

Jasper De Bock, Adrián Detavernier, Rodrigo Lassance

Robustness Quantification

using imprecise probabilities to assess the reliability of probabilistic classifiers



**GHENT
UNIVERSITY**

WUML 2026

February 3



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



MACHINE
LEARNING

... is unreliable



media saying AI will
take over the world



my neural network:

Dog

CLASSIFICATION

features x

FEATURES

photo

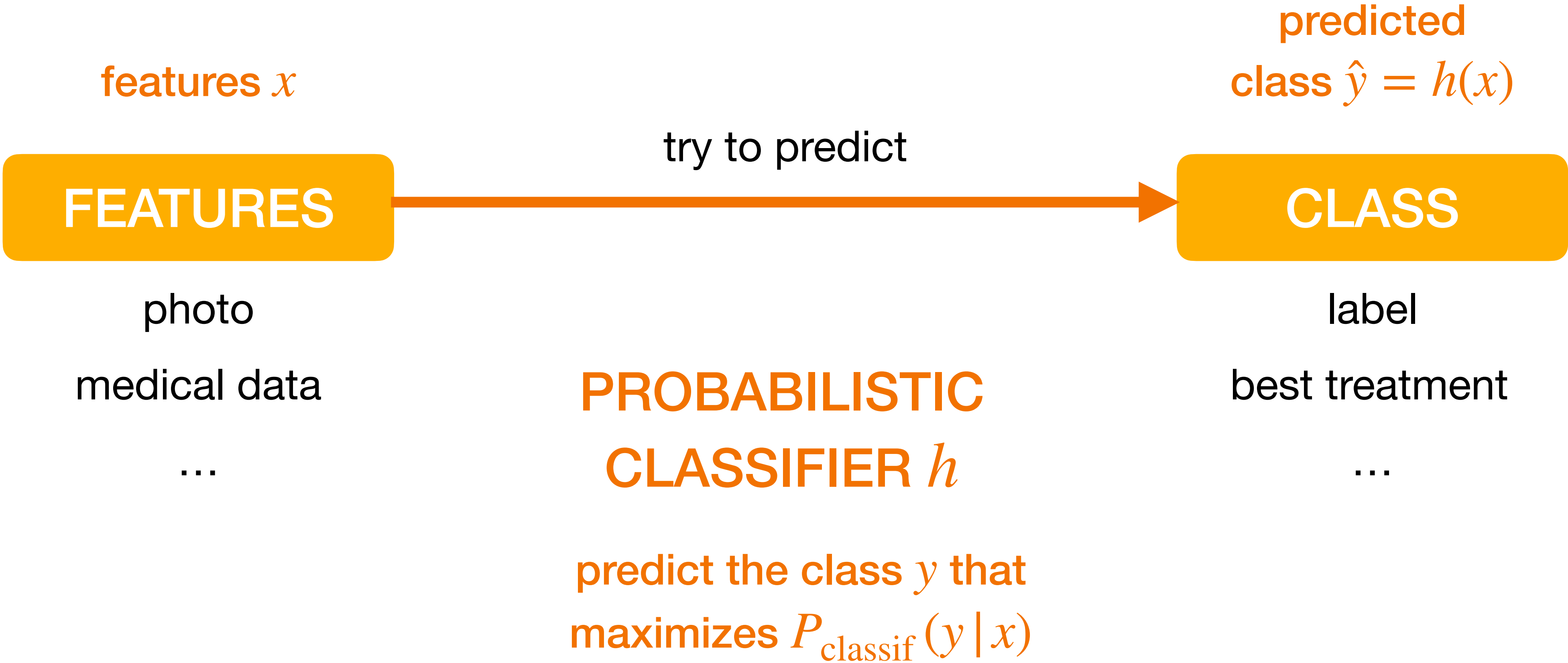
medical data

...

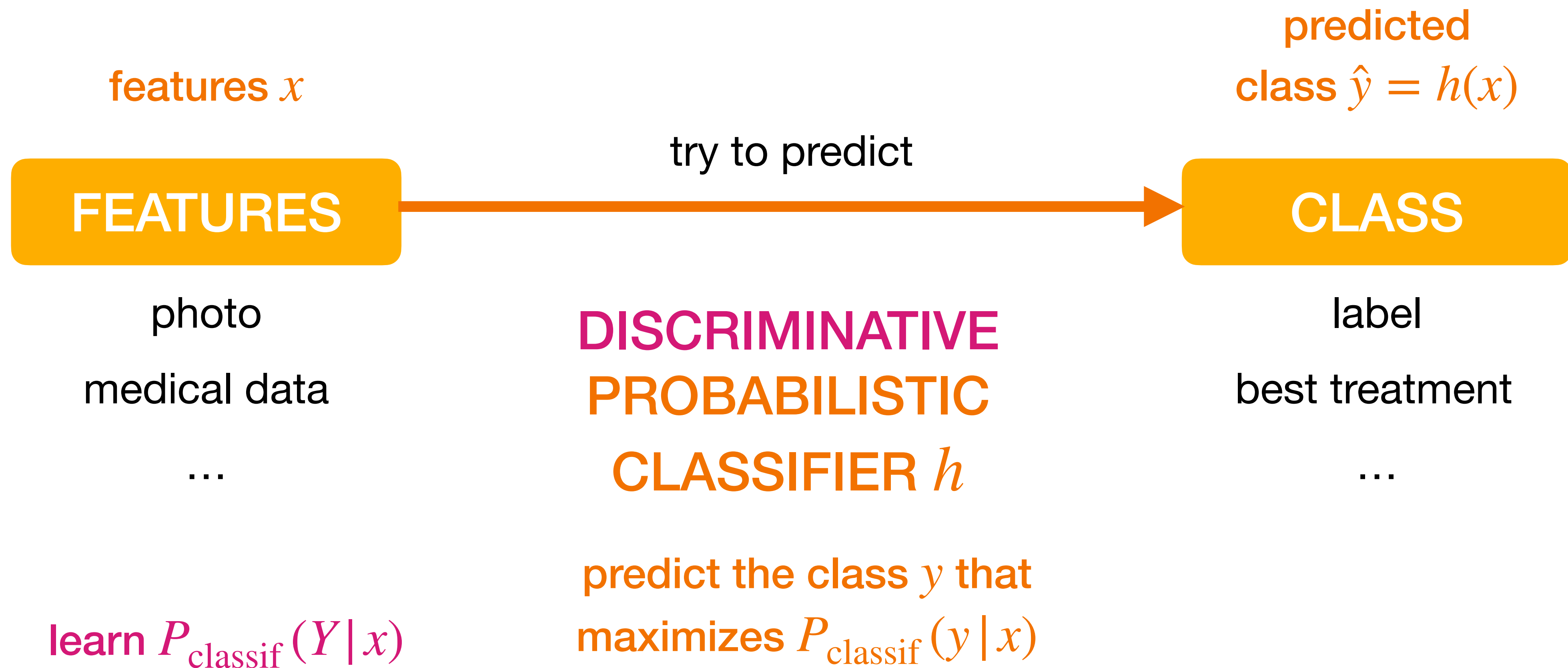
CLASSIFICATION



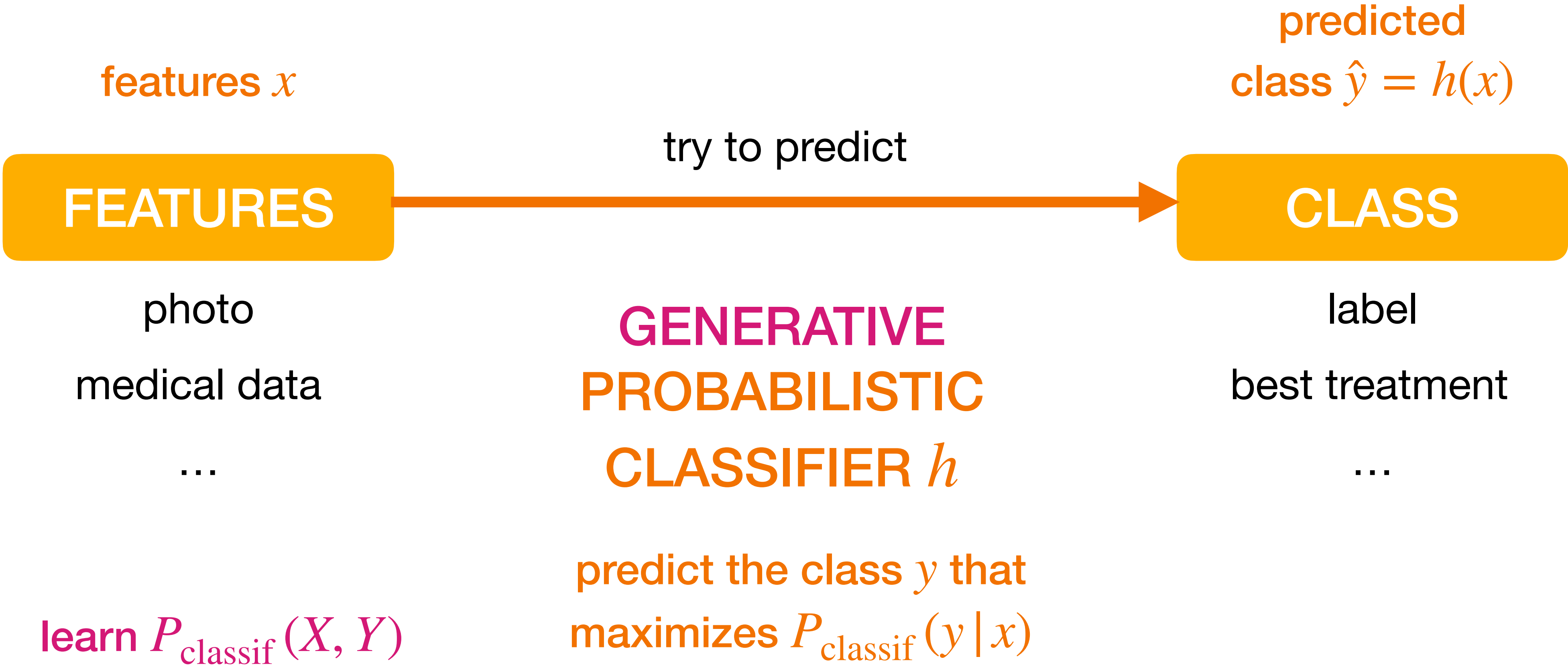
CLASSIFICATION



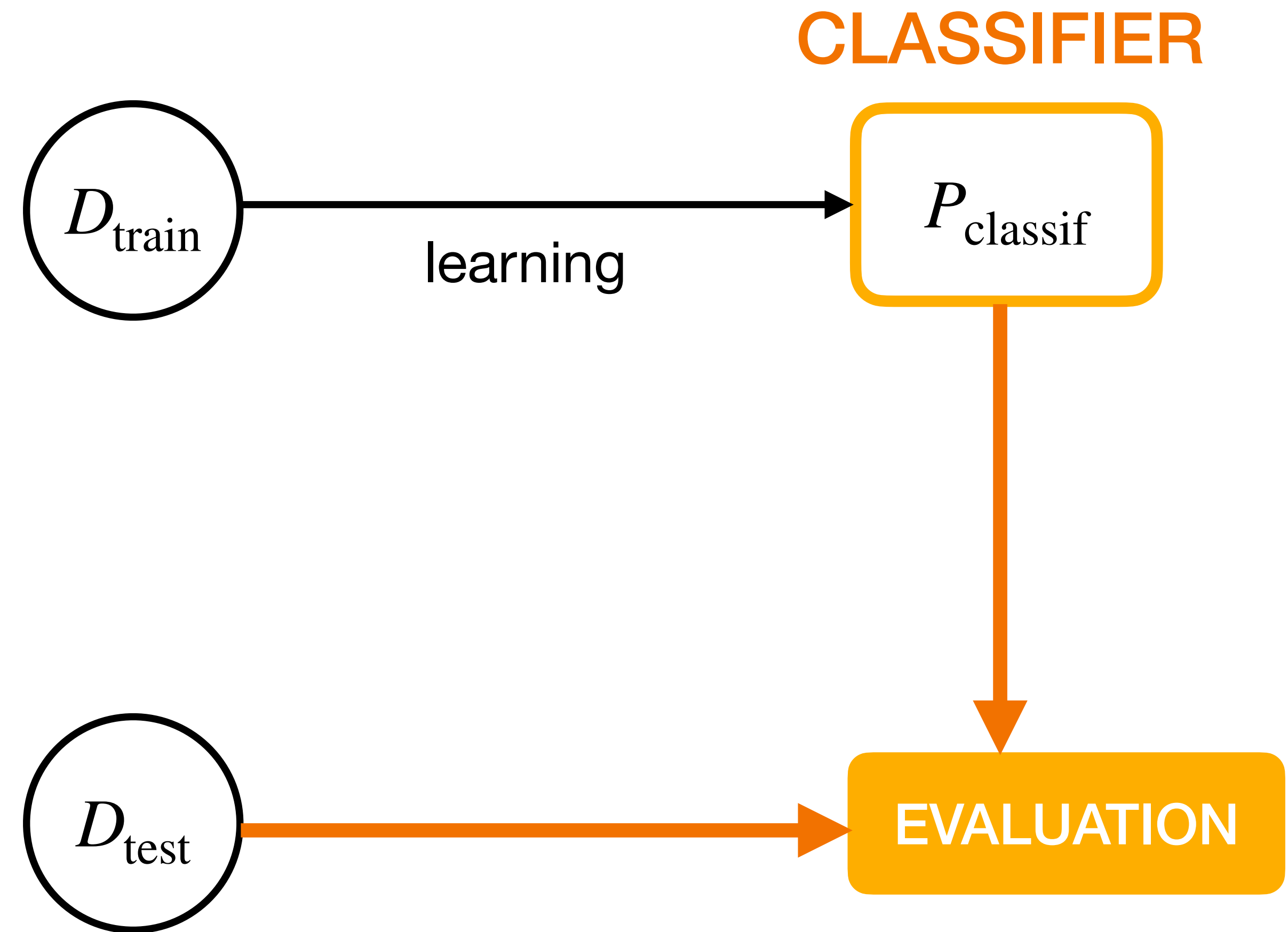
CLASSIFICATION



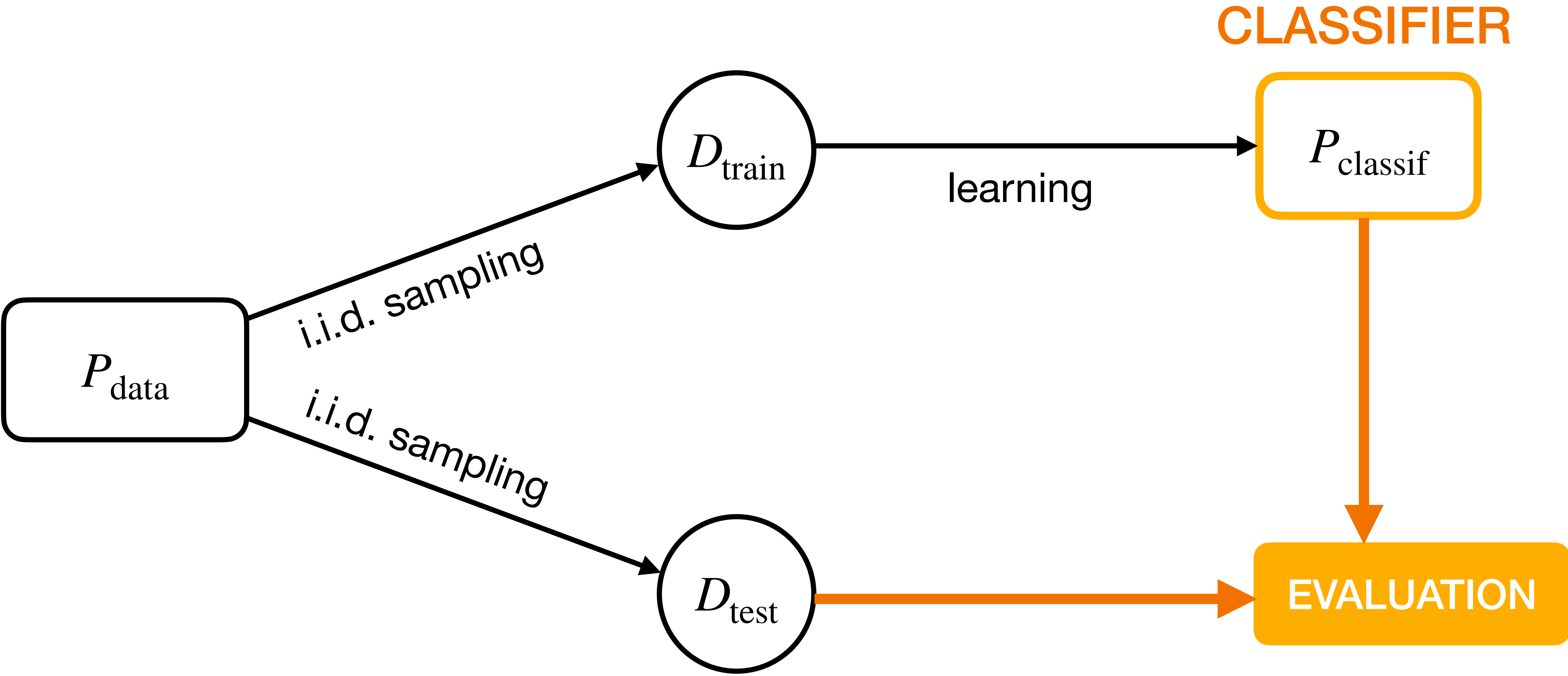
CLASSIFICATION



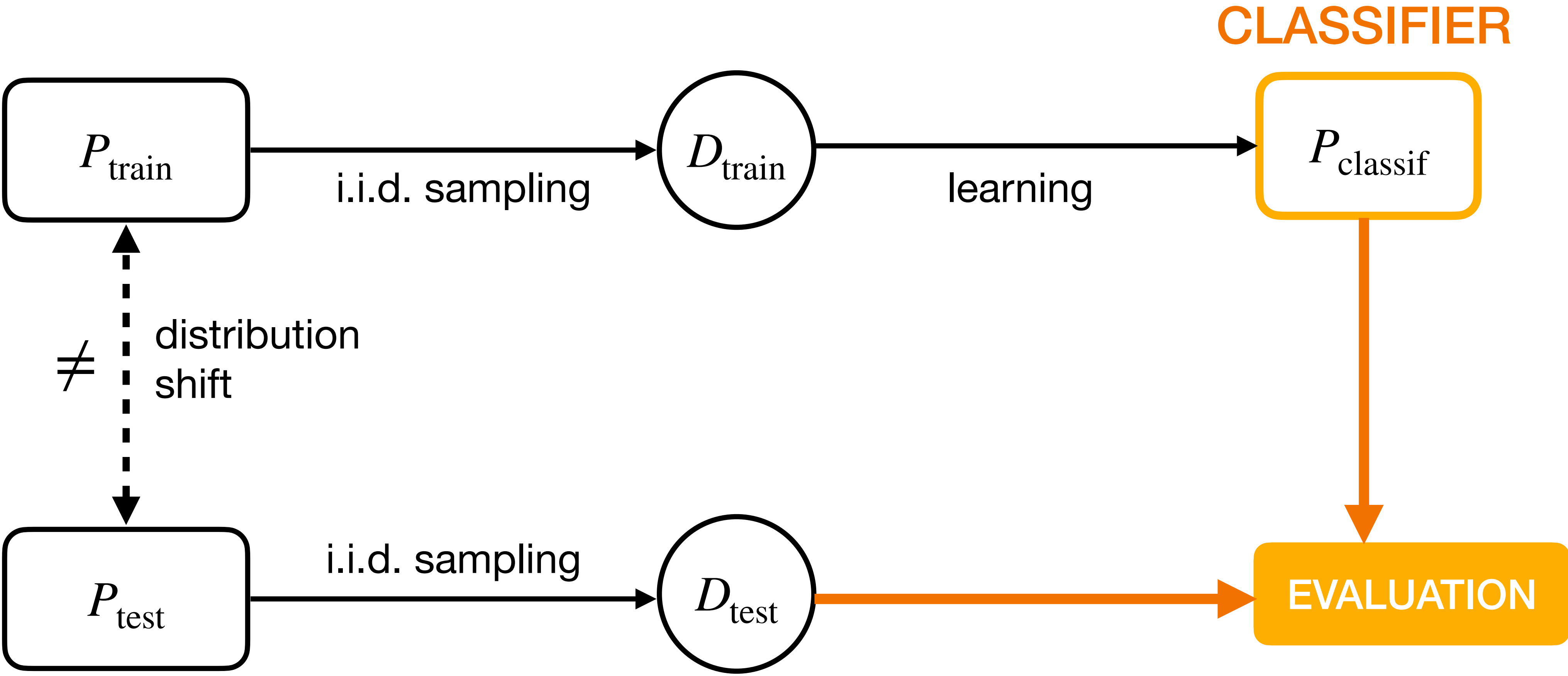
CLASSIFICATION



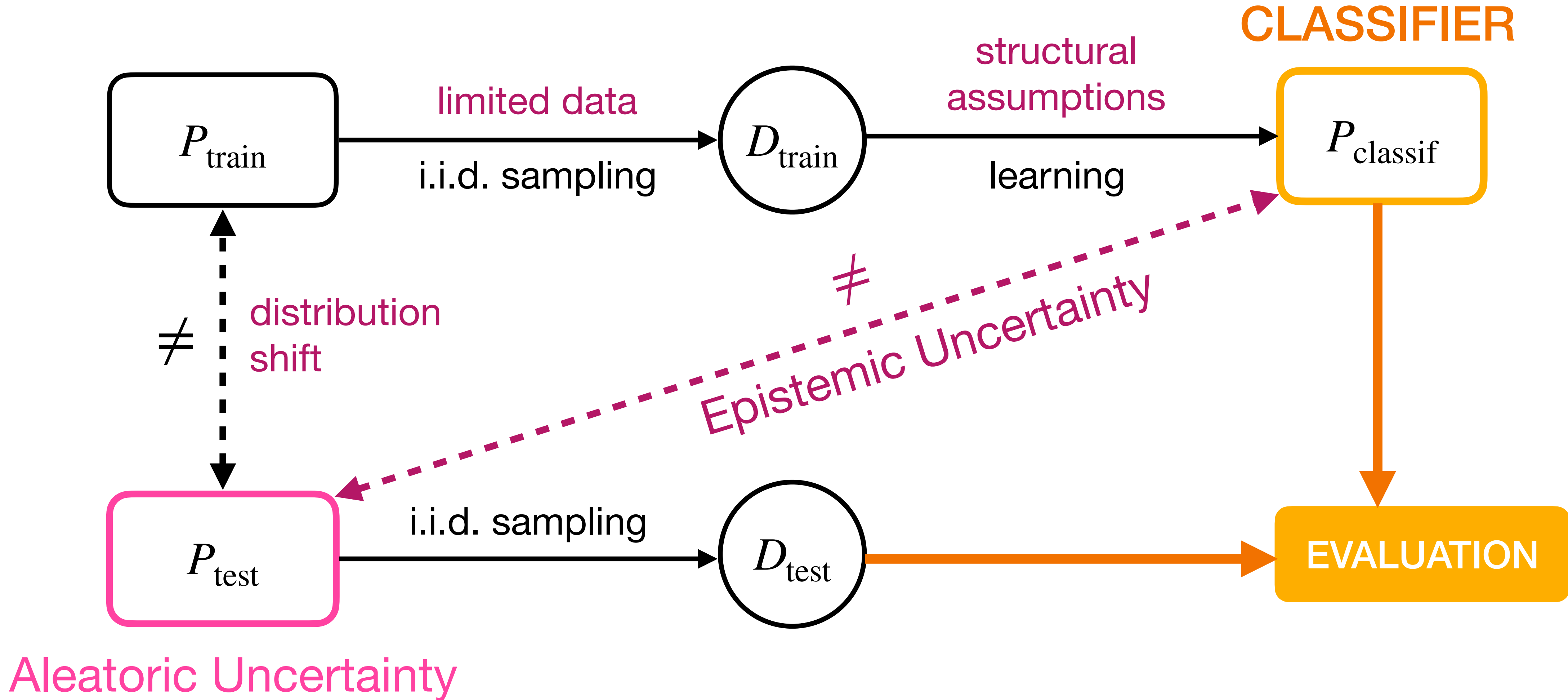
CLASSIFICATION



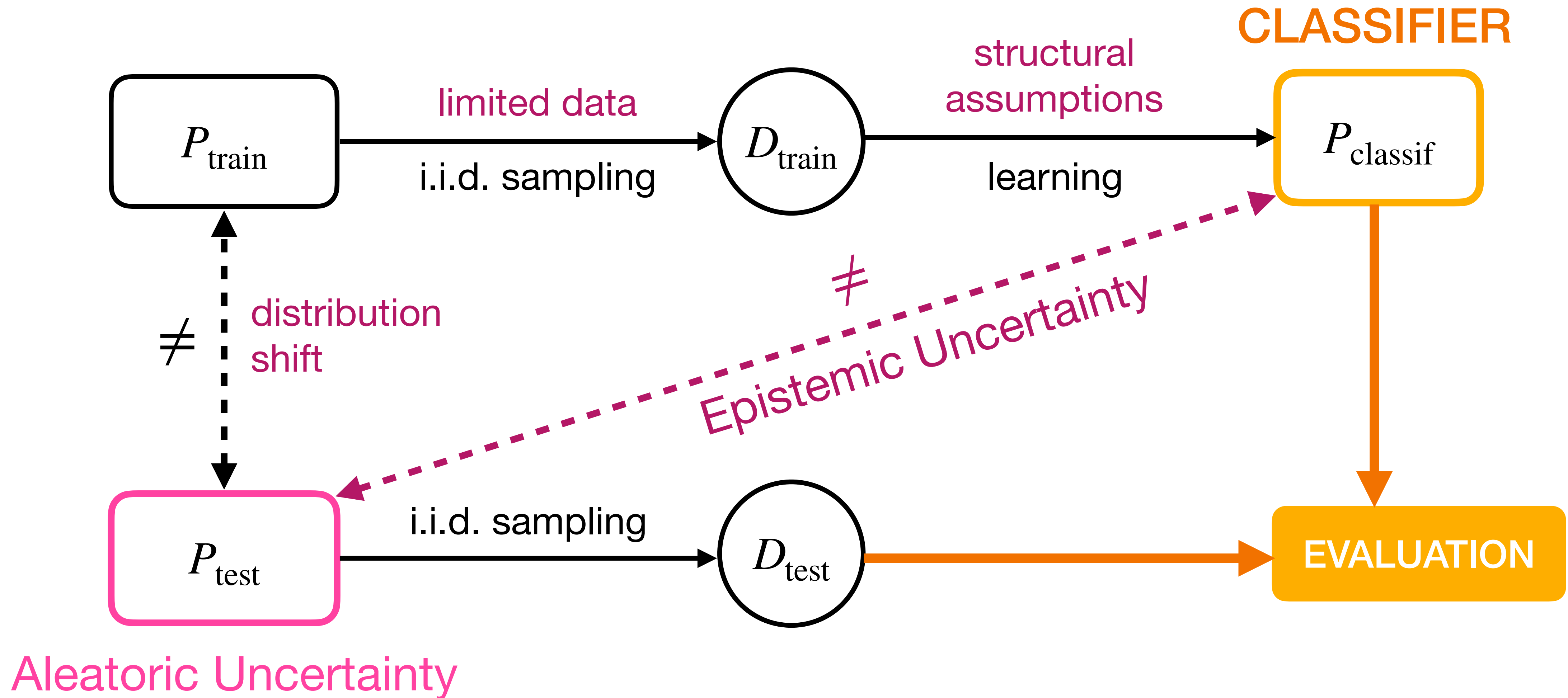
CLASSIFICATION



CLASSIFICATION ... is unreliable



UNCERTAINTY QUANTIFICATION





MACHINE
LEARNING

IMPRECISE
PROBABILITIES

ROBUSTNESS
QUANTIFICATION

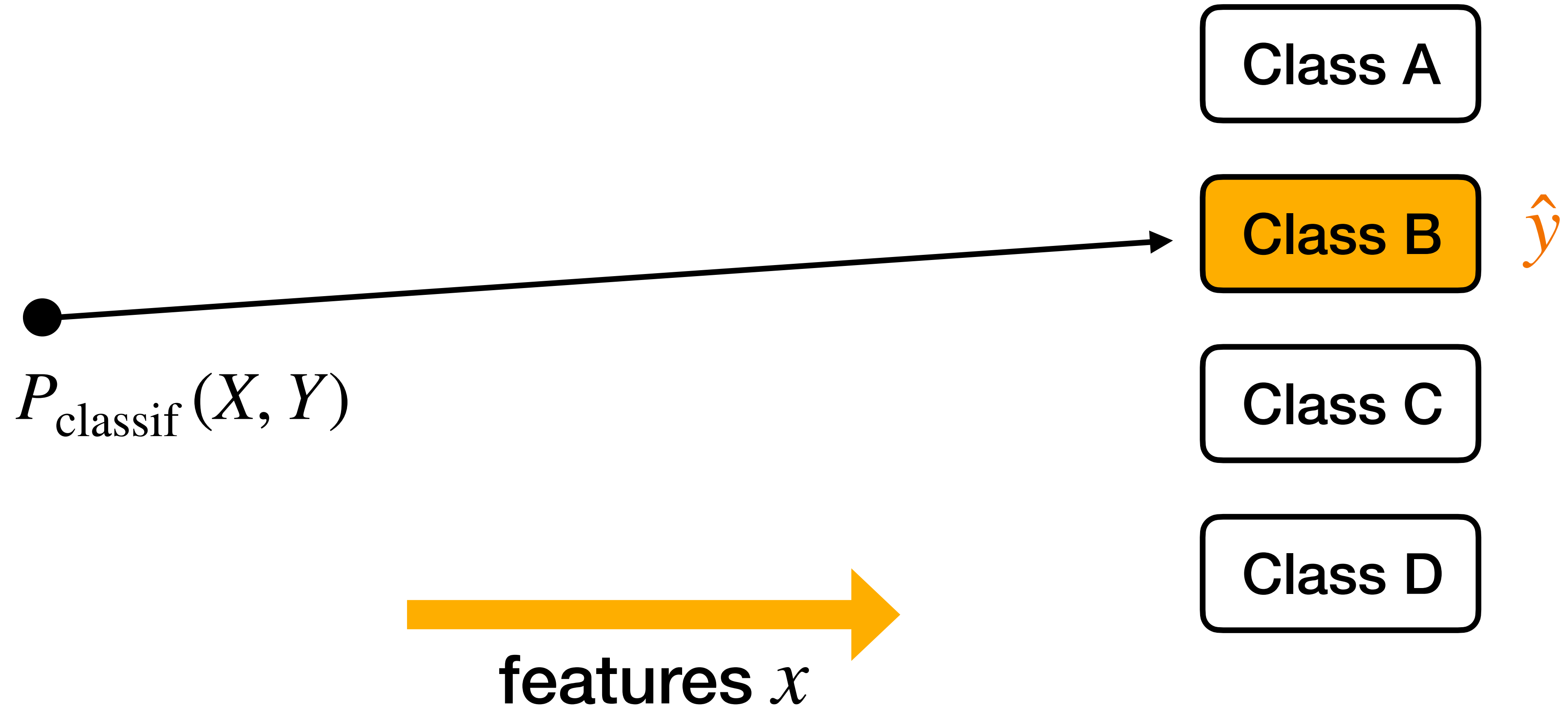


IMPRECISE
PROBABILITIES

enable us to study
robustness

PROBABILISTIC CLASSIFIER

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



PROBABILISTIC CLASSIFIER

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

**ROBUST
prediction**

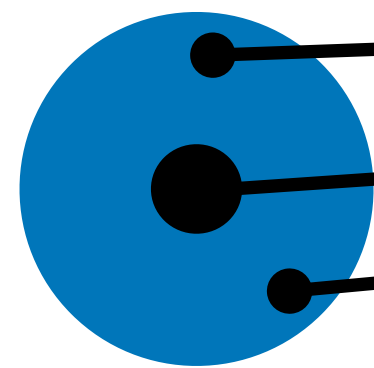
Class A

Class B

Class C

Class D

\hat{y}



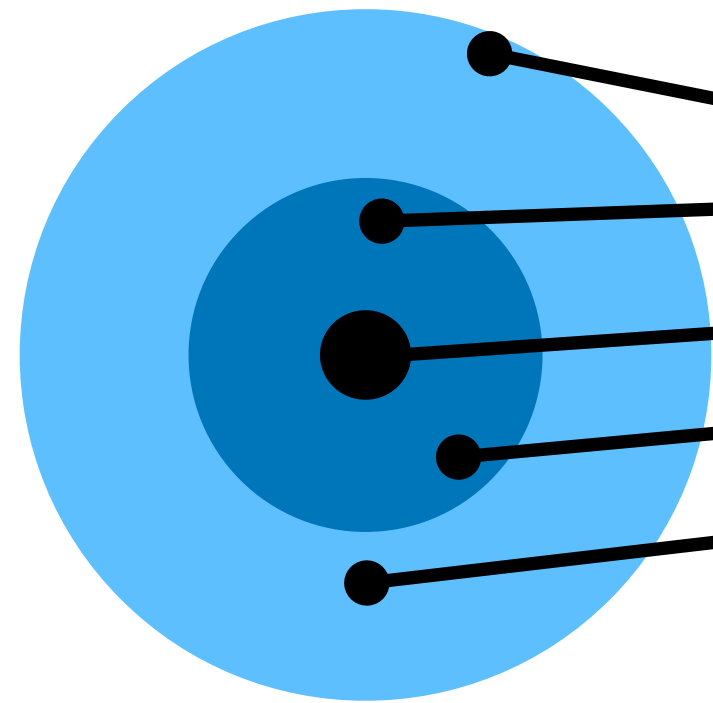
set of distributions
 \mathcal{P} that contains
 $P_{\text{classif}}(X, Y)$

features x

PROBABILISTIC CLASSIFIER

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

~~ROBUST
prediction~~



Class A

Class B

Class C

Class D

\hat{y}

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

features x

ROBUST prediction

PROBABILISTIC CLASSIFIER

~~**ROBUST prediction**~~

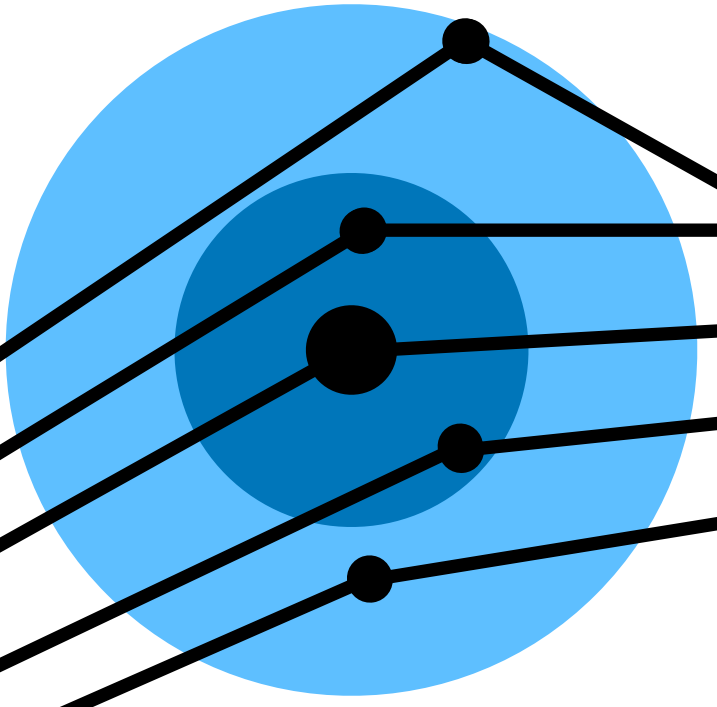
predict the class y that maximizes $P_{\text{classif}}(y | x)$

Class A

Class B

Class C

\hat{y}_2 Class D



Class A

Class B \hat{y}_1

Class C

Class D

← features x_2

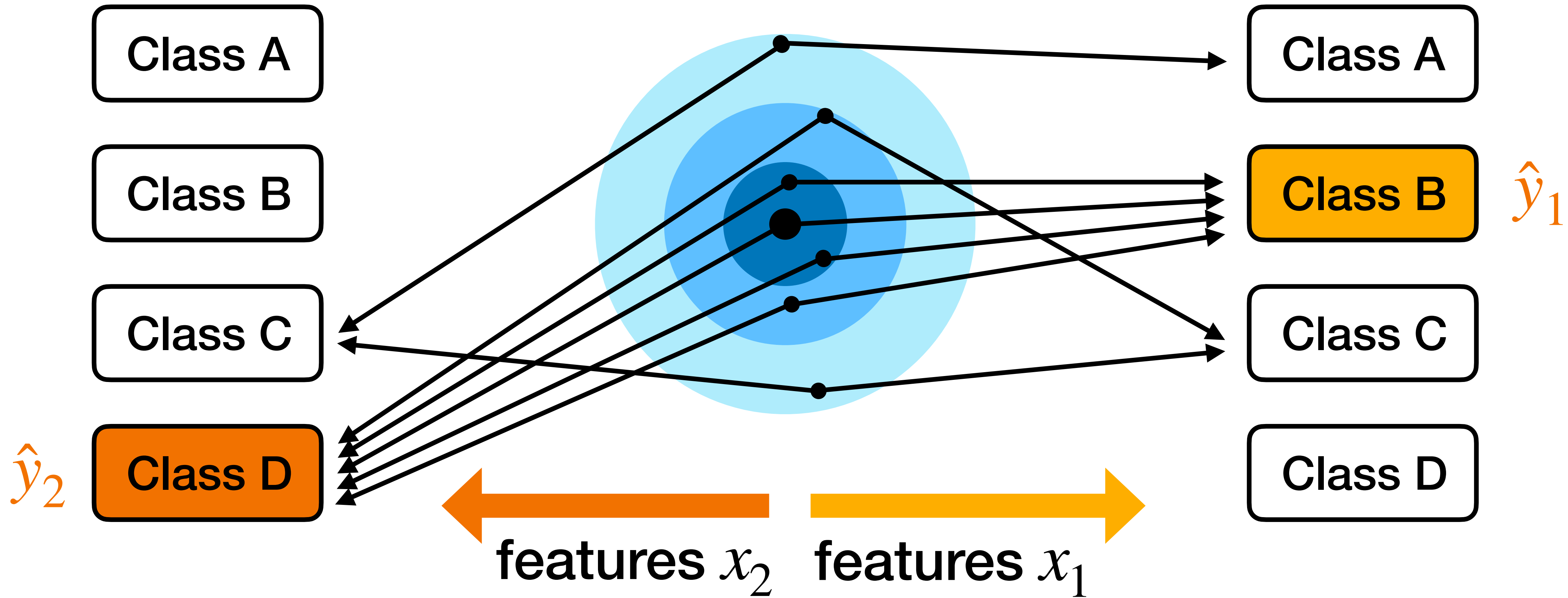
→ features x_1

PROBABILISTIC CLASSIFIER

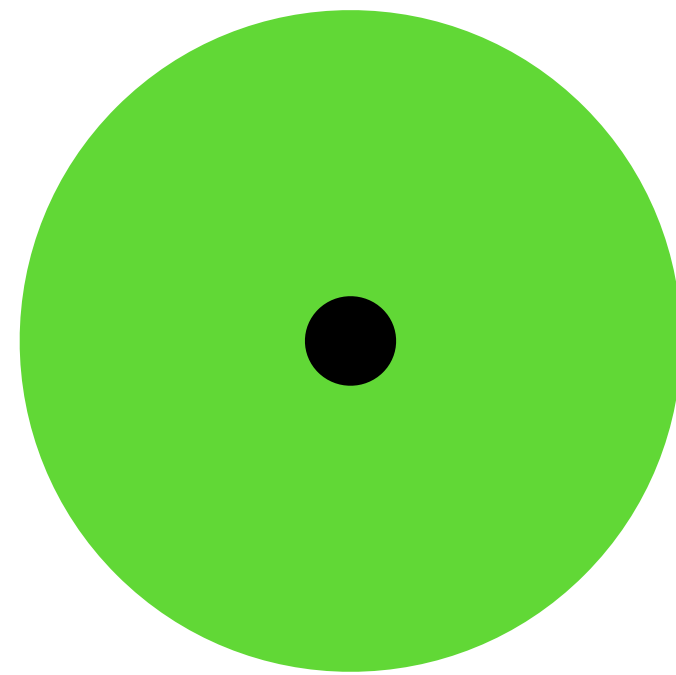
predict the class y that maximizes $P_{\text{classif}}(y | x)$

~~ROBUST prediction~~

~~ROBUST prediction~~



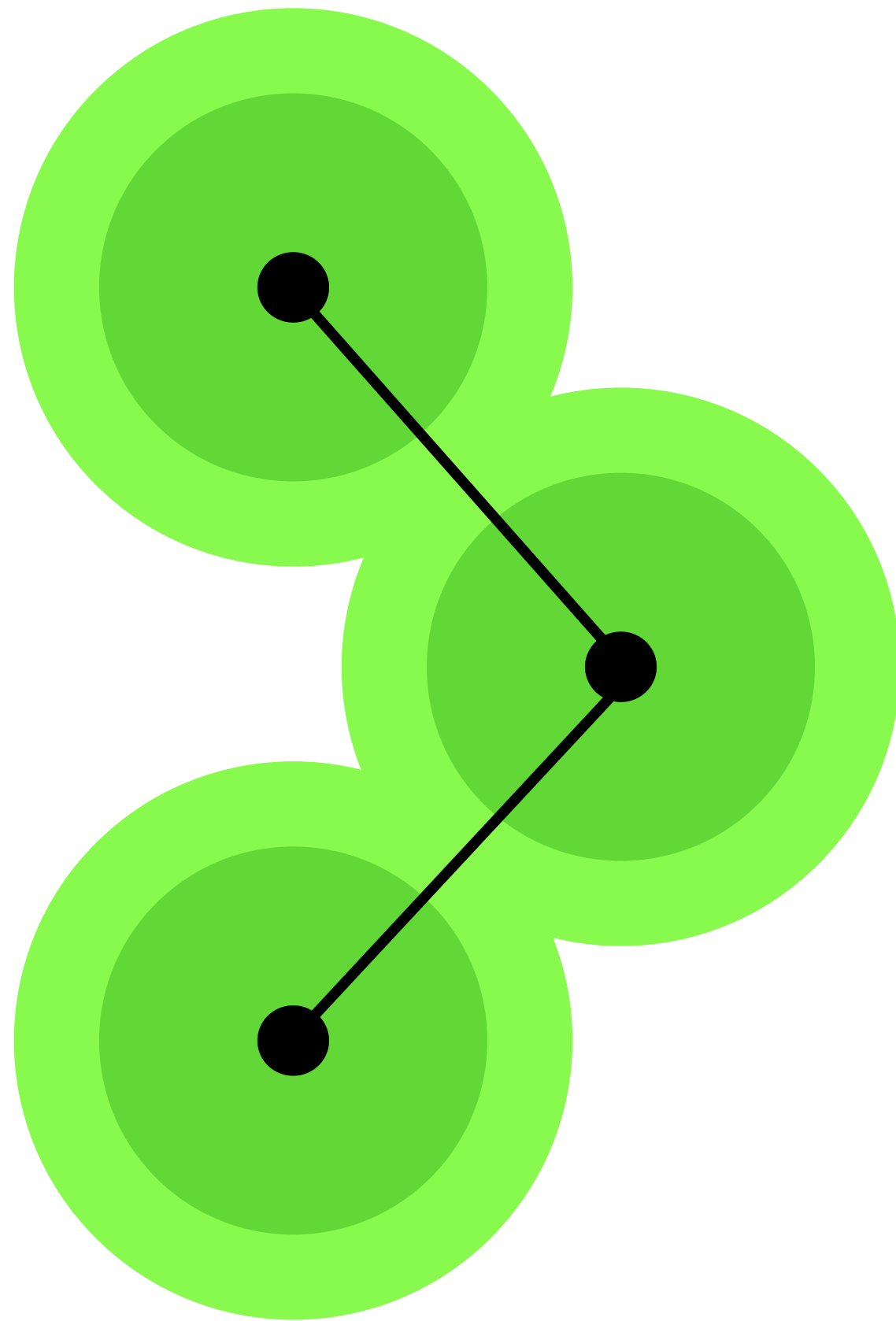
ROBUSTNESS QUANTIFICATION



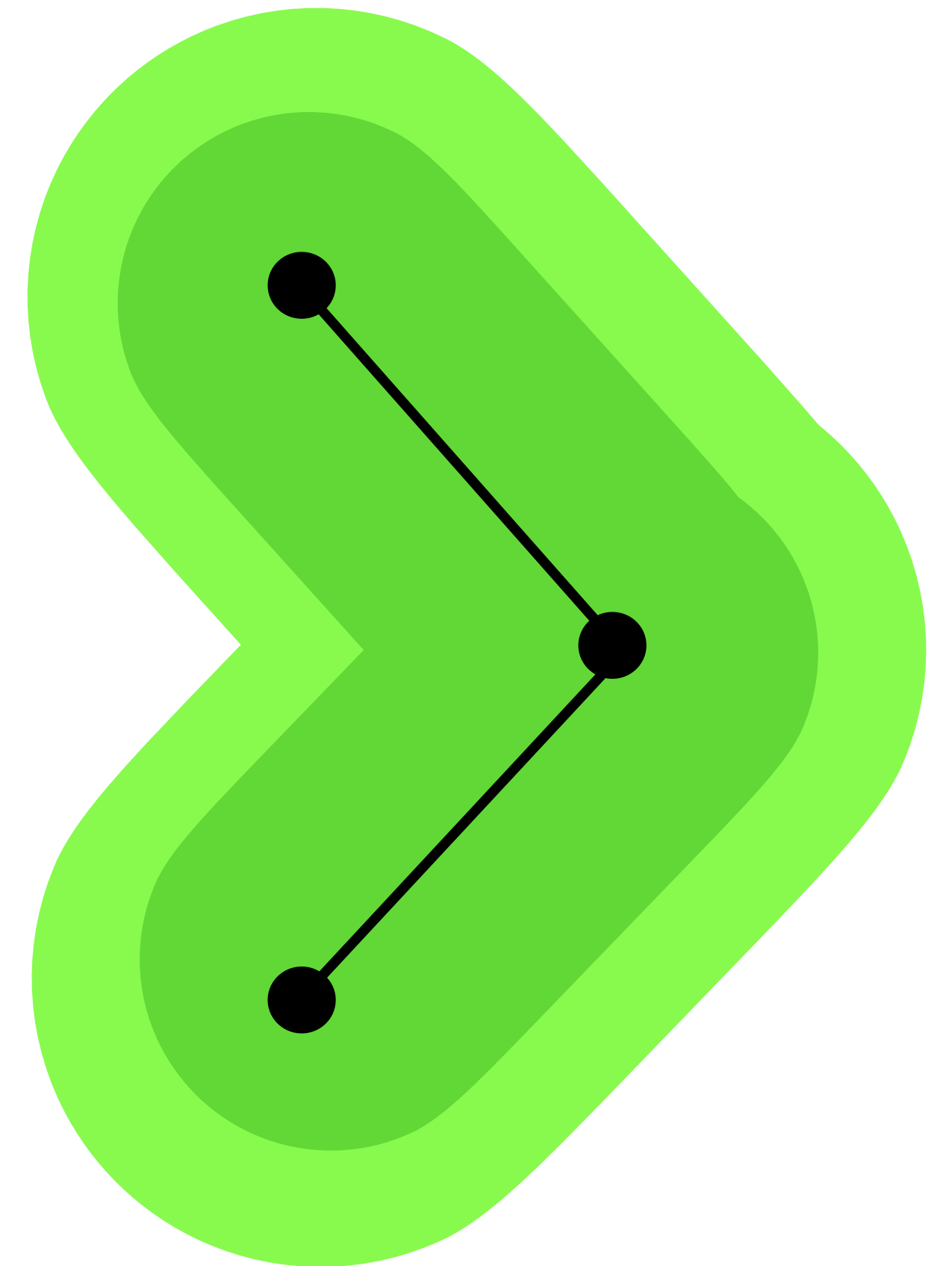
set of distributions
 \mathcal{P} that contains
 $P_{\text{classif}}(X, Y)$

ROBUSTNESS:
“size” of largest \mathcal{P} for
which that particular
prediction is robust

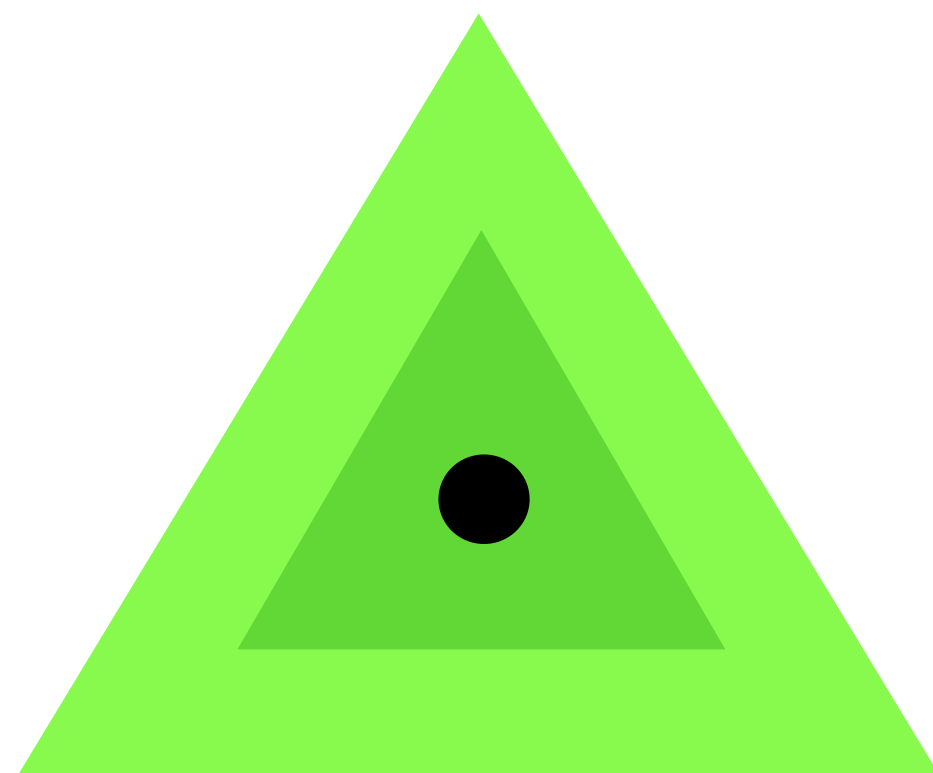
LOCAL



GLOBAL



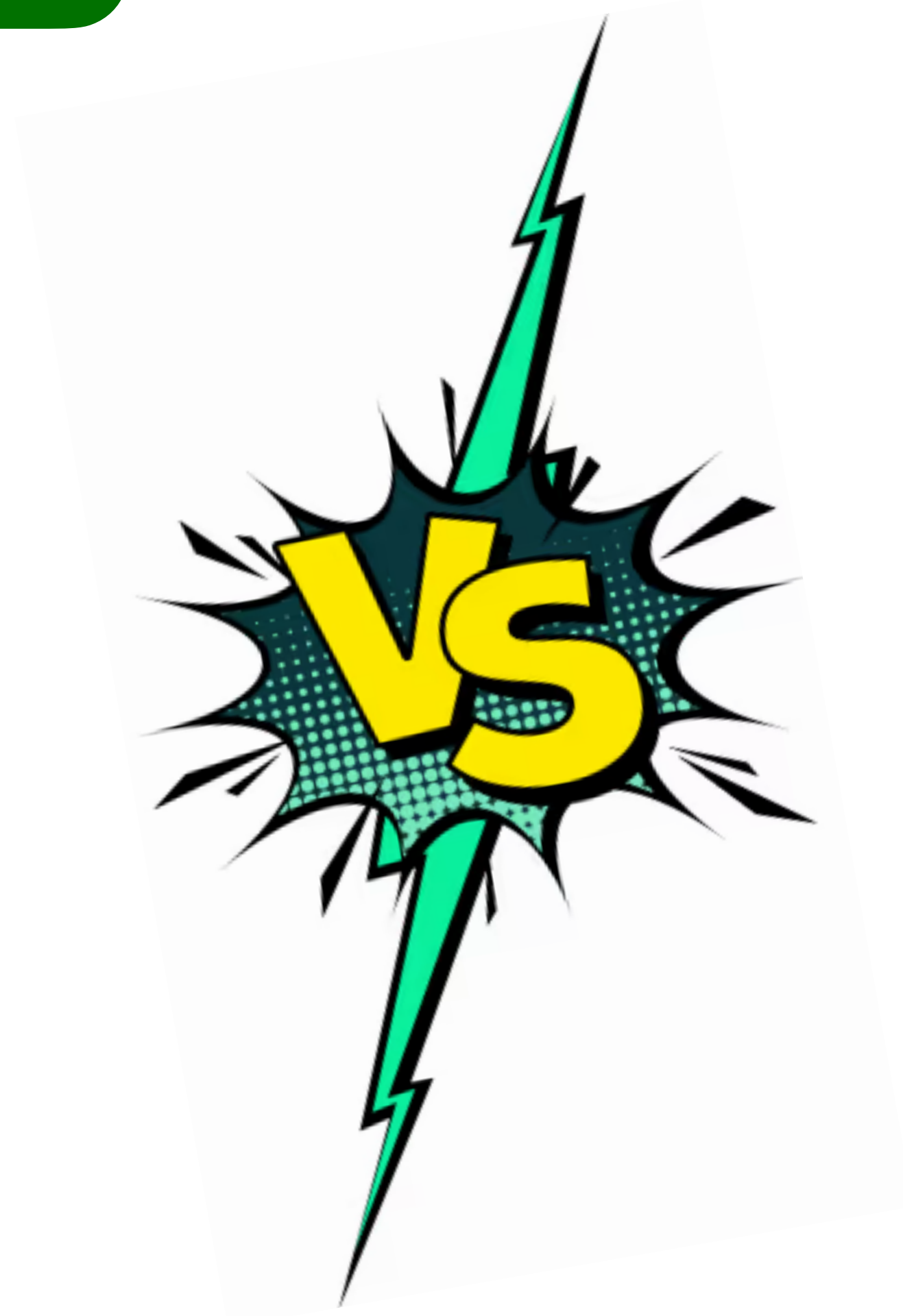
ϵ -CONTAMINATION



\mathcal{P}_ϵ

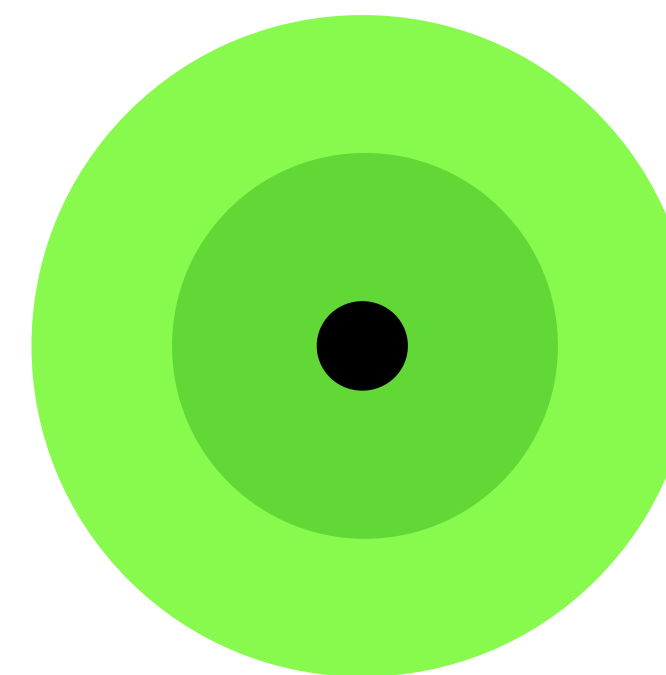
\parallel

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



OTHER STUFF

distance-based, ...

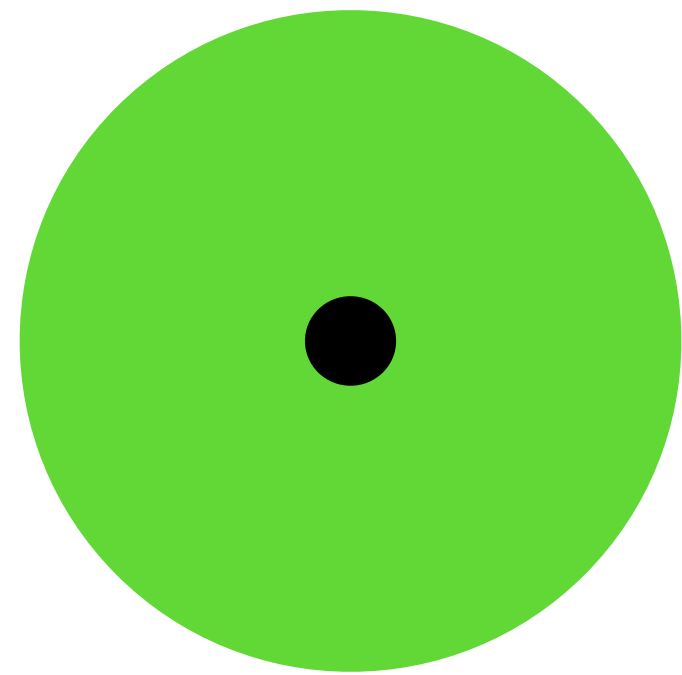


\mathcal{P}_δ

\parallel

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

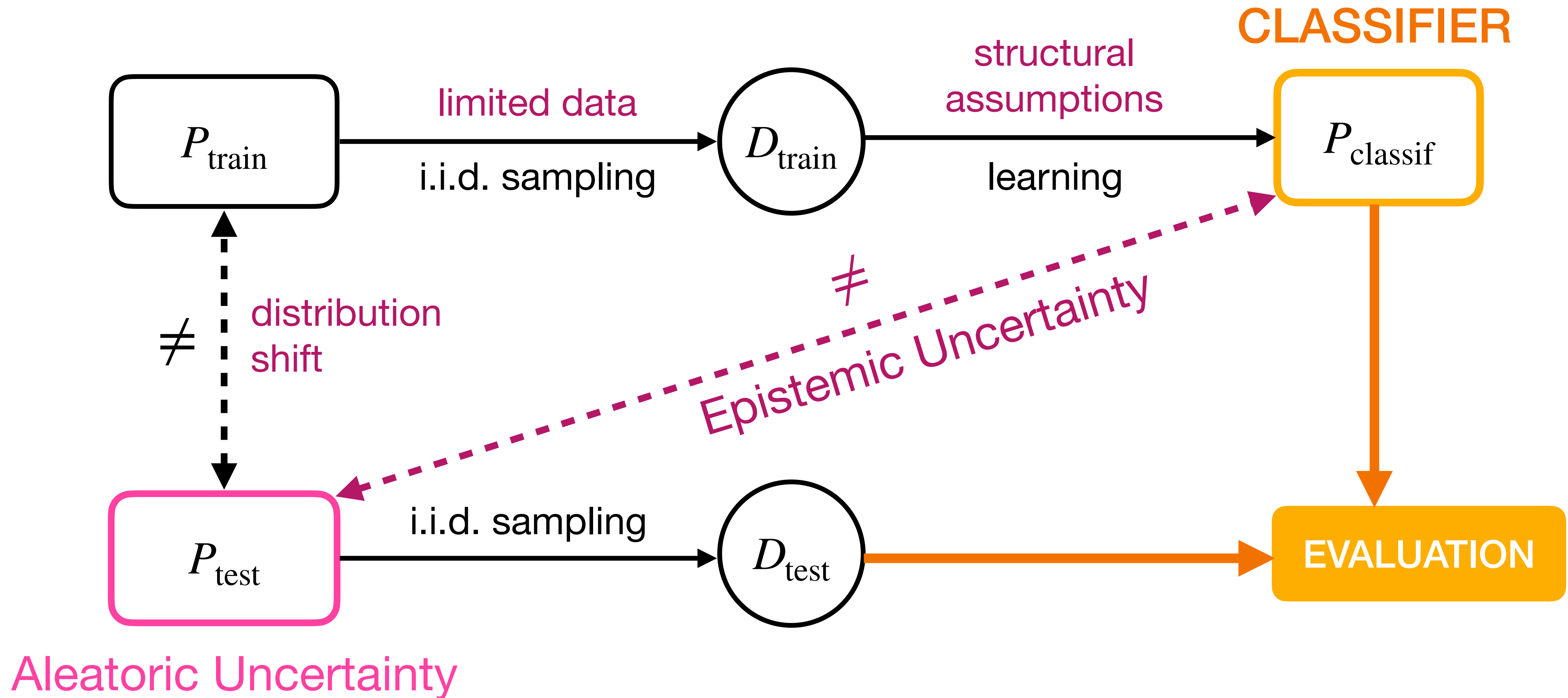
ROBUSTNESS QUANTIFICATION



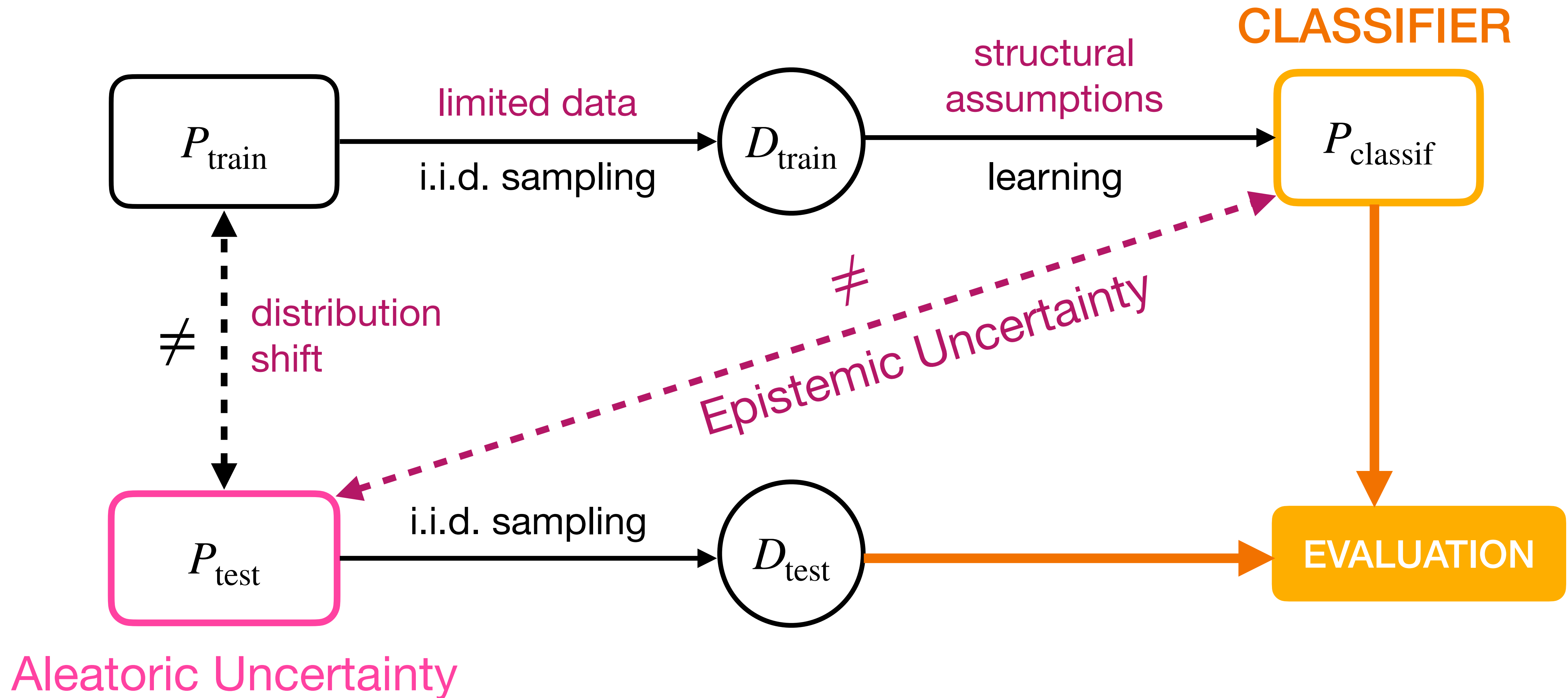
set of distributions
 \mathcal{P} that contains
 $P_{\text{classif}}(X, Y)$

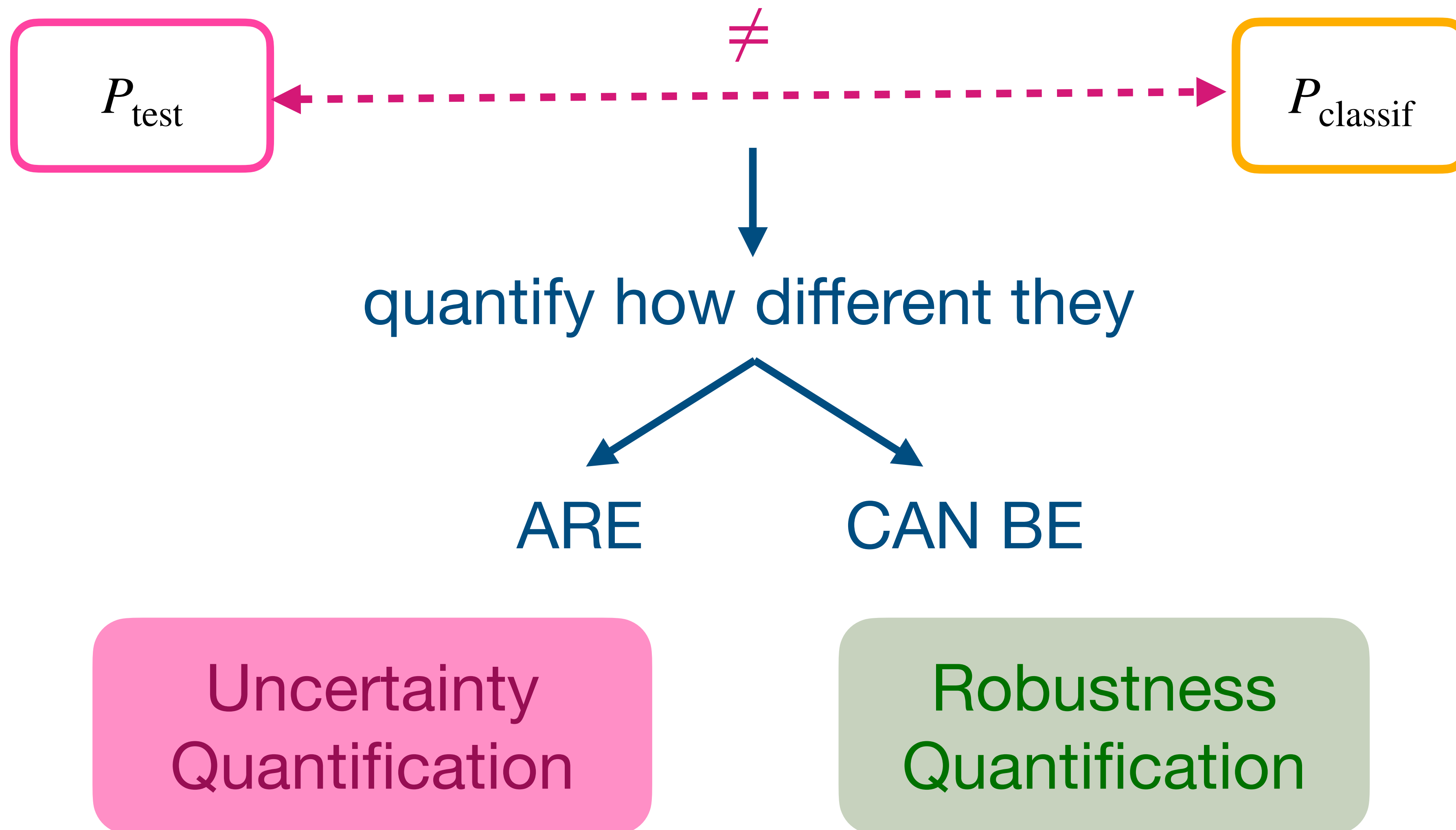
ROBUSTNESS:
“size” of largest \mathcal{P} for
which that particular
prediction is robust

UNCERTAINTY QUANTIFICATION



ROBUSTNESS QUANTIFICATION







Adrián
Detavernier



Rodrigo
Lassance



MACHINE
LEARNING

IMPRECISE
PROBABILITIES

ROBUSTNESS
QUANTIFICATION



Adrián
Detavernier

MACHINE
LEARNING

IMPRECISE
PROBABILITIES

ROBUSTNESS
QUANTIFICATION



2014

MRF
BN



Cassio
de Campos



Alessandro
Antonucci

Global Sensitivity Analysis for MAP Inference in Graphical Models

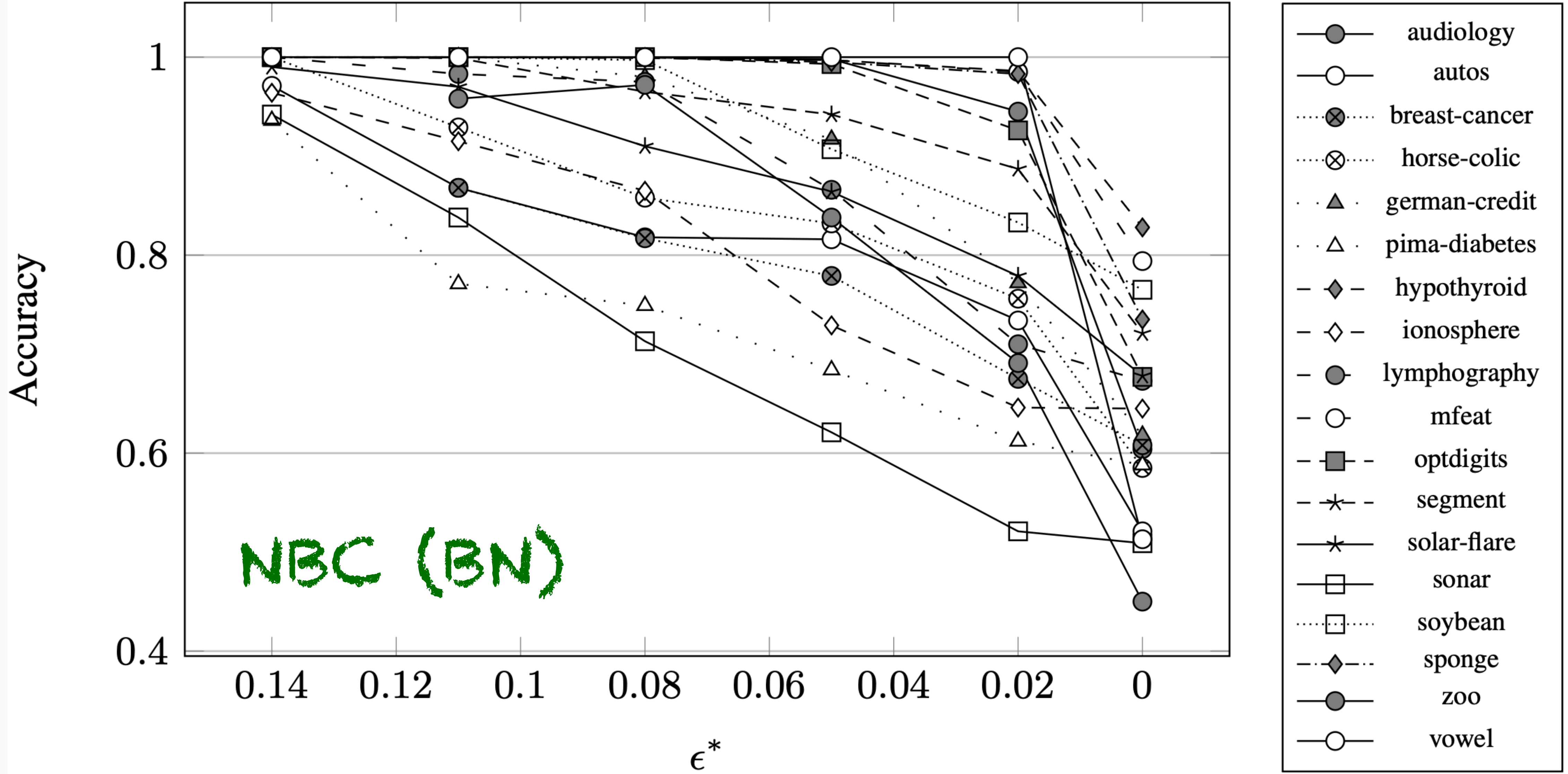
Jasper De Bock
Ghent University, SYSTeMS
Ghent (Belgium)
jasper.debock@ugent.be

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. Its complexity is essentially the same as that of obtaining the MAP configuration. It is used with minimal effort. We use our algorithm to measure the sensitivity of a MAP configuration to perturbations that do not induce a change in the MAP configuration.



[1]

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 from data. Hence, their results are prone to be unreliable and imprecise. In this paper, we propose a novel extension of credal sum-product networks, an imprecise extension of sum-product networks, that allows for common inference algorithms and complexity results for common inference tasks. We show that this extension allows for a perturbation of the parameters of learned sum-product networks, which can be used to assess the reliability of classification results. Our experiments show that this approach is able 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 they can provide quantitative (probabilistic) conclusions about uncertain knowledge. Such as Bayesian networks and Markov networks, which are graphical models that represent dependencies as graph connectivity. In this paper, we propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference algorithms and complexity results for common inference tasks. We show that this extension allows for a perturbation of the parameters of learned sum-product networks, which can be used to assess the reliability of classification results. Our experiments show that this approach is able to distinguish between reliable and unreliable classifications with high accuracy. **Keywords:** Sum-product networks; tractable probabilistic models; credal classification; sensitivity analysis; robust statistics

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

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 dependencies 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, it can be approximated by popular approximate inference algorithms based on passing messages along the edges of the graph topology [32,64,62]. In this paper, we propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference algorithms and complexity results for common inference tasks. We show that this extension allows for a perturbation of the parameters of learned sum-product networks, which can be used to assess the reliability of classification results. Our experiments show that this approach is able to distinguish between reliable and unreliable classifications with high accuracy. **Keywords:** Sum-product networks; tractable probabilistic models; credal classification; sensitivity analysis; robust statistics

Robustifying sum-product networks

Denis Deratani Mauá^{a,*}, Diarmaid Conaty^b, Fabio Gagliardi
Katja Poppenhaeger^d, Cassio Polpo de Campos^{b,e}

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

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 from data. Hence, their results are prone to be unreliable and imprecise. In this paper, we propose a novel extension of credal sum-product networks, an imprecise extension of sum-product networks, that allows for common inference algorithms and complexity results for common inference tasks. We show that this extension allows for a perturbation of the parameters of learned sum-product networks, which can be used to assess the reliability of classification results. Our experiments show that this approach is able 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

Sum-Product Networks (SPNs) [15] (conceptually similar to Circuits [4]) are a class of deep probabilistic graphical models with 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 of machine learning power has motivated several applications of SPNs to a variety of 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 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 robustness 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 learning model.

Towards Scalable and Robust Sum-Product Networks

Alvaro H. C. Correia and Cassio P. de Campos^(✉)
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

Towards Robust Classification with Deep Generative Forests

Alvaro H. C. Correia¹ Robert Peharz¹ Cassio de Campos¹

Abstract

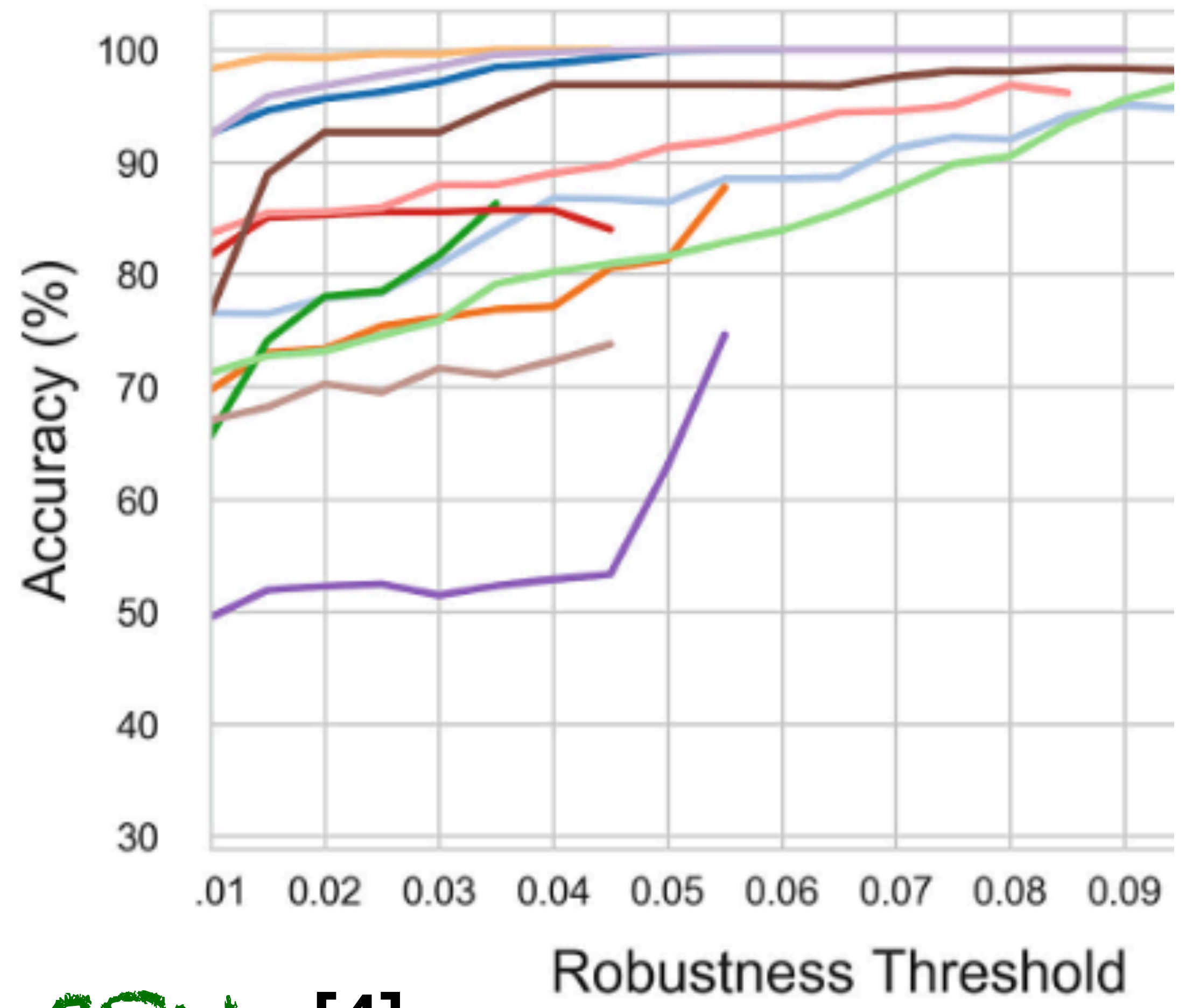
Decision Trees and Random Forests are among the most widely used machine learning models, and often achieve state-of-the-art performance in tabular, domain-agnostic datasets. Nonetheless, they are not robust to adversarial perturbations. In this paper, we propose a novel extension of Random Forests, called Generative Forests (GEF+), which is able to distinguish between reliable and unreliable classifications with high accuracy. **Keywords:** Sum-product networks; tractable probabilistic models; credal classification; sensitivity analysis; robust statistics

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 .

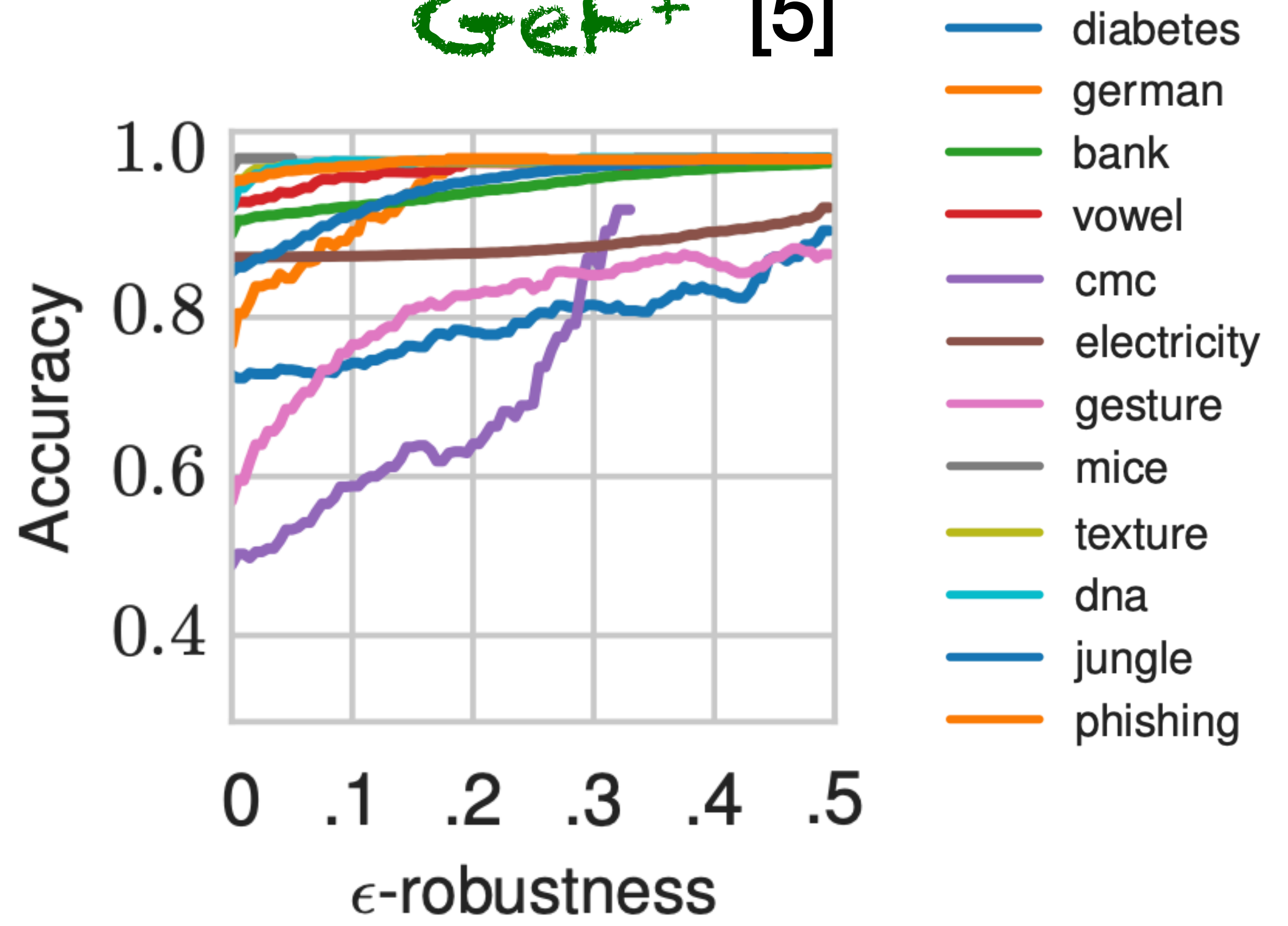
2020

- hypothyroid
- breast-cancer
- flags
- colic
- cmc
- balance-scale
- ecoli
- dermatology
- diabetes
- heart-h
- car
- bridges



SPN [4]

GeF+ [5]



ROBUSTNESS QUANTIFICATION

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



2025 ...

[6, 7, ...]

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

Adrián Detavernier¹

¹Foundations Lab for imprecise probabilities, Ghent University, Belgium

Jasper De Bock¹

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
can 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

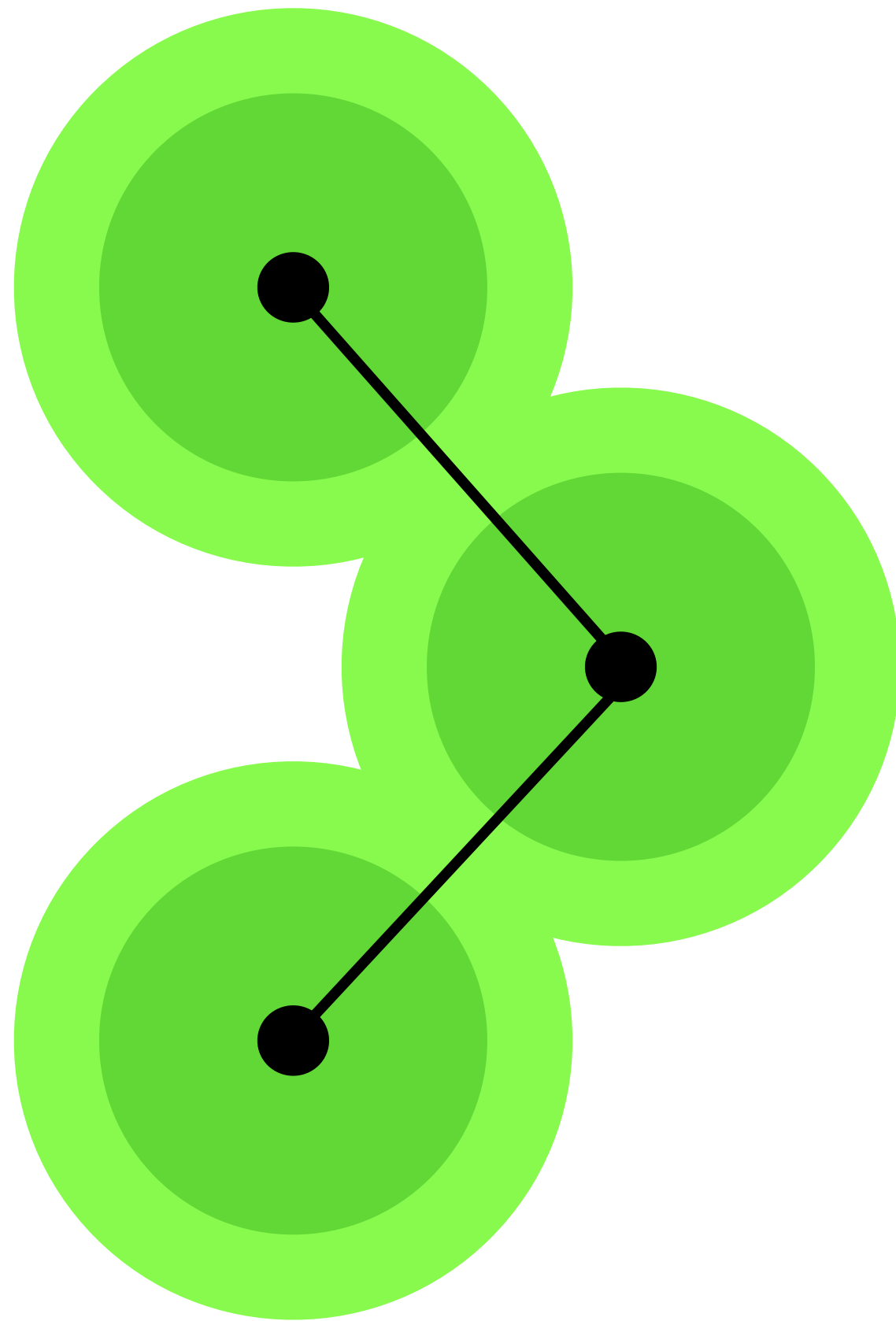
Jasper De Bock

Foundations Lab for imprecise probabilities
Ghent University
Belgium

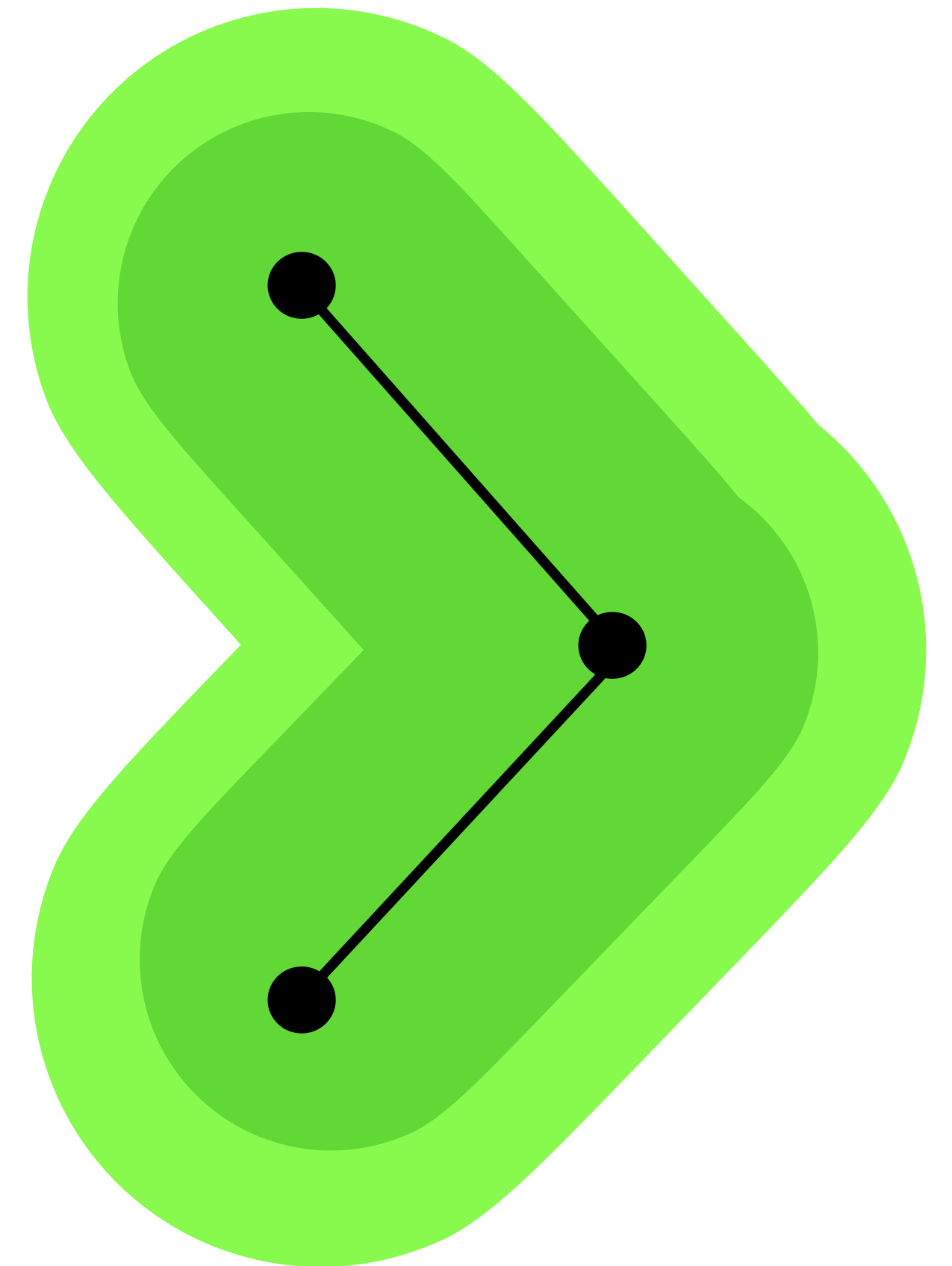
Abstract

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

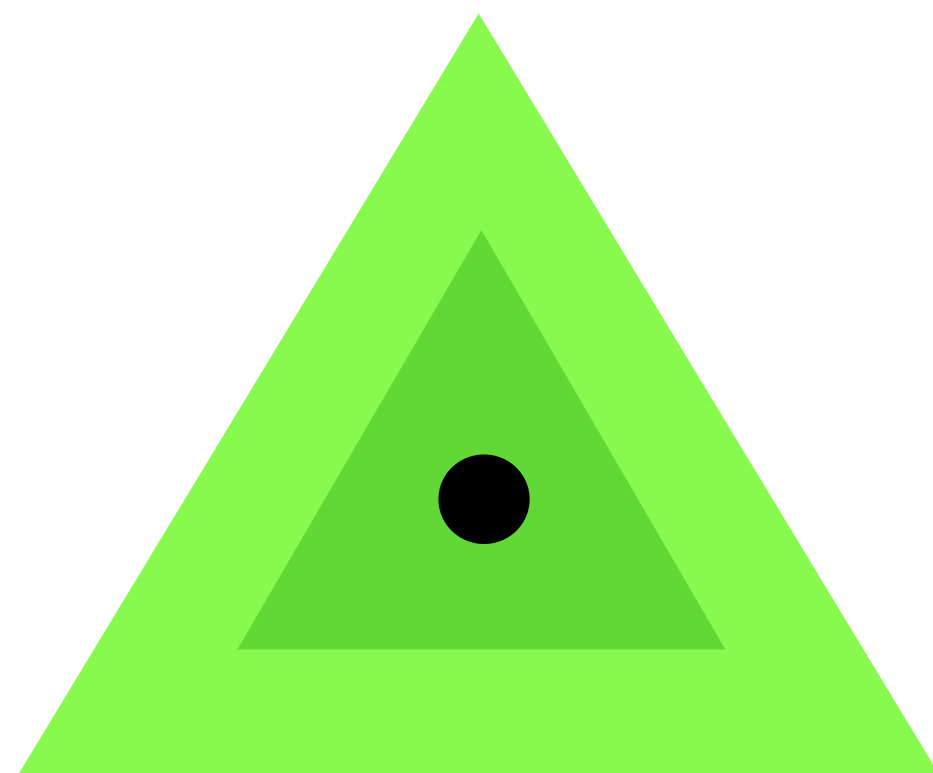
LOCAL



GLOBAL



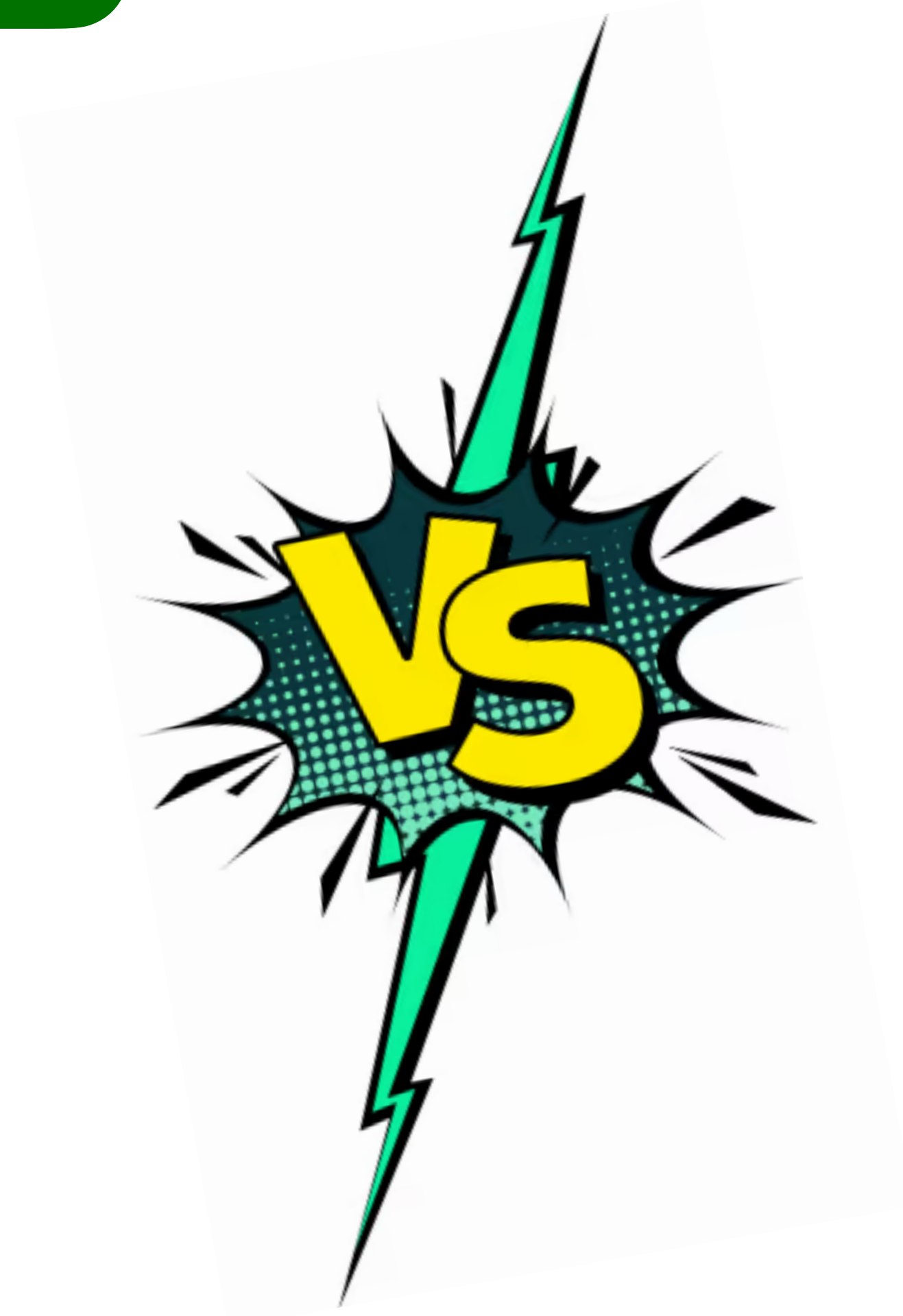
ϵ -CONTAMINATION



\mathcal{P}_ϵ

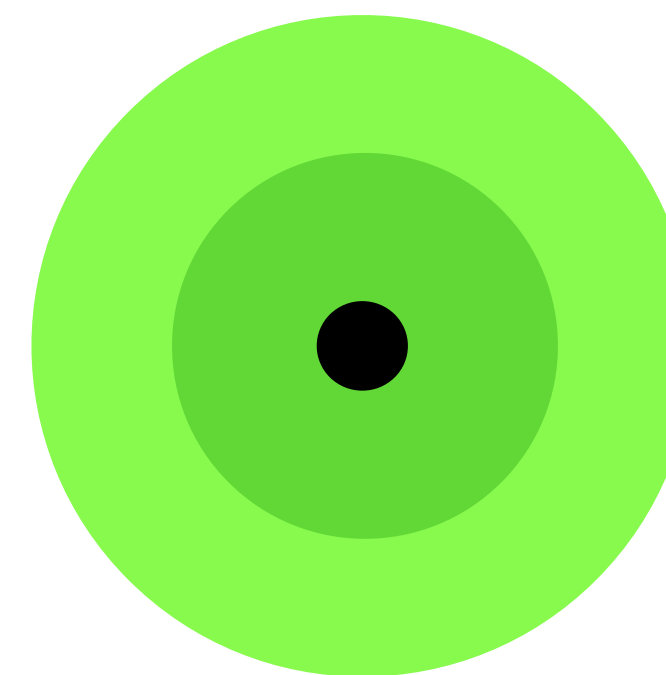
\parallel

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



OTHER STUFF

distance-based, ...



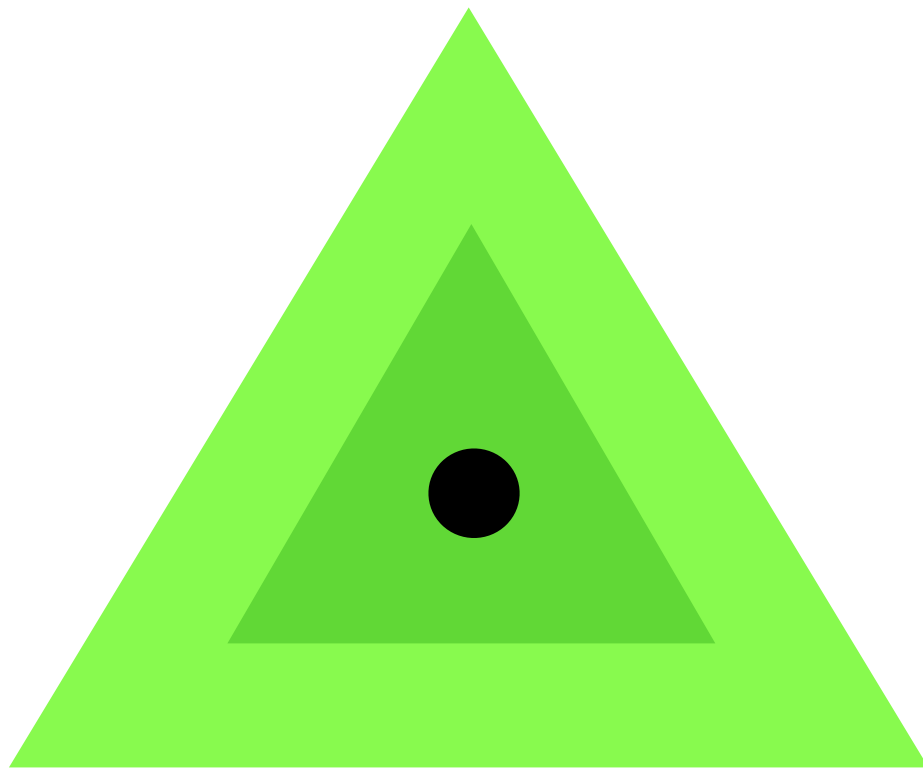
\mathcal{P}_δ

\parallel

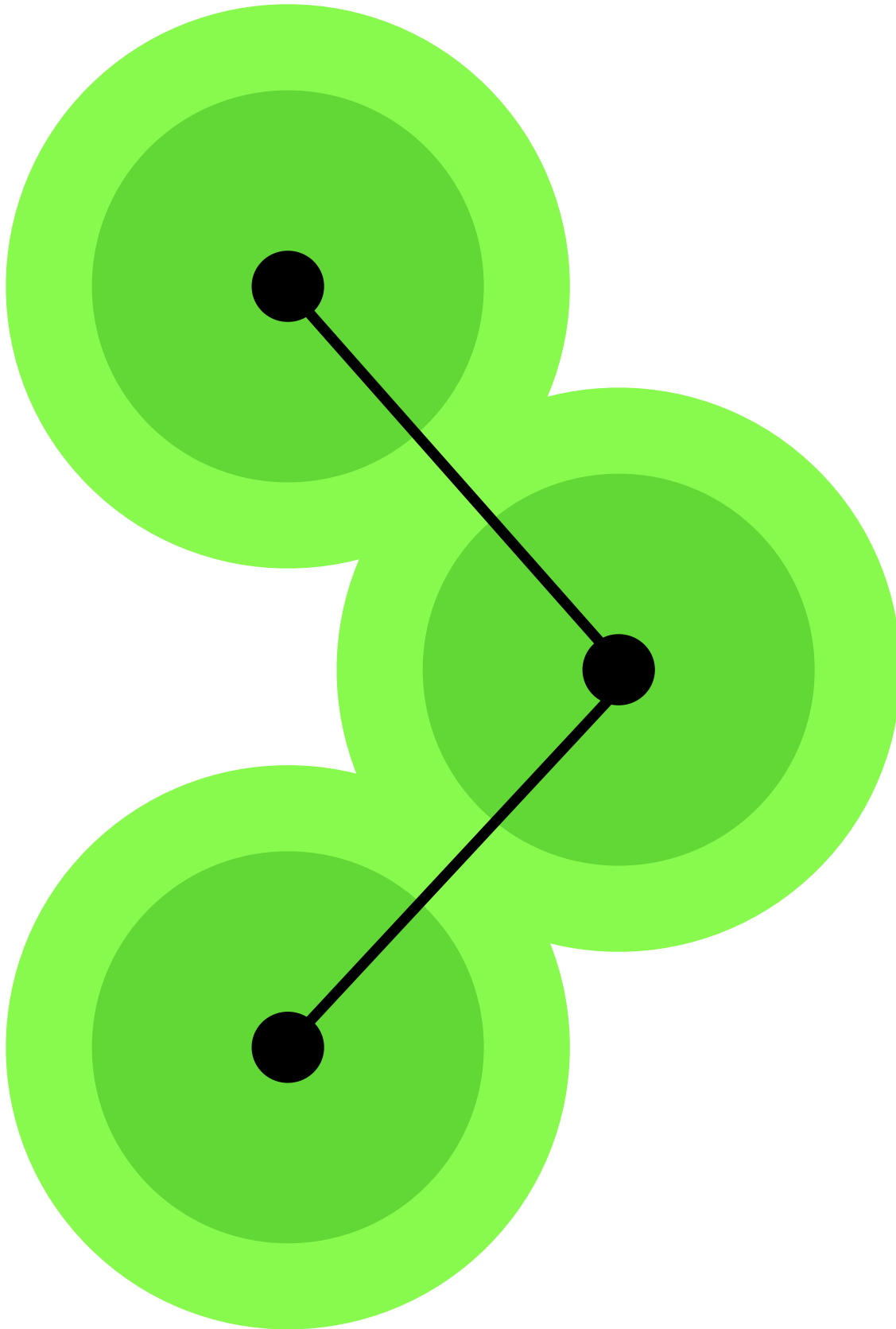
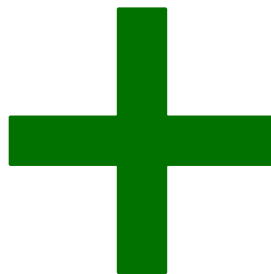
$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

ϵ -CONTAMINATION

LOCAL



earlier work

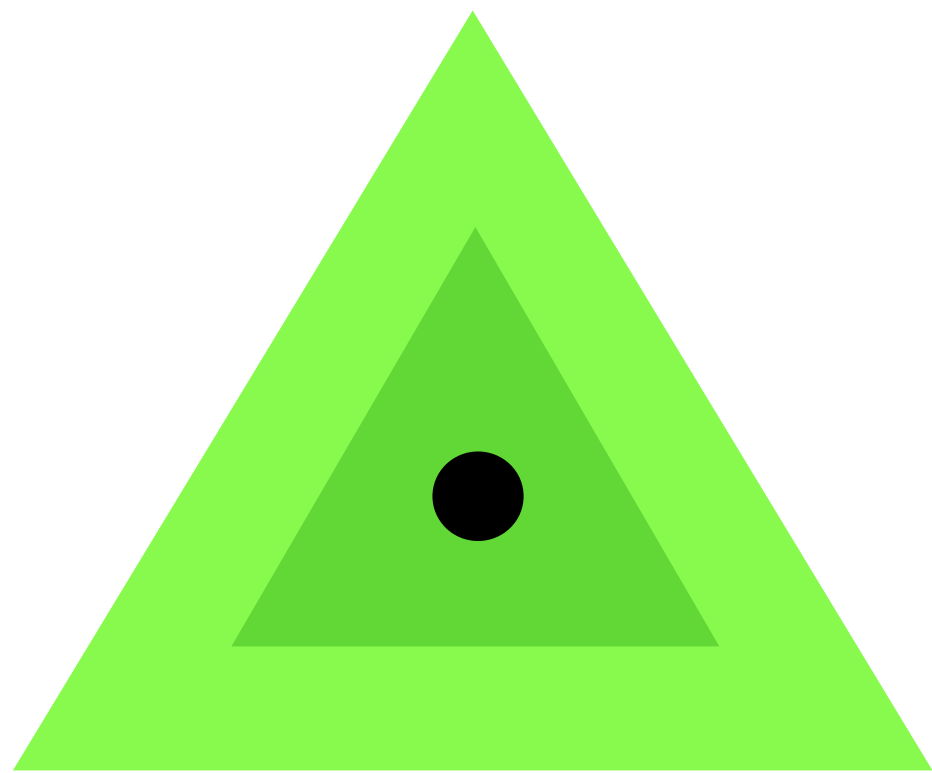


\mathcal{P}_ϵ

\parallel

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

ϵ -CONTAMINATION



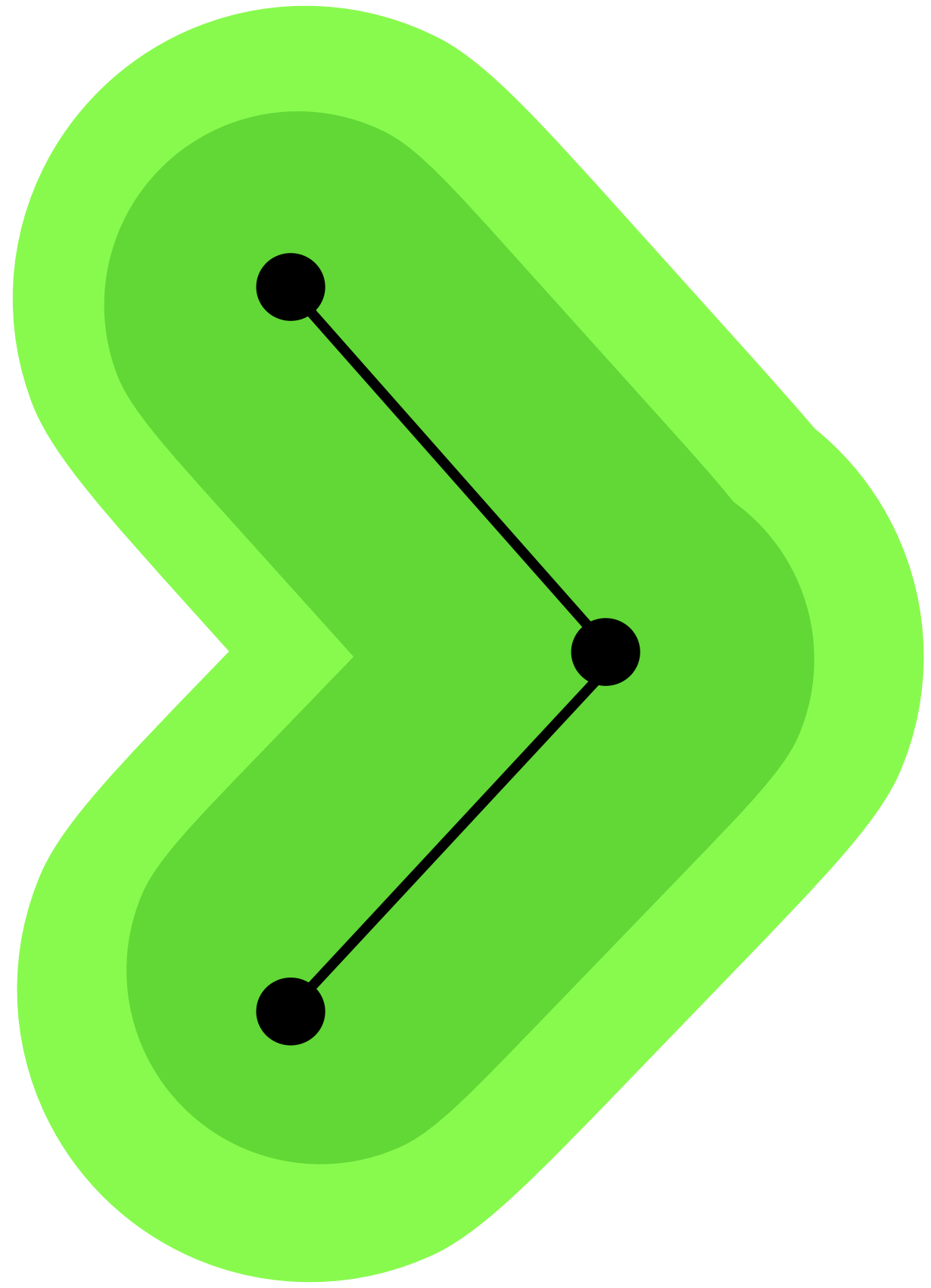
\mathcal{P}_ϵ
||

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

new work

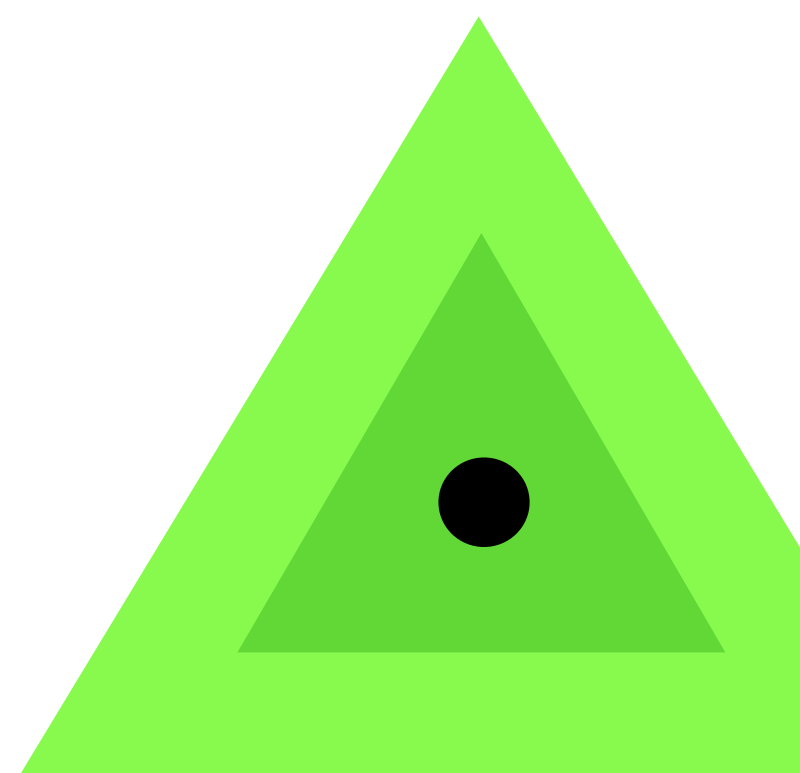


GLOBAL



ϵ -CONTAMINATION

GLOBAL



\mathcal{P}_ϵ

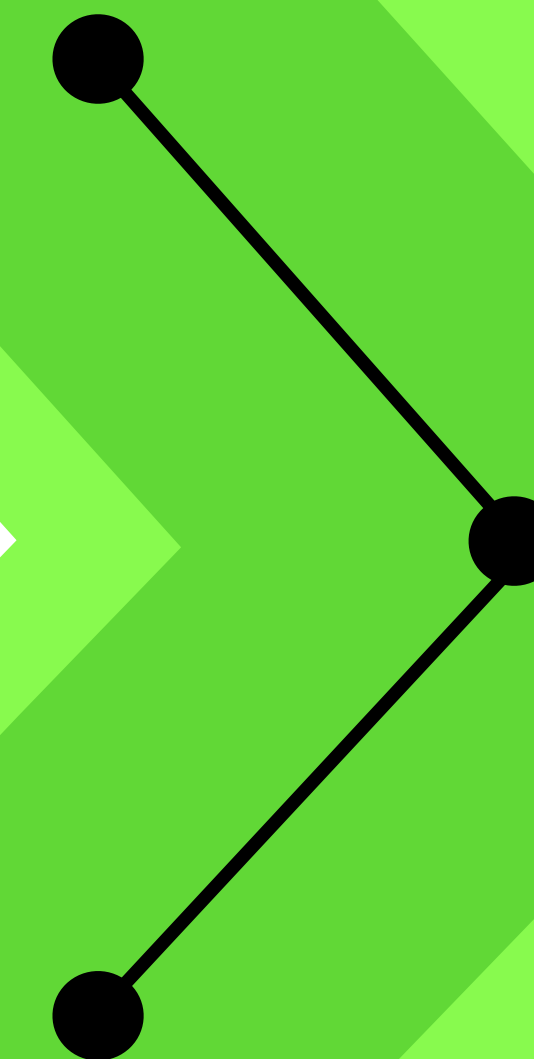
\parallel

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

$$r_{\epsilon, \text{glob}} = \frac{\Delta}{1 + \Delta}$$

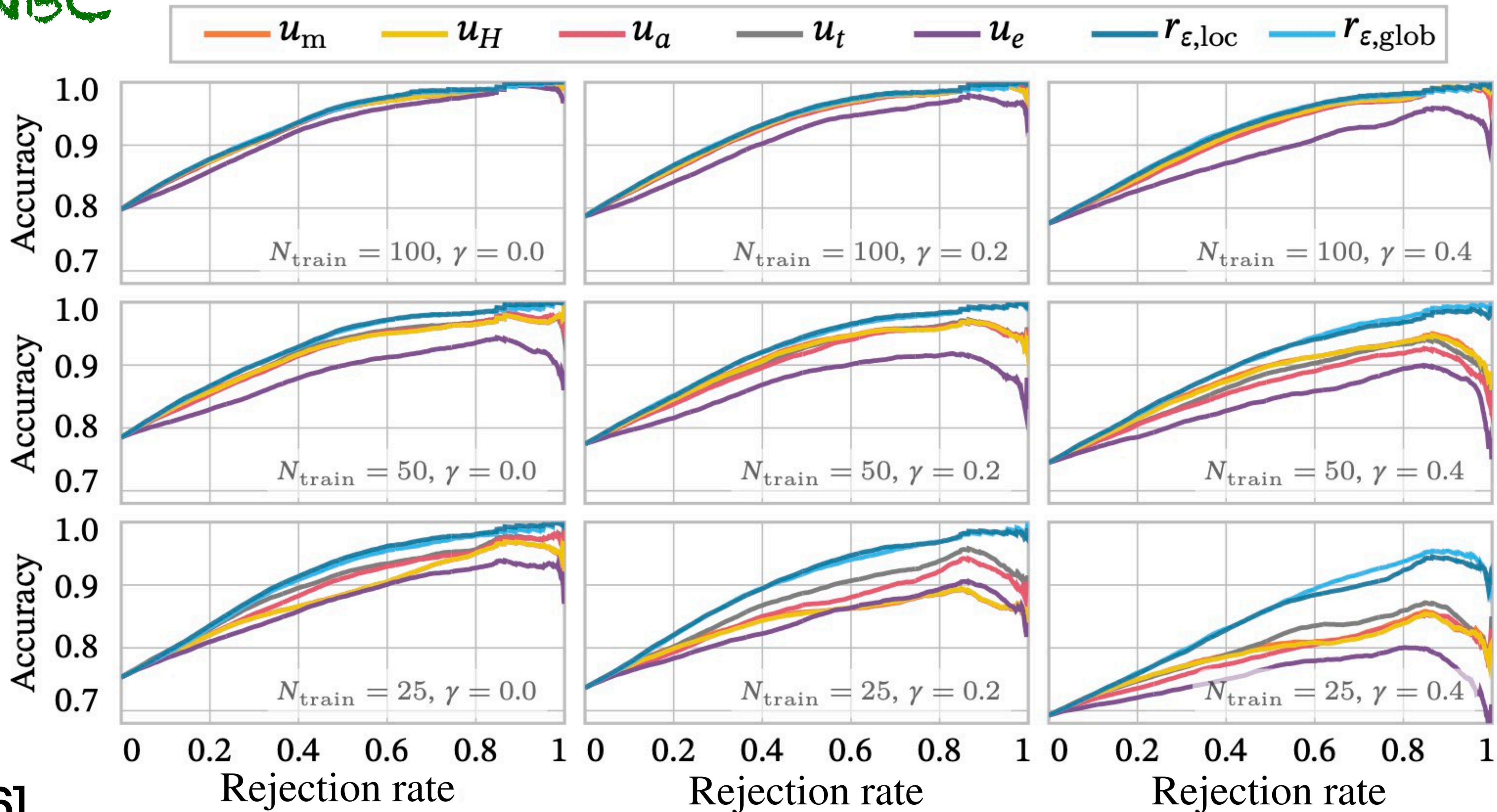
$$\Delta = p_{\text{classif}}(x, \hat{y}) - p_{\text{classif}}(x, \hat{y}_2)$$

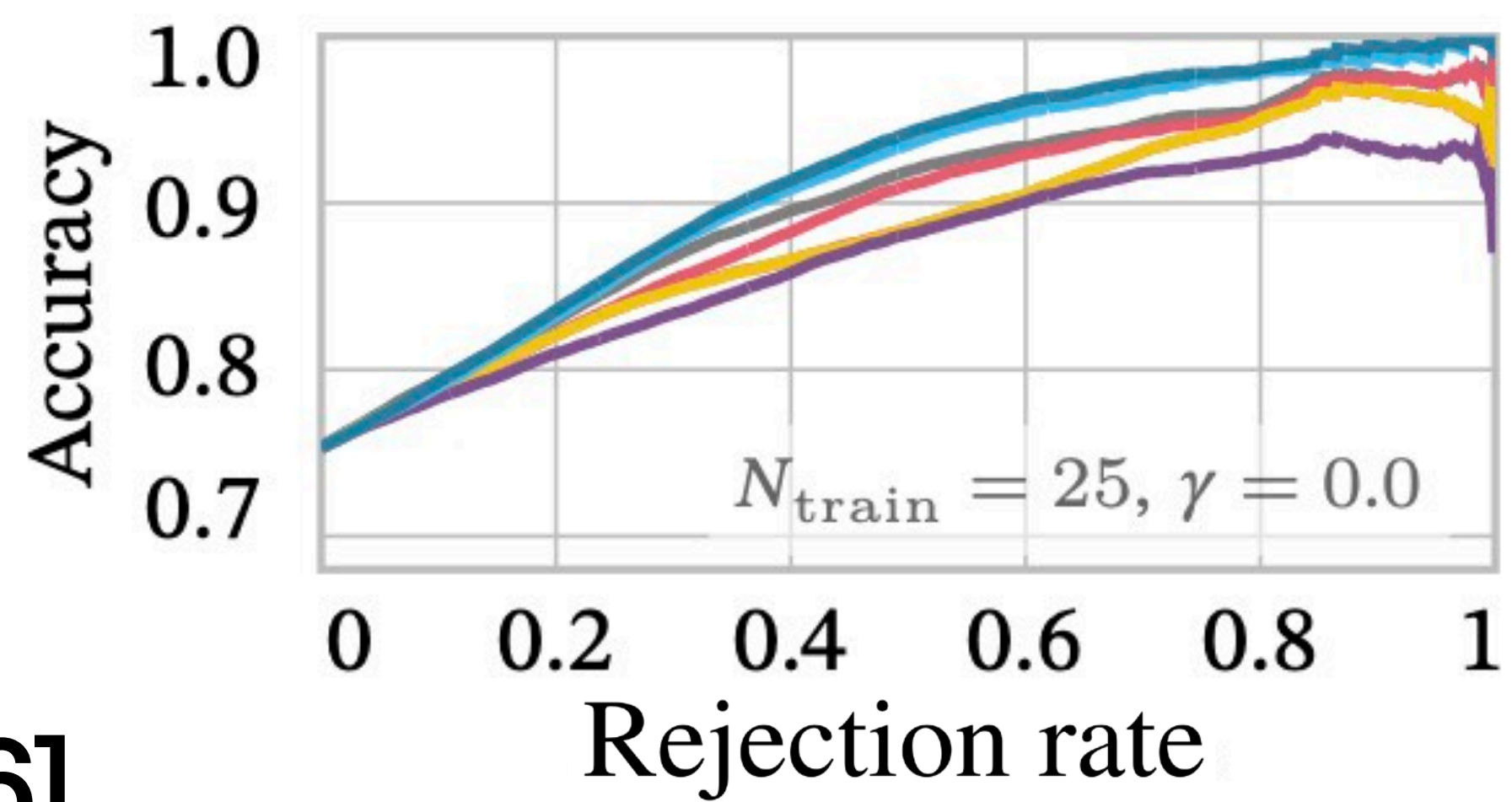
$$\hat{y}_2 = \arg \max_{y \in \mathcal{Y} \setminus \{\hat{y}\}} p_{\text{classif}}(y | x)$$

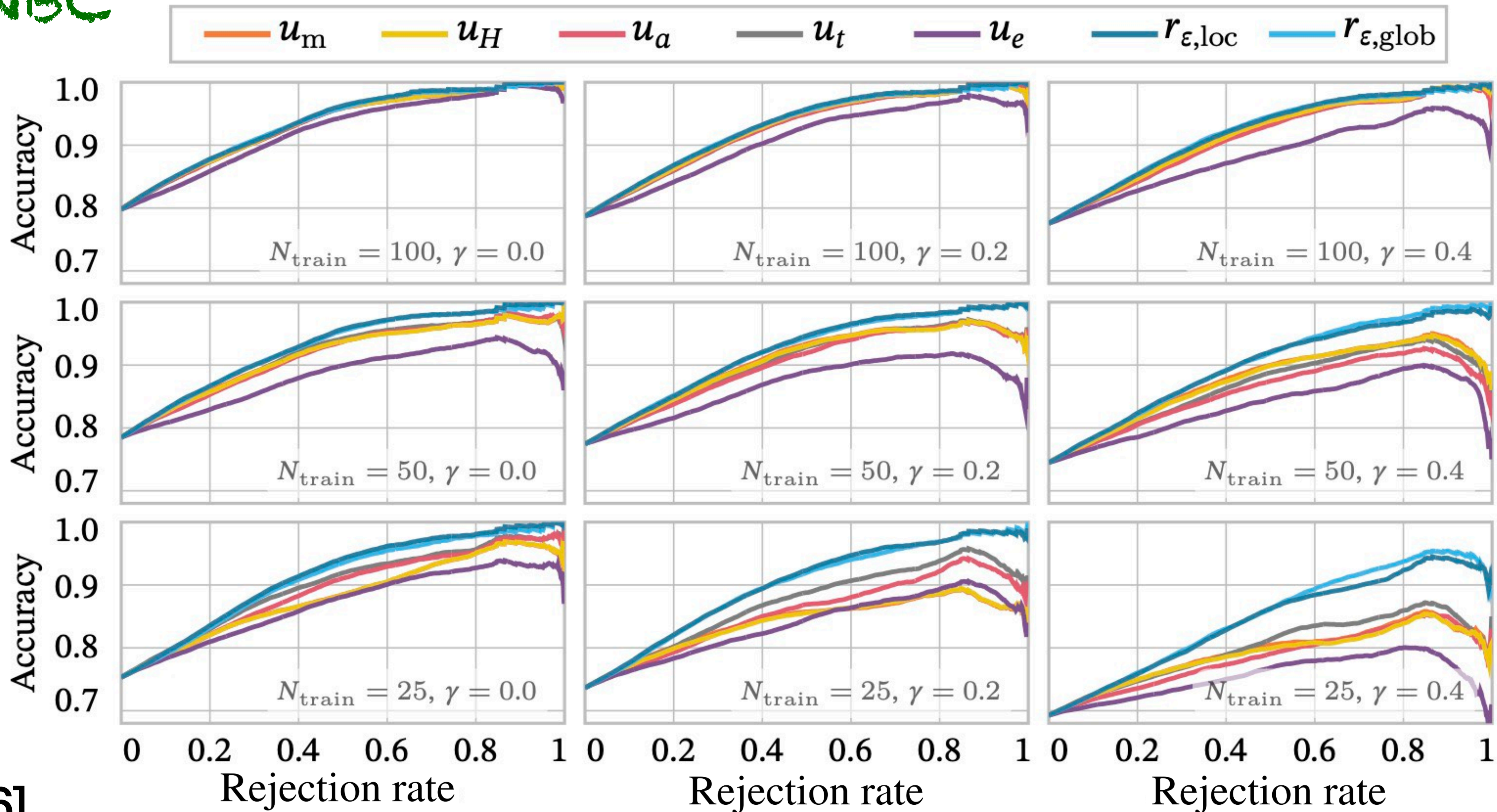


ROBUSTNESS QUANTIFICATION

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

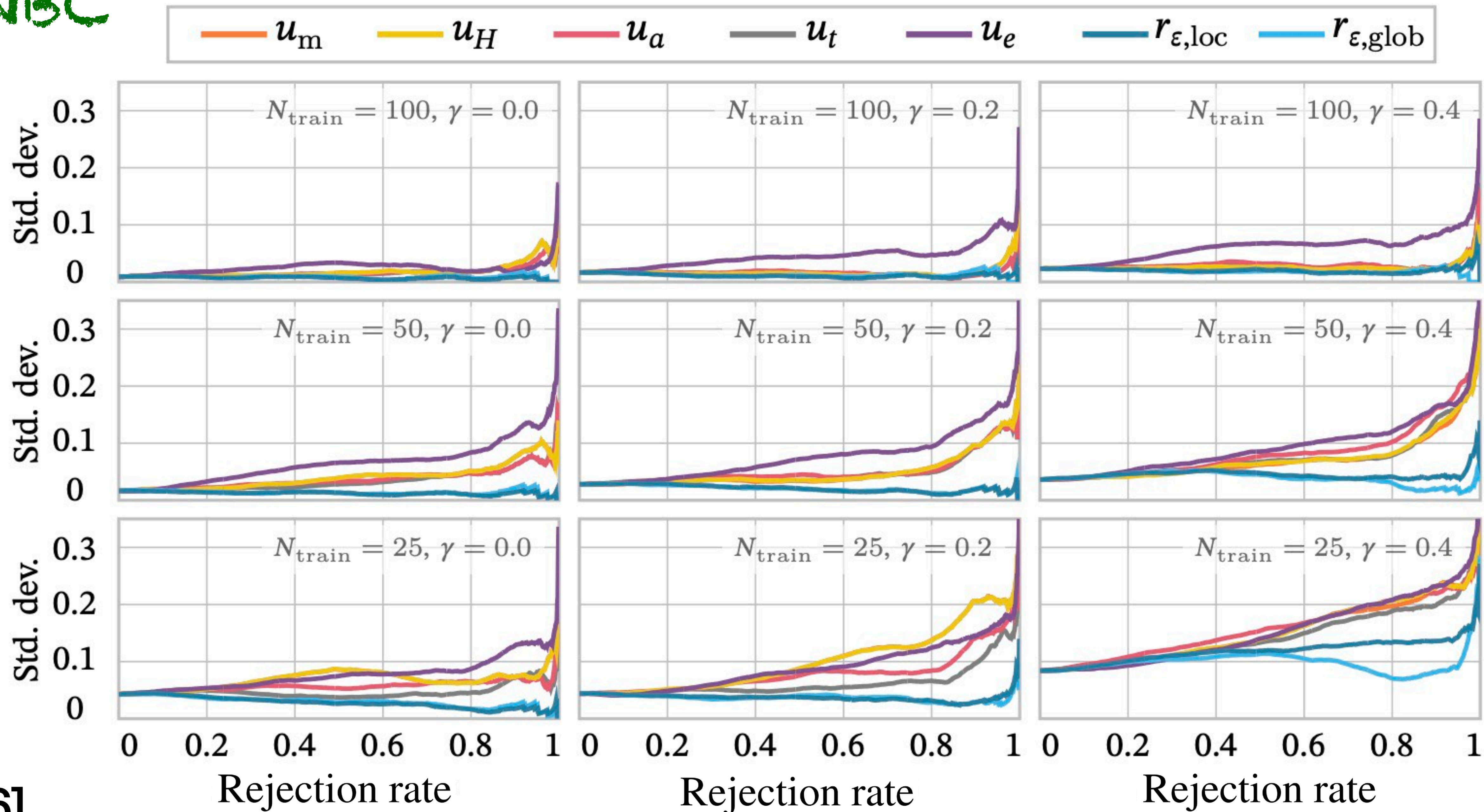






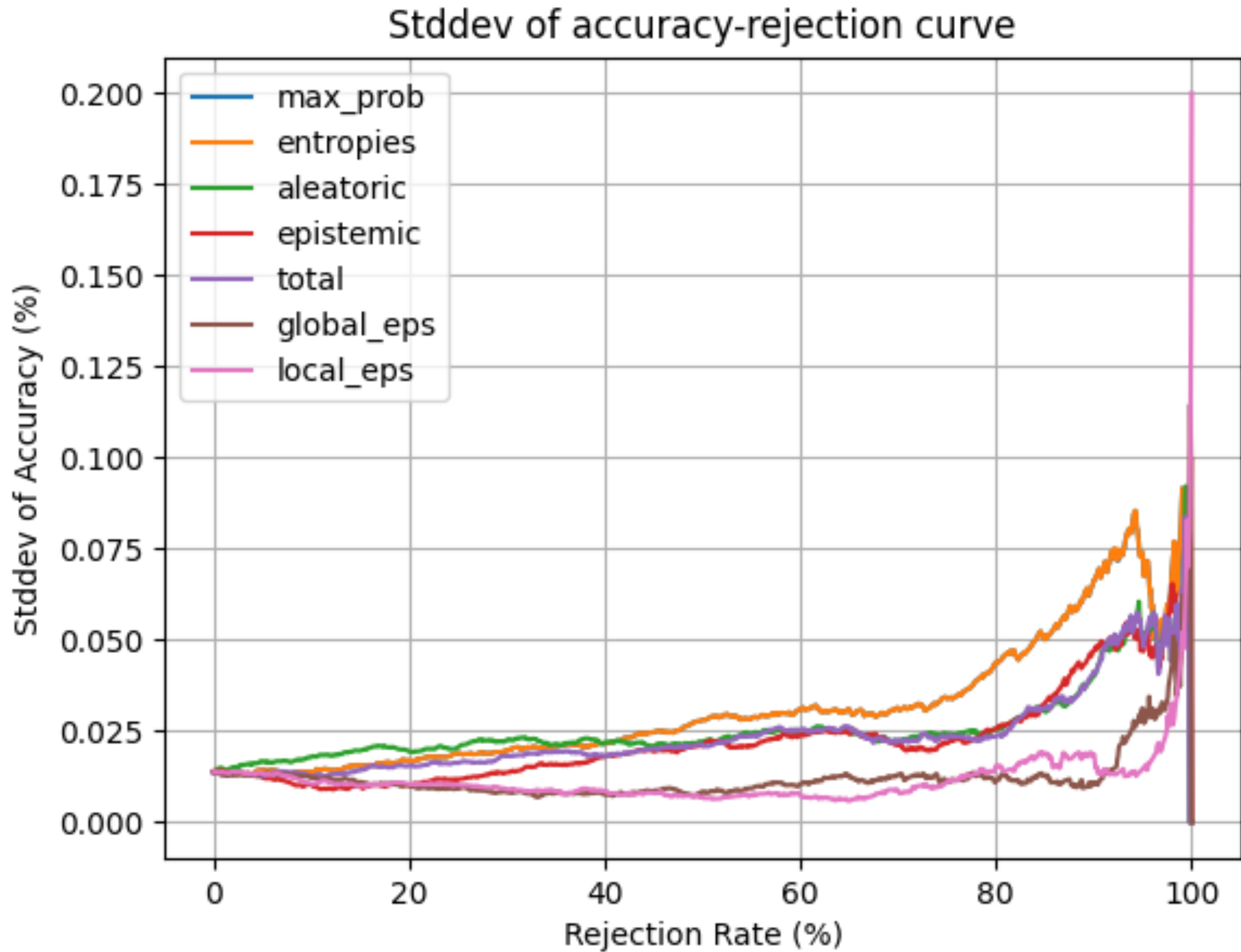
ROBUSTNESS QUANTIFICATION

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



ROBUSTNESS QUANTIFICATION

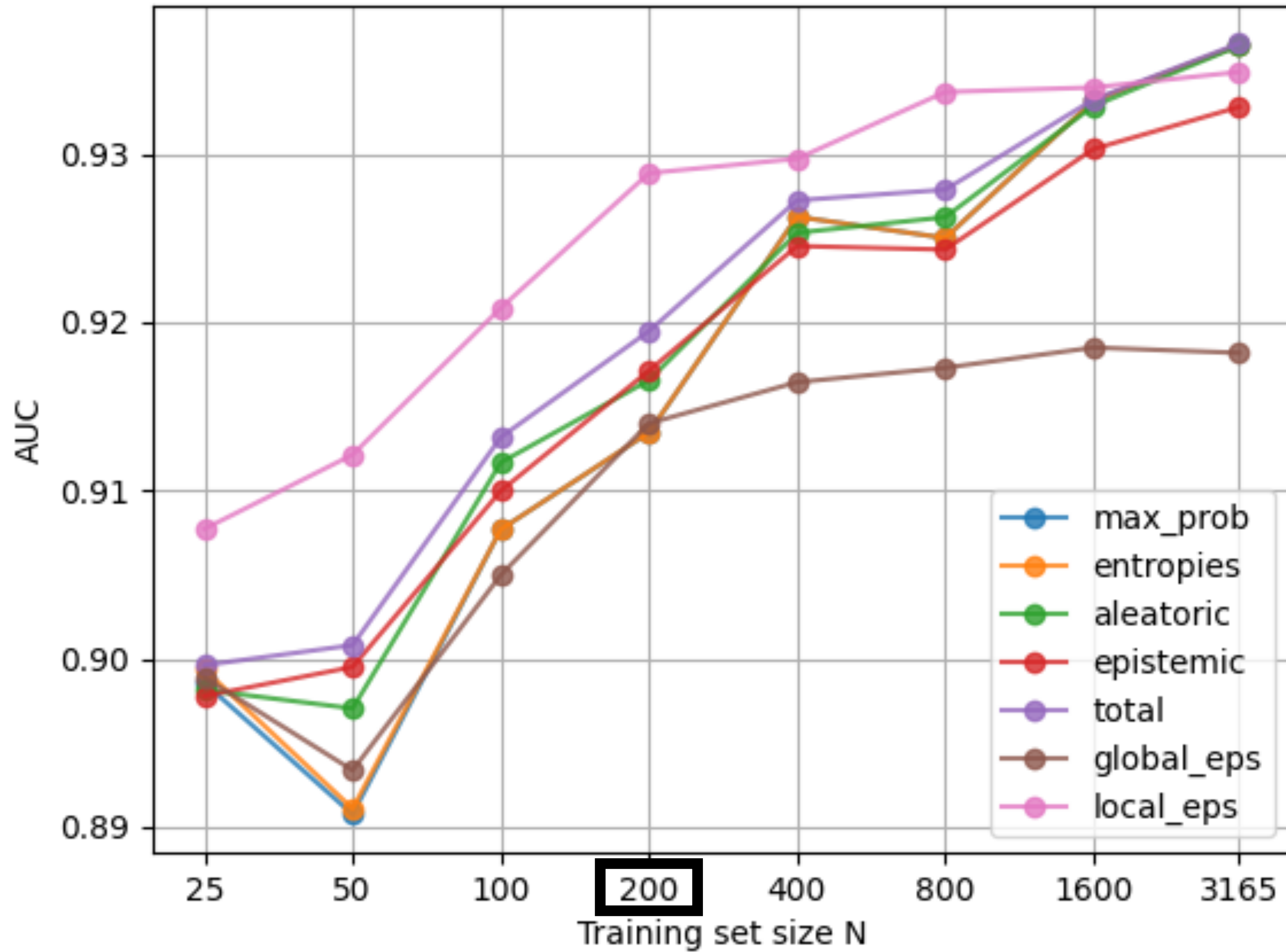
- correlates nicely with accuracy
- works for different types of model architectures
- also works with global perturbations
- is competitive with UQ
- is good with distribution shift and small data sets
- is **more stable than UQ** ✓



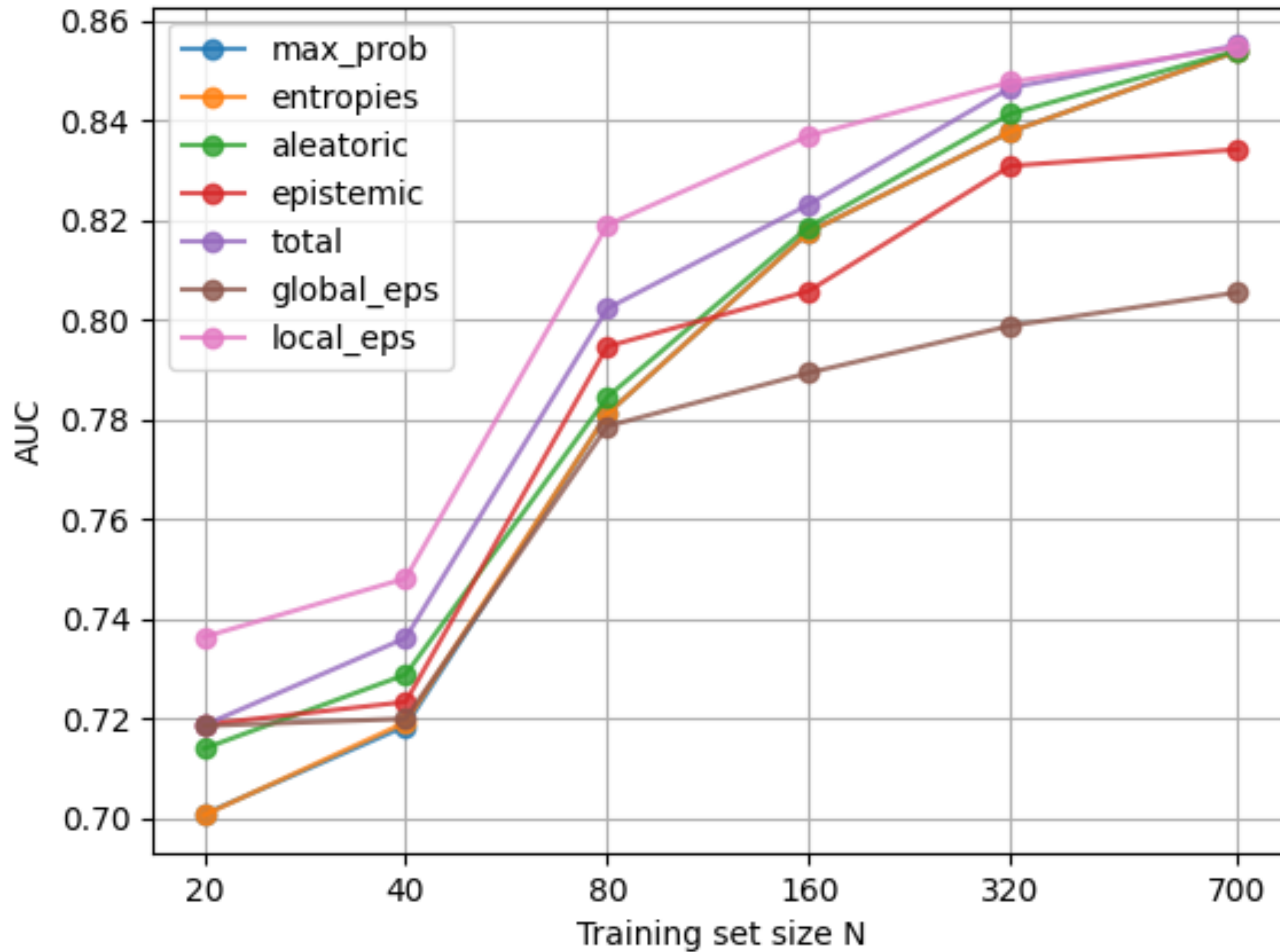
ROBUSTNESS QUANTIFICATION

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

AUC vs Training set size for dataset bank



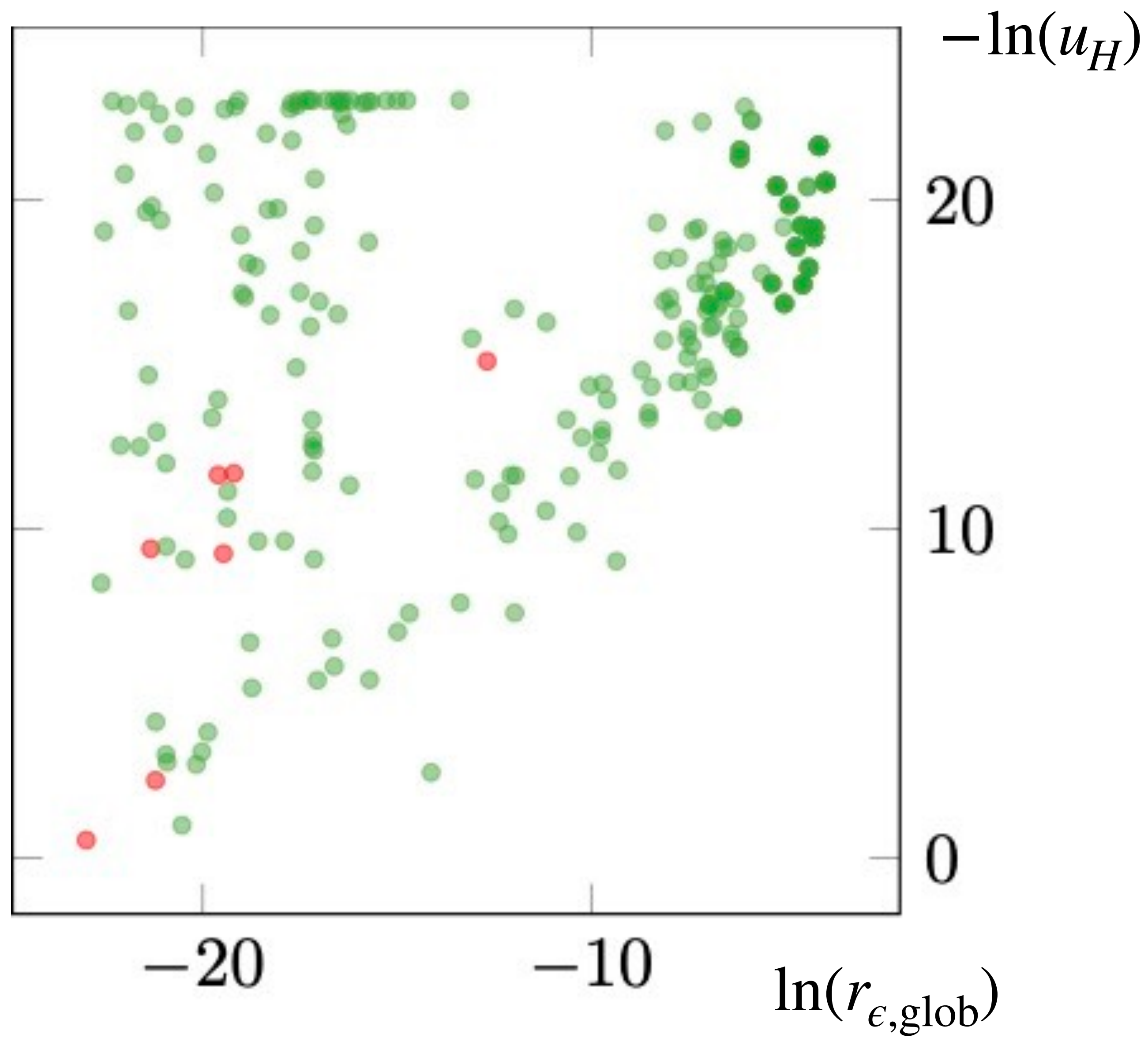
AUC vs Training set size for dataset german



ROBUSTNESS QUANTIFICATION

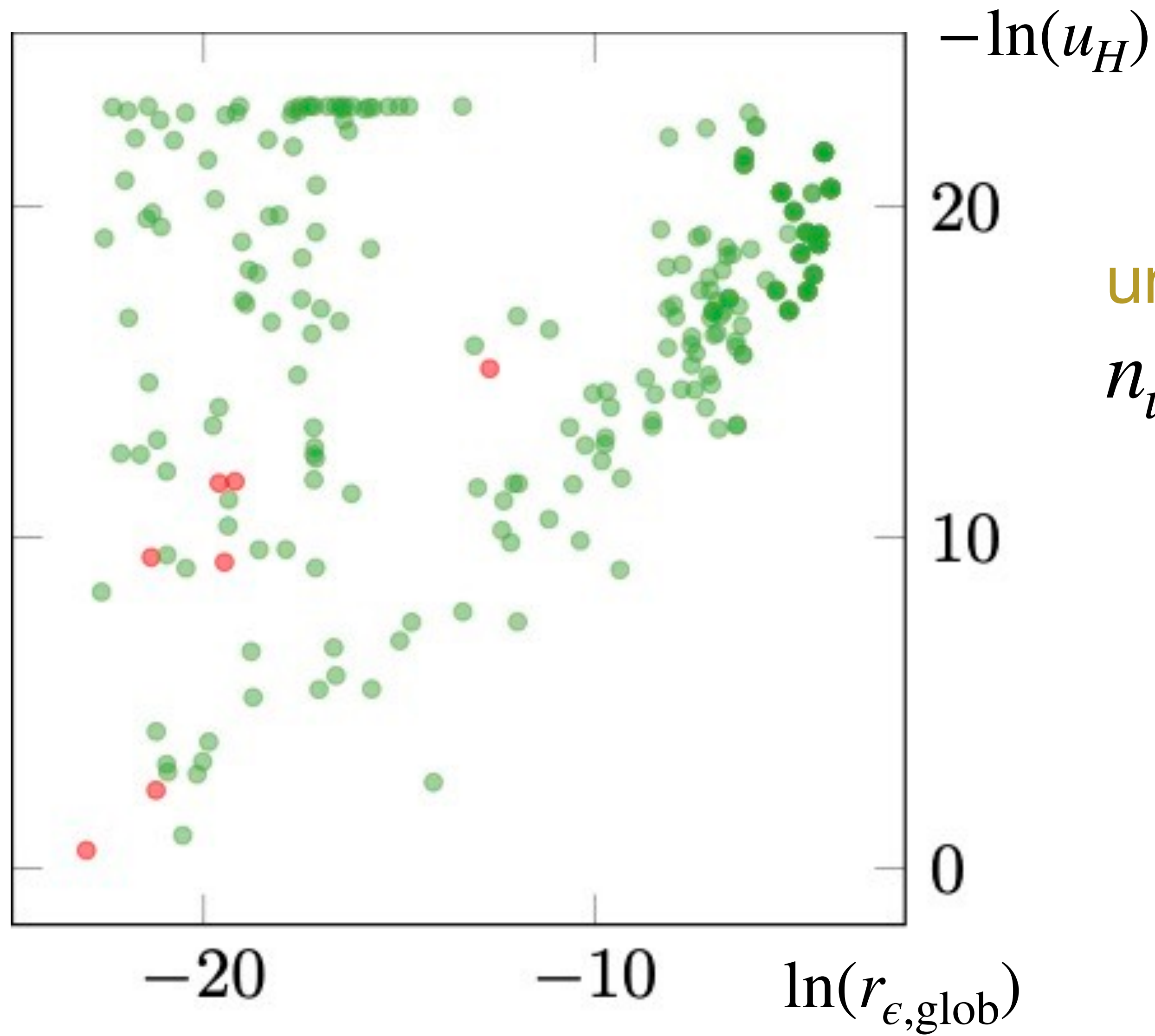
- correlates nicely with accuracy
- works for different types of model architectures
- also works with global perturbations ✓
- is competitive with UQ ✓
- is good with distribution shift and small data sets ✓
- is more stable than UQ ✓

NBC



[7]

NBC

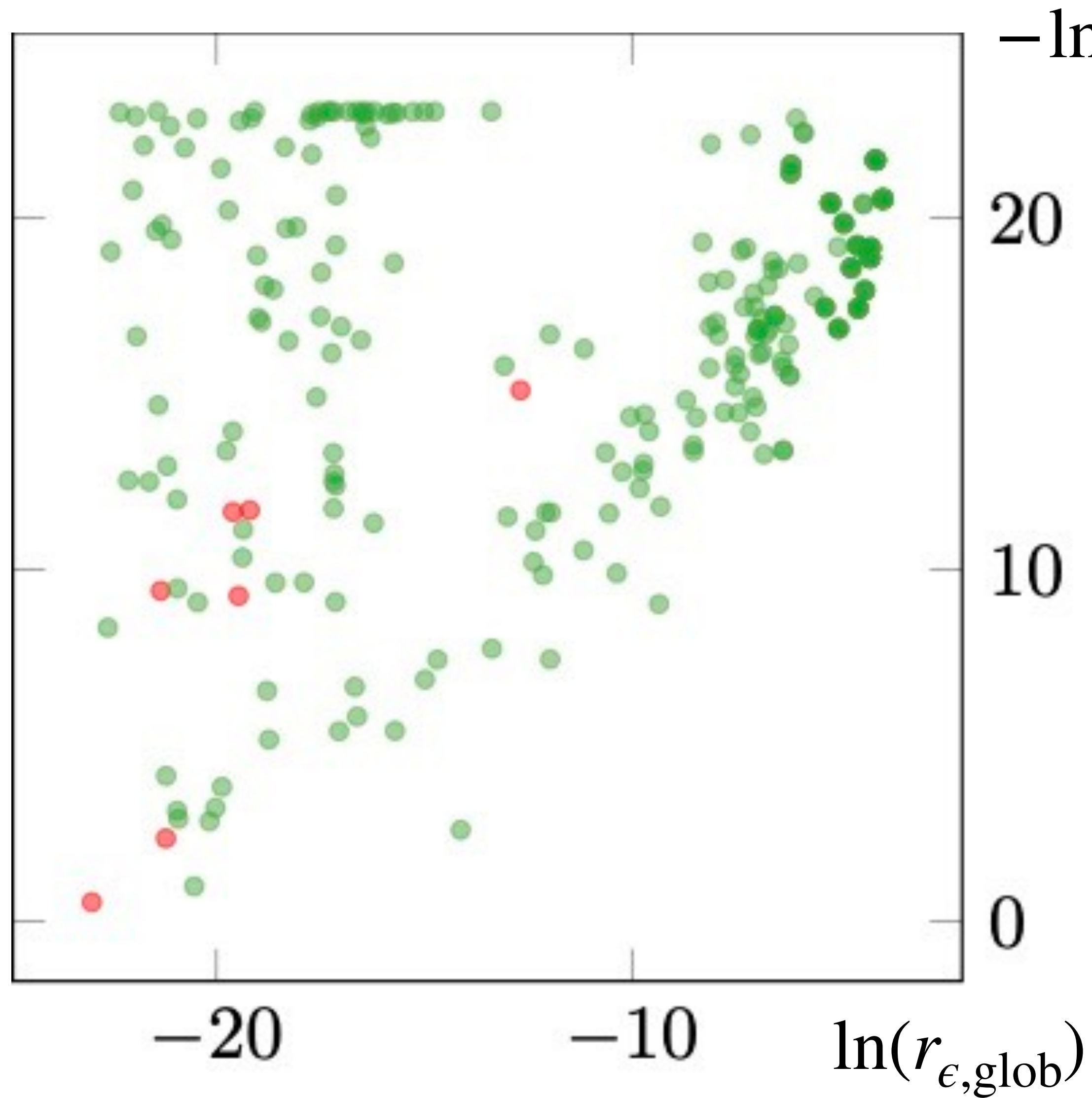


uncertainty ordering

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

[7]

NBC



$-\ln(u_H)$

20

uncertainty ordering

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

10

robustness ordering

$n_{r_{\epsilon, \text{glob}}, i}$: order of i according to $r_{\epsilon, \text{glob}}$

0

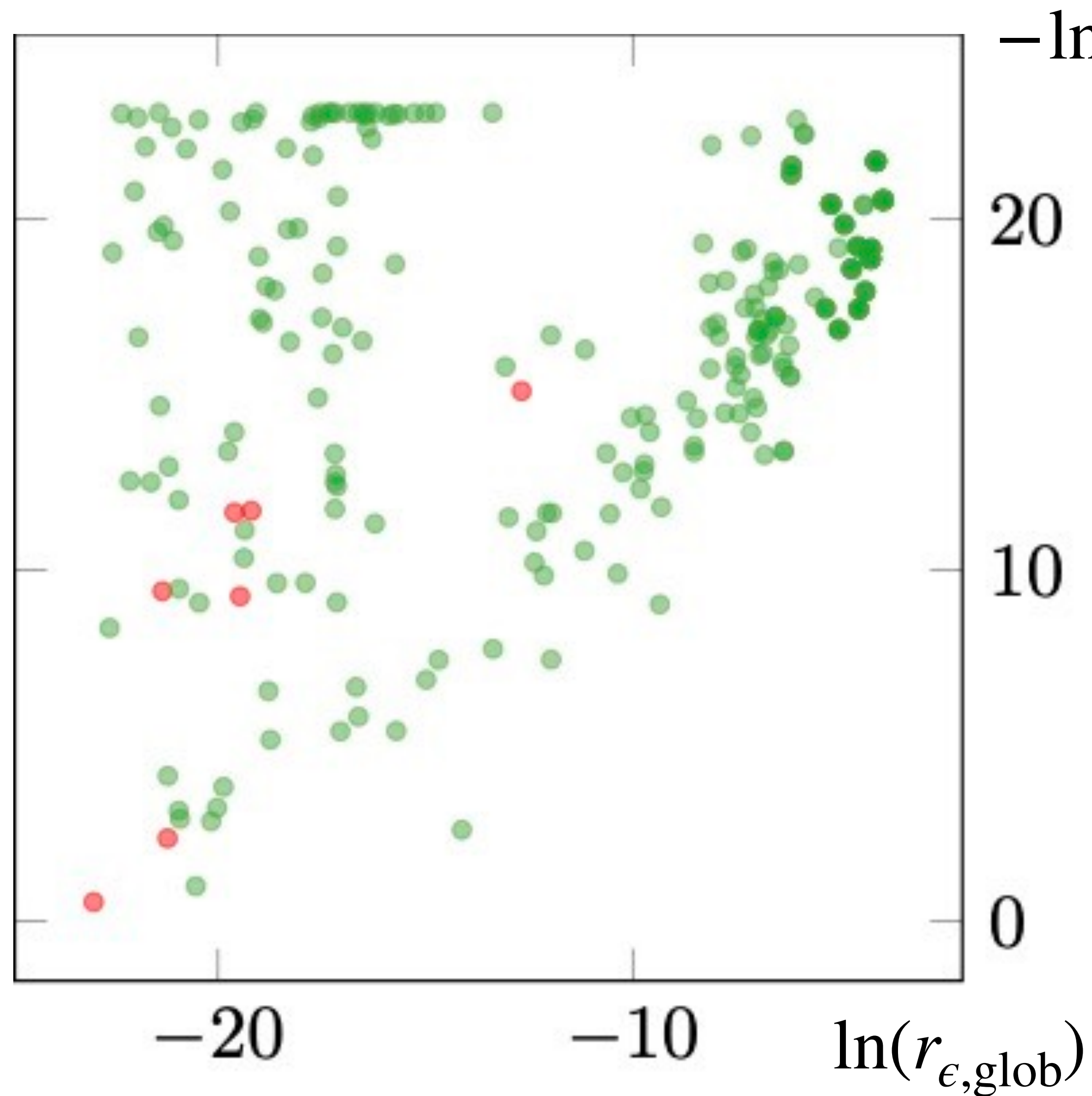
-20

-10

$\ln(r_{\epsilon, \text{glob}})$

[7]

NBC



$-\ln(u_H)$

20

uncertainty ordering

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

10

robustness ordering

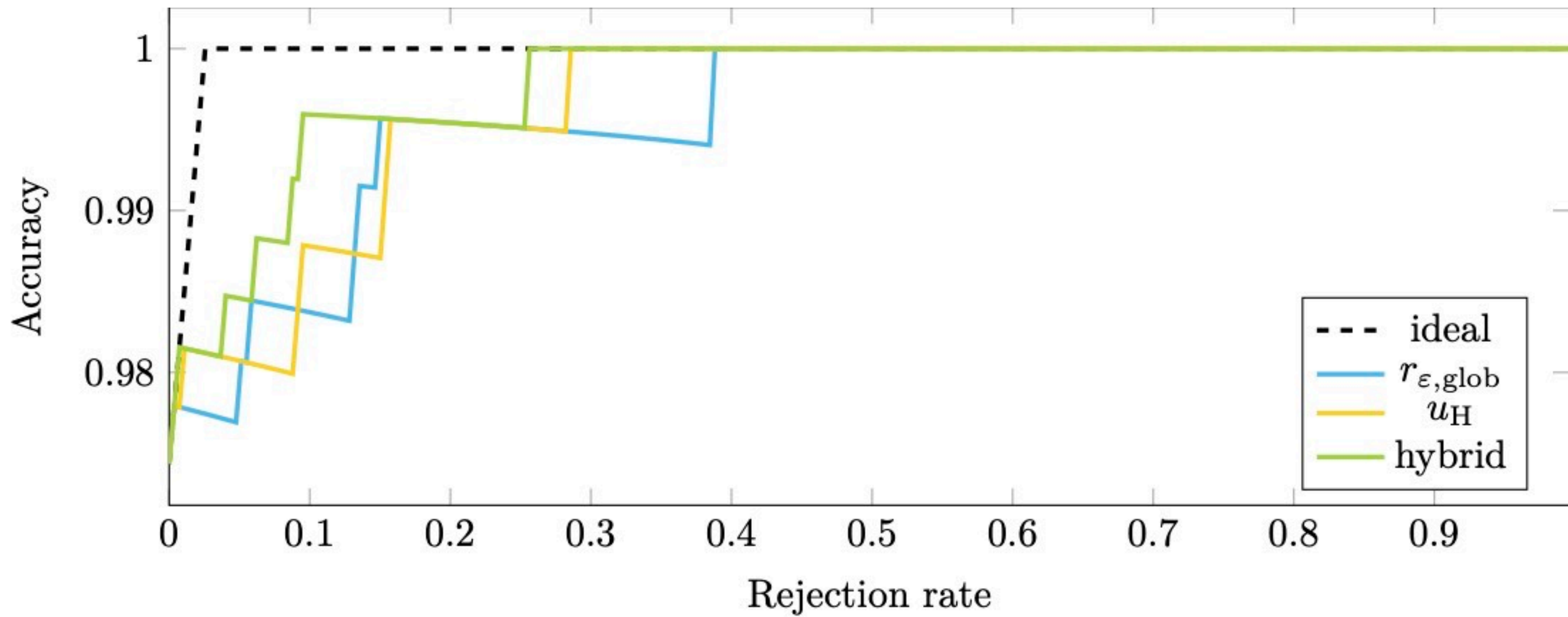
$n_{r_{\epsilon, \text{glob}}, i}$: order of i according to $r_{\epsilon, \text{glob}}$

0

hybrid ordering

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

[7]



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

Dataset	u_H	$r_{\epsilon,loc}$	hybrid	γ	γ^*	$r_{\epsilon,glob}$	hybrid	γ	γ^*
Adult	0.9322	0.9044	0.9322	1.00	1.00	0.7766	0.9322	1.00	1.00
Australian Credit	0.9268	0.9276	0.9304	0.83	0.56	0.9097	0.9290	0.88	0.65
Bank Marketing	0.9338	0.9343	0.9345	0.75	0.25	0.9241	0.9337	0.94	0.97
Breast Cancer	0.9945	0.9969	0.9959	0.62	0.15	0.9964	0.9969	0.59	0.26
German Credit	0.8670	0.8644	0.8680	0.67	0.53	0.8065	0.8678	0.86	0.92
Heart disease	0.7927	0.7852	0.7927	0.99	0.90	0.7466	0.7930	0.98	0.91
Lymphography	0.8804	0.8705	0.8867	0.39	0.60	0.8337	0.8880	0.66	0.79
NPHA	0.4947	0.5350	0.4887	0.85	0.28	0.5220	0.4856	0.91	0.26
Nursery	0.9814	0.9828	0.9827	0.33	0.17	0.9727	0.9813	0.93	0.96
Solar Flare (big)	0.8450	0.8762	0.8736	0.24	0.00	0.8638	0.8736	0.72	0.54
Solar Flare (small)	0.8635	0.8623	0.8560	0.64	0.43	0.8115	0.8706	0.77	0.84
SPECT Heart	0.9455	0.8915	0.9455	0.99	0.99	0.5738	0.9454	0.99	1.00
Student Math	0.9336	0.9381	0.9376	0.46	0.32	0.9289	0.9396	0.65	0.53
Student Port	0.8885	0.9159	0.9106	0.35	0.01	0.9032	0.9073	0.73	0.39

ROBUSTNESS QUANTIFICATION

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



Rodrigo
Lassance

MACHINE
LEARNING

IMPRECISE
PROBABILITIES

ROBUSTNESS
QUANTIFICATION



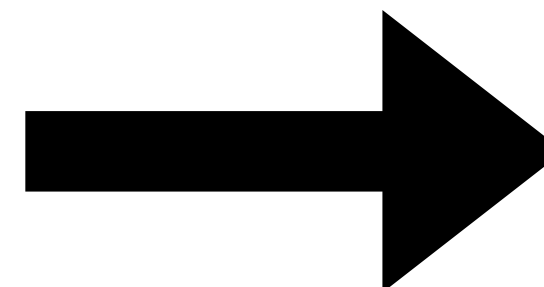
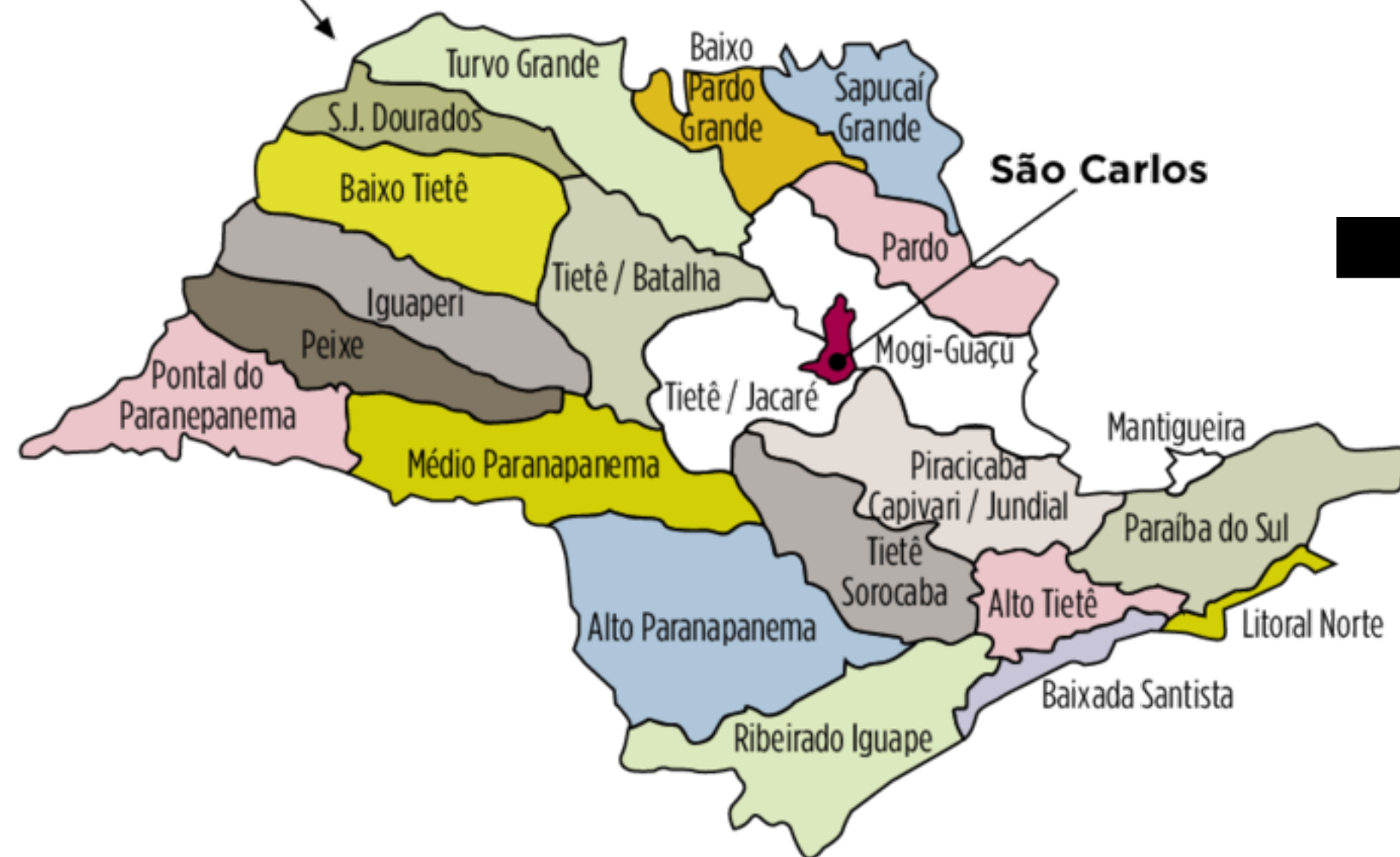
SMaLL
Statistical Machine Learning Lab

FLip

Foundations Lab for
imprecise probabilities



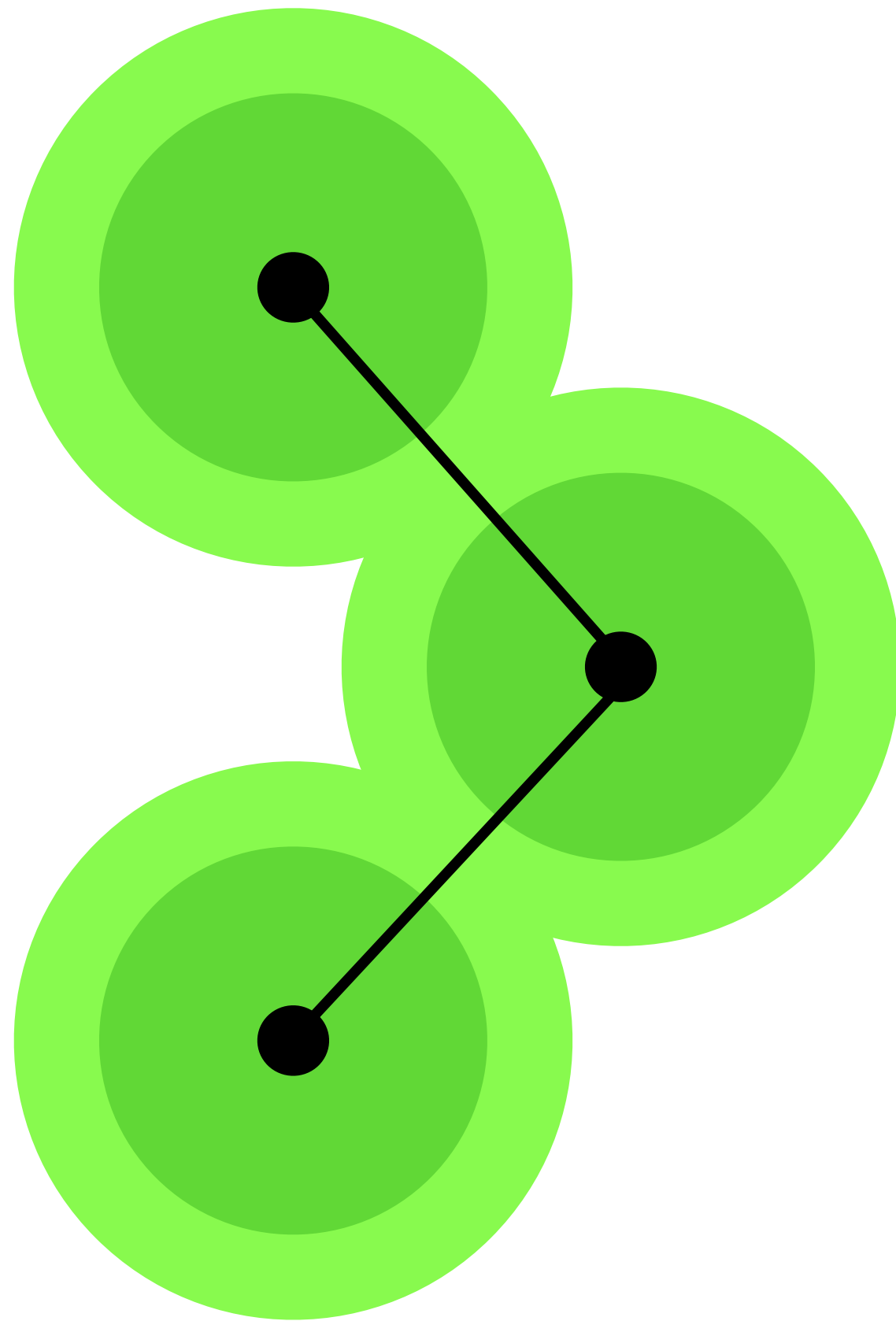
Estado de São Paulo



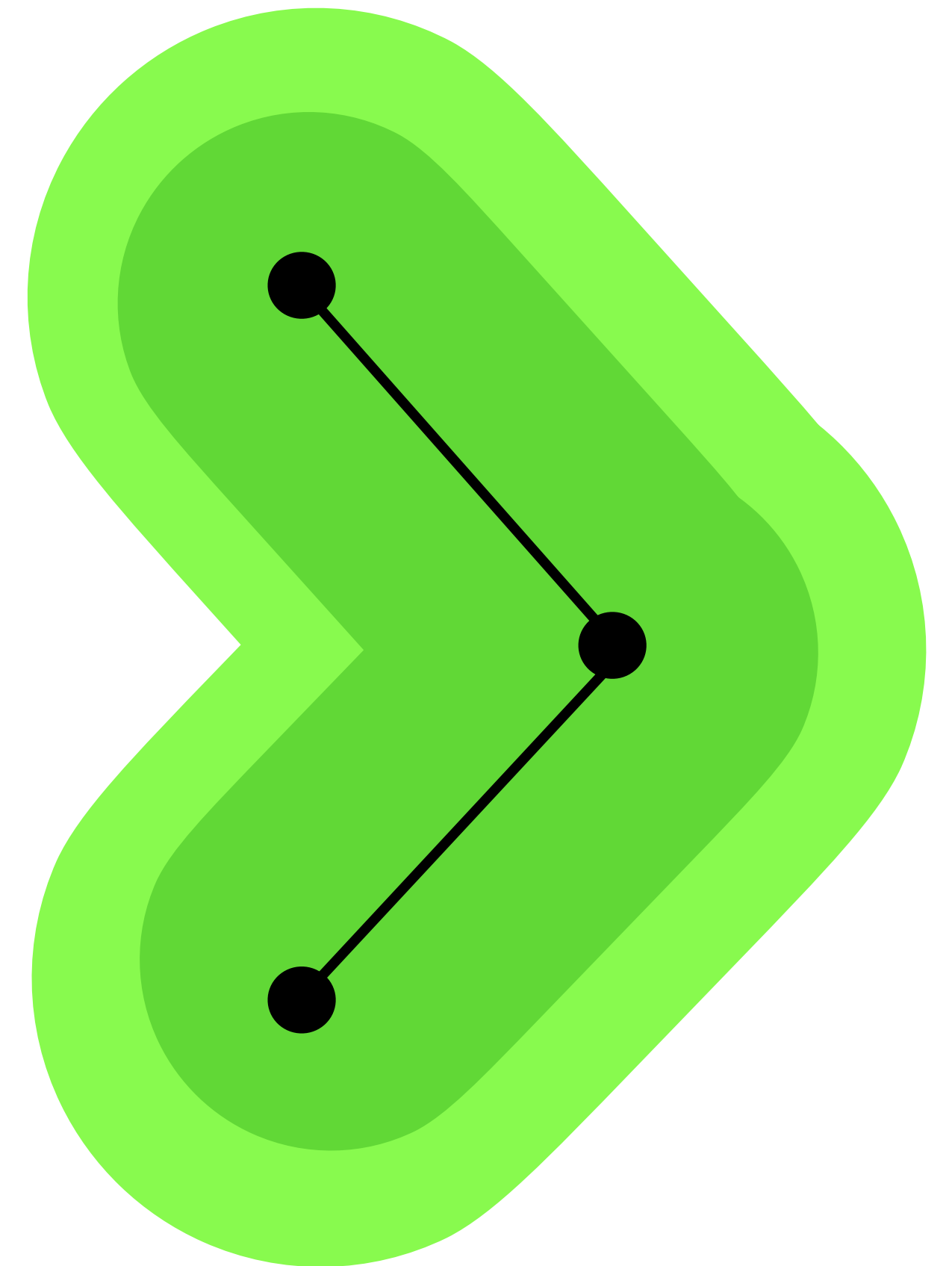
Ghent
Belgium



LOCAL



GLOBAL



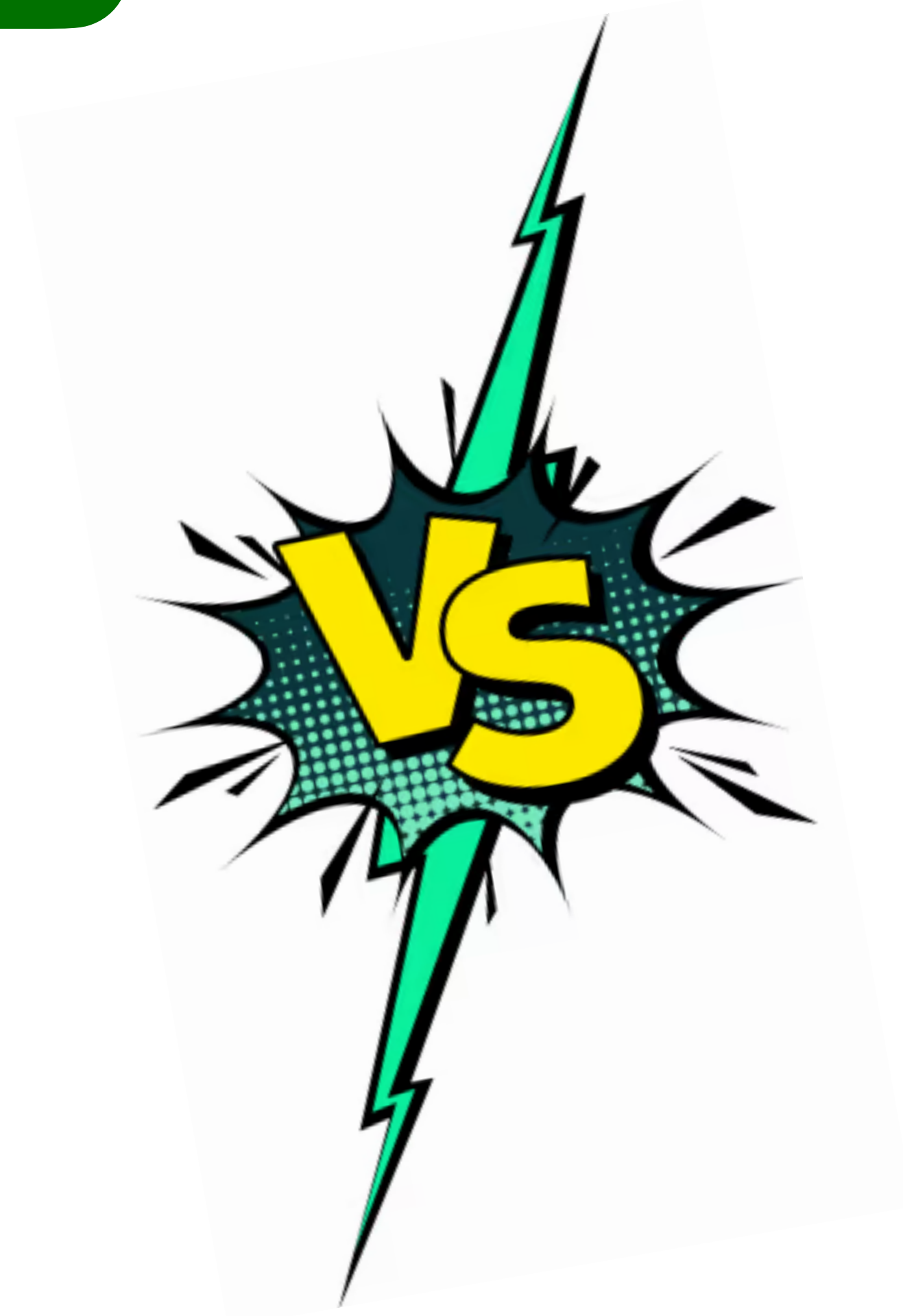
ϵ -CONTAMINATION



\mathcal{P}_ϵ

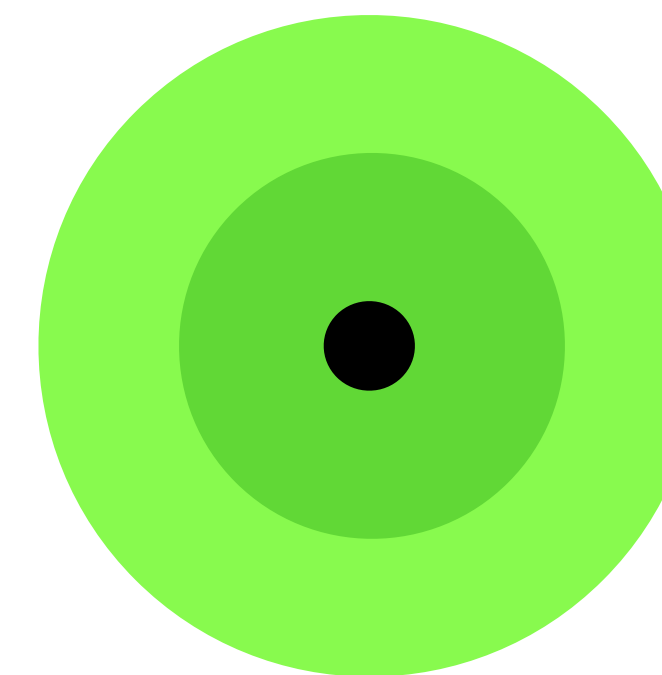
\parallel

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



OTHER STUFF

distance-based, ...

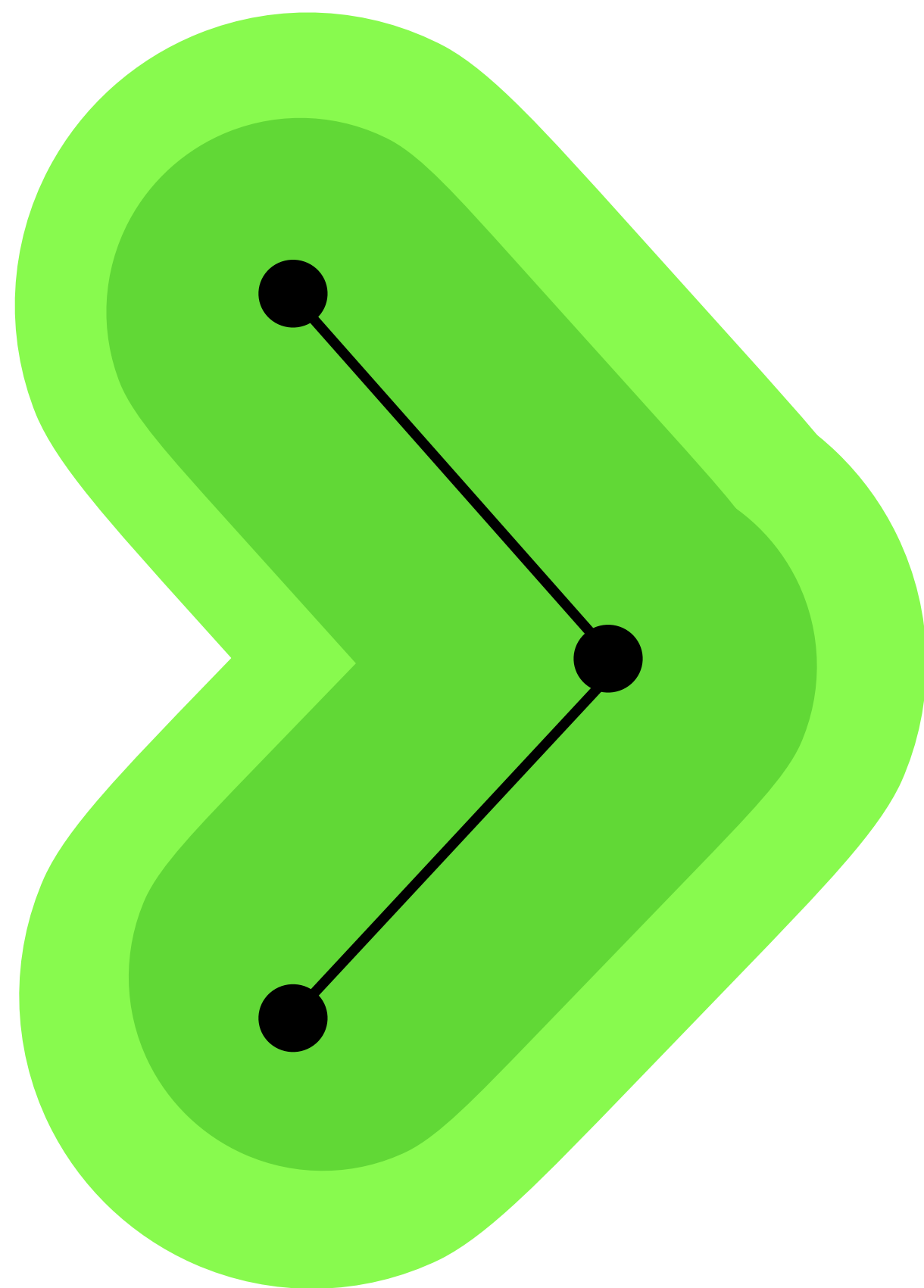


\mathcal{P}_δ

\parallel

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

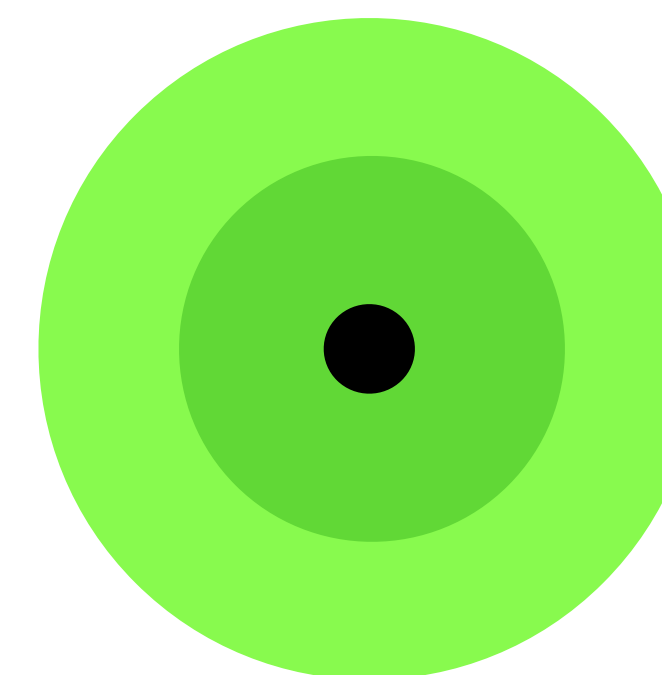
GLOBAL



+

OTHER STUFF

distance-based, ...



\mathcal{P}_δ

||

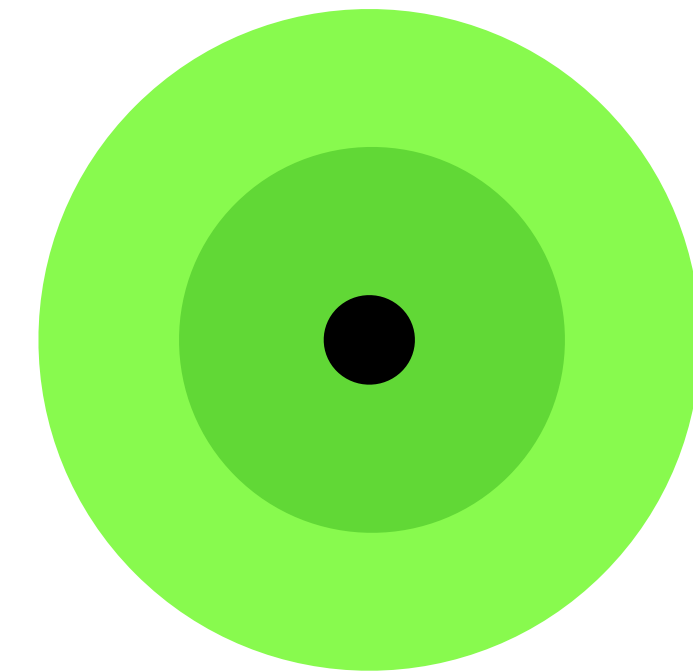
$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

GLOBAL

$$d_{\text{ratio}}(P_1, P_2) = \log \max \left\{ \sup_A \frac{P_1(A)}{P_2(A)}, \sup_A \frac{P_2(A)}{P_1(A)} \right\}$$

OTHER STUFF

distance-based, ...

 \mathcal{P}_δ \parallel

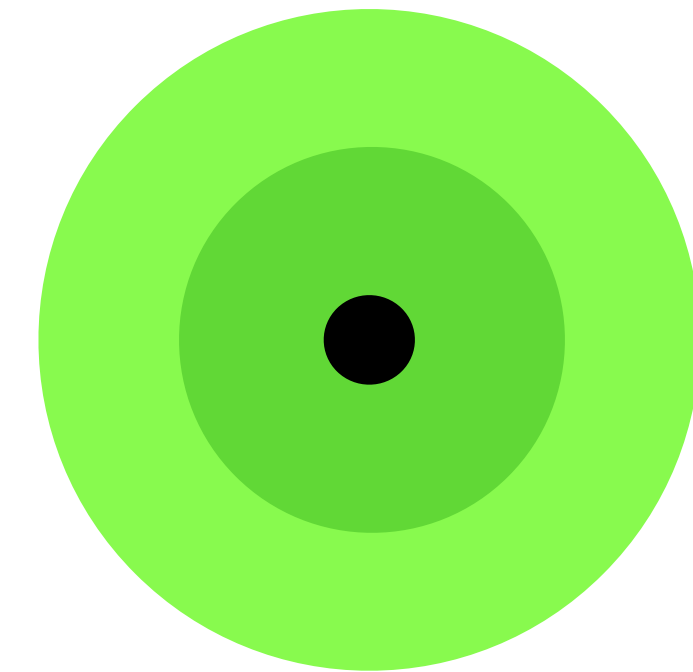
$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

GLOBAL

$$d_{\text{ratio}}(P_1, P_2) = \text{ess sup}_{(x,y) \in \Omega} \left| \log \left(\frac{p_1(x,y)}{p_2(x,y)} \right) \right|$$

OTHER STUFF

distance-based, ...

 \mathcal{P}_δ \parallel

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

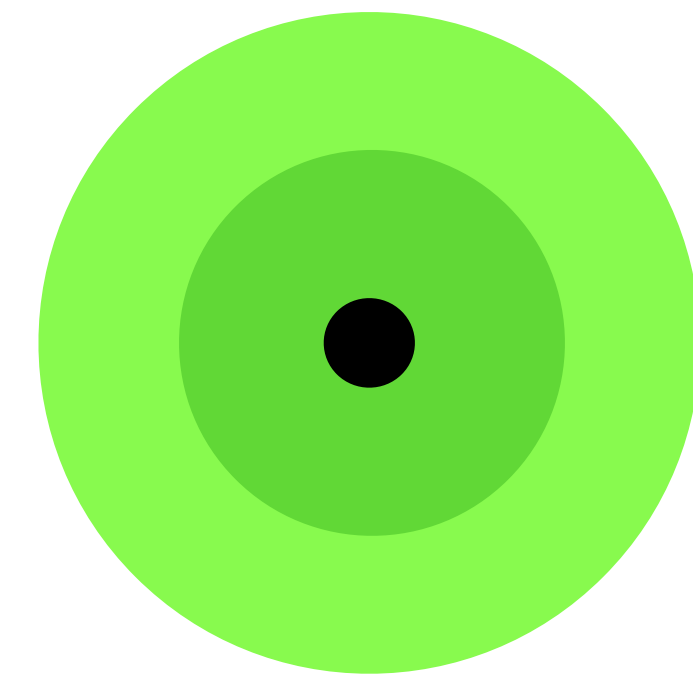
GLOBAL

$$d_{\text{ratio}}(P_1, P_2) = \text{ess sup}_{(x,y) \in \Omega} \left| \log \left(\frac{p_1(x, y)}{p_2(x, y)} \right) \right|$$

$$d_{\text{diff}}(P_1, P_2) = \text{ess sup}_{(x,y) \in \Omega} |p_1(x, y) - p_2(x, y)|$$

OTHER STUFF

distance-based, ...



\mathcal{P}_δ

||

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

GLOBAL

discrete features:

$$r_{\text{ratio}} = \log \min \left\{ \frac{1}{1 - \Delta}, \sqrt{\frac{p_{\text{classif}}(x, \hat{y})}{p_{\text{classif}}(x, \hat{y}_2)}} \right\}$$

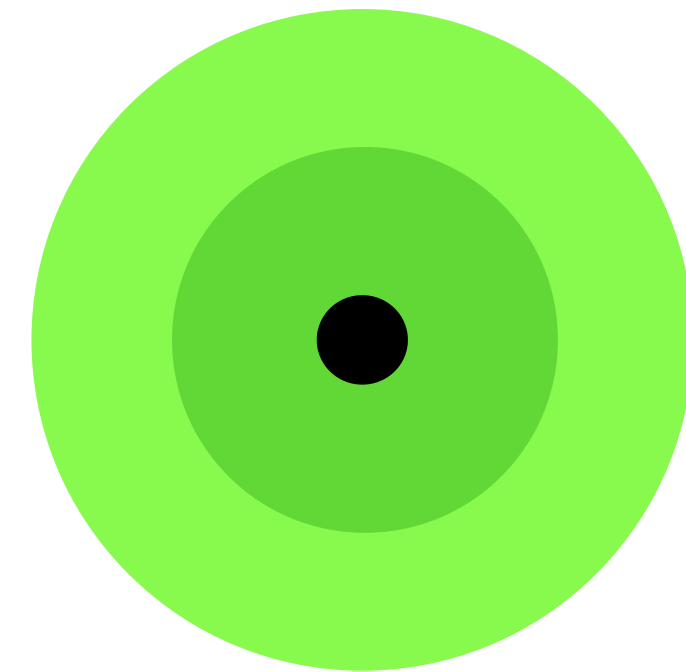
$$r_{\text{diff}} = \frac{1}{2} (p_{\text{classif}}(x, \hat{y}) - p_{\text{classif}}(x, \hat{y}_2))$$

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

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

OTHER STUFF

distance-based, ...


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

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

GLOBAL

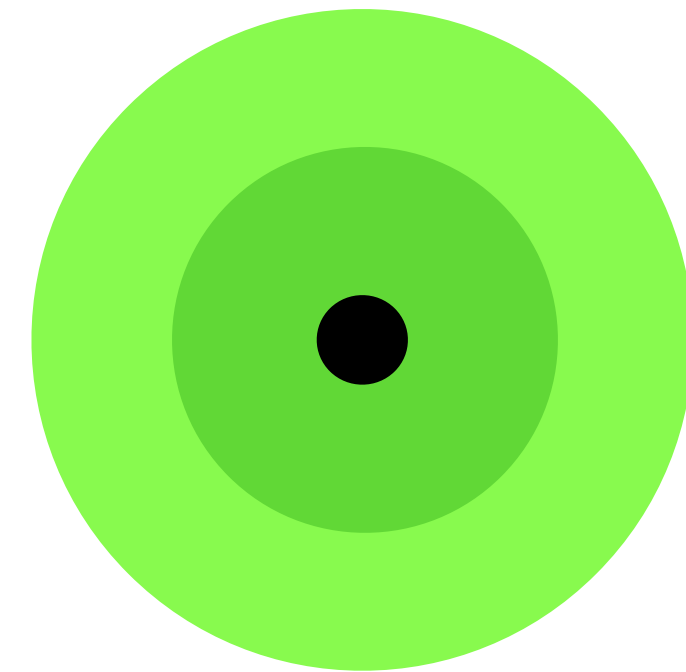
at least one continuous feature:

$$r_{\text{ratio}} = \log \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}}$$
$$r_{\text{diff}} = \frac{1}{2} (P_{\text{classif}}(x, \hat{y}) - P_{\text{classif}}(x, \hat{y}_2))$$

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

OTHER STUFF

distance-based, ...

 \mathcal{P}_δ \parallel

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

ROBUSTNESS QUANTIFICATION

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

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 from data. Hence, their results are prone to be unreliable and imprecise. In this paper, we propose a novel extension of credal sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks. We propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks. We propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks.

1. Introduction

Probabilistic models are usually built so that they can capture uncertain knowledge through a graphical language that represents variables as nodes and dependencies 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, it is tractable in popular approximate inference algorithms based on passing messages along the edges of the graph topology [32,64,62]. In this paper, we propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks.

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

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 dependencies 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, it is tractable in popular approximate inference algorithms based on passing messages along the edges of the graph topology [32,64,62]. In this paper, we propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks.

Robustifying sum-product networks

Denis Deratani Mauá^{a,*}, Diarmaid Conaty^b, Fabio Gagliardi Katja Poppenhaeger^d, Cassio Polpo de Campos^{b,e}

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

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 from data. Hence, their results are prone to be unreliable and imprecise. In this paper, we propose a novel extension of credal sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks. We propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks.

1 Introduction

Sum-Product Networks (SPNs) [15] (conceptually similar to Circuits [4]) are a class of deep probabilistic graphical models with 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 of machine learning power has motivated several applications of SPNs to a variety of 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 robustness 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 learning model.

Towards Scalable and Robust Sum-Product Networks

Alvaro H. C. Correia and Cassio P. de Campos^(✉)
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

Towards Robust Classification with Deep Generative Forests

Alvaro H. C. Correia¹ Robert Peharz¹ Cassio de Campos¹

Abstract

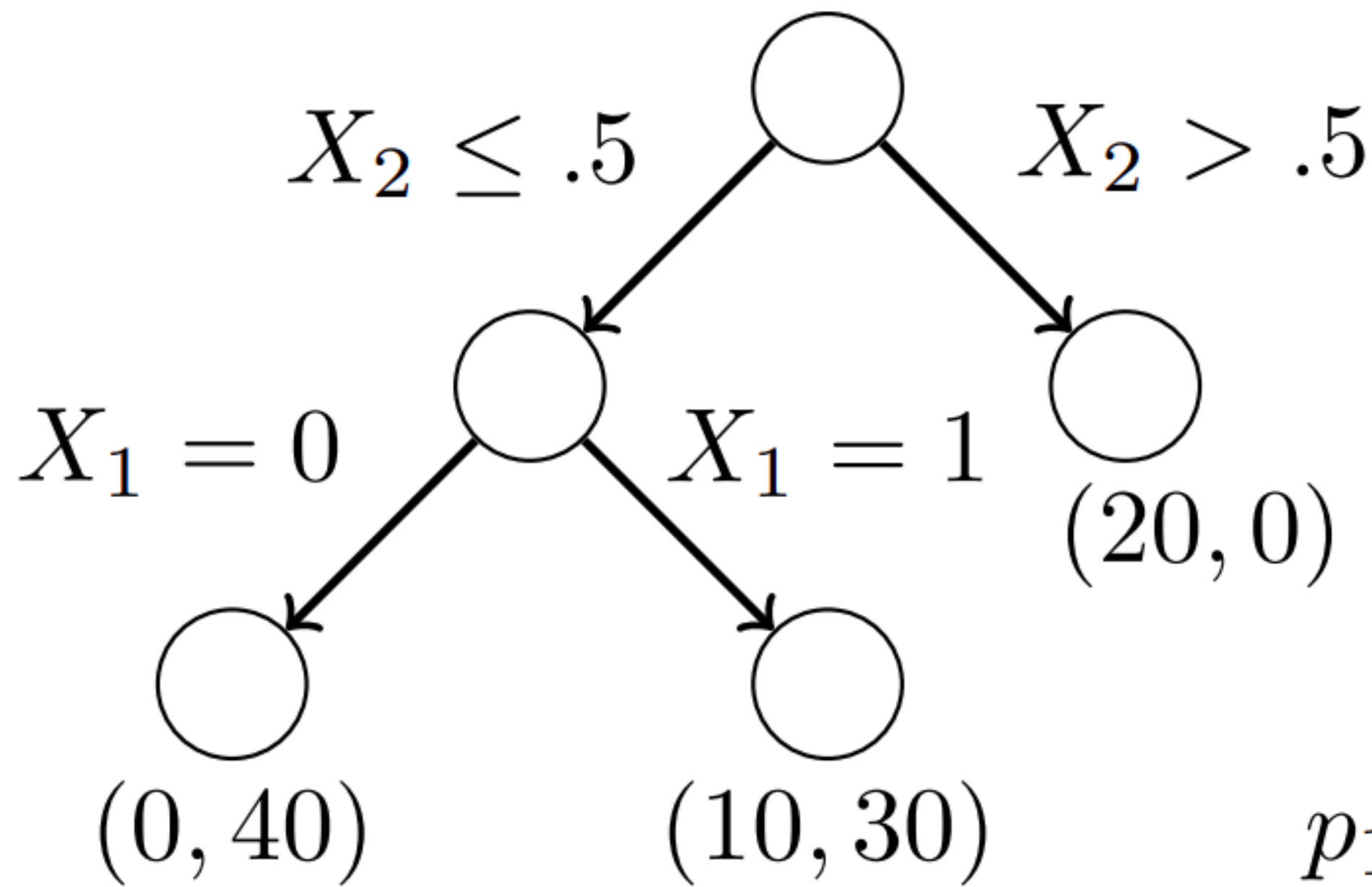
Decision Trees and Random Forests are among the most widely used machine learning models, and often achieve state-of-the-art performance in tabular, domain-agnostic datasets. Nonetheless, they are not robust to adversarial perturbations. In this paper, we propose a novel extension of sum-product networks, an imprecise extension of sum-product networks, that allows for common inference tasks and complexity results for common inference tasks.

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 .

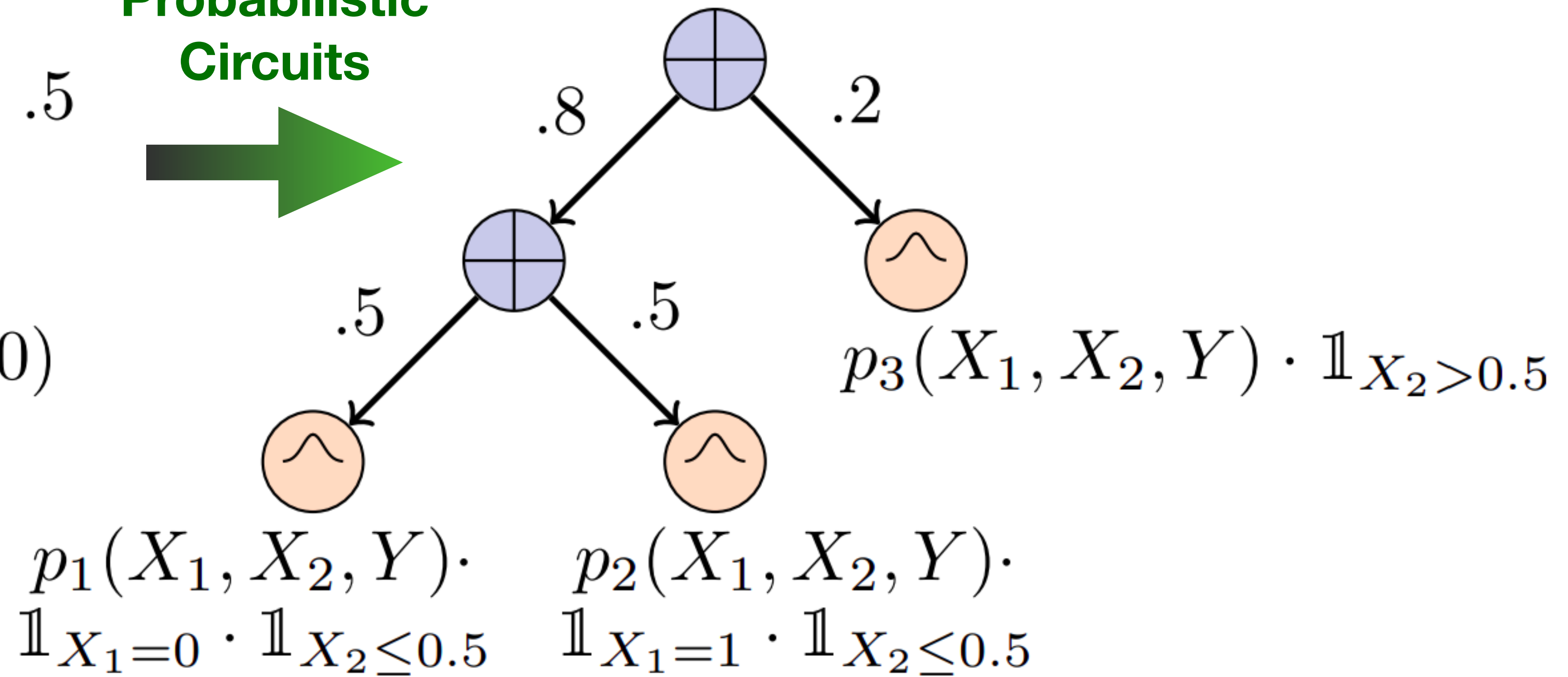
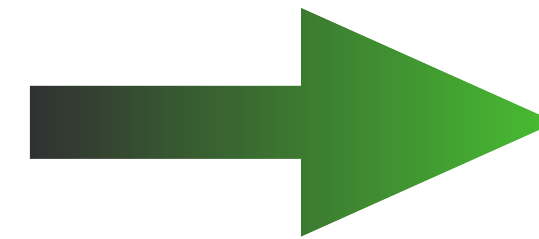
2020

Decision Tree (DT)



Generative DT

Probabilistic
Circuits



LOCAL

continuous features

$r_{\epsilon, \text{GeF}}$ = complicated

ϵ -CONTAMINATION

[5]

GeF+

Towards Robust Classification with Deep Generative Forests

Alvaro H. C. Correia¹ Robert Peharz¹ Cassio de Campos¹

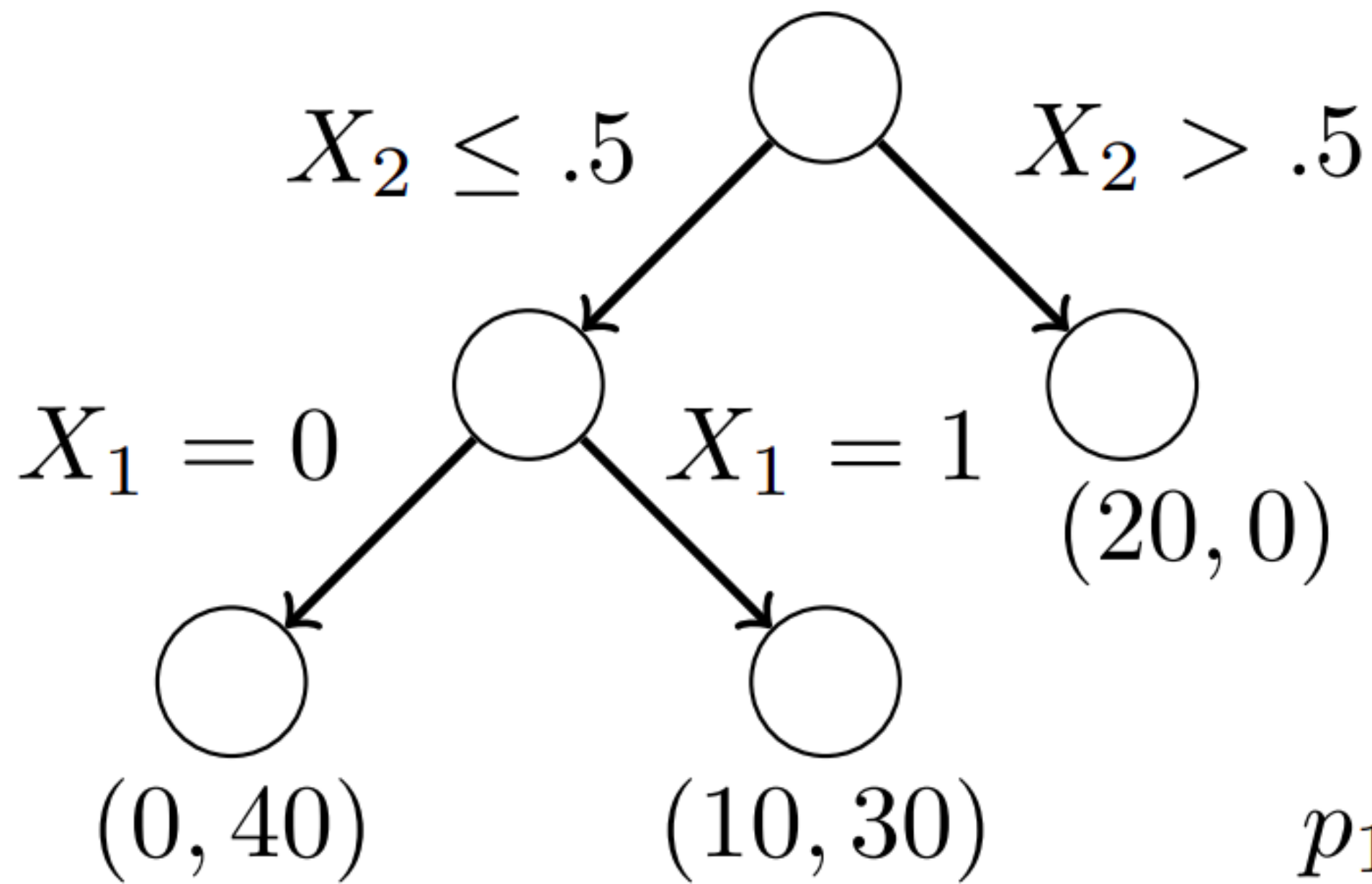
Abstract

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,

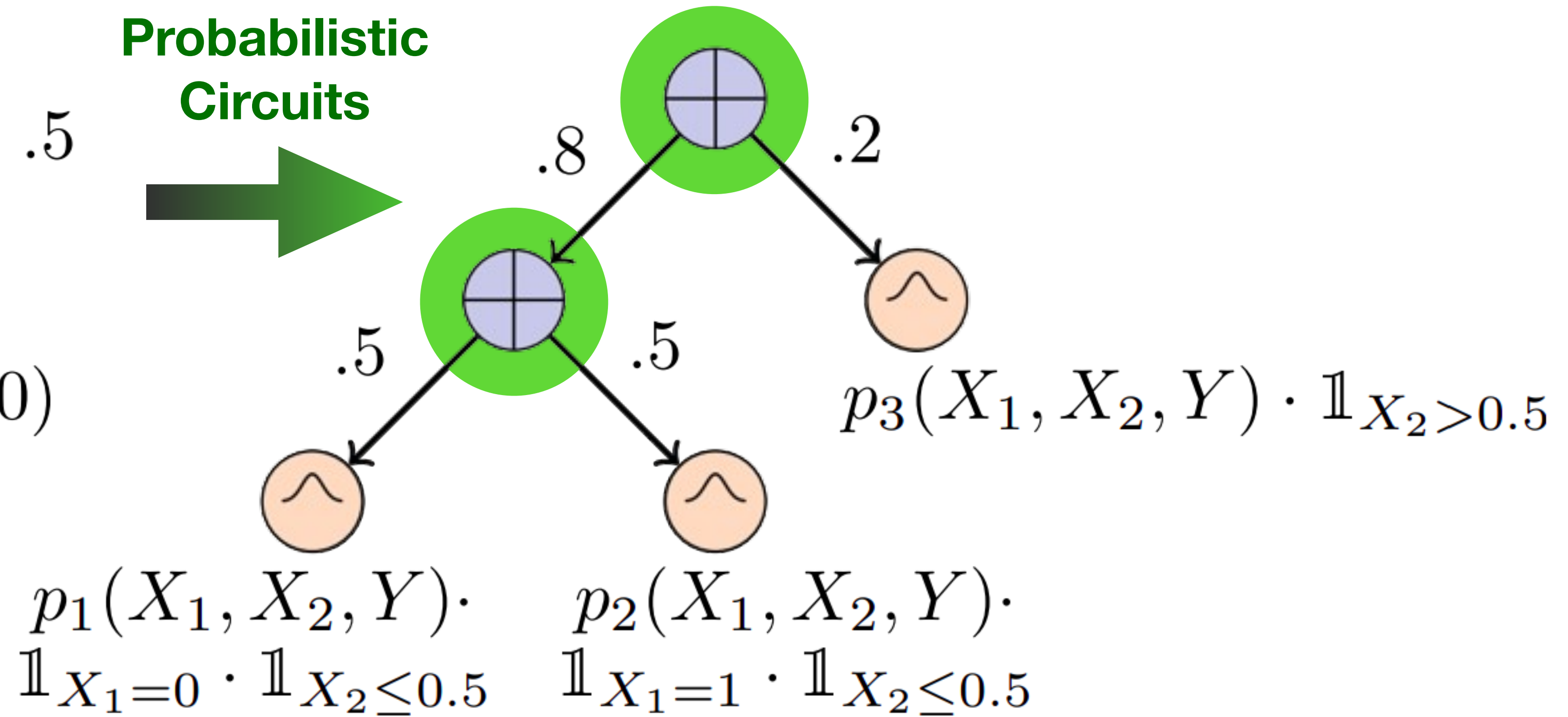
2. Generative Forests

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

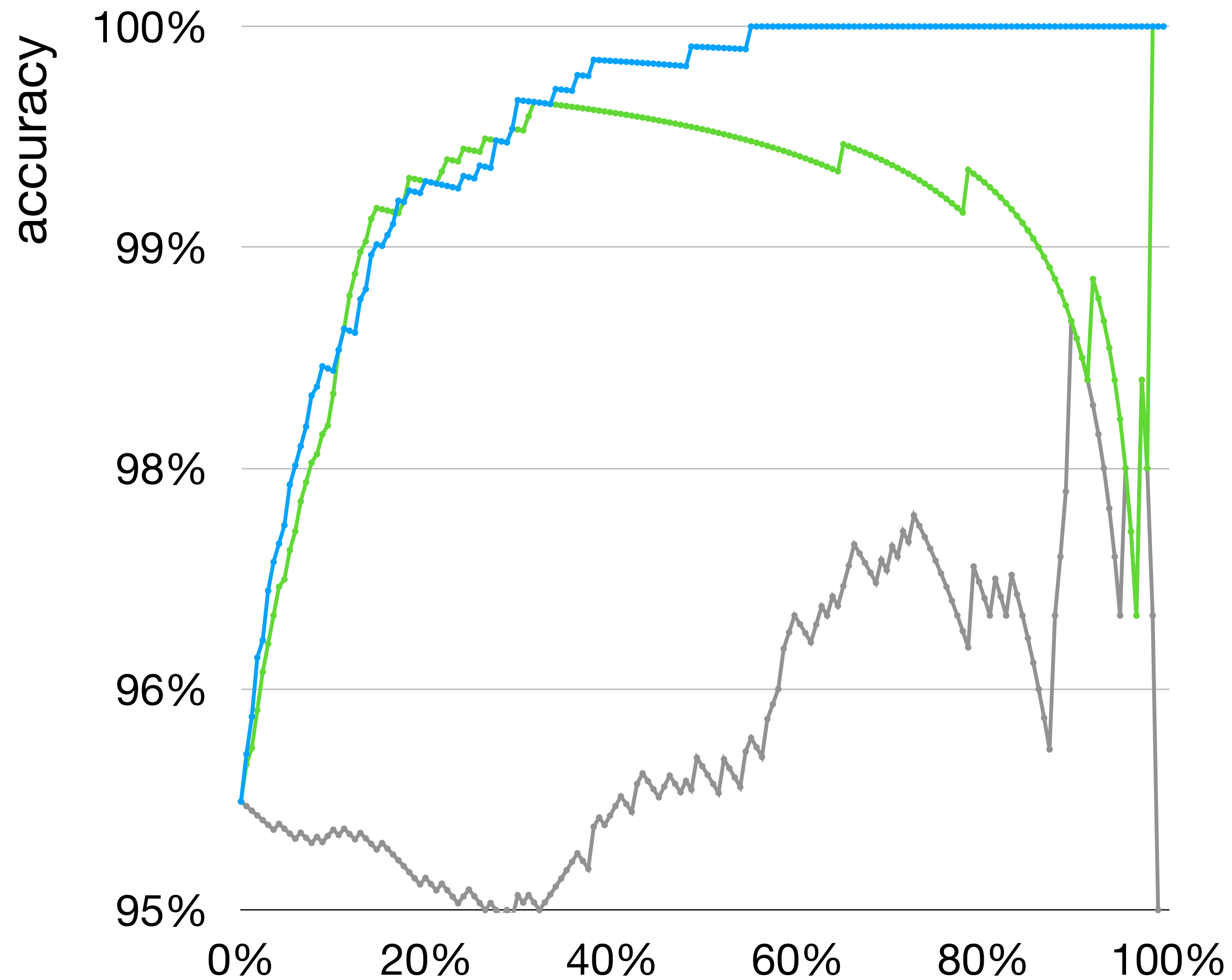
Decision Tree (DT)



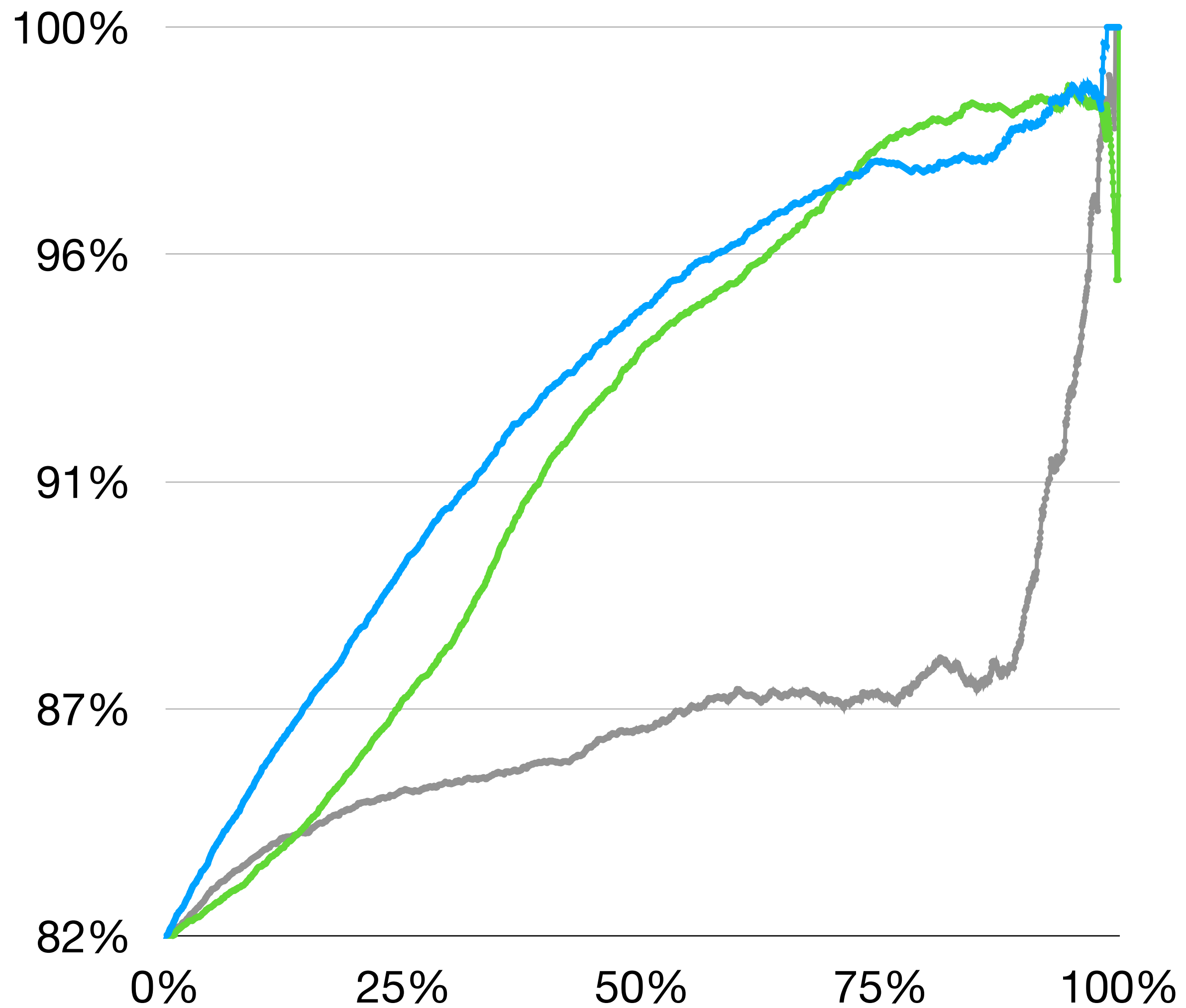
Generative DT



Cancer



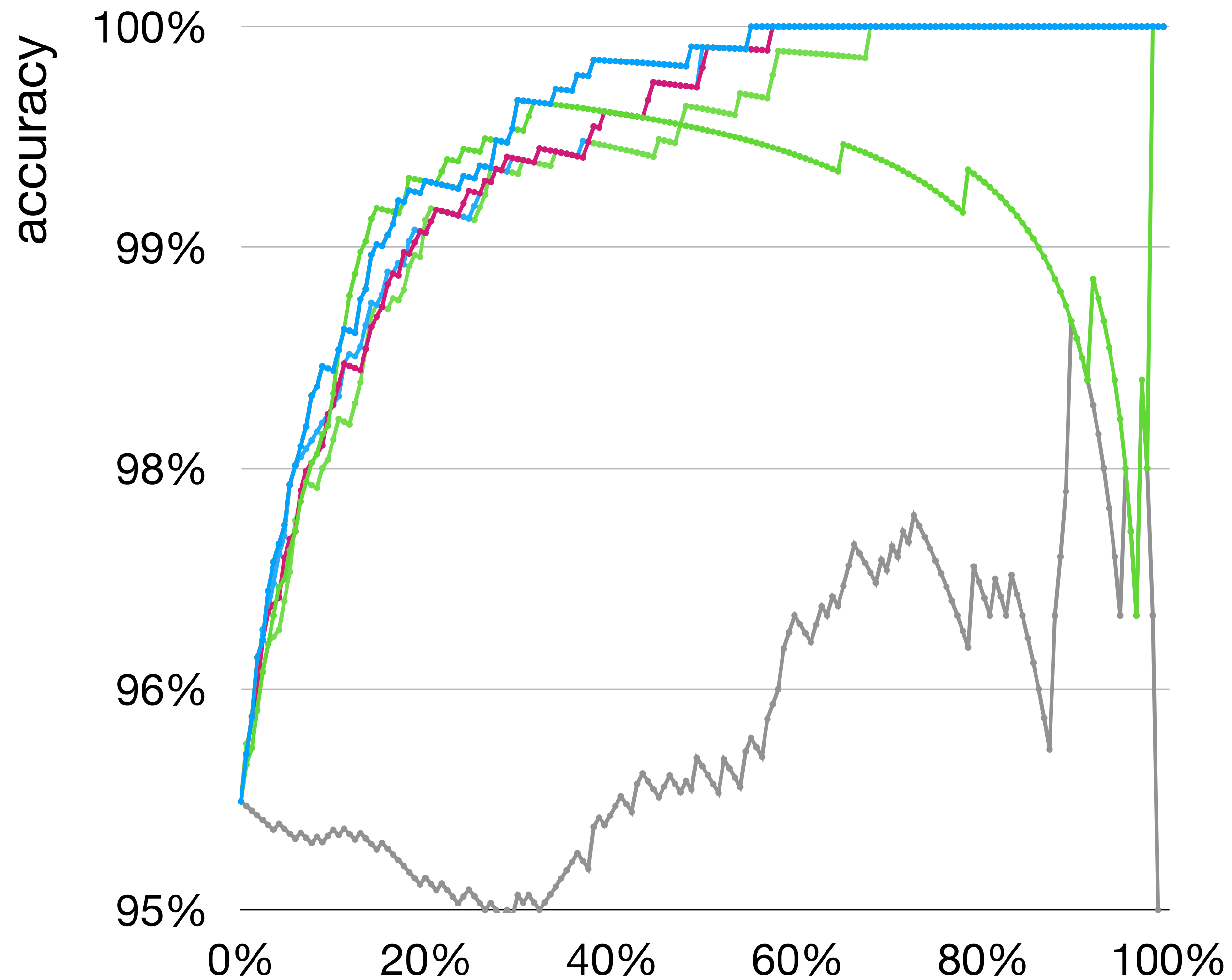
Wine



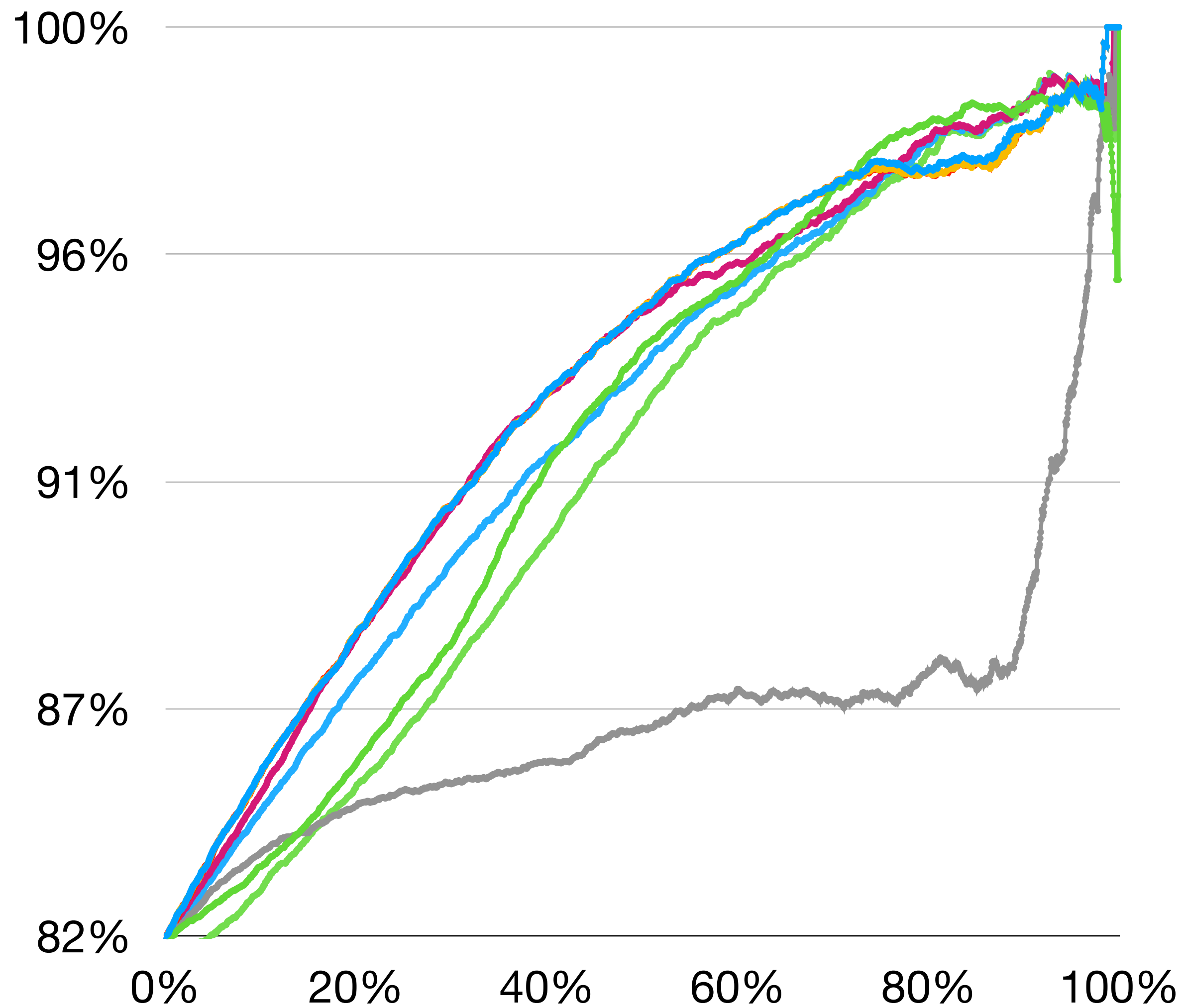
● r_{ratio} ● $r_{\epsilon, GeF}$ ● r_{diff}

% of rejected samples

Cancer



Wine



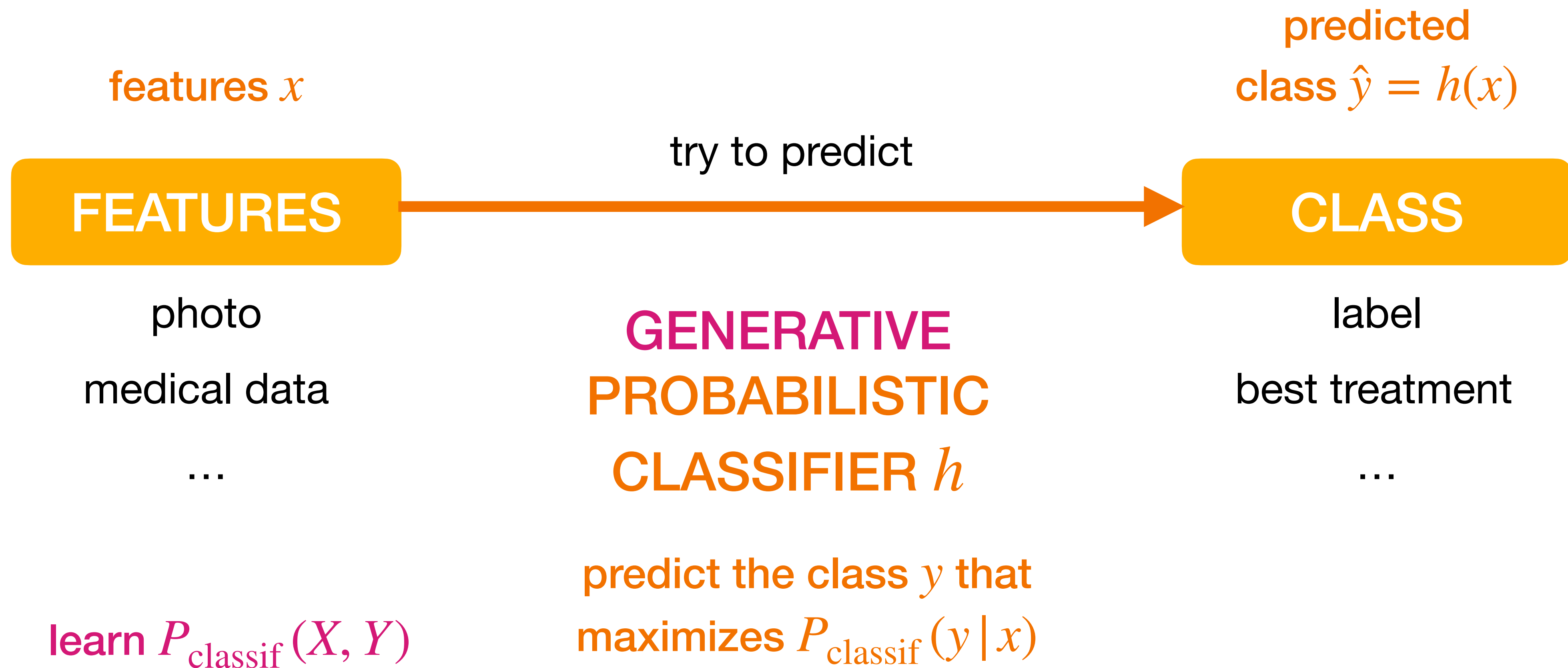
- r_{ratio}
- u_{H}
- $r_{\epsilon, \text{GeF}}$
- u_{a}
- r_{diff}
- u_{t}
- u_{m}
- u_{e}

% of rejected samples

ROBUSTNESS QUANTIFICATION

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



GLOBAL

at least one continuous feature:

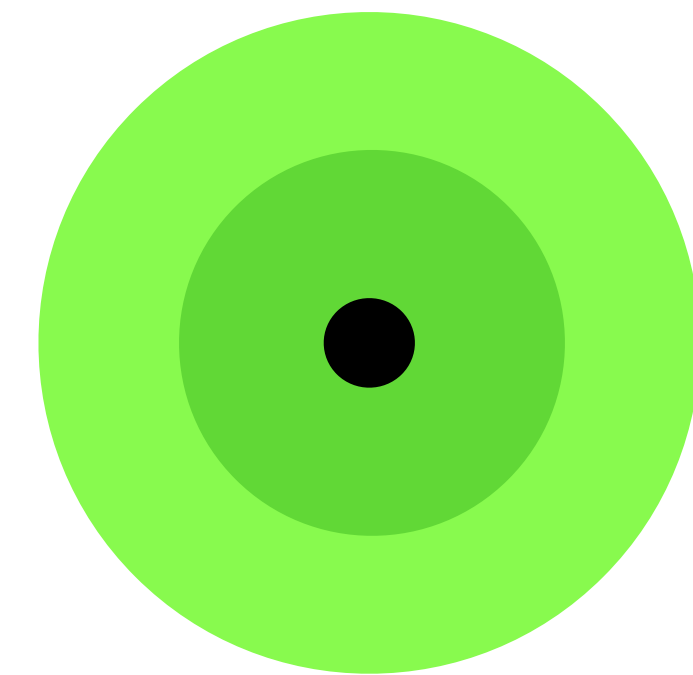
$$r_{\text{ratio}} = \log \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}}$$

~~$$r = \frac{1}{2} (P_{\text{classif}}(x, \hat{y}) - P_{\text{classif}}(x, \hat{y}_2))$$~~

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

OTHER STUFF

distance-based, ...



\mathcal{P}_δ

||

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

GLOBAL

at least one continuous feature:

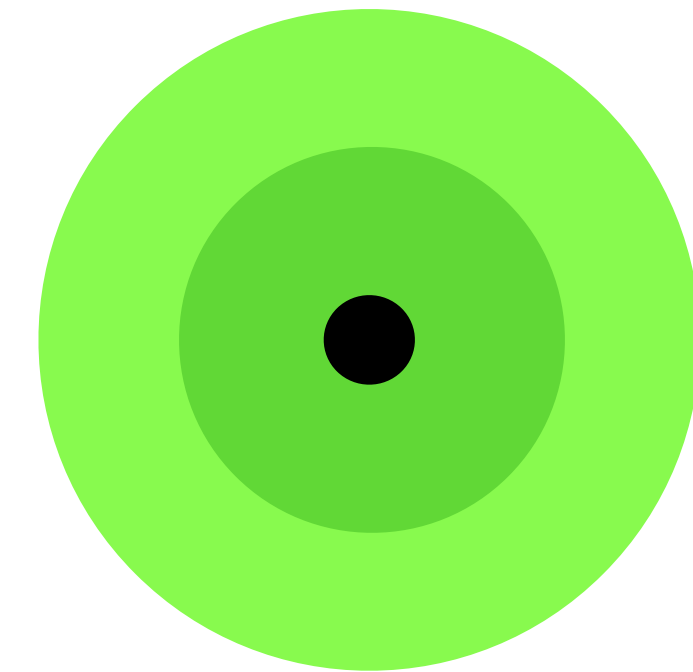
$$r_{\text{ratio}} = \log \sqrt{\frac{P_{\text{classif}}(x, \hat{y})}{P_{\text{classif}}(x, \hat{y}_2)}} = \log \sqrt{\frac{P_{\text{classif}}(\hat{y} | x)}{P_{\text{classif}}(\hat{y}_2 | x)}}$$

~~$$r = \frac{1}{2} (P_{\text{classif}}(x, \hat{y}) - P_{\text{classif}}(x, \hat{y}_2))$$~~

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

OTHER STUFF

distance-based, ...

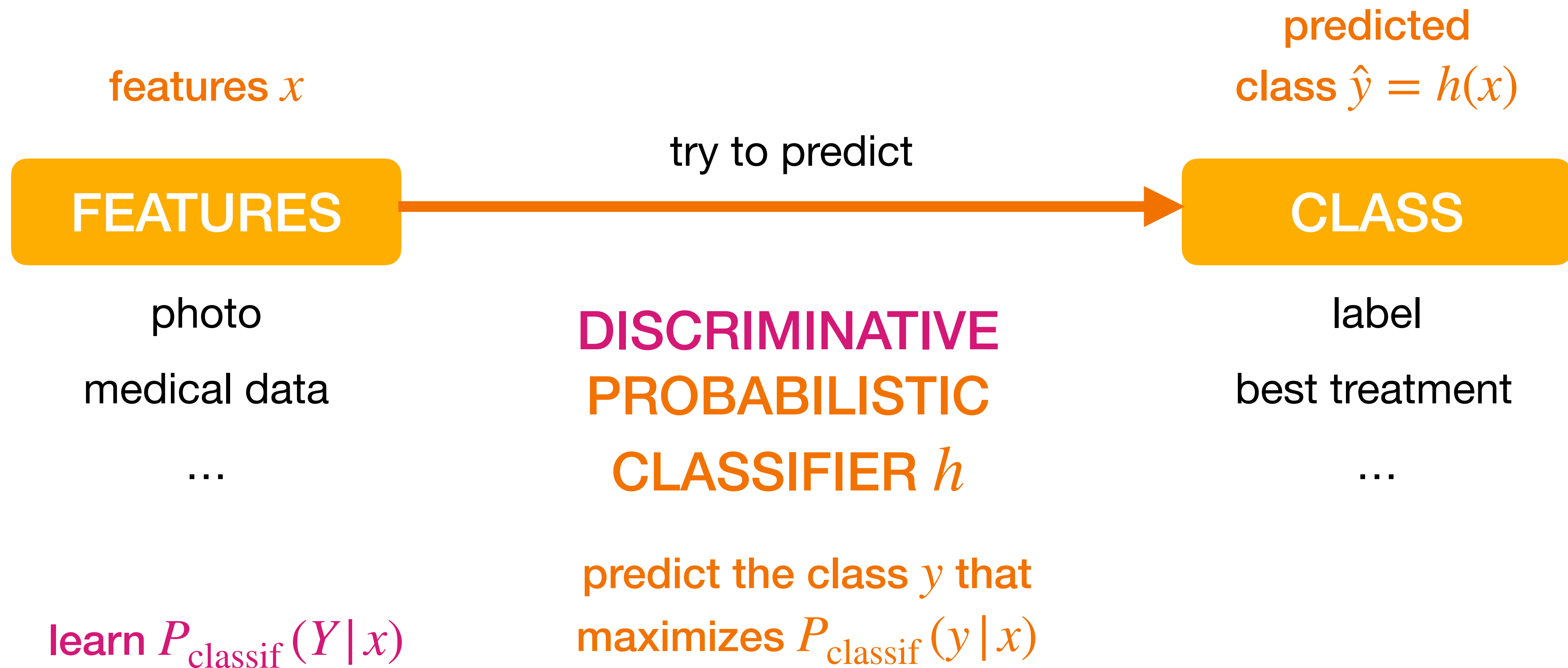


\mathcal{P}_δ

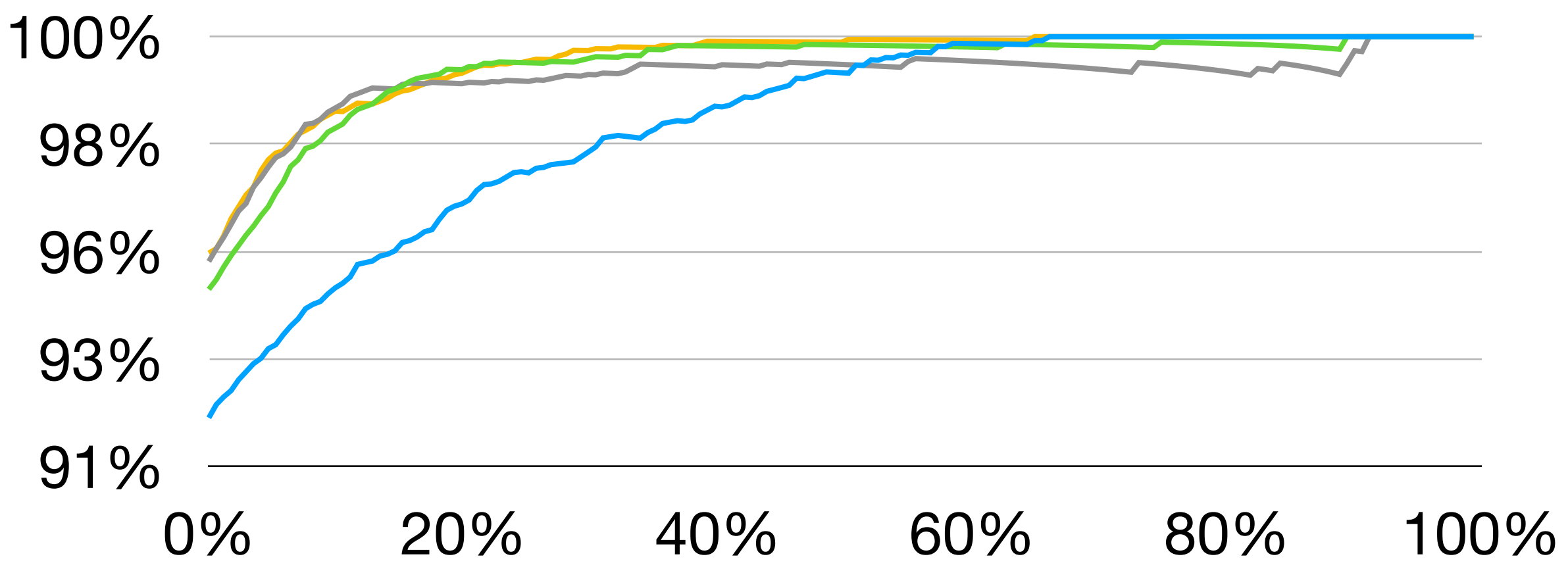
||

$$\{P \in \mathbb{P} : d(P_{\text{classif}}, P) < \delta\}$$

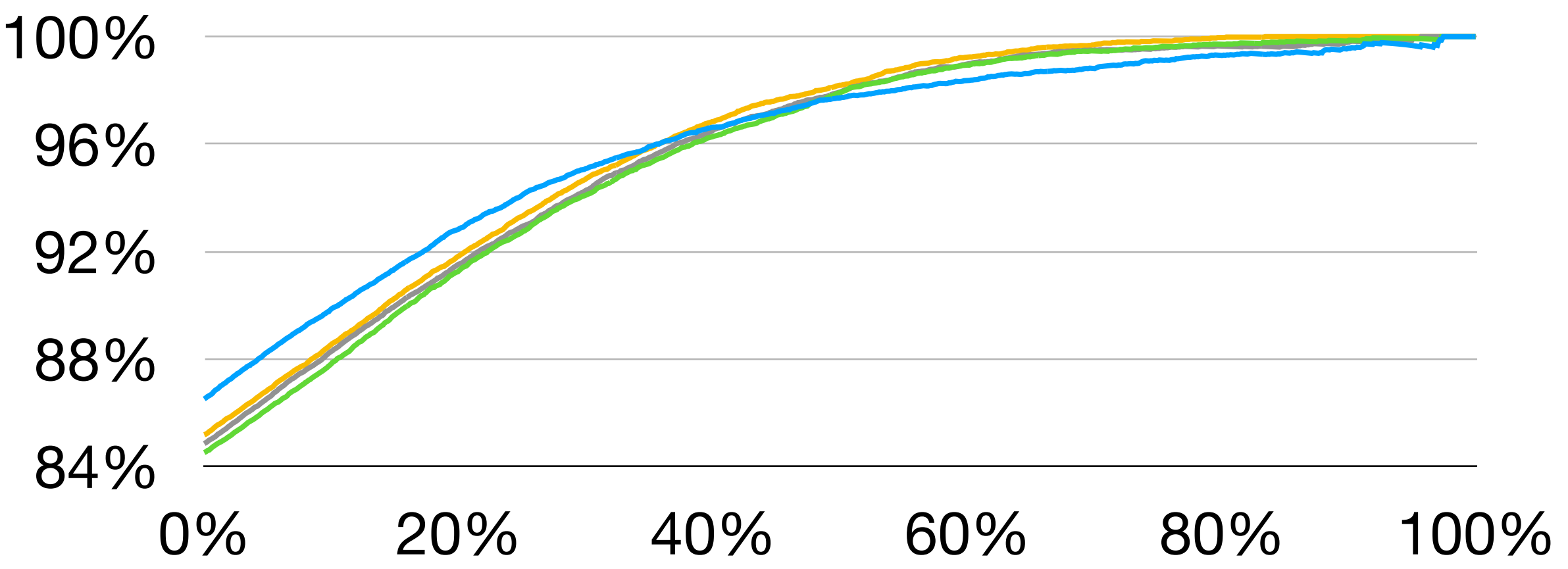
CLASSIFICATION



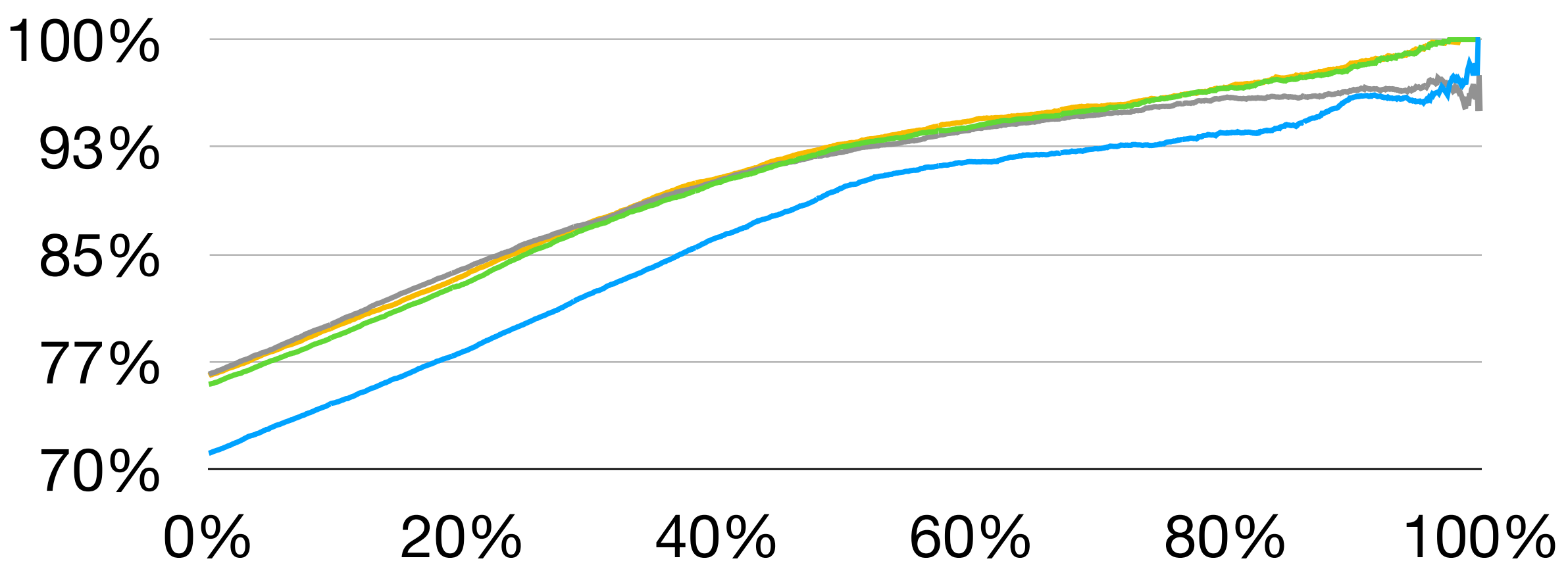
Cancer



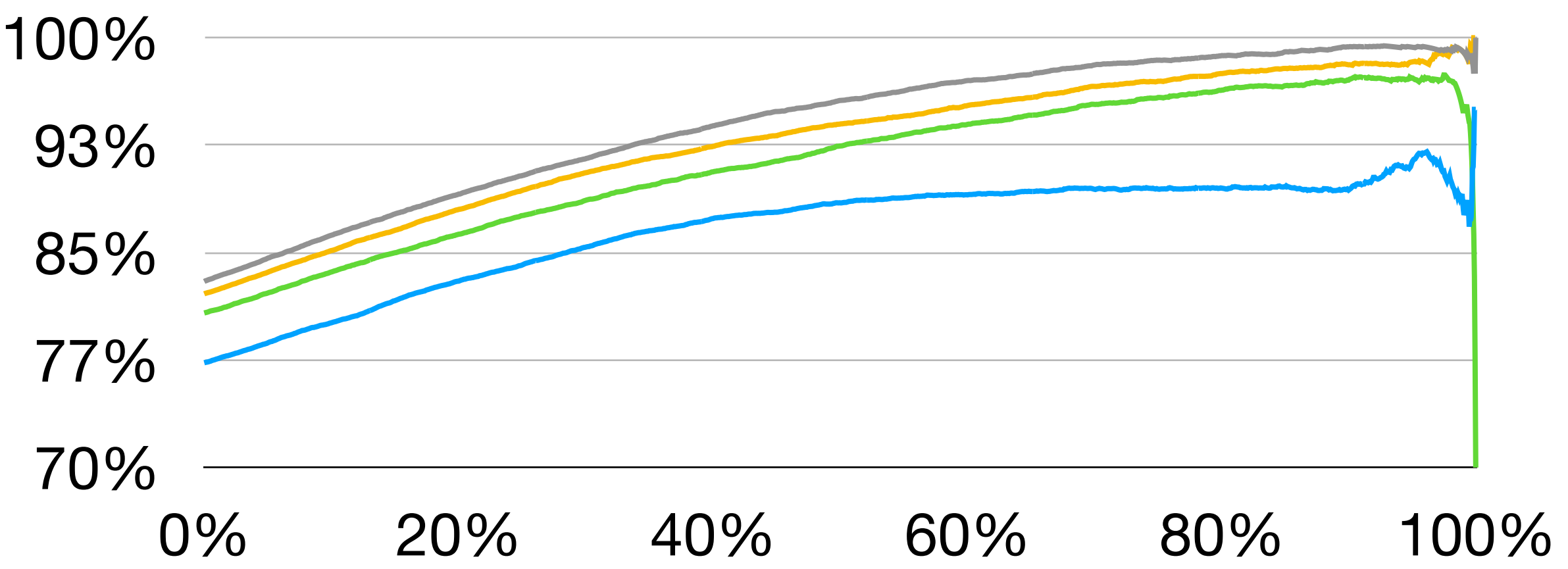
Wave



Students



Wine

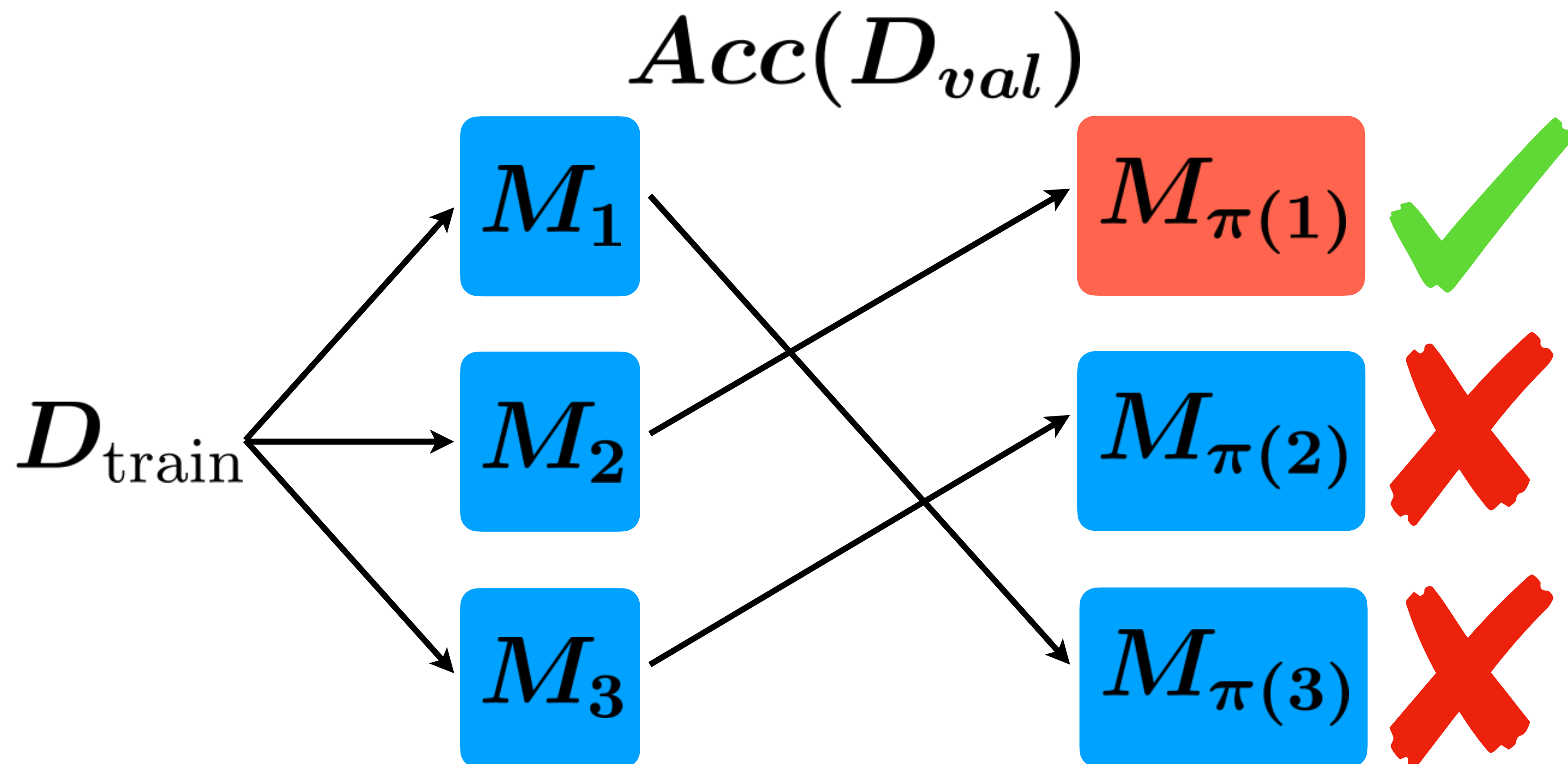


— Logistic Regression — Gradient Boosting — Random Forest — XGBoost

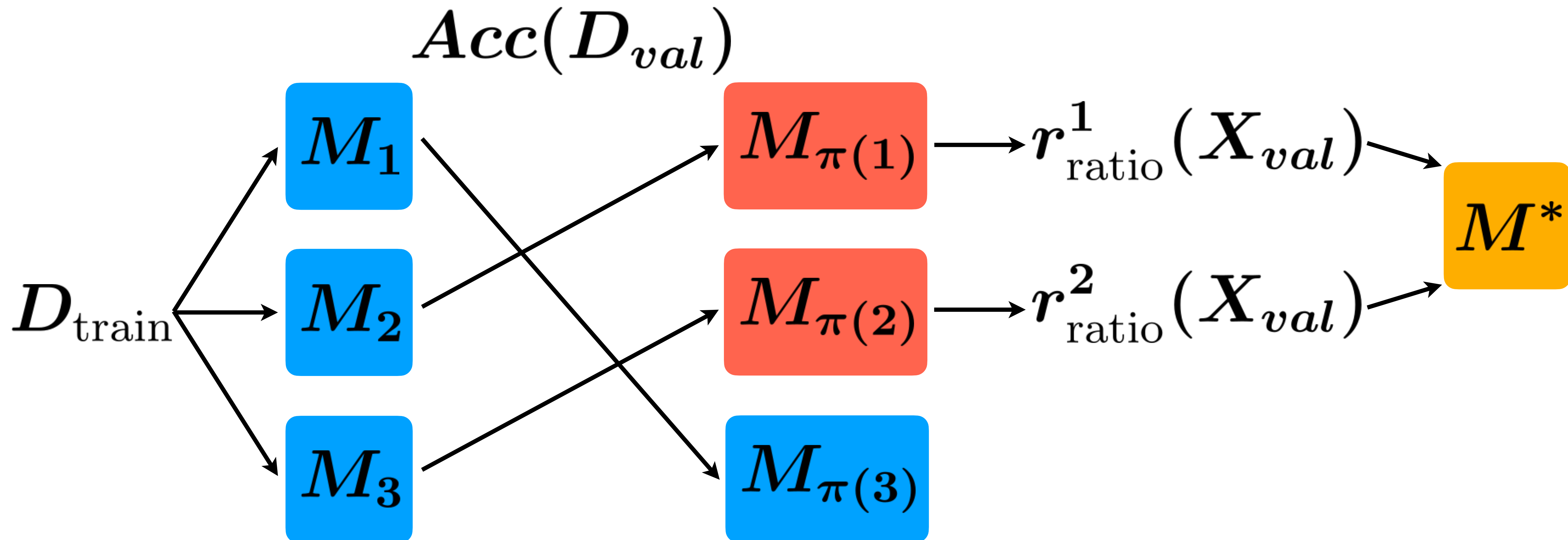
ROBUSTNESS QUANTIFICATION

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

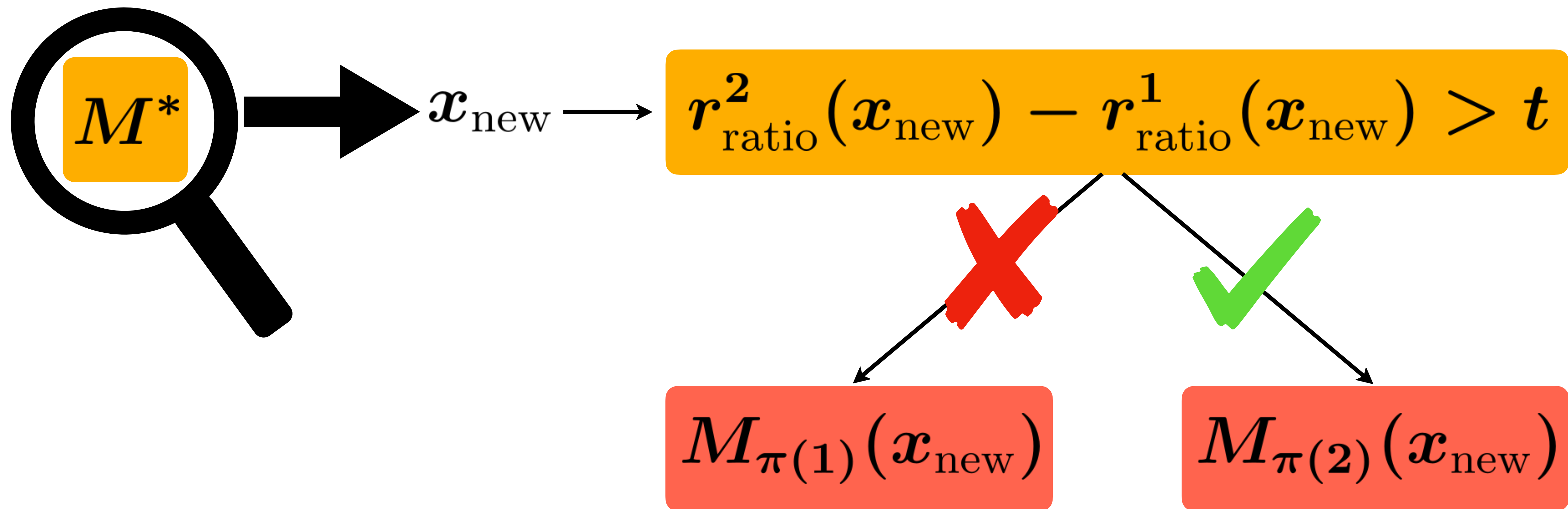
MODEL SELECTION



INSTANCE-WISE MODEL SELECTION

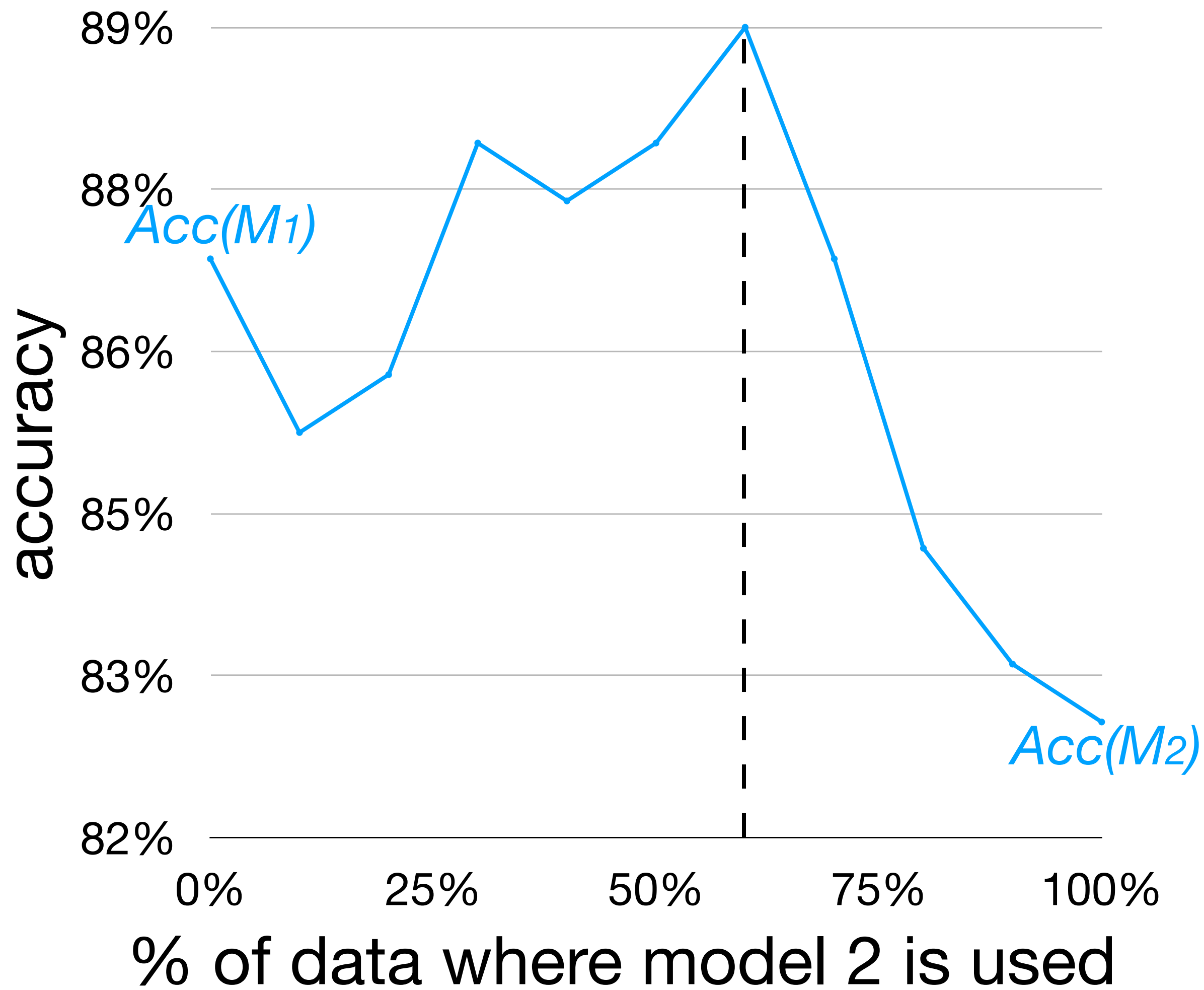


INSTANCE-WISE MODEL SELECTION

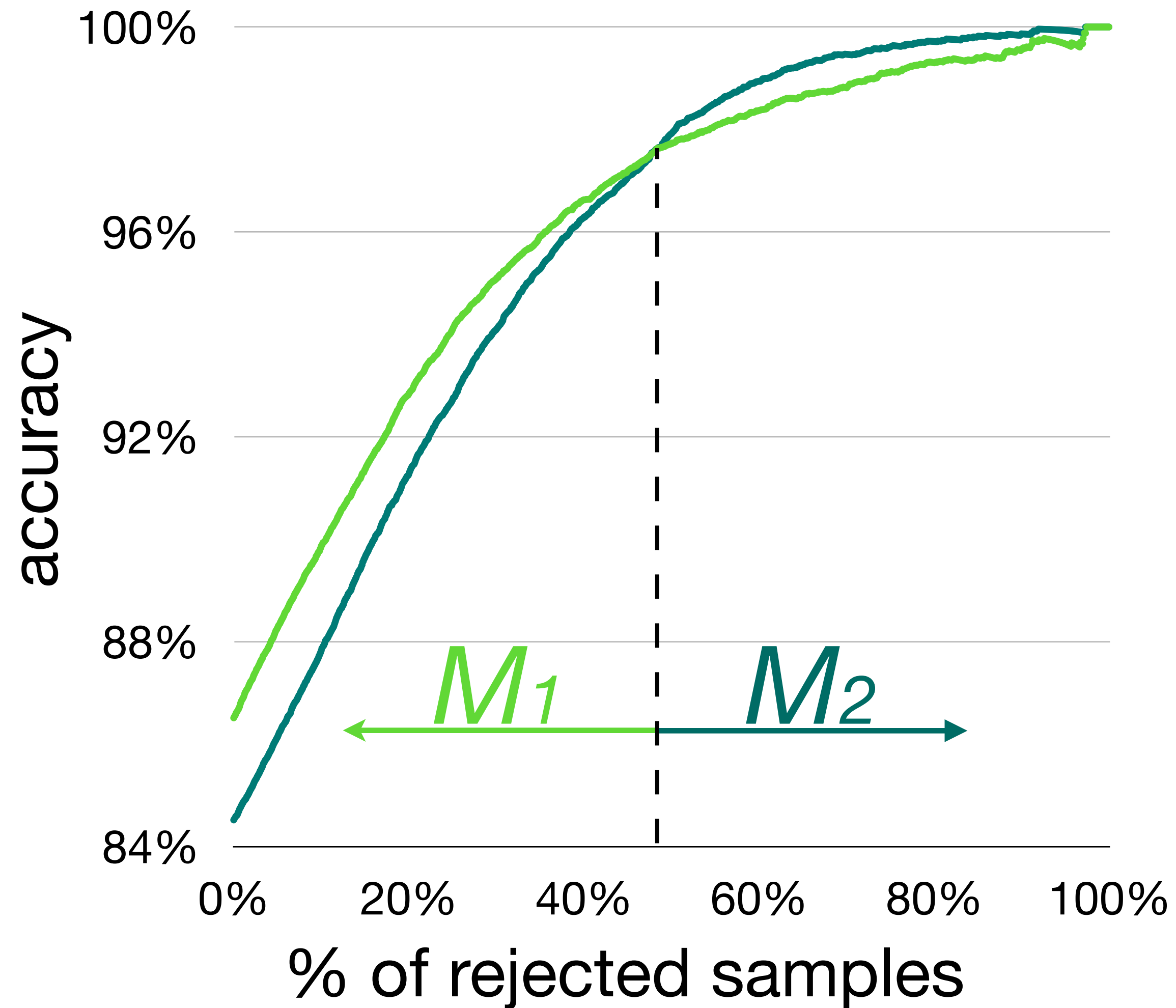


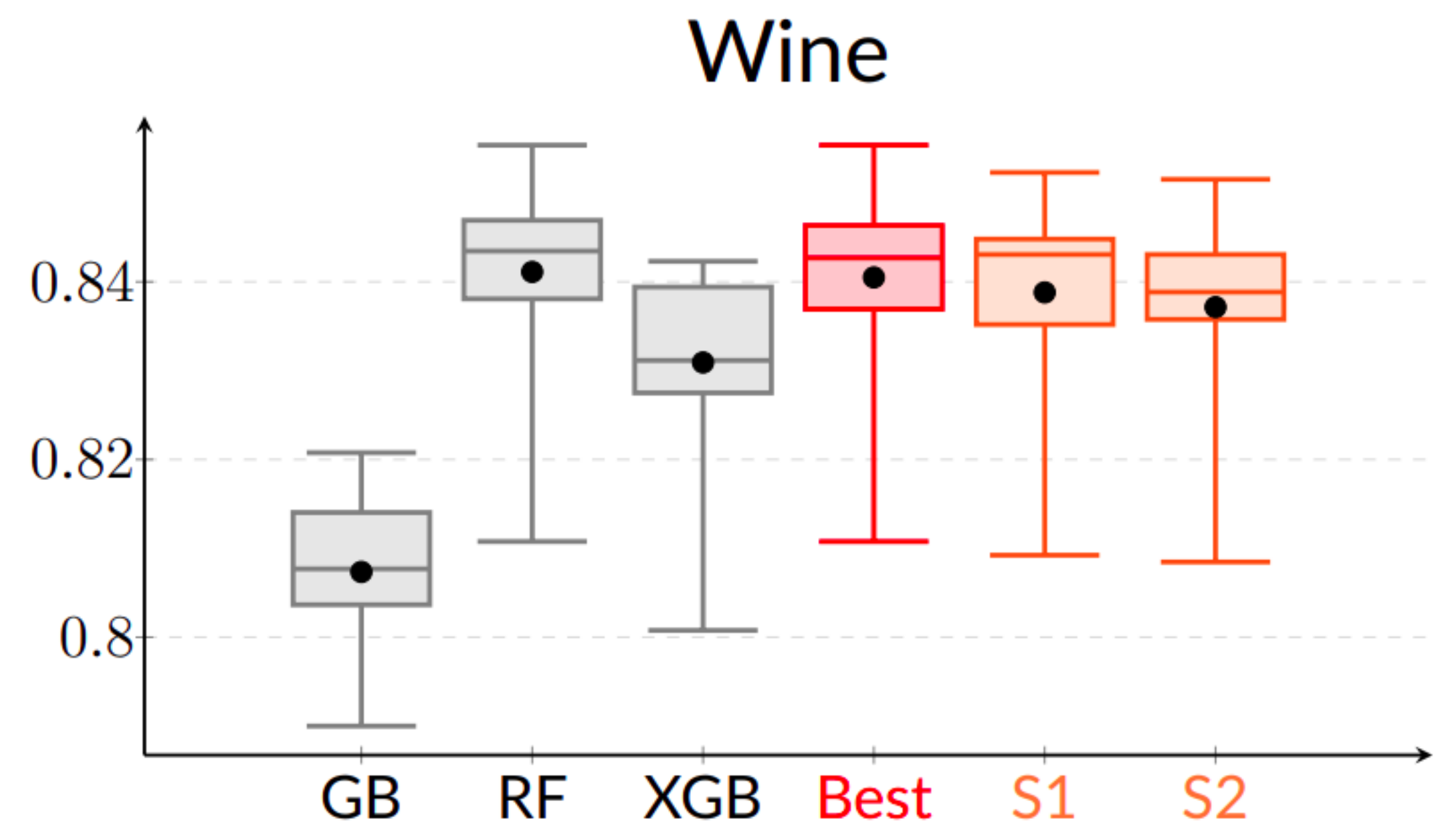
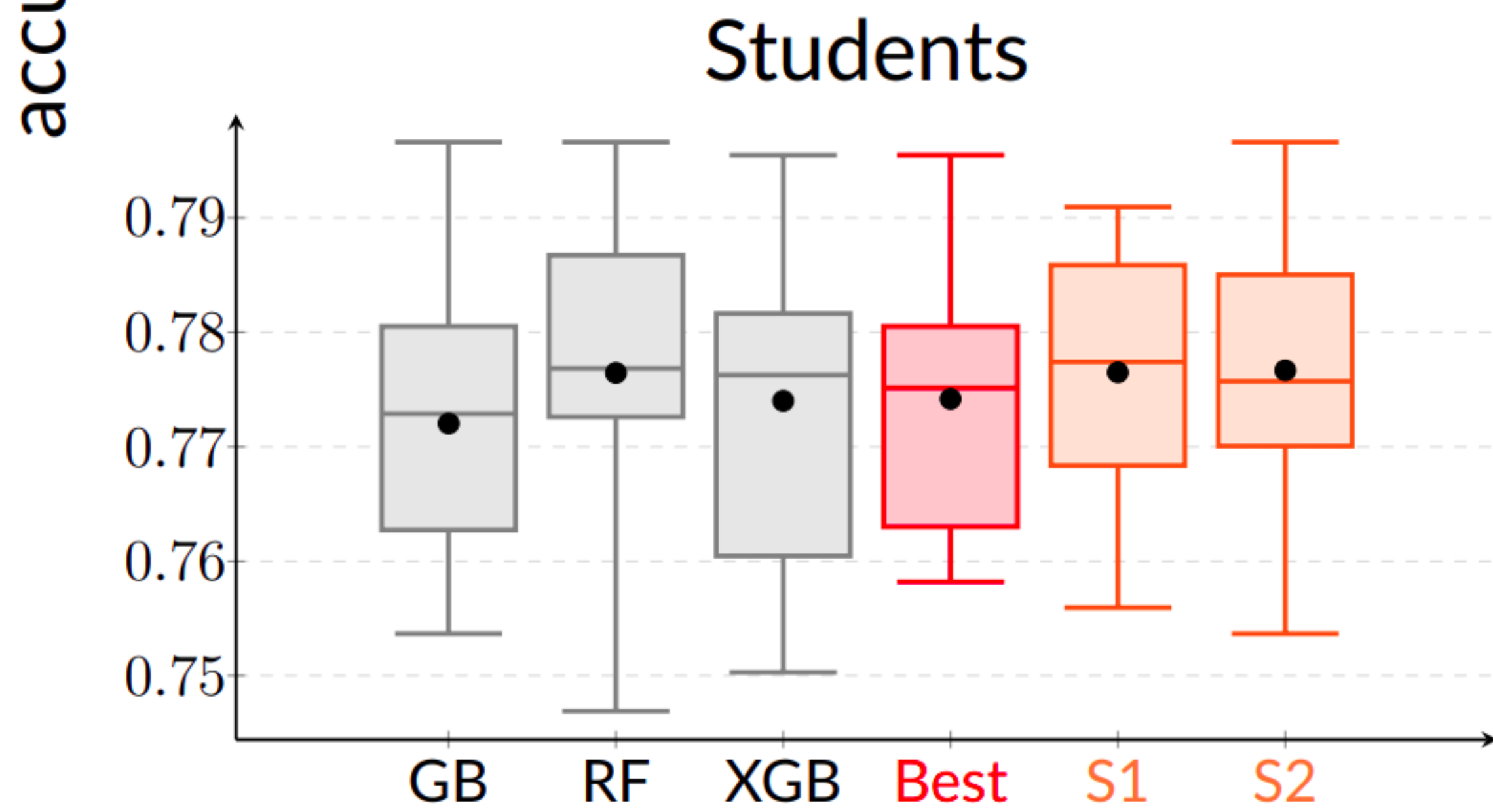
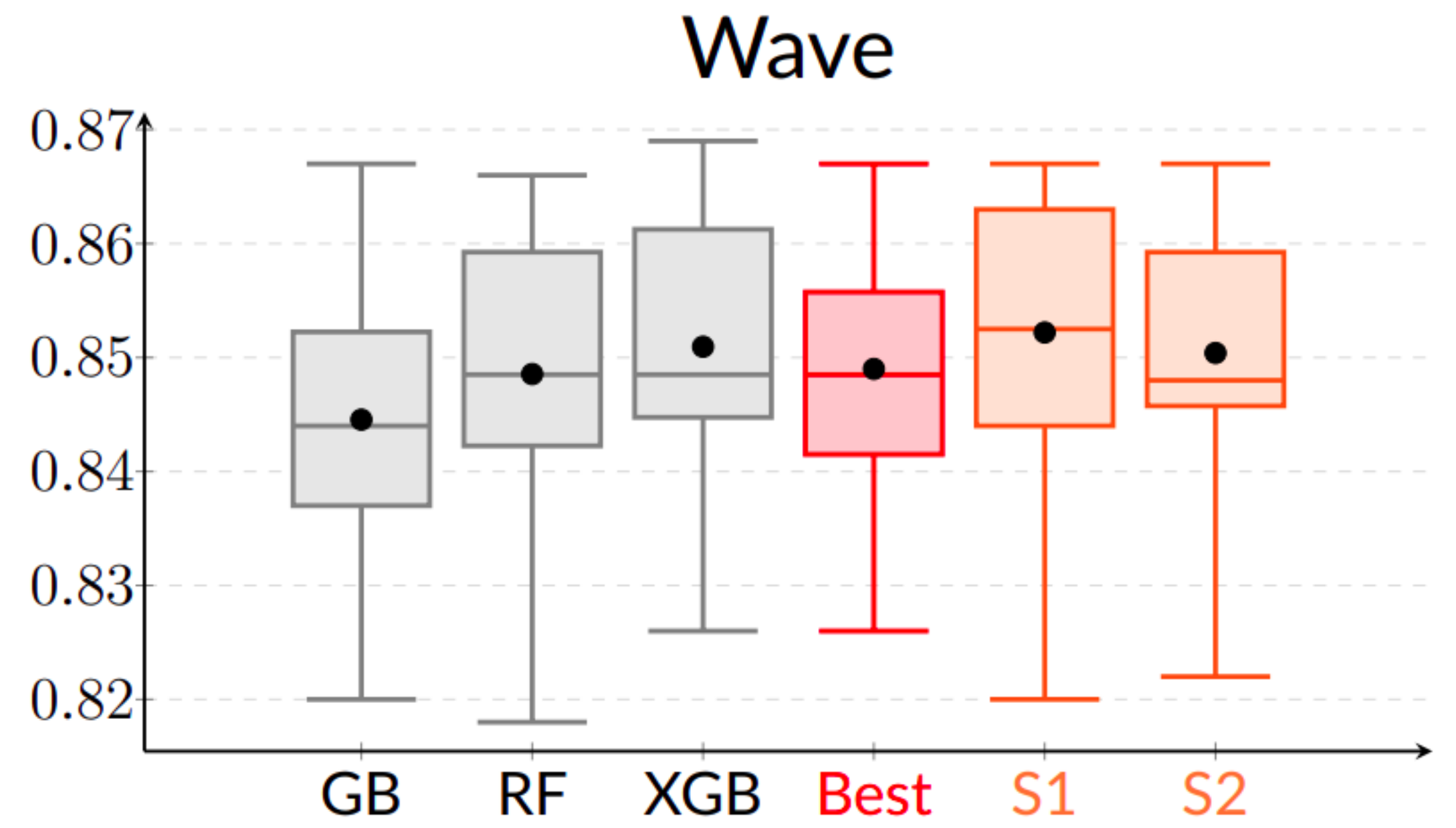
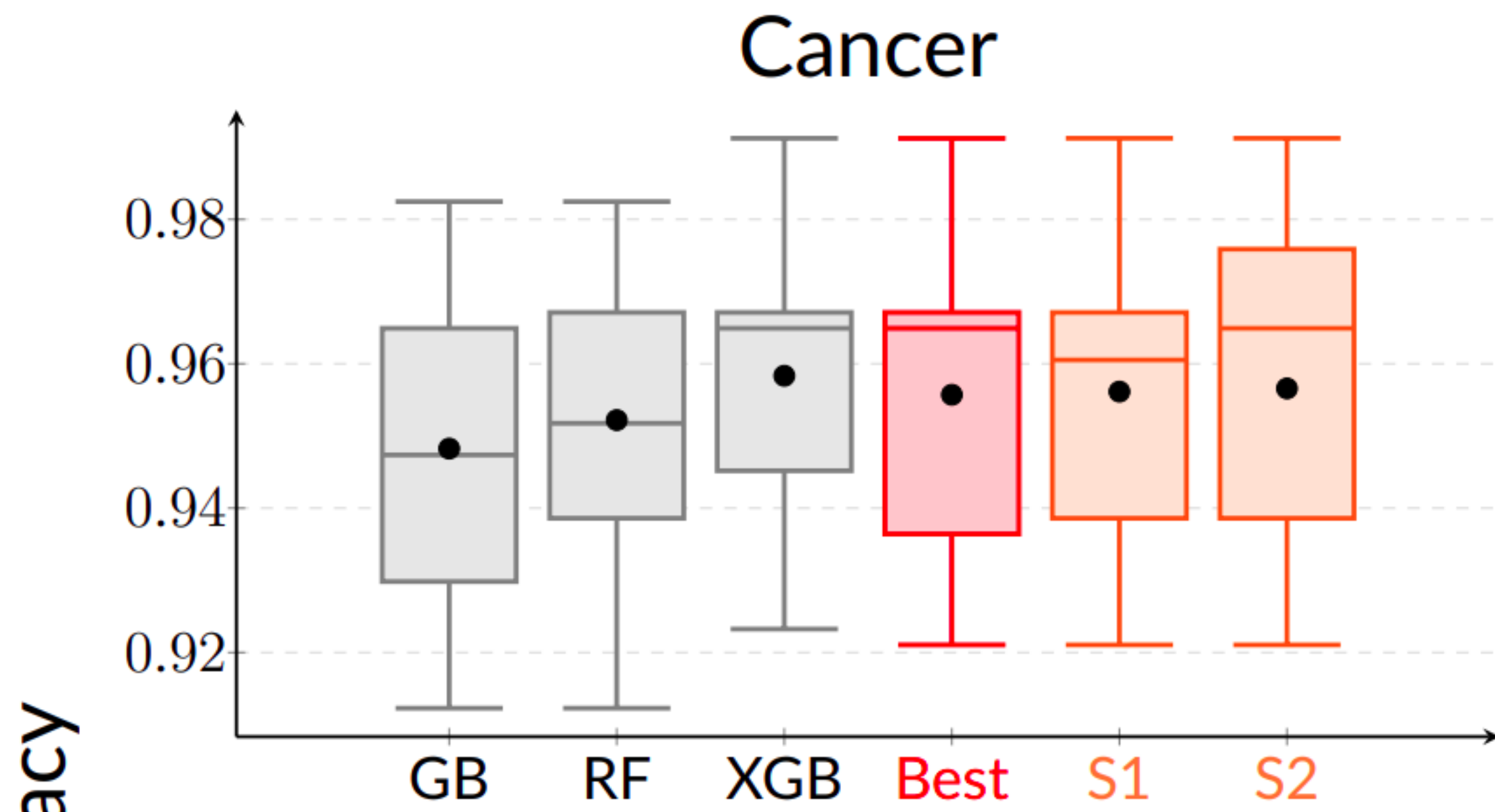
INSTANCE-WISE MODEL SELECTION

Strategy 1



Strategy 2





ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy
- works for different types of model architectures ✓
- 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 ✓
- can be used for instance-wise model selection ✓

ROBUSTNESS QUANTIFICATION

- correlates nicely with accuracy ✓
- works for different types of model architectures ✓
- 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 ✓
- can be used for instance-wise model selection ✓



FUTURE WORK MEETINGS

A futuristic meeting scene with a speech bubble. The scene is dimly lit with blue and purple ambient lighting. In the foreground, a man with a beard and a pointed hat sits on the left, looking towards the center. In the middle, a man with short hair sits on a blue chair, looking forward. On the right, a woman with long hair sits on a blue chair, looking towards the center. A large white speech bubble with a black outline is positioned in the upper right, containing the word 'CALIBRATION' in blue capital letters. The background shows a blurred futuristic interior with various structures and lights.

CALIBRATION

FUTURE WORK MEETINGS

A meme image featuring a scene from Star Wars. The background shows a dimly lit room with a man in a dark robe sitting on a throne, and another man in a dark robe standing to the left. A speech bubble is positioned in the upper left corner, containing the word "REGRESSION". At the bottom of the image, the text "FUTURE WORK MEETINGS" is written in large, bold, white capital letters.

REGRESSION

FUTURE WORK MEETINGS

A futuristic meeting scene with a speech bubble. The scene is dimly lit with blue and purple ambient lighting. In the foreground, a man with a beard and a pointed hat sits on the left, looking towards the center. In the middle, a man with short hair sits on a blue chair, looking towards the right. On the right, a woman with long hair sits on a blue chair, looking towards the center. A speech bubble with a black outline and white fill is positioned in the upper right, containing the text 'CONFORMAL PREDICTION'.

**CONFORMAL
PREDICTION**

FUTURE WORK MEETINGS



jasper.debock@ugent.be
adrian.detavernier@ugent.be
rodrigo.lassance@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.