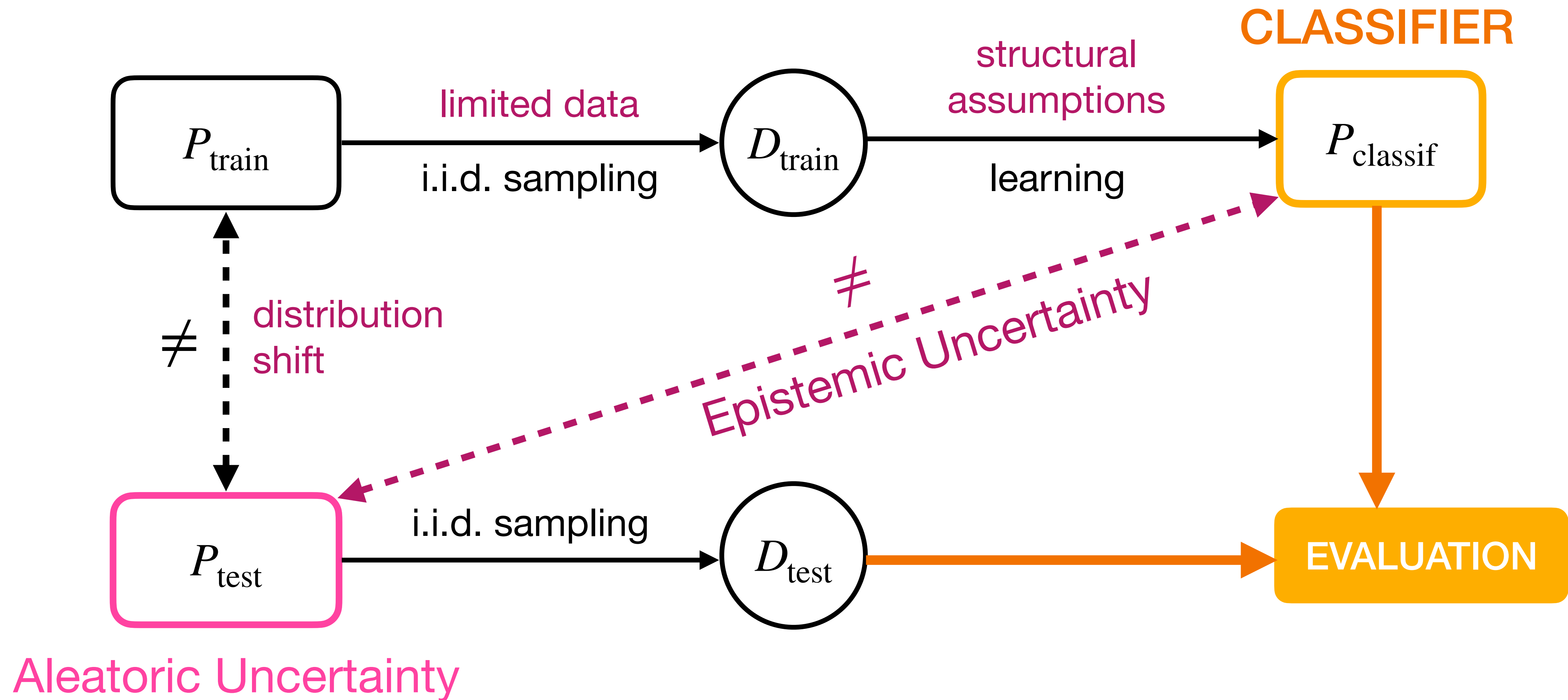
Adrián Detavernier  
Foundations Lab for imprecise probabilities  
Ghent University  
Belgium

Jasper De Bock  
Foundations Lab for imprecise probabilities  
Ghent University  
Belgium

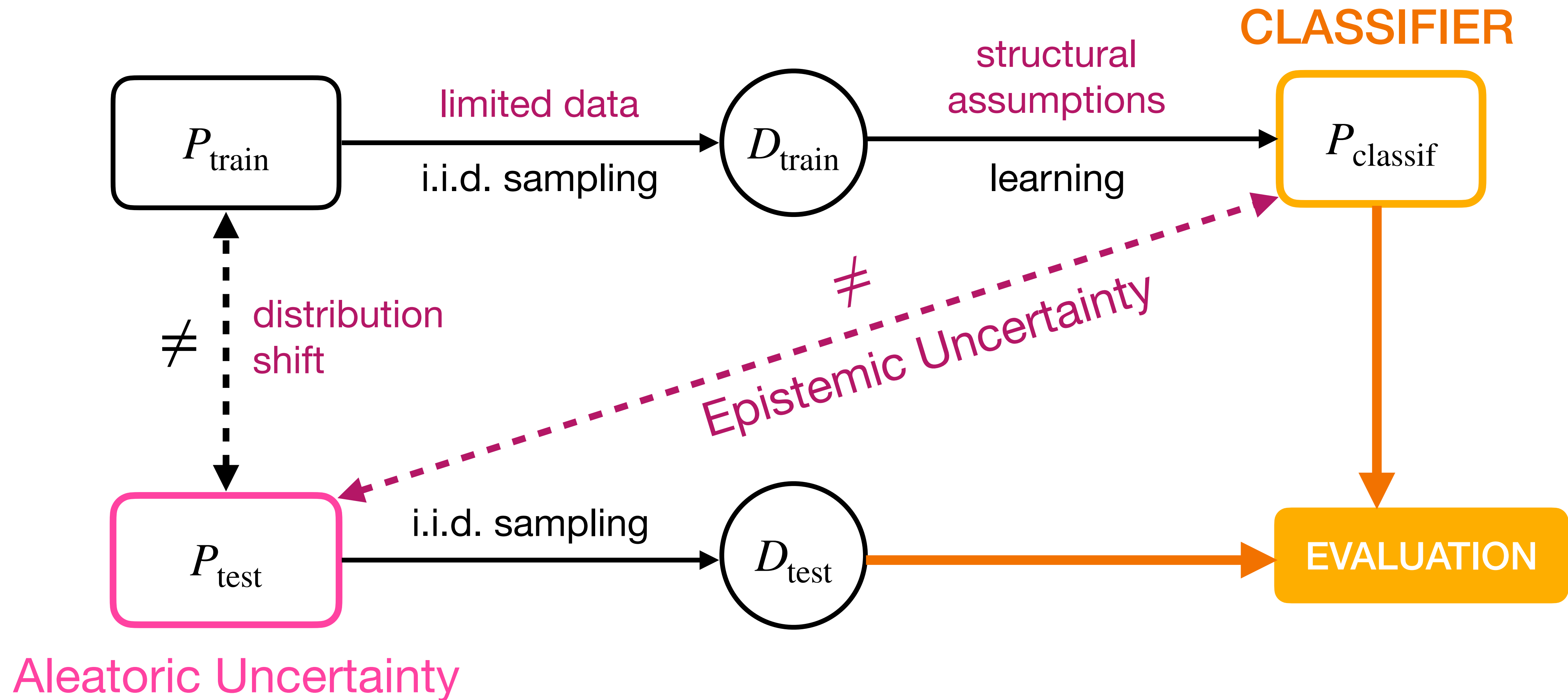
### Abstract

ally different approaches for assessing the reliability  
of a classifier: Robustness Quantification (RQ) and  
We compare both approaches on a number  
There is no clear winner between the two  
combined to obtain a hybrid approach  
of our approach, for each d  
ance of uncertainty and

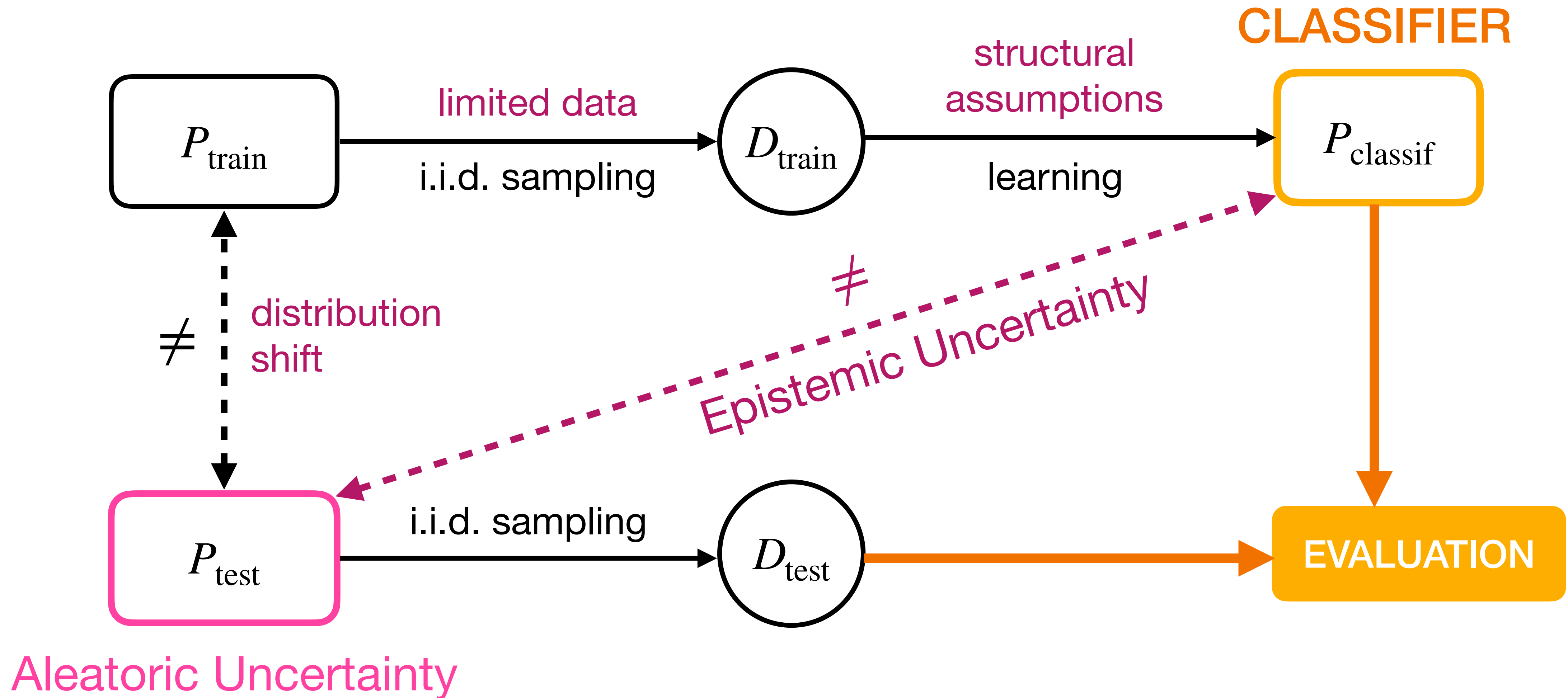
# CLASSIFICATION ... is unreliable



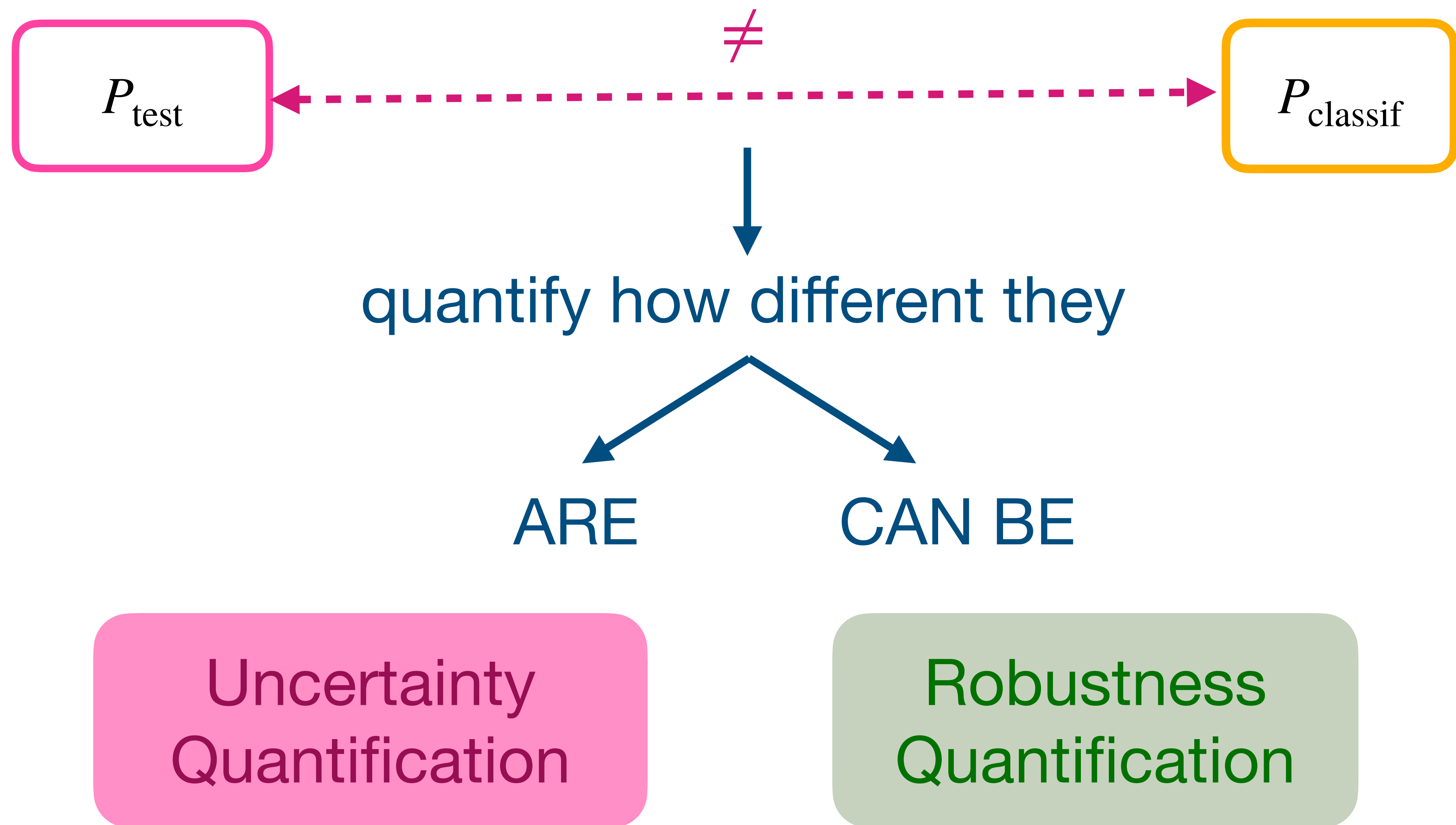
# UNCERTAINTY QUANTIFICATION



# ROBUSTNESS QUANTIFICATION





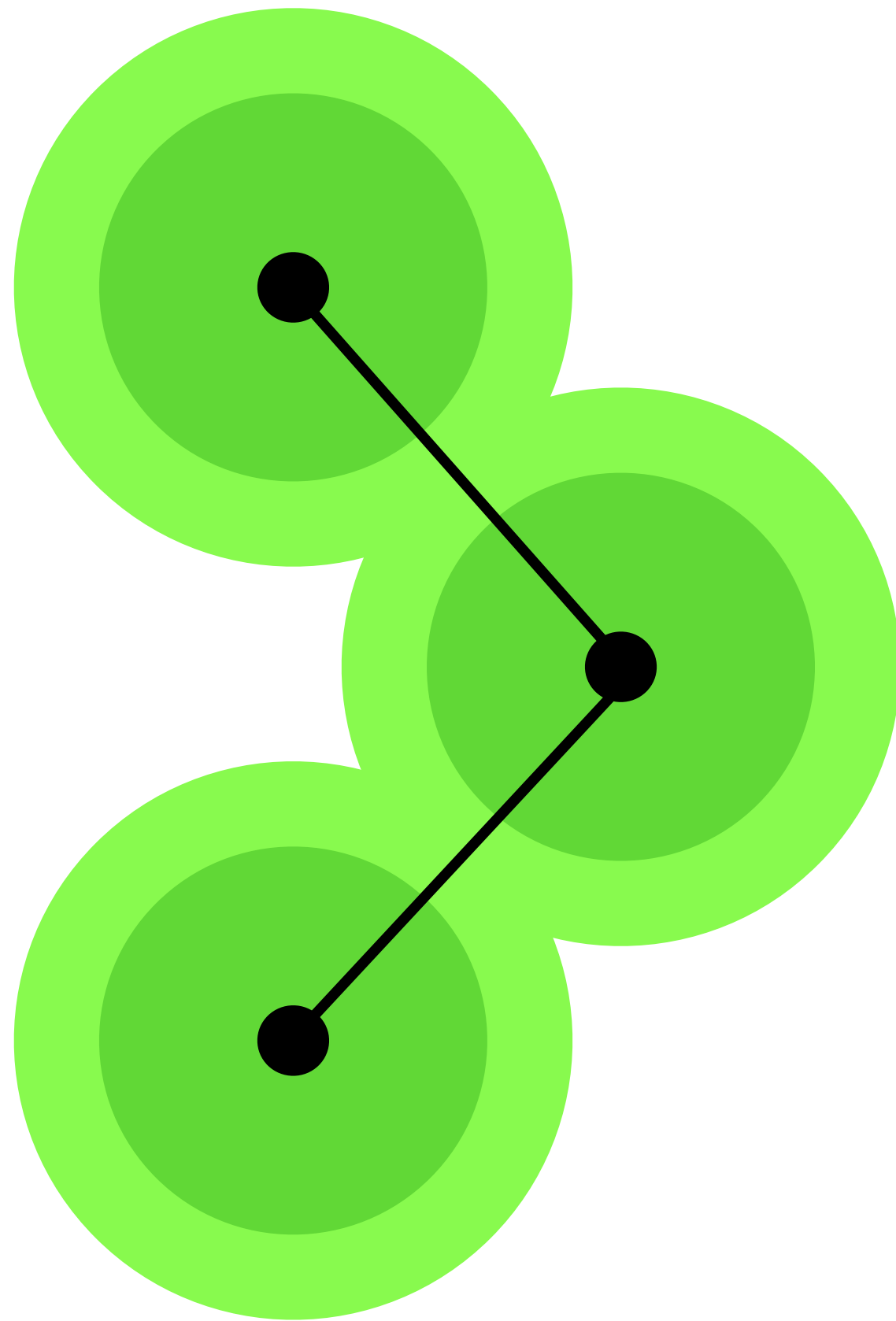


# ROBUSTNESS QUANTIFICATION

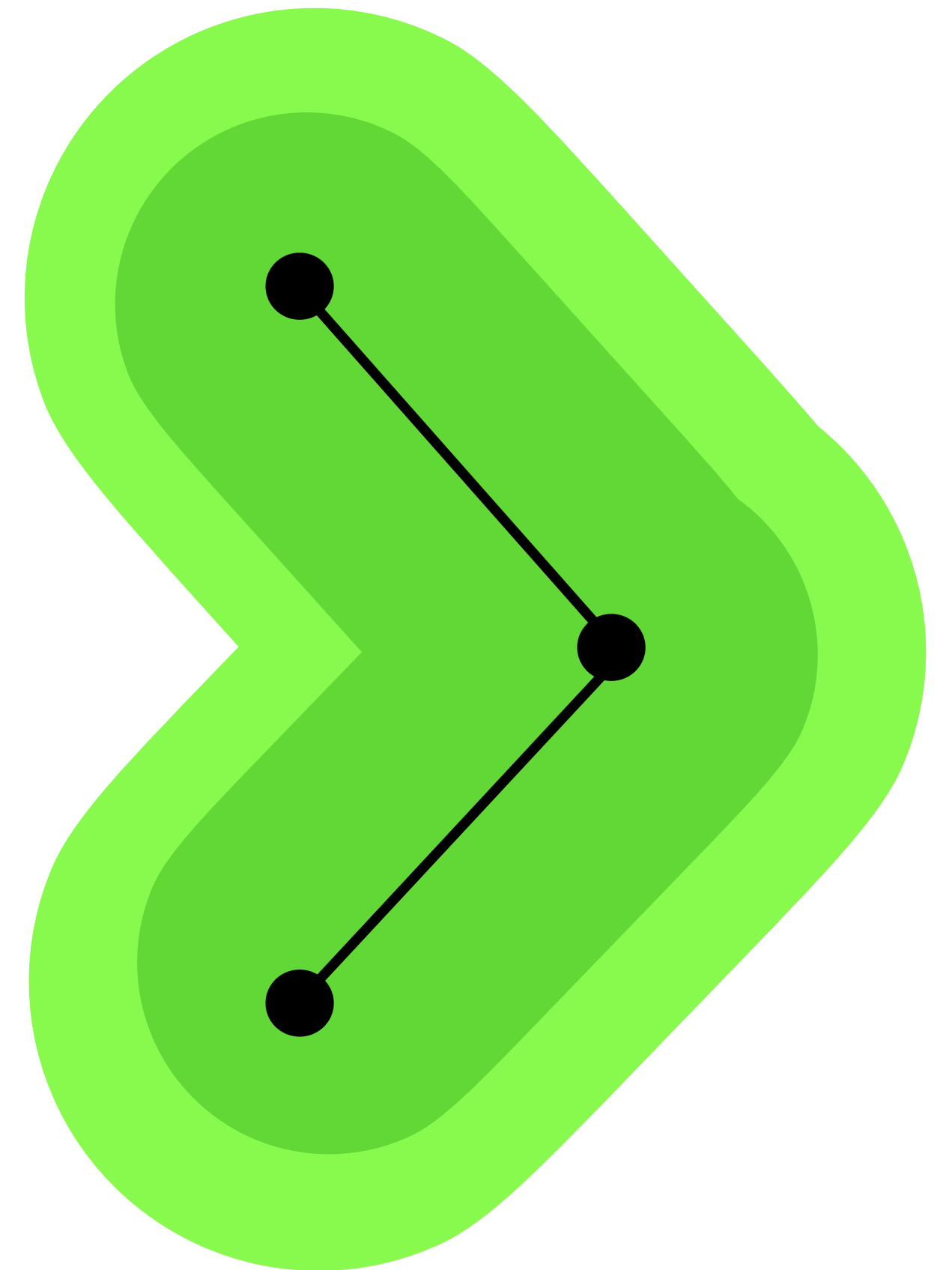
- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ ✓



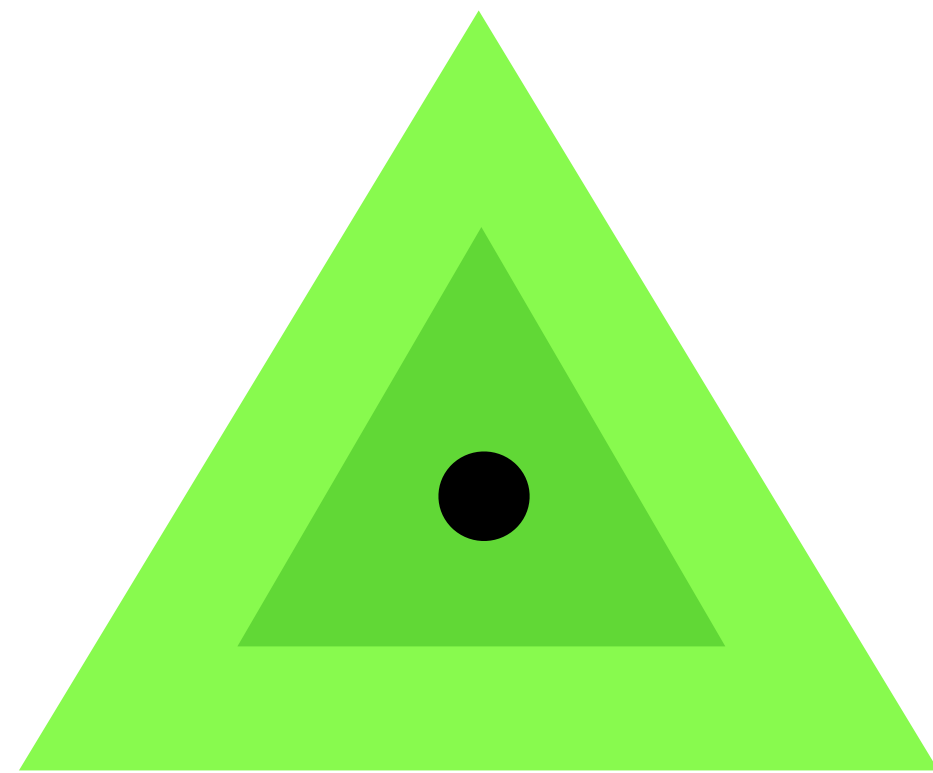
LOCAL



GLOBAL



## $\epsilon$ -CONTAMINATION



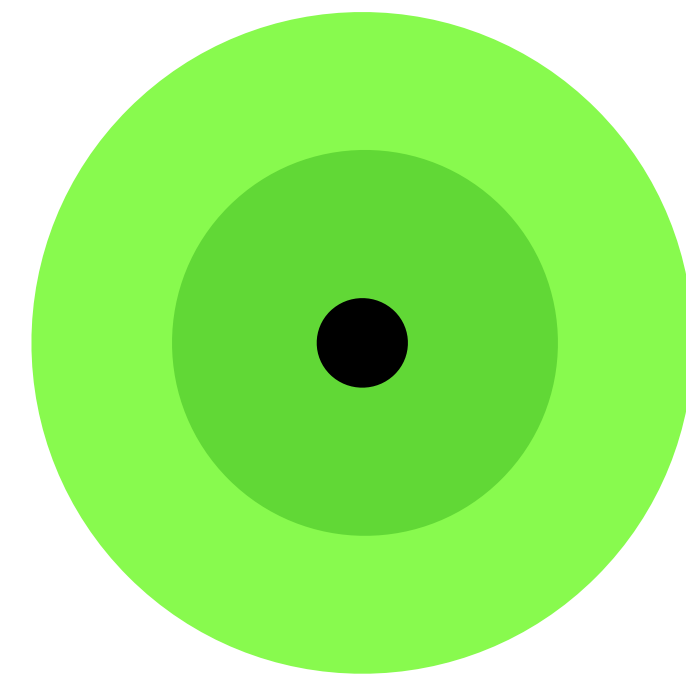
$\mathcal{P}_\epsilon$

$\parallel$

$$\{(1 - \epsilon)P_{\text{classif}} + \epsilon P : P \in \Delta\}$$

## OTHER STUFF

distance-based, ...

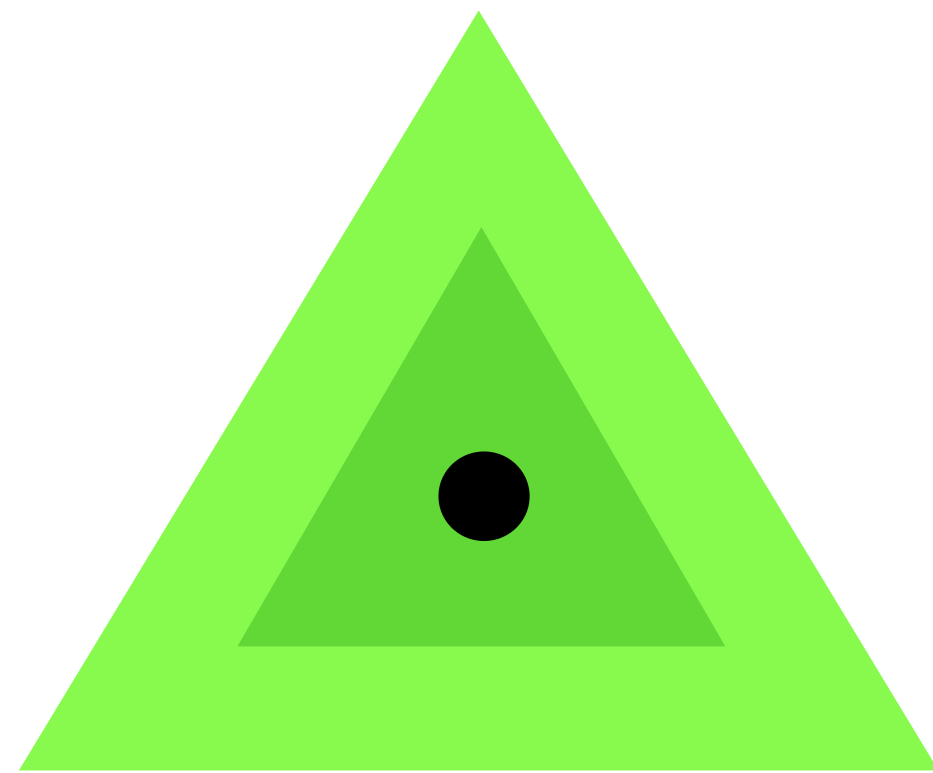


$\mathcal{P}_\epsilon$

$\parallel$

$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$

$\epsilon$ -CONTAMINATION



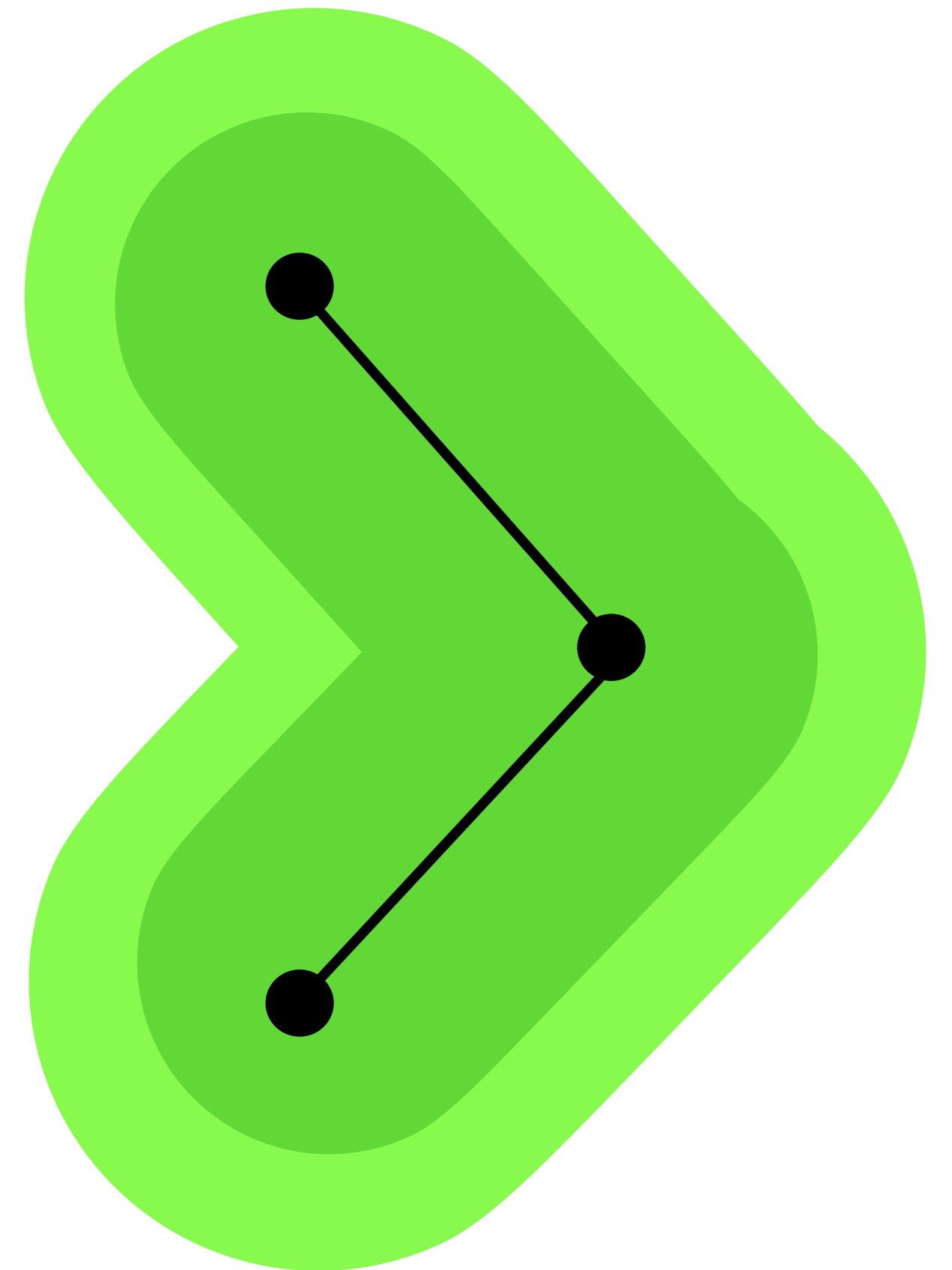
$\mathcal{P}_\epsilon$

$\parallel$

$$\left\{ (1 - \epsilon)P_{\text{classif}} + \epsilon P : P \in \Delta \right\}$$

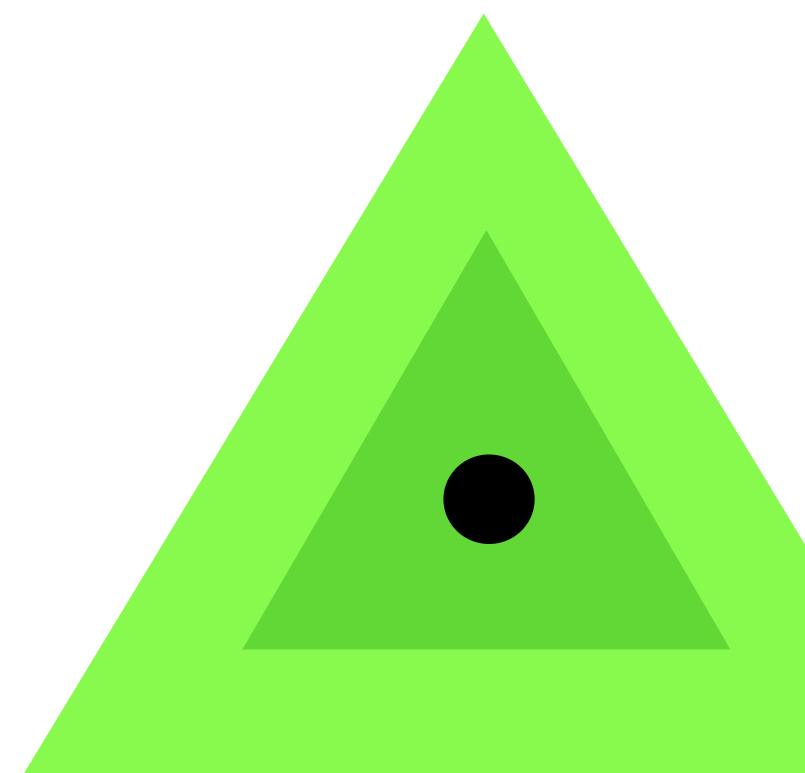


GLOBAL



$\epsilon$ -CONTAMINATION

GLOBAL



$\mathcal{P}_\epsilon$

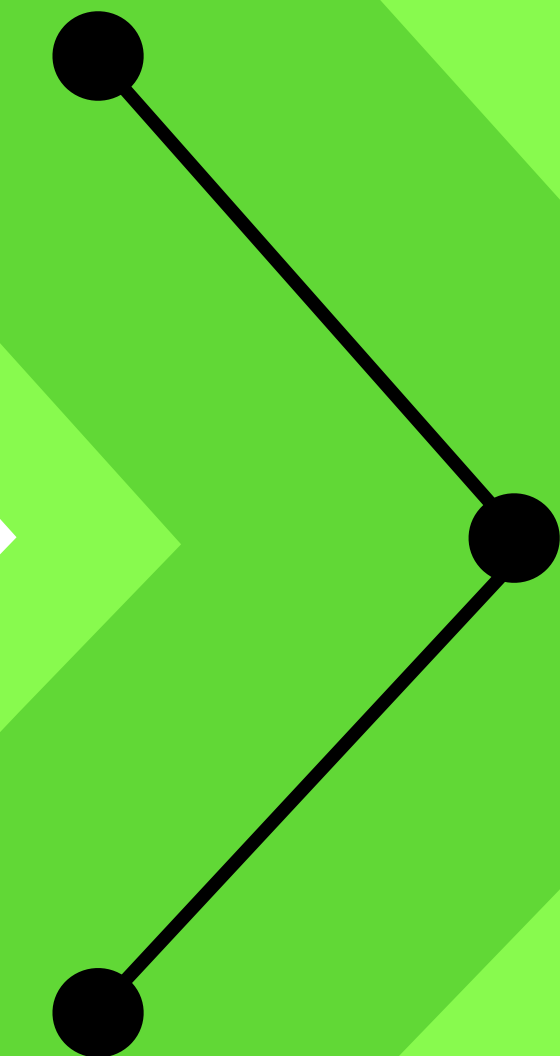
$\parallel$

$$\{(1 - \epsilon)P_{\text{classif}} + \epsilon P : P \in \Delta\}$$

$$\epsilon_{\text{glob}} = \frac{\Delta}{1 + \Delta}$$

$$\Delta = P_{\text{classif}}(x, \hat{y}) - P_{\text{classif}}(x, \hat{y}_2)$$

$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} P_{\text{classif}}(y | x)$$

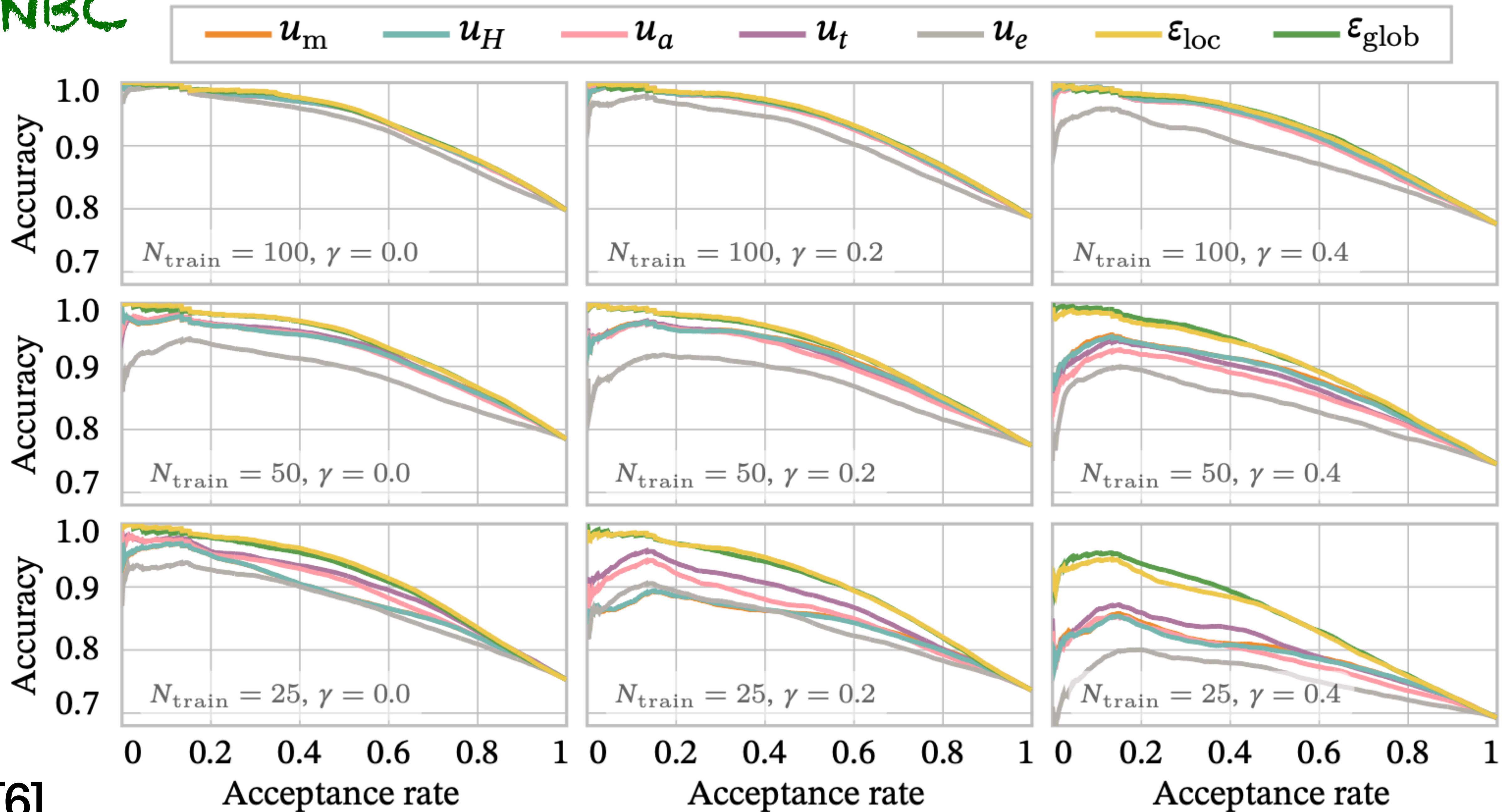


# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓



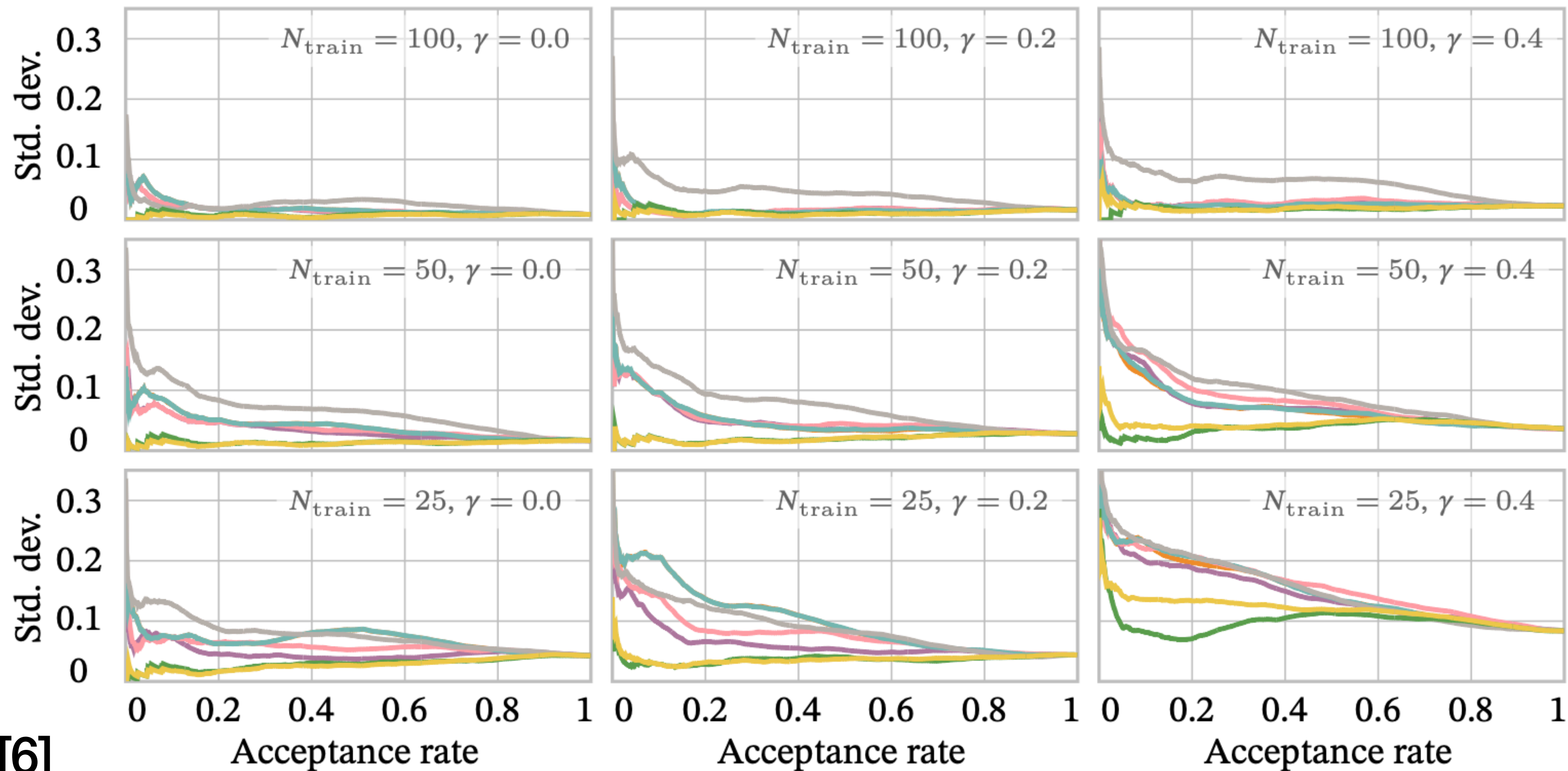
NBC



# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with UQ ✓
- is good with distribution shift and small data sets ✓



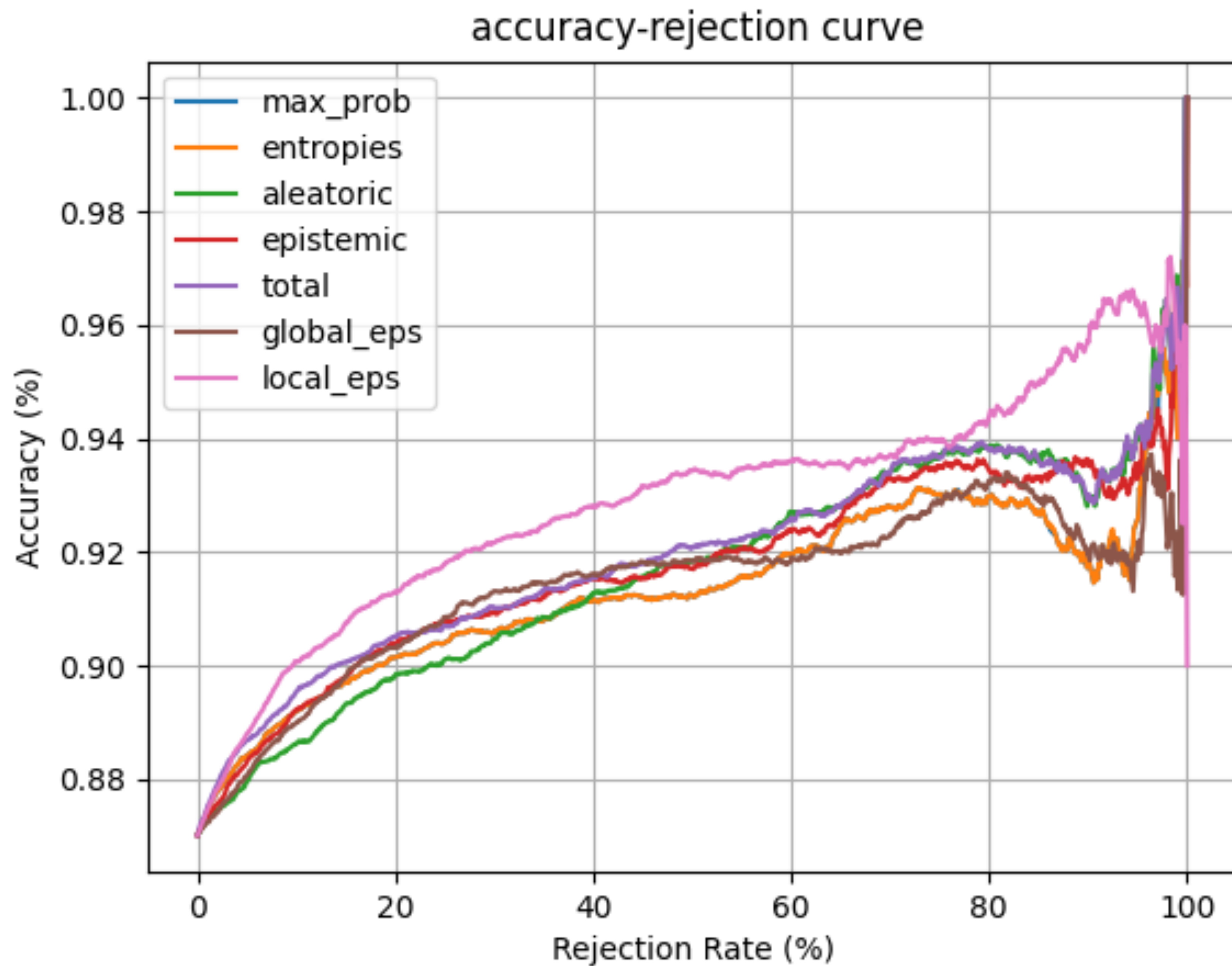




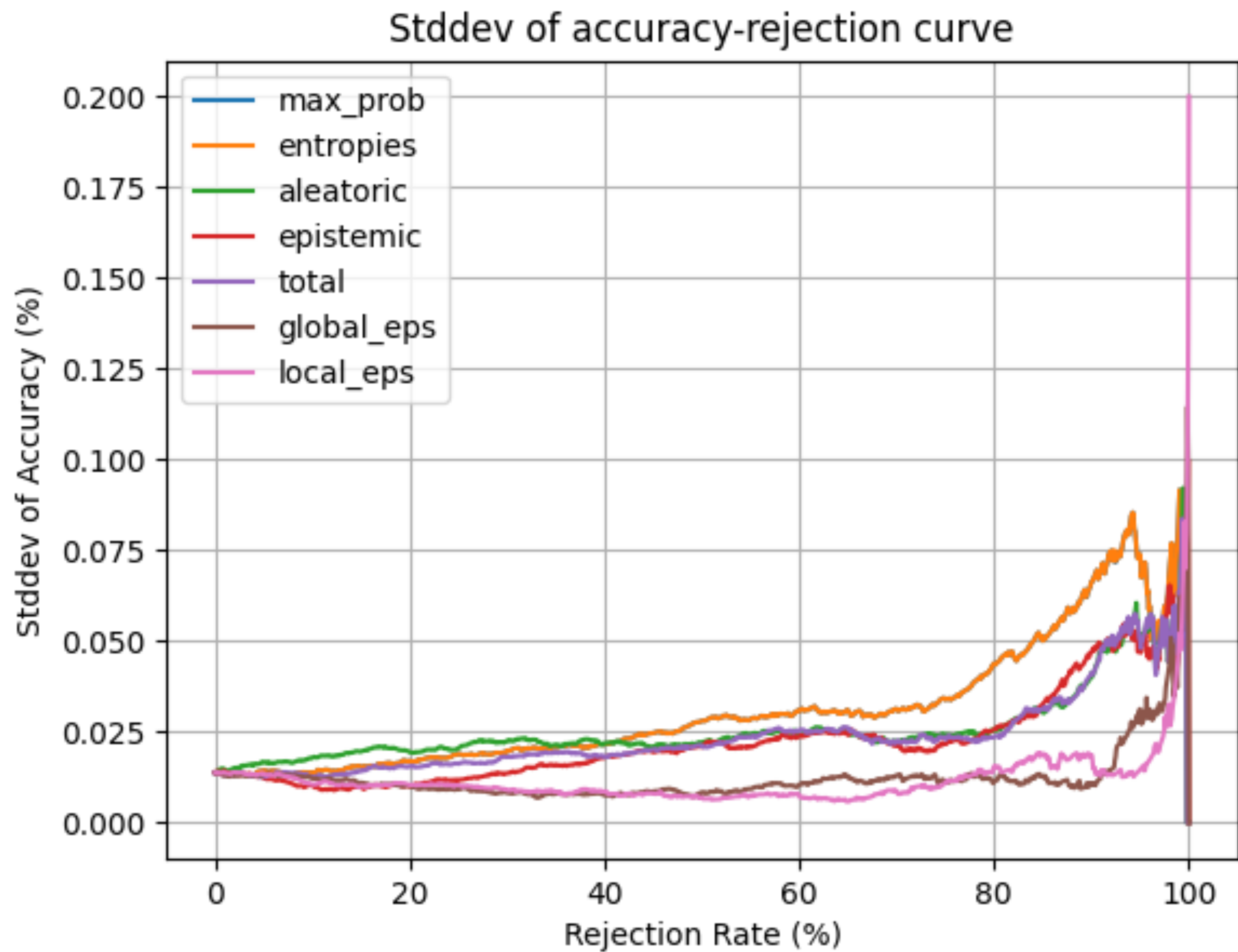
# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations
- is competitive with UQ
- is good with distribution shift and small data sets
- is more stable than UQ ✓

NBC



**NBC**

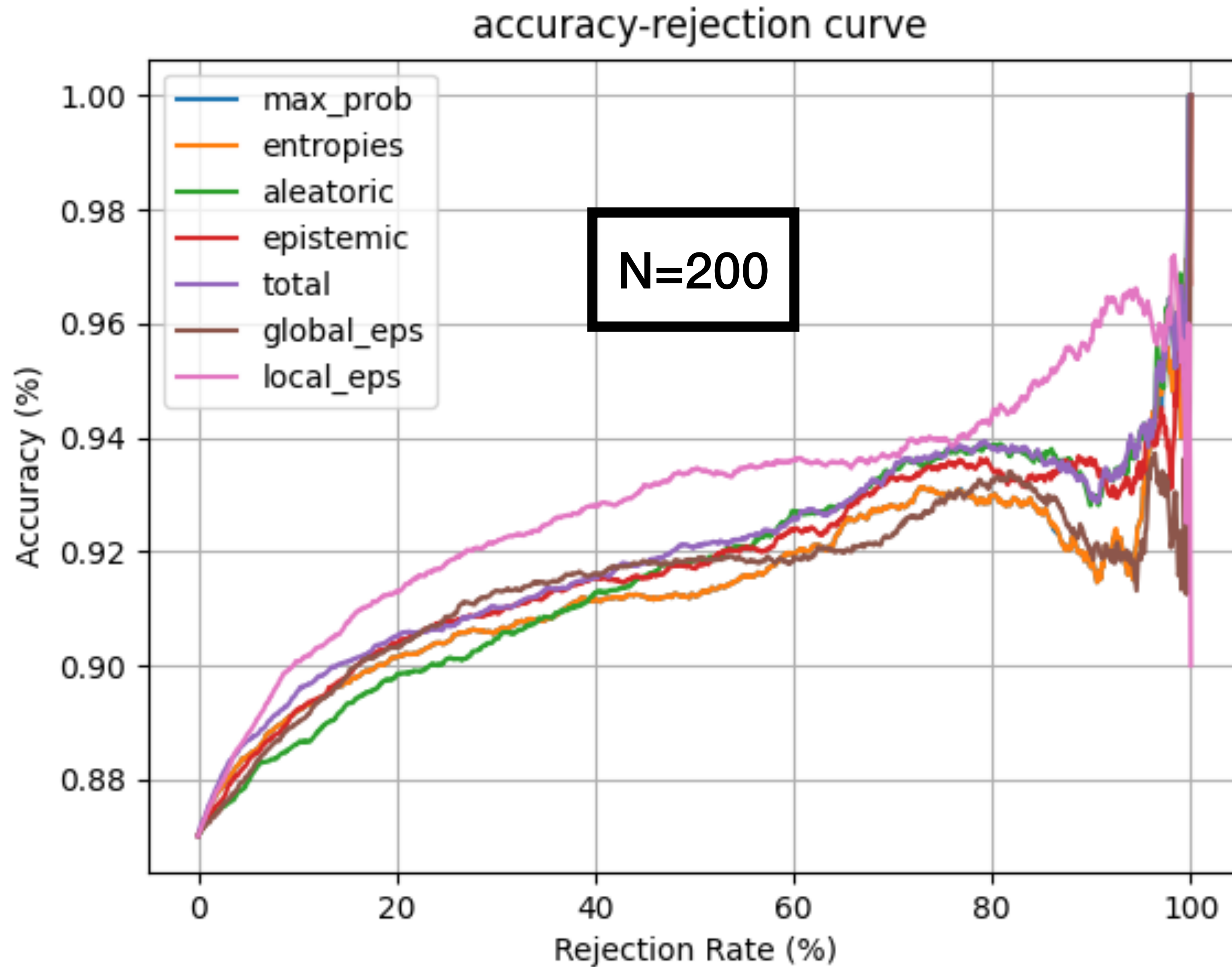


# ROBUSTNESS QUANTIFICATION

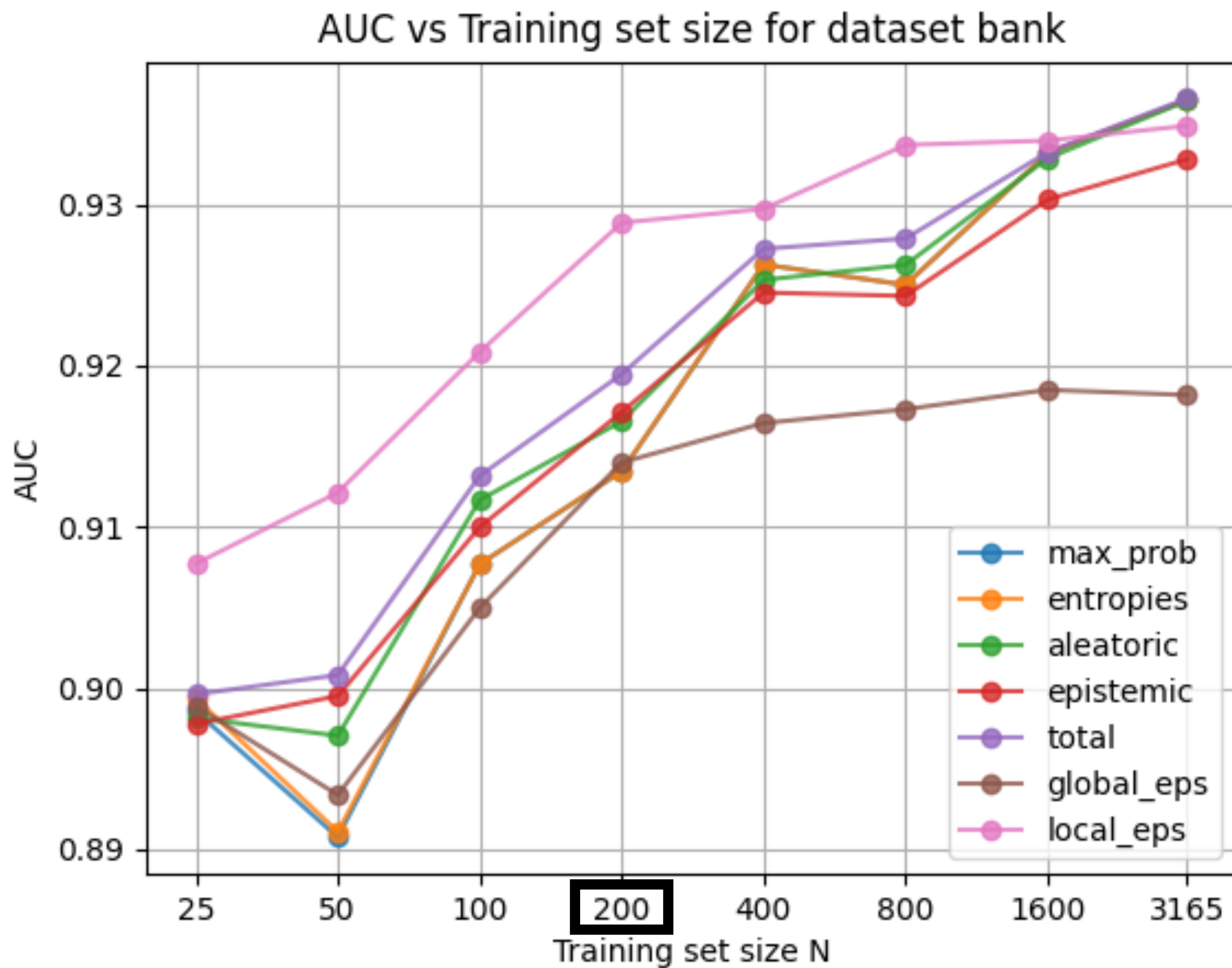
- correlates nicely with accuracy ✓
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with UQ ✓
- is good with distribution shift and small data sets
- is more stable than UQ ✓

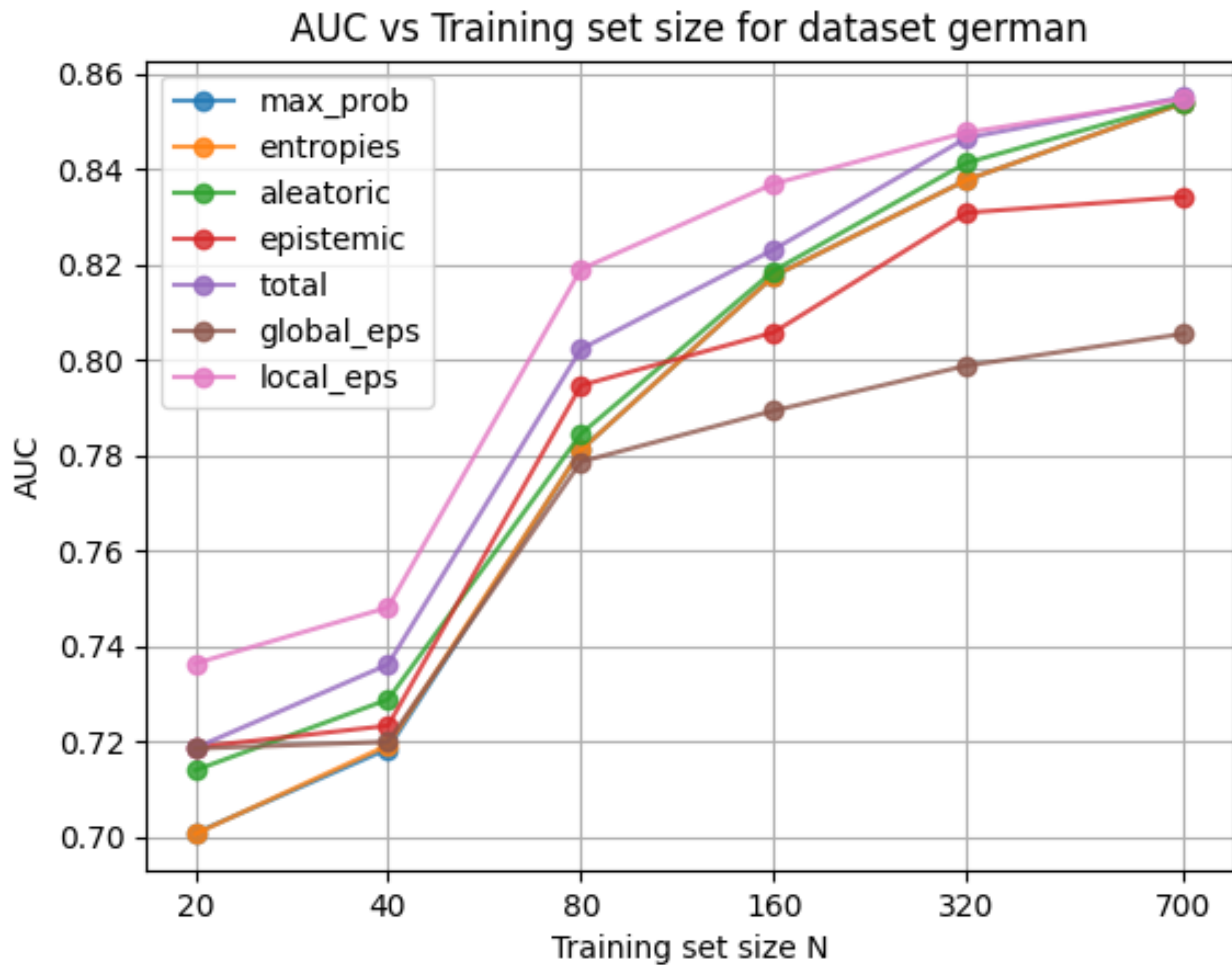


NBC

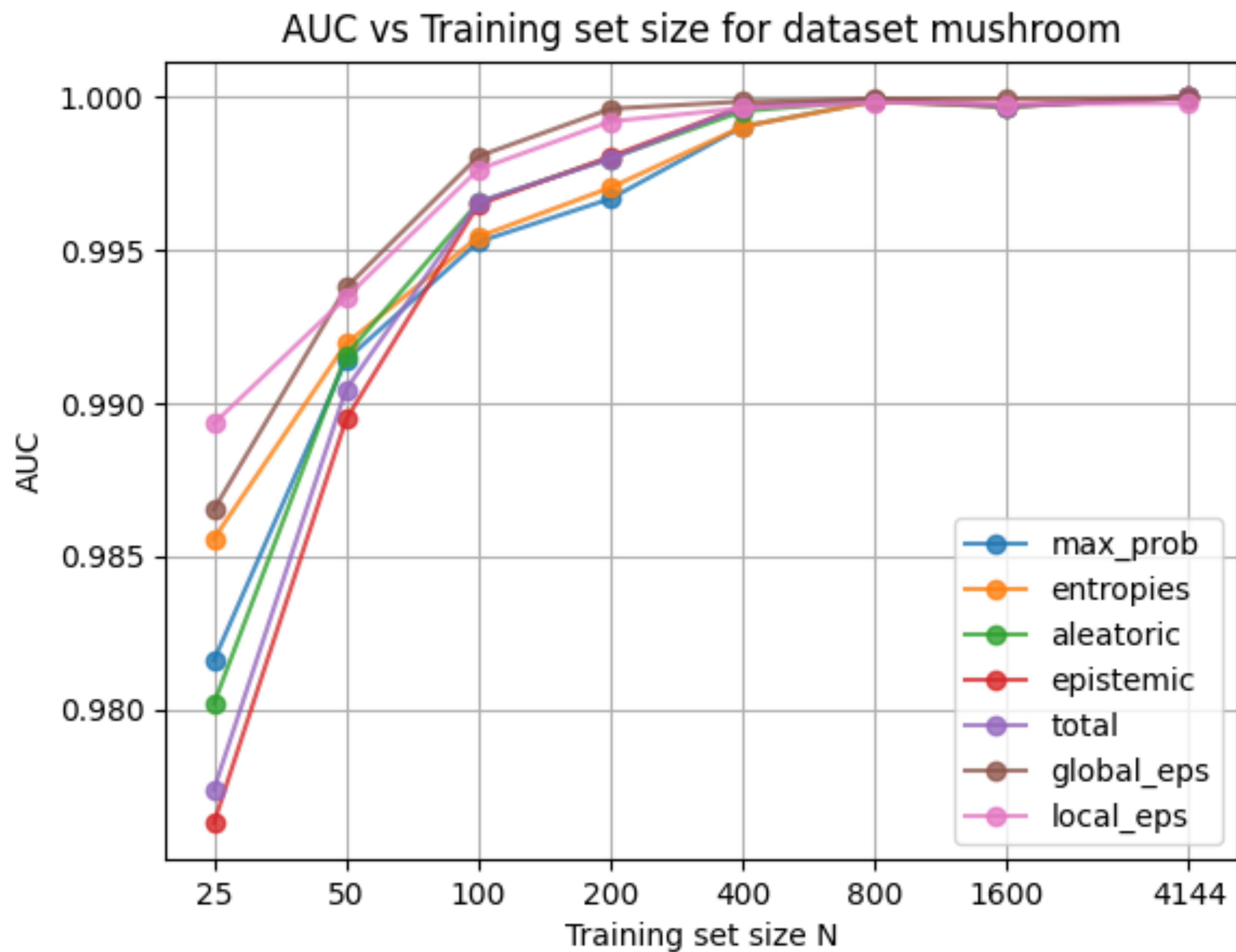








**NBC**

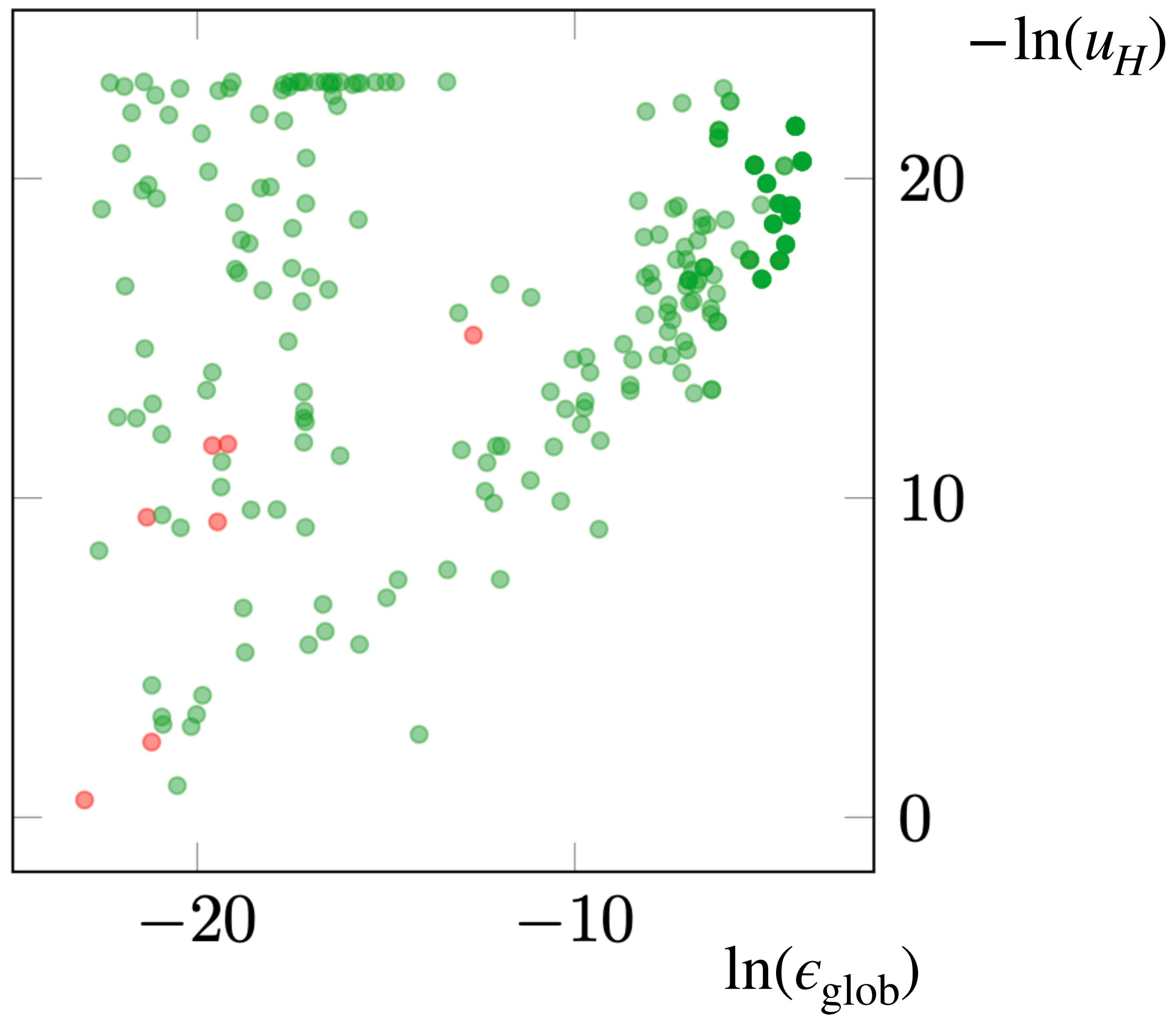


# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with UQ ✓
- is good with distribution shift and small data sets ✓
- is more stable than UQ ✓



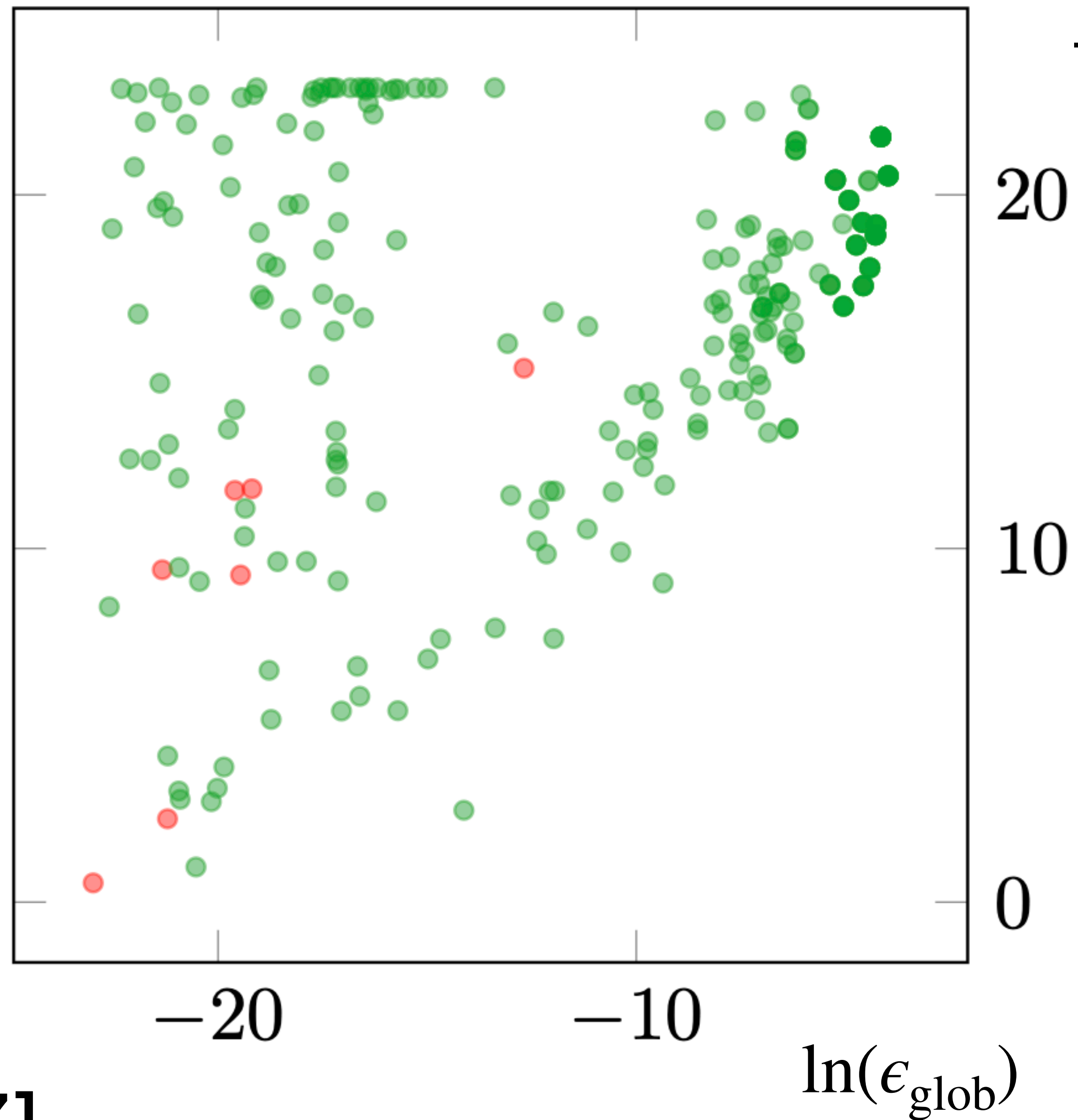
NBC



[7]

# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with and complementary to UQ ✓
- is good with distribution shift and small data sets
- is more stable than UQ

 $-\ln(u_H)$ 

uncertainty ordering

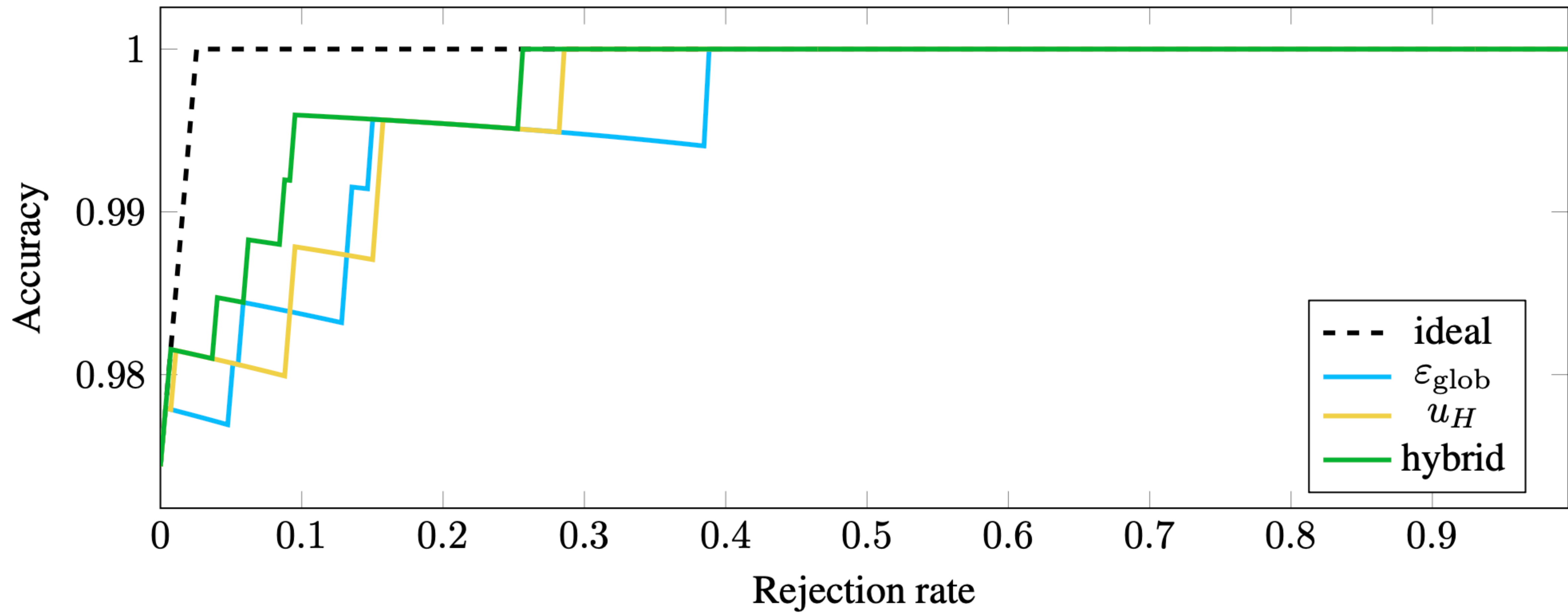
 $n_{u_H,i}$  : order of  $i$  according to  $u_H$ 

robustness ordering

 $n_{\epsilon_{\text{glob}},i}$  : order of  $i$  according to  $u_H$ 

hybrid ordering

$$h_i = \gamma n_{u_H,i} + (1 - \gamma) n_{\epsilon_{\text{glob}},i}$$



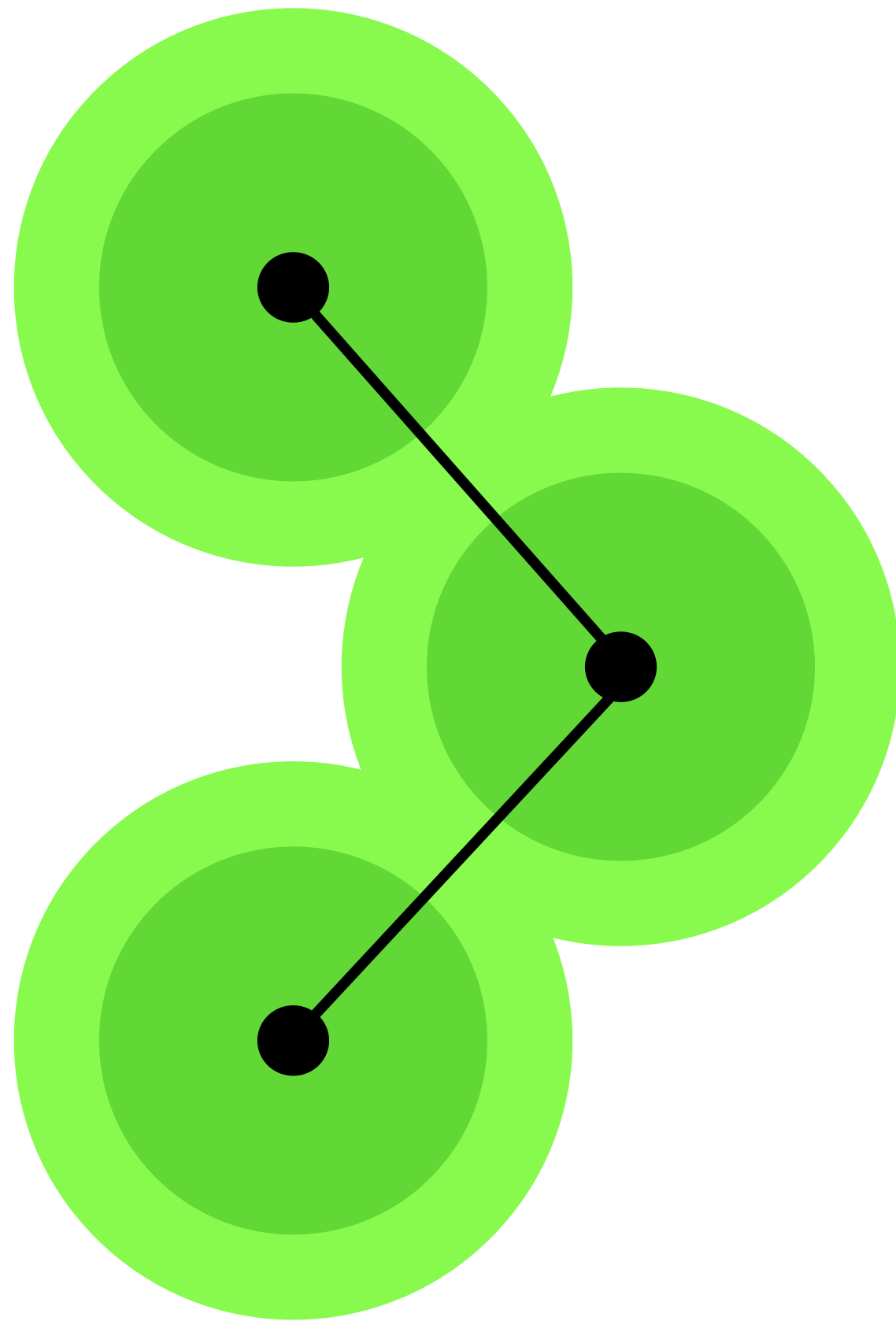


Dataset	$u_H$	$\varepsilon_{loc}$	hybrid	$\gamma$	$\varepsilon_{glob}$	hybrid	$\gamma$
Adult	0.9295	0.9066	<b>0.9295</b>	1.00	0.7690	<b>0.9295</b>	1.00
Austr. Cr.	0.9236	0.9139	<b>0.9265</b>	0.75	0.8872	<b>0.9246</b>	0.86
Bank M.	0.9485	0.9452	<b>0.9485</b>	0.55	0.9299	0.9481	0.88
BCW	0.9968	0.9962	<b>0.9974</b>	0.52	0.9961	<b>0.9978</b>	0.53
German Cr.	0.8338	<b>0.8380</b>	0.8378	0.53	0.7972	<b>0.8376</b>	0.85
Heart dis.	0.7602	0.7540	<b>0.7602</b>	0.95	0.6761	0.7600	0.95
Lymphogr.	0.9440	0.9419	0.9428	0.77	0.8981	0.9425	0.88
NPHA	0.4962	<b>0.5021</b>	0.4917	0.77	<b>0.5159</b>	0.4913	0.96
Nursery	0.9813	0.9822	<b>0.9824</b>	0.28	0.9730	<b>0.9814</b>	0.91
Solar (big)	0.8603	<b>0.8926</b>	0.8874	0.23	0.8693	<b>0.8836</b>	0.71
Solar (small)	0.8709	0.8597	0.8666	0.19	0.7990	<b>0.8797</b>	0.78
SPECT	0.9458	0.8915	<b>0.9458</b>	0.99	0.5738	0.9457	0.99
Stud. Math	0.9434	0.9465	<b>0.9468</b>	0.31	0.9205	<b>0.9445</b>	0.60
Stud. Port	0.8898	<b>0.9276</b>	0.9093	0.77	0.8952	<b>0.9067</b>	0.79

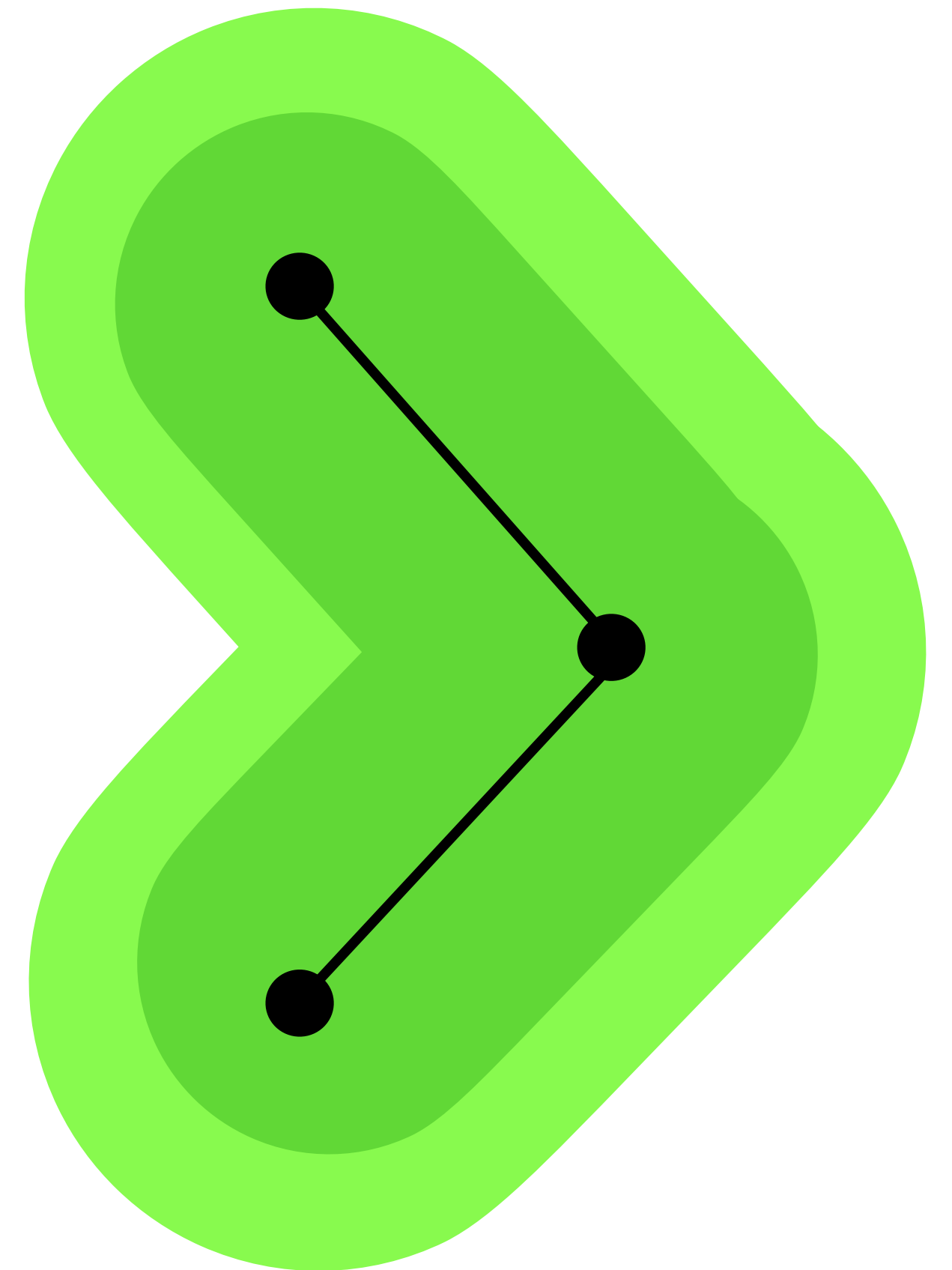
# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with and complementary to UQ ✓
- is good with distribution shift and small data sets
- is more stable than UQ

LOCAL

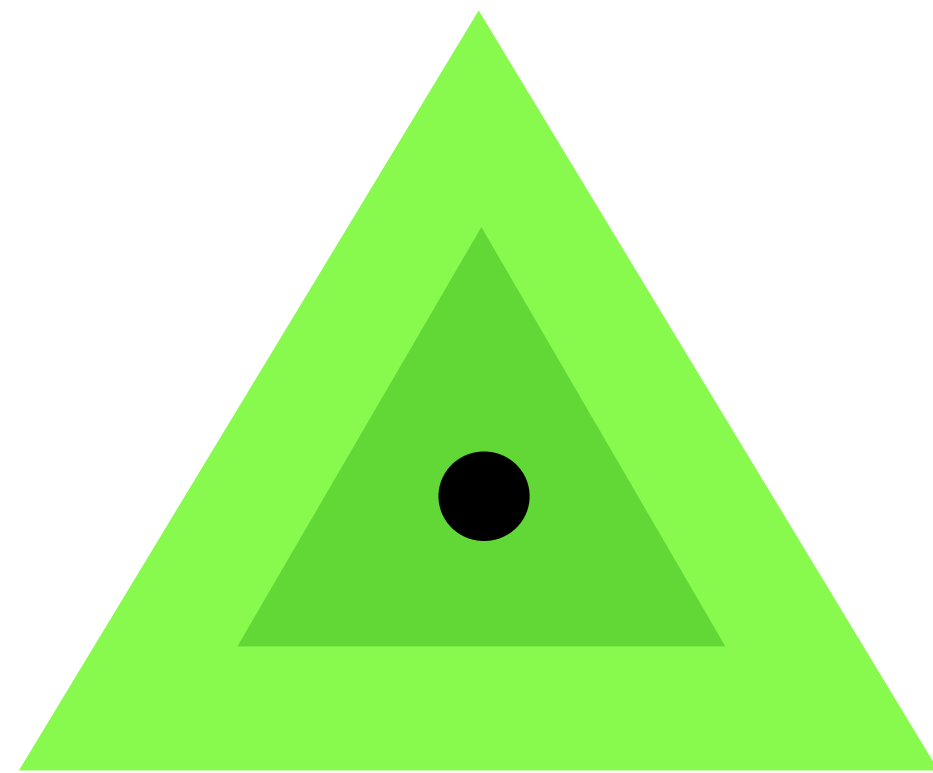


GLOBAL





## $\epsilon$ -CONTAMINATION



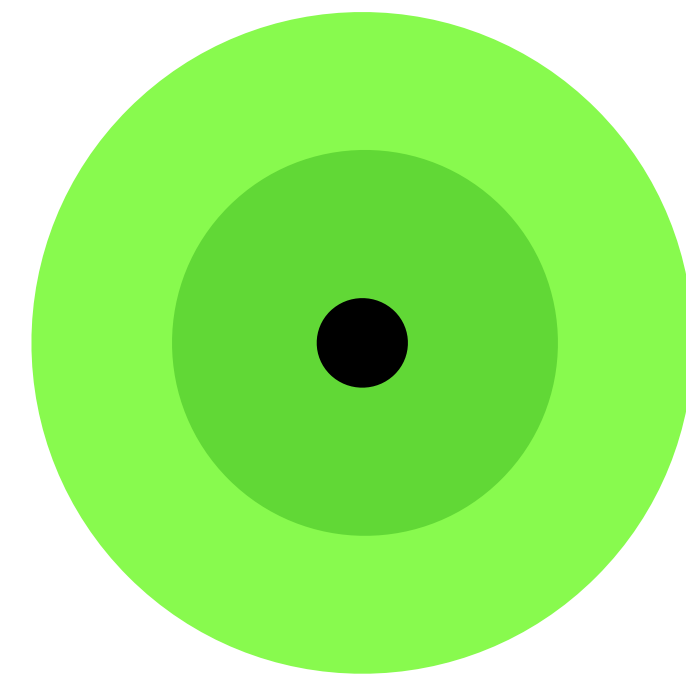
$\mathcal{P}_\epsilon$

$\parallel$

$$\left\{ (1 - \epsilon)P_{\text{classif}} + \epsilon P : P \in \Delta \right\}$$

## OTHER STUFF

distance-based, ...



$\mathcal{P}_\epsilon$

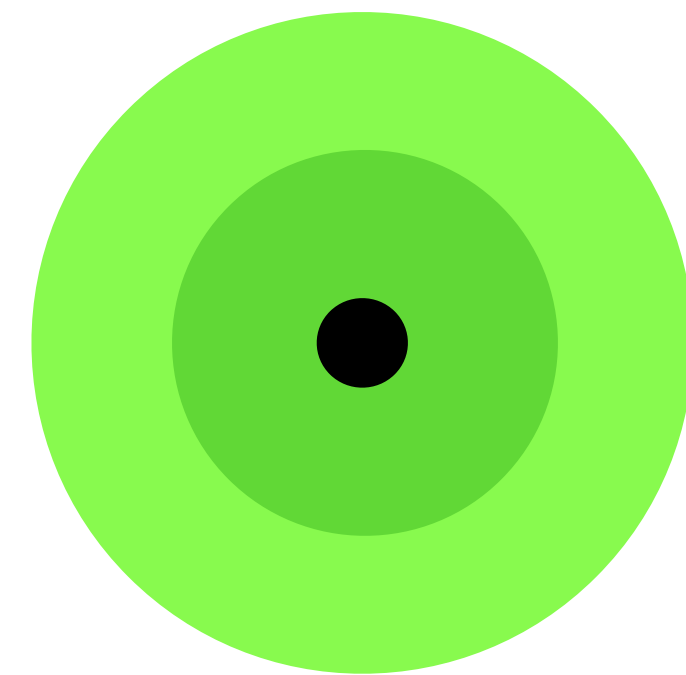
$\parallel$

$$\left\{ P \in \Delta : d(P_{\text{classif}}, P) < \epsilon \right\}$$



## OTHER STUFF

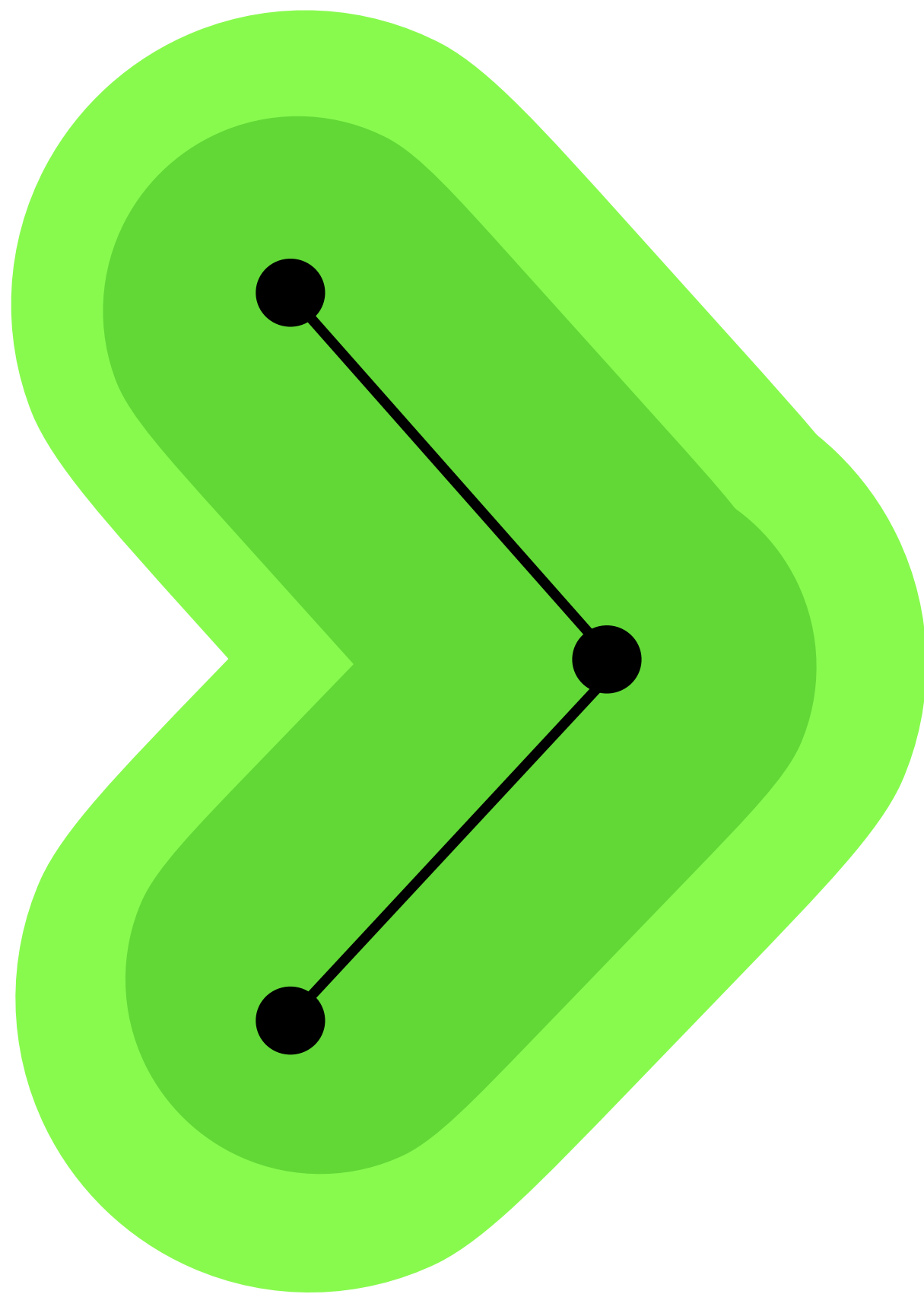
distance-based, ...



$$d(P_1, P_2) = \max \left\{ \sup_A \frac{P_1(A)}{P_2(A)}, \sup_A \frac{P_2(A)}{P_1(A)} \right\}$$

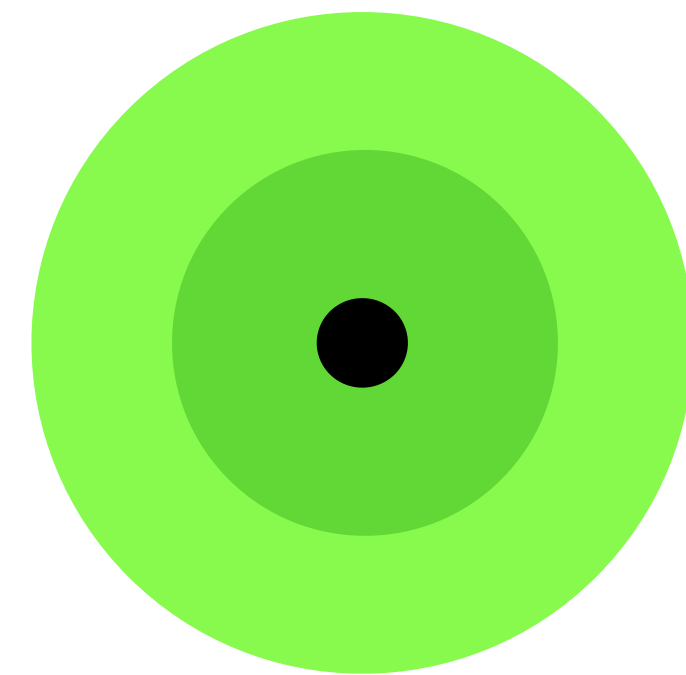
$$\begin{aligned} & \mathcal{P}_\epsilon \\ & \parallel \\ & \{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\} \end{aligned}$$

GLOBAL



OTHER STUFF

distance-based, ...



$\mathcal{P}_\epsilon$

$\parallel$

$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$

## GLOBAL

discrete features:

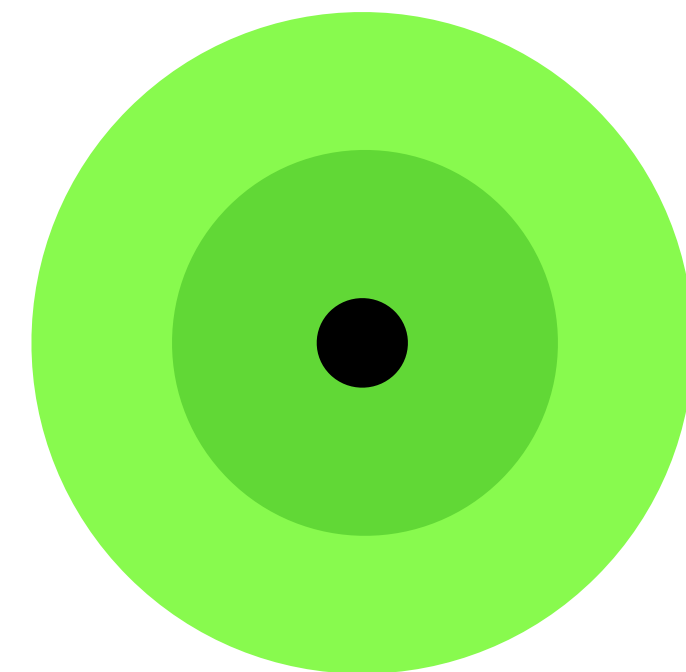
$$\epsilon_{\text{glob}} = \min \left\{ \frac{1}{1 - \Delta}, \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}} \right\}$$

$$\Delta = P_{\text{classif}}(x, \hat{y}) - P_{\text{classif}}(x, \hat{y}_2)$$

$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} P_{\text{classif}}(y | x)$$

## OTHER STUFF

distance-based, ...

 $\mathcal{P}_\epsilon$  $\parallel$ 

$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$

## GLOBAL

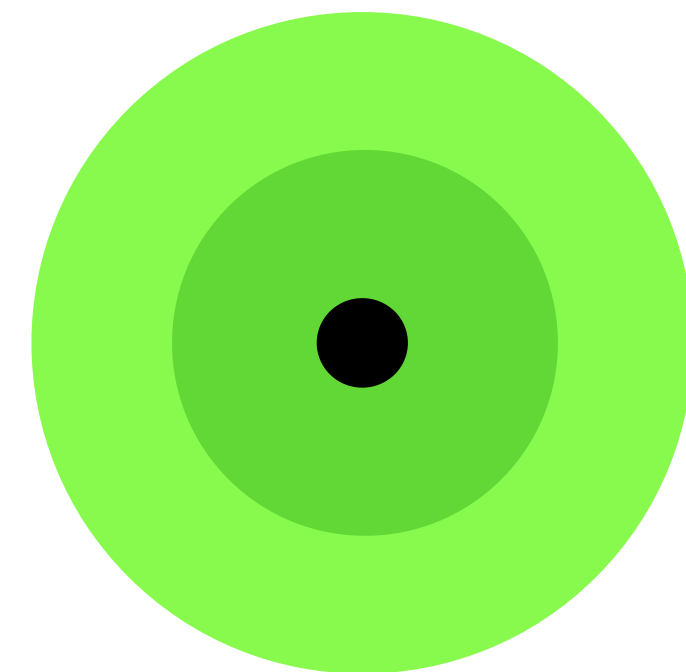
at least one continuous feature:

$$\epsilon_{\text{glob}} = \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}}$$

$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} P_{\text{classif}}(y | x)$$

## OTHER STUFF

distance-based, ...

 $\mathcal{P}_\epsilon$  $\parallel$ 

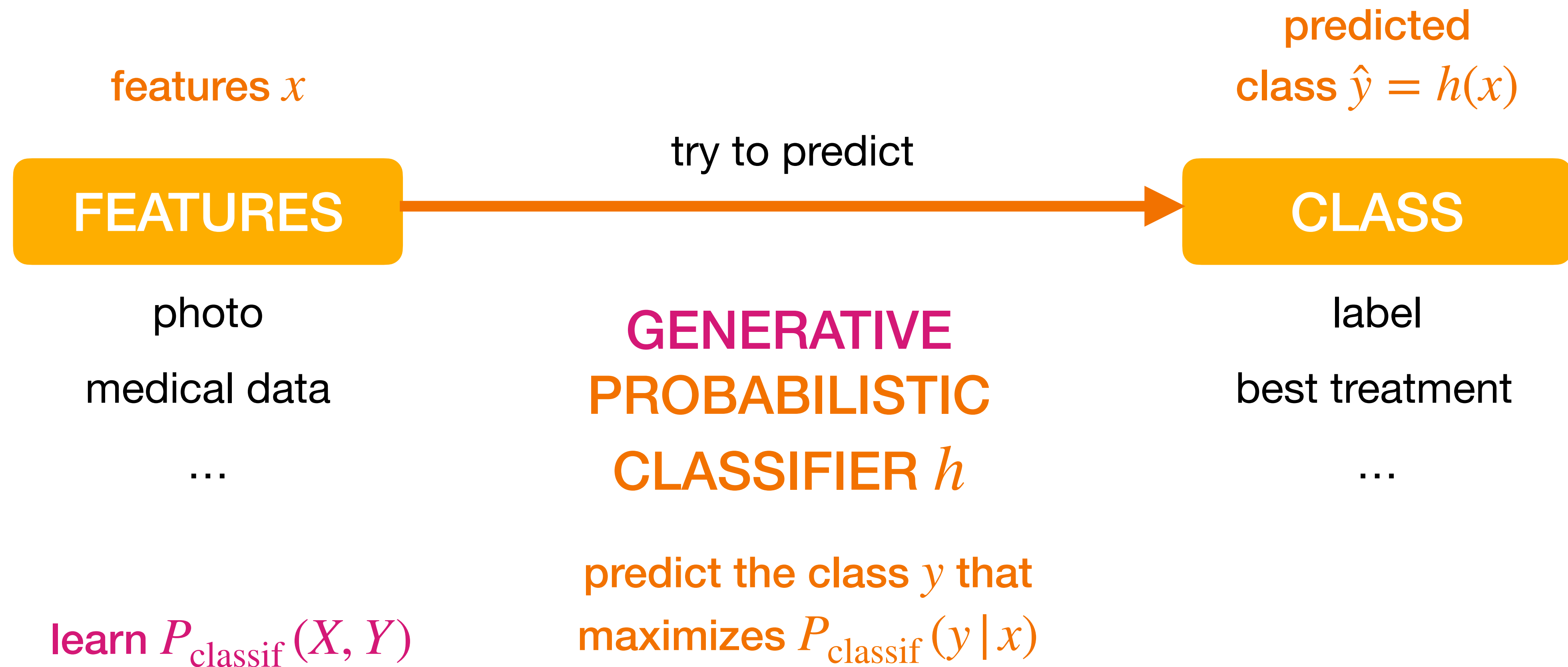
$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$



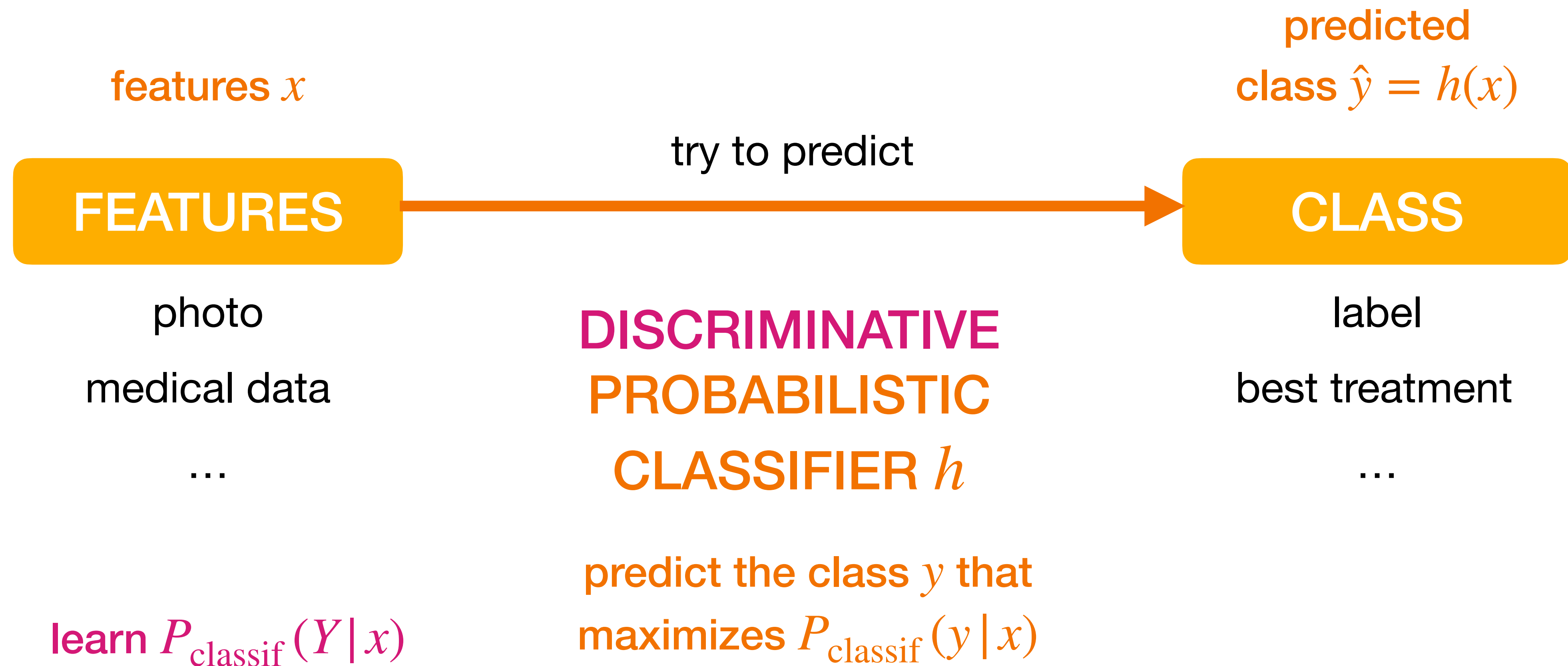
# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations
- is competitive with and complementary to UQ
- is good with distribution shift and small data sets
- is more stable than UQ
- is not limited to epsilon-contamination ✓

# CLASSIFICATION



# CLASSIFICATION



## GLOBAL

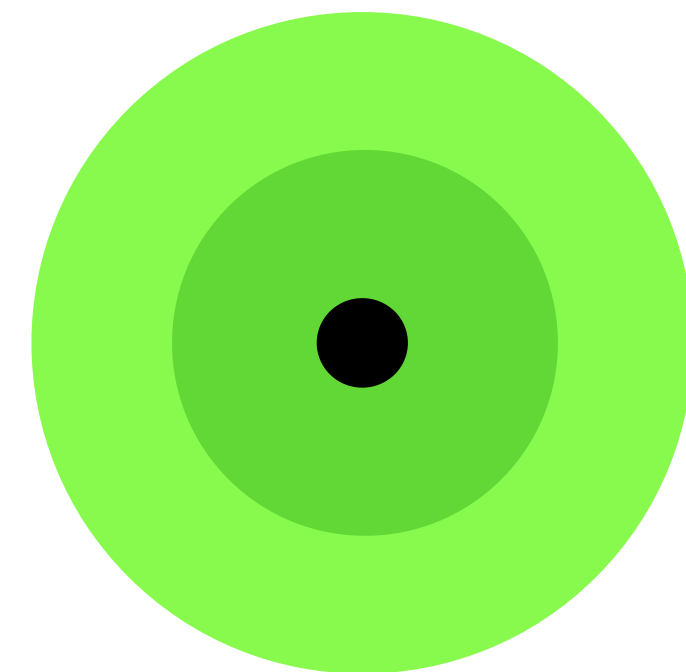
at least one continuous feature:

$$\epsilon_{\text{glob}} = \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}}$$

$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} P_{\text{classif}}(y | x)$$

## OTHER STUFF

distance-based, ...

 $\mathcal{P}_\epsilon$  $\parallel$ 

$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$



## GLOBAL

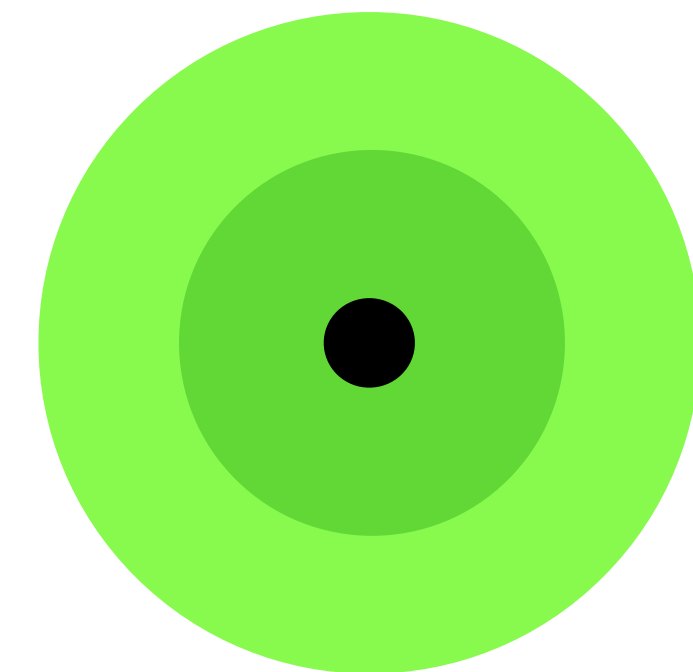
at least one continuous feature:

$$\epsilon_{\text{glob}} = \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}} = \sqrt{\frac{P_{\text{classif}}(\hat{y} | x)}{P_{\text{classif}}(\hat{y}_2 | x)}}$$

$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} P_{\text{classif}}(y | x)$$

## OTHER STUFF

distance-based, ...

 $\mathcal{P}_\epsilon$  $\parallel$ 

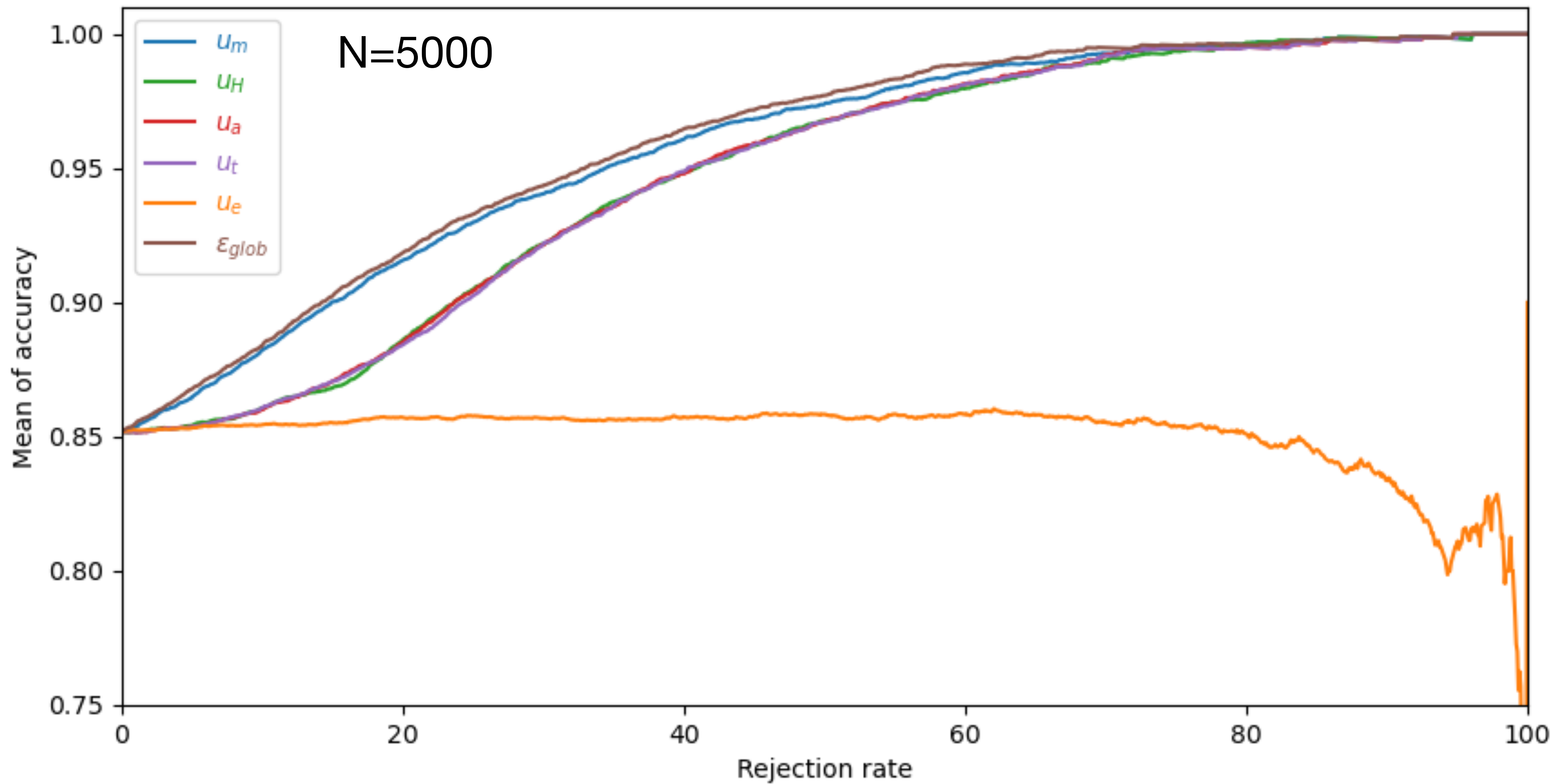
$$\{P \in \Delta : d(P_{\text{classif}}, P) < \epsilon\}$$

# ROBUSTNESS QUANTIFICATION

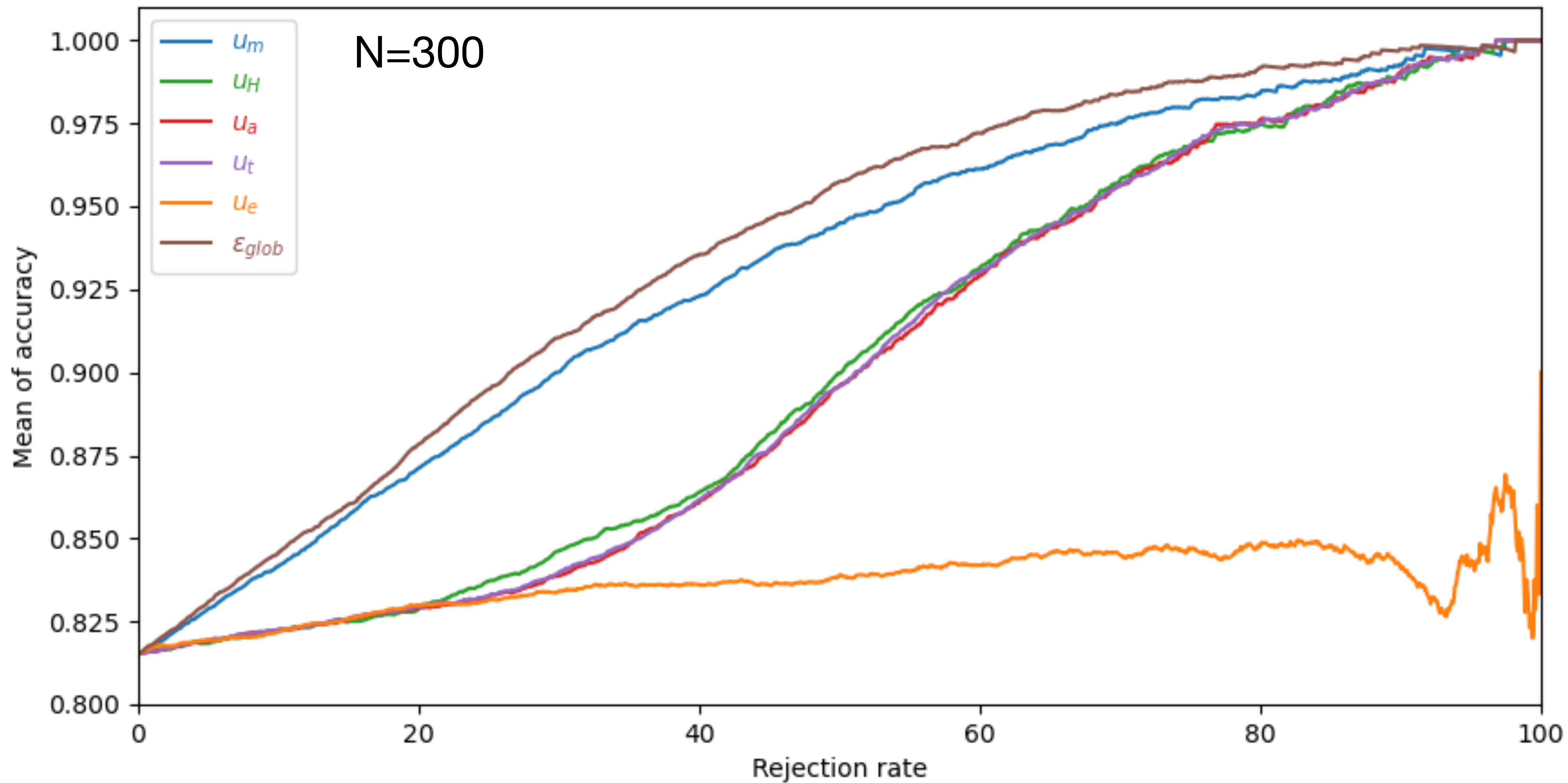
- correlates nicely with accuracy
- works for different types of model architectures
- is conceptually different from UQ
- also works with global perturbations
- is competitive with and complementary to UQ
- is good with distribution shift and small data sets
- is more stable than UQ
- is not limited to epsilon-contamination
- also works for discriminative classifiers ✓

RF

N=5000



RF





# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures ✓
- is conceptually different from UQ
- also works with global perturbations ✓
- is competitive with and complementary to UQ ✓
- is good with distribution shift and small data sets ✓
- is more stable than UQ
- is not limited to epsilon-contamination ✓
- also works for discriminative classifiers ✓

# ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures ✓
- is conceptually different from UQ ✓
- also works with global perturbations ✓
- is competitive with and complementary to UQ ✓
- is good with distribution shift and small data sets ✓
- is more stable than UQ ✓
- is not limited to epsilon-contamination ✓
- also works for discriminative classifiers ✓

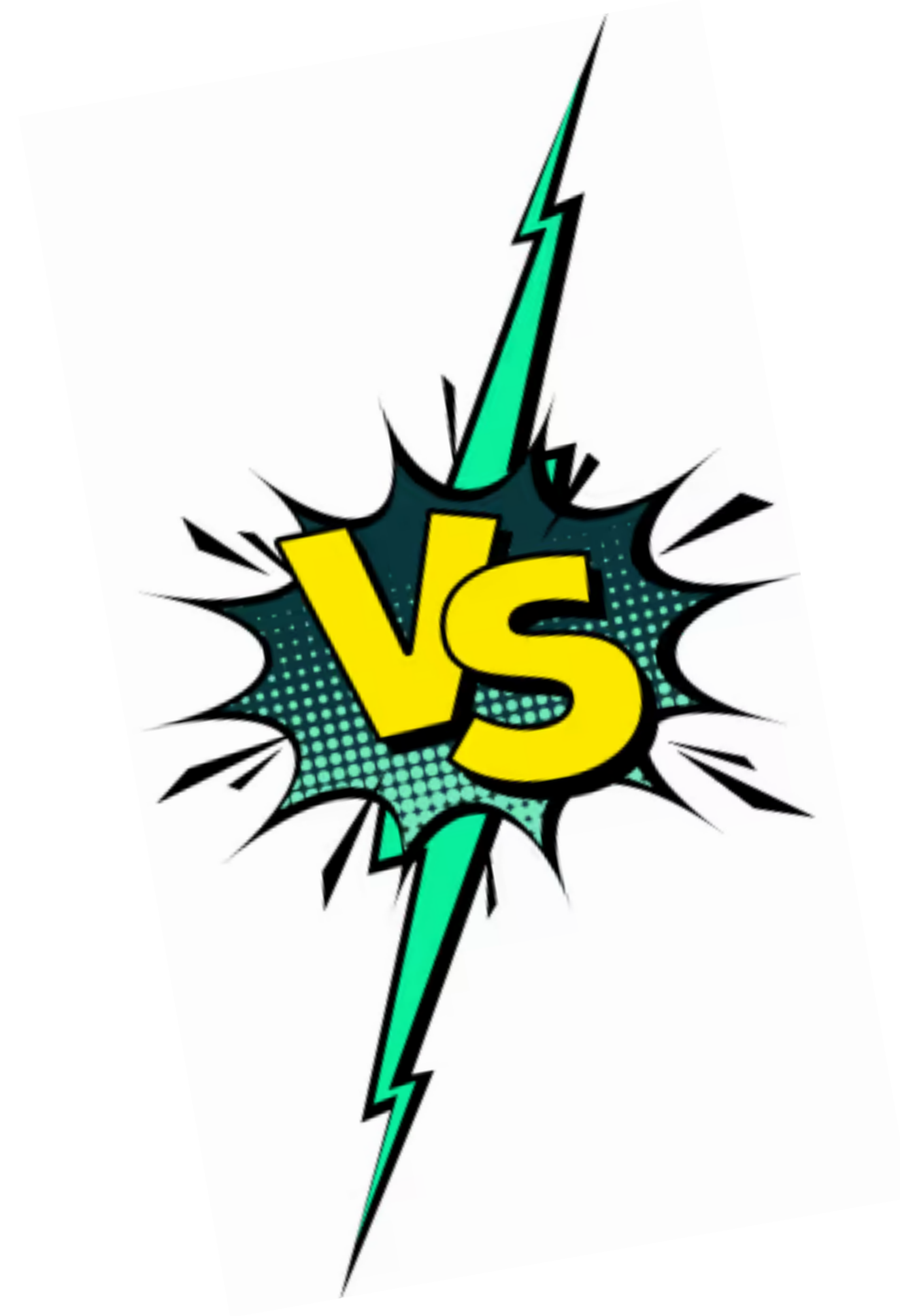
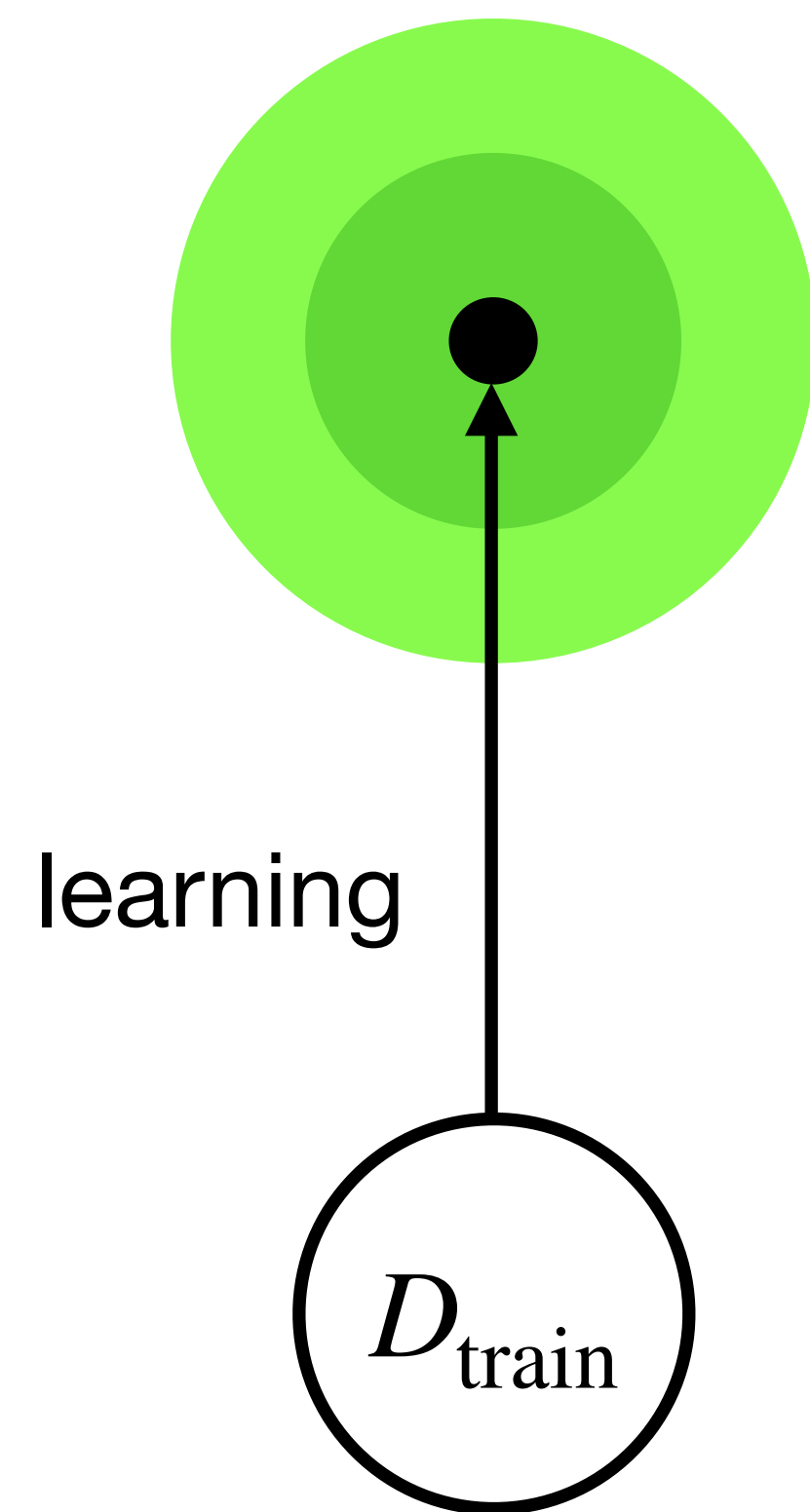


**BUT...WAIT! THERES MORE**

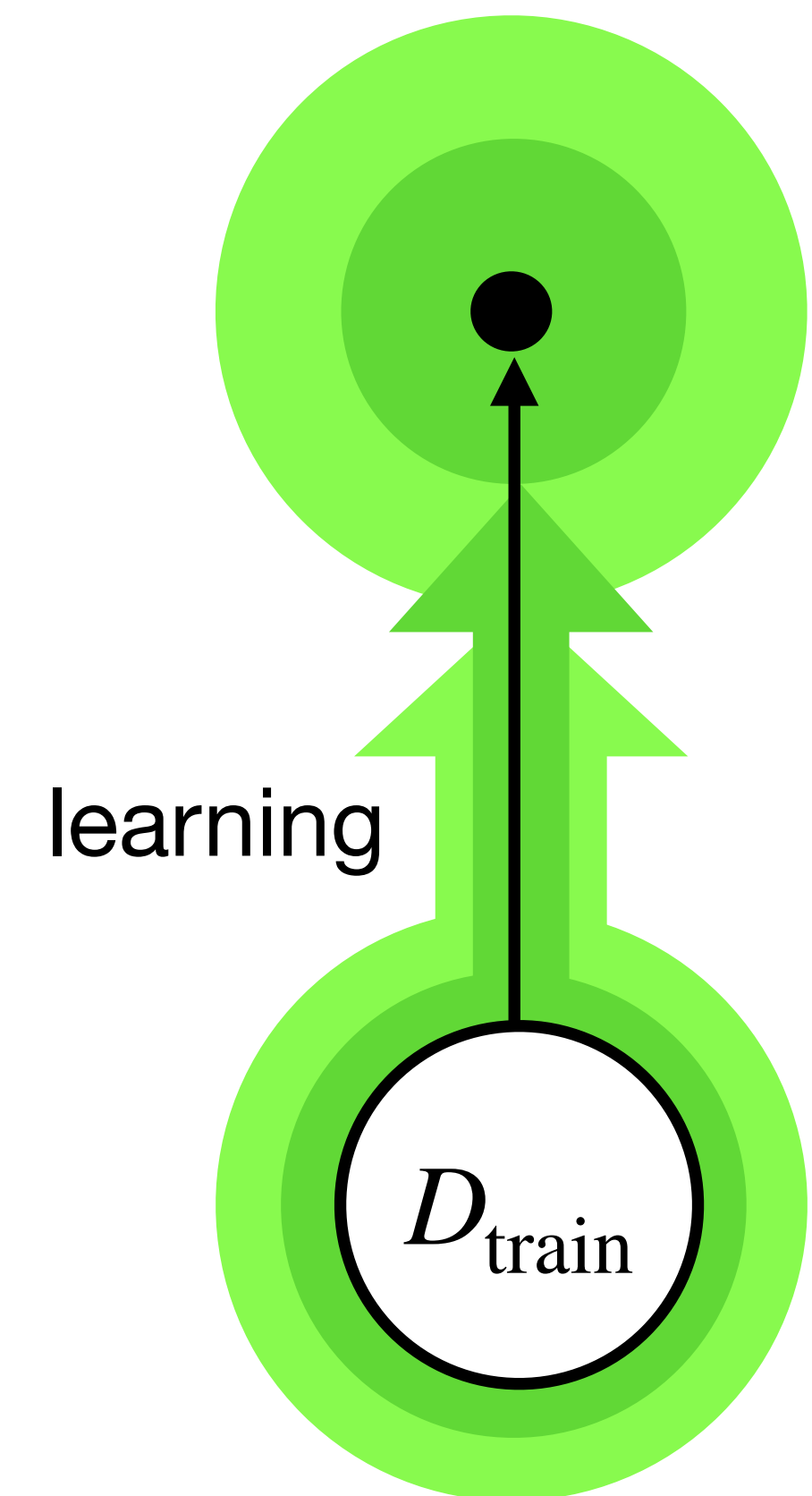




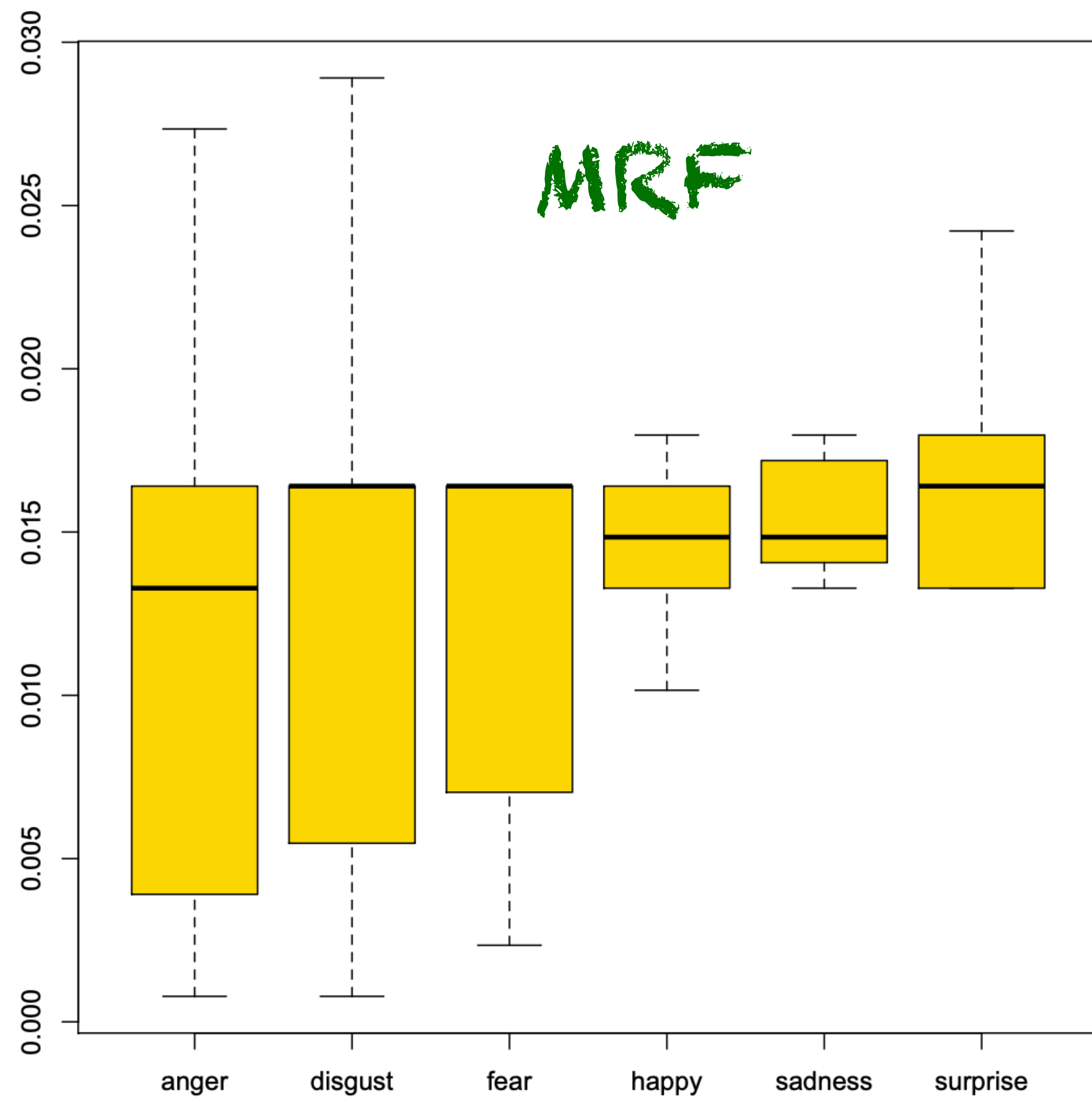
## DIRECT



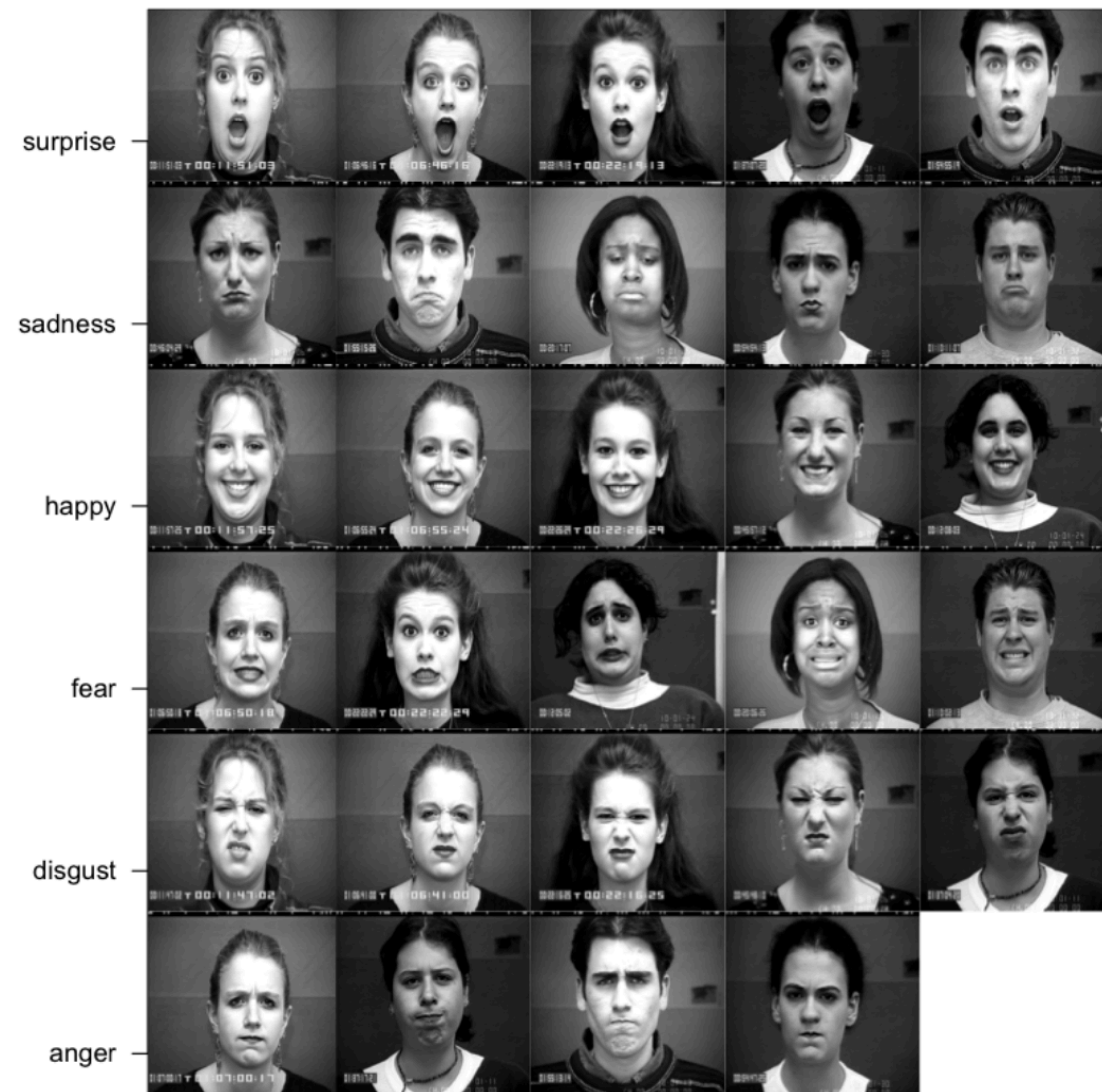
## INDIRECT








(a) Robustness split by emotions.



(b) Examples of emotions.



# MODEL SELECTION



International Journal of Approximate Reasoning 113 (2019) 245–255

Contents lists available at ScienceDirect

International Journal of Approximate Reasoning

[www.elsevier.com/locate/ijar](http://www.elsevier.com/locate/ijar)



# A hierarchy of sum-product networks using robustness

Diarmaid Conaty<sup>a,\*</sup>, Jesús Martínez del Rincon<sup>a</sup>, Cassio P. de Campos<sup>b</sup>

<sup>a</sup> Centre for Data Science and Scalable Computing, Queen's University Belfast, UK  
<sup>b</sup> Dept. of Information and Computing Sciences, Utrecht University, the Netherlands

<sup>b</sup> Dept. of Information and Computing Sciences, Utrecht University, the Netherlands

## ARTICLE INFO

**Article history:**

Received 29 March 2019

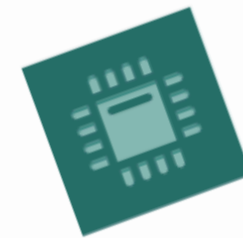
Received in revised form 26 June 2019  
Accepted 24 July 2019

Accepted 24 July 2019  
Available online 1 August 2019


Available online 2 August 2019

## ABSTRACT

Sum-product networks are a popular framework that has been shown to achieve state-of-the-art performance on product networks from scarce data, the obtained models are robust to small variations of parameters and where the characteristics of sum-product networks can be learned with respect to their parameters. Using a hierarchical approach to build a model if the model is unreliable decisions, we build a hierarchical approach testing time is deferred to another model if the model fails this approach on benchmark classification tasks and that the robustness measure can be a meaningful metric for classifiers and that our Hierarchical Sum-Product Network achieves higher accuracy.



## sensors

 **sensors**

Article

# A Robust Dynamic Classifier Selection Approach for Hyperspectral Images with Imprecise Label Information

1\* Shaoguang Huang<sup>1,\*</sup>, Jasper De Bock<sup>2</sup>, Gert de Cooman<sup>2</sup>

<sup>1</sup> Department of Data Science and Information Systems, Ghent University, 9002 Ghent, Belgium; shaoguang.huang@ugent.be (S.H.)

<sup>2</sup> Department of Communications and Information Processing, Ghent University, 9002 Ghent, Belgium; jasper.debock@ugent.be (J.D.B.) and gert.decooman@ugent.be (G.d.C.)

**Robust Dynamic Classification for Hyperspectral Images With Limited Label Information**

Meizhu Li<sup>1,\*</sup>, Shaoguang Huang<sup>1,\*</sup>, Jasper De Bock<sup>2</sup>, Gert de Cooman<sup>2</sup>

<sup>1</sup>Aleksandra Pižurica<sup>1</sup>

<sup>1</sup>Department of Telecommunications and Information Processing, Ghent University,  
aleksandra.pizurica@ugent.be (A.P.)

<sup>2</sup>Department of Electronics and Information Systems, Ghent University, 9052 Gent, Belgium;  
jasper.debock@ugent.be (J.D.B.), gert.decooman@ugent.be (G.d.C.)

<sup>3</sup>Department of Mathematics, Ghent University, 9000 Ghent, Belgium;  
shaoguang.huang@ugent.be (S.H.)

15 September 2020

accurate label information for training



accurate label information.  
training samples  
amount





**FUTURE WORK MEETINGS**





CALIBRATION

**FUTURE WORK MEETINGS**





REGRESSION

**FUTURE WORK MEETINGS**



A scene from the television series Star Trek: The Next Generation. Three characters are seated in a futuristic, dimly lit room. On the left, a Klingon warrior in traditional armor sits with a serious expression. In the center, a man in a dark, high-collared uniform sits with his hands clasped. On the right, a woman with long dark hair, wearing a light-colored uniform, sits looking towards the center. A large white speech bubble with a black outline is positioned in the upper right, containing the text 'CONFORMAL PREDICTION'.

CONFORMAL  
PREDICTION

**FUTURE WORK MEETINGS**





[jasper.debock@ugent.be](mailto:jasper.debock@ugent.be)

- [1] Global Sensitivity Analysis for MAP Inference in Graphical Models. De Bock, de Campos & Antonucci. 2014.
- [2] Credal sum-product networks.  
Mauá, Cozman, Conaty & de Campos. 2017.
- [3] Robustifying sum-product networks.  
Mauá, Conaty, Cozman, Poppenhaeger & de Campos. 2018.
- [4] Towards Scalable and Robust Sum-Product Networks.  
Correia & de Campos. 2019.
- [5] Towards Robust Classification with Deep Generative Forests.  
Correia, Peharz & de Campos. 2020



- [6] Robustness quantification: a new method for assessing the reliability of the predictions of a classifier.  
De Tavernier, De Bock. 2025.
- [7] Robustness and uncertainty: two complementary aspects of the reliability of the predictions of a classifier.  
De Tavernier, De Bock. 2025.
- [8] A hierarchy of sum-product networks using robustness.  
Conaty, Martínez del Rincon & de Campos. 2019.
- [9] A Robust Dynamic Classifier Selection Approach for Hyperspectral Images with Imprecise Label Information.  
Li, Huang, De Bock & Pižurica. 2020.