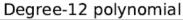
Model Selection and Optimization

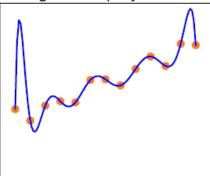
Outline

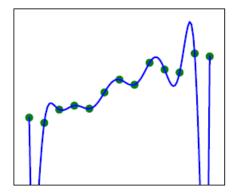
- I. Overfitting and pruning of decision trees
- II. Model selection
- III. Loss function
- IV. Regularization and tuning

^{*} Figures are from the <u>textbook site</u> or plotted by the instructor.

I. Issue of Overfitting





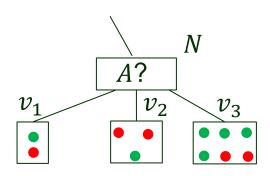


Overfitting

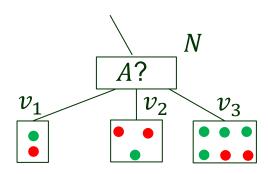
- Too much attention paid to the training set, and performs poorly on unseen data.
- More likely to happen as #attributes increases.
- Less likely with more training examples.
- ♠ Polynomials with higher degrees are more likely to overfit.
- ♠ Decision trees with more nodes have more capacity to overfit.

- Construct a full decision tree.
- Repeat the following steps:

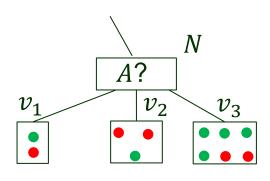
- Construct a full decision tree.
- Repeat the following steps:
 - Consider a test node N with leaf children only.



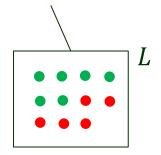
- Construct a full decision tree.
- Repeat the following steps:
 - ◆ Consider a test node N with leaf children only.



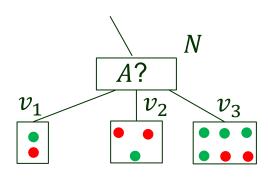
- Construct a full decision tree.
- Repeat the following steps:
 - ◆ Consider a test node N with leaf children only.
 - Replace the node with a leaf node L if the test appears to be irrelevant.



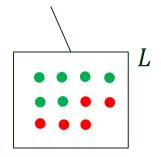




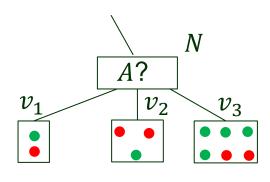
- Construct a full decision tree.
- Repeat the following steps:
 - Consider a test node N with leaf children only.
 - Replace the node with a leaf node L if the test appears to be irrelevant.



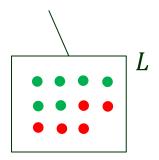




- Construct a full decision tree.
- Repeat the following steps:
 - Consider a test node N with leaf children only.
 - Replace the node with a leaf node L if the test appears to be irrelevant.
 - ♣ How to decide that the attribute *A* is irrelevant?





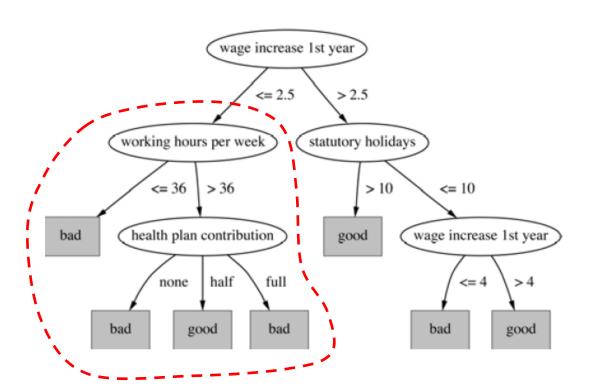


- Construct a full decision tree.
- Repeat the following steps:
 - Consider a test node N with leaf children only.
 - Replace the node with a leaf node L if the test appears to be irrelevant.
 - How to decide that the attribute A is irrelevant?

Low information gain.

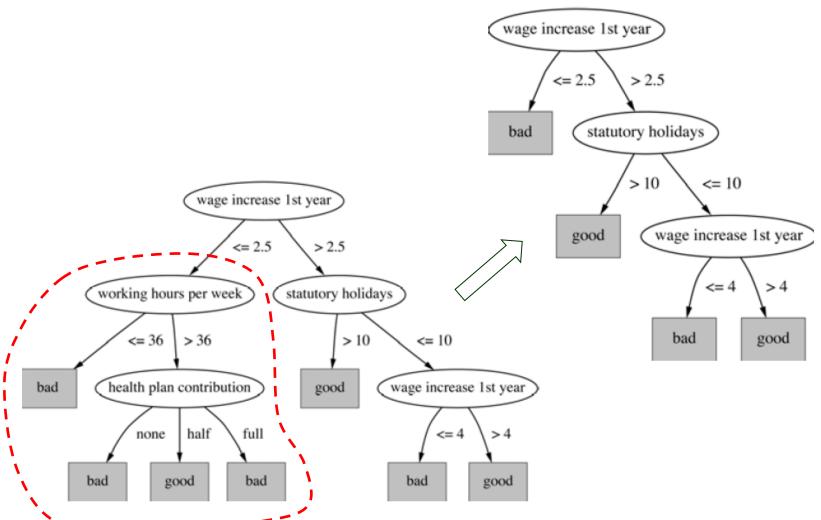
$$Gain(A) = B\left(\frac{p}{p+n}\right) - \sum_{k=1}^{d} \frac{p_k + n_k}{p+n} B\left(\frac{p_k}{p_k + n_k}\right)$$

Example of Pruning



^{*} Example from Dr. Jin Tian's notes.

Example of Pruning



^{*} Example from Dr. Jin Tian's notes.

- The node N has p positive and n negative examples.
- ◆ Testing of attribute A at N splits the set into d subsets.
- For $1 \le k \le d$, subset k has p_k positive and n_k negative examples.

- The node N has p positive and n negative examples.
- ◆ Testing of attribute A at N splits the set into d subsets.
- For $1 \le k \le d$, subset k has p_k positive and n_k negative examples.
- Expected numbers of positive and negative examples are

$$\hat{p}_k = p \cdot \frac{p_k + n_k}{p + n} \qquad \qquad \hat{n}_k = n \cdot \frac{p_k + n_k}{p + n}$$

- The node N has p positive and n negative examples.
- ◆ Testing of attribute A at N splits the set into d subsets.
- For $1 \le k \le d$, subset k has p_k positive and n_k negative examples.
- Expected numbers of positive and negative examples are

$$\hat{p}_k = p \cdot \frac{p_k + n_k}{p + n} \qquad \qquad \hat{n}_k = n \cdot \frac{p_k + n_k}{p + n}$$

Measure of the total deviation is given by

$$\Delta = \sum_{k=1}^{d} \left(\frac{(p_k - \hat{p}_k)^2}{\hat{p}_k} + \frac{(n_k - \hat{n}_k)^2}{\hat{n}_k} \right)$$

- The node N has p positive and n negative examples.
- ◆ Testing of attribute A at N splits the set into d subsets.
- For $1 \le k \le d$, subset k has p_k positive and n_k negative examples.
- Expected numbers of positive and negative examples are

$$\hat{p}_k = p \cdot \frac{p_k + n_k}{p + n} \qquad \qquad \hat{n}_k = n \cdot \frac{p_k + n_k}{p + n}$$

Measure of the total deviation is given by

$$\Delta = \sum_{k=1}^{d} \left(\frac{(p_k - \hat{p}_k)^2}{\hat{p}_k} + \frac{(n_k - \hat{n}_k)^2}{\hat{n}_k} \right)$$

 χ^2 distribution with d-1 degrees of freedom

- lacktriangle The node N has p positive and n negative examples.
- Testing of attribute A at N splits the set into d subsets.
- For $1 \le k \le d$, subset k has p_k positive and n_k negative examples.
- Expected numbers of positive and negative examples are

$$\hat{p}_k = p \cdot \frac{p_k + n_k}{p + n} \qquad \qquad \hat{n}_k = n \cdot \frac{p_k + n_k}{p + n}$$

Measure of the total deviation is given by

$$\Delta = \sum_{k=1}^{d} \left(\frac{(p_k - \hat{p}_k)^2}{\hat{p}_k} + \frac{(n_k - \hat{n}_k)^2}{\hat{n}_k} \right)$$
 Apply χ^2 pruning:

$$\Delta = 7.82 \text{ would mean the attribute is irrelevant at the 5% level. (The higher the value of Λ , the more$$

 χ^2 distribution with d-1 degrees of freedom

higher the value of Δ , the more significant the attribute is.)

II. Model Selection

Goal: Select a hypothesis that will optimally fit future examples.

Future examples are assumed to be like the past.

Stationarity.

$$P(E_j) = P(E_{j+1}) = P(E_{j+2}) = \cdots$$
 // every example has the // the same prior probability. $P(E_j) = P(E_j \mid E_{j-1}, E_{j-2}, \dots)$ // every example is independent // of the previous examples.

Optimal Fit

Split the examples into three sets:

- a training set to train candidate models (hypotheses)
- a validation set to evaluate the candidate models and choose the best one
- a test set to do a final unbiased evaluation of the best model

Optimal Fit

Split the examples into three sets:

- a training set to train candidate models (hypotheses)
- a validation set to evaluate the candidate models and choose the best one
- a test set to do a final unbiased evaluation of the best model

Two tasks:

- Model selection chooses a good hypothesis space.
- Optimization (aka training) finds the best hypothesis within that space.

Model Selection via Cross Validation

function MODEL-SELECTION(Learner, examples, k) returns a (hypothesis, error rate) pair

```
err \leftarrow an array, indexed by size, storing validation-set error rates training\_set, test\_set \leftarrow a partition of examples into two sets for \ size = 1 \ to \infty \ do err[size] \leftarrow CROSS-VALIDATION(Learner, size, training\_set, k) if err is starting to increase significantly then best\_size \leftarrow the value of size with minimum err[size] h \leftarrow Learner(best\_size, training\_set) return \ h, ERROR-RATE(h, \ test\_set)
```

function CROSS-VALIDATION(Learner, size, examples, k) returns error rate

```
N \leftarrow the number of examples errs \leftarrow 0 for i=1 to k do validation\_set \leftarrow examples[(i-1) \times N/k:i \times N/k] \\ training\_set \leftarrow examples - validation\_set \\ h \leftarrow Learner(size, training\_set) \\ errs \leftarrow errs + \text{ERROR-RATE}(h, validation\_set) return errs / k // errs = errs + e
```

Model Selection via Cross Validation

function MODEL-SELECTION(*Learner*, *examples*, *k*) **returns** a (hypothesis, error rate) pair $err \leftarrow$ an array, indexed by size, storing validation-set error rates $training_set$, $test_set \leftarrow$ a partition of examples into two sets // size is a hyperparameter for size = 1 to ∞ do // of the model class, e.g., $err[size] \leftarrow \text{CROSS-Validation}(\underline{Learner}, size, training_set, k)$ // #nodes in a decision tree **if** err is starting to increase significantly **then** // degree of polynomials. $best_size \leftarrow$ the value of size with minimum err[size] $h \leftarrow Learner(best_size, training_set)$ **return** h, ERROR-RATE(h, test_set) **function** CROSS-VALIDATION(Learner, size, examples, k) **returns** error rate

```
N \leftarrow \text{the number of } examples \\ errs \leftarrow 0 \\ \textbf{for } i = 1 \textbf{ to } k \textbf{ do} \\ validation\_set \leftarrow examples[(i-1) \times N/k:i \times N/k] \\ training\_set \leftarrow examples - validation\_set \\ h \leftarrow Learner(size, training\_set) \\ errs \leftarrow errs + \text{ERROR-RATE}(h, validation\_set) \\ \textbf{return } errs \ / \ / \ average \ error \ rate \ on \ validation \ sets, \ across \ k\text{-fold } cross\text{-validation}
```

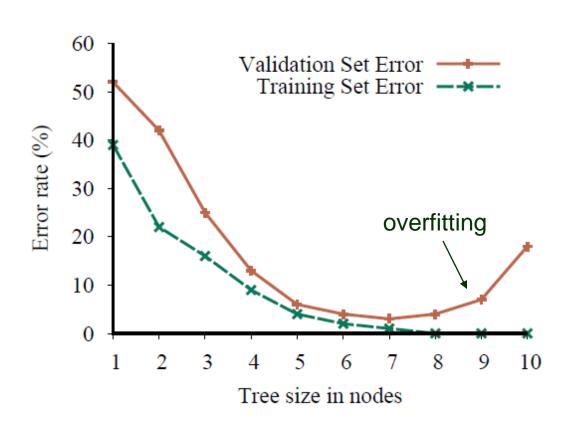
Model Selection via Cross Validation

function MODEL-SELECTION(Learner, examples, k) **returns** a (hypothesis, error rate) pair $err \leftarrow$ an array, indexed by size, storing validation-set error rates $training_set$, $test_set \leftarrow$ a partition of examples into two sets **for** size = 1 **to** ∞ **do** $err[size] \leftarrow CROSS-VALIDATION(Learner, size, training_set, k)$ **if** err is starting to increase significantly **then** $best_size \leftarrow$ the value of size with minimum err[size] $h \leftarrow Learner(best_size, training_set)$

function CROSS-VALIDATION(Learner, size, examples, k) returns error rate

return h, ERROR-RATE(h, test_set)

Training and Validation Errors (1)

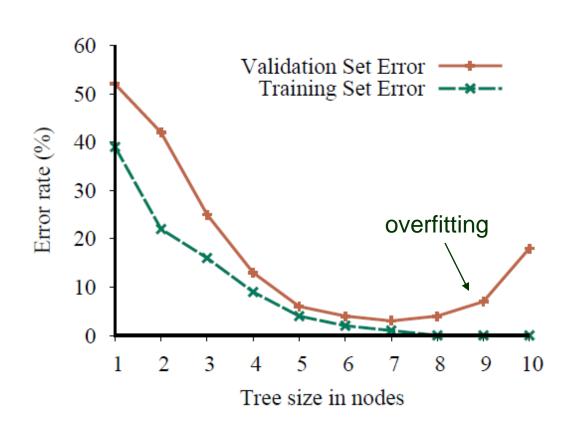


Data: obtained from a version of the restaurant problem

Model class: decision trees

Hyperparameter: #nodes

Training and Validation Errors (1)



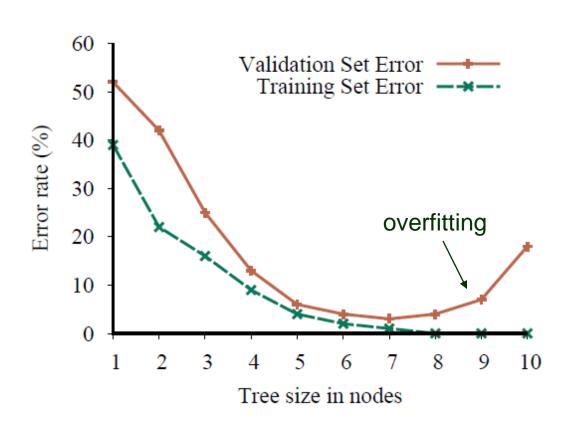
Data: obtained from a version of the restaurant problem

Model class: decision trees

Hyperparameter: #nodes

 The training set error decreases monotonically as the model complexity (tree size) increases.

Training and Validation Errors (1)



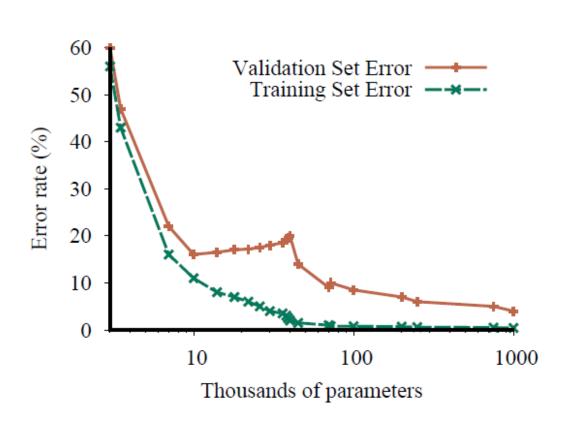
Data: obtained from a version of the restaurant problem

Model class: decision trees

Hyperparameter: #nodes

- The training set error decreases monotonically as the model complexity (tree size) increases.
- As the decision tree's size increases, the validation error initially decreases (until tree size = 7), and later increases since the model starts to overfit.

Training and Validation Errors (2)

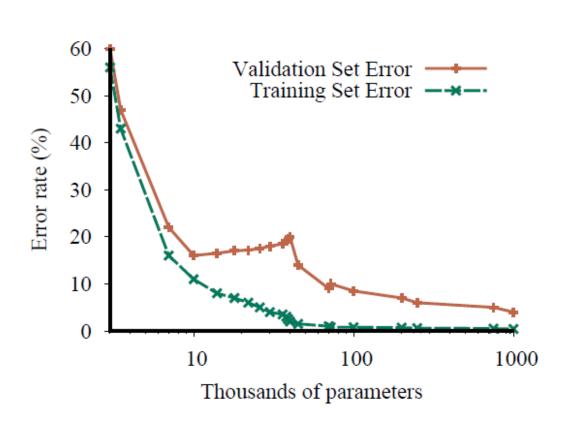


Data: MNIST data set of images of digits

Model class: convolutional neural networks (CNNs)

Hyperparameter: number of regular parameters

Training and Validation Errors (2)



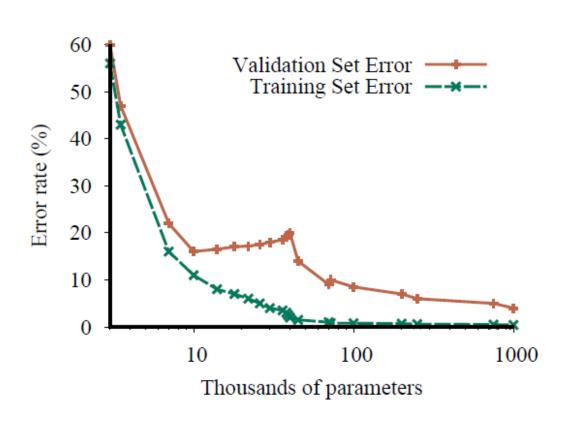
Data: MNIST data set of images of digits

Model class: convolutional neural networks (CNNs)

Hyperparameter: number of regular parameters

 The training set error decreases monotonically.

Training and Validation Errors (2)



Data: MNIST data set of images of digits

Model class: convolutional neural networks (CNNs)

Hyperparameter: number of regular parameters

- The training set error decreases monotonically.
- The validation error shows an initial U-shaped curve and then starts to decrease again, reaching the lowest value at the max number (1,000,000) of parameters.

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

 $L(x, y, \hat{y})$: the amount of utility lost by predicting $h(x) = \hat{y}$ when the correct answer is f(x) = y.

 $L(x, y, \hat{y}) = \text{Utility (result of using } y \text{ given an input } x)$ - Utility (result of using \hat{y} given x)

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

$$L(y, \hat{y}) \leftarrow L(x, y, \hat{y}) = \text{Utility (result of using } y \text{ given an input } x)$$

$$- \text{Utility (result of using } \hat{y} \text{ given } x)$$

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

$$L(y, \hat{y}) \leftarrow L(x, y, \hat{y}) = \text{Utility (result of using } y \text{ given an input } x)$$

$$- \text{Utility (result of using } \hat{y} \text{ given } x)$$

$$L(spam, nospam) = 1$$

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

$$L(y, \hat{y}) \leftarrow L(x, y, \hat{y}) = \text{Utility (result of using } y \text{ given an input } x)$$

$$- \text{Utility (result of using } \hat{y} \text{ given } x)$$

$$L(spam, nospam) = 1$$

truth prediction

Not all errors should be weighted equally.

Spam e-mail filtering: It's worse to classify non-spam as spam than to classify spam as non-spam.

Rather than maximizing a utility function, ML minimizes a loss function.

$$L(y, \hat{y}) \leftarrow L(x, y, \hat{y}) = \text{Utility (result of using } y \text{ given an input } x)$$

$$- \text{Utility (result of using } \hat{y} \text{ given } x)$$

$$L(spam, nospam) = 1$$
 $L(nospam, spam) = 10$ truth prediction

Generalization Loss

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

ML chooses the hypothesis that minimizes *expected loss* over the set \mathcal{E} of all input-output pairs.

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

ML chooses the hypothesis that minimizes *expected loss* over the set \mathcal{E} of all input-output pairs.

Generalization loss for a hypothesis *h* w.r.t. loss function *L*:

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

ML chooses the hypothesis that minimizes *expected loss* over the set \mathcal{E} of all input-output pairs.

Generalization loss for a hypothesis *h* w.r.t. loss function *L*:

$$GenLoss_L(h) = \sum_{(x,y)\in\mathcal{E}} L(y,h(x))P(x,y)$$

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

ML chooses the hypothesis that minimizes *expected loss* over the set \mathcal{E} of all input-output pairs.

Generalization loss for a hypothesis *h* w.r.t. loss function *L*:

$$GenLoss_{L}(h) = \sum_{(x,y)\in\mathcal{E}} L(y,h(x))P(x,y)$$
prior joint probability

Absolute-value loss: $L_1(y, \hat{y}) = |y - \hat{y}|$

Squared-error loss: $L_2(y, \hat{y}) = (y - \hat{y})^2$

0/1 loss: $L_{0/1}(y, \hat{y}) = 0$ if $y = \hat{y}$, and 1 otherwise

ML chooses the hypothesis that minimizes *expected loss* over the set \mathcal{E} of all input-output pairs.

Generalization loss for a hypothesis *h* w.r.t. loss function *L*:

$$GenLoss_{L}(h) = \sum_{(x,y)\in\mathcal{E}} L(y,h(x))P(x,y)$$
prior joint probability

Best hypothesis is chosen as

$$h^* = \underset{h \in \mathcal{H}}{\operatorname{argmin}} \operatorname{GenLoss}_L(h)$$

Empirical Loss

♠ $GenLoss_L(h)$ can only be estimated since P(x, y) is often unknown.

Empirical loss on a set of examples *E* of size *N*:

$$EmpLoss_{L,E}(h) = \sum_{(x,y)\in\mathcal{E}} L(y,h(x))\frac{1}{N}$$

Empirical Loss

♠ $GenLoss_L(h)$ can only be estimated since P(x, y) is often unknown.

Empirical loss on a set of examples *E* of size *N*:

$$EmpLoss_{L,E}(h) = \sum_{(x,y)\in\mathcal{E}} L(y,h(x))\frac{1}{N}$$

This defines an estimated best hypothesis:

$$\hat{h}^* = \underset{h \in \mathcal{H}}{\operatorname{argmin}} \, EmpLoss_L(h)$$

A learning problem is *realizable* if the *true function* f lies in the hypothesis space \mathcal{H} .

A learning problem is *realizable* if the *true function* f lies in the hypothesis space \mathcal{H} .

The learned best hypothesis \hat{h}^* may differ from f for several reasons:

♦ Unrealizability. No amount of data will recover f if $f \notin \mathcal{H}$.

A learning problem is *realizable* if the *true function* f lies in the hypothesis space \mathcal{H} .

The learned best hypothesis \hat{h}^* may differ from f for several reasons:

- **♦** Unrealizability. No amount of data will recover f if $f \notin \mathcal{H}$.
- ♦ Variance. Different hypotheses are returned from learning for different sets of examples.

A learning problem is *realizable* if the *true function* f lies in the hypothesis space \mathcal{H} .

The learned best hypothesis \hat{h}^* may differ from f for several reasons:

- **♦** Unrealizability. No amount of data will recover f if $f \notin \mathcal{H}$.
- ♦ Variance. Different hypotheses are returned from learning for different sets of examples.
- ♦ Noise. f may be nondeterministic or noisy, returning different values f(x) for the same x (e.g., measurements of a person's height).

A learning problem is *realizable* if the *true function* f lies in the hypothesis space \mathcal{H} .

The learned best hypothesis \hat{h}^* may differ from f for several reasons:

- **♦** Unrealizability. No amount of data will recover f if $f \notin \mathcal{H}$.
- ♦ Variance. Different hypotheses are returned from learning for different sets of examples.
- ♦ Noise. f may be nondeterministic or noisy, returning different values f(x) for the same x (e.g., measurements of a person's height).
- ♠ Computational complexity. Searching large hypothesis space ℋ systematically can be computationally intractable. Often, a subspace search is conducted to return a reasonably good (but not optimal) hypothesis.

Model selection as a minimization:

$$\hat{h}^* = \operatorname*{argmin}_{h \in \mathcal{H}} \mathsf{Cost}(h)$$

where

$$Cost(h) = EmpLoss(h) + \lambda Complexity(h)$$

Model selection as a minimization:

$$\hat{h}^* = \operatorname*{argmin}_{h \in \mathcal{H}} \mathbf{Cost}(h)$$

where

$$Cost(h) = EmpLoss(h) + \lambda Complexity(h)$$

positive hyperparameter to balance loss and hypothesis complexity

Model selection as a minimization:

$$\hat{h}^* = \operatorname*{argmin}_{h \in \mathcal{H}} \mathsf{Cost}(h)$$

where

$$Cost(h) = EmpLoss(h) + \lambda Complexity(h)$$
positive hyperparameter to balance loss and hypothesis complexity

regularization function

Model selection as a minimization:

$$\hat{h}^* = \operatorname*{argmin}_{h \in \mathcal{H}} \mathsf{Cost}(h)$$

where

$$Cost(h) = EmpLoss(h) + \lambda Complexity(h)$$
positive hyperparameter to balance loss and hypothesis complexity

regularization function

Regularization refers to the process of explicitly penalizing complex hypotheses to favor functions that are more regular.

Model selection as a minimization:

$$\hat{h}^* = \operatorname*{argmin}_{h \in \mathcal{H}} \mathsf{Cost}(h)$$

where

$$Cost(h) = EmpLoss(h) + \lambda Complexity(h)$$
positive hyperparameter to balance loss and hypothesis complexity

regularization function

Regularization refers to the process of explicitly penalizing complex hypotheses to favor functions that are more regular.

Choice of regularization function depends on the hypothesis space.

For polynomials, we could use the sum of the squares of the coefficients, of which a small value would prevent a wiggling behavior.

It is difficult to choose good values for multiple hyperparameters via cross validation.

It is difficult to choose good values for multiple hyperparameters via cross validation.

→ Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.

It is difficult to choose good values for multiple hyperparameters via cross validation.

- → Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.
- Grid search. Try all combinations of values and choose one which performs the best on the validation data. Use random sampling if the size of the space is big or the values are continuous.

It is difficult to choose good values for multiple hyperparameters via cross validation.

- → Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.
- ◆ Grid search. Try all combinations of values and choose one which performs the best on the validation data. Use random sampling if the size of the space is big or the values are continuous.
- ◆ Bayesian optimization. Treat hyperparameter tuning as a machine learning problem itself.

It is difficult to choose good values for multiple hyperparameters via cross validation.

- → Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.
- ◆ Grid search. Try all combinations of values and choose one which performs the best on the validation data. Use random sampling if the size of the space is big or the values are continuous.
- ◆ Bayesian optimization. Treat hyperparameter tuning as a machine learning problem itself.

Input: the vector *x* of hyperparameter values

Output: the total loss y on the validation set for the resulting model

It is difficult to choose good values for multiple hyperparameters via cross validation.

- → Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.
- ◆ Grid search. Try all combinations of values and choose one which performs the best on the validation data. Use random sampling if the size of the space is big or the values are continuous.
- ◆ Bayesian optimization. Treat hyperparameter tuning as a machine learning problem itself.

Input: the vector *x* of hyperparameter values

Output: the total loss y on the validation set for the resulting model Training set: $(x_1, y_1), (x_2, y_2), ..., (x_n, y_N)$ generated from training runs

It is difficult to choose good values for multiple hyperparameters via cross validation.

- → Hand-tuning. Guess some values, train a model, measure its performance, and then suggest new values.
- ◆ Grid search. Try all combinations of values and choose one which performs the best on the validation data. Use random sampling if the size of the space is big or the values are continuous.
- ◆ Bayesian optimization. Treat hyperparameter tuning as a machine learning problem itself.

Input: the vector *x* of hyperparameter values

Output: the total loss y on the validation set for the resulting model Training set: $(x_1, y_1), (x_2, y_2), ..., (x_n, y_N)$ generated from training runs

Task: find a function h(x) to minimize y over the N pairs $(y_i, h(x_i))$