

HOMework 2: DECISION TREES

10-601 Introduction to Machine Learning (Spring 2018)

Carnegie Mellon University

<https://piazza.com/cmu/spring2018/10601>

OUT: Jan 24, 2018*

DUE: Feb 05, 2018 11:59 PM

TAs: Bowei, Brynn, Mo, Soham

Summary It's time to build your first end-to-end learning system! In this assignment, you will build a Decision Tree classifier and apply it to several binary classification problems. This assignment consists of several parts: In Section 1.1, you will work through some Information Theory basics in order to “learn” a Decision Tree on paper. Then in Section 2, you will implement Decision Tree learning, prediction, and evaluation. Using that implementation, you will answer a few empirical questions in Section 1.2

START HERE: Instructions

- **Collaboration Policy:** Collaboration on solving the homework is allowed, after you have thought about the problems on your own. It is also OK to get clarification (but not solutions) from books or online resources, again after you have thought about the problems on your own. There are two requirements: first, cite your collaborators fully and completely (e.g., “Jane explained to me what is asked in Question 3.4”). Second, write your solution *independently*: close the book and all of your notes, and send collaborators out of the room, so that the solution comes from you only. See the collaboration policy on the website for more information: <http://www.cs.cmu.edu/~mgormley/courses/10601-s18/about.html>
- **Late Submission Policy:** See the late submission policy here: <http://www.cs.cmu.edu/~mgormley/courses/10601-s18/about.html>
- **Submitting your work:** You will use Gradescope to submit answers to all questions, and Autolab to submit your code. Please follow instructions at the end of this PDF to correctly submit all your code to Autolab.
 - **Gradescope:** For written problems such as derivations, proofs, or plots we will be using Gradescope (<https://gradescope.com/>). Submissions can be handwritten, but should be labeled and clearly legible. If your writing is not legible, you will not be awarded marks. Alternatively, submissions can be written in LaTeX. Upon submission, label each question using the template provided. Regrade requests can be made, however this gives the TA the opportunity to regrade your entire paper, meaning if additional mistakes are found then points will be deducted. Each derivation/proof should be completed on a separate page.

*Compiled on Friday 26th January, 2018 at 01:51

- **Autolab:** You will submit your code for programming questions on the homework to Autolab (<https://autolab.andrew.cmu.edu/>). After uploading your code, our grading scripts will autograde your assignment by running your program on a virtual machine (VM). The software installed on the VM is identical to that on `linux.andrew.cmu.edu`, so you should check that your code runs correctly there. If developing locally, check that the version number of the programming language environment (e.g. Python 2.7, Octave 3.8.2, OpenJDK 1.8.0, g++ 4.8.5) and versions of permitted libraries (e.g. `numpy` 1.7.1) match those on `linux.andrew.cmu.edu`. (Octave users: Please make sure you do not use any Matlab-specific libraries in your code that might make it fail against our tests.) You have a **total of 10 Autolab submissions**. Use them wisely. In order to not waste Autolab submissions, we recommend debugging your implementation on your local machine (or the linux servers) and making sure your code is running correctly first before any Autolab submission.
- **Materials:** Download from autolab the tar file ("Download handout"). The tar file will contain all the data that you will need in order to complete this assignment.

1 Written Questions [20pts]

Answer the following questions in the HW2 solutions template provided. Then upload your solutions to Gradescope.

1.1 Warm-up

First, let's think a little bit about decision trees. The following dataset consists of 7 examples, each with 3 attributes, (A, B, C) , and a label, Y .

A	B	C	Y
1	1	0	0
1	1	2	1
1	0	0	1
1	1	2	1
0	0	2	0
0	1	1	0
0	0	0	0

Use the data above to answer the following questions.

A few important notes:

- *All calculations should be done without rounding!* After you have finished all of your calculations, write your rounded solutions in the boxes below.
- Note that, throughout this homework, we will use the convention that the leaves of the trees do not count as nodes, and as such are not included in calculations of depth and number of splits. (For example, a tree which classifies the data based on the value of a single attribute will have depth 1, and contain 1 split.)

1. What is the entropy of Y in bits, $H(Y)$? In this and subsequent questions, when we request the units in *bits*, this simply means that you need to use log base 2 in your calculations.¹ (Please include one number rounded to the fourth decimal place, e.g. 0.1234)
2. What is the mutual information² of Y and A in bits, $I(Y; A)$? (Please include one number rounded to the fourth decimal place, e.g. 0.1234)
3. What is the mutual information of Y and B in bits, $I(Y; B)$? (Please include one number rounded to the fourth decimal place, e.g. 0.1234)
4. What is the mutual information of Y and B in bits, $I(Y; C)$? (Please include one number rounded to the fourth decimal place, e.g. 0.1234)
5. Consider the dataset given above. Which attribute (A , B , or C) would a decision tree algorithm pick first to branch on, if its splitting criterion is mutual information?

¹If instead you used log base e , the units would be *nats*; log base 10 gives *bats*.

²In the context of decision trees, and therefore in this assignment, the terms “information gain” and “mutual information” are synonymous (e.g. they have the same meaning as one another). However, in information theory and machine learning in general, “information gain” is synonymous with “Kullback-Leibler (K-L) divergence”, often referred to as relative entropy, which is not the same as mutual information. For more information, go [here](#).

6. Consider the dataset given above. Which is the second attribute you would pick to branch on, if its splitting criterion is mutual information? (*Hint*: Notice that this question correctly presupposes that there is *exactly one* second attribute.)
7. If the same algorithm continues until the tree perfectly classifies the data, what would the depth of the tree be?
8. Draw your completed Decision Tree. Label the non-leaf nodes with which attribute the tree will split on (e.g. B), the edges with the value of the attribute (e.g. 1 or 0), and the leaf nodes with the classification decision (e.g. $Y = 0$).

1.2 Empirical Questions

The following questions should be completed as you work through the programming portion of this assignment (Section 2).

9. Train and test your decision tree on the politician dataset and the education dataset with four different values of max-depth, $\{0, 1, 2, 4\}$. Report your findings in the HW2 solutions template provided. A Decision Tree with max-depth 0 is simply a *majority vote classifier*; a Decision Tree with max-depth 1 is called a *decision stump*. If desired, you could even check that your answers for these two simple cases are correct using your favorite spreadsheet application (e.g. Excel, Google Sheets).

Dataset	Max-Depth	Train Error	Test Error
politician	0		
politician	1		
politician	2		
politician	4		
education	0		
education	1		
education	2		
education	4		

10. For the politicians dataset, create a plot showing error on the y-axis against depth of the tree on the x-axis. Plot *both* training error and testing error, clearly labeling which is which. That is, for each possible value of max-depth ($0, 1, 2, \dots$, up to the number of attributes in the dataset), you should train a decision tree and report train/test error of the model's predictions.
11. Suppose your research advisor asks you to run some model selection experiments and then report your results. You select the Decision Tree model's max-depth to be the one with lowest test error in metrics.txt and then report that model's test error as the performance of our classifier on held out data. Is this a good experimental setup? If so, what is the name for this type of model selection? If not, why not?
12. In this assignment, we used max-depth as our stopping criterion, and as a mechanism to prevent overfitting. Alternatively, we could stop splitting a node whenever the mutual information for the best attribute is lower than a threshold value. This threshold would be another hyperparameter. How would this threshold value affect the number of nodes and depth of the learned trees? In a practical setting, how would you choose this parameter?
13. Print the decision tree which is produced by your algorithm for the politician data with max depth 3. Instructions on how to print the tree could be found in section 2.3.4.

14. After you have completed all other components of this assignment, report your answers to the collaboration policy questions detailed in the Academic Integrity Policies found [here](#). (a) Did you receive any help whatsoever from anyone in solving this assignment? Is so, include full details. (b) Did you give any help whatsoever to anyone in solving this assignment? Is so, include full details? (c) Did you find or come across code that implements any part of this assignment ? If so, include full details.

2 Programming

Your goal in this assignment is to implement a binary classifier, entirely from scratch—specifically a Decision Tree learner. In addition, we will ask you to run some end-to-end experiments on two tasks (predicting the party of a politician / predicting final grade for high school students) and report your results. You will write two programs: `inspect.{py|java|cpp|m}` (Section 2.2) and `decisionTree.{py|java|cpp|m}` (Section 2.3). The programs you write will be automatically graded using the Autolab system. You may write your programs in **Octave**, **Python**, **Java**, or **C++**. However, you should use the same language for all parts below.

2.1 The Tasks and Datasets

Materials Download the tar file from Autolab ("Download handout"). The tar file will contain all the data that you will need in order to complete this assignment.

Datasets The handout contains three datasets. Each one contains attributes and labels and is already split into training and testing data. The first line of each `.csv` file contains the name of each attribute, and *the class is always the last column*.

1. **politician:** The first task is to predict whether a US politician is a member of the Democrat or Republican party, based on their past voting history. Attributes (aka. features) are short descriptions of bills that were voted on, such as *Aid_to_nicaraguan_contras* or *Duty_free_exports*. Values are given as 'y' for yes votes and 'n' for no votes. The training data is in `politicians_train.csv`, and the test data in `politicians_test.csv`.
2. **education:** The second task is to predict the final *grade* (A, not A) for high school students. The attributes (covariates, predictors) are student grades on 5 multiple choice assignments *M1* through *M5*, 4 programming assignments *P1* through *P4*, and the final exam *F*. The training data is in `education_train.csv`, and the test data in `education_test.csv`.
3. **small:** We also include `small_train.csv` and `small_test.csv`—a small, purely for demonstration version of the politicians dataset, with *only* attributes *Anti_satellite_test_ban* and *Export_south_africa*. For this small dataset, the handout tar file also contains the predictions from a reference implementation of a Decision Tree with max-depth 3 (see `small_3_train.labels`, `small_3_test.labels`, `small_3_metrics.txt`). You can check your own output against these to see if your implementation is correct.³

Note: For simplicity, all attributes are discretized into just two categories (i.e. each node will have at most two descendents). This applies to all the datasets in the handout, as well as the additional datasets on which we will evaluate your Decision Tree.

³Yes, you read that correctly: we are giving you the correct answers.

2.2 Program #1: Inspecting the Data [5pts]

Write a program `inspect.{py|java|cpp|m}` to calculate the label entropy at the root (i.e. the entropy of the labels before any splits) and the error rate (the percent of incorrectly classified instances) of classifying using a majority vote (picking the label with the most examples). You do not need to look at the values of any of the attributes to do these calculations, knowing the labels of each example is sufficient. Entropy should be calculated in bits using log base 2.

Command Line Arguments The autograder runs and evaluates the output from the files generated, using the following command:

```
For Python: $ python inspect.py <input> <output>
For Java:   $ java inspect.java <input> <output>
For C++:    $ g++ inspect.cpp; ./a.out <input> <output>
For Octave: $ octave -qH inspect.m <input> <output>
```

Your program should accept two command line arguments: an input file and an output file. It should read the `.csv` input file (of the format described in Section 2.1), compute the quantities above, and write them to the output file so that it contains:

```
entropy: <entropy value>
error: <error value>
```

Example For example, suppose you wanted to inspect the file `small_train.csv` and write out the results to `small_inspect.txt`. For Python, you would run the command below:

```
$ python inspect.py small_train.csv small_inspect.txt
```

Afterwards, your output file `small_inspect.txt` should contain the following:

```
entropy: 0.996316519559
error: 0.464285714286
```

Our autograder will run your program on several input datasets to check that it correctly computes entropy and error, and will take minor differences due to rounding into account.

For your own records, run your program on each of the datasets provided in the handout—this error rate for a majority vote classifier is a baseline over which we would (ideally) like to improve.

2.3 Program #2: Decision Tree Learner [75pts]

In `decisionTree.{py | java | cpp | m}`, implement a Decision Tree learner. This file should learn a decision tree with a specified maximum depth, print the decision tree in a specified format, predict the labels of the training and testing examples, and calculate training and testing errors.

Your implementation must satisfy the following requirements:

- Use mutual information to determine which attribute to split on.
- Be sure you're correctly weighting your calculation of mutual information. For a split on attribute X , $I(Y; X) = H(Y) - H(Y|X) = H(Y) - P(X = 0)H(Y|X = 0) - P(X = 1)H(Y|X = 1)$. Equivalently, you can calculate $I(Y; X) = H(Y) + H(X) - H(Y, X)$.
- As a stopping rule, only split on an attribute if the mutual information is > 0 .
- Do not grow the tree beyond a max-depth specified on the command line. For example, for a maximum depth of 3, split a node only if the mutual information is > 0 and the current level of the node is < 3 .
- Use a majority vote of the labels at each leaf to make classification decisions.
- Do not hard-code any aspects of the datasets into your code. We will autograde your programs on two (hidden) datasets that include different attributes and output labels.

Careful planning will help you to correctly and concisely implement your Decision Tree learner. Here are a few *hints* to get you started:

- Write helper functions to calculate entropy and mutual information.
- Write a function to train a stump (tree with only one level). Then call that function recursively to create the sub-trees.
- In the recursion, keep track of the depth of the current tree so you can stop growing the tree beyond the max-depth.
- Implement a function that takes a learned decision tree and data as inputs, and generates predicted labels. You can write a separate function to calculate the error of the predicted labels with respect to the given (ground-truth) labels.
- Be sure to correctly handle the case where the specified maximum depth is greater than the total number of attributes.
- Be sure to handle the case where max-depth is zero (i.e. a majority vote classifier).

2.3.1 Command Line Arguments

The autograder runs and evaluates the output from the files generated, using the following command:

For Python:	<code>\$ python decisionTree.py [args...]</code>
For Java:	<code>\$ java decisionTree.java [args...]</code>
For C++:	<code>\$ g++ decisionTree.cpp; ./a.out [args...]</code>
For Octave:	<code>\$ octave -qH decisionTree.m [args...]</code>

Where above `[args...]` is a placeholder for six command-line arguments: `<train input>` `<test input>` `<max depth>` `<train out>` `<test out>` `<metrics out>`. These arguments are described in detail below:

1. `<train input>`: path to the training input `.csv` file (see Section 2.1)
2. `<test input>`: path to the test input `.csv` file (see Section 2.1)
3. `<max depth>`: maximum depth to which the tree should be built
4. `<train out>`: path of output `.labels` file to which the predictions on the *training* data should be written (see Section 2.3.2)
5. `<test out>`: path of output `.labels` file to which the predictions on the *test* data should be written (see Section 2.3.2)
6. `<metrics out>`: path of the output `.txt` file to which metrics such as train and test error should be written (see Section 2.3.3)

As an example, if you implemented your program in Python, the following command line would run your program on the politicians dataset and learn a tree with max-depth of two. The train predictions would be written to `pol_2_train.labels`, the test predictions to `pol_2_test.labels`, and the metrics to `pol_2_metrics.txt`.

```
$ python decisionTree.py politicians_train.csv politicians_test.csv \
  2 pol_2_train.labels pol_2_test.labels pol_2_metrics.txt
```

The following example would run the same learning setup except with max-depth three, and conveniently writing to analogously named output files, so you can compare the two runs.

```
$ python decisionTree.py politicians_train.csv politicians_test.csv \
  3 pol_3_train.labels pol_3_test.labels pol_3_metrics.txt
```

2.3.2 Output: Labels Files

Your program should write two output `.labels` files containing the predictions of your model on training data (`<train out>`) and test data (`<test out>`). Each should contain the predicted labels for each example printed on a new line. Use `'\n'` to create a new line.

Your labels should exactly match those of a reference decision tree implementation—this will be checked by the autograder by running your program and evaluating your output file against the reference solution.

Note: You should output your predicted labels using the same string identifiers as the original training data: e.g., for the politicians dataset you should output `democrat/republican` and for the education dataset you should output `A/notA`. The first few lines of an example output file is given below for the politician dataset:

```
democrat
democrat
democrat
republican
democrat
...
```

2.3.3 Output: Metrics File

Generate another file where you should report the training error and testing error. This file should be written to the path specified by the command line argument `<metrics out>`. Your reported numbers should be within 0.01 of the reference solution. The file should be formatted as follows:

```
error(train): 0.3076532
error(test): 0.4523292
```

2.3.4 Output: Printing the Tree

Finally, you should write a function to pretty-print your learned decision tree. (You may find it more convenient to print the tree *as* you are learning it.) Each row should correspond to a node in the tree. They should be printed in a *depth-first-search* order. Print the attribute of the node's parent and the attribute value corresponding to the node. Also include the sufficient statistics (i.e. count of positive / negative examples) for the data passed to that node. The row for the root should include *only* those sufficient statistics. A node at depth d , should be prefixed by d copies of the string `'| '`.

Below, we have provided the recommended format for printing the tree (example for python). You can print it directly to standard out rather than to a file. **This functionality of your program will not be autograded.**

```
$ python decisionTree.py small_train.csv small_test.csv 2 \
small_2_train.labels small_2_test.labels small_2_metrics.txt

[15 democrat /13 republican]
| Anti_satellite_test_ban = y: [13 democrat /1 republican]
| | Export_south_africa = y: [13 democrat /0 republican]
| | Export_south_africa = n: [0 democrat /1 republican]
| Anti_satellite_test_ban = n: [2 democrat /12 republican]
| | Export_south_africa = y: [2 democrat /7 republican]
| | Export_south_africa = n: [0 democrat /5 republican]
```

However, you should be careful that the tree might not be full. For example, after swapping the train/test files in the example above, you could end up with a tree like the following.

```
$ python decisionTree.py small_test.csv small_train.csv 2 \
swap_2_train.labels swap_2_test.labels swap_2_metrics.txt

[13 democrat/15 republican]
| Anti_satellite_test_ban = y: [9 democrat/0 republican]
| Anti_satellite_test_ban = n: [4 democrat/15 republican]
| | Export_south_africa = y: [4 democrat/10 republican]
| | Export_south_africa = n: [0 democrat/5 republican]
```

The following pretty-print shows the education dataset with max-depth 3. Use this example to check your code before submitting your pretty-print of the politics dataset (asked in question 13 of the Empirical questions).

```
$ python decisionTree.py education_train.csv education_test.csv 3 \
edu_3_train.labels edu_3_test.labels edu_3_metrics.txt
```

```

[135 A/65 notA]
| F = A: [119 A/23 notA]
| | M4 = A: [56 A/2 notA]
| | | P1 = A: [41 A/0 notA]
| | | P1 = notA: [15 A/2 notA]
| | M4 = notA: [63 A/21 notA]
| | | M2 = A: [37 A/3 notA]
| | | M2 = notA: [26 A/18 notA]
| F = notA: [16 A/42 notA]
| | M2 = A: [13 A/15 notA]
| | | M4 = A: [6 A/1 notA]
| | | M4 = notA: [7 A/14 notA]
| | M2 = notA: [3 A/27 notA]
| | | M4 = A: [3 A/5 notA]
| | | M4 = notA: [0 A/22 notA]

```

The numbers in brackets give the number of positive and negative labels from the training data in that part of the tree.

At this point, you should be able to go back and answer questions 9-13 in the "Written Questions" section of this handout. Write your solutions in the template provided.

2.3.5 Evaluation

In addition to the politician and education datasets, Autolab will test your code on two more datasets, which will not be shown to you. One set contains information about various cars, and whether or not consumers decided to buy them. The other contains data about songs, and whether or not they became top hits. The data will be in .csv files formatted like the ones provided, again with the class as the last column. Shown below are the attributes and the values they can take:

Music data:

- Attribute:year('before1950' or 'after1950')
- Attribute:solo('yes' or 'no')
- Attribute:vocal('yes' or 'no')
- Attribute:length('morethan3min' or 'lessthan3min')
- Attribute:original('yes' or 'no')
- Attribute:tempo('fast' or 'slow')
- Attribute:folk('yes' or 'no')
- Attribute:classical('yes' or 'no')
- Attribute:rhythm('yes' or 'no')
- Attribute:jazz('yes' or 'no')

- `Attribute:rock('yes'or'no')`
- `Class Label:hit('yes'or'no')`

Cars data:

- `Attribute:buying('expensive'or'cheap')`
- `Attribute:maint('high'or'low')`
- `Attribute:doors('Two'or'MoreThanTwo')`
- `Attribute:length('morethan3min'or'lessthan3min')`
- `Attribute:person('Two'or'MoreThanTwo')`
- `Attribute:boot('large'or'small')`
- `Attribute:safety('high'or'low')`
- `Class Label:class('yes'or'no')`

Please ensure your solution can handle data with these values.

2.4 Submission Instructions

Programming Please ensure you have completed the following files for submission.

```
inspect.{py|java|cpp|m}  
decisionTree.{py|java|cpp|m}
```

When submitting your solution, compress the two files listed above containing your implementation into a tar `handin.tar` by running:

```
$ tar -cvf handin.tar *.{py|java|cpp|m}
```

DO NOT put the above files in a folder and then tar that folder. You must compress the files directly into a tar file and submit it to Autolab. **Note:** Please make sure the programming language that you use is consistent within this assignment (e.g. don't use C++ for `inspect` and Python for `decisionTree`).

Written Questions Make sure you have completed all questions from Section 1 (including the collaboration policy questions) in the template provided. When you have done so, please submit your document in **pdf format** to the corresponding assignment slot on Gradescope.