Scaling Data-Driven Probabilistic Robustness Analysis for Semantic Segmentation Neural Networks

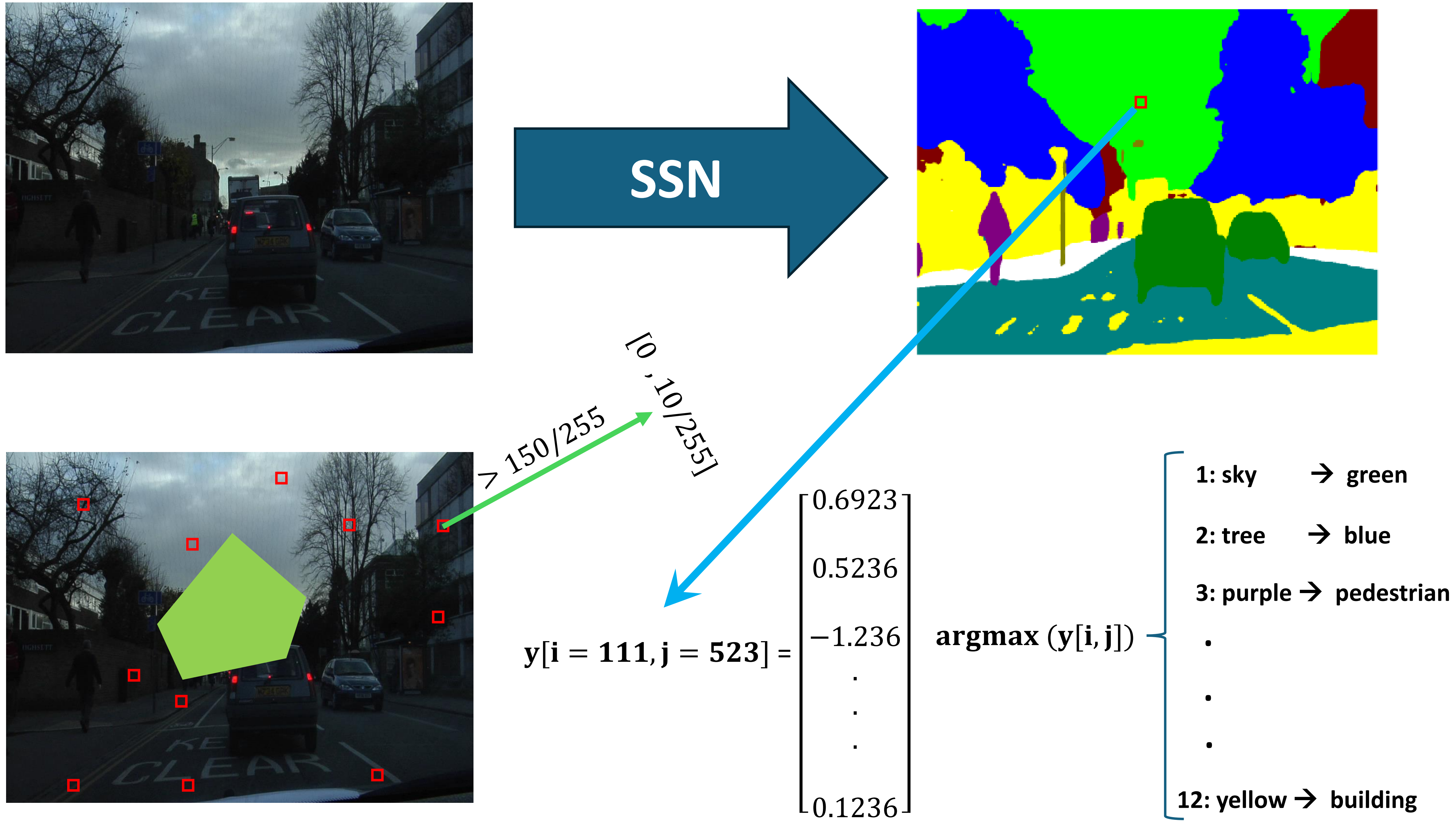
Navid Hashemi, Samuel Sasaki, Ipek Oguz, Meiyi Ma, Taylor T Johnson

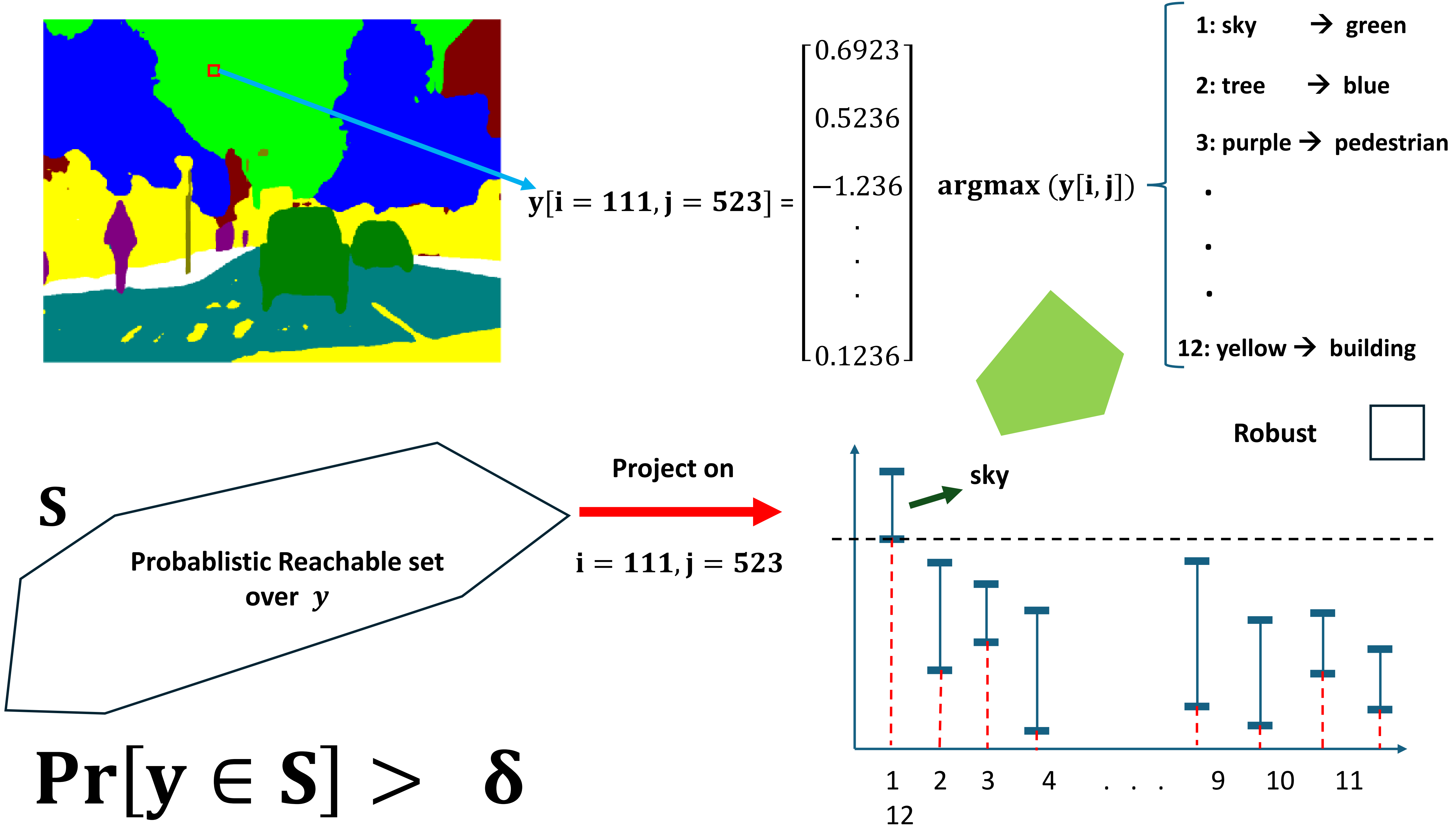
Department of Computer Science, Institute for Software Integrated Systems

Vanderbilt University

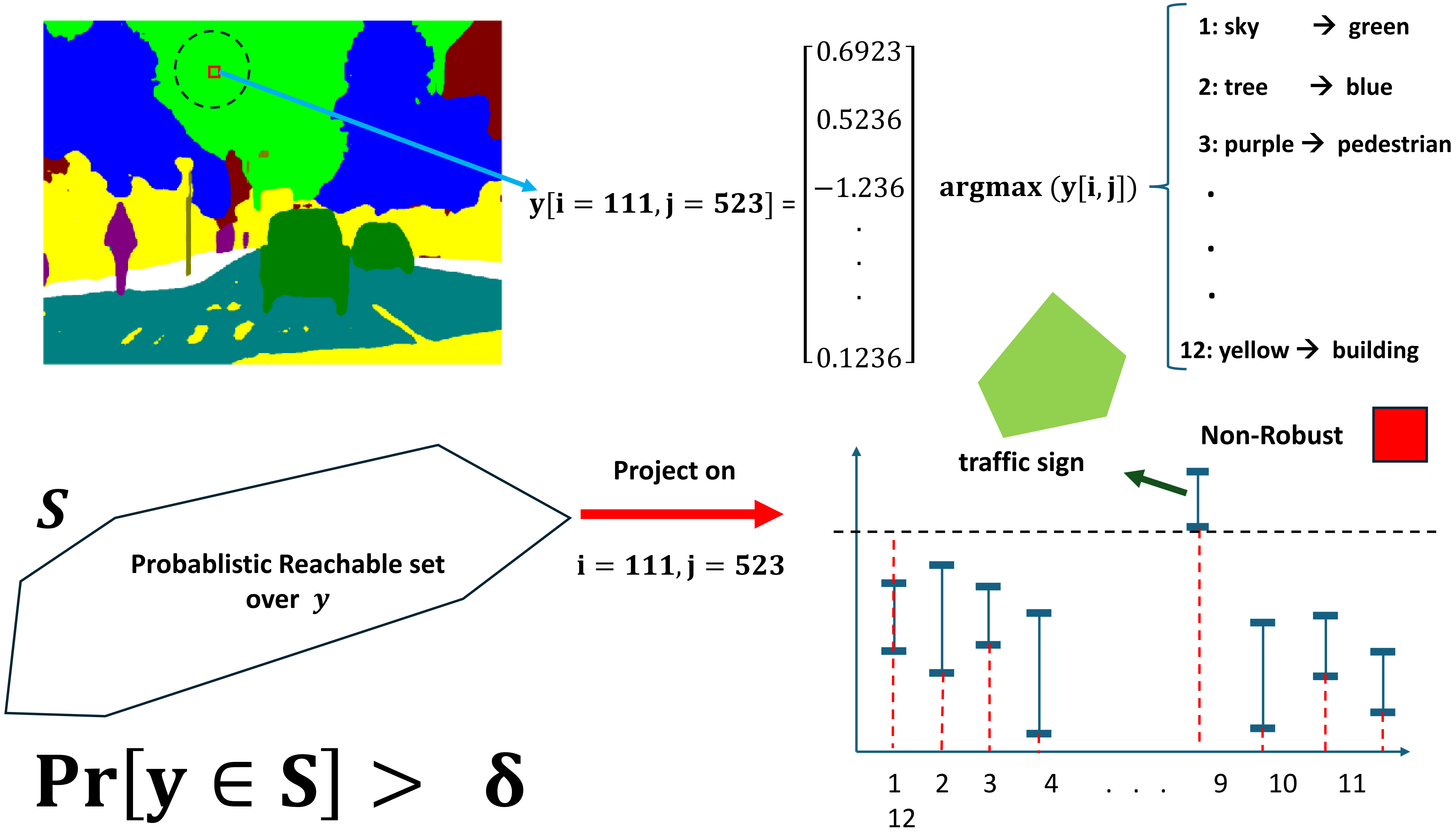
VANDERBILT UNIVERSITY

NEURAL INFORMATION PROCESSING SYSTEMS

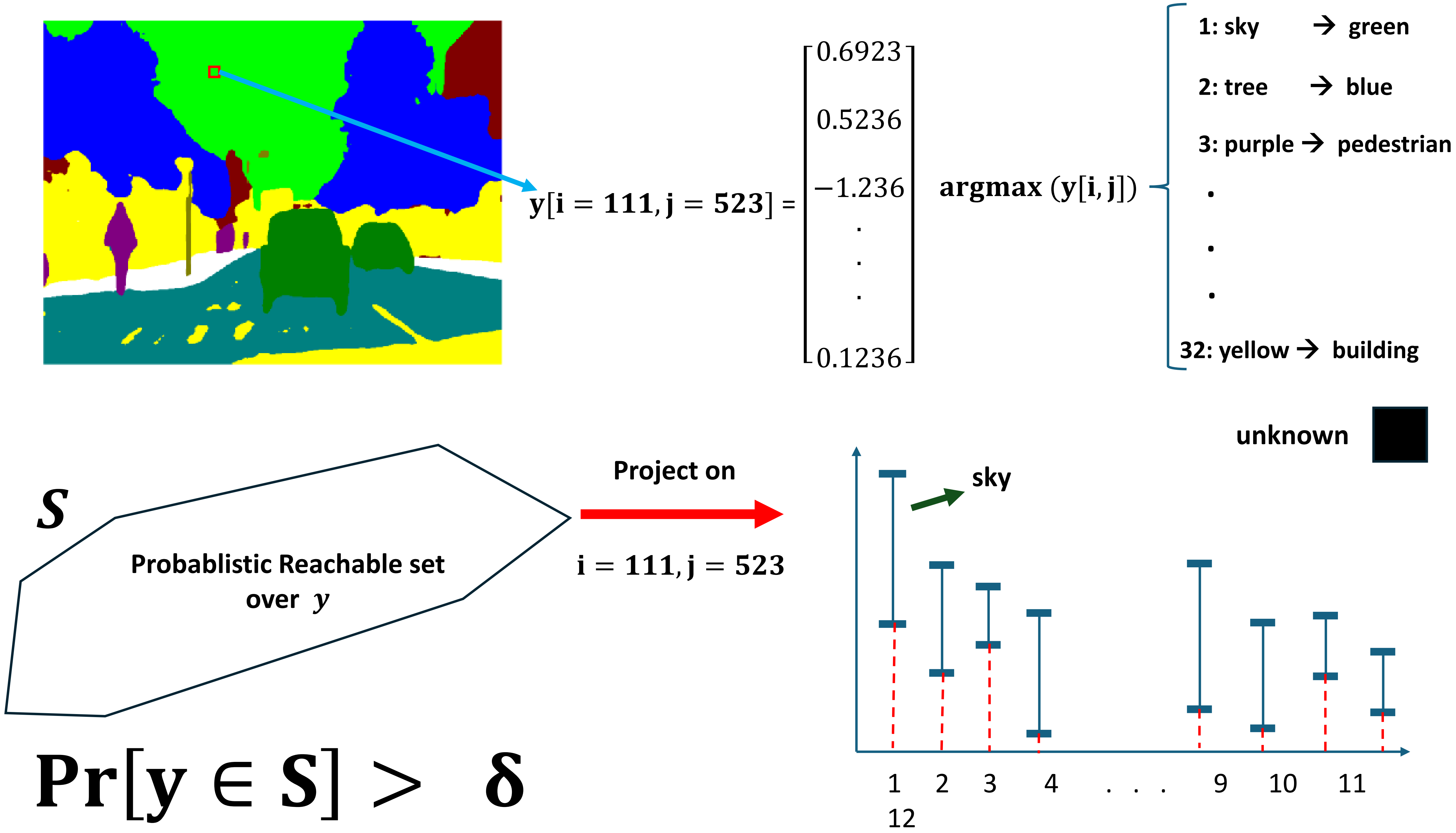

SSN
> 150/255
[0 , 10/255]
y[i = 111, j = 523] =
0.6923
0.5236
−1.236
.
.
.
0.1236
argmax (y[i, j])
1: sky → green
2: tree → blue
3: purple → pedestrian
.
.
.
12: yellow → building

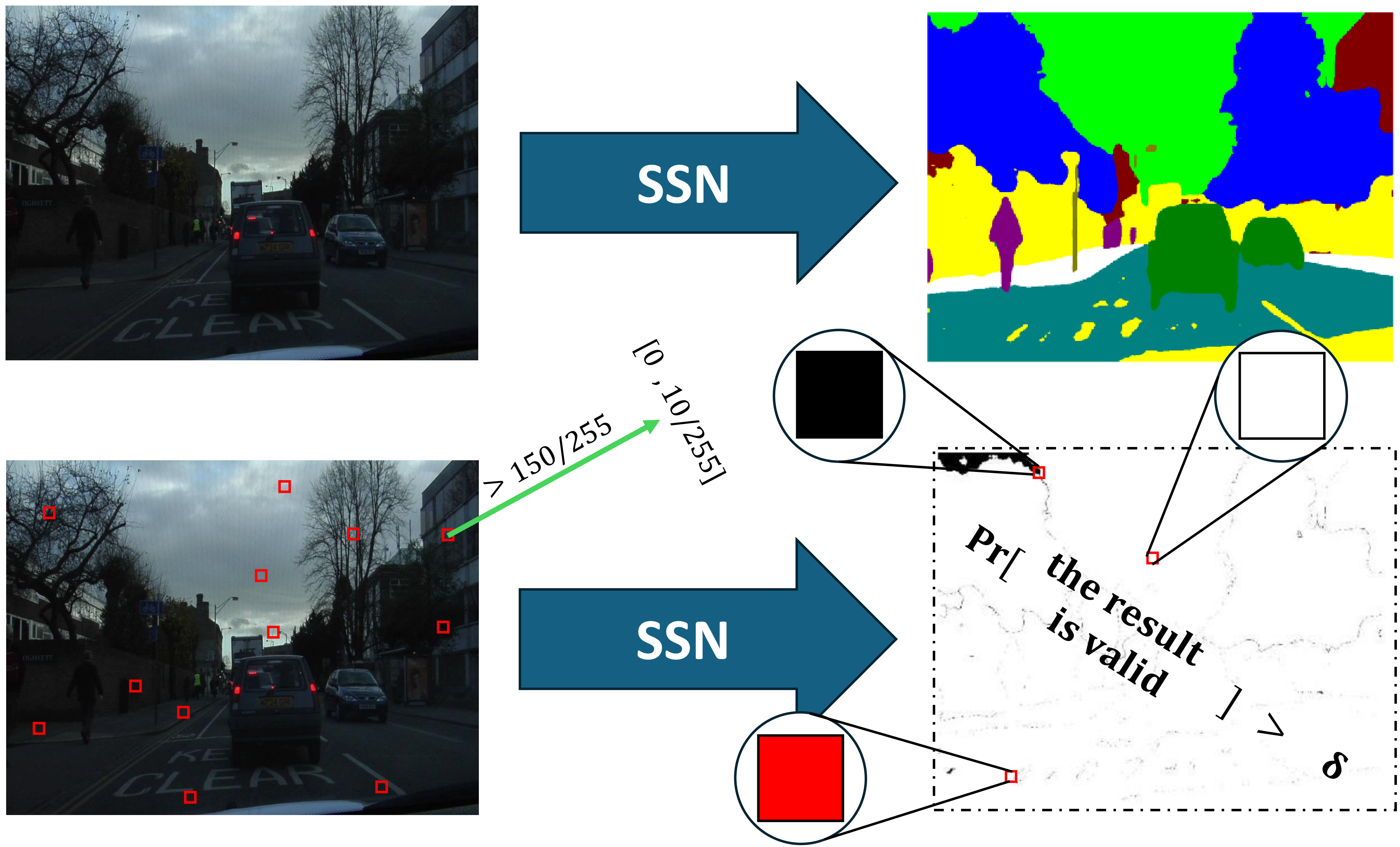


y[i = 111, j = 523] =
0.6923
0.5236
−1.236
0.1236
argmax (y[i, j])
1: sky → green
2: tree → blue
3: purple → pedestrian
12: yellow → building
Robust
S
Probablistic Reachable set over y
Project on
i = 111, j = 523
sky
1
2
3
4
. . .
9
10
11
12
Pr[y ∈ S] > δ

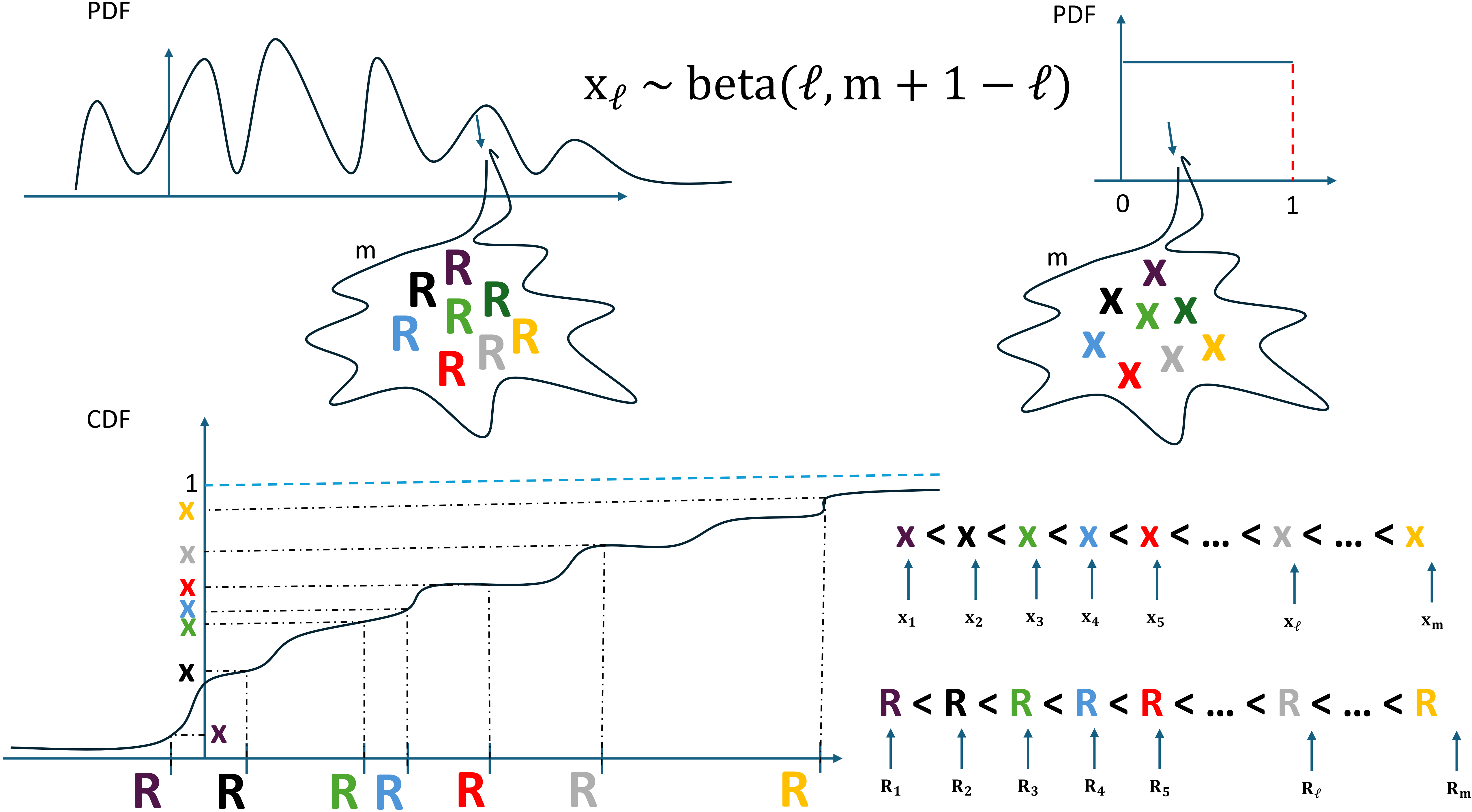


$y[i = 111, j = 523] = \begin{bmatrix} 0.6923 \\ 0.5236 \\ -1.236 \\ \vdots \\ 0.1236 \end{bmatrix}$
$\text{argmax}\,(y[i,j])$
1: sky → green
2: tree → blue
3: purple → pedestrian
12: yellow → building
Non-Robust
traffic sign
Project on
$i = 111, j = 523$
S
Probablistic Reachable set over y
$\Pr[y \in S] > \delta$
1
12
2
3
4
. . .
9
10
11

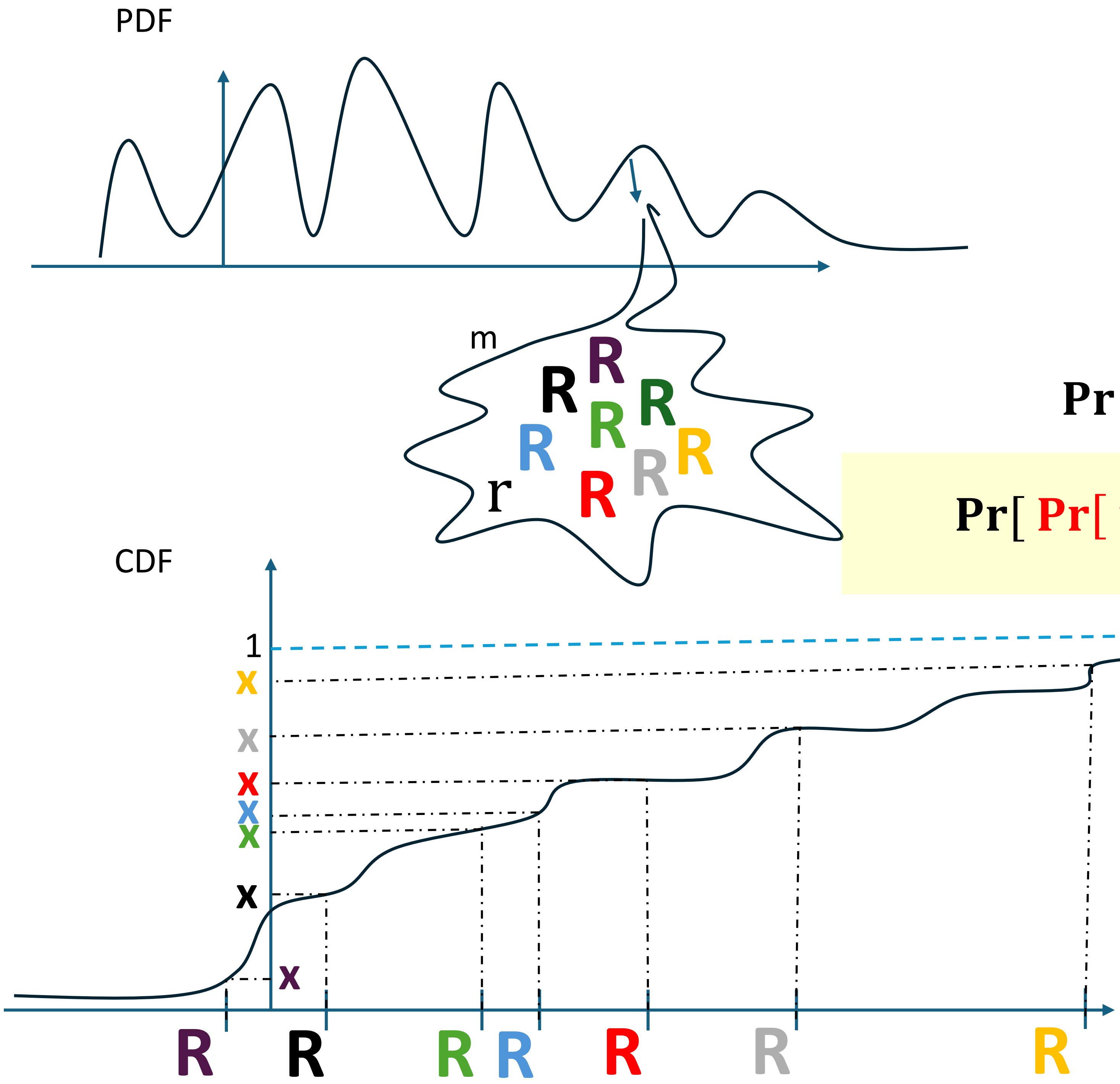

y[i = 111, j = 523] =
0.6923
0.5236
−1.236
0.1236
argmax (y[i, j])
1: sky → green
2: tree → blue
3: purple → pedestrian
32: yellow → building
unknown
S
Probablistic Reachable set
over y
Project on
i = 111, j = 523
sky
1
2
3
4
. . .
9
10
11
12
Pr[y ∈ S] > δ



SSN
SSN
> 150/255
[0 , 10/255]
Pr[the result is valid] > δ



PDF
$x_\ell \sim \text{beta}(\ell, m + 1 - \ell)$
PDF
0
1
m
R R R R R R R R
m
X X X X X X X X
CDF
1
x x x x x x x
R R R R R R R
$x < x < x < x < x < \ldots < x < \ldots < x$
x_1 x_2 x_3 x_4 x_5 x_ℓ x_m
$R < R < R < R < R < \ldots < R < \ldots < R$
R_1 R_2 R_3 R_4 R_5 R_ℓ R_m



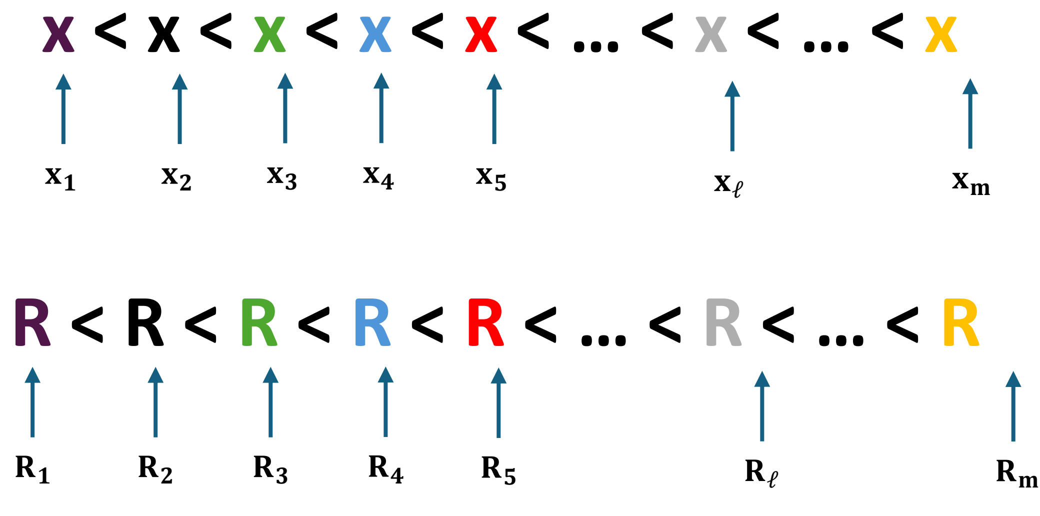
$$\Pr[\, r < R_\ell \,] = x_\ell$$

$$x_\ell \sim \mathrm{beta}(\ell, m + 1 - \ell)$$

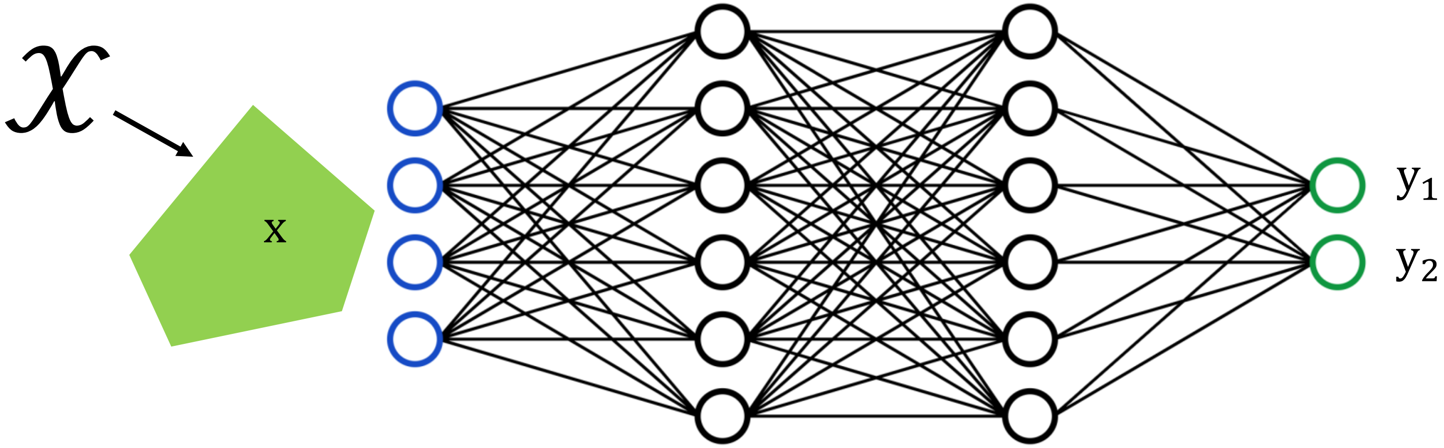
m = 200,000 , ℓ =199,998

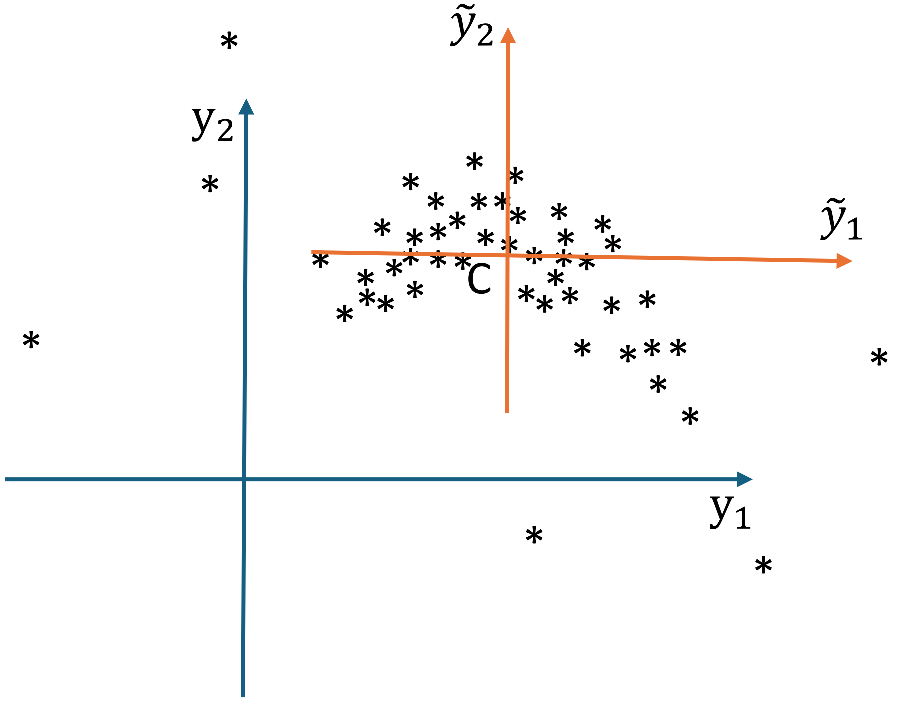
$$\mathbf{Pr}[\mathbf{x}_\ell > \mathbf{0.9999}] > \mathbf{0.999999}$$

$$\mathbf{Pr}[\, \mathbf{Pr}[\, \mathbf{r} < \mathbf{R}_\ell] > \mathbf{0.9999} \,] > \mathbf{0.999999}$$



Application on Reachability Analysis of DNN



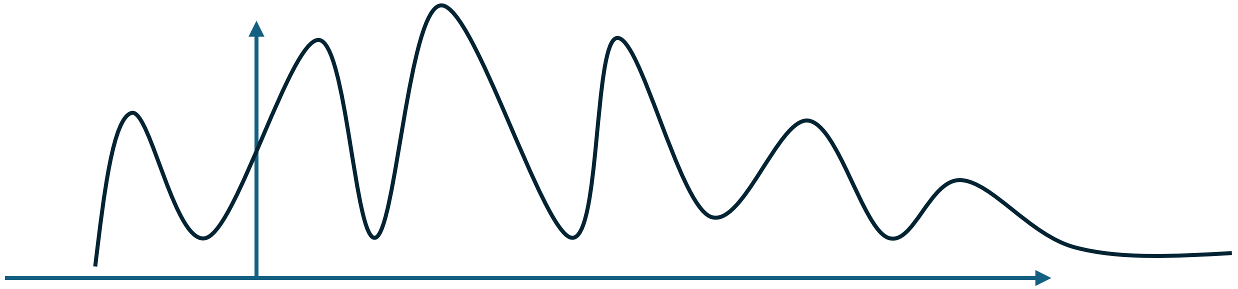


$$\tilde{y}_{1,max} = \max(\forall\, |\tilde{y}_1|\,)$$

$$\tilde{y}_{2,max} = \max(\forall\, |\tilde{y}_2|\,)$$

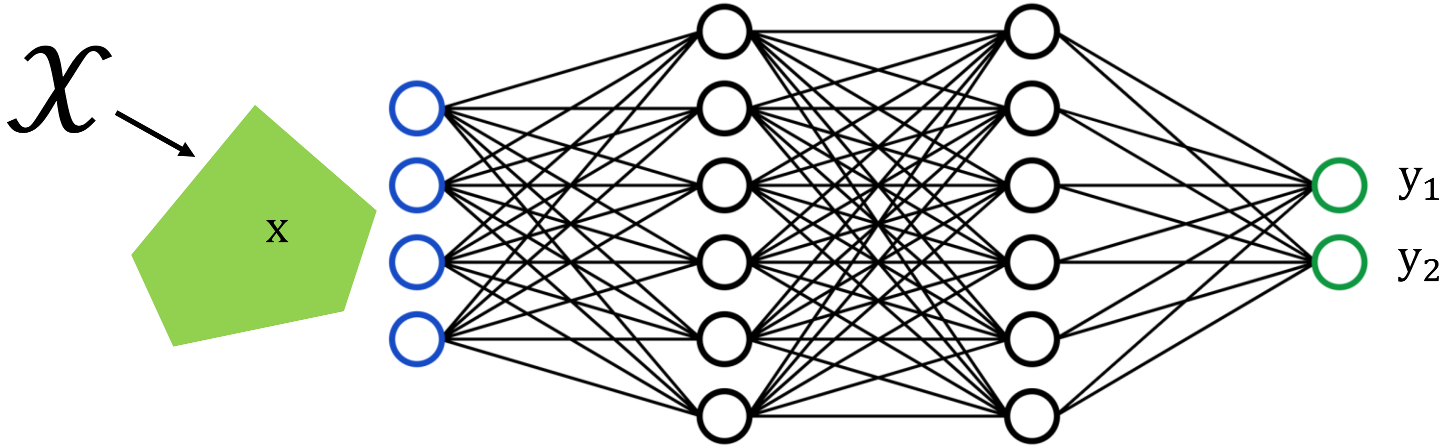
$$R = \max\left(\frac{|\tilde{y}_1|}{\tilde{y}_{1,max}} \;,\; \frac{|\tilde{y}_2|}{\tilde{y}_{2,max}} \right)$$

PDF

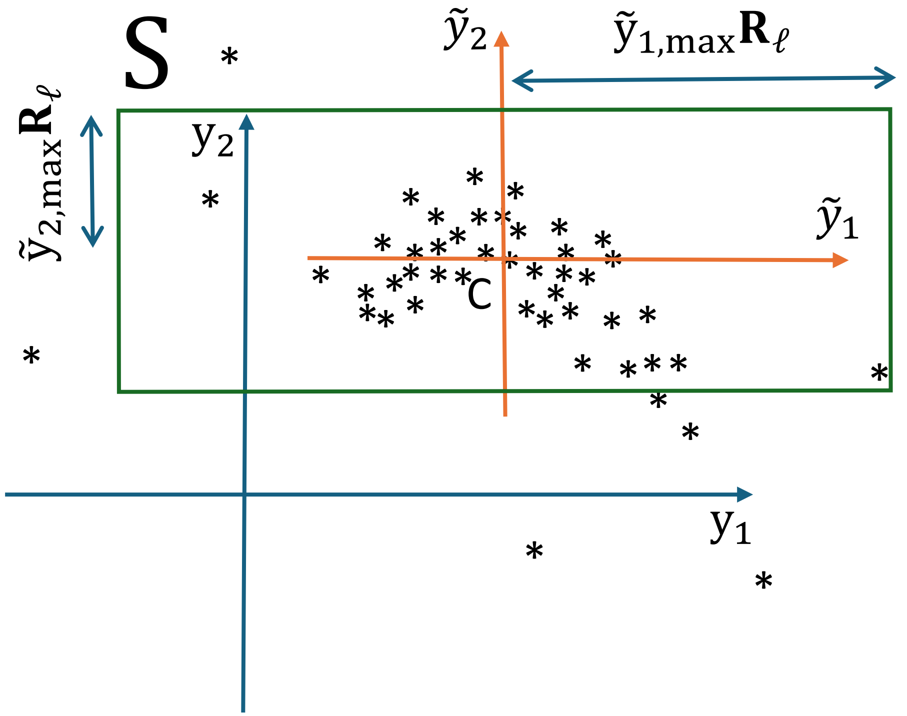


$m = 200{,}000$, $\ell = 199{,}998$

$$\mathbf{Pr}[\ \mathbf{Pr}[\mathbf{R} < \mathbf{R}_{\ell}] > \ \mathbf{0.9999}\ ] \ > \mathbf{0.999999}$$



$$\tilde{y}_{1,max} = \max(\forall\, |\tilde{y}_1|)$$
$$\tilde{y}_{2,max} = \max(\forall\, |\tilde{y}_2|)$$
$$R = \max\left(\frac{|\tilde{y}_1|}{\tilde{y}_{1,max}} \;,\; \frac{|\tilde{y}_2|}{\tilde{y}_{2,max}} \right)$$

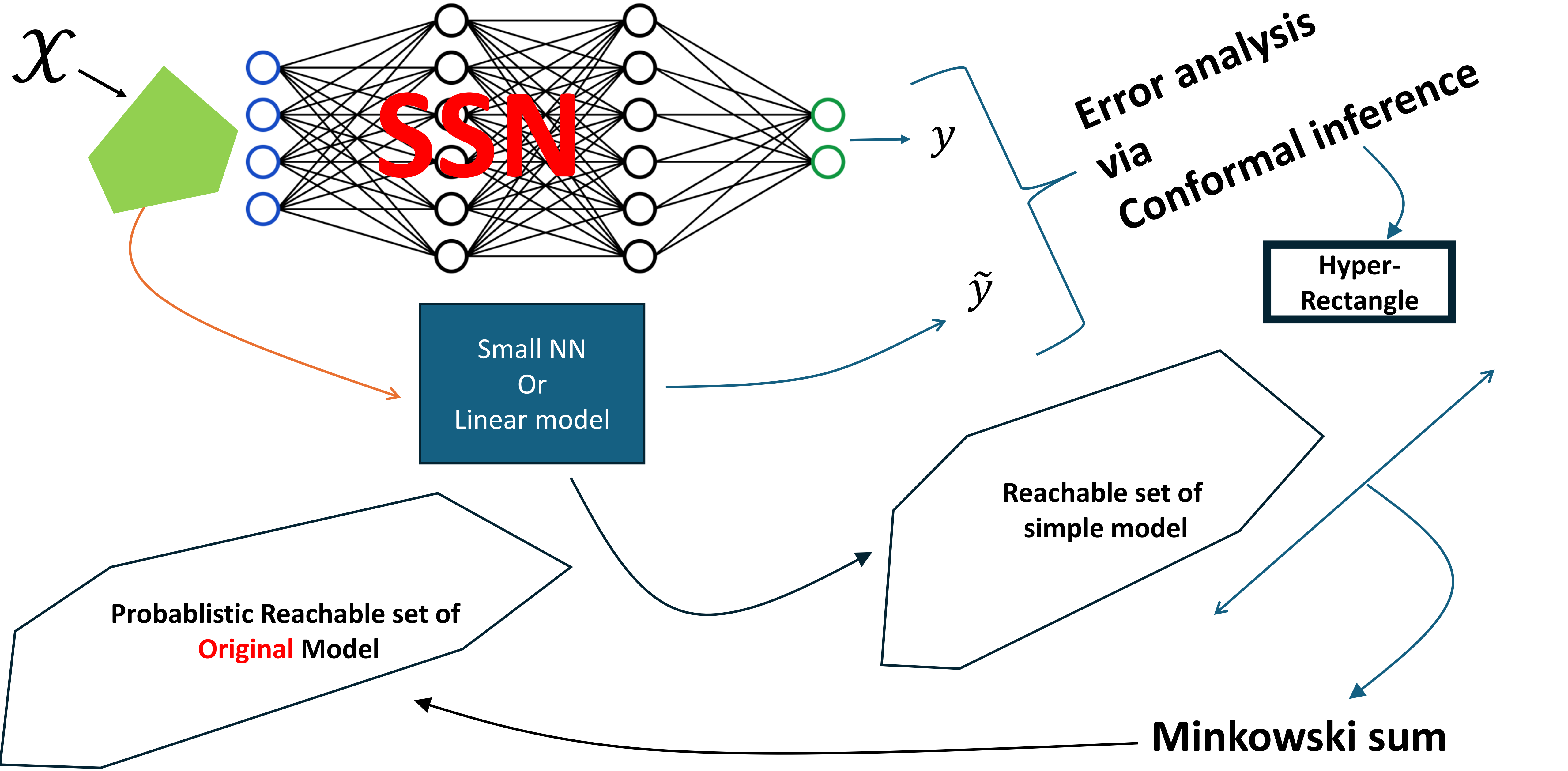


$$\mathbf{R} < \mathbf{R}_\ell \iff \left(|\tilde{\boldsymbol{y}}_1| < \tilde{y}_{1,max}\mathbf{R}_\ell\right) \wedge \left(|\tilde{\boldsymbol{y}}_2| < \tilde{y}_{2,max}\mathbf{R}_\ell\right)$$

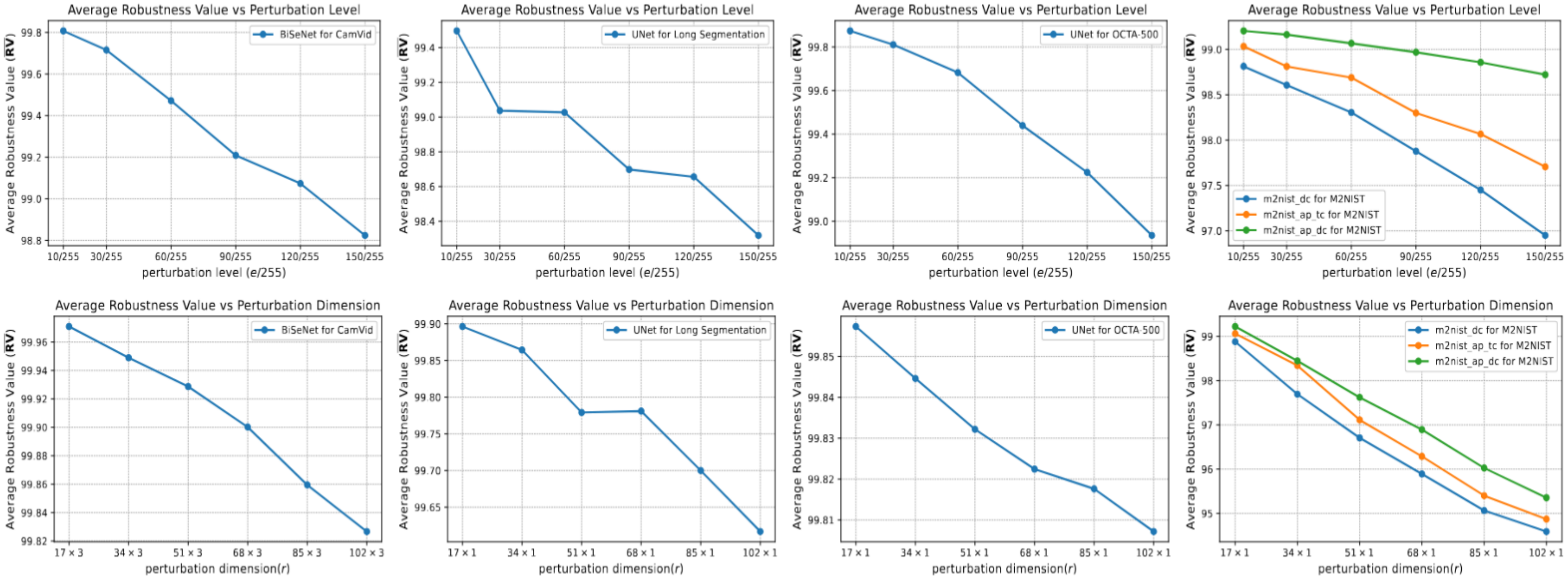
$$\mathbf{Pr}[\, \mathbf{Pr}[\, \mathbf{y} \in \mathbf{S}] > \mathbf{0.9999}\,] > \mathbf{0.999999}$$

m = 200,000 , ℓ =199,998

$$\mathbf{Pr}[\, \mathbf{Pr}[\, \mathbf{R} < \mathbf{R}_\ell] > \mathbf{0.9999}\,] > \mathbf{0.999999}$$



$\mathcal{X}$
SSN
y
$\tilde{y}$
Error analysis via Conformal inference
Hyper-Rectangle
Small NN Or Linear model
Reachable set of simple model
Probablistic Reachable set of Original Model
Minkowski sum



CamVid Dataset:

Logits dimension:
8294400

Lung Segmentation:

Logits dimension:
262144

OCTA- 500:

Logits dimension:
92416

M2NIST:

Logits dimension:
59136

Thank You