Decision Tree Learning
Goals for the lecture

you should understand the following concepts

• the decision tree representation
• the standard top-down approach to learning a tree
• Occam’s razor
• entropy and information gain
• types of decision-tree splits
• test sets and unbiased estimates of accuracy
• overfitting
• early stopping and pruning
• tuning (validation) sets
• regression trees
• $m$-of-$n$ splits
• using lookahead in decision tree search
A decision tree to predict heart disease

Each internal node tests one feature $x_i$.

Each branch from an internal node represents one outcome of the test.

Each leaf predicts $y$ or $P(y | x)$.
Decision tree exercise

Suppose $x_1 \ldots x_5$ are Boolean features, and $y$ is also Boolean

How would you represent the following with decision trees?

$$y = x_2 x_5 \quad (\text{i.e. } y = x_2 \land x_5)$$

$$y = x_2 \lor x_5$$

$$y = x_2 x_5 \lor x_3 \neg x_1$$
History of decision tree learning

- **AID**: 1963
- **THAID**: 1973
- **CHAID**: 1980
- **CART**: 1984
- **ID3**: 1986

Many DT variants have been developed since CART and ID3.

Dated dates of seminal publications: work on these 2 was contemporaneous.

CART developed by Leo Breiman, Jerome Friedman, Charles Olshen, R.A. Stone.

ID3, C4.5, C5.0 developed by Ross Quinlan.
Top-down decision tree learning

\textbf{MakeSubtree}(set of training instances }D)\\
\quad C = \text{DetermineCandidateSplits}(D)\\
\quad \text{if stopping criteria met}\\
\quad \quad \text{make a leaf node } N\\
\quad \quad \text{determine class label/probabilities for } N\\
\quad \text{else}\\
\quad \quad \text{make an internal node } N\\
\quad S = \text{FindBestSplit}(D, C)\\
\quad \text{for each outcome } k \text{ of } S\\
\quad \quad D_k = \text{subset of instances that have outcome } k\\
\quad \quad k^{th} \text{ child of } N = \text{MakeSubtree}(D_k)\\
\quad \text{return subtree rooted at } N
Candidate splits in ID3, C4.5

- splits on nominal features have one branch per value

  - thal
    - normal
    - fixed_defect
    - reversible_defect

- splits on continuous features use a threshold

  - weight ≤ 35
    - true
    - false
Candidate splits on continuous features

given a set of training instances $D$ and a specific feature $F$

- sort the values of $F$ in $D$
- evaluate split thresholds in intervals between instances of different classes

• could use midpoint of each considered interval as the threshold
• C4.5 instead picks the largest value of $F$ in the entire training set that does not exceed the midpoint
Candidate splits on a numeric feature

// Run this subroutine for each numeric feature at each node of DT induction

DetermineCandidateNumericSplits(set of training instances $D$, feature $x_i$)

$C = \{\}$  // initialize set of candidate splits for feature $x_i$

$S =$ partition instances in $D$ into sets $s_1 \ldots s_V$ where the instances in each set have the same value for $x_i$

let $v_j$ denote the value of $x_i$ for set $s_j$

sort the sets in $S$ using $v_j$ as the key for each $s_j$

for each pair of adjacent sets $s_j, s_{j+1}$ in sorted $S$

    if $s_j$ and $s_{j+1}$ contain a pair of instances with different class labels

        // use midpoints for splits

        add candidate split $x_i \leq (v_j + v_{j+1})/2$ to $C$

return $C$
Candidate splits

- instead of using $k$-way splits for $k$-valued features, could require binary splits on all discrete features (CART does this)

Breiman et al. proved for the 2-class case, the optimal binary partition can be found considered only $O(k)$ possibilities instead of $O(2^k)$
Finding the best split

• How should we select the best feature to split on at each step?

• Key hypothesis: the simplest tree that classifies the training examples accurately will work well on previously unseen examples
Occam’s razor

- attributed to 14th century William of Ockham

- “Nunquam ponenda est pluralitis sin necesitate”

- “Entities should not be multiplied beyond necessity”

- “should proceed to simpler theories until simplicity can be traded for greater explanatory power”

- “when you have two competing theories that make exactly the same predictions, the simpler one is the better”
But a thousand years earlier, I said, “We consider it a good principle to explain the phenomena by the simplest hypothesis possible.”
Occam’s razor and decision trees

Why is Occam’s razor a reasonable heuristic for decision tree learning?

- there are fewer short models (i.e. small trees) than long ones
- a short model is unlikely to fit the training data well by chance
- a long model is more likely to fit the training data well coincidentally
Finding the best splits

• Can we return the smallest possible decision tree that accurately classifies the training set?

  NO! This is an NP-hard problem

• Instead, we’ll use an information-theoretic heuristic to greedily choose splits
Information theory background

• consider a problem in which you are using a code to communicate information to a receiver

• example: as bikes go past, you are communicating the manufacturer of each bike
Information theory background

- Suppose there are only four types of bikes.
- We could use the following code:

<table>
<thead>
<tr>
<th>type</th>
<th>code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trek</td>
<td>11</td>
</tr>
<tr>
<td>Specialized</td>
<td>10</td>
</tr>
<tr>
<td>Cervelo</td>
<td>01</td>
</tr>
<tr>
<td>Serrota</td>
<td>00</td>
</tr>
</tbody>
</table>

- Expected number of bits we have to communicate: 2 bits/bike.
Information theory background

- we can do better if the bike types aren’t equiprobable
- optimal code uses \(-\log_2 P(y)\) bits for event with probability \(P(y)\)

<table>
<thead>
<tr>
<th>Type/probability</th>
<th># bits</th>
<th>code</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P(\text{Trek}) = 0.5)</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>(P(\text{Specialized}) = 0.25)</td>
<td>2</td>
<td>01</td>
</tr>
<tr>
<td>(P(\text{Cervelo}) = 0.125)</td>
<td>3</td>
<td>001</td>
</tr>
<tr>
<td>(P(\text{Serrota}) = 0.125)</td>
<td>3</td>
<td>000</td>
</tr>
</tbody>
</table>

- expected number of bits we have to communicate: 1.75 bits/bike

\[- \sum_{y \in \text{values}(Y)} P(y) \log_2 P(y)\]
Entropy

- entropy is a measure of uncertainty associated with a random variable

- defined as the expected number of bits required to communicate the value of the variable

\[ H(Y) = - \sum_{y \in \text{values}(Y)} P(y) \log_2 P(y) \]
Conditional entropy

- What’s the entropy of $Y$ if we condition on some other variable $X$?

$$H(Y \mid X) = \sum_{x \in \text{values}(X)} P(X = x) \cdot H(Y \mid X = x)$$

where

$$H(Y \mid X = x) = -\sum_{y \in \text{values}(Y)} P(Y = y \mid X = x) \log_2 P(Y = y \mid X = x)$$
Information gain
(a.k.a. mutual information)

• choosing splits in ID3: select the split $S$ that most reduces the conditional entropy of $Y$ for training set $D$

$$\text{InfoGain}(D, S) = H_D(Y) - H_D(Y | S)$$

$D$ indicates that we’re calculating probabilities using the specific sample $D$
### PlayTennis: training examples

<table>
<thead>
<tr>
<th>Day</th>
<th>Outlook</th>
<th>Temperature</th>
<th>Humidity</th>
<th>Wind</th>
<th>PlayTennis</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>Sunny</td>
<td>Hot</td>
<td>High</td>
<td>Weak</td>
<td>No</td>
</tr>
<tr>
<td>D2</td>
<td>Sunny</td>
<td>Hot</td>
<td>High</td>
<td>Strong</td>
<td>No</td>
</tr>
<tr>
<td>D3</td>
<td>Overcast</td>
<td>Hot</td>
<td>High</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D4</td>
<td>Rain</td>
<td>Mild</td>
<td>High</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D5</td>
<td>Rain</td>
<td>Cool</td>
<td>Normal</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D6</td>
<td>Rain</td>
<td>Cool</td>
<td>Normal</td>
<td>Strong</td>
<td>No</td>
</tr>
<tr>
<td>D7</td>
<td>Overcast</td>
<td>Cool</td>
<td>Normal</td>
<td>Strong</td>
<td>Yes</td>
</tr>
<tr>
<td>D8</td>
<td>Sunny</td>
<td>Mild</td>
<td>High</td>
<td>Weak</td>
<td>No</td>
</tr>
<tr>
<td>D9</td>
<td>Sunny</td>
<td>Cool</td>
<td>Normal</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D10</td>
<td>Rain</td>
<td>Mild</td>
<td>Normal</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D11</td>
<td>Sunny</td>
<td>Mild</td>
<td>Normal</td>
<td>Strong</td>
<td>Yes</td>
</tr>
<tr>
<td>D12</td>
<td>Overcast</td>
<td>Mild</td>
<td>High</td>
<td>Strong</td>
<td>Yes</td>
</tr>
<tr>
<td>D13</td>
<td>Overcast</td>
<td>Hot</td>
<td>Normal</td>
<td>Weak</td>
<td>Yes</td>
</tr>
<tr>
<td>D14</td>
<td>Rain</td>
<td>Mild</td>
<td>High</td>
<td>Strong</td>
<td>No</td>
</tr>
</tbody>
</table>
What’s the information gain of splitting on Humidity?

\[
H_D(Y) = - \frac{9}{14} \log_2 \left( \frac{9}{14} \right) - \frac{5}{14} \log_2 \left( \frac{5}{14} \right) = 0.940
\]

\[
H_D(Y | \text{high}) = - \frac{3}{7} \log_2 \left( \frac{3}{7} \right) - \frac{4}{7} \log_2 \left( \frac{4}{7} \right) = 0.985
\]

\[
H_D(Y | \text{normal}) = - \frac{6}{7} \log_2 \left( \frac{6}{7} \right) - \frac{1}{7} \log_2 \left( \frac{1}{7} \right) = 0.592
\]

\[
\text{InfoGain}(D, \text{Humidity}) = H_D(Y) - H_D(Y | \text{Humidity})
\]

\[
= 0.940 - \left[ \frac{7}{14} (0.985) + \frac{7}{14} (0.592) \right]
\]

\[
= 0.151
\]
Information gain example

• Is it better to split on Humidity or Wind?

\[ H_D(Y \mid \text{weak}) = 0.811 \quad H_D(Y \mid \text{strong}) = 1.0 \]

\[ \text{InfoGain}(D, \text{Humidity}) = 0.940 - \left[ \frac{7}{14} (0.985) + \frac{7}{14} (0.592) \right] = 0.151 \]

\[ \text{InfoGain}(D, \text{Wind}) = 0.940 - \left[ \frac{8}{14} (0.811) + \frac{6}{14} (1.0) \right] = 0.048 \]
One limitation of information gain

- information gain is biased towards tests with many outcomes

- e.g. consider a feature that uniquely identifies each training instance
  - splitting on this feature would result in many branches, each of which is “pure” (has instances of only one class)
  - maximal information gain!
Gain ratio

- To address this limitation, C4.5 uses a splitting criterion called *gain ratio*

- Consider the potential information generated by splitting on $S$

$$\text{SplitInfo}(D, S) = - \sum_{k \in \text{outcomes}(S)} \frac{|D_k|}{|D|} \log_2 \left( \frac{D_k}{D} \right)$$

use this to normalize information gain

$$\text{GainRatio}(D, S) = \frac{\text{InfoGain}(D, S)}{\text{SplitInfo}(D, S)}$$
Stopping criteria

We should form a leaf when
• all of the given subset of instances are of the same class
• we’ve exhausted all of the candidate splits

Is there a reason to stop earlier, or to prune back the tree?
How can we assess the accuracy of a tree?

- Can we just calculate the fraction of training examples that are correctly classified?

- Consider a problem domain in which instances are assigned labels at random with \( P(Y = T) = 0.5 \)

  - How accurate would a learned decision tree be on previously unseen instances?

  - How accurate would it be on its training set?
How can we assess the accuracy of a tree?

- to get an unbiased estimate of a learned model’s accuracy, we must use a set of instances that are held-aside during learning
- this is called a test set
Overfitting

• consider error of model $h$ over
  • training data: $error_D(h)$
  • entire distribution of data: $error(h)$

• model $h \in H$ overfits the training data if there is an alternative model $h' \in H$ such that

\[
error(h) > error(h')
\]

\[
error_D(h) < error_D(h')
\]
Overfitting with noisy data

suppose

- the target concept is \( Y = X_1 \land X_2 \)
- there is noise in some feature values
- we’re given the following training set

<table>
<thead>
<tr>
<th>( X_1 )</th>
<th>( X_2 )</th>
<th>( X_3 )</th>
<th>( X_4 )</th>
<th>( X_5 )</th>
<th>...</th>
<th>( Y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>...</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>...</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>...</td>
<td>F</td>
</tr>
</tbody>
</table>
Overfitting with noisy data

- **Correct tree**
  - $X_1$
  - $X_2$
  - $X_3$
  - $X_4$

- **Tree that fits noisy training data**
  - $X_1$
  - $X_2$
  - $X_3$
  - $X_4$
Overfitting visualized

Consider a problem with:
- 2 continuous features
- 3 classes
- Some noisy training instances
Overfitting with **noise-free** data

suppose

- the target concept is \( Y = X_1 \land X_2 \)
- \( P(X_3 = T) = 0.5 \) for both classes
- \( P(Y = T) = 0.67 \)
- we’re given the following training set

<table>
<thead>
<tr>
<th>( X_1 )</th>
<th>( X_2 )</th>
<th>( X_3 )</th>
<th>( X_4 )</th>
<th>( X_5 )</th>
<th>...</th>
<th>( Y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>...</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>...</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>...</td>
<td>F</td>
</tr>
</tbody>
</table>
Overfitting with noise-free data

- because the training set is a limited sample, there might be (combinations of) features that are correlated with the target concept by chance
Overfitting in decision trees
Avoiding overfitting in DT learning

two general strategies to avoid overfitting

1. *early stopping*: stop if further splitting not justified by a statistical test
   • Quinlan’s original approach in ID3

2. *post-pruning*: grow a large tree, then prune back some nodes
   • more robust to myopia of greedy tree learning
Pruning in ID3, C4.5

1. split given data into training and tuning (validation) sets
2. grow a complete tree
3. do until further pruning is harmful
   • evaluate impact on tuning-set accuracy of pruning each node
   • greedily remove the one that most improves tuning-set accuracy
Tuning sets

- a tuning set (a.k.a. validation set) is a subset of the training set that is held aside
  - not used for primary training process (e.g. tree growing)
  - but used to select among models (e.g. trees pruned to varying degrees)
Regression trees

- in a regression tree, leaves have functions that predict numeric values instead of class labels
- the form of these functions depends on the method
  - CART uses constants: regression trees
  - some methods use linear functions: model trees
Regression trees in CART

- CART does *least squares regression* which tries to minimize

\[
\sum_{i=1}^{D} (y_i - \hat{y}_i)^2
\]

- target value for \(i^{th}\) training instance
- value predicted by tree for \(i^{th}\) training instance (average value of \(y\) for training instances reaching the leaf)

\[
= \sum_{L \in \text{leaves}} \sum_{i \in L} (y_i - \hat{y}_i)^2
\]

- at each internal node, CART chooses the split that most reduces this quantity
$m$-of-$n$ splits

- A few DT algorithms have used $m$-of-$n$ splits [Murphy & Pazzani ‘91]
- Each split is constructed using a heuristic search process
- This can result in smaller, easier to comprehend trees

Test is satisfied if 5 of 10 conditions are true

Tree for exchange rate prediction

[Craven & Shavlik, 1997]
Searching for $m$-of-$n$ splits

$m$-of-$n$ splits are found via a hill-climbing search
- initial state: best 1-of-1 (ordinary) binary split
- evaluation function: information gain
- operators:

$$m$-of-$n \Rightarrow m$-of-$(n+1)$$

$$1 \text{ of } \{ X_1=T, X_3=F \} \Rightarrow 1 \text{ of } \{ X_1=T, X_3=F, X_7=T \}$$

$$m$-of-$n \Rightarrow (m+1)$-of-$(n+1)$$

$$1 \text{ of } \{ X_1=T, X_3=F \} \Rightarrow 2 \text{ of } \{ X_1=T, X_3=F, X_7=T \}$$
Lookahead

• most DT learning methods use a hill-climbing search
• a limitation of this approach is myopia: an important feature may not appear to be informative until used in conjunction with other features
• can potentially alleviate this limitation by using a lookahead search [Norton ‘89; Murphy & Salzberg ‘95]
• empirically, often doesn’t improve accuracy or tree size
Choosing best split in ordinary DT learning

**OrdinaryFindBestSplit** *(set of training instances $D$, set of candidate splits $C$)*

\[ \text{maxgain} = -\infty \]

for each split $S$ in $C$

\[ \text{gain} = \text{InfoGain}(D, S) \]

if \( \text{gain} > \text{maxgain} \)

\[ \text{maxgain} = \text{gain} \]

\[ S_{\text{best}} = S \]

return $S_{\text{best}}$
Choosing best split with lookahead (part 1)

\textbf{LookaheadFindBestSplit}(set of training instances }D, \text{ set of candidate splits }C)\text{)

\begin{align*}
\text{maxgain} &= -\infty \\
\text{for each split } S \text{ in } C \\
\text{gain} &= \text{EvaluateSplit}(D, C, S) \\
\text{if } \text{gain} > \text{maxgain} \\
\text{maxgain} &= \text{gain} \\
S_{\text{best}} &= S \\
\text{return } S_{\text{best}}
\end{align*}
Choosing best split with lookahead
(part 2)

EvaluateSplit($D, C, S$)

if a split on $S$ separates instances by class (i.e. $H_D(Y \mid S) = 0$)

// no need to split further

return $H_D(Y) - H_D(Y \mid S)$

else

for outcomes $k \in \{1, 2\}$ of $S$ // let’s assume binary splits

// see what the splits at the next level would be

$D_k = \text{subset of instances that have outcome } k$

$S_k = \text{OrdinaryFindBestSplit}(D_k, C - S)$

// return information gain that would result from this 2-level subtree

return $H_D(Y) - H_D(Y \mid S, S_1, S_2)$
Calculating information gain with lookahead

Suppose that when considering Humidity as a split, we find that Wind and Temperature are the best features to split on at the next level.

We can assess value of choosing Humidity as our split by $H_D(Y) - H_D(Y \mid \text{Humidity, Wind, Temperature})$.
Calculating information gain with lookahead

Using the tree from the previous slide:

\[ H_D(Y \mid \text{Humidity}, \text{Wind}, \text{Temperature}) = \frac{5}{23} H_D(Y \mid \text{Humidity} = \text{high}, \text{Wind} = \text{strong}) + \]
\[ \frac{9}{23} H_D(Y \mid \text{Humidity} = \text{high}, \text{Wind} = \text{weak}) + \]
\[ \frac{4}{23} H_D(Y \mid \text{Humidity} = \text{low}, \text{Temperature} = \text{high}) + \]
\[ \frac{5}{23} H_D(Y \mid \text{Humidity} = \text{low}, \text{Temperature} = \text{low}) \]

\[ H_D(Y \mid \text{Humidity} = \text{high}, \text{Wind} = \text{strong}) = -\frac{2}{5} \log\left(\frac{2}{5}\right) - \frac{3}{5} \log\left(\frac{3}{5}\right) \]

...
Comments on decision tree learning

- widely used approach
- many variations
- fast in practice
- provides humanly comprehensible models when trees not too big
- insensitive to monotone transformations of numeric features
- standard methods learn axis-parallel hypotheses
- standard methods not suited to on-line setting
- usually not among most accurate learning methods

* although variants exist that are exceptions to this