Plagiarism Detection Model

Now that you've created training and test data, you are ready to define and train a model. Your goal in this notebook, will be to train a binary classification model that learns to label an answer file as either plagiarized or not, based on the features you provide the model.

This task will be broken down into a few discrete steps:

- Upload your data to S3.
- Define a binary classification model and a training script.
- · Train your model and deploy it.
- Evaluate your deployed classifier and answer some questions about your approach.

To complete this notebook, you'll have to complete all given exercises and answer all the questions in this notebook.

All your tasks will be clearly labeled **EXERCISE** and questions as **QUESTION**.

It will be up to you to explore different classification models and decide on a model that gives you the best performance for this dataset.

Load Data to S3

In the last notebook, you should have created two files: a training.csv and test.csv file with the features and class labels for the given corpus of plagiarized/non-plagiarized text data.

The below cells load in some AWS SageMaker libraries and creates a default bucket. After creating this bucket, you can upload your locally stored data to S3.

Save your train and test .csv feature files, locally. To do this you can run the second notebook "2_Plagiarism_Feature_Engineering" in SageMaker or you can manually upload your files to this notebook using the upload icon in Jupyter Lab. Then you can upload local files to S3 by using sagemaker_session.upload_data and pointing directly to where the training data is saved.

```
In [1]:
```

```
import pandas as pd
import boto3
import sagemaker
import os
```

In [2]:

```
"""
DON'T MODIFY ANYTHING IN THIS CELL THAT IS BELOW THIS LINE
"""

# session and role
sagemaker_session = sagemaker.Session()
role = sagemaker.get_execution_role()

# create an S3 bucket
bucket = sagemaker_session.default_bucket()
```

EXERCISE: Upload your training data to S3

Specify the data_dir where you've saved your train.csv file. Decide on a descriptive prefix that defines where your data will be uploaded in the default S3 bucket. Finally, create a pointer to your training data by calling sagemaker_session.upload_data and passing in the required parameters. It may help to look at the <u>Session documentation</u>

(https://sagemaker.readthedocs.io/en/stable/session.html#sagemaker.session.Session.upload_data) or previous SageMaker code examples.

You are expected to upload your entire directory. Later, the training script will only access the train.csv file.

In [3]:

```
# should be the name of directory you created to save your features data
data_dir = 'plagiarism_data'

# set prefix, a descriptive name for a directory
prefix = 'plagiarism-data'

# upload all data to S3
s3_test_data = sagemaker_session.upload_data(os.path.join(data_dir, 'test.csv'),
key_prefix=prefix)
s3_train_data = sagemaker_session.upload_data(os.path.join(data_dir, 'train.csv'),
key_prefix=prefix)
```

Test cell

Test that your data has been successfully uploaded. The below cell prints out the items in your S3 bucket and will throw an error if it is empty. You should see the contents of your data_dir and perhaps some checkpoints. If you see any other files listed, then you may have some old model files that you can delete via the S3 console (though, additional files shouldn't affect the performance of model developed in this notebook).

```
In [4]:
```

```
"""
DON'T MODIFY ANYTHING IN THIS CELL THAT IS BELOW THIS LINE
"""
# confirm that data is in S3 bucket
empty_check = []
for obj in boto3.resource('s3').Bucket(bucket).objects.all():
    empty_check.append(obj.key)
    print(obj.key)

assert len(empty_check) !=0, 'S3 bucket is empty.'
print('Test passed!')
```

plagiarism-data/test.csv
plagiarism-data/train.csv
Test passed!

Modeling

Now that you've uploaded your training data, it's time to define and train a model!

The type of model you create is up to you. For a binary classification task, you can choose to go one of three routes:

- Use a built-in classification algorithm, like LinearLearner.
- Define a custom Scikit-learn classifier, a comparison of models can be found https://scikit-learn.org/stable/auto-examples/classification/plot-classifier-comparison.html).
- Define a custom PyTorch neural network classifier.

It will be up to you to test out a variety of models and choose the best one. Your project will be graded on the accuracy of your final model.

EXERCISE: Complete a training script

To implement a custom classifier, you'll need to complete a train.py script. You've been given the folders source_sklearn and source_pytorch which hold starting code for a custom Scikit-learn model and a PyTorch model, respectively. Each directory has a train.py training script. To complete this project you only need to complete one of these scripts; the script that is responsible for training your final model.

A typical training script:

- · Loads training data from a specified directory
- Parses any training & model hyperparameters (ex. nodes in a neural network, training epochs, etc.)
- · Instantiates a model of your design, with any specified hyperparams
- · Trains that model
- Finally, saves the model so that it can be hosted/deployed, later

Defining and training a model

Much of the training script code is provided for you. Almost all of your work will be done in the if __name__ == '__main__': section. To complete a train.py file, you will:

- 1. Import any extra libraries you need
- 2. Define any additional model training hyperparameters using parser.add_argument
- 3. Define a model in the if __name__ == '__main__': section
- 4. Train the model in that same section

Below, you can use !pygmentize to display an existing train.py file. Read through the code; all of your tasks are marked with TODO comments.

Note: If you choose to create a custom PyTorch model, you will be responsible for defining the model in the model.py file, and a predict.py file is provided. If you choose to use Scikit-learn, you only need a train.py file; you may import a classifier from the sklearn library.

In [5]:

directory can be changed to: source_sklearn or source_pytorch
!pygmentize source_sklearn/train.py

```
from __future__ import print function
import <u>argparse</u>
import os
import pandas as pd
from sklearn.externals import joblib
## TODO: Import any additional libraries you need to define a model
from sklearn.ensemble import GradientBoostingClassifier
# Provided model load function
def model fn(model dir):
    """Load model from the model_dir. This is the same model that is
    in the main if statement.
    print("Loading model.")
    # load using joblib
    model = joblib.load(os.path.join(model dir, "model.joblib"))
    print("Done loading model.")
    return model
## TODO: Complete the main code
if name == ' main ':
    # All of the model parameters and training parameters are sent a
s arguments
    # when this script is executed, during a training job
    # Here we set up an argument parser to easily access the paramet
ers
    parser = argparse.ArgumentParser()
    # SageMaker parameters, like the directories for training data a
nd saving models; set automatically
    # Do not need to change
    parser.add_argument('--output-data-dir', type=str, default=os.en
viron['SM OUTPUT DATA DIR'])
    parser.add argument('--model-dir', type=str, default=os.environ[
'SM MODEL DIR'])
    parser.add argument('--data-dir', type=str, default=os.environ['
SM CHANNEL TRAIN'])
    ## TODO: Add any additional arguments that you will need to pass
into your model
    parser.add argument('--n estimators', type=int, default=100)
    parser.add_argument('--learning_rate', type=float, default=1.0)
    parser.add_argument('--max_depth', type=int, default=1)
    parser.add argument('--random state', type=int, default=0)
    # args holds all passed-in arguments
    args = parser.parse args()
    # Read in csv training file
    training dir = args.data dir
    train_data = pd.read_csv(os.path.join(training_dir, "train.csv"
), header=None, names=None)
```

```
# Labels are in the first column
train y = train data.iloc[:,0]
train_x = train_data.iloc[:,1:]
## --- Your code here --- ##
# Extract hyperparameters
n estimators = args.n estimators
learning rate = args.learning rate
max depth = args.max depth
random state = args.random state
## TODO: Define a model
model = GradientBoostingClassifier(n_estimators=n_estimators,
                                   learning rate=learning rate,
                                   max depth=max depth,
                                   random state=random state)
## TODO: Train the model
model = model.fit(train x, train y)
## --- End of your code --- ##
# Save the trained model
joblib.dump(model, os.path.join(args.model dir, "model.joblib"))
```

Provided code

If you read the code above, you can see that the starter code includes a few things:

- Model loading (model fn) and saving code
- · Getting SageMaker's default hyperparameters
- Loading the training data by name, train.csv and extracting the features and labels, $train_x$, and $train_y$

If you'd like to read more about model saving with joblib for sklearn (https://scikit-learn.org/stable/modules/model_persistence.html) or with torch.save (https://pytorch.org/tutorials/beginner/saving_loading_models.html), click on the provided links.

Create an Estimator

When a custom model is constructed in SageMaker, an entry point must be specified. This is the Python file which will be executed when the model is trained; the train.py function you specified above. To run a custom training script in SageMaker, construct an estimator, and fill in the appropriate constructor arguments:

- entry_point: The path to the Python script SageMaker runs for training and prediction.
- source_dir: The path to the training script directory source sklearn OR source pytorch.
- role: Role ARN, which was specified, above.
- train_instance_count: The number of training instances (should be left at 1).
- train_instance_type: The type of SageMaker instance for training. Note: Because Scikit-learn does not natively support GPU training, Sagemaker Scikit-learn does not currently support training on GPU instance types.
- sagemaker_session: The session used to train on Sagemaker.
- hyperparameters (optional): A dictionary { 'name':value, ..} passed to the train function as hyperparameters.

Note: For a PyTorch model, there is another optional argument **framework_version**, which you can set to the latest version of PyTorch, 1.0.

EXERCISE: Define a Scikit-learn or PyTorch estimator

To import your desired estimator, use one of the following lines:

```
from sagemaker.sklearn.estimator import SKLearn
from sagemaker.pytorch import PyTorch
```

```
In [6]:
```

```
# your import and estimator code, here
from sagemaker.sklearn.estimator import SKLearn
```

EXERCISE: Train the estimator

Train your estimator on the training data stored in S3. This should create a training job that you can monitor in your SageMaker console.

In [7]:

```
%%time
# Reference: https://github.com/awslabs/amazon-sagemaker-examples/blob/master/sa
gemaker-python-sdk/scikit learn iris/Scikit-learn%20Estimator%20Example%20With%2
OBatch%20Transform.ipynb
# Train your estimator on S3 training data
script_path = 'source_sklearn/train.py'
# Load the model
model = SKLearn(
   entry_point=script_path,
   role=role,
   train_instance_count=1,
   train instance type="ml.m4.xlarge",
   sagemaker session=sagemaker session,
   hyperparameters={'n_estimators':100, 'learning_rate':1.0, 'max_depth':1, 'ra
ndom_state':0})
# Train the model
model.fit({'train': s3 train data})
```

```
2020-05-17 09:43:40 Starting - Starting the training job...
2020-05-17 09:43:42 Starting - Launching requested ML instance
2020-05-17 09:44:44 Starting - Preparing the instances for trainin
2020-05-17 09:45:27 Downloading - Downloading input data...
2020-05-17 09:45:59 Training - Downloading the training image..2020-
05-17 09:46:19,621 sagemaker-containers INFO
                                                Imported framework
sagemaker sklearn container.training
2020-05-17 09:46:19,624 sagemaker-containers INFO
                                                      No GPUs detect
ed (normal if no gpus installed)
2020-05-17 09:46:19,637 sagemaker sklearn container.training INFO
Invoking user training script.
2020-05-17 09:46:19,906 sagemaker-containers INFO
                                                      Module train d
oes not provide a setup.py.
Generating setup.py
2020-05-17 09:46:19,906 sagemaker-containers INFO
                                                      Generating set
up.cfq
2020-05-17 09:46:19,907 sagemaker-containers INFO
                                                      Generating MAN
IFEST.in
2020-05-17 09:46:19,907 sagemaker-containers INFO
                                                      Installing mod
ule with the following command:
/miniconda3/bin/python -m pip install .
Processing /opt/ml/code
Building wheels for collected packages: train
  Building wheel for train (setup.py): started
  Building wheel for train (setup.py): finished with status 'done'
  Created wheel for train: filename=train-1.0.0-pv2.pv3-none-anv.whl
size=6113 sha256=f44054c93ea6ff8ce7848b7f48de3bbc090168ff107940e295d
bleae22a36ccc
  Stored in directory: /tmp/pip-ephem-wheel-cache-xhn7_bpt/wheels/3
5/24/16/37574d11bf9bde50616c67372a334f94fa8356bc7164af8ca3
Successfully built train
Installing collected packages: train
Successfully installed train-1.0.0
2020-05-17 09:46:21,442 sagemaker-containers INFO
                                                      No GPUs detect
ed (normal if no gpus installed)
2020-05-17 09:46:21,455 sagemaker-containers INFO
                                                      Invoking user
script
Training Env:
{
    "additional framework parameters": {},
    "channel input dirs": {
        "train": "/opt/ml/input/data/train"
    "current host": "algo-1",
    "framework module": "sagemaker sklearn container.training:main",
    "hosts": [
        "algo-1"
    "hyperparameters": {
        "max depth": 1,
        "n estimators": 100,
        "random state": 0,
        "learning rate": 1.0
    "input config dir": "/opt/ml/input/config",
    "input data config": {
        "train": {
```

```
"TrainingInputMode": "File",
            "S3DistributionType": "FullyReplicated",
            "RecordWrapperType": "None"
        }
    "input dir": "/opt/ml/input",
    "is master": true,
    "job name": "sagemaker-scikit-learn-2020-05-17-09-43-40-180",
    "log level": 20,
    "master hostname": "algo-1",
    "model_dir": "/opt/ml/model",
    "module dir": "s3://sagemaker-eu-west-1-957610599433/sagemaker-s
cikit-learn-2020-05-17-09-43-40-180/source/sourcedir.tar.gz",
    "module name": "train",
    "network interface name": "eth0",
    "num cpus": 4,
    "num gpus": 0,
    "output data dir": "/opt/ml/output/data",
    "output dir": "/opt/ml/output",
    "output intermediate dir": "/opt/ml/output/intermediate",
    "resource config": {
        "current host": "algo-1",
        "hosts": [
            "algo-1"
        ],
        "network interface name": "eth0"
    "user entry point": "train.py"
}
Environment variables:
SM HOSTS=["algo-1"]
SM NETWORK INTERFACE NAME=eth0
SM HPS={"learning rate":1.0, "max depth":1, "n estimators":100, "random
state":0}
SM USER ENTRY POINT=train.py
SM FRAMEWORK PARAMS={}
SM RESOURCE CONFIG={"current host": "algo-1", "hosts": ["algo-1"], "netw
ork interface name":"eth0"}
SM INPUT DATA CONFIG={"train":{"RecordWrapperType":"None","S3Distrib
utionType":"FullyReplicated","TrainingInputMode":"File"}}
SM OUTPUT DATA DIR=/opt/ml/output/data
SM_CHANNELS=["train"]
SM CURRENT HOST=algo-1
SM MODULE NAME=train
SM LOG LEVEL=20
SM_FRAMEWORK_MODULE=sagemaker_sklearn_container.training:main
SM INPUT DIR=/opt/ml/input
SM_INPUT_CONFIG_DIR=/opt/ml/input/config
SM OUTPUT DIR=/opt/ml/output
SM NUM CPUS=4
SM NUM GPUS=0
SM MODEL DIR=/opt/ml/model
SM MODULE DIR=s3://sagemaker-eu-west-1-957610599433/sagemaker-scikit
-learn-2020-05-17-09-43-40-180/source/sourcedir.tar.gz
SM_TRAINING_ENV={"additional_framework_parameters":{}, "channel_input
dirs":{"train":"/opt/ml/input/data/train"}, "current host":"algo-
1", "framework module": "sagemaker sklearn container.training:main", "h
osts":["algo-1"], "hyperparameters":{"learning rate":1.0, "max depth":
1, "n_estimators":100, "random_state":0}, "input_config_dir":"/opt/ml/i
```

```
nput/config","input data config":{"train":{"RecordWrapperType":"Non
e", "S3DistributionType": "FullyReplicated", "TrainingInputMode": "Fil
e"}},"input dir":"/opt/ml/input","is master":true,"job name":"sagema
ker-scikit-learn-2020-05-17-09-43-40-180", "log_level":20, "master_hos
tname":"algo-1","model dir":"/opt/ml/model","module dir":"s3://sagem
aker-eu-west-1-957610599433/sagemaker-scikit-learn-2020-05-17-09-43-
40-180/source/sourcedir.tar.gz", "module_name": "train", "network_inter
face name": "eth0", "num cpus":4, "num gpus":0, "output data dir": "/opt/
ml/output/data", "output dir": "/opt/ml/output", "output intermediate d
ir":"/opt/ml/output/intermediate","resource config":{"current hos
t": "algo-1", "hosts": ["algo-1"], "network_interface_name": "eth0"}, "use
r entry point":"train.py"}
SM USER ARGS=["--learning rate","1.0","--max depth","1","--n estimat
ors","100","--random state","0"]
SM OUTPUT INTERMEDIATE DIR=/opt/ml/output/intermediate
SM CHANNEL TRAIN=/opt/ml/input/data/train
SM HP MAX DEPTH=1
SM HP N ESTIMATORS=100
SM_HP_RANDOM_STATE=0
SM HP LEARNING RATE=1.0
PYTHONPATH=/miniconda3/bin:/miniconda3/lib/python37.zip:/miniconda3/
lib/python3.7:/miniconda3/lib/python3.7/lib-dynload:/miniconda3/lib/
python3.7/site-packages
Invoking script with the following command:
/miniconda3/bin/python -m train --learning rate 1.0 --max depth 1 --
n_estimators 100 --random_state 0
/miniconda3/lib/python3.7/site-packages/sklearn/externals/joblib/ext
ernals/cloudpickle/cloudpickle.py:47: DeprecationWarning: the imp mo
dule is deprecated in favour of importlib; see the module's document
ation for alternative uses
  import imp
2020-05-17 09:46:22,793 sagemaker-containers INFO
                                                       Reporting trai
ning SUCCESS
2020-05-17 09:46:31 Uploading - Uploading generated training model
2020-05-17 09:46:31 Completed - Training job completed
Training seconds: 64
Billable seconds: 64
CPU times: user 368 ms, sys: 19.4 ms, total: 387 ms
Wall time: 3min 11s
```

EXERCISE: Deploy the trained model

After training, deploy your model to create a predictor. If you're using a PyTorch model, you'll need to create a trained PyTorchModel that accepts the trained <model>.model_data as an input parameter and points to the provided source pytorch/predict.py file as an entry point.

To deploy a trained model, you'll use <model>.deploy, which takes in two arguments:

- initial_instance_count: The number of deployed instances (1).
- **instance_type**: The type of SageMaker instance for deployment.

Note: If you run into an instance error, it may be because you chose the wrong training or deployment instance_type. It may help to refer to your previous exercise code to see which types of instances we used.

In [8]:

```
%%time

# uncomment, if needed
# from sagemaker.pytorch import PyTorchModel

# deploy your model to create a predictor
predictor = model.deploy(initial_instance_count=1, instance_type="ml.m4.xlarge")
-----!CPU times: user 222 ms, sys: 15.5 ms, total: 238 ms
Wall time: 7min 32s
```

Evaluating Your Model

Once your model is deployed, you can see how it performs when applied to our test data.

The provided cell below, reads in the test data, assuming it is stored locally in data_dir and named test.csv . The labels and features are extracted from the .csv file.

In [9]:

```
"""
DON'T MODIFY ANYTHING IN THIS CELL THAT IS BELOW THIS LINE
"""
import os

# read in test data, assuming it is stored locally
test_data = pd.read_csv(os.path.join(data_dir, "test.csv"), header=None, names=None)

# labels are in the first column
test_y = test_data.iloc[:,0]
test_x = test_data.iloc[:,1:]
```

EXERCISE: Determine the accuracy of your model

Use your deployed <code>predictor</code> to generate predicted, class labels for the test data. Compare those to the <code>true</code> labels, <code>test_y</code>, and calculate the accuracy as a value between 0 and 1.0 that indicates the fraction of test data that your model classified correctly. You may use sklearn.metrics (https://scikit-learn.org/stable/modules/classes.html#module-sklearn.metrics) for this calculation.

To pass this project, your model should get at least 90% test accuracy.

```
In [10]:
```

```
# First: generate predicted, class labels
test_y_preds = predictor.predict(test_x.values)

"""

DON'T MODIFY ANYTHING IN THIS CELL THAT IS BELOW THIS LINE
"""

# test that your model generates the correct number of labels
assert len(test_y_preds)==len(test_y), 'Unexpected number of predictions.'
print('Test passed!')
```

Test passed!

```
In [11]:
```

```
# Second: calculate the test accuracy
from sklearn.metrics import accuracy_score
accuracy = accuracy_score(test_y, test_y_preds)
print(accuracy)

## print out the array of predicted and true labels, if you want
print('\nPredicted class labels: ')
print(test_y_preds)
print('\nTrue class labels: ')
print(test_y.values)
```

```
0.96
```

```
Predicted class labels:
[1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 0 0]

True class labels:
[1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 0 0]
```

Question 1: How many false positives and false negatives did your model produce, if any? And why do you think this is?

Answer: we have one false positive for the 7th document. If we check the document features, it is indeed very low: (0.38095238095238093, 0.0, 0.3950617283950617).

The error seems to provide by the third feature (LCS) which is less than 0.4. But with just a value of 0.35 like in the 13th document, the model classify it correctly as true positive. We can presume here that the weight of the LCS feature is here too high compare to the other feature.

If we look to the corresponding answer document (g0pE_taskd.txt), we can see that the answer is quite short compare to the original source text, so the probability to find a LCS is higher.

Question 2: How did you decide on the type of model to use?

Answer: we already have make some assumptions during the feature engineering phase with the relation between containement/LCS features and the plagiarism probability. As we have seen, the more the features is closed to 1, the more the plagiarism is high. So, a linear pattern seems to exist and that why we can use a linear model. An ensemble classifier like GradientBoosting classifier is enough powerful without having to construct an entire neural network like PyTorch. More over, we have very few training sample here.

EXERCISE: Clean up Resources

After you're done evaluating your model, **delete your model endpoint**. You can do this with a call to .delete_endpoint() . You need to show, in this notebook, that the endpoint was deleted. Any other resources, you may delete from the AWS console, and you will find more instructions on cleaning up all your resources, below.

```
In [12]:
```

```
# uncomment and fill in the line below!
# <name_of_deployed_predictor>.delete_endpoint()
model.delete_endpoint()
```

Deleting S3 bucket

When you are *completely* done with training and testing models, you can also delete your entire S3 bucket. If you do this before you are done training your model, you'll have to recreate your S3 bucket and upload your training data again.

```
# deleting bucket, uncomment lines below
bucket_to_delete = boto3.resource('s3').Bucket(bucket)
bucket_to_delete.objects.all().delete()
```

```
Out[13]:
[{'ResponseMetadata': {'RequestId': '2FE3D7E8F9D61E20',
   'HostId': 'mAZF113LEtvsqu6yVEZzPCwAXlxqfDVv+RBbOHoBlNHPkRS2OzT0s/
LuRKxuXI2QWldpRv4zhj8=',
   'HTTPStatusCode': 200,
   'HTTPHeaders': {'x-amz-id-2': 'mAZF113LEtvsgu6yVEZzPCwAX1xqfDVv+R
BbOHoBlNHPkRS2OzT0s/LuRKxuXI2QWldpRv4zhj8=',
    'x-amz-request-id': '2FE3D7E8F9D61E20',
    'date': 'Sun, 17 May 2020 09:54:26 GMT',
    'connection': 'close',
    'content-type': 'application/xml',
    'transfer-encoding': 'chunked',
    'server': 'AmazonS3'},
   'RetryAttempts': 0},
  'Deleted': [{'Key': 'plagiarism-data/test.csv'},
   {'Key': 'sagemaker-scikit-learn-2020-05-17-09-43-40-180/output/mo
del.tar.gz'},
   {'Key': 'sagemaker-scikit-learn-2020-05-17-09-43-40-180/debug-out
put/training job end.ts'},
   {'Key': 'sagemaker-scikit-learn-2020-05-17-09-43-40-180/source/so
urcedir.tar.gz'},
   {'Key': 'plagiarism-data/train.csv'}]}]
```

Deleting all your models and instances

When you are *completely* done with this project and do **not** ever want to revisit this notebook, you can choose to delete all of your SageMaker notebook instances and models by following <u>these instructions</u> (https://docs.aws.amazon.com/sagemaker/latest/dg/ex1-cleanup.html). Before you delete this notebook instance, I recommend at least downloading a copy and saving it, locally.

Further Directions

There are many ways to improve or add on to this project to expand your learning or make this more of a unique project for you. A few ideas are listed below:

- Train a classifier to predict the category (1-3) of plagiarism and not just plagiarized (1) or not (0).
- Utilize a different and larger dataset to see if this model can be extended to other types of plagiarism.
- Use language or character-level analysis to find different (and more) similarity features.
- Write a complete pipeline function that accepts a source text and submitted text file, and classifies the submitted text as plagiarized or not.
- Use API Gateway and a lambda function to deploy your model to a web application.

These are all just options for extending your work. If you've completed all the exercises in this notebook, you've completed a real-world application, and can proceed to submit your project. Great job!