Where the hell does the loss come from?

MAP, MLE view of regression, classification and other problems

Karel Zimmermann
Czech Technical University in Prague
Faculty of Electrical Engineering, Department of Cybernetics



Procrastination idea: come up with original logo https://beta.dreamstudio.ai/dream

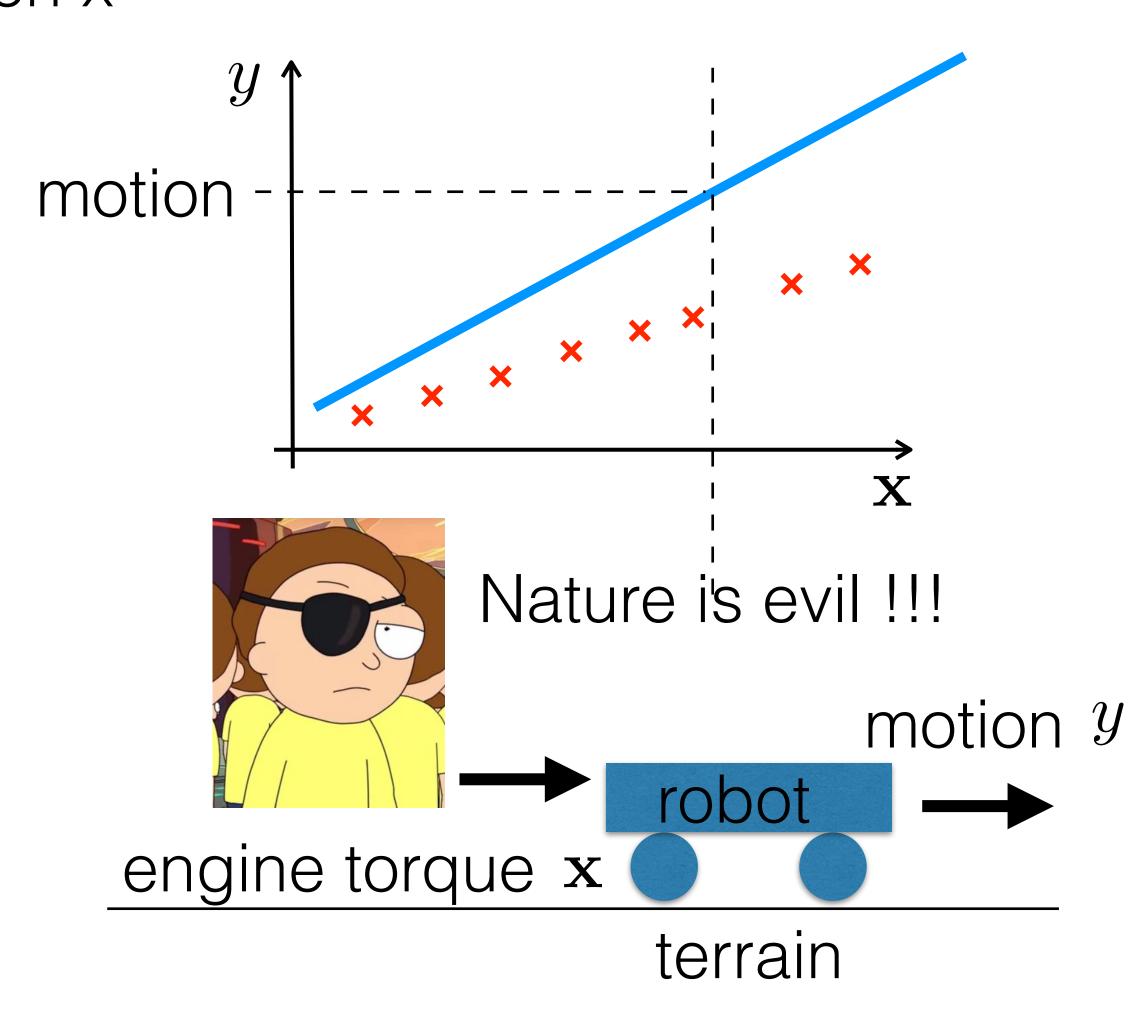
Pre-requisites:

- linear algebra,
- probability laws:
 - Bayes rule: p(A,B) = p(B,A) = p(A|B)*p(B) = p(B|A)*p(A)
 - Independence of A and B: p(A,B) = p(A)p(B)

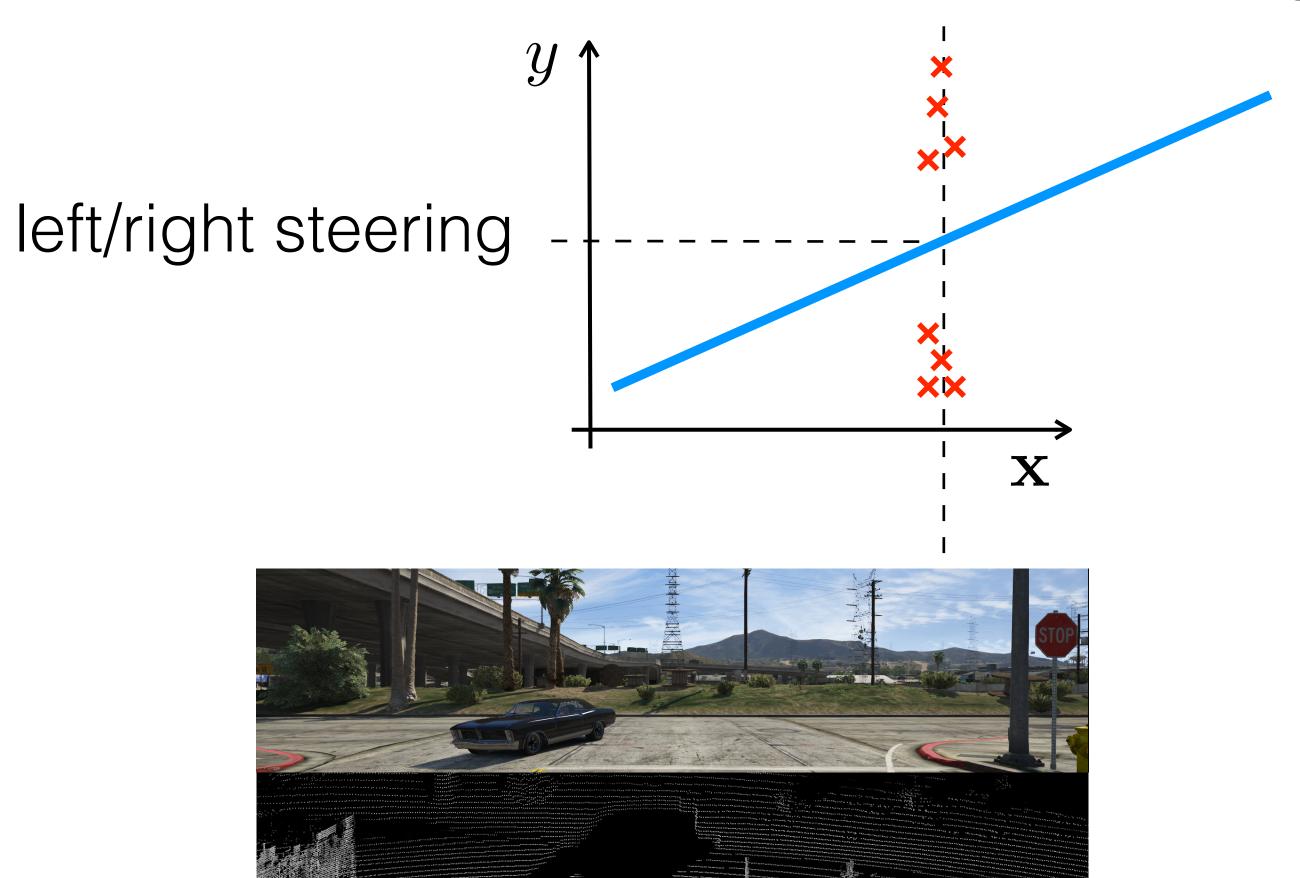
This lecture is (at least for me) take-home message of this course.

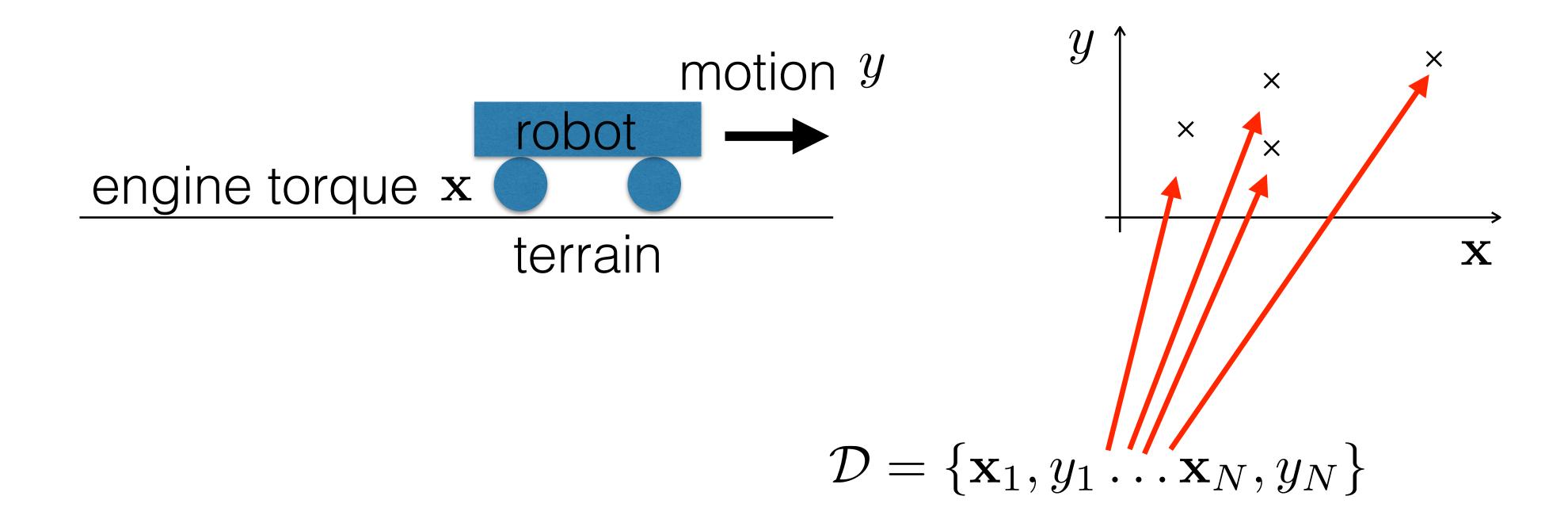
What can go wrong: inappropriate choice of loss function

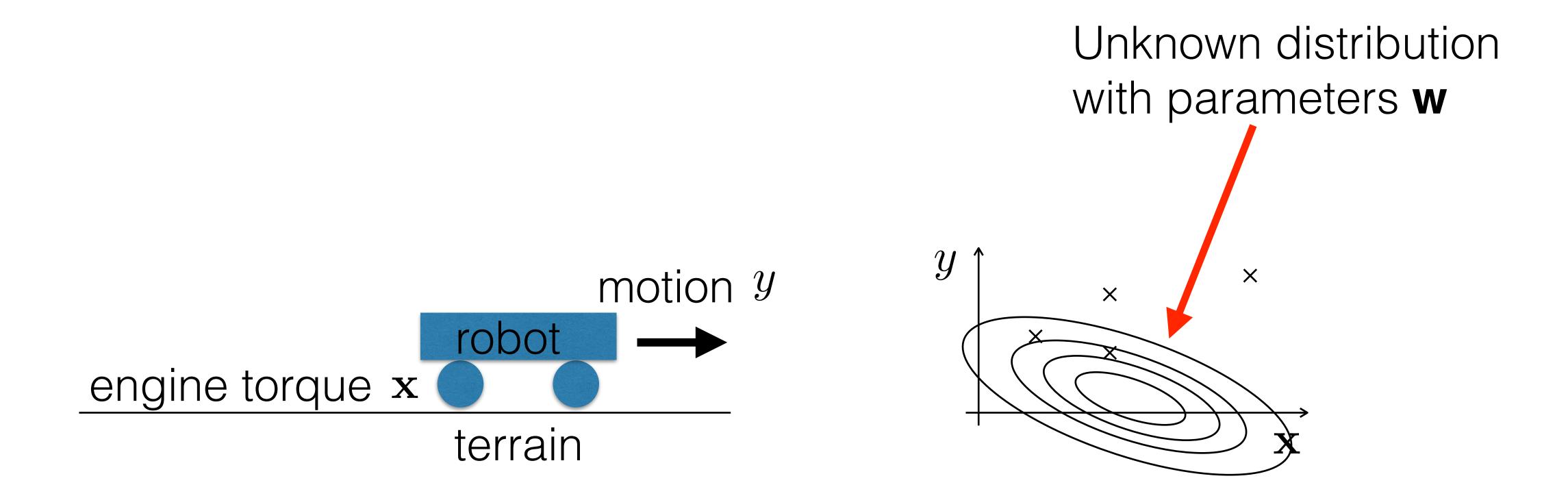
What should I do instead of fitting a curve??? Search for probability distribution of y given x

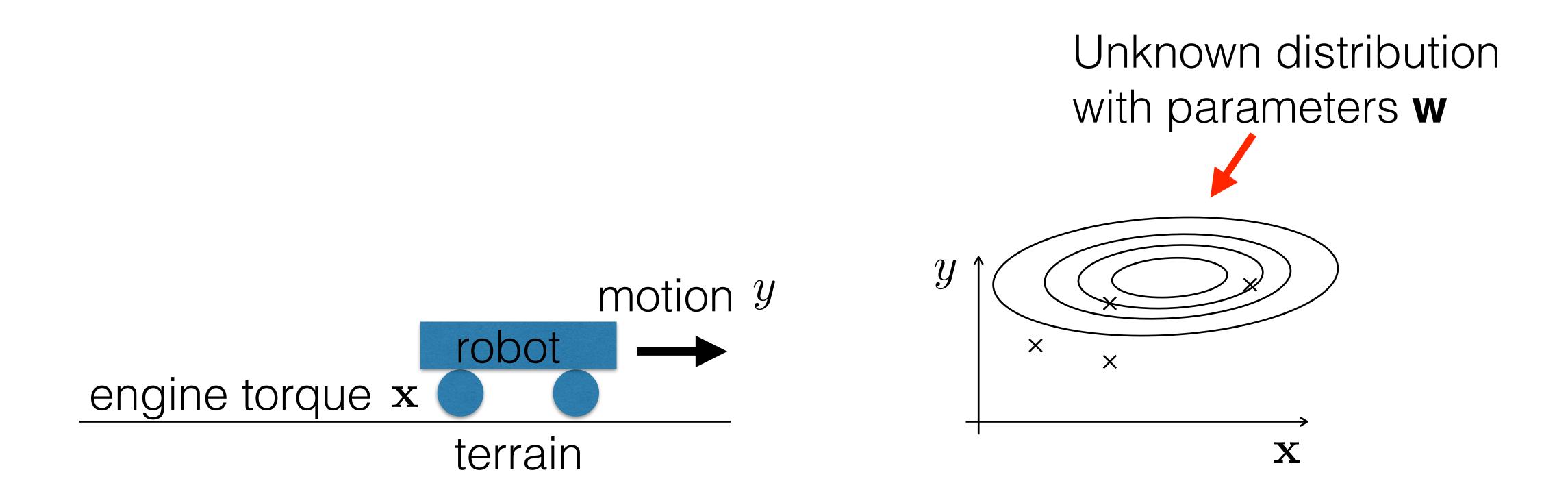


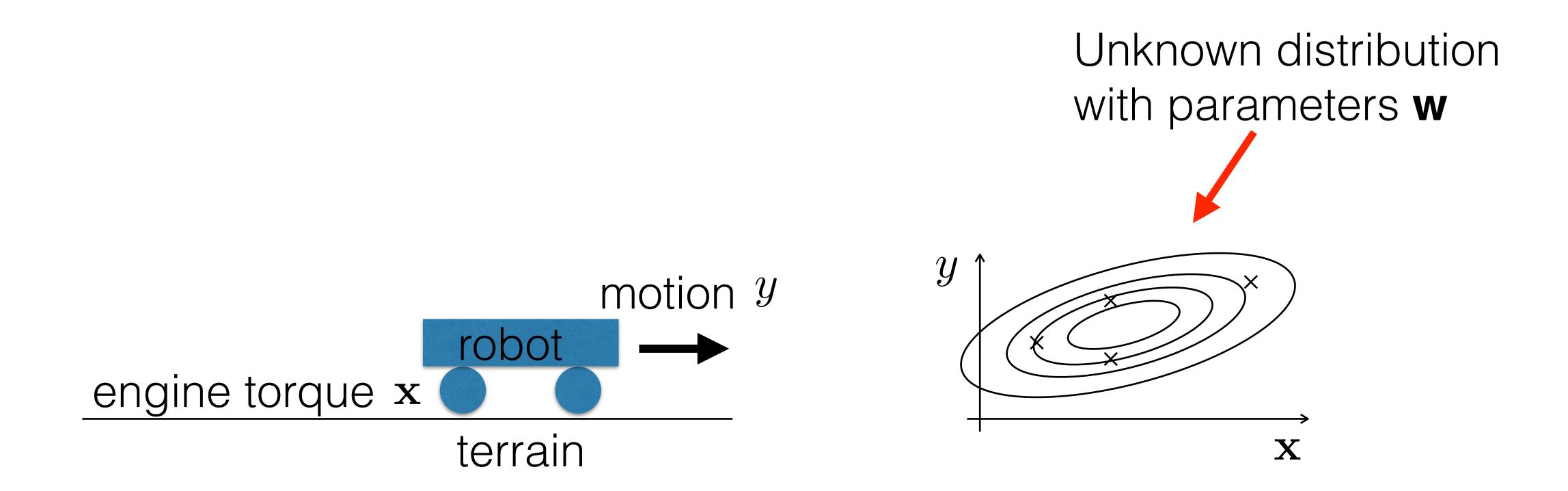
outlier











$$\mathbf{w}^* = \arg\max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D})$$

$$\mathbf{w}^* = \arg\max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg\max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{D})}$$

$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{D})}$$
$$= \arg \max_{\mathbf{w}} p(\mathcal{D}|\mathbf{w})p(\mathbf{w})$$

$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{D}|\mathbf{w})}$$
$$= \arg \max_{\mathbf{w}} p(\mathcal{D}|\mathbf{w})p(\mathbf{w}) = \arg \max_{\mathbf{w}} p(\mathbf{x}_1, y_1 \dots \mathbf{x}_N, y_N|\mathbf{w})p(\mathbf{w})$$

$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{D})}$$

$$= \arg \max_{\mathbf{w}} p(\mathcal{D}|\mathbf{w})p(\mathbf{w}) = \arg \max_{\mathbf{w}} p(\mathbf{x}_1, y_1 \dots \mathbf{x}_N, y_N|\mathbf{w})p(\mathbf{w})$$
i.i.d.
$$= \arg \max_{\mathbf{w}} \left(\prod_{i} p(\mathbf{x}_i, y_i|\mathbf{w})\right) p(\mathbf{w})$$

$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{D})}$$

$$= \arg \max_{\mathbf{w}} p(\mathcal{D}|\mathbf{w})p(\mathbf{w}) = \arg \max_{\mathbf{w}} p(\mathbf{x}_1, y_1 \dots \mathbf{x}_N, y_N|\mathbf{w})p(\mathbf{w})$$
i.i.d.
$$= \arg \max_{\mathbf{w}} \left(\prod_{i} p(\mathbf{x}_i, y_i|\mathbf{w})\right) p(\mathbf{w})$$

$$= \arg \max_{\mathbf{w}} \left(\prod_{i} p(y_i|\mathbf{x}_i, \mathbf{w})p(\mathbf{x}_i)\right) p(\mathbf{w})$$

$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \max_{\mathbf{w}} \frac{p(\mathcal{D}|\mathbf{w})p(\mathbf{w})}{p(\mathcal{T})}$$

$$= \arg \max_{\mathbf{w}} p(\mathcal{D}|\mathbf{w})p(\mathbf{w}) = \arg \max_{\mathbf{w}} p(\mathbf{x}_1, y_1 \dots \mathbf{x}_N, y_N|\mathbf{w})p(\mathbf{w})$$
i.i.d.
$$= \arg \max_{\mathbf{w}} \left(\prod_{i} p(\mathbf{x}_i, y_i|\mathbf{w})\right) p(\mathbf{w})$$

$$= \arg \max_{\mathbf{w}} \left(\prod_{i} p(y_i|\mathbf{x}_i, \mathbf{w})p(\mathbf{x}_i)\right) p(\mathbf{w})$$

$$= \arg \max_{\mathbf{w}} \left(\sum_{i} \log(p(y_i|\mathbf{x}_i, \mathbf{w})) + \log p(\mathbf{x}_i)\right) + \log p(\mathbf{w})$$

$$= \arg \max_{\mathbf{w}} \left(\sum_{i} \log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + \log p(\mathbf{w})$$

$$= \arg \max_{\mathbf{w}} \left(\sum_{i} \log(p(y_i | \mathbf{x}_i, \mathbf{w})) \right) + \log p(\mathbf{w})$$

$$= \arg \min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i | \mathbf{x}_i, \mathbf{w})) \right) + \left(-\log p(\mathbf{w}) \right)$$

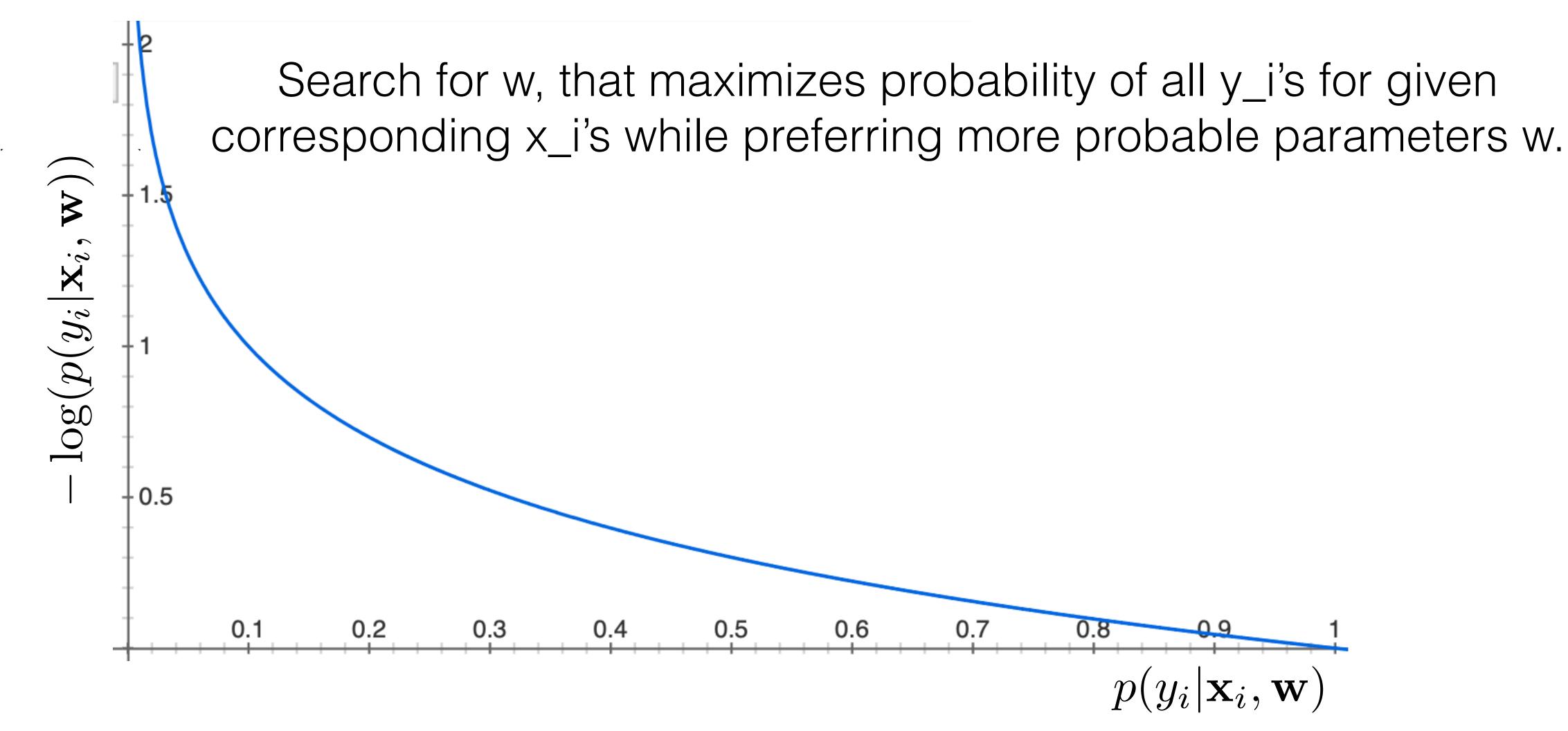
log likelihood

prior/regulariser

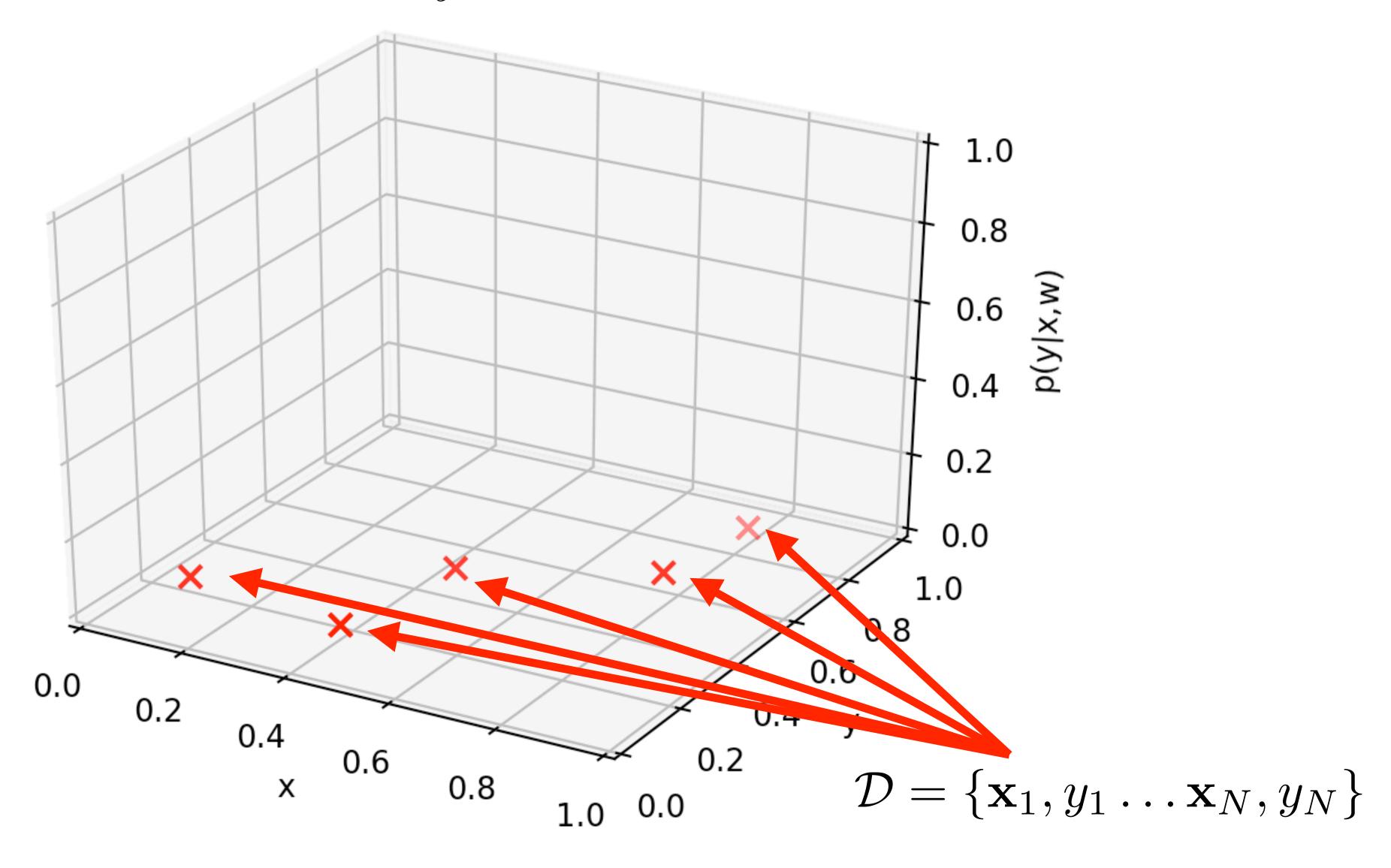
$$\mathbf{w}^* = \arg \max_{\mathbf{w}} p(\mathbf{w}|\mathcal{D}) = \arg \min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + \left(-\log p(\mathbf{w}) \right)$$

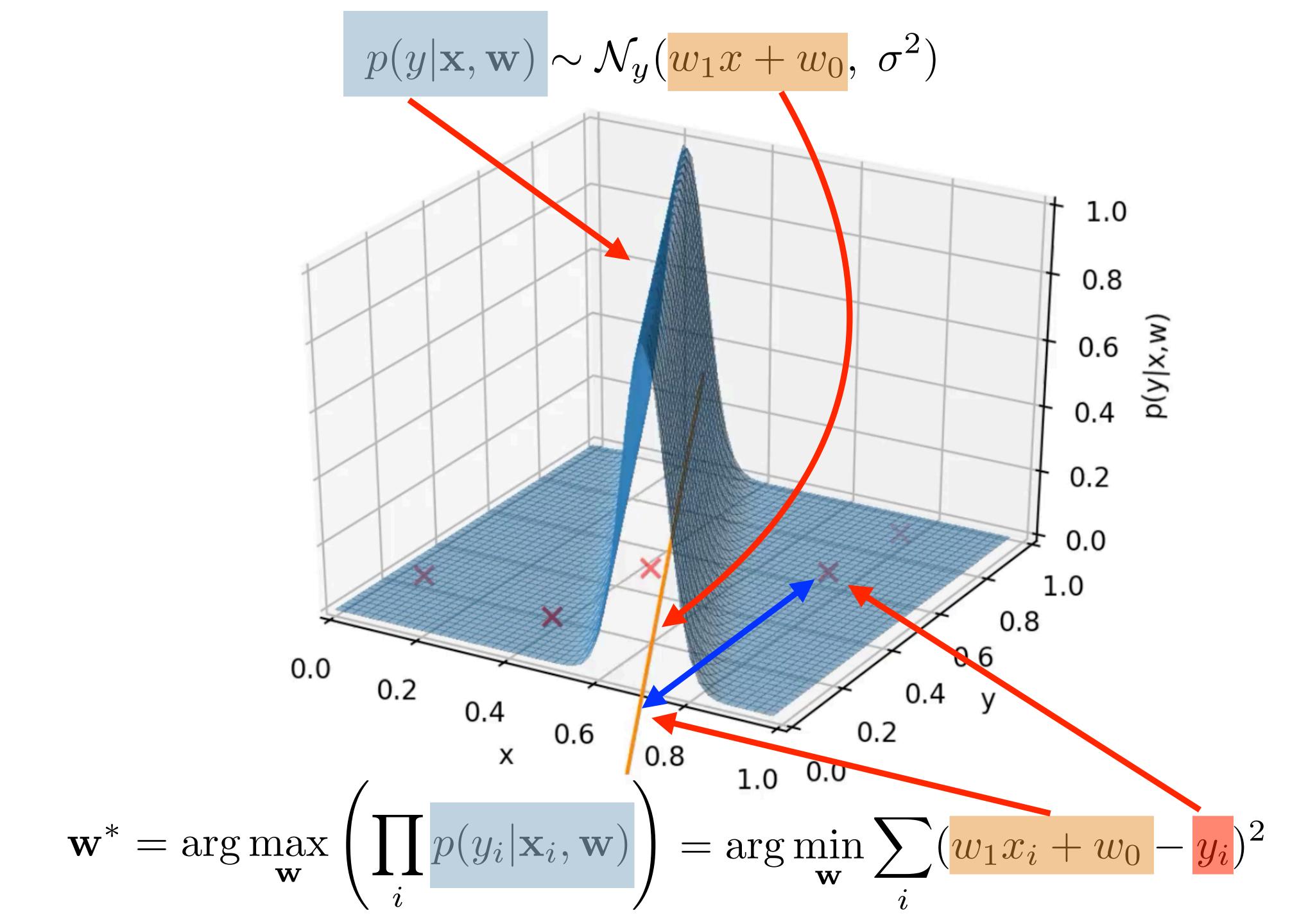
log likelihood

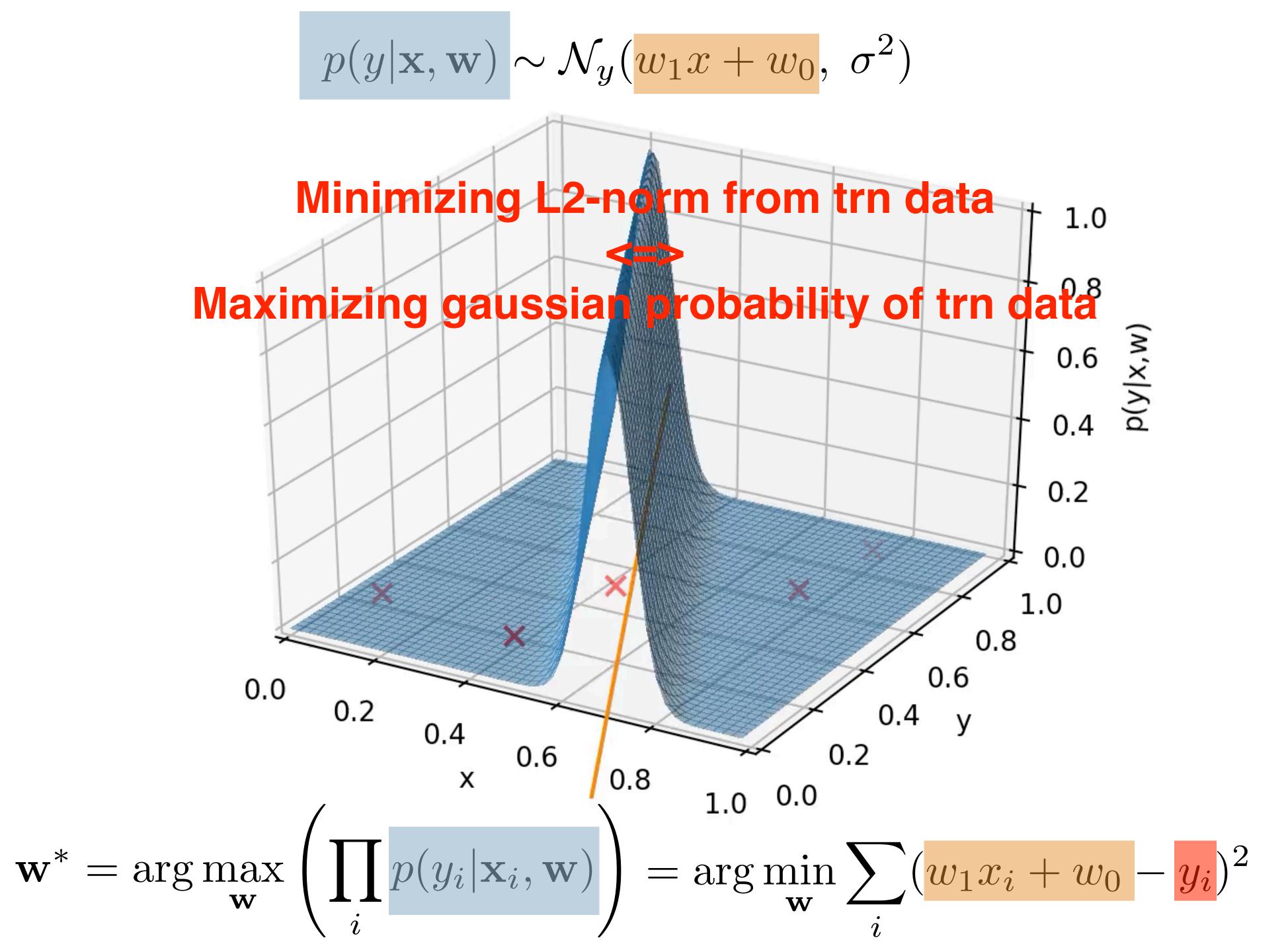
prior/regulariser



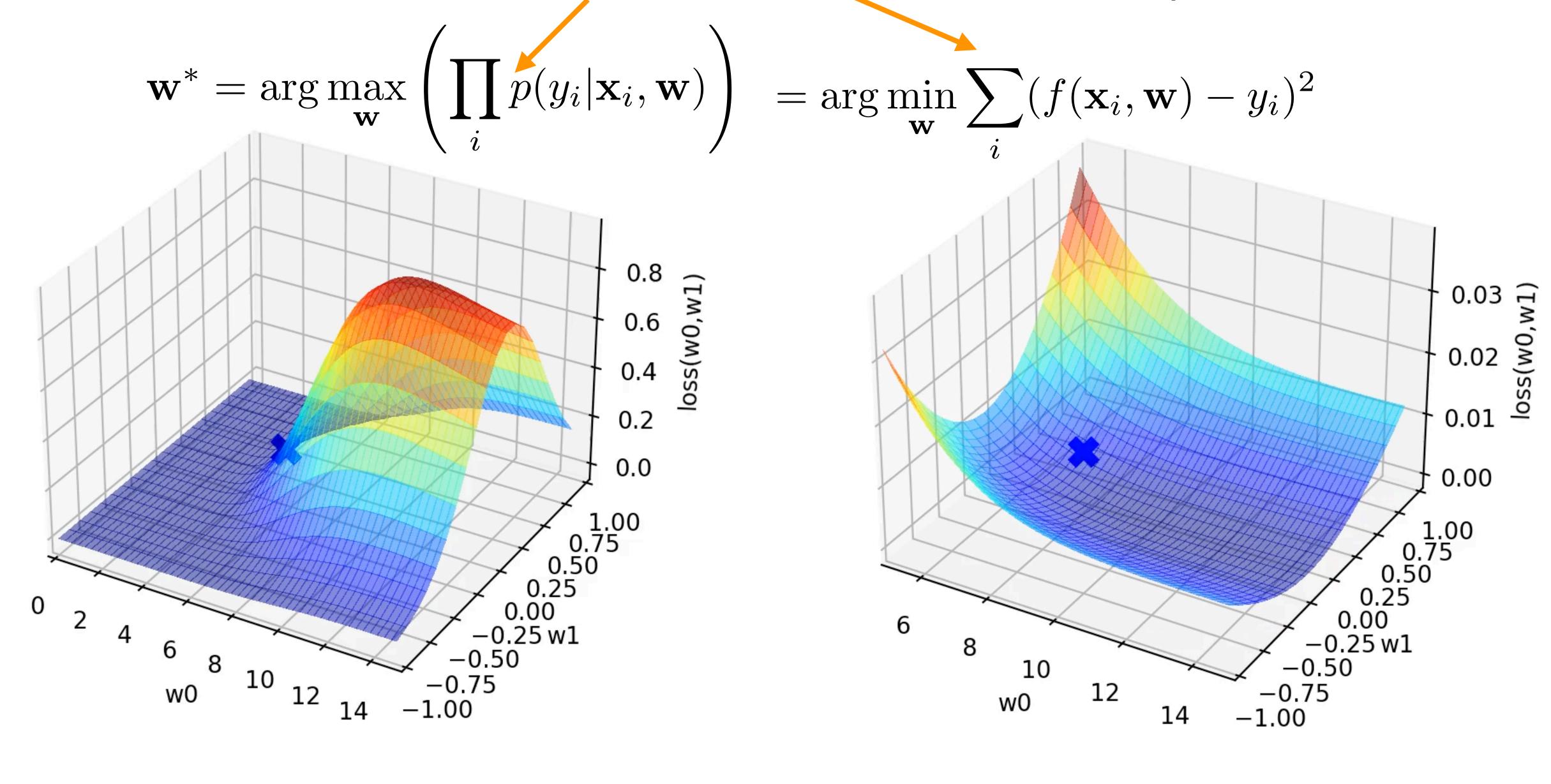
$$p(y|\mathbf{x},\mathbf{w}) \sim \mathcal{N}_y(w_1x + w_0, \sigma^2)$$







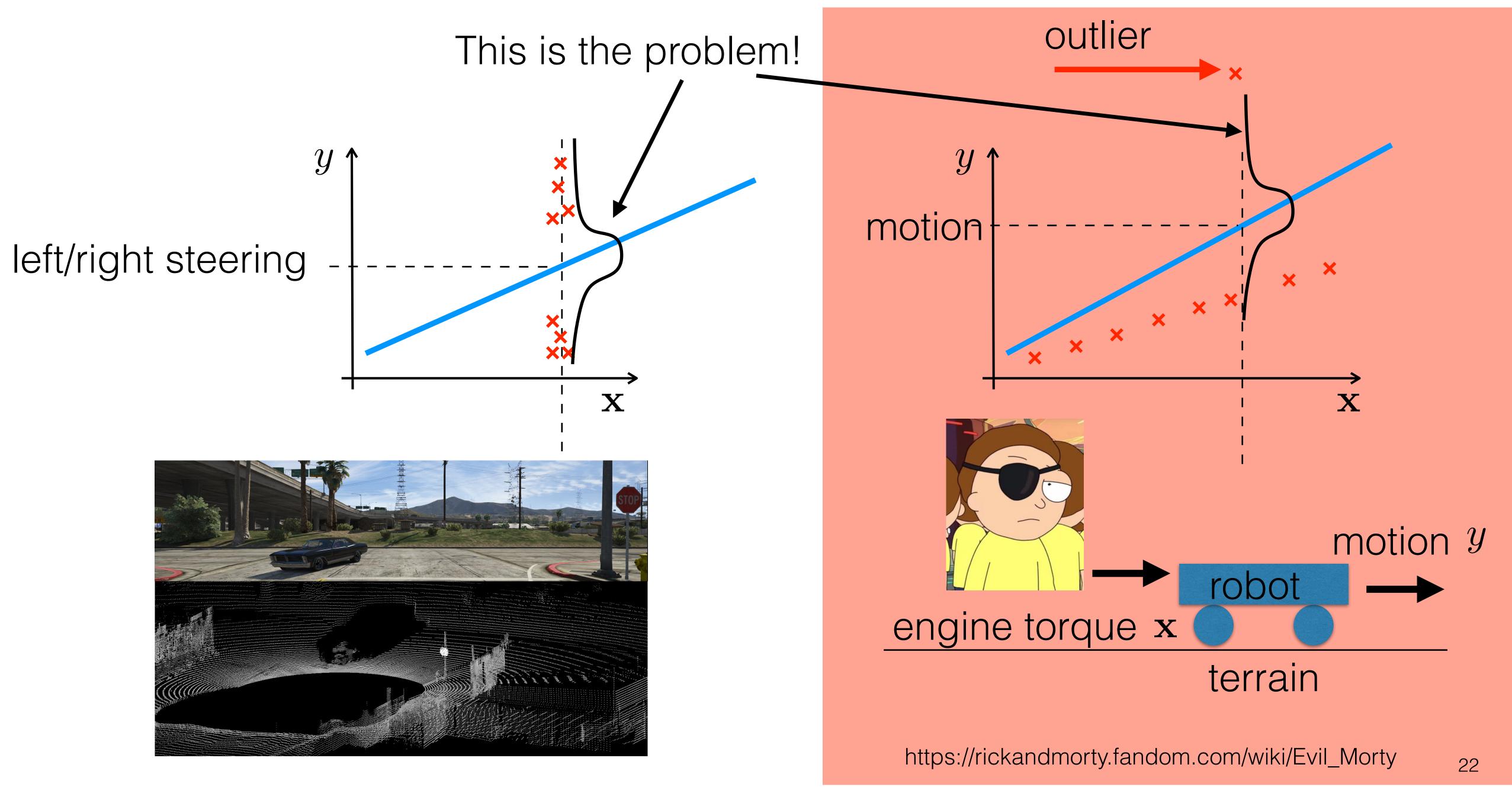
• In what sense is the MLE and the LSQ formulations equivalent?

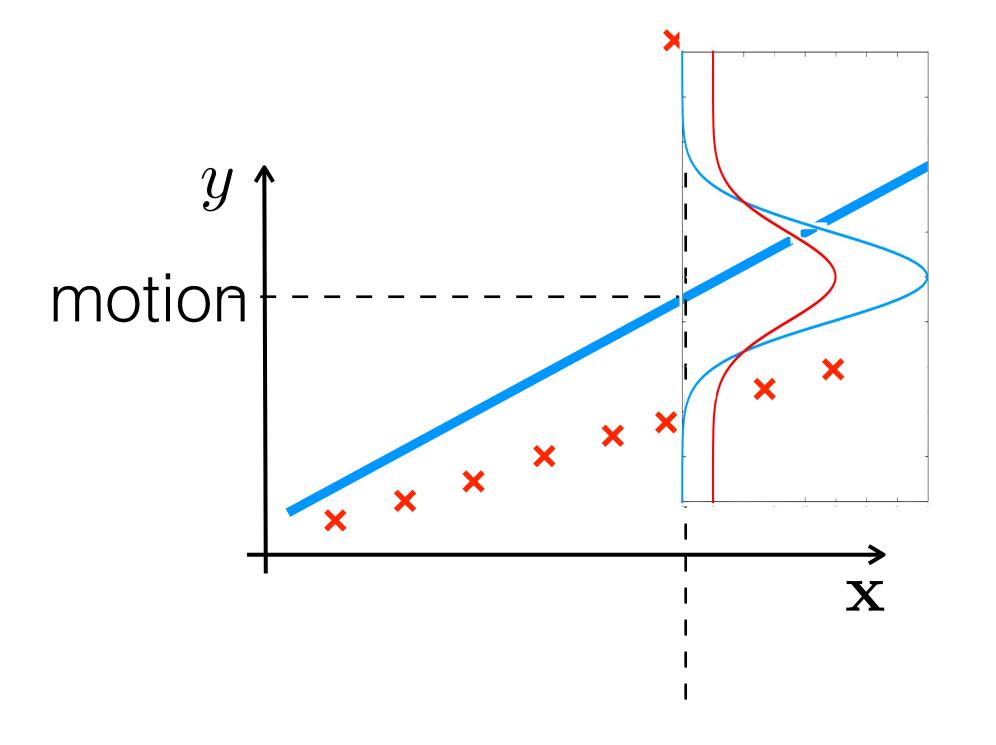


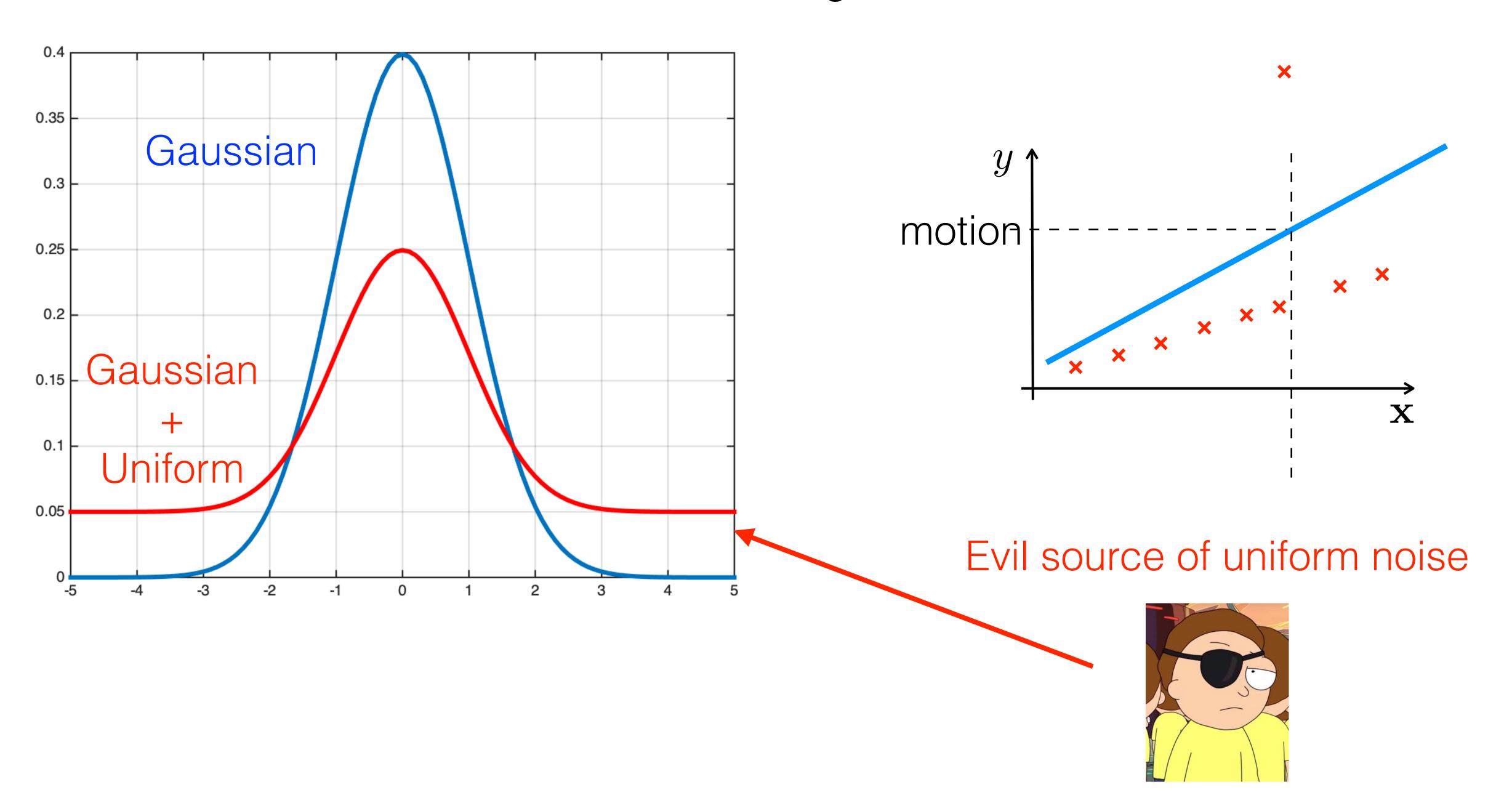
MLE

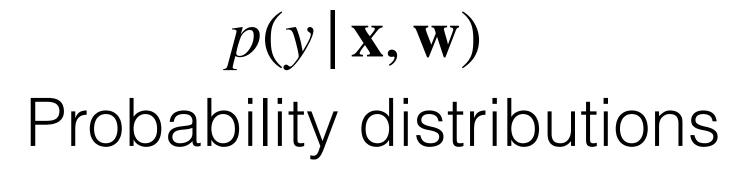
LSQ

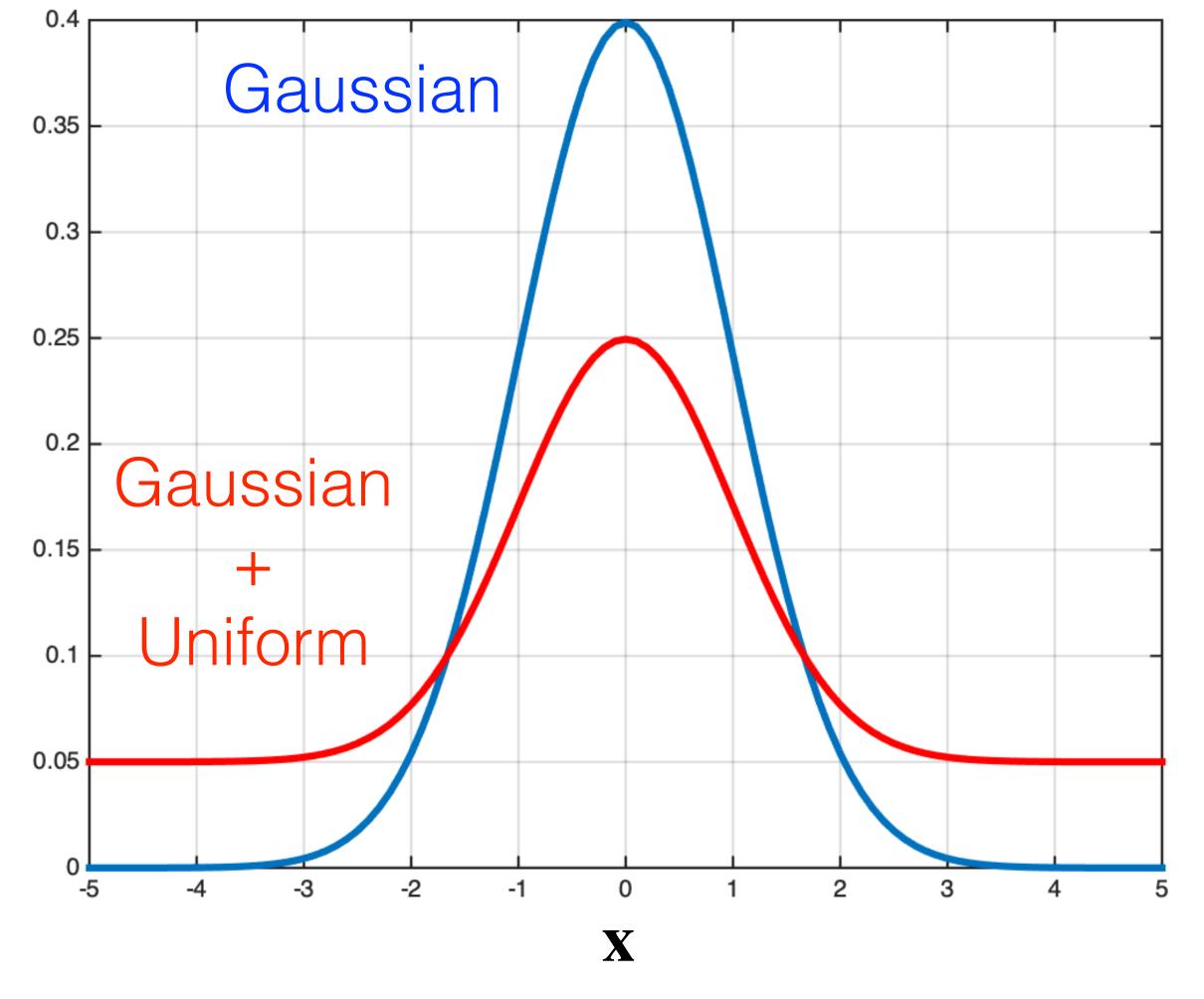
What can go wrong: inappropriate choice of loss function



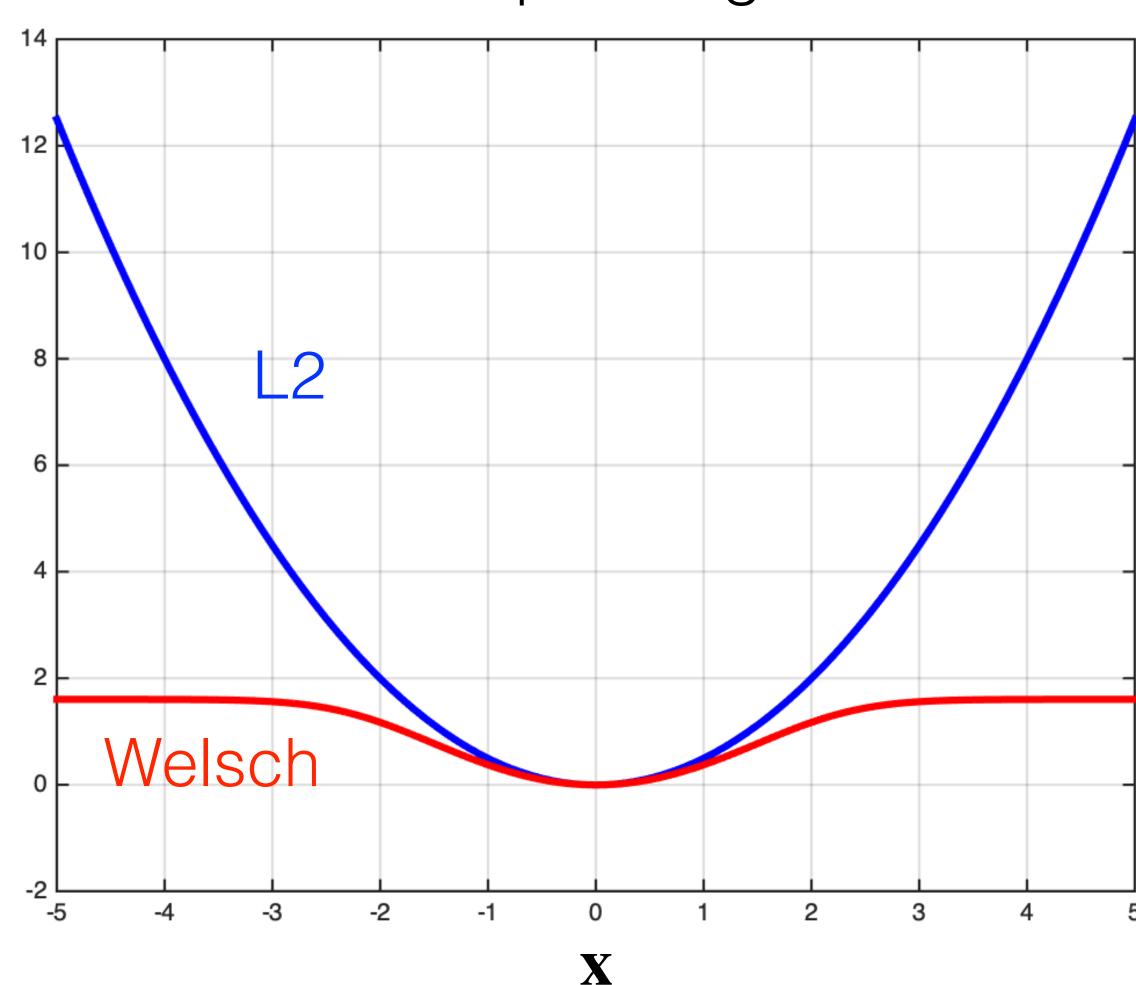








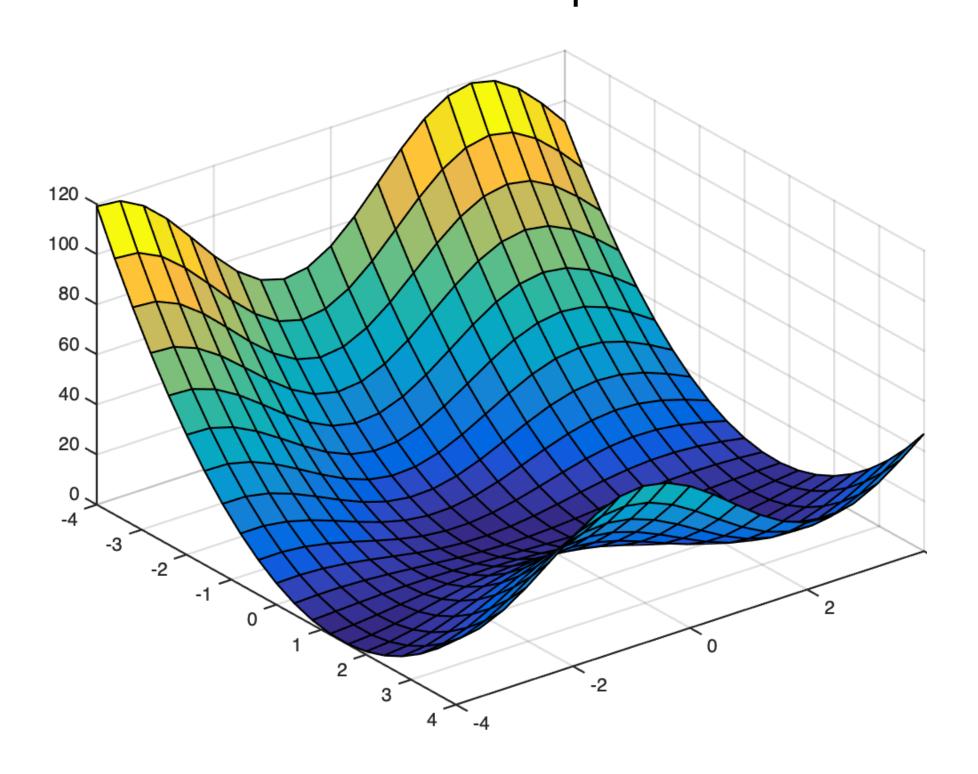
$\mathcal{L}(\mathbf{w}) = -\log(p(y|\mathbf{x}, \mathbf{w}))$ Corresponding losses





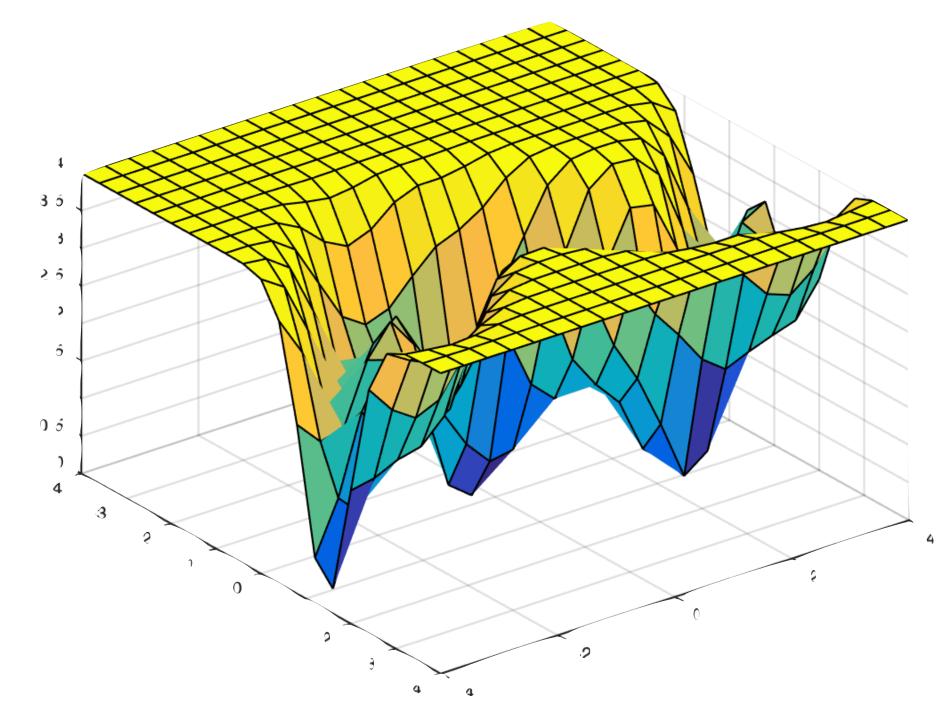


Welsch landscape





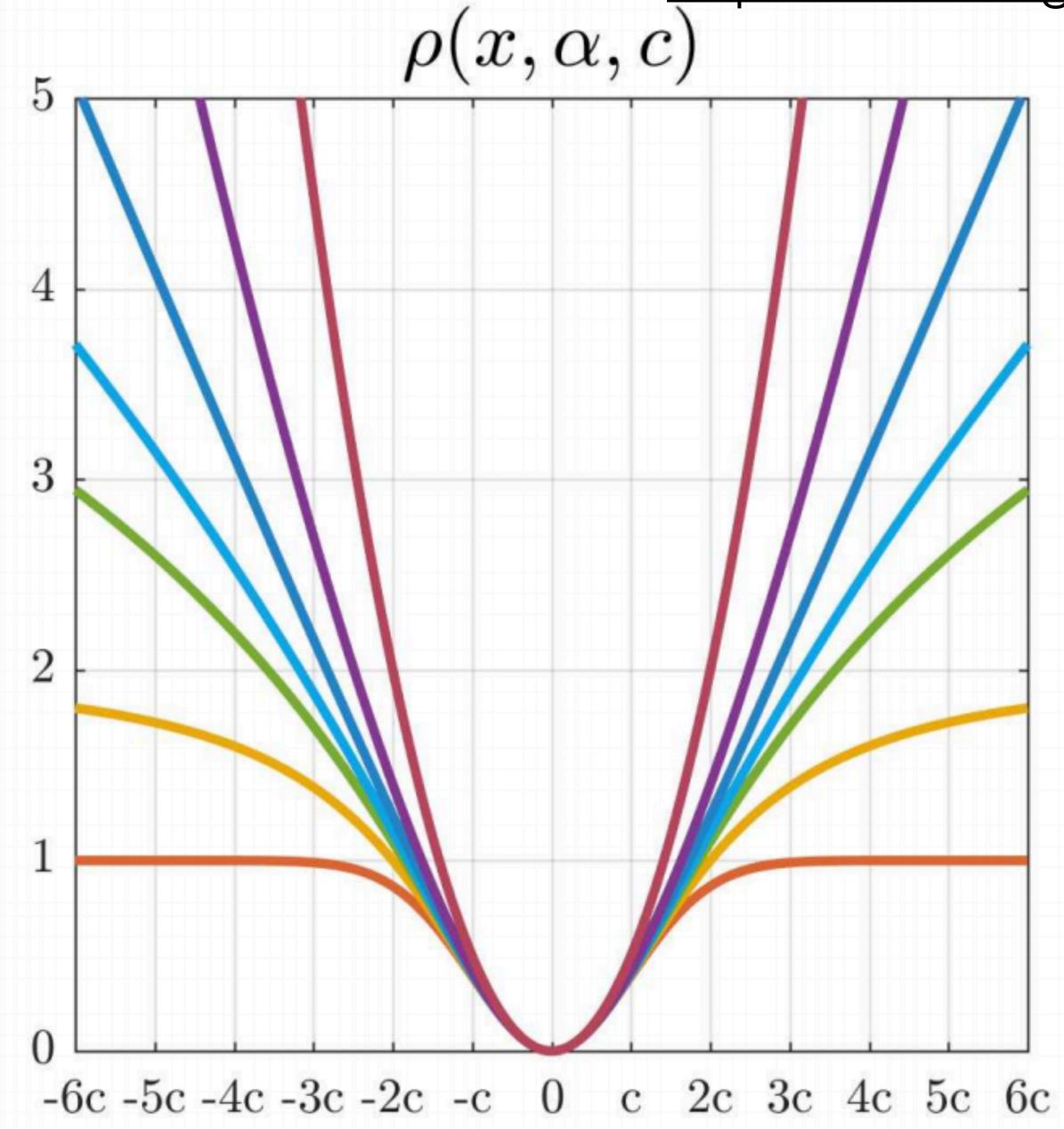
- => GD-friendly landscape
- Gradient size encodes distance
- Easy to optimize



Uniform noise modelled

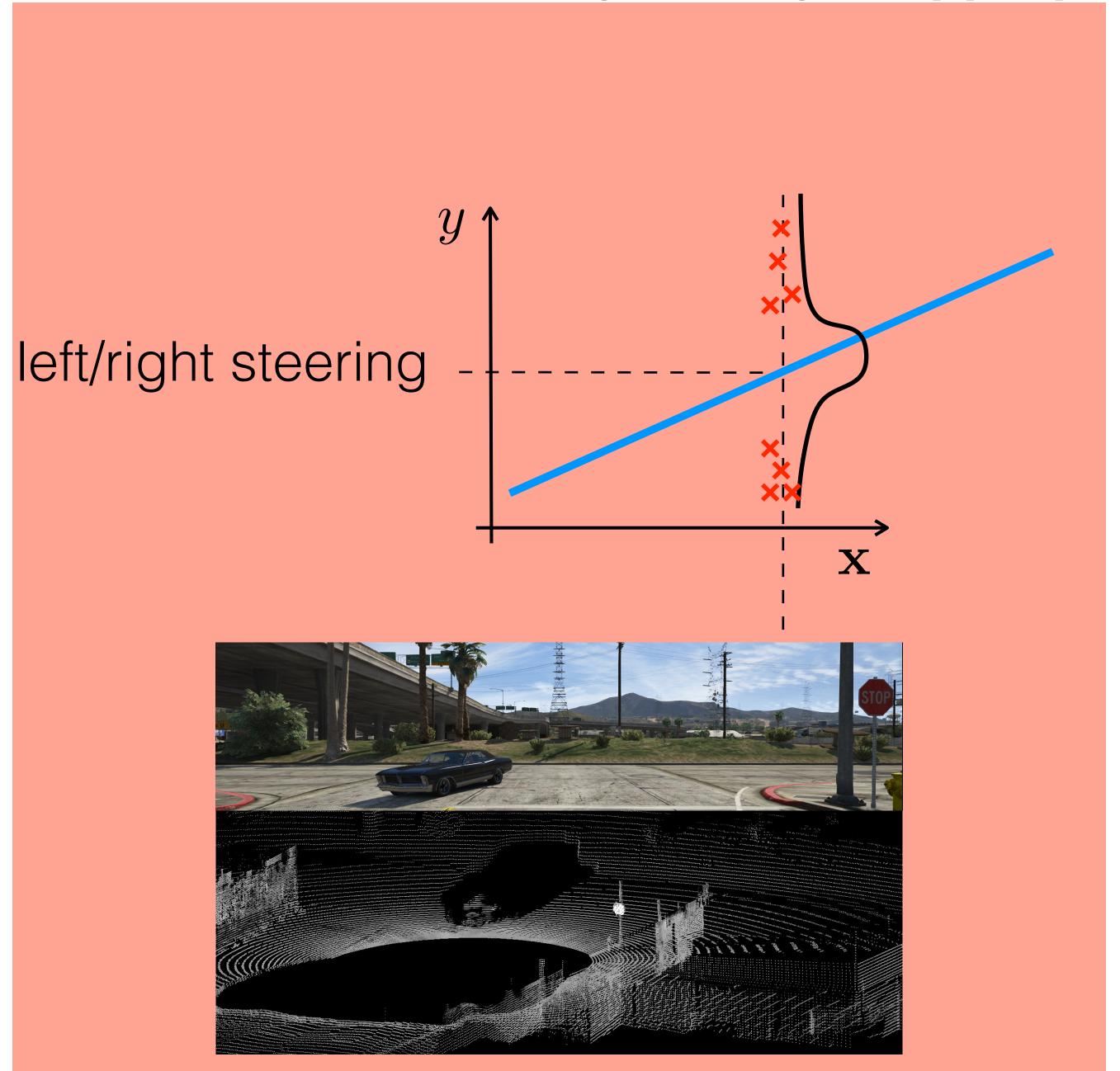
- => unfriendly landscape
- Non-convex: Large narrow plateaus with zero gradient
- Good initialization required

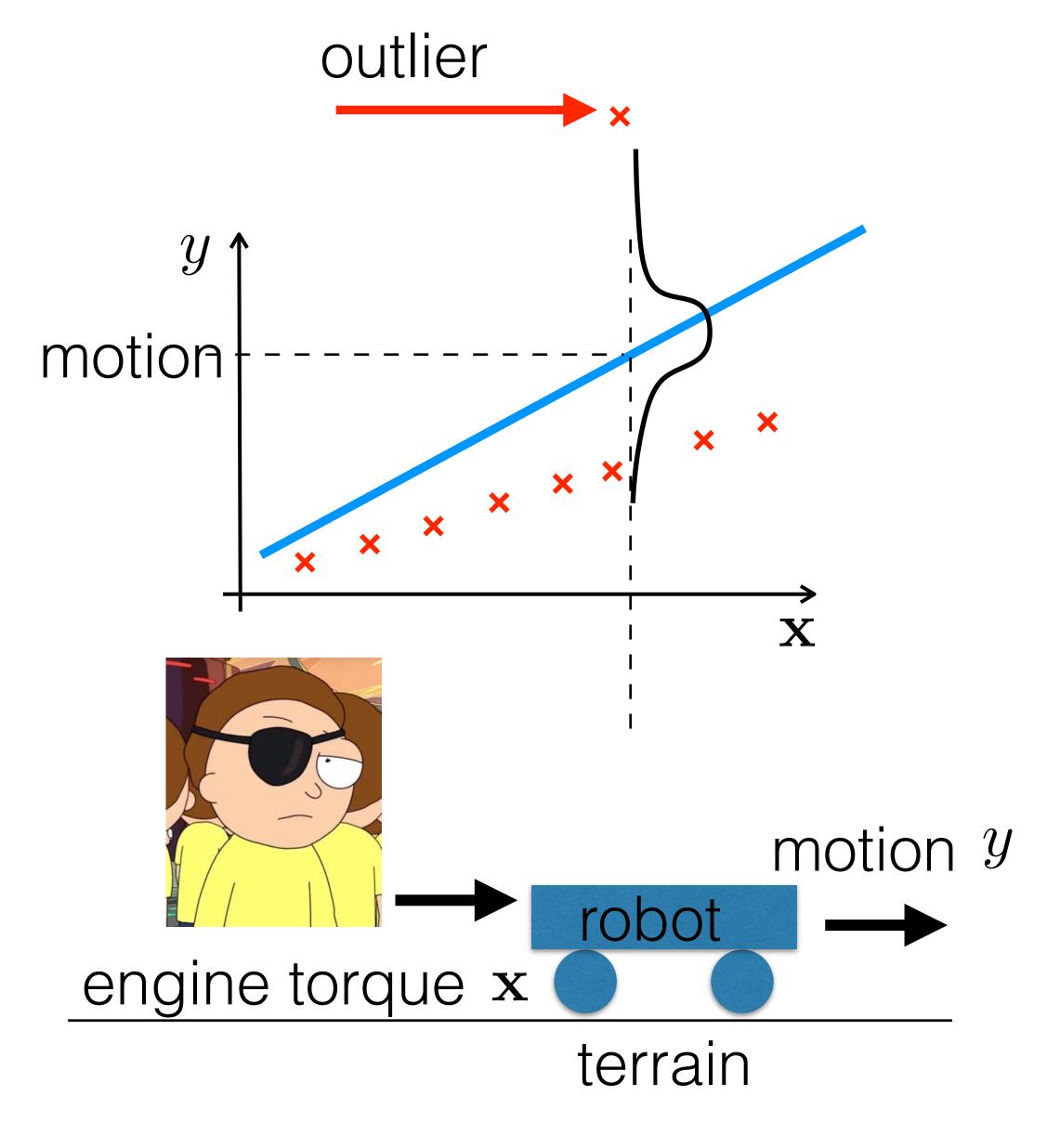
Shape of robust regression functions [Barron CVPR 2019] https://arxiv.org/abs/1701.03077 $\rho(x,\alpha,c)$



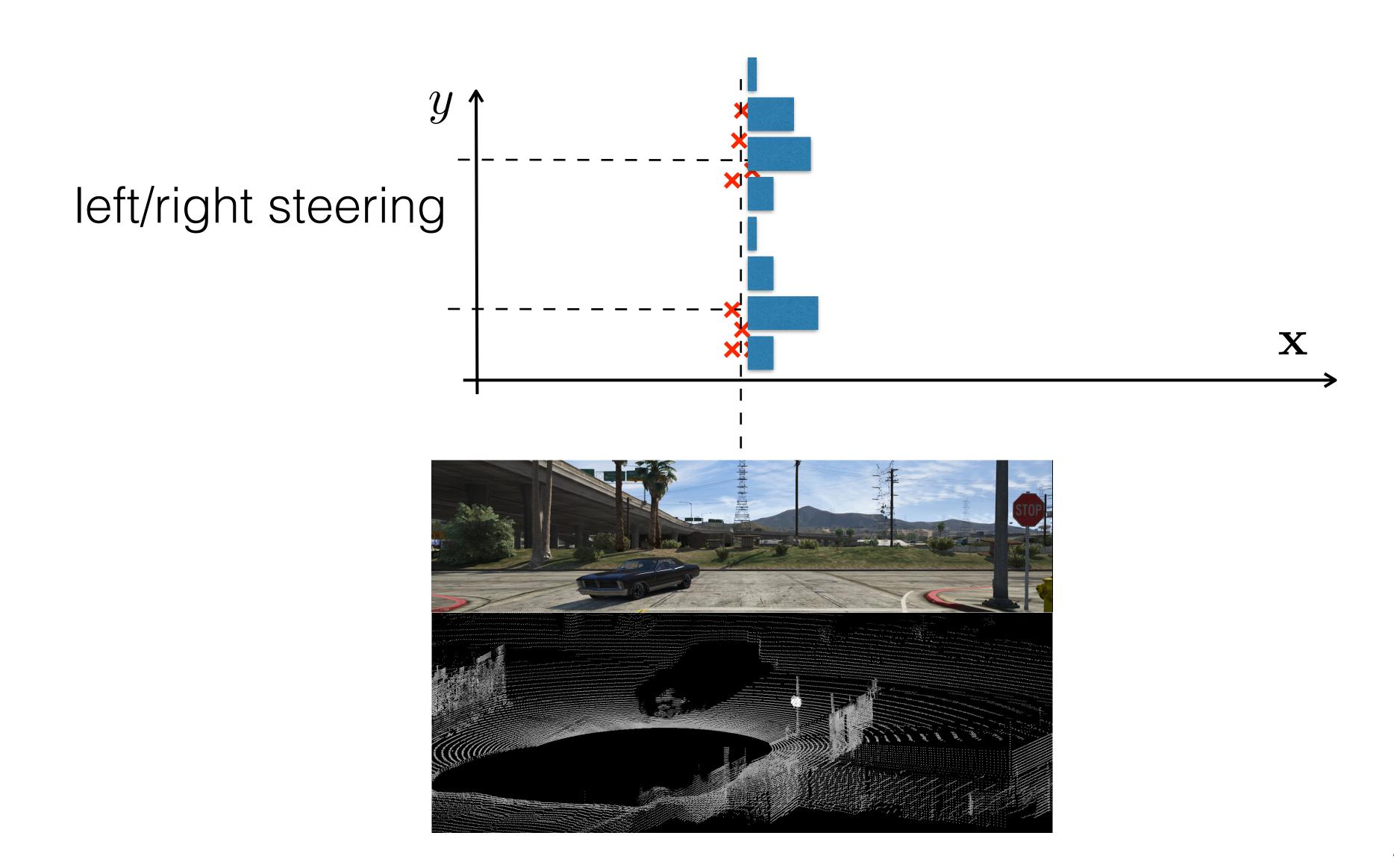
$$ho\left(x,lpha,c
ight)=rac{|lpha-2|}{lpha}\left(\left(rac{\left(x/c
ight)^2}{|lpha-2|}+1
ight)^{lpha/2}-1
ight)$$

What can go wrong: inappropriate choice of loss function

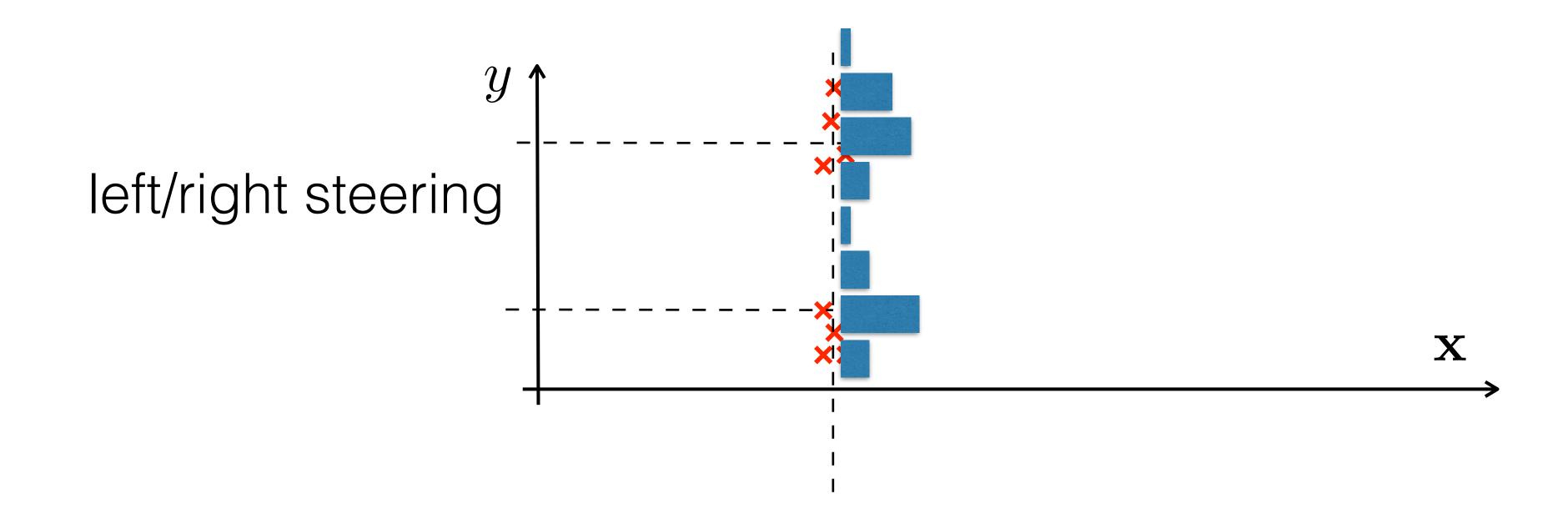




Work-around 1: discretize y-domain and treat the problem as classification



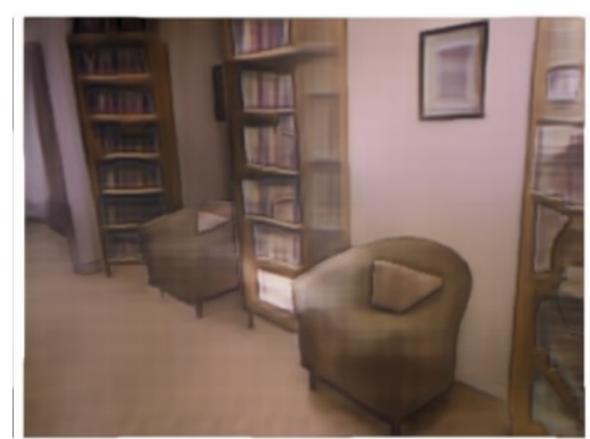
Work-around 1: discretize y-domain and treat the problem as classifcation

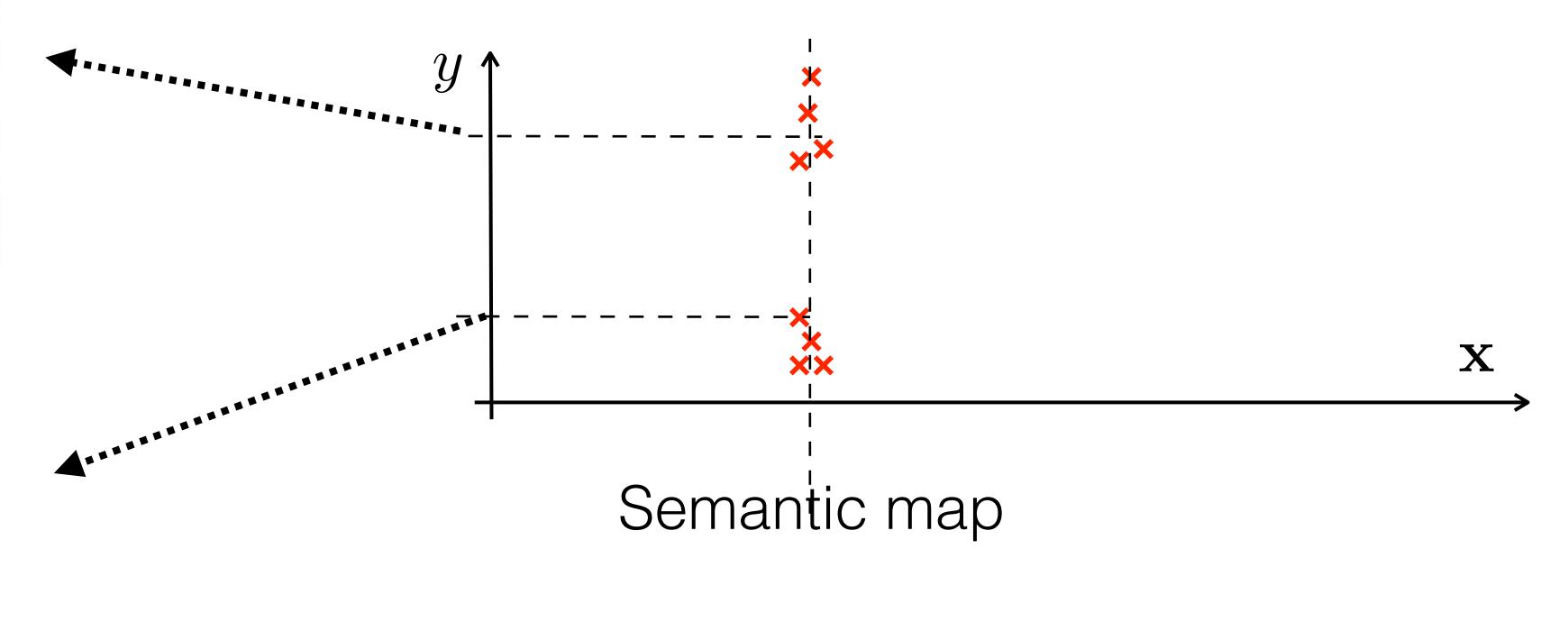


Works reasonably for low-dim y





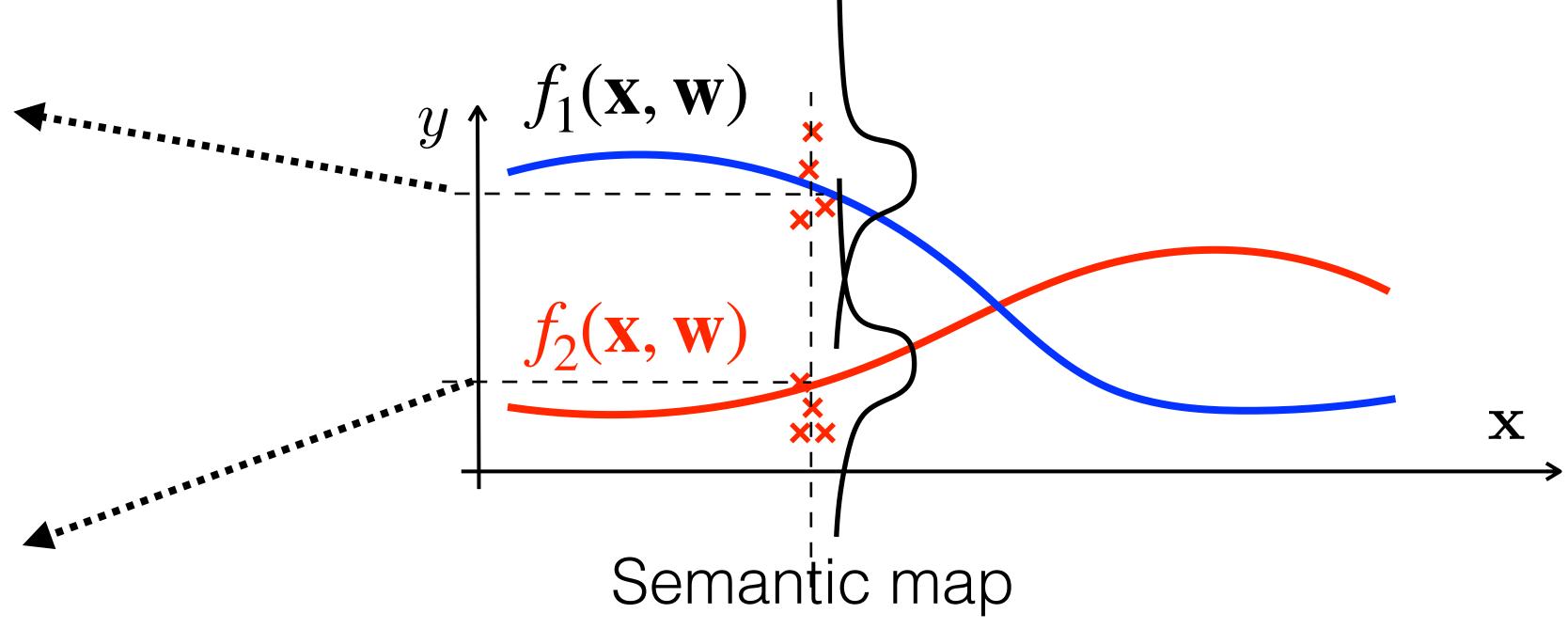




What if y are images?

Work-around 2: allow multiple hypothesis





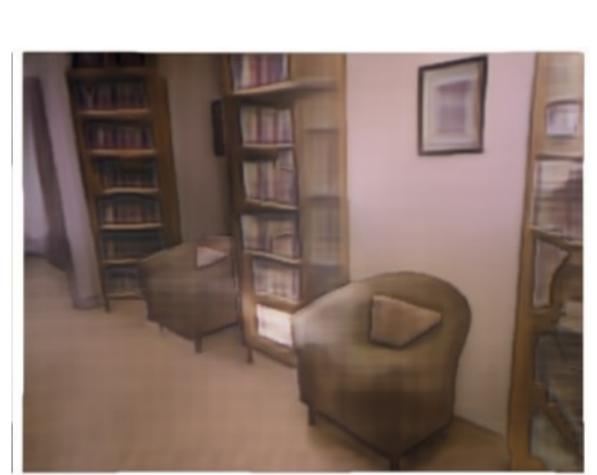


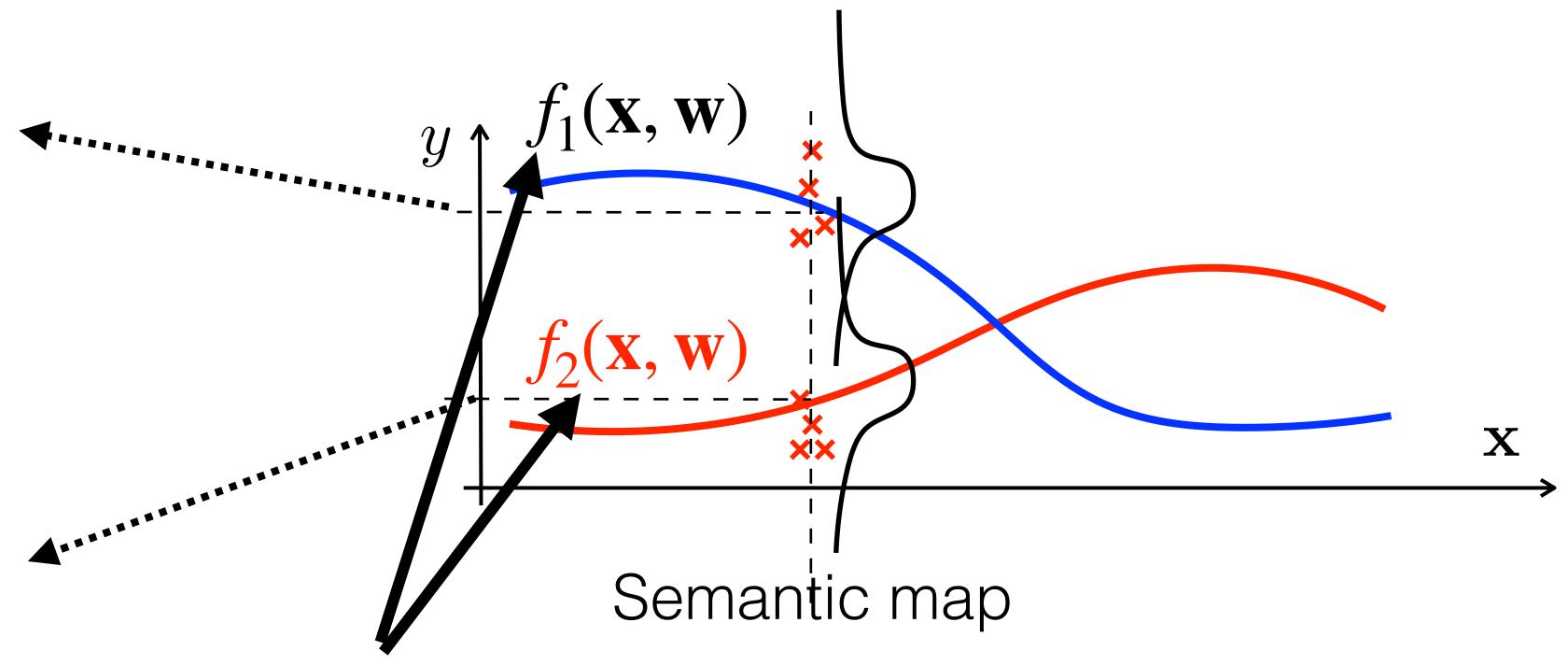
Multiple choice loss [Microsoft, NIPS, 2012], [Koltun, ICCV, 2017]

$$\mathcal{L}(\mathbf{w}) = \min_{i} \|f_i(\mathbf{x}, \mathbf{w}) - y\|$$

Work-around 2: allow multiple hypothesis







Problem 1: number of hypothesis may grow exponentially

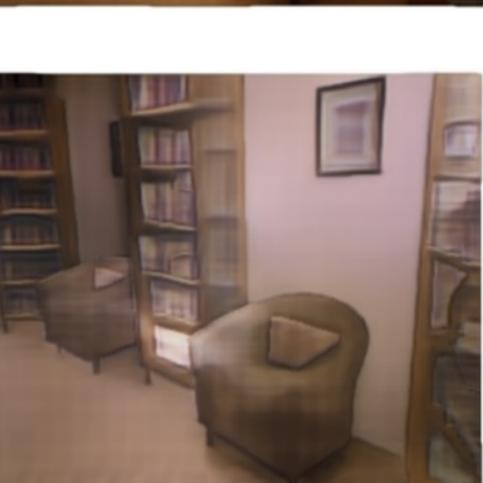
Multiple choice loss [Microsoft, NIPS, 2012], [Koltun, ICCV, 2017]

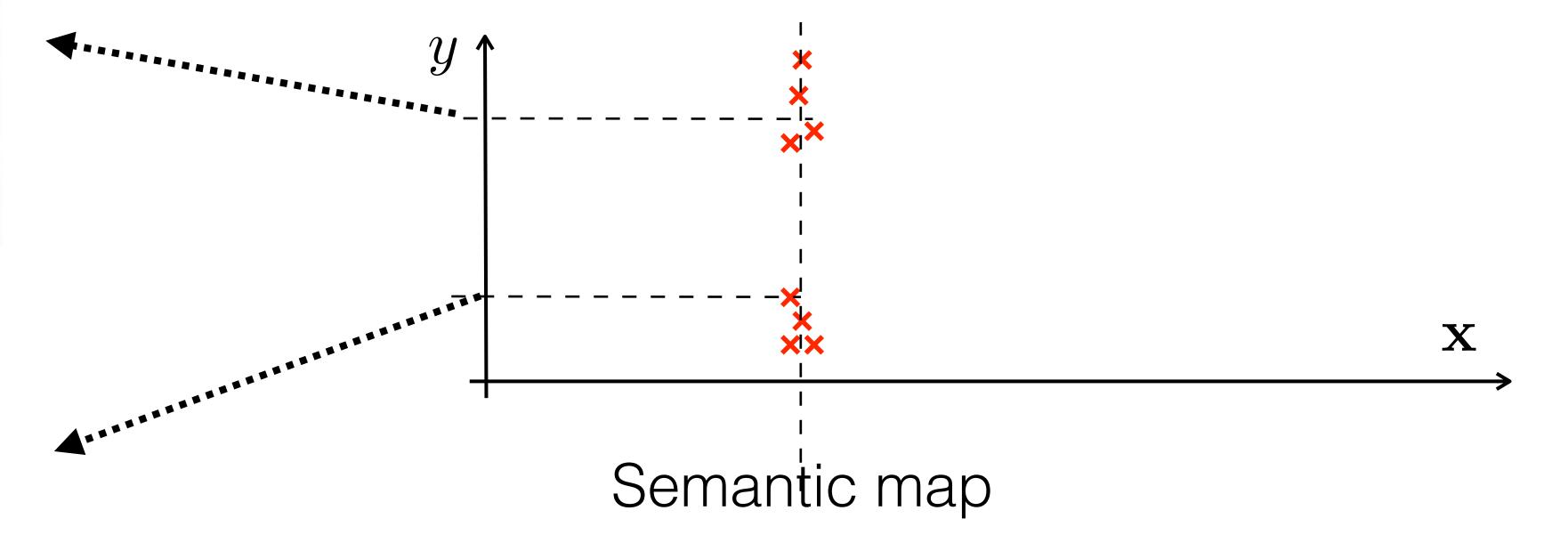
$$\mathcal{L}(\mathbf{w}) = \min_{i} \|f_i(\mathbf{x}, \mathbf{w}) - \mathbf{y}\|$$

Work-around 3: Conditional Generative Adversarial Networks





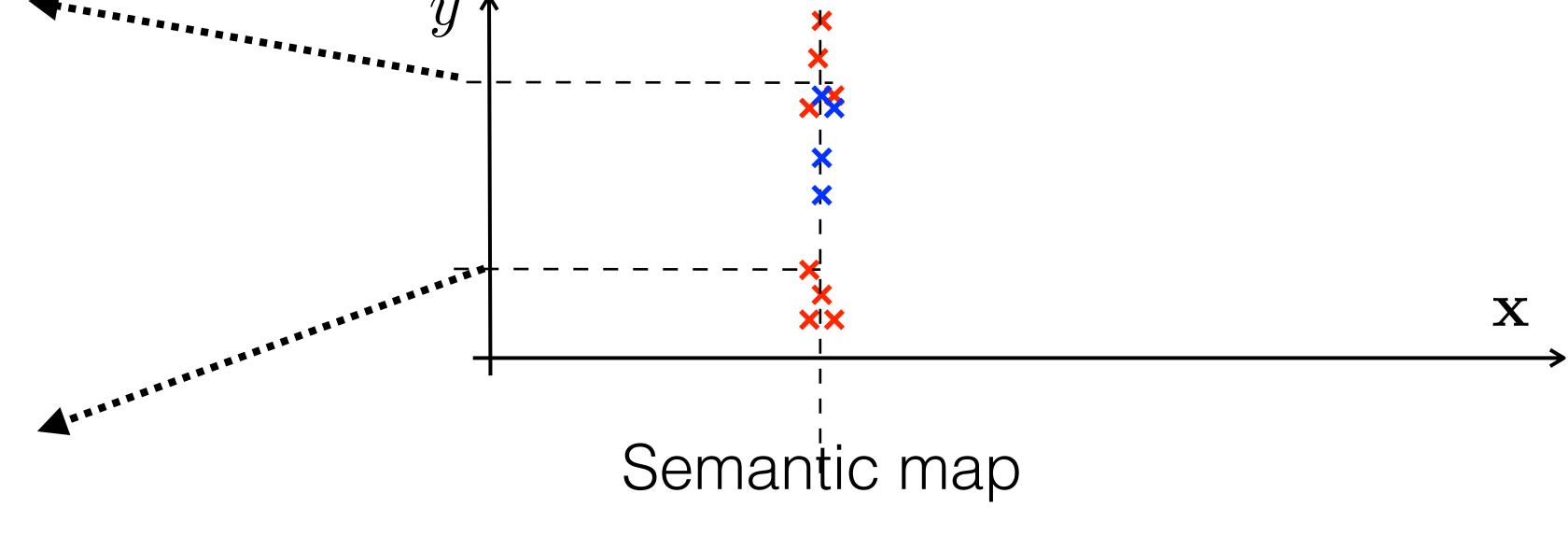




Work-around 3: Conditional Generative Adversarial Networks









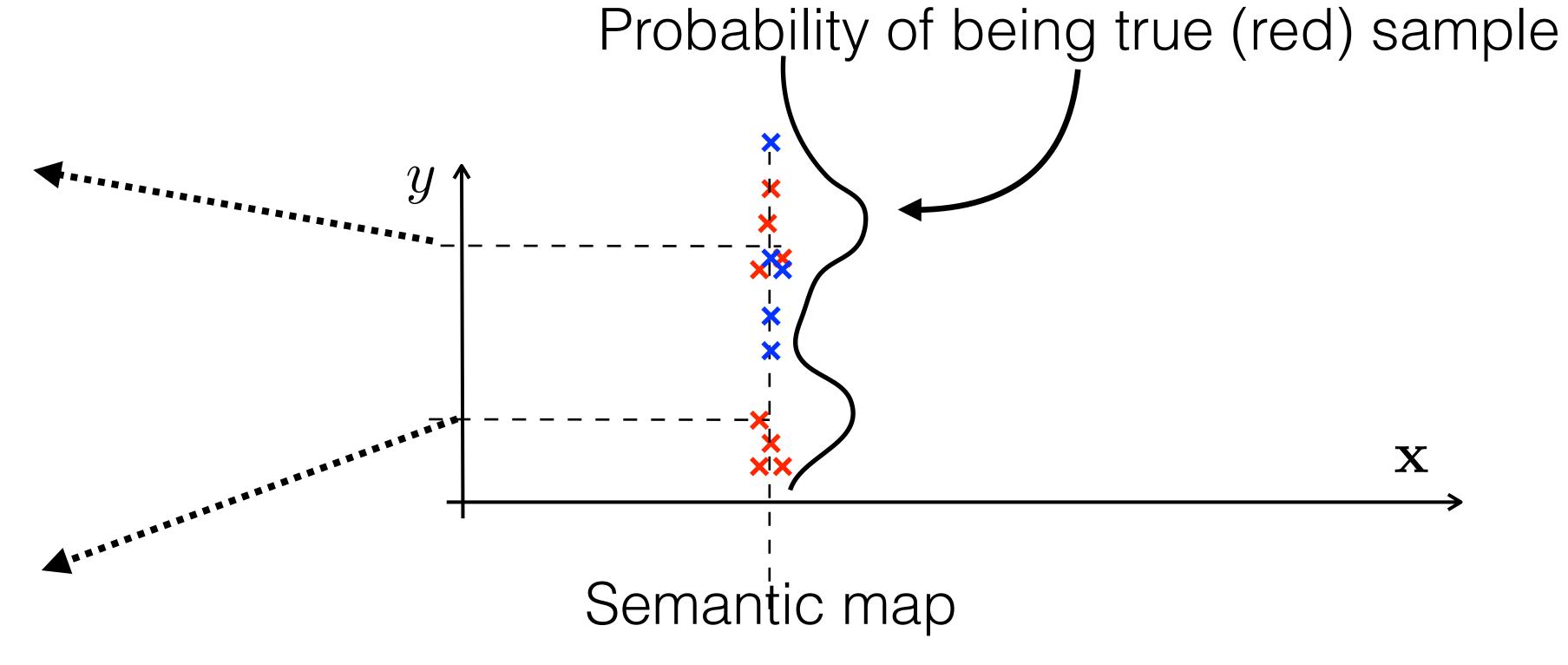
(1) Define generative model that generates blue samples (net with injected noise)

Work-around 3: Conditional Generative Adversarial Networks

Problem 2: Measuring similarity of images









- (1) Define **generative model** that generates blue samples (net with injected noise)
- (2) Learn discriminator (i.e. 2-class classifier that discriminate blue from red)

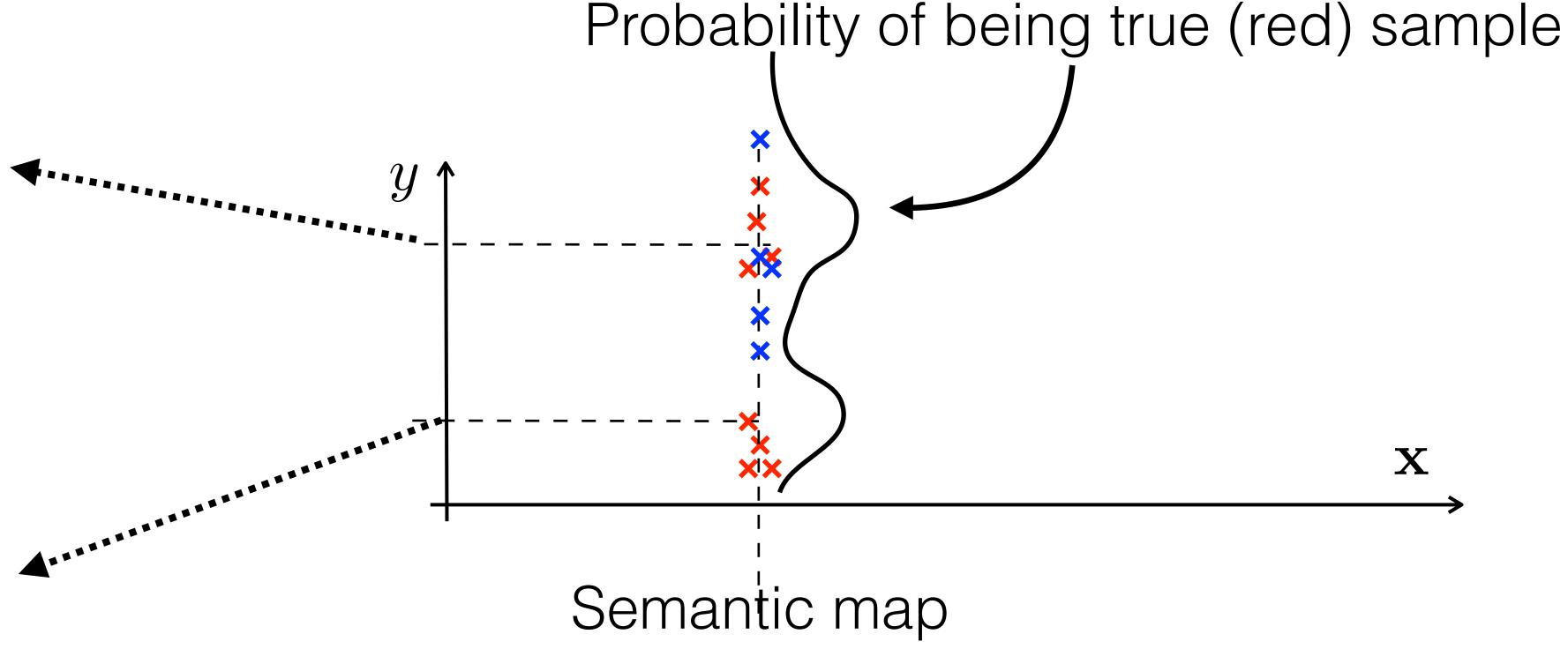
Work-around 3: Conditional Generative Adversarial Networks

Problem 2: Measuring similarity of images









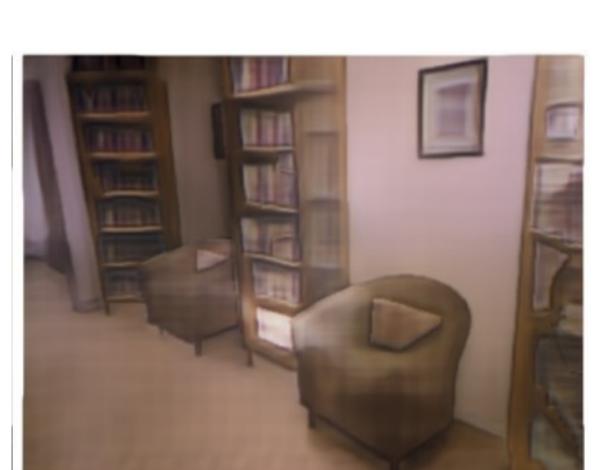
- (1) Define generative model that generates blue samples (net with injected noise)
- (2) Learn discriminator (i.e. 2-class classifier that discriminate blue from red)
- (3) Learn the blue sample generator to maximize discriminative loss (fool discrimin.)

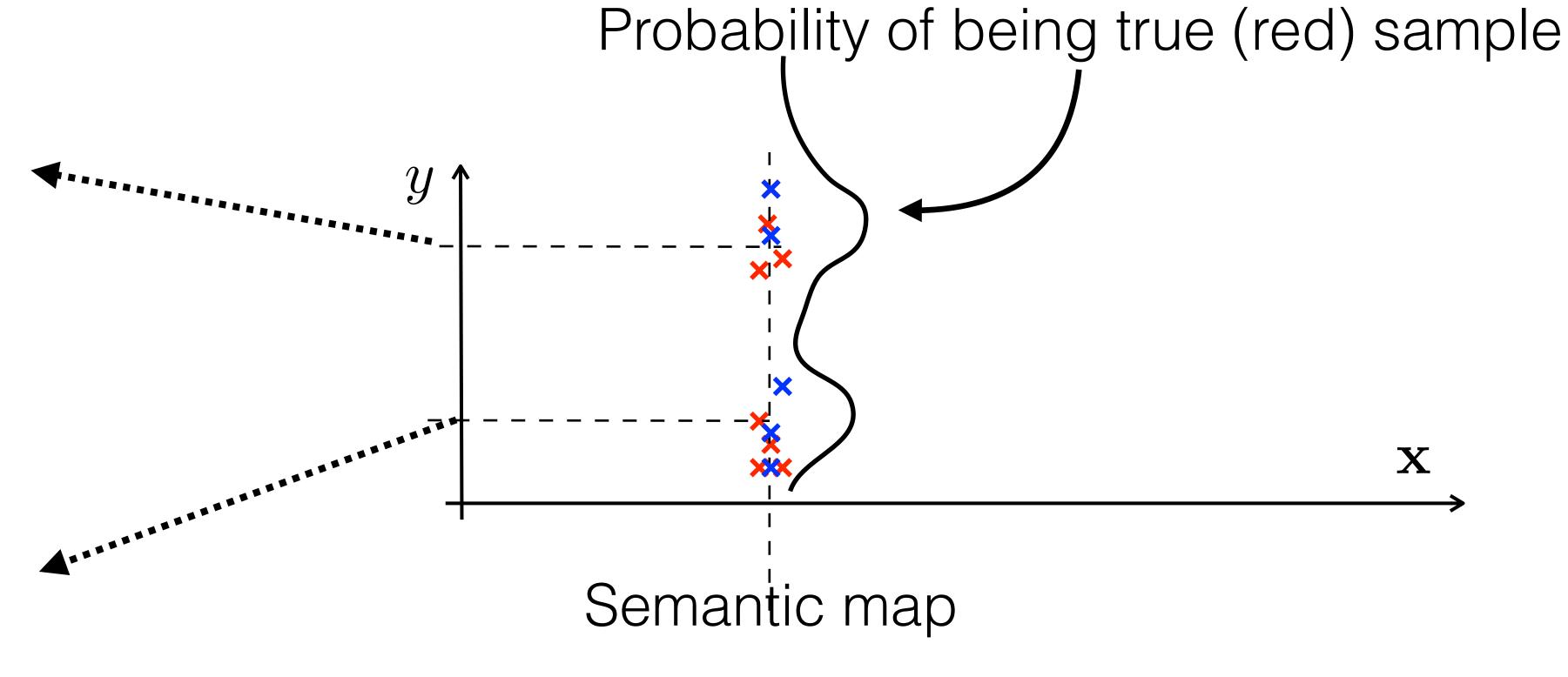
Work-around 3: Conditional Generative Adversarial Networks

Problem 2: Measuring similarity of images









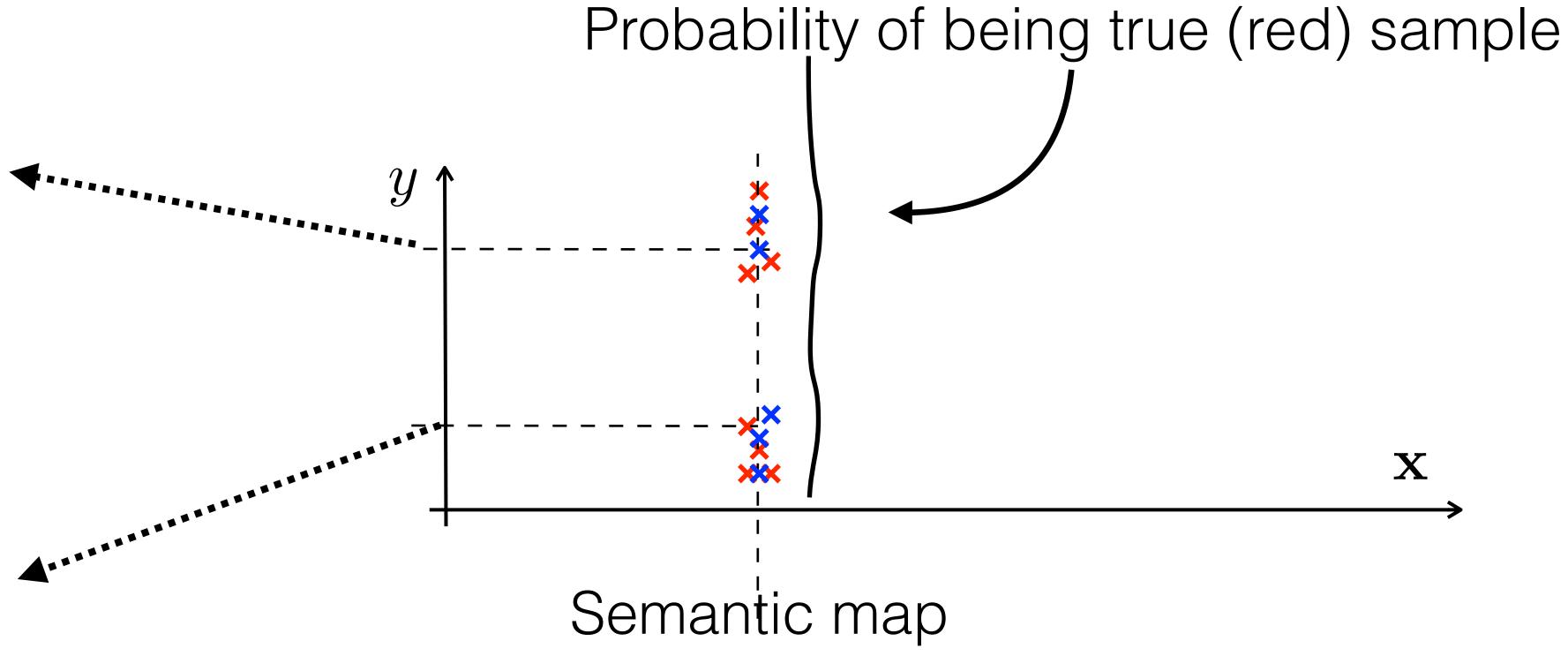
- (1) Define generative model that generates blue samples (net with injected noise)
- (2) Learn discriminator (i.e. 2-class classifier that discriminate blue from red)
- (3) Learn the blue sample generator to maximize discriminative loss (fool discrimin.)

Work-around 3: Conditional Generative Adversarial Networks

Problem 2: Measuring similarity of images







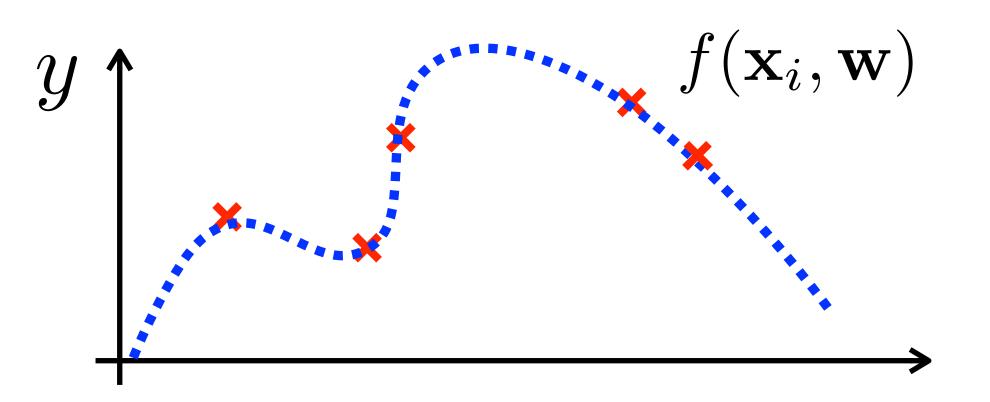


- (1) Define **generative model** that generates blue samples (net with injected noise)
- (2) Learn discriminator (i.e. 2-class classifier that discriminate blue from red)
- (3) Learn the blue sample generator to maximize discriminative loss (fool discrimin.)

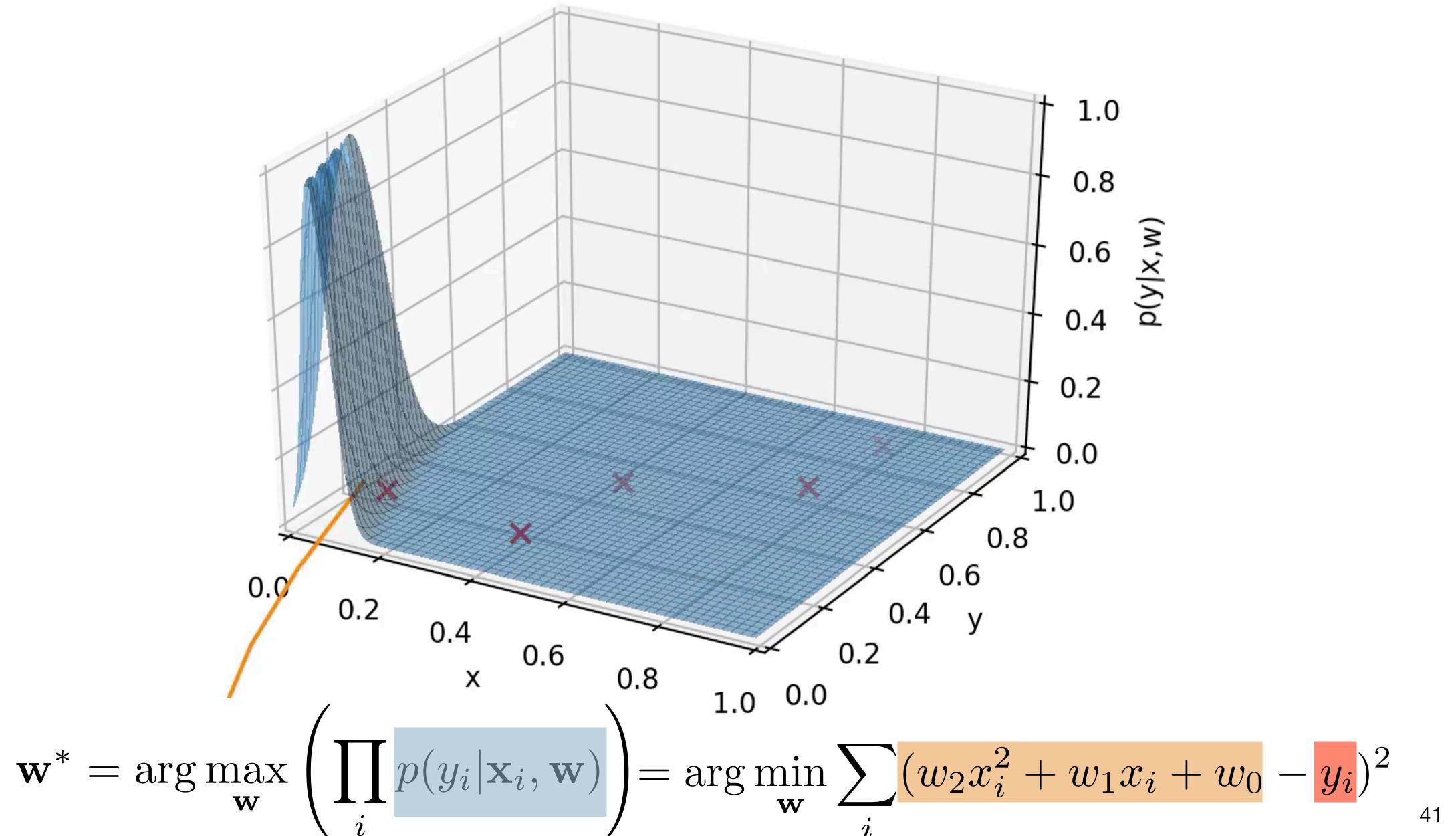
Iterate

$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_i -\log(p(y_i|\mathbf{x}_i,\mathbf{w})) \right)$$
 log likelihood prior/regulariser

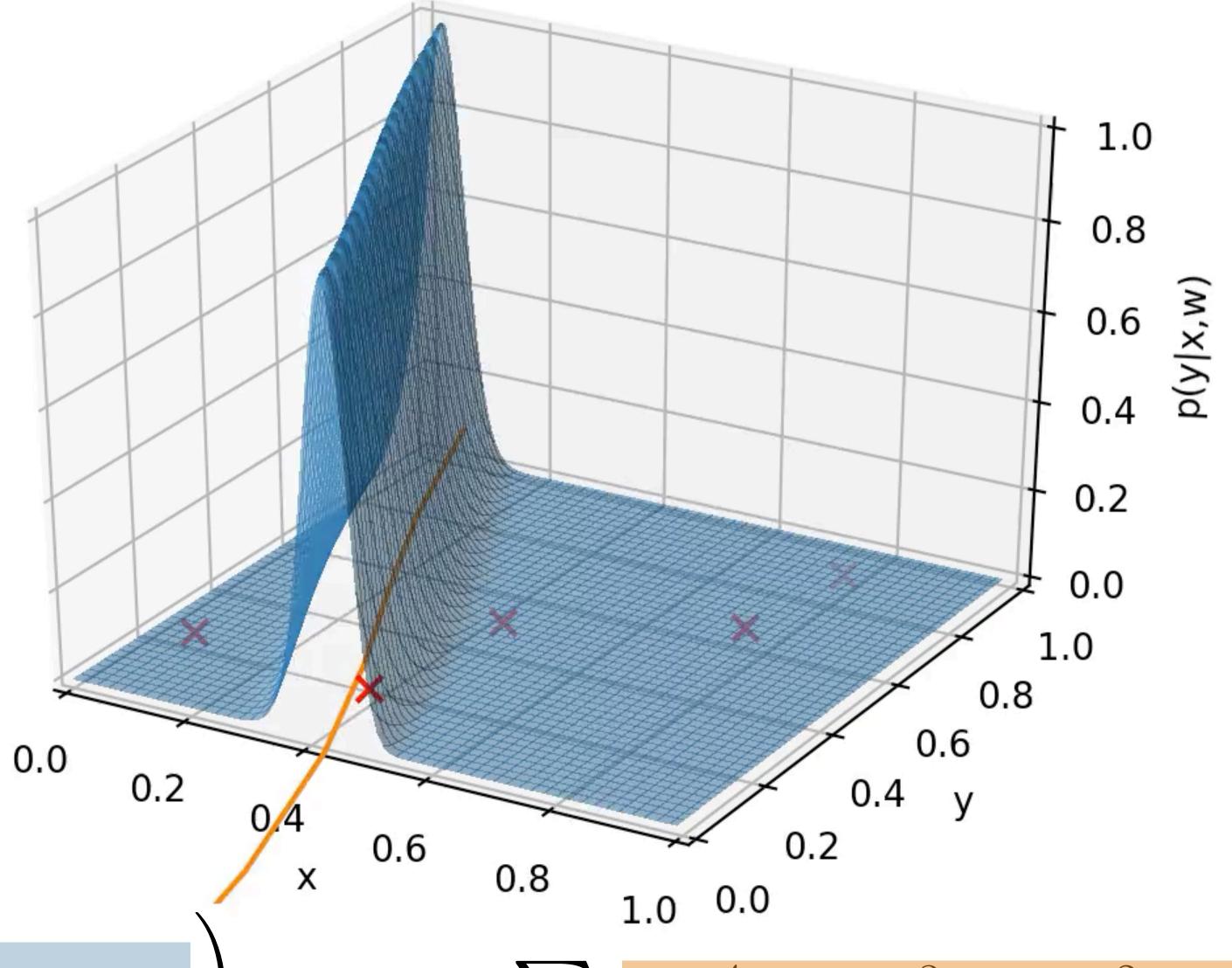
no prior, powerful class of f, learner is oraculum => zero trn error + overfitting



$p(y|\mathbf{x}, \mathbf{w}) \sim \mathcal{N}_y(w_2 x^2 + w_1 x + w_0, \sigma^2)$

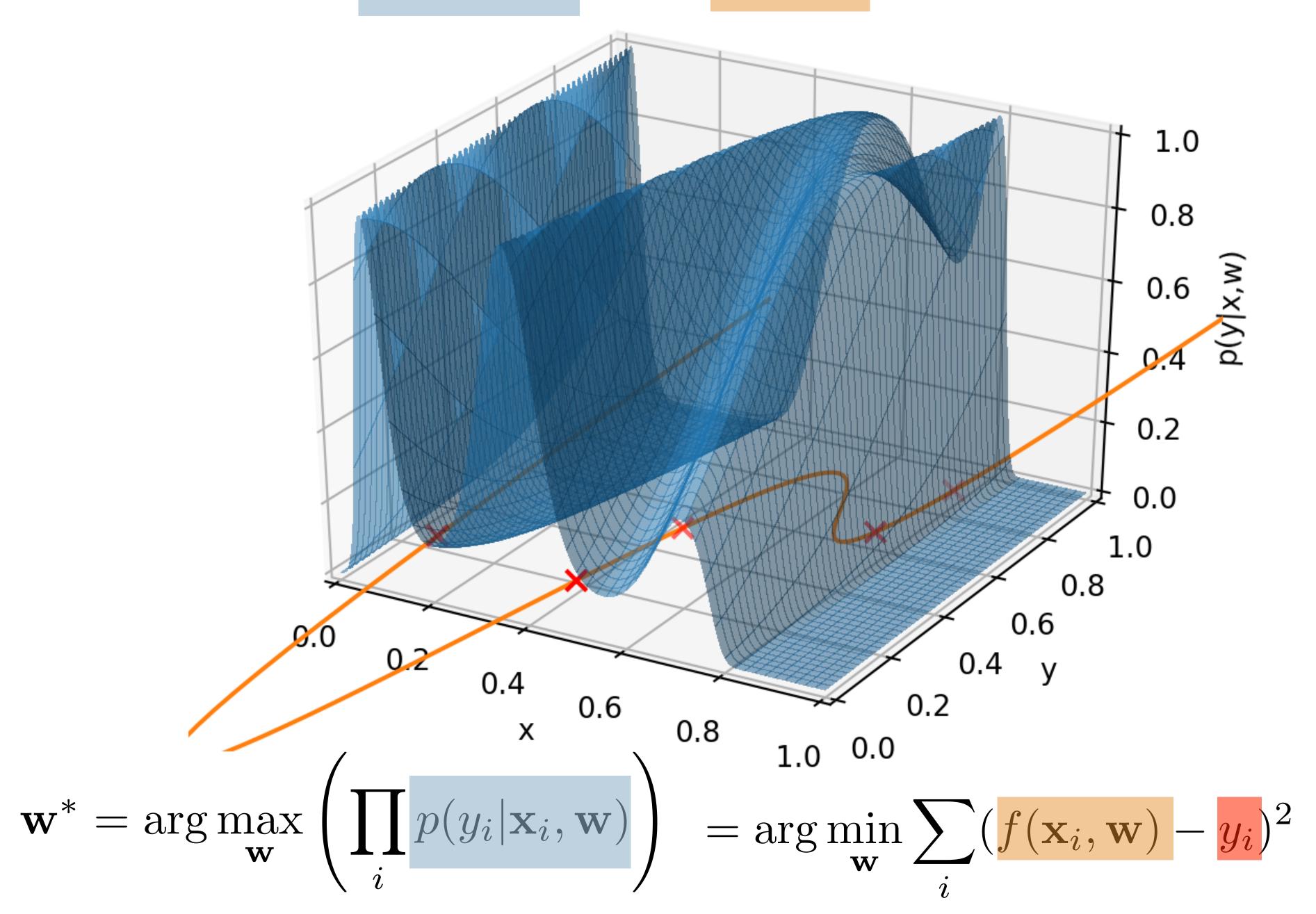




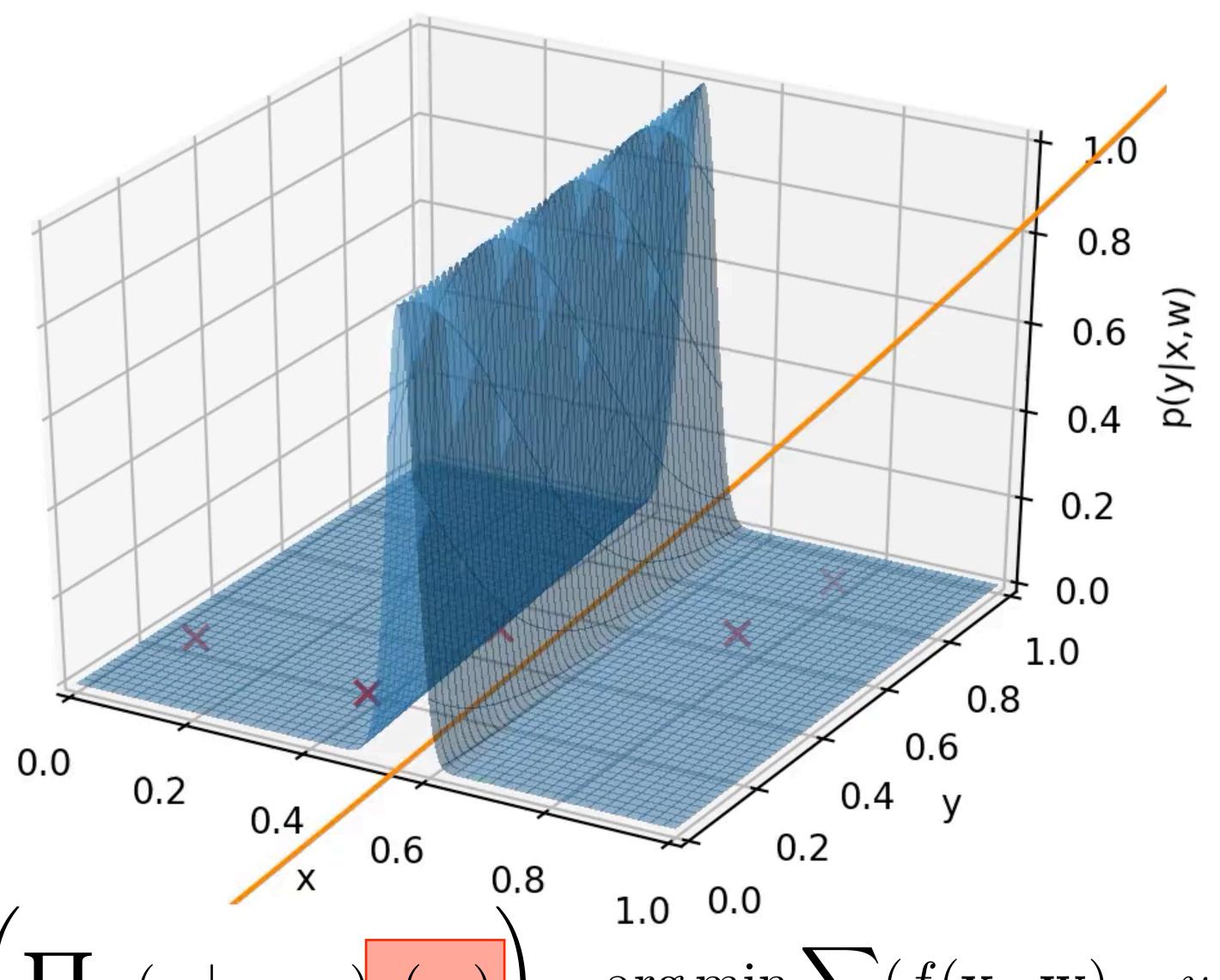


$$\mathbf{w}^* = \arg\max_{\mathbf{w}} \left(\prod_i \frac{p(y_i|\mathbf{x}_i, \mathbf{w})}{\mathbf{v}^*} \right) = \arg\min_{\mathbf{w}} \sum_i (\frac{w_4 x_i^4 + w_3 x_i^3 + w_2 x_i^2 + w_1 x_i + w_0}{42} - \frac{\mathbf{y}_i}{42})^2$$

$p(y|\mathbf{x},\mathbf{w}) \sim \mathcal{N}_y(f(\mathbf{x},\mathbf{w}),\sigma^2)$

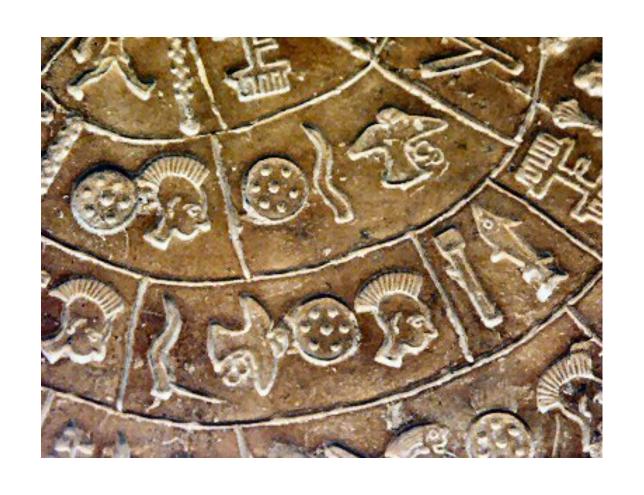


$$p(y|\mathbf{x}, \mathbf{w}) \sim \mathcal{N}_y(f(\mathbf{x}, \mathbf{w}), \sigma^2)$$
 $p(\mathbf{w}) \sim \mathcal{N}_w(\mathbf{0}, \sigma^2)$



$$\mathbf{w}^* = \arg\max_{\mathbf{w}} \left(\prod_{i} p(y_i | \mathbf{x}_i, \mathbf{w}) p(\mathbf{w}) \right) = \arg\min_{\mathbf{w}} \sum_{i} (f(\mathbf{x}_i, \mathbf{w}) - y_i)^2 + \mathbf{w}^\top \mathbf{w}$$

Phaistos disc

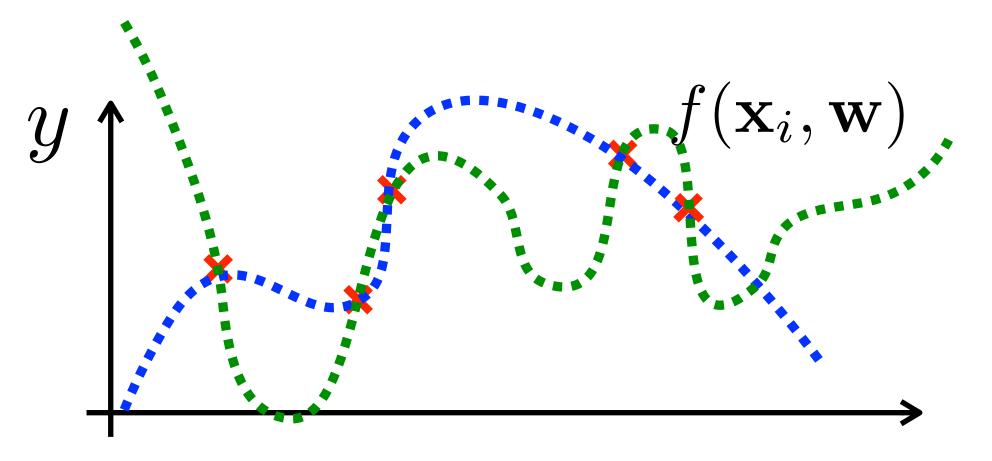




Unicode

PHAISTOS DISC SIGN PEDESTRIAN 101D1 PHAISTOS DISC SIGN PLUMED HEAD 101D2 PHAISTOS DISC SIGN TATTOOED HEAD 101D3 PHAISTOS DISC SIGN CAPTIVE PHAISTOS DISC SIGN CHILD 101D4 101D5 PHAISTOS DISC SIGN WOMAN 101D6 PHAISTOS DISC SIGN HELMET 101D7 PHAISTOS DISC SIGN GAUNTLET 101D8 🐧 PHAISTOS DISC SIGN TIARA 101D9 PHAISTOS DISC SIGN ARROW 101DA 🎉 PHAISTOS DISC SIGN BOW 101DB PHAISTOS DISC SIGN SHIELD

no prior, powerful class of f, learner is oraculum => zero trn error + overfitting



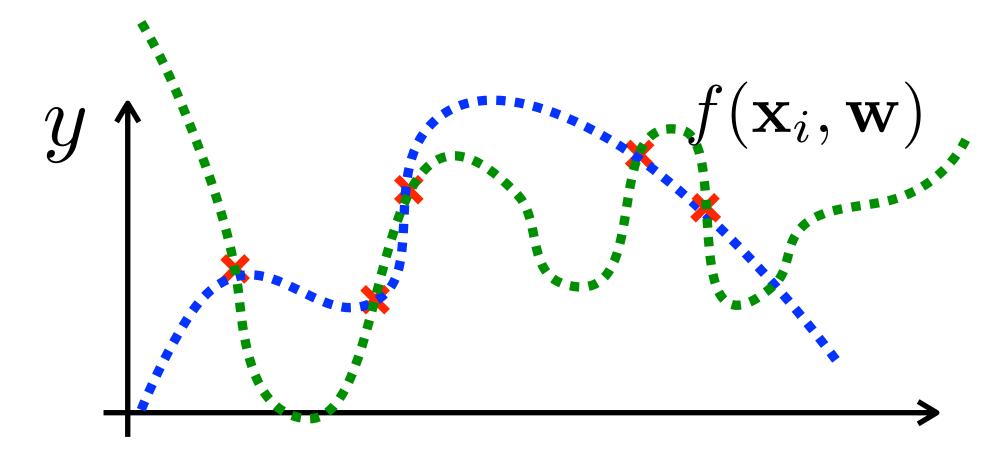
William of Ockham (1287-1347)



Prior is important
leprechauns can be involved in any explanation



no prior, powerful class of f, learner is oraculum => zero trn error + overfitting

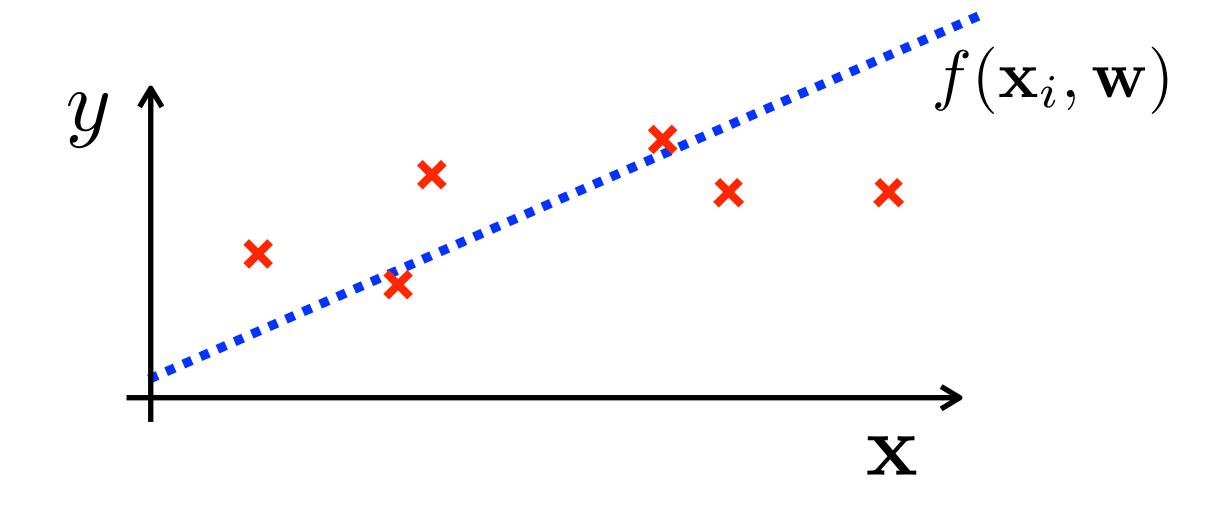


$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + (-\log p(\mathbf{w}))$$

log likelihood

prior/regulariser

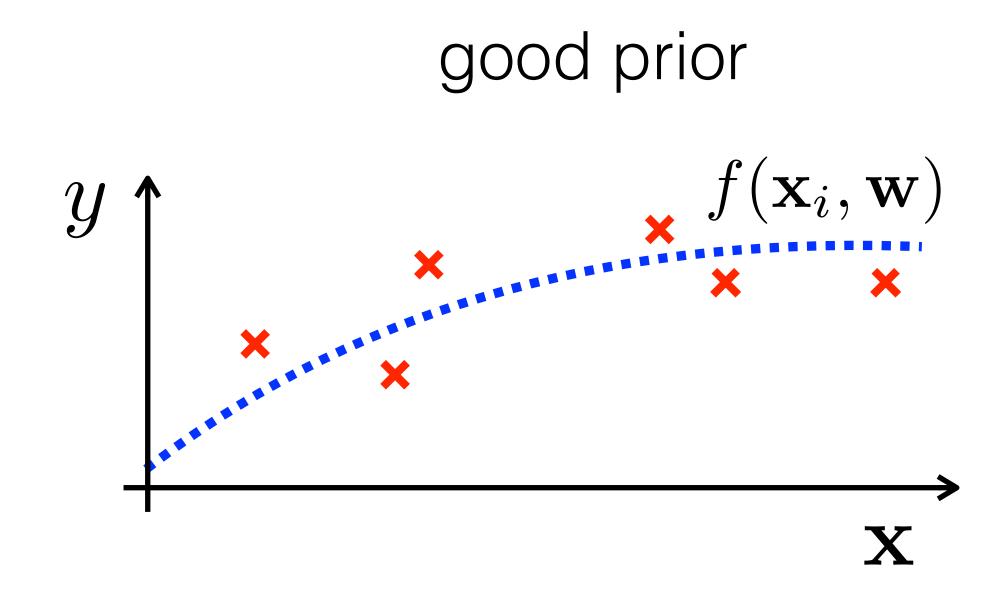
too strong prior, simple f => underfitting



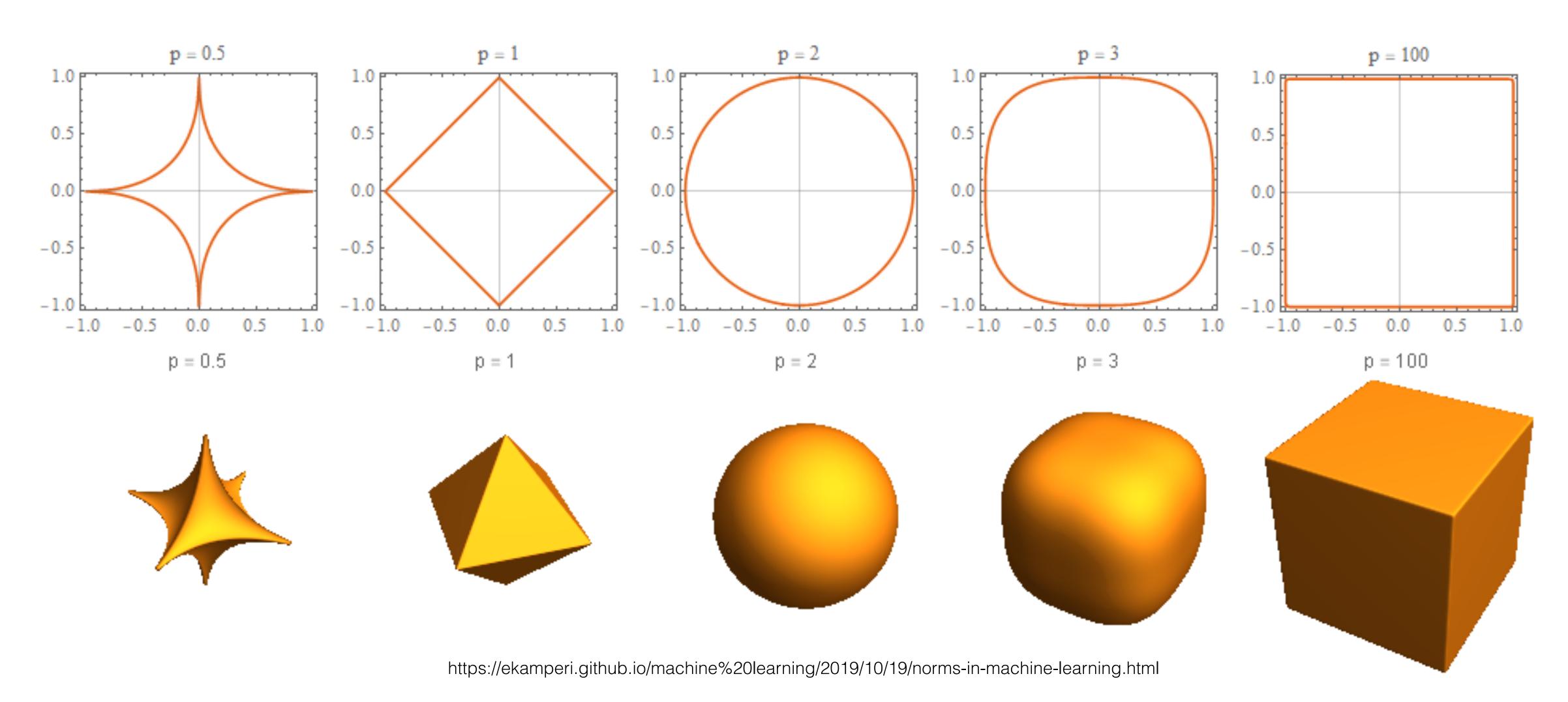
$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + (-\log p(\mathbf{w}))$$

log likelihood

prior/regulariser



Lp-norm:
$$\|x\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{\frac{1}{p}}$$



$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + (-\log p(\mathbf{w}))$$

log likelihood

prior/regulariser

• Gaussian prior $p(\mathbf{w}) = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{\|\mathbf{w}\|_2^2}{2\sigma^2}} = \sum L2\text{-regularization: } \|\mathbf{w}\|_2^2$

It says: the smaller the better (does everyone agree???)

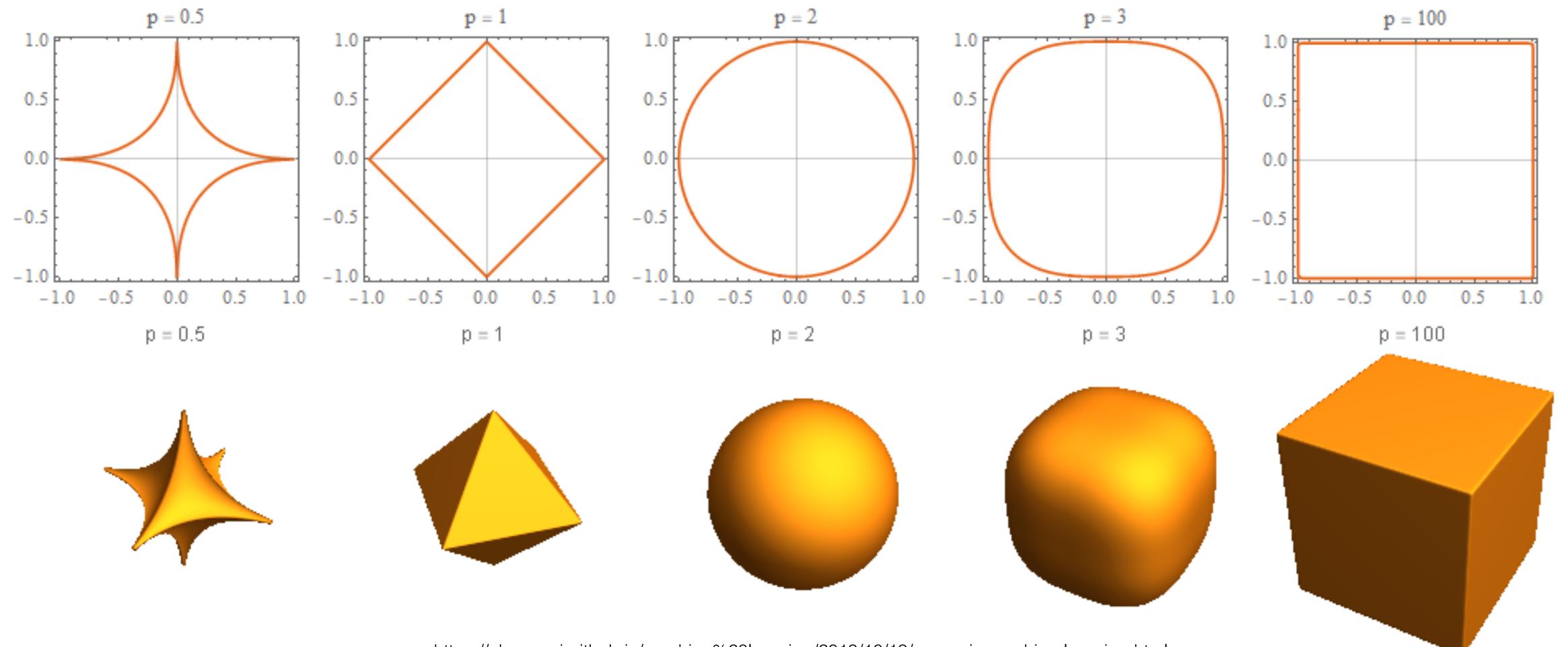
 $\|x\|_p = \left(\sum_{i=1}^n |x_i|^p\right)$

Lp-norm:

Prior is important

Spikes are always good to fight leprechauns





$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + (-\log p(\mathbf{w}))$$

log likelihood

prior/regulariser

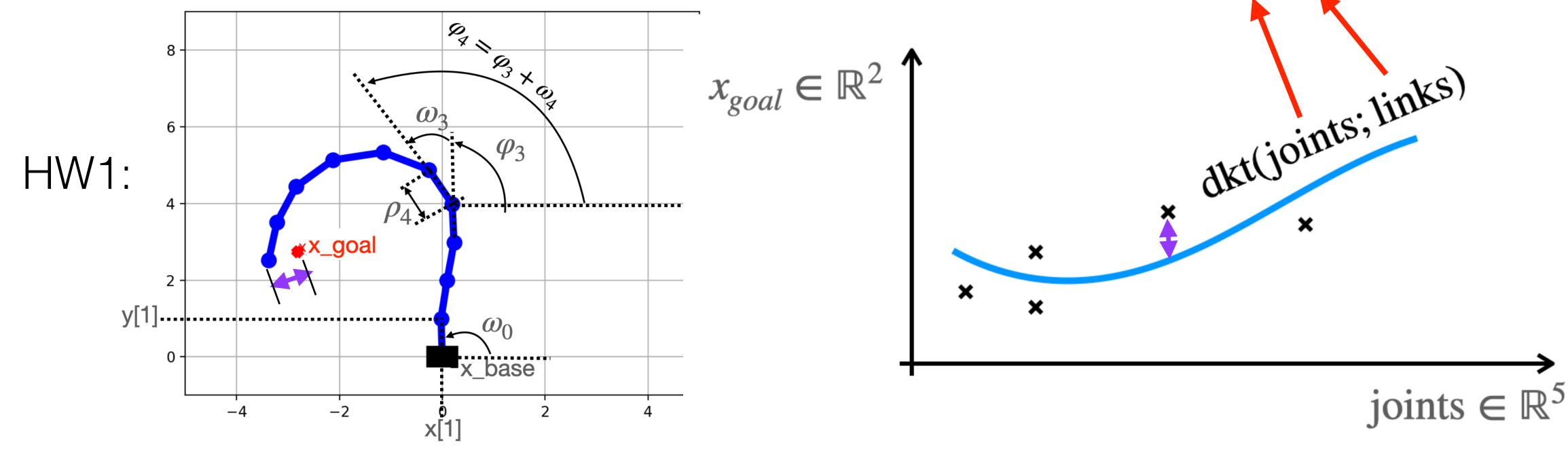
- Gaussian prior $p(\mathbf{w}) = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{\|\mathbf{w}\|_2^2}{2\sigma^2}} > \text{L2-regularization: } \|\mathbf{w}\|_2^2$
 - It says: the smaller the better (does everyone agree???)
- Laplace prior $p(\mathbf{w}) = \frac{1}{2b} e^{(-\frac{|\mathbf{w}|}{b})} => L1$ -regularization: $\|\mathbf{w}\|_1$ It says: the sparser the better
- L2-regression with L1-regularization is known as Lasso
- Interesting way to avoid overfitting is using a weak learner

$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i, \mathbf{w})) \right) + \left(-\log p(\mathbf{w}) \right)$$

log likelihood

prior/regulariser

• Any prior knowledge that restricts the class of functions $f(\mathbf{x}_i, \mathbf{w})$ is $p(\mathbf{w})$



Well restricted class of functions is your fortress, where you hide from leprechauns

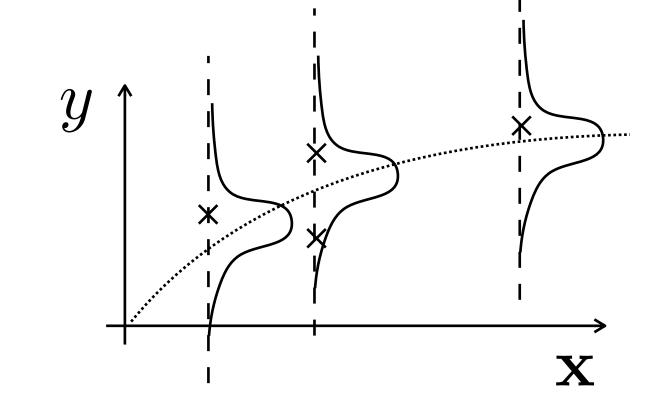
$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i,\mathbf{w})) \right)$$

log likelihood

Regression: ML estimate of cont. unimodal distribution (Gauss, Laplace) with mean in $f(\mathbf{x}, \mathbf{w})$ $p(y|\mathbf{x}, \mathbf{w}) \sim \mathcal{N}_{y}(f(\mathbf{x}, \mathbf{w}), \sigma^{2})$

• Probability of observing y_i when measuring \mathbf{x}_i is

$$p(y_i|\mathbf{x}_i, \mathbf{w}) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(f(\mathbf{x}_i, \mathbf{w}) - y_i)^2}{2\sigma^2}\right)$$



• Training: minimize L2 loss

$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \sum_{i} (f(\mathbf{x}_i, \mathbf{w}) - y_i)^2$$

• Especially $f(\mathbf{x}, \mathbf{w})$ linear in \mathbf{w} yields quadratic loss and has closed-form solution

$$\mathbf{w}^* = \arg\min_{\mathbf{w}} \left(\sum_{i} -\log(p(y_i|\mathbf{x}_i,\mathbf{w})) \right)$$

log likelihood

• Classification: ML estimate of discrete prob.d. modelled by soft-max function:

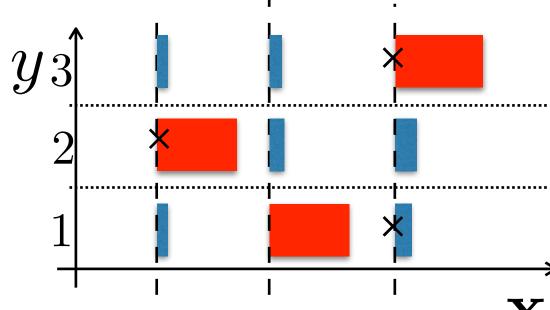
$$p(y|\mathbf{x}, \mathbf{W}) = \begin{bmatrix} \exp(f(\mathbf{x}, \mathbf{w}_1)) \\ \exp(f(\mathbf{x}, \mathbf{w}_2)) \\ \exp(f(\mathbf{x}, \mathbf{w}_3)) \end{bmatrix} / \sum_k \exp(f(\mathbf{x}, \mathbf{w}_k) = \mathbf{s}(\mathbf{f}(\mathbf{x}, \mathbf{W}))$$

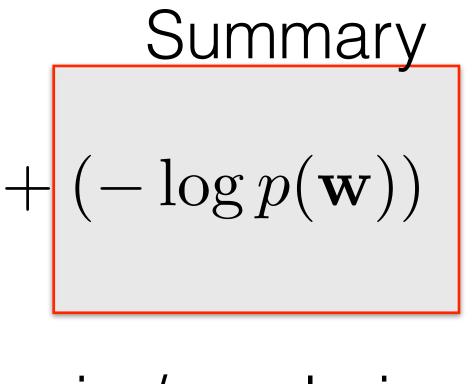
• Probability of observing y_i when measuring \mathbf{x}_i is

$$p(y_i|\mathbf{x}_i, \mathbf{W}) = \mathbf{s}_{y_i}(\mathbf{f}(\mathbf{x}_i, \mathbf{W}))$$

Training: minimization of cross-entropy/logistic loss

$$\mathbf{W}^* = \arg\min_{\mathbf{W}} \sum_{i} -\log \mathbf{s}_{y_i}(\mathbf{f}(\mathbf{x}_i, \mathbf{W}))$$





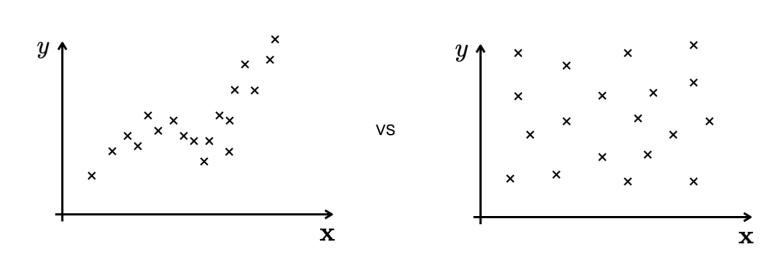
prior/regulariser

- Prior is important: Ideally restricts the model to the class of functions that:
 - Avoid any "not-well justified leprechauns" in the model, => avoid overfitting
 - Avoid oversimplifications of the model, => avoid underfitting
- Robotics study different models to solve different problems:
 - Projective transformation of pinhole cameras (for camera calibration or stereo)
 - Geometry of Euclidean motion (for point cloud alignment, direct kinematic tasks)
 - Motion model of robots such Dubins car, flight, pendulum (for planning/control)
 - Structure of animal cortex (for ConvNets)

Golden grale:

• Solve only "Pilcik-free" problems

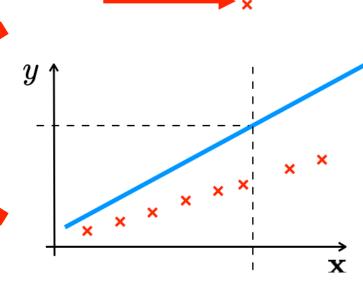


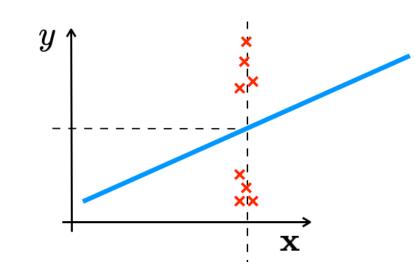


Lecture 1

Use "Morty-free" data (or at least correct noise model)

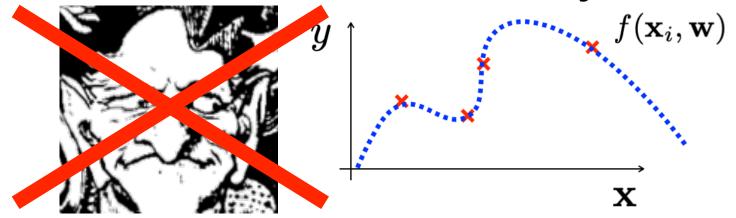






Lecture 3

• Provide "sufficiently rich" + "lepricon-free" model.



Lecture 4 ConvNets

Avoid traps in learning

Lecture 5 Optimizers

Conclusions

- Explained regression and classification as MAP/ML estimator
- Discussed under/overfitting and regularisations
- Summarized

Competencies required for the test T1

- Derive MAP/ML estimate for regression and classification for different noise models
- Derive L2/L1/cross-entropy/logistic losses,
- Understand difference between loss, likelihood and prior
- Understand role of prior in underfitting/overfitting.